

Norbert Pohlmann

# Cyber-Sicherheit

Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung

**EXTRAS ONLINE**



Springer Vieweg

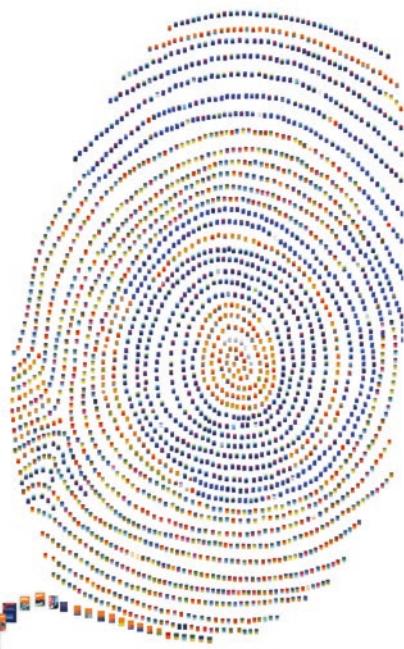
---

# Cyber-Sicherheit

# Lizenz zum Wissen.

Sichern Sie sich umfassendes Technikwissen mit Sofortzugriff auf tausende Fachbücher und Fachzeitschriften aus den Bereichen: Automobiltechnik, Maschinenbau, Energie + Umwelt, E-Technik, Informatik + IT und Bauwesen.

Exklusiv für Leser von Springer-Fachbüchern: Testen Sie Springer für Professionals 30 Tage unverbindlich. Nutzen Sie dazu im Bestellverlauf Ihren persönlichen Aktionscode **C0005406** auf [www.springerprofessional.de/buchaktion/](http://www.springerprofessional.de/buchaktion/)



Jetzt  
30 Tage  
testen!

**Springer für Professionals.**  
Digitale Fachbibliothek. Themen-Scout. Knowledge-Manager.

- ⌚ Zugriff auf tausende von Fachbüchern und Fachzeitschriften
- ⌚ Selektion, Komprimierung und Verknüpfung relevanter Themen durch Fachredaktionen
- ⌚ Tools zur persönlichen Wissensorganisation und Vernetzung

[www.entschieden-intelligenter.de](http://www.entschieden-intelligenter.de)

**Springer für Professionals**

 **Springer**

---

Norbert Pohlmann

# Cyber-Sicherheit

Das Lehrbuch für Konzepte, Prinzipien,  
Mechanismen, Architekturen  
und Eigenschaften von Cyber-  
Sicherheitssystemen in der  
Digitalisierung

Norbert Pohlmann  
Institut für Internet-Sicherheit  
Westfälische Hochschule  
Gelsenkirchen, Deutschland

Ergänzendes Material zu diesem Buch finden Sie auf <http://extras.springer.com>.

ISBN 978-3-658-25397-4      ISBN 978-3-658-25398-1 (eBook)  
<https://doi.org/10.1007/978-3-658-25398-1>

Die Deutsche Nationalbibliothek verzeichnetet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Springer Vieweg

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2019  
Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags.  
Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von allgemein beschreibenden Bezeichnungen, Marken, Unternehmensnamen etc. in diesem Werk bedeutet nicht, dass diese frei durch jedermann benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des jeweiligen Zeicheninhabers sind zu beachten.

Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag, noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature

Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

*Für Milla*

---

# Vorwort

Wir leben inmitten der Zeit des digitalen Wandels, der eine radikale Umgestaltung unseres Alltags und unserer Arbeitswelt sowie aller Geschäftsmodelle und Verwaltungsprozesse bedeutet.

Wirtschaftskraft und Wohlstand sowie die Leistungsfähigkeit unserer modernen Gesellschaft werden durch den gelungenen digitalen Wandel bestimmt.

**Nur mit angemessener Cyber-Sicherheit wird eine nachhaltige Digitalisierung gelingen!**

**Cyber-Sicherheit** – Das Lehrbuch für Architekturen, Konzepte, Prinzipien, Mechanismen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung – soll helfen, ein sicheres und vertrauenswürdiges Fundament für unsere digitale Zukunft zu schaffen.

Welchen Anspruch hat das Buch?

Das Lehrbuch Cyber-Sicherheit verfolgt das Anliegen, dem Leser eine fundierte und anwendungsorientierte Einführung in das Themenfeld Cyber-Sicherheit zu geben. Es werden Cyber-Sicherheitsarchitekturen vermittelt, die aufzeigen, wie zukünftige IT-Systeme besser aufgebaut werden können. Das Lehrbuch behandelt Cyber-Sicherheitskonzepte, die dabei unterstützen, einen angemessenen Level an Cyber-Sicherheit in der sich immer schneller verändernden Gesellschaft zur Verfügung zu stellen. Die Diskussion von Cyber-Sicherheitsprinzipien soll dazu dienen, sich in der komplexen Welt der Cyber-Sicherheit zurechtzufinden. Cyber-Sicherheitsmechanismen werden als Basisinstrumente ausführlich behandelt, weil sie die Grundlage eines Cyber-Sicherheitssystems sind. Aber auch die Cyber-Sicherheitseigenschaften werden aufgezeigt, um Wirksamkeit und weitere Aspekte von Cyber-Sicherheitslösungen beurteilen zu können.

Dabei wird der Schwerpunkt auf exemplarisches Lernen gelegt, weil der Stoff zu mächtig ist, um vollständig behandelt zu werden. Es werden die wichtigen Aspekte der Cyber-Sicherheit als Grundlage mit exemplarischen Beispielen behandelt. Mithilfe von Übungsaufgaben kann das erworbene Verständnis überprüft werden.

### Für wen ist das Buch gedacht?

Das Lehrbuch richtet sich in erster Linie an Studierende all der Fachbereiche, in denen die Digitalisierung eine besondere Rolle spielt, vor allem die Fachrichtungen Informatik, IT-Sicherheit, Internet- oder Cyber-Sicherheit und angrenzende Disziplinen.

Es ist aber auch geeignet für Auszubildende im Bereich Fachinformatik und für Mitarbeiter\*innen aller Branchen und Unternehmen, die sich mit der Digitalisierung beschäftigen und das Thema Cyber-Sicherheit berücksichtigen wollen.

Um den Lesefluss nicht zu beeinträchtigen, wird in diesem Lehrbuch zwar hauptsächlich die männliche Form genannt, stets ist aber die weibliche Form und andere Formen gleichermaßen gemeint.

Als ich mit viel Freude begann, das Buch Cyber-Sicherheit zu schreiben, habe ich feststellen müssen, dass ich den Umfang dieser selbstgewählten Aufgabe weit unterschätzt habe, obwohl ich es mit meinen Erfahrungen hätte besser wissen müssen.

Meine Begeisterung ist dennoch geblieben, weil ich das Thema Cyber-Sicherheit spannend finde und die intensive Auseinandersetzung damit für mich persönlich eine Bereicherung darstellt.

Ich wünsche mir, dass meine Faszination für die Cyber-Sicherheit zu Ihnen überschwwappt, weil wir sehr viele Cyber-Sicherheitsexperten brauchen, die helfen, den Weg der Digitalisierung mit sicheren und vertrauenswürdigen IT-Systemen und IT-Infrastrukturen auf ein stabiles Fundament für unsere digitale Zukunft zu setzen.

Besonders möchte ich den Menschen in meiner Umgebung für ihr Verständnis danken, dass meine Aufmerksamkeit und Energie während der Zeit des Schreibens nicht auf sie gerichtet war. Dazu gehören in erster Linie meine Familie sowie die vielen Mitarbeiter\*innen und Kollegen\*innen vom Institut für Internet-Sicherheit – if(is), der Westfälischen Hochschule und den Verbänden, bei denen ich engagiert bin.

Mein besonderer Dank gilt den Cyber-Sicherheitsspezialisten des Instituts für Internet-Sicherheit, die immer wieder unverzichtbare Anregungen für Verbesserungen und Erweiterungen gegeben sowie bei der Konzeption und Umsetzung der Übungsaufgaben geholfen haben.

Hierzu gehören die Doktoranden des if(is)

- Rene Riedel
- Tobias Urban
- Matteo Cagnazzo

Mein Dank geht auch an Johnny Hoang, Wissenschaftliche Hilfskraft, der mich bei der Umsetzung meiner Ideen unterstützt hat.

Besonders danke ich Farina Lehmann, die mir geholfen hat, alle Grafiken nach einem einheitlichen Schema zu gestalten und umzusetzen, was viel Flexibilität und Durchhaltevermögen brauchte.

Ich danke auch meiner Frau, Bettina, die mich besonders unterstützt und die Verantwortung für die Rechtschreibung übernommen hat.

Da ich dieses Buch nicht für mich, sondern für eine breite und interessierte Leserschaft geschrieben habe, bin ich sehr an Rückmeldungen interessiert und bitte alle Leser\*innen, die Anmerkungen, Anregungen oder Verbesserungsvorschläge für die nächste Auflage haben oder Ideen, wie die Übungen auf den Webseiten optimiert und erweitert werden können, sich mit mir in Verbindung zu setzen.

Jedes Feedback ist wichtig und willkommen!

E-Mail: [cyber-sicherheit@norbert-pohlmann.com](mailto:cyber-sicherheit@norbert-pohlmann.com)

Ich wünsche allen Leser\*innen dieses Lehrbuches, dass sie das finden, was sie suchen und Freude und Spaß beim Lesen haben.

### Weitere Unterstützungen auf meiner Webseite

Auf dieser Webseite finden Sie weitere Informationen und Hilfestellungen, die das Buch Cyber-Sicherheit betreffen: <https://norbert-pohlmann.com/cyber-sicherheit/>



Die Ergebnisse der Übungsaufgaben aus dem Buch finden Sie unter:

<https://norbert-pohlmann.com/cyber-sicherheit/uebungen/>

Kollegen\*innen, Lehrbeauftragte, Lehrer\*innen und weitere Interessierte finden zu diesem Lehrbuch auch noch Folien mit den Bildern sowie darauf basierende Vorlesungen aus diesem Buch auf meiner Webseite:

<https://norbert-pohlmann.com/cyber-sicherheit/vorlesungen/>

Und vieles mehr ...

### Übersicht

Im Folgenden finden Sie einen Überblick über das Lehrbuch Cyber-Sicherheit

### Sichtweisen auf die Cyber-Sicherheit

In dieser Art Einleitung werden unterschiedliche Sichtweisen auf die Cyber-Sicherheit diskutiert, um eine Grundlage für das Verständnis des Themas Cyber-Sicherheit, die Probleme, Herausforderungen, Wirksamkeitskonzepte, Strategien, Motivationen und Bedürfnisse aufzubauen.

## **Kryptografie**

Im Kapitel Kryptografie werden Kenntnisse über den Aufbau, die Prinzipien, die Architektur und die Funktionsweise von grundlegenden kryptografischen Verfahren vermittelt. Kryptografische Verfahren spielen eine besondere Rolle bei vielen wichtigen Cyber-Sicherheitssystemen zur Gewährleistung der Cyber-Sicherheitsbedürfnisse, wie Vertraulichkeit, Authentifikation, Authentizität, Integrität und Verbindlichkeit.

## **Hardware-Sicherheitsmodule zum Schutz von sicherheitsrelevanten Informationen**

Immer mehr sicherheitsrelevante Informationen, wie zum Beispiel geheime Schlüssel und Transaktionsdaten, werden durch Bezahlsysteme sowie Verschlüsselungs- und Authentifikationslösungen im Internet genutzt. In diesem Kapitel werden unterschiedliche Hardware-Sicherheitsmodule beschrieben, die helfen, besonders sensible sicherheitsrelevante Informationen angemessen zu schützen.

## **Digitale Signatur, elektronische Zertifikate sowie Public Key Infrastruktur (PKI) und PKI-enabled Application (PKA)**

In diesem Kapitel werden die Themen digitale Signatur, elektronische Zertifikate sowie Public-Key-Infrastrukturen und PKI-enabled Application behandelt. Diese Cyber-Sicherheitsprinzipien und Cyber-Sicherheitsmechanismen sind in einer modernen Informations- und Wissensgesellschaft von enormer Wichtigkeit und helfen dabei, zentrale Vertrauensdienste und ein modernes Schlüsselmanagement aufzubauen.

## **Identifikation und Authentifikation**

Die Identifikation und Authentifikation spielen in der modernen IT und im Internet eine besondere Rolle. Aus diesem Grund werden in diesem Kapitel die unterschiedlichen Identifikations- und Authentifikationsverfahren behandelt und die Vor- und Nachteile diskutiert.

Außerdem werden die Konzepte risikobasierte und adaptive Authentifizierung und Identity Provider sowie weitere Ideen und Initiativen behandelt.

## **Enterprise Identity und Access Management**

Der Begriff Enterprise Identity und Access Management beschreibt jeglichen Einsatz von digitalen Identitäten, deren Attributen, deren Berechtigungen für IT-Systeme sowie IT-Dienste und schließt die Erzeugung, Nutzung, Pflege und Löschung dieser digitalen Identitäten mit ein. Ziel ist es, vertrauenswürdige, identitätsbezogene und regelkonforme Prozesse durchzusetzen, die unabhängig von Organisationen und Plattformen standardisiert nutzbar sind. Dazu werden Aufgaben, Prinzipien und Mechanismen in diesem Kapitel dargestellt und erläutert.

## **Trusted Computing**

Trusted Computing ist eine Cyber-Sicherheits- und Vertrauenswürdigkeitstechnologie. Mithilfe von Trusted Computing stehen moderne und intelligente Cyber-Sicherheitsarchitekturen, -konzepte und -funktionen zur Verfügung, mit denen IT-Systeme mit einer höheren Robustheit und einem höheren Cyber-Sicherheits-level umgesetzt werden können. Der besondere Schwerpunkt liegt dabei auf der Verifikation der Integrität eines IT-Systems.

## **Cyber-Sicherheit Frühwarn- und Lagebildsysteme**

In diesem Kapitel geht es um die Bedeutung und Grundstruktur eines Cyber-Sicherheit Frühwarn- und Lagebildsystems. Außerdem werden die notwendigen Prozesse und die Probleme, die durch die Entwicklung eines Cyber-Sicherheit Frühwarn- und Lagebildsystems entstehen, behandelt.

## **Firewall-Systeme**

Ein Firewall-System ist ein Cyber-Sicherheitsmechanismus, der zwischen verbundenen Netzen, Sicherheitsdomänen mit unterschiedlichem Schutzbedarf schafft. Es wird meist zum Schutz eigener Netze vor Gefahren aus unsicheren Netzen wie dem Internet, aber auch zur Strukturierung eigener Netze in einer Organisation eingesetzt. Dabei müssen unterschiedliche Aspekte berücksichtigt werden, damit mithilfe eines Firewall-Systems das gewünschte Sicherheitsmaß auch erreicht werden kann. In diesem Kapitel werden Idee, Definitionen, Grundlagen, Konzepte sowie Möglichkeiten und Grenzen von Firewall-Systemen behandelt.

## **IPSec-Verschlüsselung**

Im Kapitel IPSec-Verschlüsselung werden die Cyber-Sicherheitsarchitektur, Cyber-Sicherheitsprinzipien, Cyber-Sicherheitsmechanismen und Cyber-Sicherheitsprotokolle des IETF Sicherheitsstandards für die Cyber-Sicherheit von IP-Paketen vermittelt.

## **Transport Layer Security (TLS)/Secure Socket Layer (SSL)**

Das Kapitel TLS/SSL vermittelt die Cyber-Sicherheitsarchitektur, Cyber-Sicherheitsprinzipien, Cyber-Sicherheitsmechanismen und Cyber-Sicherheitsprotokolle des IETF Sicherheitsstandards für die Transport-Ebene.

## **Cyber-Sicherheitsmaßnahmen gegen DDoS-Angriffe**

Die Gewährleistung der Verfügbarkeit von IT-Systemen ist ein wichtiges Cyber-Sicherheitsbedürfnis, um Informationen und Dienste immer nutzen zu können. In diesem Kapitel werden DDoS-Angriffe, Ziele von DDoS-Angriffsmethoden und hilfreiche Cyber-Sicherheitsmaßnahmen gegen DDoS-Angriffe beschrieben.

## **E-Mail-Sicherheit**

Die E-Mail-Anwendung ist eine der wichtigsten Kommunikationsmöglichkeiten, insbesondere im Business-Bereich. Aus diesem Grund wird in diesem Kapitel das

Thema E-Mail-Sicherheit behandelt und die verschiedenen Cyber-Sicherheitskonzepte und Möglichkeiten diskutiert.

### **Blockchain-Technologie**

Dieses Kapitel erläutert und diskutiert die Grundzüge der Blockchain-Technologie, das Cyber-Sicherheitskonzept, die notwendigen Netzwerk-, Cyber-Sicherheits- und Vertrauenswürdigkeitsmechanismen sowie Beispieleanwendungen der Blockchain-Technologie.

### **Künstliche Intelligenz und Cyber-Sicherheit**

In diesem Kapitel wird behandelt, wie die Algorithmen aus dem Maschinellen Lernen und Künstlicher Intelligenz genutzt werden können, um die Cyber-Sicherheit zu verbessern. Potenziale liegen in den Bereichen Verbesserung der Erkennungsrate von Angriffen, Unterstützung von Cyber-Sicherheitsexperten, die die Wirkung von Cyber-Sicherheitslösungen erhöhen.

### **Social Web Cyber-Sicherheit**

Soziale Netzwerke bringen Nutzer aus verschiedenen Gesellschaftsgruppen zusammen und ermöglichen ihnen, sich darzustellen, Informationen und Meinungen auszutauschen sowie sich einfacher und zielgerichteter real zu begegnen. Aber der Erfolg der sozialen Netzwerke hat auch bekannte Nachteile und Herausforderungen im Bereich der Cyber-Sicherheit, die in diesem Kapitel behandelt werden.

### **Wirtschaftlichkeit von Cyber-Sicherheitsmaßnahmen**

Cyber-Sicherheitsmaßnahmen sind kein Selbstzweck. Mithilfe von Cyber-Sicherheitsmaßnahmen kann das Risiko bei der Nutzung von IT-Systemen erheblich reduziert und damit ein Schaden verhindert werden. In diesem Kapitel werden die Kosten und der Nutzen der Cyber-Sicherheitsmaßnahmen behandelt.

### **Anhang**

Im Anhang befindet sich eine Übersicht der im Lehrbuch Cybersicherheit genutzten Symbole. Außerdem ist dort ein Sachwortverzeichnis zu finden.

Norbert Pohlmann

---

# Inhaltsverzeichnis

<b>1</b>	<b>Sichtweisen auf die Cyber-Sicherheit . . . . .</b>	<b>1</b>
1.1	Einleitung . . . . .	1
1.2	Cyber-Sicherheitsprobleme . . . . .	2
1.2.1	Cyber-Sicherheitsproblem: „Zu viele Schwachstellen in Software“ . . . . .	3
1.2.2	Cyber-Sicherheitsproblem: „Ungenügender Schutz vor Malware“ . . . . .	4
1.2.3	Cyber-Sicherheitsproblem: „Keine internationalen Lösungen für Identifikation und Authentifikation“ . . . . .	6
1.2.4	Cyber-Sicherheitsproblem: „Unsichere Webseiten im Internet“ . . . . .	7
1.2.5	Cyber-Sicherheitsproblem: „Gefahren durch die Nutzung mobiler Geräte“ . . . . .	7
1.2.6	Cyber-Sicherheitsproblem: „Eine E-Mail ist wie eine Postkarte!“ . . . . .	9
1.2.7	Cyber-Sicherheitsproblem: „Geschäftsmodell: Bezahlen mit persönlichen Daten“ . . . . .	9
1.2.8	Cyber-Sicherheitsproblem: „Internetnutzer haben zu wenig Internet-Kompetenz“ . . . . .	10
1.2.9	Cyber-Sicherheitsproblem: „Manipulierte IT und IT-Sicherheitstechnologien“ . . . . .	11
1.2.10	Cyber-Sicherheitsproblem: „Unsichere IoT-Geräte“ . . . . .	11
1.2.11	Cyber-Sicherheitsproblem: „Fake News“ und weitere unerwünschte Inhalte . . . . .	13
1.3	Problematische Rahmenbedingungen . . . . .	14

1.4	Gesellschaftliche Sichtweise auf die Cyber-Sicherheitsprobleme . . . . .	14
1.4.1	Privatsphäre und Datenschutz . . . . .	14
1.4.2	Selbstbestimmung und Autonomie . . . . .	16
1.4.3	Wirtschaftsspionage . . . . .	17
1.4.4	Cyberwar . . . . .	17
1.5	Herausforderungen der Cyber-Sicherheit . . . . .	18
1.5.1	Paradigmenwechsel „Verantwortung versus Gleichgültigkeit“ . . . . .	18
1.5.2	Paradigmenwechsel „Proaktive versus reaktive Cyber-Sicherheitslösungen“ . . . . .	19
1.5.3	Paradigmenwechsel „Objekt-Sicherheit versus Perimeter-Sicherheit“ . . . . .	20
1.5.4	Paradigmenwechsel „Cloud-Service versus Lokal-IT“ . . . . .	21
1.5.5	Paradigmenwechsel „Dezentrale versus zentrale Cyber-Sicherheit“ . . . . .	21
1.5.6	Paradigmenwechsel „datengetriebene-versus eventgetriebene-Sicherheit“ . . . . .	21
1.5.7	Paradigmenwechsel „Zusammenarbeit versus Isolierung“ . . . . .	22
1.6	Konzept der Wirksamkeit von Cyber-Sicherheitssystemen . . . . .	22
1.7	Cyber-Sicherheitsstrategien . . . . .	26
1.7.1	Vermeiden von Angriffen . . . . .	26
1.7.2	Entgegenwirken von Angriffen . . . . .	28
1.7.3	Erkennen von Angriffen . . . . .	29
1.8	Angreifer und deren Motivationen . . . . .	30
1.9	Cyber-Sicherheitsbedürfnisse . . . . .	32
1.10	Das Pareto-Prinzip der Cyber-Sicherheit . . . . .	33
1.11	Cyber-Sicherheitsrisiko . . . . .	34
1.12	Zusammenfassung . . . . .	37
1.13	Übungsaufgaben . . . . .	37
	Literatur . . . . .	41
<b>2</b>	<b>Kryptografie . . . . .</b>	<b>43</b>
2.1	Grundlagen der Kryptografie . . . . .	43
2.1.1	Grundlagen der Verschlüsselung . . . . .	44
2.1.2	Definition eines kryptografischen Verfahrens . . . . .	46
2.1.3	No Security by Obscurity . . . . .	46
2.1.4	Die wichtigsten Begriffe in Kurzdefinition . . . . .	47
2.1.5	Begriffe aus der Kryptoanalyse . . . . .	48

---

2.1.6	Strategien der Analyse eines Kryptosystems .....	48
2.1.7	Bewertung der kryptografischen Stärke.....	50
2.1.8	Unterstützung bei der Einschätzung von Verfahren und Schlüssellängen .....	53
2.1.9	Zusammenfassung: Grundlagen der Kryptografie.....	53
2.1.10	Monoalphabetische Substitution .....	54
2.1.11	Homofone Substitution .....	55
2.1.12	Polyalphabetische Substitution .....	57
2.1.13	Transpositionsverfahren.....	58
2.1.14	Zusammenfassung: Elementare Verschlüsselungsverfahren.....	59
2.1.15	Data Encryption Standard .....	61
2.1.16	Advanced Encryption Standard .....	62
2.1.17	Verwaltung von Schlüsseln (Key Management).....	66
2.1.18	Betriebsart: Electronic Code Book Mode (ECB-Mode) .....	68
2.1.19	Betriebsart: Cipher Block Chaining Mode (CBC-Mode) .....	69
2.1.20	Betriebsart: Cipher Feedback Mode (CFB-Mode).....	70
2.1.21	Betriebsart: Output Feedback Mode (OFB-Mode) .....	71
2.1.22	Betriebsart: Counter Mode (CTR-Mode).....	72
2.1.23	Betriebsart: Galois/Counter Mode (GCM-Mode) .....	73
2.1.24	Modes of Operation: Zusammenfassung .....	74
2.2	Asymmetrische Verschlüsselungsverfahren.....	77
2.2.1	Das RSA-Verfahren .....	79
2.2.2	Das Diffie-Hellman-Verfahren.....	82
2.2.3	Elliptische Kurven .....	83
2.2.4	Hybride Verschlüsselungsverfahren.....	84
2.3	Quantencomputer: Das Damoklesschwert der Verschlüsselung .....	84
2.4	One-Way-Hashfunktionen .....	86
2.4.1	Besondere Eigenschaften von Hashfunktionen .....	87
2.4.2	SHA-3 (SHA = Secure Hash Algorithm).....	88
2.4.3	Message Authentication Code (MAC).....	88
2.4.4	Keyed-Hashing for Message Authentication (HMAC) .....	89
	Literatur.....	99

<b>3</b>	<b>Hardware-Sicherheitsmodule zum Schutz von sicherheitsrelevanten Informationen . . . . .</b>	101
3.1	Einleitung . . . . .	101
3.2	Hardware-Sicherheitsmodul: Smartcards . . . . .	102
3.3	Hardware-Sicherheitsmodul: Trusted Platform Module (TPM) . . . . .	104
3.4	Hardware-Sicherheitsmodul: High-Level Security Module (HLSM) . . . . .	106
3.5	Zusammenfassung: Kategorien von Hardware-Sicherheitsmodulen . . . . .	109
3.6	Evaluierung und Zertifizierung für eine höhere Vertrauenswürdigkeit von Hardware-Sicherheitsmodulen . . . . .	110
3.7	Key-Management von Hardware- Sicherheitsmodulen . . . . .	110
3.7.1	Das Management von TPMs . . . . .	111
3.7.2	Vier-Augen-Prinzip . . . . .	111
3.8	Zusammenfassung . . . . .	111
3.9	Übungsaufgaben . . . . .	112
	Literatur . . . . .	114
<b>4</b>	<b>Digitale Signatur, elektronische Zertifikate sowie Public Key-Infrastruktur (PKI) und PKI-enabled Application (PKA) . . . . .</b>	115
4.1	Digitale Signatur . . . . .	115
4.2	Elektronische Zertifikate/digitale Zertifikate . . . . .	119
4.3	Public Key-Infrastrukturen . . . . .	122
4.3.1	Idee und Definition von Public Key-Infrastrukturen . . . . .	123
4.3.2	Offene und geschlossene PKI-Systeme . . . . .	127
4.3.3	Umsetzungskonzepte von Public Key-Infrastrukturen . . . . .	130
4.4	Vertrauensmodelle von Public Key-Infrastrukturen . . . . .	131
4.4.1	Vertrauensmodell: Übergeordnete CA (Wurzel-CA, Root CA) . . . . .	132
4.4.2	Vertrauensmodell B: n:n-Cross- Zertifizierung . . . . .	133
4.4.3	Vertrauensmodell: 1:n Cross- Zertifizierung (Bridge CA) . . . . .	133
4.5	Gesetzlicher Hintergrund . . . . .	134
4.6	PKI-enabled Application . . . . .	138
4.6.1	E-Mail-Sicherheit . . . . .	138
4.6.2	Lotto – Online-Glückspiel . . . . .	145
4.7	Zusammenfassung . . . . .	147
4.8	Übungsaufgaben . . . . .	147
	Literatur . . . . .	148

<b>5</b>	<b>Identifikation und Authentifikation</b>	151
5.1	Was ist eine Identifikation und Authentifikation?	151
5.1.1	Identifikation	151
5.1.2	Authentifikation	152
5.1.3	Klassen von Authentifizierungsverfahren	153
5.2	Identifikationsverfahren	155
5.2.1	Vorlage eines Personalausweises	155
5.2.2	Fernidentifizierung – Allgemeine Aspekte	155
5.2.3	Videoidentifikation	156
5.2.4	Das eID Verfahren des elektronischen Personalausweises	159
5.2.5	Das PostIdent-Verfahren der Deutschen Post AG	161
5.2.6	Vergleich der verschiedenen Identifikationsverfahren	162
5.2.7	Weitere Identifikationsverfahren	164
5.2.8	Abgeleitete Identitäten	165
5.3	Authentifikationsverfahren	166
5.3.1	Passwort-Verfahren	167
5.3.2	Einmal-Passwort-Verfahren	178
5.3.3	Challenge-Response-Verfahren	179
5.3.4	Biometrische Verfahren	181
5.4	Mehr faktor-Authentifizierung	187
5.5	Konzept der risikobasierten und adaptiven Authentifizierung	189
5.6	Modernes Multifaktor-Authentifizierungssystem und Identifikationsverfahren	190
5.7	Fast Identity Online Alliance (FIDO)	197
5.7.1	Ziele der FIDO Alliance	197
5.7.2	Die FIDO-Architektur	198
5.7.3	Authentifizierung des Nutzers	200
5.8	Identity Provider	201
5.8.1	OpenID	201
5.8.2	OAuth 2.0	204
5.8.3	OpenID Connect	208
5.9	Zusammenfassung	209
5.10	Übungsaufgaben	209
	Literatur	210
<b>6</b>	<b>Enterprise Identity und Access Management</b>	213
6.1	Szenario eines Enterprise Identity and Access Management-Systems	215
6.2	Enterprise Identity and Access Management-Referenzmodell	215

6.3	Policies & Workflows . . . . .	218
6.3.1	Policy Management . . . . .	219
6.3.2	Workflow Management . . . . .	219
6.3.3	Beispiel für Policies & Workflows . . . . .	219
6.4	Repository Management . . . . .	219
6.4.1	Auf einer Datenbank basierendes Directory . . . . .	220
6.4.2	Metadirectory . . . . .	220
6.4.3	Virtual Directory . . . . .	221
6.4.4	Identity Repository . . . . .	221
6.4.5	Policy Repository . . . . .	221
6.4.6	Beispiel für Repository Management . . . . .	221
6.5	Life Cycle Management . . . . .	222
6.5.1	Identity-Administration . . . . .	222
6.5.2	Provisionierung . . . . .	223
6.5.3	Rollenmanagement . . . . .	223
6.5.4	Privileged User Management . . . . .	224
6.5.5	Delegierte Administration . . . . .	224
6.5.6	Synchronisierung . . . . .	224
6.5.7	Self-Service . . . . .	225
6.5.8	Credential Management . . . . .	225
6.5.9	Beispiel für Life Cycle Management . . . . .	225
6.6	Access Management . . . . .	226
6.6.1	Authentisierungs- und Authentifizierungs- Management . . . . .	226
6.6.2	Autorisierungs-Management . . . . .	227
6.6.3	Single Sign-On/Single Log-out . . . . .	228
6.6.4	Access Control . . . . .	228
6.6.5	Remote Access Control . . . . .	229
6.6.6	Network Access Control . . . . .	229
6.6.7	Policy Enforcement . . . . .	230
6.6.8	Beispiel für Access Management . . . . .	230
6.7	Information Protection . . . . .	230
6.7.1	Secure Sharing . . . . .	231
6.7.2	Information Rights Management . . . . .	232
6.7.3	Content Security . . . . .	232
6.7.4	Beispiel für Information Protection . . . . .	232
6.8	Federation . . . . .	232
6.8.1	Trust Management . . . . .	233
6.8.2	Identity Federation . . . . .	233
6.8.3	Beispiel für Federation . . . . .	234
6.9	Compliance & Audit . . . . .	234
6.9.1	Compliance Management . . . . .	235
6.9.2	Monitoring . . . . .	235
6.9.3	Reporting . . . . .	235
6.9.4	Auditing . . . . .	236
6.9.5	Beispiel für Compliance & Audit . . . . .	236

6.10	Allgemeine Mehrwerte eines Enterprise Identity and Access Management-Systems . . . . .	236
6.11	Zusammenfassung . . . . .	239
6.12	Übungsaufgaben. . . . .	239
	Literatur. . . . .	240
<b>7</b>	<b>Trusted Computing. . . . .</b>	241
7.1	Einleitung. . . . .	241
7.2	Trusted Computing auf den Punkt gebracht . . . . .	244
7.2.1	Robustheit und Modularität . . . . .	244
7.2.2	Integritätsüberprüfung . . . . .	245
7.2.3	Trusted Process . . . . .	246
7.2.4	Trusted Plattform . . . . .	247
7.3	Trusted Computing – Grundlagen . . . . .	247
7.3.1	Kernelarchitekturen von Betriebssystemen . . . . .	247
7.3.2	Core Root of Trust for Measurement (CRTM) . . . . .	250
7.3.3	Identitäten von TPMs. . . . .	251
7.3.4	TPM-Schlüssel und deren Eigenschaften . . . . .	252
7.3.5	Trusted Computing-Funktionen. . . . .	256
7.3.6	Trusted Platform (Security-Plattform, Sicherheitsplattform) . . . . .	260
7.3.7	Beispielanwendungen . . . . .	263
7.4	Trusted Network Connect (TNC). . . . .	268
7.4.1	Problemstellung . . . . .	268
7.4.2	Anforderungen an heutige Netzwerke . . . . .	270
7.4.3	Vertrauenswürdige Netzwerkverbindungen. . . . .	270
7.4.4	Trusted Network Connect (TNC) im Detail. . . . .	272
7.4.5	Anwendungsfelder. . . . .	275
7.4.6	Kritische Diskussion . . . . .	276
7.4.7	Fazit: Trusted Network Connect (TNC). . . . .	278
7.5	Festlegung einer sicheren und vertrauenswürdigen Systemkonfiguration . . . . .	278
7.6	Zusammenfassung . . . . .	279
7.7	Übungsaufgaben. . . . .	279
	Literatur. . . . .	280
<b>8</b>	<b>Cyber-Sicherheit-Frühwarn- und Lagebildsysteme . . . . .</b>	281
8.1	Einleitung. . . . .	281
8.2	Angriffe und ihre Durchführung . . . . .	281
8.3	Idee eines Cyber-Sicherheit Frühwarnsystems . . . . .	287
8.3.1	Reaktionszeit für die Frühwarnung . . . . .	287
8.3.2	Definition eines Cyber-Sicherheit Frühwarnsystems . . . . .	288
8.3.3	Obligatorische funktionelle Anforderungen. . . . .	288
8.3.4	Asymmetrische Bedrohungen . . . . .	289

8.4	Aufbau eines Cyber-Sicherheit Frühwarnsystems.....	289
8.4.1	Rechtliche Rahmenbedingungen .....	290
8.4.2	Beteiligte Organisationen.....	290
8.5	Technische Realisierung eines Cyber-Sicherheit Frühwarnsystems .....	290
8.5.1	Architektur.....	290
8.5.2	Sensoren.....	291
8.5.3	Analyse- und Erkennungsmodul .....	292
8.6	Prinzipielle Aspekte von Sensoren.....	294
8.6.1	Grundprinzip von Sensoren .....	294
8.6.2	Messmethoden .....	296
8.6.3	Ort der Messung.....	296
8.7	Diskussion unterschiedlicher Sensoren .....	297
8.7.1	NetFlow-Sensor .....	297
8.7.2	Netzwerk-Sensor .....	299
8.7.3	SNMP-Sensor.....	303
8.7.4	Wireshark-Sensor.....	305
8.7.5	Honeypot-Sensor .....	306
8.7.6	Logdaten-Sensor .....	308
8.7.7	Verfügbarkeitssensor .....	310
8.8	Analysekonzepte .....	311
8.8.1	Erkennen von bekannten sicherheitsrelevanten Aktionen .....	311
8.8.2	Erkennen von Anomalien.....	312
8.9	Cyber-Sicherheit-Frühwarnprozess .....	313
8.10	Kommunikationslagebild .....	314
8.11	Zusammenfassung .....	321
8.12	Übungsaufgaben.....	321
	Literatur.....	323
<b>9</b>	<b>Firewall-Systeme.....</b>	<b>325</b>
9.1	Bedrohungen im Netz .....	325
9.1.1	Angriffsmöglichkeiten in Kommunikationssystemen.....	325
9.1.2	Passive Angriffe .....	326
9.1.3	Aktive Angriffe .....	327
9.2	Idee und Definition von Firewall-Systemen .....	329
9.2.1	Elektronische Brandschutzmauer.....	330
9.2.2	Elektronischer Pförtner .....	330
9.3	Das Sicherheitskonzept .....	330
9.4	Aufgaben von Firewall-Systemen .....	331
9.5	Grundlage von Firewall-Systemen.....	333
9.6	Definition eines Firewall-Elements .....	340
9.7	Designkonzept aktiver Firewall-Elemente.....	343
9.8	Packet Filter .....	345

9.9	Zustandsorientierte Packet Filter (stateful inspection) . . . . .	347
9.10	Application Gateway/Proxy-Technik . . . . .	349
9.11	Next-Generation-Firewall . . . . .	353
9.12	Firewall-Konzepte . . . . .	355
9.13	Konzeptionelle Möglichkeiten und Grenzen von Firewall-Systemen . . . . .	357
9.13.1	Common Point of Trust . . . . .	357
9.13.2	Konzeptionelle Grenzen eines Firewall-Systems . . . . .	359
9.14	Das richtige Firewall-Konzept für jeden Anwendungsfall . . . . .	361
9.15	Definition des Kommunikationsmodells mit integriertem Firewall-Element . . . . .	364
9.16	Zusammenfassung . . . . .	369
9.17	Übungsaufgaben . . . . .	370
	Literatur . . . . .	372
<b>10</b>	<b>IPSec-Verschlüsselung . . . . .</b>	<b>373</b>
10.1	Einleitung . . . . .	373
10.2	IPSec Header . . . . .	374
10.2.1	Authentication Header . . . . .	375
10.2.2	Encapsulated Security Payload . . . . .	376
10.3	Cyber-Sicherheitsdienste der IPSec-Header und Realisierungsformen . . . . .	378
10.4	IPSec-Schlüsselmanagement . . . . .	383
10.4.1	Manual Keying . . . . .	384
10.4.2	Internet-Key-Exchange-Protocol (IKE) . . . . .	384
10.5	Anwendungsformen von IPSec-Lösungen . . . . .	395
10.6	Protokollmitschnitt . . . . .	397
10.7	Zusammenfassung . . . . .	403
10.8	Übungsaufgaben . . . . .	403
	Literatur . . . . .	405
<b>11</b>	<b>Transport Layer Security (TLS)/Secure Socket Layer (SSL) . . . . .</b>	<b>407</b>
11.1	Einleitung . . . . .	407
11.2	Einbindung in die Kommunikationsarchitektur . . . . .	408
11.3	Protokolle der TLS/SSL-Schicht . . . . .	410
11.4	TLS/SSL-Zertifikate . . . . .	424
11.5	Authentifikationsmethoden . . . . .	426
11.6	Anwendungsformen von TLS/SSL-Lösungen . . . . .	428
11.7	Protokollmitschnitt . . . . .	430
11.8	Zusammenfassung . . . . .	437
11.9	Übungsaufgaben . . . . .	437
	Literatur . . . . .	438

<b>12</b>	<b>Cyber-Sicherheitsmaßnahmen gegen DDoS-Angriffe</b>	439
12.1	Einleitung	439
12.2	Gezielte Überlastung	441
12.3	Reflection und Amplification	442
12.4	Abwehrstrategien gegen Angriffe auf die Verfügbarkeit	443
12.4.1	Cyber-Sicherheitsrichtlinien zum Schutz vor Verfügbarkeitsangriffen	443
12.4.2	On-Site-Robustheitsmaßnahmen	444
12.4.3	Off-Site-Dienstleistungsmodelle	446
12.5	Präventiv gegen Beteiligung – Sichere Konfiguration von Diensten	450
12.6	Zusammenfassung	450
12.7	Übungsaufgaben	451
	Literatur	451
<b>13</b>	<b>E-Mail-Sicherheit</b>	453
13.1	Einleitung	453
13.2	Generelle Cyber-Sicherheitsprobleme des E-Mail-Dienstes	454
13.3	E-Mail-Verschlüsselung	455
13.3.1	PGP und S/MIME sowie deren Unterschiede	456
13.3.2	Weitere Alternativen für E-Mail-Sicherheit	460
13.4	Zusammenfassung	466
13.5	Übungsaufgaben	466
	Literatur	466
<b>14</b>	<b>Blockchain-Technologie</b>	467
14.1	Einleitung	467
14.2	Aufbau der Blockchain-Technologie	470
14.2.1	Element: Daten	470
14.2.2	Element: Block	471
14.2.3	Element: HashPrev	472
14.2.4	Element: Merkle Hash	473
14.2.5	Element: Transaktionen	474
14.2.6	Element: Node	477
14.2.7	Element: Wallet	478
14.2.8	Element: Blockchain-Adresse	480
14.2.9	Prinzip: Keine „zentrale Instanz“	481
14.2.10	Konsensfindungsverfahren	482
14.2.11	Struktur: Berechtigungsarchitektur	490
14.3	Hard und Soft Forks von Blockchains	492
14.4	Anwendungsformen und Anwendungen der Blockchain	501

14.5	Blockchain-as-a-Service .....	507
14.6	Sicherheit und Vertrauenswürdigkeit der Blockchain-Technologie .....	507
14.6.1	Sicherheit der Blockchain-Infrastruktur.....	508
14.6.2	Sicherheit der Blockchain-Anwendung.....	512
14.7	Gegenüberstellung PKI- und Blockchain-Technologien .....	514
14.8	Zusammenfassung .....	516
14.9	Übungsaufgaben.....	517
	Literatur.....	519
<b>15</b>	<b>Künstliche Intelligenz und Cyber-Sicherheit.....</b>	<b>521</b>
15.1	Einleitung.....	521
15.2	Einordnung der Künstlichen Intelligenz .....	522
15.3	Erfolgsfaktoren der Künstlichen Intelligenz .....	523
15.4	Das Prinzip des Maschinellen Lernens .....	525
15.5	Kategorien und Algorithmen des Maschinellen Lernens.....	526
15.5.1	ML-Algorithmus: Support-Vector-Machine (SVM) .....	526
15.5.2	ML-Algorithmus: k-Nearest-Neighbor (kNN).....	530
15.5.3	ML-Algorithmus: k-Means-Algorithmus .....	533
15.5.4	ML-Algorithmus: Hierarchische Clustering-Verfahren .....	535
15.5.5	Künstliche Neuronale Netze (KNN) .....	536
15.5.6	Deep Learning .....	541
15.6	Anwendungsszenarien von KI und Cyber-Sicherheit .....	542
15.7	Manipulationen von Künstlicher Intelligenz .....	545
15.8	Beispiele von KI und Cyber-Sicherheit.....	546
15.8.1	Alert-System auf der Basis eines kontinuierlichen Lagebilds über die aktuelle Gefahrenlage im Online-Banking .....	546
15.8.2	Identifikation/Authentifikation eines Nutzers mittels Smartphone- Sensoren .....	552
15.8.3	Erkennung von netzwerkbasierten Angriffen mittels Künstlicher Intelligenz .....	554
15.9	Zusammenfassung .....	557
15.10	Übungsaufgaben.....	558
	Literatur.....	558
<b>16</b>	<b>Social Web Cyber-Sicherheit .....</b>	<b>561</b>
16.1	Soziale Netzwerke .....	562
16.2	Fake-News .....	564
16.2.1	Was sind Fake-News? .....	564
16.2.2	Social Bot (die digitale Propaganda-Maschine). . . . .	565

16.3	Filterblasen und Echokammern . . . . .	569
16.4	Psychometrie bei sozialen Netzwerken . . . . .	570
16.5	Zusammenfassung . . . . .	571
16.6	Übungsaufgaben. . . . .	571
	Literatur. . . . .	572
<b>17</b>	<b>Wirtschaftlichkeit von Cyber-Sicherheitsmaßnahmen</b> . . . . .	<b>573</b>
17.1	Einführung . . . . .	573
17.2	Cyber-Sicherheit . . . . .	574
17.2.1	Schutzbedarf von IT-Systemen . . . . .	574
17.2.2	Wie sicher ist „sicher“? . . . . .	575
17.2.3	Verwundbarkeit . . . . .	576
17.3	Return on Security Investment RoSI – Nutzenaspekt . . . . .	576
17.4	Beispielberechnung RoSI: Notebookverluste . . . . .	578
17.5	Zusammenfassung . . . . .	582
17.6	Übungsaufgaben. . . . .	582
	Literatur. . . . .	583
	<b>Anhang</b> . . . . .	<b>585</b>
	<b>Stichwortverzeichnis</b> . . . . .	<b>589</b>

---

## Über den Autor

**Norbert Pohlmann** ist Informatikprofessor für Verteilte Systeme und Informationssicherheit im Fachbereich Informatik und Kommunikation sowie geschäftsführender Direktor des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen.

Von 1988 bis 1999 war er geschäftsführender Gesellschafter der Firma KryptoKom, Gesellschaft für kryptografische Informationssicherheit und Kommunikationstechnologie mbH, in der forschungsnahe und innovative Cyber-Sicherheitsprojekte und -produkte realisiert wurden. Nach der Fusion der KryptoKom mit der Utimaco Safeware war er von 1999 bis 2003 Mitglied des Vorstandes der Utimaco Safeware AG, verantwortlich für Entwicklungsprojekte und Technologiearchitekturen der IT-Sicherheitsprodukte und -lösungen.

Seit April 1998 ist Prof. Norbert Pohlmann Vorstandsvorsitzender des Bundesverbands für IT-Sicherheit – TeleTrusT und seit Mai 2015 Mitglied des Vorstandes des Verbands der Internetwirtschaft – eco.

Außerdem ist Prof. Norbert Pohlmann Mitglied des wissenschaftlichen Beirates der Gesellschaft für Datenschutz und Datensicherung – GDD und Mitglied im Lenkungskreis der Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Technologie – BMWi.

Er war fünf Jahre Mitglied der „Permanent Stakeholders‘ Group“ der ENISA (European Union Agency for Network and Information Security), die Sicherheitsagentur der europäischen Gemeinschaft.

Norbert Pohlmann ist Träger des Preises der Stadt Aachen für Innovation und Technologie für wissenschaftliche und unternehmerische Leistungen 1997.

2011 wurde es als „Professor des Jahres 2011“ in der Kategorie „Ingenieurwissenschaften/Informatik“ ausgezeichnet.

Im Wintersemester 2008 war er als Gastprofessur am Stevens Institute of Technology in der Studienrichtung „Cybersecurity“, Hoboken, NJ, USA (New York Metropolitan Area) und im Sommersemester 2013 an der Stanford University im Fachbereiche Computer Science, Silicon Valley, USA.

Mehr als 390 Fachartikel und 7 Bücher sowie viele Herausgeberschaften, über 360 Vorträge auf dem Gebiet der Informationssicherheit dokumentieren seine Fachkompetenz und sein Engagement auf dem Gebiet Cyber-Sicherheit (siehe auch: [www.norbert-pohlmann.com](http://www.norbert-pohlmann.com)).

**Institut für Internet-Sicherheit – if(is)**

Westfälische Hochschule Gelsenkirchen

Neidenburger Str. 43

45877 Gelsenkirchen

E-Mail: [pohlmann@internet-sicherheit.de](mailto:pohlmann@internet-sicherheit.de)

URL: <https://www.internet-sicherheit.de>

<https://norbert-pohlmann.com>



# Sichtweisen auf die Cyber-Sicherheit

1

In diesem Kapitel werden unterschiedliche Sichtweisen auf die Cyber-Sicherheit diskutiert, um eine Grundlage für das Verständnis des Themas Cyber-Sicherheit, die Probleme, Herausforderungen, Wirksamkeitskonzepte, Strategien, Motivationen und Bedürfnisse aufzubauen.

---

## 1.1 Einleitung

Informationstechnik (IT) und das Internet sind Motor und Basis für das Wohlergehen der modernen und globalen Informations- und Wissensgesellschaft. Klar ist auch, dass seit Beginn der IT und des Internets die Cyber-Sicherheitsprobleme jedes Jahr größer und nicht kleiner werden. Eine wichtige Erkenntnis ist, dass die heutigen IT-Architekturen der genutzten IT-Systeme, wie Endgeräte, Server und Netzkomponenten, nicht sicher genug konzipiert und aufgebaut sind, um den Fähigkeiten von intelligenten Hackern standzuhalten.

Täglich kann den Medien entnommen werden, wie sich kriminelle Hacker die unzureichende Qualität der Software für erfolgreiche Angriffe zunutze machen, Malware installieren, Passwörter sowie Identitäten stehlen und Endgeräte aus-spionieren. Ungesicherte IT-Systeme genießen zurzeit zu viel Toleranz bei Nutzern und Unternehmen. Diese Einstellung wird sich in Zukunft mit der Bedeutung der IT und des globalen Internets radikal ändern müssen.

Eine angemessene, sichere und vertrauenswürdige IT zu erreichen, ist für die erfolgreiche Zukunft der Informations- und Wissensgesellschaft entscheidend. Letztlich muss die voranschreitende Digitalisierung auch die Nachhaltigkeit als

strategisches Ziel haben. Das gelingt nur, wenn die IT-Technologien- und Services sicher und vertrauenswürdig sind.

**Wichtig** Die meisten der heutigen IT-Architekturen der genutzten IT-Systeme sind nicht sicher genug konzipiert und aufgebaut, um den Fähigkeiten von intelligenten Hackern standzuhalten.

---

### Definition von Cyber-Sicherheit

Cyber-Sicherheit befasst sich mit allen Aspekten der IT-Sicherheit, wobei das Aktionsfeld auf den gesamten Cyber-Raum ausgeweitet wird. Cyber-Raum umfasst in dieser Definition sämtliche mit dem globalen Internet verbundene IT und IT-Infrastrukturen sowie deren Kommunikation, Anwendungen, Prozesse mit Daten, Informationen und Intelligenzen. Mit der zunehmenden Digitalisierung wird im Cyber-Raum auch die strikte Trennung zwischen Arbeit und Freizeit aufgelöst. Cyber-Angriffe im Cyber-Raum können die Unternehmen und Bürger treffen, aber auch zu erheblichen Beeinträchtigungen der gesellschaftlichen Lebensgrundlagen führen.

---

## 1.2 Cyber-Sicherheitsprobleme

Die Angriffsflächen der IT- und Internet-Technologie werden durch komplexere Software-Systeme und kompliziertere Zusammenhänge zwischen Protokollen, Diensten und globalen Infrastrukturen vielfältiger und deutlich größer, was erfolgreich durchgeführte Angriffe jeden Tag dokumentieren.

Die Angriffe auf die immer höheren Werte, wie Kundendaten, Entwicklungsdaten usw., auf den IT-Systemen und deren Verfügbarkeit werden verteilter, raffinierter und professioneller ausgeführt, was Milliardenschäden verursacht. Die IT-Kriminalität erfährt eine zunehmende Industrialisierung und damit eine nicht zu unterschätzende und nie dagewesene professionalisierte Nachhaltigkeit, die sich in der Wahrscheinlichkeit von erfolgreichen Angriffen widerspiegelt. Zurzeit besteht ein starkes Ungleichgewicht zwischen Angreifern und Verteidigern.

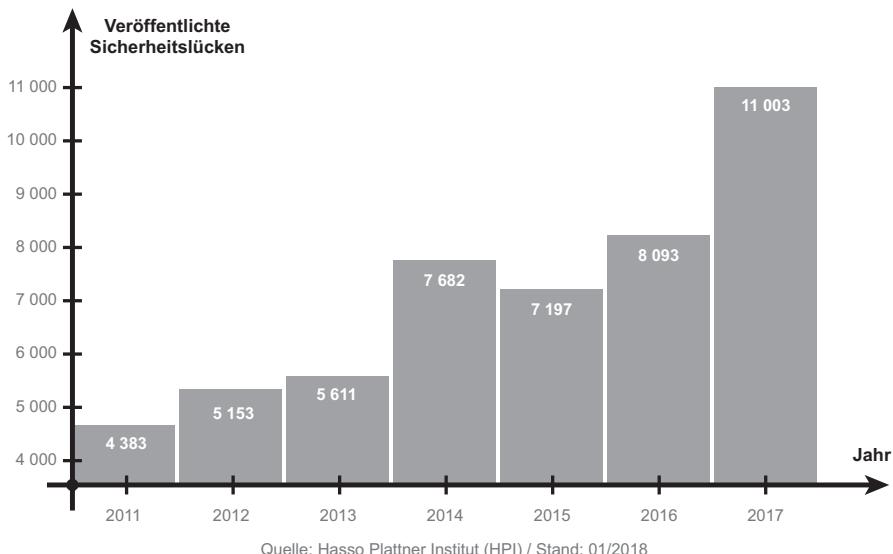
Bei der kritischen Beurteilung der aktuellen Cyber-Sicherheitssituation fallen einige sehr unterschiedliche Cyber-Sicherheitsprobleme besonders deutlich auf, die gelöst werden müssen, um mehr notwendige IT-Sicherheit und Vertrauenswürdigkeit aufzubauen [1]. Im Folgenden werden einige wichtige Cyber-Sicherheitsprobleme aufgezeigt, die sehr unterschiedlich sind.

**Wichtig** Die Angriffsflächen auf IT-Systeme werden vielfältiger und deutlich größer.

### 1.2.1 Cyber-Sicherheitsproblem: „Zu viele Schwachstellen in Software“

Software stellt in allen Branchen einen immer größeren Wertschöpfungsanteil dar. Software wird in PCs, Notebooks, Smartphones, in sehr großen Rechenzentren, aber auch immer mehr in Autos, in Industrieanlagen, im Haus, beim Sport, im Bereich der Dinge und zukünftig in allen Bereichen des privaten und beruflichen Lebens genutzt. Ein großes Cyber-Sicherheitsproblem ist, dass in der aktuell genutzten Software zu viele Schwachstellen vorhanden sind. Die Software-Qualität der Betriebssysteme und Anwendungen ist für die heutige Bedrohungslage nicht mehr ausreichend (siehe Abb. 1.1). Die Fehlerdichte, die Anzahl der Softwarefehler pro 1000 Zeilen Code, ist bei qualitativ hochwertiger Software heute im Schnitt 0,3. Da gängige Betriebssysteme ca. 10. Mio. Zeilen Code haben, sind hier im Schnitt 3000 Software-Fehler zu finden [2].

Eine qualitativ schlechte Software hat viele Softwarefehler (Schwachstellen, Bugs usw.) und ist damit grundlegende Ursache für erfolgreiche Remote-Angriffe auf IT-Systeme. Das Risiko für die Ausnutzung der Schwachstellen und damit für Schäden ist entsprechend groß, da sich kriminelle Organisationen und Nachrichtendienste zunehmend auf dieses Problem konzentrieren. Die Erfolgsaussichten eines positiven Remote-Angriffes auf IT-Systeme und die gespeicherten Werte sind sehr gut. Aus diesem Grund ist eine schlechte Software eine besondere Herausforderung unserer modernen IT und sorgt dafür, dass so viele IT-Systeme mit Malware (Schadsoftware) infiziert sind. Die Ursachen für schlechte Software sind immer noch: steigende Komplexität der Software,



**Abb. 1.1** Schwachstellen in Software

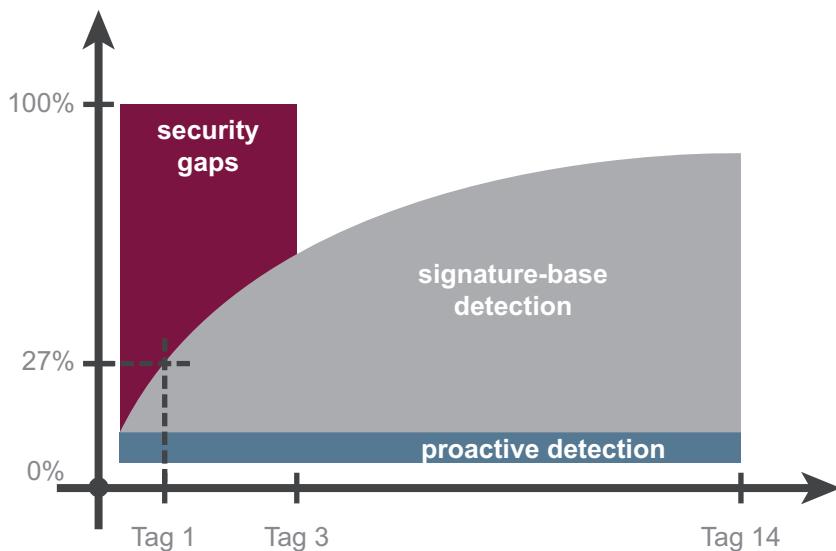
zu wenig Sicherheitsbewusstsein der Softwareentwickler, fehlende Expertisen der Softwareentwickler (schlechter Programmierstil, mangelnde Informationen über eingesetzte Bibliotheken und Komponenten), fehlendes Wissen über aktuelle Sicherheitsbedrohungen, der Zeitdruck für die Fertigstellung der Software (Time-to-Market) und damit verbunden unzureichendes Testen und kurze Anforderungsphasen und ein daraus resultierender unsystematischer Entwurf. Diese Liste der Gründe für schlechte Software ist noch erweiterbar. Der Softwareentwicklungsprozess verläuft häufig unsystematisch und für heutige Anforderungen an die Software nicht professionell genug.

Bei allen Softwaresystemen wird aus heutiger Sicht in den nächsten zehn Jahren mit keiner sprunghaften Verbesserung der Softwarequalität zu rechnen sein. Selbst wenn: Auch bei verbesserter Softwarequalität benötigen die professionellen Angreifer immer weniger Softwareschwachstellen für erfolgreiche Angriffe. Aus diesem Grund müssen passende Cyber-Sicherheitssysteme geplant sowie geeignete Qualitätskontrollen umgesetzt werden, da ein sehr hohes Bedrohungspotenzial durch Softwareschwachstellen vorhanden ist.

**Wichtig** Die Softwarequalität ist für die heutige Bedrohungslage nicht mehr ausreichend.

### 1.2.2 Cyber-Sicherheitsproblem: „Ungenügender Schutz vor Malware“

Malware ist der Oberbegriff für „Schadsoftware“ wie Viren, Würmer, trojanische Pferde usw. Angreifer (kriminelle Organisationen, politisch und wirtschaftlich orientierte Spione, Terroristen, Strafverfolger usw.) nutzen Softwareschwachstellen und menschliche Unzulänglichkeiten aus, um Malware auf IT-Systemen zu installieren. Über E-Mail-Anhänge oder unsichere Webseiten mithilfe von sogenannten Drive-by-Downloads wird Malware hauptsächlich in IT-Endgeräte unbemerkt eingeschleust. Das Institut für Internet-Sicherheit geht zurzeit davon aus, dass auf jedem 10. IT-Endgerät in Deutschland ungewollte intelligente Malware vorhanden ist, die über ein Botnetz gesteuert wird. Ein Botnetz ist eine Gruppe von IT-Endgeräten, die unter zentraler Kontrolle eines Angreifers stehen und von ihm für Angriffe genutzt werden. Dadurch können Angreifer Informationen von IT-Systemen mithilfe von Keyloggern und Trojanern auslesen, IT-Systeme für die Spam-Verteilung und DDoS-Angriffe nutzen sowie mit Ransomware Daten verschlüsseln und Lösegeld für die Entschlüsselung verlangen. Bei Ransomware verschlüsseln die Angreifer mithilfe der Malware wichtige Daten auf dem IT-System und verlangen vom Besitzer zum Beispiel 3000 EUR für den Schüssel, mit dem die Daten wieder entschlüsselt werden können [3]. Aber auch Staatstrojaner gehören zur Malware und haben das Ziel, „verschlüsselte Kommunikationsdaten“ auf den Endgeräten durch die Strafverfolgungsbehörden abzugreifen.



**Abb. 1.2** Ungenügender Schutz vor Malware

Die Anti-Malware-Lösungen haben heute bei Massen-Angriffen mit 75 % bis 95 % eine zu schwache Erkennungsrate. Bei gezielten und direkten Angriffen auf ein IT-System liegt die Erkennungsrate im Schnitt sogar nur bei 27 %. Hintergrund dieser Entwicklung ist, dass signaturbasierte Erkennungen bei gezielten Angriffen ihre Wirkung verlieren, weil keine Signaturen mehr erstellt und verteilt werden und die Signaturen bei jedem direkten Angriff individuell sind, siehe Abb. 1.2.

Symantec, als größter Hersteller von Anti-Malware-Lösungen, erkennt nach eigenen Angaben nur noch 45 % der Malware. Diese Zahl spiegelt sicherlich das neue Verhältnis zwischen gezielten und Massen-Angriffen wider.

**Wichtig** Anti-Malware-Produkte haben heute in gewissen Situationen eine zu schlechte Erkennungsrate.

### Advanced Persistent Threat (APT)

Unter einem Advanced Persistent Threat (APT) wird in der Regel ein gezielter Angriff mit komplexen Angriffstechnologien- und Taktiken sowie aufwendigen Hintergrundinformationen eines Opfer-IT-Systems und dessen Umgebung verstanden. Dabei nimmt der Angreifer einen großen Aufwand auf sich (Advanced), um erfolgreich auf ein Opfer-IT-System zuzugreifen und möglichst lange (Persistent) unentdeckt zu bleiben. So kann er über einen längeren Zeitraum Informationen ausspähen oder Schaden anrichten. APTs sind vor allem durch intelligente Malware wie Stuxnet und Flame bekannt geworden.

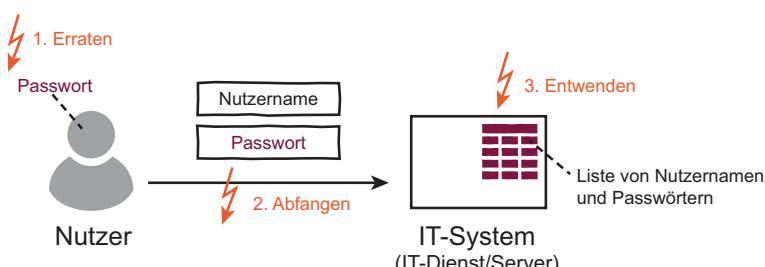
**Wichtig** Advanced Persistent Threats (APT) sind gezielte Angriffe mit komplexen Angriffstechnologien- und Taktiken sowie aufwendigen Hintergrundinformationen eines Opfer-IT-Systems und dessen Umgebung und stellen ein sehr großes Problem dar.

### 1.2.3 Cyber-Sicherheitsproblem: „Keine internationalen Lösungen für Identifikation und Authentifikation“

Im Jahr 2019 werden immer noch Passwörter für die Authentifikation im Internet genutzt, da dieses Verfahren einfach umzusetzen ist. Die Probleme sind bekannt: Verwendung von schlechten Passwörtern oder ein gutes Passwort, das für viele Anwendungen verwendet wird. Passwörter werden zum Beispiel im Klartext in E-Mails durch das Internet übertragen. Viele Internetnutzer fallen auf Phishing-E-Mails herein, die Passwörter abgreifen. Auch das Abgreifen von Passwörtern mithilfe von sogenannten Keyloggern, die alle Eingaben auf der Tastatur mitlesen, ist eine Möglichkeit, um die Sicherheit des Authentifikationsverfahrens Passwort auszuhebeln. Aber auch der Zugriff auf die Liste von Nutzernamen und Passwörtern ist eine erfolgreiche Angriffsmethode, siehe Abb. 1.3.

Durch die Nutzung von unsicheren Authentifikations-Technologien entsteht im Bankenbereich allein in den USA jährlich ein Schaden von mehr als 1,6 Mrd. EUR (Credential Spill Report, 2018). Sehr gute Identifikations- und Authentifikationslösungen sind vorhanden, wie zum Beispiel die ID-Funktion des neuen Personalausweises in Deutschland, nur werden diese kaum angeboten oder genutzt und haben international wenig Bedeutung.

**Wichtig** Es werden immer noch Passwörter für die Authentifikation im Internet verwendet, obwohl das Passwortverfahren nicht sicher ist.



**Abb. 1.3** Passwort-Verfahren und deren Probleme

**Abb. 1.4** Unsichere Webseiten



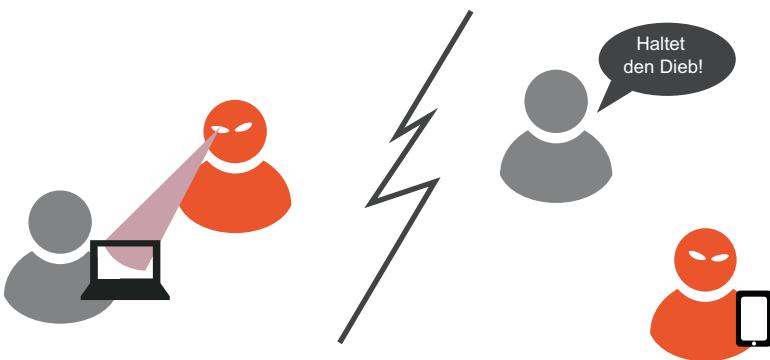
#### **1.2.4 Cyber-Sicherheitsproblem: „Unsichere Webseiten im Internet“**

Heute wird Malware hauptsächlich über unsichere Webseiten im Internet verteilt, siehe Abb. 1.4. Das Institut für Internet-Sicherheit hat in einem Projekt zum Thema Internet-Kennzahlen evaluiert und festgestellt, dass auf 2,5 % der gemessenen deutschen Webseiten direkt oder indirekt Malware vorhanden war, die potenziell dafür sorgen konnte, dass die Nutzer der Webseiten ebenfalls mit Malware infiziert werden. Dieser Wert war im internationalen Vergleich sehr hoch. Die USA hatten ca. 1 % und die Japaner 0,57 %.

Jeder kann eine Webseite erstellen, aber nur die wenigsten haben das nötige Fachwissen oder die finanziellen Mittel für die Einbindung von existierenden Cyber-Schutzmechanismen. Daraus ergibt sich eine große Angriffsfläche im Internet, insbesondere falls die Webseiten von großen Unternehmen Schwachstellen aufweisen. Webseiten im Internet, die nicht sicher genug sind, werden von Angreifern so manipuliert, dass sie Nutzer mit Malware infizieren. Die eigenen potenziellen und vorhandenen Kunden laden sich so beim Besuch der Firmenseite die Malware auf ihre IT-Systeme. Das Problem bei Webseiten ist, dass zu viele Organisationen zwar viel Wert auf Nutzerführung, Farbgestaltung sowie ihre eigene Darstellung legen, aber nicht auf die Cyber-Sicherheit. Große Firmen wie Sony wurden sogar mehrmals hintereinander gehackt, da sie sicherheitsrelevante Standards auf ihren Webseiten nicht einhielten.

#### **1.2.5 Cyber-Sicherheitsproblem: „Gefahren durch die Nutzung mobiler Geräte“**

Die Vorteile von mobilen Geräten, wie Smartphones, Tablets und Wearables, sind bestechend. Über die vielfältigen Kommunikationsschnittstellen (UMTS/LTE/5G, WLAN, Bluetooth, NFC, ...) ist das Internet mit seinen Diensten stets und überall verfügbar. Sehr leistungsstarke Endgeräte sind immer und fast überall nutzbar, sowie einfach und schnell über Touchscreens zu bedienen. Mobile Geräte sind multifunktional: Handy, Navi, Musik/TV-Gerät, Medizin-/Gesundheitsgerät ..., Zugang zum Unternehmen, Internet-Dienste ..., universeller Computer/Apps – alles in einem mobilen Gerät. Mit „Local Based Service“ kommen nützliche und innovative Dienste vor Ort hinzu.



**Abb. 1.5** Risiken bei mobilen Geräten

Mit diesen mobilen Geräten sind aber auch neue Angriffsvektoren entstanden, die weitere Risiken verursachen. Ständig wechselnde unsichere Umgebungen (Flughäfen, Bahnhöfe, Cafés) erhöhen die Wahrscheinlichkeit des unabsichtlichen Verlustes oder des gezielten Diebstahls der mobilen Geräte, auf denen zunehmend wertvolle Daten gespeichert werden, siehe Abb. 1.5. Die Gefahr für die Privatsphäre der Nutzer (zum Beispiel durch eine Bewegungsprofilbildung) und die einfache Möglichkeit der Einsichtnahme in der Öffentlichkeit sind nicht zu unterschätzen. Die Nutzung von „bösaartigen“ Apps, das heißt, Malware auf mobilen Geräten, die Daten auslesen, wird durch das Prinzip „Masse statt Klasse“ wahrscheinlicher. Aber auch die Nutzung von falschen oder manipulierten Hotspots wird durch „mal schnell E-Mails checken“ immer häufiger zum Angriffspunkt auf die Werte. Eine weitere Gefahrenquelle für Unternehmen ist die parallele Nutzung von mobilen Geräten für private und berufliche Zwecke (zum Beispiel Bring Your Own Device). Ein großes Problem dabei ist, dass die meisten mobilen Geräte für den Consumer-Markt erstellt werden. Hier wird von den Anbietern die folgende Strategie verfolgt: Die mobilen Geräte, wie zum Beispiel das iPhone, müssen für den unerfahrenen anzunehmenden Nutzer erstellt werden und praktisch intuitiv bedient werden können. Erst einmal funktioniert alles; wenn der Nutzer mehr Sicherheit möchte, dann müsste er Einschränkungen vornehmen, was er meistens gar nicht kann. Eine Business-Strategie mit dem Fokus auf Sicherheit hingegen wäre: Es funktioniert erst einmal gar nichts und der Nutzer muss Funktionen freischalten, die er unbedingt für die Erfüllung seiner Aufgabenstellung braucht (Principle of Least Privilege). Dadurch würde die Angriffsfläche auf mobilen Geräten schon deutlich reduziert.

**Wichtig** Mobile Geräte haben neue Angriffsvektoren hervorgerufen, die weitere Risiken verursachen.

### **1.2.6 Cyber-Sicherheitsproblem: „Eine E-Mail ist wie eine Postkarte!“**

Es wird vom E-Mail-Dienst keine Vertraulichkeit garantiert. Passwörter, Kreditkartennummern und weitere Bankdaten sowie vertrauliche Informationen werden im Klartext übertragen und stellen so ein großes Risiko dar. Die Möglichkeiten, eine E-Mail unerlaubt abzugreifen sind sehr hoch. In einigen Ländern werden alle E-Mails analysiert, um zum Beispiel an das Know-how von Firmen anderer Länder zu kommen. Damit sind E-Mails gegenwärtig ein weiterer großer Risikofaktor.

Untersuchungen und Befragungen zeigen auf, dass zurzeit zu wenig E-Mails (wahrscheinlich 5 %) verschlüsselt werden [4]. Es ist aber auch bekannt, dass mindesten 43 % der E-Mails in Business-Prozessen verwendet werden. Aus diesem Grund sollten den Mitarbeitern im Unternehmen E-Mail-Verschlüsselungstechnologien zur Verfügung gestellt werden. Typischerweise kommen in der Regel zwei verschiedene Standards zum Einsatz. Dies ist zum einen S/MIME, der vermehrt in größeren Unternehmen verwendet wird, und zum anderen OpenPGP, der schnell und unabhängig ohne Unternehmensserver auf den IT-Systemen des Anwenders betrieben werden kann. Außerdem müssen die Mitarbeiter wissen, wie und – ganz wichtig – wann diese Verschlüsselungstechnologien für vertrauliche E-Mails verwendet werden sollten. Hier muss der Arbeitgeber für Sensibilisierung seiner Angestellten sorgen. Den Mitarbeitern muss bewusst sein, dass Kunden- und Firmendaten besonders sensibel und schützenswert für das Unternehmen und seinen Arbeitsplatz sind.

**Wichtig** E-Mail ist eine wichtige Kommunikationsinfrastruktur, insbesondere im Geschäftsumfeld, aber die Umsetzung und Nutzung von Cyber-Sicherheitslösungen ist viel zu gering.

### **1.2.7 Cyber-Sicherheitsproblem: „Geschäftsmodell: Bezahlen mit persönlichen Daten“**

Viele Online-Dienste und vor allem soziale Netzwerke wie Facebook, Partnerbörsen, YouTube, XING, LinkedIn, Twitter und Co. bringen Nutzer aus verschiedenen Gesellschaftsgruppen zusammen und ermöglichen den Nutzern, sich darzustellen und sich real zu begegnen. Soziale Netzwerke schaffen auch neue Wege, Demokratie und Bürgerbeteiligungen zu gestalten, was eine neue und ungewohnte Herausforderung für alle Beteiligten darstellt. Außerdem bringen soziale Netzwerke die Diskussion über die Informationelle Selbstbestimmung und den Datenschutz auf. Die Technologien für das Sammeln und Verknüpfen von Daten im Hintergrund werden immer vielfältiger. Gesetzliche Limitierungen hinken dem Innovationspotenzial der Datensammler hinterher, insbesondere wenn es um internationale Lösungen geht.

Eine Frage dazu ist, inwieweit Internetangebote zu tolerieren sind, bei denen nicht mit Geld, sondern mit persönlichen Daten bezahlt wird. Mit der Akzeptanz der AGB wird zugelassen, dass die Anbieter und deren Partner über Profilbildungen indirekt Geld verdienen können. Aus den erhobenen persönlichen Daten der Nutzer erstellen Betreiber sozialer Netze Nutzerprofile, die unter anderem für den Verkauf von Waren und Dienstleistungen genutzt werden, weil sie passgenaue, individualisierte Werbung ermöglichen. Zielgenaue Werbung lassen sich die Betreiber vieler sozialer Netzwerke durch das Schalten von individualisierten Anzeigen gut bezahlen. Dieses Prinzip „Bezahlen mit persönlichen Daten“ wird auch bei anderen Diensten, wie Suchmaschinen, E-Mail-Diensten und Nachrichten-Diensten, angewendet. Aber auch im Bereich von E-Commerce, wie beispielsweise beim Online-Versandhaus Amazon, werden personenbezogene Daten erhoben, gespeichert und ausgewertet, um den Kunden individuelle Angebote machen zu können [5]. Hier werden die wichtigen und notwendigen Persönlichkeitsrechte sehr stark berührt. Die Herausforderung in diesem Bereich ist, die Aufklärung der Nutzer über die Risiken und eine gemeinsame angemessene Lösung mit den Anbietern von sozialen Netzwerken zu finden und umzusetzen.

Nur eine klare Übersicht über die eigenen persönlichen Daten, die bei den Internet-Dienstanbietern gespeichert sind, hilft, sich selbstbestimmt im Internet zu bewegen. Der Online Privacy Service (OPS) stellt einen zukunftsweisenden Lösungsvorschlag für die Anbieter von Internet-Diensten dar und ist eine pragmatische Umsetzungsmöglichkeit des Rechtes, vergessen zu werden (neue EU-Datenschutzverordnung – DSGVO). OPS zeigt auf, wie eine aktive informationelle Selbstbestimmung im Internet umgesetzt werden kann, die die Wahrung der Grundrechte der Nutzer gewährleistet und damit das Internet vertrauenswürdiger macht [6].

**Wichtig** Das Geschäftsmodell „Bezahlen mit persönlichen Daten“ birgt Risiken für die Persönlichkeitsrechte.

### 1.2.8 Cyber-Sicherheitsproblem: „Internetnutzer haben zu wenig Internet-Kompetenz“

Internetnutzer müssen die Gefahren des Internets kennen, sonst schaden sie sich und – über beispielsweise infizierte E-Mails, Dateien, USB-Geräte – anderen. Laut einer BITKOM-Umfrage von 2012 haben 30 % der Internetnutzer keine Personal Firewall und 28 % keine Anti-Malware-Lösung auf ihrem IT-System und sind damit nicht angemessen geschützt. Es besteht noch ein sehr großer Nachholbedarf, die Internetnutzer so auszubilden, dass sie in der Lage sind, sich selbst angemessen zu schützen [7].

Auf der anderen Seite wird zurzeit sehr viel von den Nutzern verlangt. Bei einem Vergleich der Situation mit dem Kauf eines Autos würde das bedeuten, dass

der Verkäufer zum Käufer sagt: „Nehmen Sie sich ein paar Airbags, Sicherheitsgurte und Bremsschläuche mit. Bitte denken Sie daran, dass Sie dies einbauen müssen, bevor Sie losfahren.“ Autos würden heute so nicht verkauft werden. In der IT wird dieser Zustand akzeptiert und die Herausforderungen müssen mit viel Kompetenz kompensiert werden.

Hier muss noch viel Aufklärungsarbeit in einfacher, zugänglicher Form geleistet werden. Ein gutes Beispiel dafür ist die Initiative „Der 7. Sinn im Internet“: Ein Netzwerk von Experten erstellt Videos zum Umgang im Internet sowie mit mobilen Endgeräten. Angelehnt an die Stilistik der aus den 70er-Jahren bekannten TV-Reihe „Der 7. Sinn“ möchten die kurzweiligen Videoclips auf Gefahren und Hindernisse im digitalen Alltag aufmerksam machen und den Zuschauern zeigen, wie sie selbst etwas für ihre eigene Cyber-Sicherheit tun können.

Die Videos sind kostenlos verfügbar unter: <https://www.it-sicherheit.de/videos/cyberschutzraum/>.

**Wichtig** Wegen der großen Cyber-Sicherheitsprobleme besteht ein hoher Bedarf, die Internetnutzer über die Risiken aufzuklären und sicheres Verhalten zu schulen.

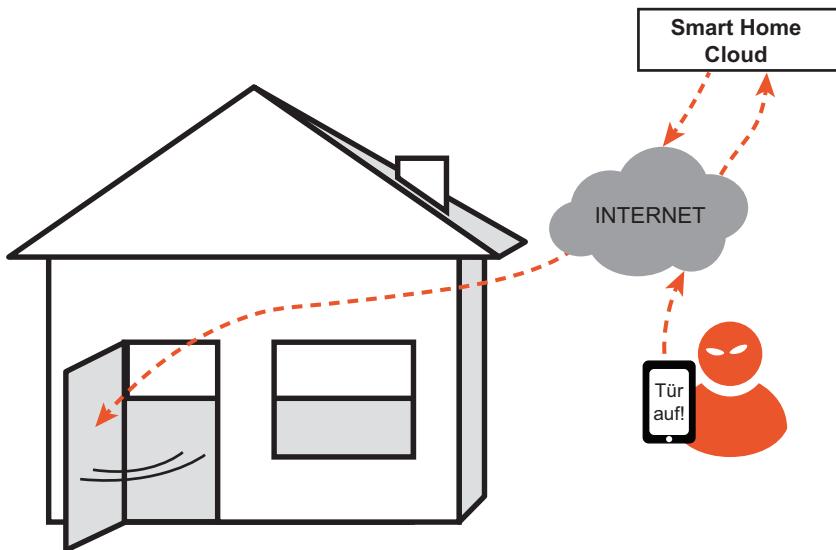
### 1.2.9 Cyber-Sicherheitsproblem: „Manipulierte IT und IT-Sicherheitstechnologien“

Es passiert immer wieder, dass Firmen und/oder Geheimdienste in Cyber-Sicherheitsprodukte Hintertüren einfügen sowie Cyber-Sicherheitsstandards- und -technologien manipulieren. Schlechte Zufallszahlengeneratoren in Cyber-Sicherheitsprodukten machen zum Beispiel die Verschlüsselung nutzlos, weil der Angreifer den verwendeten Schlüssel „leicht“ bestimmen kann. Es wird viel Geld für Verschlüsselungsprodukte ausgegeben, die keinen Nutzen haben. Das ist eine wirklich schlechte Situation für alle.

**Wichtig** Firmen und/oder Geheimdienste fügen in Cyber-Sicherheitsprodukte Hintertüren ein, manipulieren Cyber-Sicherheitsstandards und -technologien und machen so das Geschäftsleben und die Internetaktivitäten unsicher!

### 1.2.10 Cyber-Sicherheitsproblem: „Unsichere IoT-Geräte“

Die Hersteller von IT-Geräten aus dem Bereich des Internet der Dinge, wie zum Beispiel Internet-Videokameras, haben IT-Technologie zur Verfügung gestellt, bei der bei weitem nicht die Cyber-Sicherheitsanforderungen erfüllt waren. Wenn



**Abb. 1.6** Einbruch durch Hacken von Smart Home Devices

einfache Internet-Videokameras gehackt werden können, ist das erst mal ein Problem des Anwenders. Wenn Angreifer ein Wohnzimmer beobachten können, verletzt das die Persönlichkeitsrechte des Bewohners und erhöht die Wahrscheinlichkeit eines Einbruches, wenn dieser nicht zu Hause ist.

Einbruch durch Hacken von Smart Home Devices, siehe Abb. 1.6.

1. IP-Kameras: Überprüfen, ob jemand im Haus ist
2. Türe öffnen
3. Haus leer räumen, ...

Ein weit größeres Problem ist auch schon als Herausforderung identifiziert. Angreifer haben sehr viele Internet-Videokameras und weitere IT-Geräte, die mit dem Internet verbunden sind, wie Drucker, Föne, Kaffeemaschinen usw. fremdgenutzt, um die Infrastruktur des Internets insgesamt erfolgreich mithilfe von DDoS anzugreifen. Dies ist ein sehr großes Problem und macht das Internet sehr verletzlich und damit nicht verlässlich. Dieser Zustand sorgt dafür, dass viele wichtige Cyber-Sicherheitsexperten eine generelle Zulassung von IT-Geräten auf der Basis von Zertifizierungen für das Internet als Lösung verlangen.

Die IT-Hersteller müssen eine besondere Verantwortung übernehmen und nur noch sichere und vertrauenswürdige IT-Geräte im Internet zu Verfügung stellen, die den Stand der Technik im Bereich der Cyber-Sicherheit berücksichtigen. Außerdem muss die Produkthaftung deutlich schärfer umgesetzt werden, damit die IT-Hersteller und Anbieter ihr Interesse an sicheren Lösungen erhöhen. Die wichtigen Player im Internet müssen mehr Verantwortung übernehmen, sonst

sind „der Motor“ und die Basis für das Wohlergehen der modernen und globalen Gesellschaft in Gefahr. Aber auch die Nutzer müssen verantwortungsvoll handeln und die Konsequenzen des Tuns tragen: Anzahl und Funktionalität der Geräte sollte mit Bedacht gewählt werden. Denn jedes IT-Gerät kann Sicherheitslücken aufweisen und sensible Werte angreifbar machen. Deshalb muss dem Nutzenden bewusst sein, wie hoch das Schutzniveau seiner IoT-Geräte ist und wie sorgsam er bei der Verwendung sein sollte.

**Wichtig** IoT-Geräte geraten immer mehr in das Visier von Angreifern und benötigen daher besonderen Schutz von Anwendern und Anbietern.

### 1.2.11 Cyber-Sicherheitsproblem: „Fake News“ und weitere unerwünschte Inhalte

Eine weitere Herausforderung liegt im Bereich von Fake News, rechtswidrige Inhalte, Hasskommentare, Cyber-Mobbing, Wahlmanipulation, Gewaltvideos ...

Mit Web 2.0 generieren die Nutzer Inhalte. Jeder Nutzer stellt seine Inhalte selber ein. Aber wie kann erkannt werden, ob der Inhalt echt, richtig, vertrauenswürdig usw. ist?

Wie schnell können die Dienstanbieter die Inhalte löschen, und zwar ohne dass sie zu viel löschen? Welchen Institutionen kann diese Verantwortung übertragen werden? Eine überwachende Instanz ist zwingend nötig, um die Persönlichkeitsrechte von potenziellen Opfern zu schützen. Aber wie kann Kontrolle bei dieser Schnelllebigkeit und den unvorstellbaren Mengen an Daten (bei Facebook allein 60 Mio. Bilder pro Tag, die gepostet werden, Statistik [Socialmedia-Institute.com](http://Socialmedia-Institute.com) 7/2016) überhaupt funktionieren und Zensur verhindert werden? Auch hier würden aufgeklärte und selbstbestimmte Nutzer für erhebliche Erleichterung sorgen. Eine sensible Eigenverantwortlichkeit der Nutzer aus allen Altersklassen und sozialen Schichten sowie empfindliche Strafen bei Zu widerhandlungen wären Schritte in die richtige Richtung.

**Wichtig** Mittels Fake-News lassen sich Menschen in ihrem Handeln stark beeinflussen (zum Beispiel bei Wahlen).

Sicherlich gibt es noch viele weitere Herausforderungen, die hier beschrieben werden könnten und noch deutlich mehr, die erst in der Zukunft auftreten werden. Der Druck, mehr wirkungsvolle Cyber-Sicherheitslösungen einzuführen, ist daher immens.

### 1.3 Problematische Rahmenbedingungen

Weitere Herausforderungen resultieren auch aus den Veränderungen der Rahmenbedingungen, die mit der Dynamik des Internets und der Digitalisierung einhergehen. Das Internet ist global und geht über alle Grenzen und Kulturen hinaus. Es gibt insbesondere im E-Commerce unterschiedliche Auffassungen darüber, was richtig und was falsch ist. Die Unsicherheiten bei verschiedenen Rechtssystemen müssen berücksichtigt werden. Es gibt noch zu viele Länder, in denen keine Strafverfolgung möglich ist. Außerdem findet eine radikale Entwicklung und Veränderung in der IT und im Internet statt, zum Beispiel durch mobile Geräte, soziale Netze wie Facebook und Twitter oder durch Cloud Computing sowie die Internetfizierung von Kritischen Infrastrukturen. Der Alltag wird immer mehr durch künstliche Intelligenzen begleitet (zum Beispiel autonome Fahrzeuge), was neue ethische Fragen aufwirft und das Leben nachhaltig ändern wird. Durch neue Technologien, neue IT-Konzepte, neue Angriffsstrategien und neue Player im IT-Markt treten neue Gegebenheiten und Rahmenbedingungen auf, die immer wieder sehr schnell berücksichtigt und bewertet werden müssen.

**Wichtig** Die Dynamik im Internet verändert die Rahmenbedingungen sehr schnell und damit die Notwendigkeit, die IT-Sicherheitsarchitekturen rasch und bedarfsgerecht anzupassen.

---

### 1.4 Gesellschaftliche Sichtweise auf die Cyber-Sicherheitsprobleme

In diesem Abschnitt werden unterschiedliche gesellschaftliche Sichtweisen auf die Cyber-Sicherheitsprobleme dargestellt und diskutiert.

#### 1.4.1 Privatsphäre und Datenschutz

Der Aspekt Privatsphäre spielt für jeden Bürger eine sehr wichtige Rolle. Eine Gesellschaft, die wirtschaftlich und politisch auf die Eigenverantwortlichkeit des Einzelnen setzt, muss umgekehrt das schützen, was den einzelnen als Sozialwesen und als Wirtschaftsfaktor ausmacht: einerseits seine persönliche Integrität und andererseits seinen materiellen Besitz. Wenn eine Gesellschaft nicht mehr in der Lage ist, diese Anforderungen zu erfüllen, dann verliert sie einen Teil der Demokratie und gibt Freiheit auf. Die gesellschaftlichen Reaktionen sind in der Summe, bezogen auf die Schwere des Angriffes auf die Privatsphäre und die Auswirkungen für die Gesellschaft, unangemessen und viel zu zurückhaltend. Eine offene und aktive Diskussion darüber, wie der Datenschutz und die Privatsphäre in

der Zukunft gestaltet werden können sowie welche Rolle sie spielen sollen, wird intransparent und für den Endverbraucher nicht nachvollziehbar von einigen wenigen Fachleuten geführt.

Es können unterschiedliche Sichtweisen betrachtet werden:

### Kulturelle Unterschiede

Wenn in den USA Nutzer gefragt werden, wem die Daten in einem sozialen Netzwerk gehören, dann sagen 76 %: Dem Unternehmen, das das soziale Netzwerk betreibt, zum Beispiel Facebook oder Google. Bei der gleichen Frage in Deutschland würden diese Sicht nur 22 % teilen und 78 % wären der Meinung, dass die Daten, demjenigen gehören, der sie eingestellt hat, also dem Nutzer (Quelle: Pemon Institute).

Da die meisten wichtigen sozialen Netzwerke aus den USA kommen, verwundert es nicht, dass die AGB so gestaltet sind, wie sie sind.

### Geschäftsmodell „Bezahlen mit persönlichen Daten“

Fast alle Internet-Nutzer nutzen die Google-Suche. Die Google-Suche gibt es schon seit 1997 und ein Leben ohne sie ist nicht mehr vorstellbar. Kein Nutzer musste bis jetzt für diesen wertvollen Dienst Geld bezahlen. Die Nutzer zahlen kein Geld, sondern erlauben stattdessen, dass die Internet-Dienstanbieter ihre persönlichen Daten nutzen können, in der Regel für das Schalten von personalisierter Werbung. Google weiß durch dessen Aktivitäten viel über den Nutzer. Diese Informationen werden für Werbung genutzt, könnten aber potenziell auch anders verwendet werden, siehe auch Kap. 16, Teil „Web 2.0 Sicherheit“.

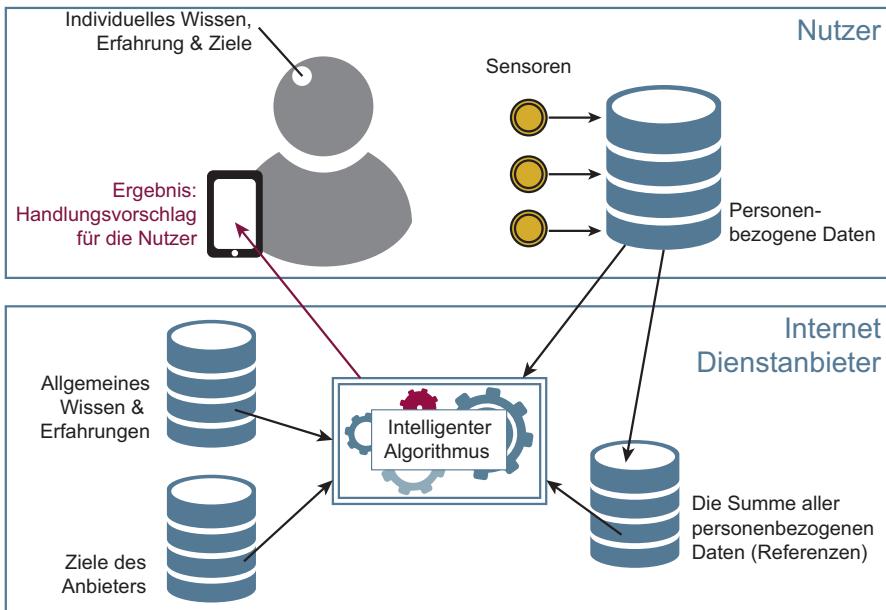
Viele Nutzer würden gerne für die Google-Suche bezahlen, aber das bietet Google nicht an.

Google verdient zum Beispiel zurzeit über 100 Mrd. US\$ mit Werbung! Das Geschäftsmodell „Bezahlen mit persönlichen Daten“ birgt große Risiken für die Persönlichkeitsrechte.

### Identifizieren von terroristischen Aktivitäten durch den Staat

Viele Staaten versuchen über das Mitlesen von persönlichen Daten in sozialen Netzwerken, auf den IT-Systemen und während der Übertragung der Daten über das Internet terroristischen Aktivitäten zu identifizieren. Dazu nehmen die Staaten die Schwächung des allgemeinen IT-Sicherheitslevels in Kauf. Klar ist, dass Straftaten im Internet aufgedeckt werden müssen, aber nicht auf der Grundlage der Unsicherheit aller Bürger und Unternehmen.

**Wichtig** Der Aspekt Privatsphäre spielt für jeden Bürger eine sehr wichtige Rolle.



**Abb. 1.7** Handlungsvorschläge für die Nutzer auf der Basis intelligenter Algorithmen

#### 1.4.2 Selbstbestimmung und Autonomie

Internet-Dienste machen Handlungsvorschläge für die Nutzer auf der Basis verschiedener Arten von Sensoren, wie Wearables, Smartphones, Internet-Dienste usw. Intelligente Algorithmen nutzen diese vielen privaten Sensordaten, bewerten sie, vergleichen sie mit privaten Daten von anderen Menschen und nutzen allgemeines Wissen und Erfahrungen, um Handlungsempfehlungen für die Nutzer zu berechnen, siehe Abb. 1.7.

Das kann sehr nützlich sein, bezogen auf eine gute Entscheidung für eine Handlung. Der individuelle Mensch mit seinem persönlichen Wissen, seinen Erfahrungen und seiner Intuition sowie zusätzlich intelligente Algorithmen mit sehr vielen Daten und fast unbegrenzter Rechnerpower sind eine optimale Ergänzung.

Wenn die Internet-Dienste das transparent machen, sind gut berechnete Handlungsempfehlungen für eine optimale Handlungsentscheidung sehr hilfreich.

Verdienen die Internet-Dienste aber mit solchen Diensten indirekt Geld, wird die berechnete Handlungsempfehlung eher im Interesse des Internet-Dienstes und dessen Kunden liegen als im Interesse der Nutzer. Jeder Nutzer wird zwangsläufig zum Produkt. Das Problem dabei ist, dass die Menschen dadurch ihre Selbstbestimmung verlieren können. Das kann eine moderne Gesellschaft nicht wollen.

**Wichtig** Selbstbestimmung im Internet bei der Nutzung von Diensten erlaubt es, das Handeln selbst zu gestalten und autark zu agieren.

### 1.4.3 Wirtschaftsspionage

Die Wirtschaftsspionage ist eine weitere gesellschaftliche Herausforderung. 100 Mrd. EUR Schaden entstehen jährlich im Bereich der Wirtschaftsspionage laut dem Verein Deutscher Ingenieure (VDI). Die Schäden beinhalten insbesondere Umsatzeinbußen von 23 Mrd. EUR durch Plagiate, Kosten von 18,8 Mrd. EUR durch Patentrechtsverletzungen und Verluste durch Ausfall, Diebstahl oder Beeinträchtigen von IT-Systemen sowie Produktions- und Betriebsabläufen von 13 Mrd. EUR.

Diesen hohen Betrag an Schaden kann sich Deutschland als große Wissensgesellschaft nicht leisten. Die Angreifbarkeit der IT und des Internets wird immer größer und Werte, die als Bits und Bytes zur Verfügung stehen, werden immer risikobehafteter für die einzelnen Unternehmen, die Bürger und den Staat. Experten aus der Cyber-Sicherheit, Wirtschaft und Politik müssen aktiv werden und mit den unterschiedlichen Stakeholdern geeignete Cyber-Sicherheitsmaßnahmen einleiten, um das Know-how deutlich wirkungsvoller zu schützen.

Der Bereich Internet-Kriminalität mit erfolgreichen Angriffen auf Online-Banking und Distributed Denial of Service (DDoS)-Angriffen, verursacht jährlich einen Schaden von ca. 100 Mio. Euro. Zusätzlich sollte beachtet werden, dass die Dunkelziffer in diesem Bereich sehr hoch sein wird. Insbesondere die Bereiche DDoS und Erpressungen mit der Androhung von DDoS sind zurzeit ein lukrativer Bereich für kriminelle Organisationen.

**Wichtig** Die Angreifbarkeit der IT und des Internet werden immer größer und Werte, die als Bits und Bytes zur Verfügung stehen, werden immer risikobehafteter. Damit steigt auch der Schaden, wenn nicht weitere wirkungsvolle Cyber-Sicherheitssysteme genutzt werden.

### 1.4.4 Cyberwar

Eine weitere und immer bedeutsamere Herausforderung ist Cyberwar. Cyberwar ist, wenn Staaten oder Terroristen ihre politischen Ziele „einfach“ und „preiswert“ durch Angriffe auf Kritische Infrastrukturen von Gesellschaften umsetzen.

Angriffe auf Kritische Infrastrukturen wie die Energieversorgung stellen eine prinzipiell höhere Verwundbarkeit der Gesellschaft dar und bilden eine neue Ebene der existenziellen Bedrohung.

Mit *Stuxnet* wurde dokumentiert, dass mit einem Kostenaufwand von rund 9 Mio. US\$ für eine intelligente Malware politische Ziele einfach und sehr erfolgreich umgesetzt werden können. Mit der intelligenten Malware *Stuxnet* haben die Amerikaner und Israelis zusammen die Uran-Aufbereitung im Iran um zwei Jahre verzögern können.

Die schreckliche Alternative dieses politischen Ziels wäre gewesen, dass mehrere hunderttausend Soldaten in den Iran einmarschiert wären, was nicht nur Kosten von mehreren Milliarden US\$ verursacht, sondern auch Menschenleben aufs Spiel gesetzt hätte. Auf diese neue Wirklichkeit von Cyberwar muss professionell reagiert werden.

**Wichtig** Die erfolgreiche Umsetzung von politischen Zielen mithilfe von Cyberwar muss in ihrer Wirkung deutlich reduziert werden.

## 1.5 Herausforderungen der Cyber-Sicherheit

Die Cyber-Sicherheitsprobleme sind hinreichend bekannt, doch die heute vorhandene und genutzten IT- und Cyber-Sicherheitsmaßnahmen reduzieren das Cyber-Sicherheitsrisiko nicht ausreichend. Es ist ein Paradigmenwechsel in der Cyber-Sicherheit notwendig, um das Risiko für die Gesellschaft auf ein angemessenes Maß zu reduzieren.

**Im Folgenden werden einige innovative Ideen exemplarisch und prinzipiell aufgezeigt:**

### 1.5.1 Paradigmenwechsel „Verantwortung versus Gleichgültigkeit“

Zurzeit bestimmen die großen Technologiehersteller und Dienstleistungs-Anbieter was Nutzer brauchen. Doch die Verantwortung für Cyber-Sicherheit und Vertrauenswürdigkeit ihrer IT-Lösungen übernehmen sie nicht ausreichend. Was allerdings dringend benötigt wird, ist eine Herstellerverantwortung wie in der Automobilbranche. Wenn heute ein Auto gekauft wird, übernimmt der Hersteller, bei dem das Auto gekauft wird, dem Kunden gegenüber die volle Verantwortung. Auch die Automobilhersteller arbeiten mit mehreren hundert Zulieferern zusammen. Und doch gibt es für den Kunden immer nur einen Ansprechpartner. Die Hersteller lassen die Autos überprüfen und wenn sie einen Fehler erkennen, werden große Rückrufaktionen gestartet, um Fehler zu beheben, bevor die eigentlichen Probleme auftreten. Dies hat ein sehr großes Vertrauen zu den Herstellern aufgebaut. Bei IT-Systemen ist bis dato keine klare Struktur der Verantwortung etabliert. Die IT-Hersteller müssten beginnen, die Gesamtverantwortung zu übernehmen – dann würden die heutigen Cyber-Sicherheitsprobleme deutlich geringer ausfallen. Alle Softwareprogramme und die Hardware wären besser aufeinander abgestimmt und Fehler würden einfacher gefunden und behoben werden.

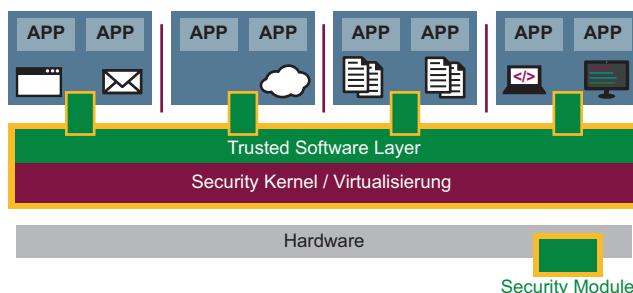
**Wichtig** Die Übernahme von Verantwortung für die übergreifende Umsetzung von Cyber-Sicherheitssystemen ist ein besonders wichtiger Aspekt für den Level der Cyber-Sicherheit.

### 1.5.2 Paradigmenwechsel „Proaktive versus reaktive Cyber-Sicherheitslösungen“

Bei den heutigen reaktiven Cyber-Sicherheitssystemen, wie Anti-Spam-, Anti-Malware-, Intrusion-Detection-Systemen, wird den IT-Angriffen hinterhergerannt. Das bedeutet, wenn die Cyber-Sicherheitslösungen einen Angriff durch eine entsprechende Angriffssignatur oder eine Anomalie erkennen, dann versuchen sie, so schnell wie möglich zu schützen, um den Schaden zu reduzieren. Die zunehmende Vielfalt und Komplexität der IT-Systeme und IT-Infrastrukturen brauchen aber deutlich verlässlichere, robustere und wirkungsvollere Cyber-Sicherheitskonzepte. Daher sollte die Strategie, weg von ausschließlich reaktiven hin zu modernen proaktiven Cyber-Sicherheitssystemen sein, damit eine Ausführung von intelligenter Malware, eines der größten Probleme zurzeit, verhindert werden kann. Solche proaktiven Cyber-Sicherheitssysteme arbeiten mit einem kleinen Sicherheitskern (sichere Betriebssysteme) und Virtualisierung, können Software messbar machen und mit einer starken Isolation Anwendungen mit ihren Daten separieren und so nachhaltige und angemessene Cyber-Sicherheit bieten [8]. Die prinzipielle Architektur ist in Abb. 1.8 dargestellt.

Für proaktive Cyber-Sicherheitssysteme muss die Softwarearchitektur der IT-Systeme allerdings grundlegend anders aufgebaut sein als bisher. Außerdem müssen Sicherheits-Infrastrukturkomponenten gemeinsam umgesetzt werden, damit diese Cyber-Sicherheits- und Vertrauenstechnologien organisationsübergreifend genutzt werden können.

Auf der Forschungsebene wurden die Vorteile der proaktiven Cyber-Sicherheitssysteme schon längst dargestellt und nachgewiesen [9]. Die ersten Cyber-Sicherheitsunternehmen bieten ausgereifte Lösungen. Jetzt wird es Zeit,



**Abb. 1.8** Moderne und wirkungsvolle IT-Sicherheitsarchitekturen

dass diese von der Industrie und den Behörden eingeführt werden, damit eine notwendige höhere Sicherheit und Vertrauenswürdigkeit der IT-Systeme und IT-Infrastrukturen erzielt werden kann, siehe Kap. 7, „Trusted Computing“.

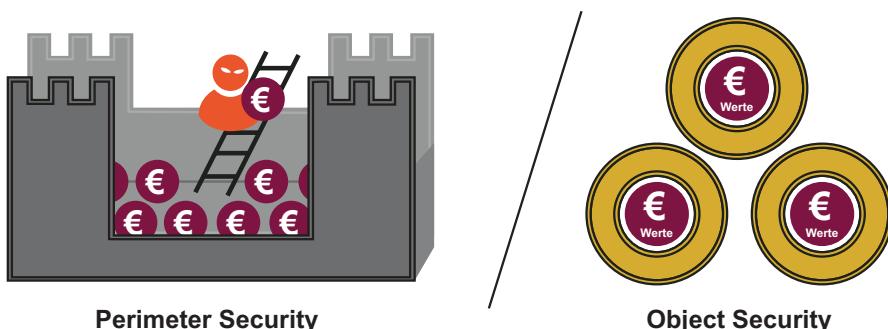
**Wichtig** Proaktive Cyber-Sicherheit muss zusammen mit den Marktführern in der IT flächendeckend umgesetzt werden.

### 1.5.3 Paradigmenwechsel „Objekt-Sicherheit versus Perimeter-Sicherheit“

Perimeter-Sicherheit soll zum Beispiel mithilfe von Firewall- und VPN-Systemen verhindern, dass Fremde aus dem Internet auf das eigene Unternehmensnetz zugreifen können (Abschottung) und dass die ausgetauschten Daten nicht von anderen gelesen und manipuliert werden können. Da aber immer mehr mobile Geräte über alternative Kommunikationswege, wie Mobilfunknetze und Hotspots, vorbei an der zentralen Unternehmens-Firewall ins Internet gehen, verliert die Perimeter-Sicherheit an Wirkung und Bedeutung. Bei Objekt-Sicherheit und Informationsflusskontrolle werden die Objekte mit Rechten versehen, die definieren, wer sie in welcher IT-Umgebung wie nutzen darf. Die Objekte werden dadurch über ihren ganzen Lebenszyklus vertrauenswürdig gesichert, siehe Abb. 1.9.

Voraussetzung ist, dass mithilfe von proaktiven Cyber-Sicherheitssystemen die Umsetzung von Policies auch auf fremden IT-Systemen durchgeführt werden kann. Auch hier werden internationale Cyber-Sicherheitsinfrastrukturen gebraucht, damit im Prinzip jeder mit jedem sicher und vertrauenswürdig Objekte austauschen kann, siehe Kap. 7, „Trusted Computing“.

**Wichtig** Objekt-Sicherheit auf der Basis von vertrauenswürdigen IT-Systemen bietet strategisch eine sehr hohe Wirksamkeit für die Cyber-Sicherheit.



**Abb. 1.9** Objekt-Sicherheit versus Perimeter-Sicherheit

#### 1.5.4 Paradigmenwechsel „Cloud-Service versus Lokal-IT“

Eine vollständige „Cloudifizierung“ im Gegensatz zur heutigen nur teilweisen Nutzung von Cloud-Diensten wird sich durchsetzen. Es ist keine Frage von „ob in die Cloud“, sondern lediglich „wann“, und bei diesem Prozess spielen Cyber-Sicherheitslösungen für die Cloud eine wichtige Rolle. Der vergleichsweise mittelmäßige Cyber-Sicherheitslevel von heute wird deutlich höher werden, um die Werte der Unternehmen, die Daten, angemessen zu schützen.

**Wichtig** Cloud-Sicherheit spielt in der Zukunft eine wichtige Rolle.

#### 1.5.5 Paradigmenwechsel „Dezentrale versus zentrale Cyber-Sicherheit“

Statt aufwendige, zentrale Cyber-Sicherheitslösungen wie PKIs werden für die automatisierte vertrauenswürdige Zusammenarbeit verschiedener Unternehmen dezentrale Cyber-Sicherheitslösungen immer wichtiger. Die Blockchain-Technologie stellt ein „programmiertes Vertrauen“ zur Verfügung, weil alle Cyber-Sicherheitseigenschaften als Security-by-Design inhärent in die Blockchain-Technologie eingebunden sind. Die Blockchain-Technologie (siehe Kap. 14) schafft eine Grundlage für verteilte, automatisierte und vertrauenswürdige Zusammenarbeit und hat ein hohes Potenzial für neue Geschäftsmodelle und Ökosysteme.

**Wichtig** Die Blockchain-Technologie schafft eine Grundlage für verteilte, automatisierte und vertrauenswürdige Zusammenarbeit und hat ein hohes Potenzial für neue Geschäftsmodelle und Ökosysteme.

#### 1.5.6 Paradigmenwechsel „datengetriebene- versus eventgetriebene-Sicherheit“

Heute wird überwiegend über identifizierbare Events versucht, Angriffe zu erkennen. Zukünftig werden mithilfe von Künstlicher Intelligenz aus immer mehr vorhandenen Daten sicherheitsrelevante Informationen extrahiert, die helfen, für bessere und schnelle Cyber-Sicherheit zu sorgen. Data Science mit Technologien des maschinellen Lernens und Künstlicher Intelligenz verspricht Innovationen bei der Erkennung von Angriffen, neben vielen anderen wichtigen Aspekten wie Authentifizierung oder Threat Intelligence im Bereich der Cyber-Sicherheit (siehe auch Kap. 15 „Künstliche Intelligenz und Cyber-Sicherheit“).

**Wichtig** Zukünftig werden mithilfe Künstlicher Intelligenz aus immer mehr vorhandenen Daten sicherheitsrelevante Informationen extrahiert, die helfen werden, für bessere Cyber-Sicherheit zu sorgen.

### 1.5.7 Paradigmenwechsel „Zusammenarbeit versus Isolierung“

Die grundsätzlich unsichere und schlecht umgesetzte Technologie sowie die unzureichende Internet-Kompetenz der Nutzer sorgen dafür, dass Angriffe Schäden verursachen. Ist eine Firma Opfer eines Angriffes geworden, versucht sie in der Regel, das Problem alleine und isoliert zu lösen. Die Informationen über erfolgte Angriffe, die Vorgehensweise der Angreifer, den Umfang von Schäden und die Wirkung von Gegenmaßnahmen bleiben somit für die Gesellschaft ungenutzt. Durch eine geordnete und vertrauenswürdige Zusammenarbeit von Firmen und Behörden würde eine deutlich höhere Gesamt-Cyber-Sicherheit erreicht werden können. Dann wäre zum Beispiel die Sicherheitslage besser einschätzbar, die kritischen Schwachstellen würden gemeinsam identifiziert, die Widerstandsfähigkeit zusammen erhöht, die Verteidigungskosten reduziert und der Zugang zu qualifizierten Cyber-Sicherheitsexperten optimiert. Aus diesem Grund werden Business-Modelle und Vertrauenskonzepte benötigt, die zu einer Zusammenarbeit motivieren (sollen) – Business-Modelle, die insgesamt weniger Geld für Cyber-Sicherheitsmaßnahmen erfordern und als Resultat ein gemeinsames geringeres Schadensrisiko für alle kooperierenden Firmen erzielen.

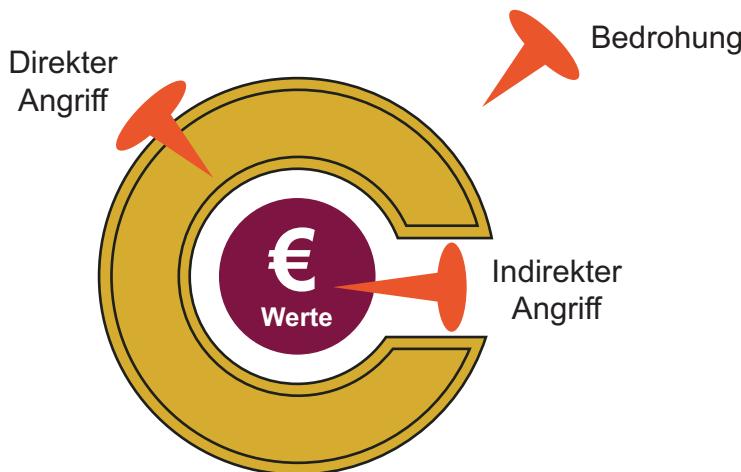
**Wichtig** Die Zusammenarbeit bei der Cyber-Sicherheit erhöht den Level und reduziert die Kosten.

## 1.6 Konzept der Wirksamkeit von Cyber-Sicherheitssystemen

Für die Beurteilung von Cyber-Sicherheitssystemen ist es eine wichtige Frage, ob die Cyber-Sicherheitssysteme auch tatsächlich geeignet sind, den realen Angriffen wirkungsvoll entgegenzuwirken.

Im Folgenden wird dargestellt, wie die Wirksamkeit von Cyber-Sicherheitssystemen generell beurteilt werden kann [10].

In Abb. 1.10 werden die Werte einer Organisation, die vor einem Angriff geschützt werden sollen, durch einen roten Punkt (€ Werte) dargestellt. Die Angriffe, denen ein IT-System ausgesetzt ist, werden durch Nägel repräsentiert, deren Länge proportional zur Größe der Fachkenntnisse, der Gelegenheiten und Ressourcen ist, über die der Angreifer verfügt.



**Abb. 1.10** Wirksamkeit von Cyber-Sicherheitssystemen

Die Cyber-Sicherheitsmechanismen, die eingesetzt werden, sind durch eine gelbe Wand dargestellt. Die Stärke dieser Wand ist proportional zur Stärke des Cyber-Sicherheitsmechanismus. Je länger also der Nagel ist, desto schwerwiegender ist der Angriff. Je stärker die Wand, desto größer die Fähigkeit der Cyber-Sicherheitsmechanismen, diesen Angriff auf die Werte einer Organisation abzuwehren.

Cyber-Sicherheitsmechanismen sind dann sicher, wenn die Werte vollständig von einer gelben Wand umgeben sind, deren Stärke an ihrer schwächsten Stelle mindestens gleich groß oder größer als die Länge des größten Nagels ist.

### Indirekte Angriffe

Es kann aber auch der Fall auftreten, dass die gewählten Cyber-Sicherheitsdienste zur Abwehr des Angriffes nicht ausreichen, obwohl ihre Cyber-Sicherheitsmechanismen eigentlich stark genug sind, weil ein indirekter Angriff durchgeführt wird, siehe Abb. 1.11.

**Abb. 1.11** Indirekte Angriffe



**Tab. 1.1** Unterscheidung der Stärke eines Cyber-Sicherheitsmechanismus

Stärke eines Cyber-Sicherheitsmechanismus	Beschreibung
Niedrig	Es muss erkennbar sein, dass der Cyber-Sicherheitsmechanismus Schutz gegen zufällige Überwindung bietet, während er durch sachkundige Angreifer überwunden werden kann
Mittel	Es muss erkennbar sein, dass der Cyber-Sicherheitsmechanismus Schutz gegen Angreifer mit beschränkten Gelegenheiten oder Ressourcen bietet
Hoch	Es muss erkennbar sein, dass der Cyber-Sicherheitsmechanismus nur von Angreifern überwunden werden kann, die über sehr gute Fachkenntnisse, Gelegenheiten und Ressourcen verfügen, wobei ein solcher erfolgreicher Angriff als normalerweise nicht durchführbar beurteilt wird

Beispiele für indirekte Angriffe sind:

- Ein Angreifer greift nicht das sichere Verschlüsselungsverfahren an, sondern den schwachen Schlüssel, der zum Beispiel eines der meist verwendeten Passwörter darstellt, „12345678“.
- Ein Angreifer versucht nicht eine Firewall zu überwinden, sondern nutzt die Kommunikation eines Mitarbeiters, der von seinem Notebook über das Mobilfunknetz im Internet aktiv ist.

### Stärke eines Cyber-Sicherheitsmechanismus

Grundsätzlich kann die Stärke der Cyber-Sicherheitsmechanismen von Cyber-Sicherheitssystemen unterschiedlich bewertet werden. Hierbei wird die Bewertung niedrig, mittel und hoch verwendet, siehe Tab. 1.1.

Eine wichtige Größe für die Bewertung von Cyber-Sicherheitsmechanismen ist die Mindeststärke des Cyber-Sicherheitsmechanismus, die notwendig ist, um allen Angriffen erfolgreich entgegenzuwirken.

### Zur Erklärung der Begriffe Fachkenntnisse, Gelegenheiten und Ressourcen

Fachkenntnisse betreffen das Wissen, über das Personen verfügen müssen, um ein Cyber-Sicherheitssystem angreifen zu können. Ein Laie ist definiert als eine Person ohne besondere Fachkenntnisse, zum Beispiel ein normaler Internetanwender. Eine kenntnisreiche Person hingegen ist mit den internen Arbeitsweisen des Cyber-Sicherheitssystems vertraut. Ein Experte kennt die grundlegenden Prinzipien und Algorithmen des Cyber-Sicherheitssystems (zum Beispiel ein guter Informatiker, Hacker, Sicherheitsexperten, ...).

Ressourcen sind Mittel, die ein Angreifer für den erfolgreichen Angriff auf das Cyber-Sicherheitssystem einsetzen muss. Unterschieden werden zwei Arten von Ressourcen: Zeit und Ausstattung. Zeit ist die Zeit, die ein Angreifer für

die Durchführung eines Angriffs benötigt; nicht mitgerechnet wird hierbei die vorab für die Planung des Angriffs notwendige Zeit. Zur Ausstattung gehören IT-Systeme, elektronische Geräte, Hardware, Werkzeuge, Software etc.

Hierbei bedeutet „innerhalb von Minuten“, dass ein Angriff in weniger als 10 min erfolgreich durchgeführt werden kann. „Innerhalb von Tagen“ bedeutet, dass ein Angriff in weniger als einem Monat erfolgreich durchgeführt werden kann. „Innerhalb von Monaten“ bedeutet, dass für einen erfolgreichen Angriff mindestens ein Monat benötigt wird.

„Ohne Ausstattung“ bedeutet, dass die Durchführung eines Angriffs ohne besondere Hilfsmittel möglich ist, zum Beispiel nur mit einem Browser. „Vorhandene Ausstattung“ bedeutet Ausstattung, die ohne weiteres in der Betriebsumgebung des IT-Systems verfügbar oder Teil des eigentlichen IT-Systems ist oder käuflich erworben werden kann. „Sonderausstattung“ heißt, dass eine besondere Ausstattung zur Durchführung eines Angriffs erforderlich ist.

Gelegenheiten bezieht sich auf Faktoren, die im Allgemeinen außerhalb der Kontrolle eines Angreifers liegen würden: Hilfestellungen durch andere Person (geheime Absprachen), die Wahrscheinlichkeit eines Zusammentreffens bestimmter Umstände (Zufall), und die Wahrscheinlichkeit und die Konsequenz einer Ermittlung des Angreifers (Entdeckung). Diese Faktoren sind generell nur sehr schwer zu bewerten.

### Überwindung des Cyber-Sicherheitsmechanismus (unzureichende Wirkung)

Abb. 1.12 zeigt eine erfolgreiche Überwindung der Cyber-Sicherheitsmechanismen. Die Stärke der grauen Wand entspricht nicht der erforderlichen Mindeststärke des Cyber-Sicherheitsmechanismus.

Sie kann daher vom Angreifer mit den richtigen Fachkenntnissen, den passenden Gelegenheiten und geeigneten Ressourcen überwunden werden.

**Abb. 1.12** Angreifer überwindet den Cyber-Sicherheitsmechanismus



**Abb. 1.13** Erfolgreiche Abwehr



### Erfolgreiche Abwehr mit der Wirkung eines Cyber-Sicherheitsmechanismus (ausreichende Wirkung)

Die Stärke der gelben Wand entspricht der erforderlichen Mindeststärke des Cyber-Sicherheitsmechanismus.

In Abb. 1.13 kann der Angreifer, obwohl er die richtigen Fachkenntnisse hat, eine passende Gelegenheit nutzt und geeignete Ressourcen einsetzt, den Cyber-Sicherheitsmechanismus nicht überwinden, weil eine ausreichende Wirkung entgegengesetzt wird.

Die eingeführten Symbole werden in den weiteren Kapiteln genutzt, um eine Aussage über die Wirksamkeit der verschiedenen Cyber-Sicherheitsmechanismen tätigen zu können.

**Wichtig** Es ist besonders wichtig und notwendig, dass Cyber-Sicherheitslösungen eingesetzt werden, die eine ausreichende Wirkung gegen reale Angriffe haben.

## 1.7 Cyber-Sicherheitsstrategien

Im Folgenden werden drei prinzipielle Cyber-Sicherheitsstrategien beschrieben, die helfen können, Cyber-Sicherheitsmechanismen in strategische Wirkungen einzuteilen. So kann die Wirkung auf Angriffe besser verstanden und geeignete Cyber-Sicherheitsstrategien können umgesetzt werden.

### 1.7.1 Vermeiden von Angriffen

Ein genereller Aspekt der Vermeidungsstrategie ist das Prinzip der digitalen Sparsamkeit, das heißt, so wenige Daten generieren wie möglich und so viele wie nötig. Daten, die nicht auf IT-Systemen vorhanden sind, können auch nicht angegriffen

**Abb. 1.14** Cyber-Sicherheitsstrategie „Vermeiden von Angriffen“

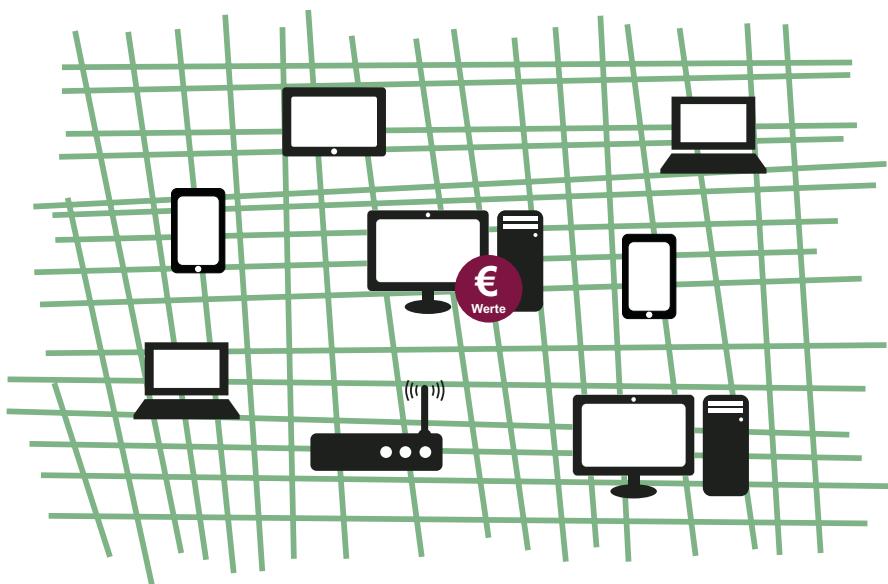


werden. Durch diese Vorgehensweise wird eine Reduzierung der Angriffsfläche erreicht, siehe Abb. 1.14.

Ein weiteres Prinzip des Vermeidens von Angriffen ist: „Keine Technologien, Produkte und Dienste mit bekannten Schwachstellen verwenden“. Auch dieses Prinzip hilft, Angriffe zu vermeiden. Beispiele von Technologien, bei denen dieses Prinzip umgesetzt werden kann, sind zum Beispiel Browser, Betriebssysteme und Internet-Dienste. Die Realisierung einer Zwei-Hersteller-Strategie bei Browsern hat beispielsweise den Vorteil, dass wenn ein Browser bekannte Schwachstellen hat, der zweite Browser, ohne bekannte Schwachstelle, weiter verwendet werden kann.

### Fokussierung

Aus Studien ist bekannt, dass im Schnitt ca. 5 % aller vorhandenen Daten in Unternehmen besonders schützenswert sind. Welche Daten in einem Unternehmen die 5 % der besonders schützenswerten Daten sind, wissen die Verantwortlichen in der Regel nicht genau. Aus diesem Grund sollte eine Schutzbedarfsanalyse der vorhandenen IT-Systeme gemacht werden, um zu identifizieren, auf welchen IT-Systemen diese vorhanden sind. Damit wären die Verantwortlichen in der Lage, sich auf möglichst wenige IT-Systeme zu konzentrieren und zum anderen, diese wenigen IT-Systeme besonders zu schützen. Durch diese Fokussierung können die besonders schützenswerten Daten einer Organisation einfacher geschützt werden. In Abb. 1.15. ist angedeutet, dass nur im IT-System in der Mitte besonders sicherheitsrelevante Werte des Unternehmens gespeichert sind, die dann auch besonders geschützt werden müssen.



**Abb. 1.15** Idee der Fokussierung

### Bewertung der Vermeidung

Das Vermeiden von Angriffen ist die beste Cyber-Sicherheitsstrategie, um Schäden zu reduzieren. Leider ist die Vermeidungsstrategie aber praktisch nur begrenzt umsetzbar, da zum Beispiel IT-Systeme in der Regel an das Internet angeschlossen sind, um die vielfältigen Vorteile nutzen zu können.

### 1.7.2 Entgegenwirken von Angriffen

Das Entgegenwirken von Angriffen ist die meist verwendete Cyber-Sicherheitsstrategie, um Schäden zu vermeiden. Wie in Abb. 1.16 zu sehen ist, werden

**Abb. 1.16** Cyber-Sicherheitsstrategie „Entgegenwirken von Angriffen“



Cyber-Sicherheitsmechanismen verwendet, die eine hohe Wirkung gegen bekannte Angriffe zur Verfügung stellen und damit die Werte angemessen schützen. Cyber-Sicherheitsmechanismen sind Verschlüsselung (Datei-, Festplatten-, E-Mail-Verschlüsselung, VPN-Systeme, SSL/TLS, ...), Multifaktor-Authentifikationsverfahren, Firewall-Systeme, Anti-Malware-Lösungen, Anti-DDoS-Verfahren, Signaturverfahren, Security Kernel, Isolierung- und Separierungstechnologien usw.

### Bewertung des Entgegenwirkens

Die Cyber-Sicherheitsstrategien „Entgegenwirken von Angriffen“ ist eine nahe-liegende Vorgehensweise, digitale Werte angemessen zu schützen.

Leider stehen zurzeit nicht genug wirkungsvolle Cyber-Sicherheitstechnologien, -lösungen und -produkte zur Verfügung oder werden nicht angemessen eingesetzt, was die erfolgreichen professionellen Angreifer jeden Tag demonstrieren.

### 1.7.3 Erkennen von Angriffen

Wenn Angriffen mithilfe von Cyber-Sicherheitsmechanismen nicht angemessen entgegengewirkt werden kann oder eine Vermeidung nicht möglich ist, dann bleibt nur noch die Strategie, Angriffe zu erkennen und zu versuchen, den Schaden so schnell wie möglich zu minimieren, siehe Abb. 1.17.

In diesem Bereich gibt es zum Beispiel Cyber-Sicherheit Frühwarn- und Lagebildsysteme, die Warnungen erzeugen, wenn Angriffe erkannt werden. Hier ist die Idee, dass in einem definierten Bereich (Kommunikationsinfrastruktur, Endgeräte, ...) nach Angriffssignaturen oder Anomalien gesucht wird, um dann entsprechend reagieren zu können, damit Schaden verhindert oder reduziert werden kann, siehe auch Kap. 8.

**Abb. 1.17** Cyber-Sicherheitsstrategie „Erkennen von Angriffen“



## Bewertung des Erkennens

Die Cyber-Sicherheitsstrategie „Erkennen von Angriffen“ ist sehr hilfreich, hat aber definierte Grenzen.

**Wichtig** Cyber-Sicherheitsstrategien helfen, die richtigen Cyber-Sicherheitsmechanismen mit ihren speziellen Wirkungen an der richtigen Stelle einzusetzen.

---

## 1.8 Angreifer und deren Motivationen

Bei der Beurteilung der Angriffspotenziale macht es Sinn, auch die Motivation von Angreifern mit zu berücksichtigen.

Ein Angreifer versucht gezielt und absichtlich, auf ein IT-System zuzugreifen, um an bestimmte Informationen zu gelangen, die nicht für ihn bestimmt sind, Aktionen auszulösen, die er nicht auslösen darf, oder Ressourcen zu nutzen, die er nicht nutzen darf.

Welche Motivation hat ein Angreifer typischerweise?

### Neugierde

Der Angreifer greift an, weil er durch einen erfolgreichen Angriff seine Neugierde befriedigen kann.

### Zerstörungswut

Der Angreifer greift an, weil er die IT und die Informationen zerstören will, zum Beispiel weil der Angreifer ein ehemaliger Mitarbeiter ist und aus seiner Sicht unberechtigt entlassen worden ist.

### Geld

Der Angreifer (IT-Spione, Berufskriminelle, Unternehmens-Cracker, ...) greift an, weil er damit Geld verdienen kann.

### Anerkennung

Der Angreifer, typischerweise ein „weißer“ Hacker, greift an, weil er durch einen erfolgreichen Angriff Anerkennung für diese Leistung haben möchte. Ein „weißer“ Hacker verwendet sein Wissen innerhalb der Gesetze.

### Herausforderung

Der Angreifer greift an, weil der Angriff für ihn eine Herausforderung darstellt und der Erfolg eine Befriedigung ist.

### Spaß an der Technik

Der Angreifer greift an, weil er Spaß an der Technik hat und ein erfolgreicher Angriff dies befriedigt.

## **Strafverfolgung**

Der Angreifer greift an, weil dadurch Strafverfolgung gesetzlich geregt umgesetzt werden kann.

Neben der Frage der Motivation, ist es auch von Bedeutung zu wissen, wer IT-Systeme angreift. Im Folgenden werden einige Kategorien beschrieben.

### **Hacker**

Hacker brechen in IT-Systeme und Netzwerke ein, weil sie darin eine Herausforderung sehen und mit dem Erfolg ihren Status vergrößern wollen. Oft handelt es sich um Jugendliche, die aus Spieltrieb, also ohne böse Absicht, handeln. Sie sind aber unberechenbar und können hohen Schaden verursachen.

### **IT-Spione**

Bezahlte Spezialisten – teilweise mit einem sehr hohen Budget – versuchen, über gezielte Angriffe an Informationen zu kommen. Ihre Ziele sind politisch oder auch wirtschaftlich begründet.

### **IT-Terroristen**

Terroristen können IT-Systeme und Netzwerke angreifen, um aus politischen Gründen Angst und Chaos zu verursachen. Sie wollen oft auf Missstände und/oder politische Ziele aufmerksam machen.

### **Unternehmens-Cracker**

Dies sind Mitarbeiter, die auf IT-Systeme und Netzwerke von Konkurrenzunternehmen zugreifen, um ihrem Unternehmen finanzielle Vorteile zu verschaffen. Dazu spähen sie beispielsweise Entwicklungsunterlagen, Strategiepläne, Vertriebsinformationen, Kundendaten usw. aus.

### **Professionelle Kriminelle/Berufskriminelle**

Diese Personen wollen sich mit Angriffen persönlich bereichern, beispielsweise durch die nicht bezahlte Nutzung von Dienstleistungen, durch die unberechtigten Abbuchungen von fremden Konten, Erpressungen usw.

### **Vandalen**

Das sind Personen, die Angriffe durchführen, um Organisationen oder Personen gezielt Schaden zuzufügen. Oft ist die Motivation reine Zerstörungswut.

### **Behörden**

Mitarbeiter der Strafverfolgungsbehörden greifen IT-System und Netzwerke an, um Strafverfolgung zu betreiben.

**Wichtig** Die Motivation der Angreifer zu kennen ist hilfreich, um geeignete Gegenmaßnahmen zu ergreifen.

## 1.9 Cyber-Sicherheitsbedürfnisse

In diesem Abschnitt werden die Cyber-Sicherheitsbedürfnisse als Grundwerte der Cyber-Sicherheit beschrieben, die mithilfe von Cyber-Sicherheitsmechanismen befriedigt werden können. Cyber-Sicherheitsbedürfnisse werden auch als Cyber-Sicherheitsziel bezeichnet.

### Gewährleistung der Vertraulichkeit

Dies ist wichtig, damit keine unautorisierten Personen oder Organisationen in der Lage sind, übertragene oder gespeicherte Informationen zu lesen.

### Gewährleistung der Authentifikation

Mithilfe des Cyber-Sicherheitsmechanismus Authentifikation wird verifiziert, wer der Partner bei der Kommunikation oder Transaktion ist beziehungsweise welcher Nutzer auf Betriebsmittel und Informationen zugreift.

### Gewährleistung der Authentizität

Mithilfe des Cyber-Sicherheitsmechanismus Authentizität wird verifiziert, dass Informationen oder Identitäten echt sind.

### Gewährleistung der Integrität

Beim Cyber-Sicherheitsbedürfnis „Gewährleistung der Integrität“ wird überprüft, ob Informationen, die übertragen werden oder gespeichert sind, unverändert, das heißt original sind.

### Gewährleistung der Verbindlichkeit

Das Cyber-Sicherheitsbedürfnis „Gewährleistung der Verbindlichkeit“ sorgt für die Gewissheit, dass die Prozesse und die damit verbundenen Aktionen auch verbindlich sind.

### Gewährleistung der Verfügbarkeit

Dieses Cyber-Sicherheitsbedürfnis sorgt für die Gewissheit, dass die Informationen und Dienste auch zur Verfügung stehen.

### Gewährleistung der Anonymisierung/Pseudonymisierung

Mit diesem Cyber-Sicherheitsbedürfnis wird gewährleistet, dass eine Person nicht oder nicht unmittelbar identifiziert werden kann.

**Wichtig** Cyber-Sicherheitsbedürfnisse beschreiben, mit welchen prinzipiellen Cyber-Sicherheitsmechanismen welche Grundwerte der Cyber-Sicherheit befriedigt werden können.

## 1.10 Das Pareto-Prinzip der Cyber-Sicherheit

Die Motivation, digitale Werte anzugreifen, steigt mit der immer größer werdenen Digitalisierung und der damit steigende Angriffsfläche.

Die Frage, die dabei eine besondere Rolle spielt, ist, welche Strategie zur Anwendung kommen kann, um sich angemessen schützen zu können oder wann der Aufwand für Cyber-Sicherheitsmaßnahmen größer ist als die Reduzierung von Schäden.

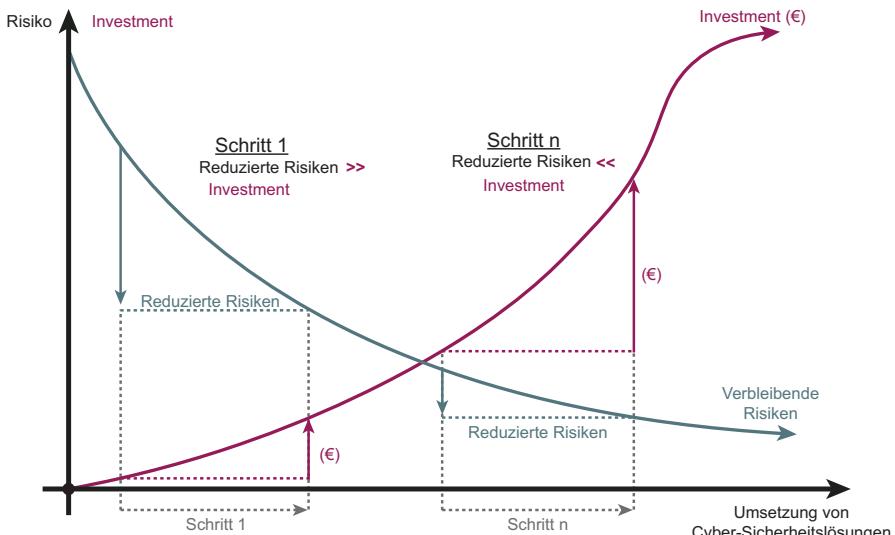
In Abb. 1.18 wird auf der Y-Achse das Risiko eines Schadens in Grün und die Investition in Cyber-Sicherheitsmaßnahmen in Rot dargestellt. Auf der X-Achse werden die schon umgesetzten Cyber-Sicherheitsmaßnahmen aufgeführt.

Wie in der Grafik zu sehen ist, wird in einem ersten Schritt durch die Implementierung richtiger Cyber-Sicherheitsmaßnahmen mit einer kleinen Investment-Summe eine hohe Reduzierung der Risiken erzielt. Dieser Effekt wird auch Pareto-Prinzip oder 80:20-Regel genannt. 20 % der richtigen Cyber-Sicherheitsmechanismen richtig eingesetzt liefern 80 % der Reduzierung der Risiken.

Das bedeutet, dass mit dem Einsatz der richtigen Cyber-Sicherheitsmaßnahmen mit einem relativ geringen Investitionsaufwand ein angemessener Schutz für IT-Systeme hergestellt werden kann.

In der Grafik ist auch zu sehen, wie in einem Schritt „n“ durch die Umsetzung weiterer Cyber-Sicherheitsmaßnahmen mit einer hohen Investitionssumme nur noch eine kleine Reduzierung der Risiken erzielt werden kann. Hier ist es wichtig, abschätzen zu können, ob die Investitionssumme größer ist als ein potenzieller Schaden.

Egal wie viel Geld investiert wird, verbleibende Restrisiken müssen immer mit einkalkuliert werden, die dann zum Beispiel mithilfe von Versicherungen gedeckt werden können.



**Abb. 1.18** Pareto-Prinzip

## 1.11 Cyber-Sicherheitsrisiko

Unternehmen schließen Versicherungen als Cyber-Risikoabsicherung ab, um einen Schaden durch potenziell eintretende Sach- und Personenschäden sowie Vermögensschäden zu minimieren. Das ist eine Methode, die große Anwendung in der Wirtschaft findet. Durch die immer größer werdende Verlagerung von Dienstleistungen und Unternehmensprozessen in die digitale Welt sowie die zunehmende Abhängigkeit von Unternehmen gegenüber funktionierenden Systemen IT-gestützter Datenverarbeitung und webbasierter Geschäftsprozesse entstehen stetig neue und komplexere Schadensrisiken durch Cyber-Kriminalität und IT-Ausfälle. Die Digitalisierung schreitet immer weiter voran. Durch aufkommende Technologie-Konzepte, wie das Internet of Things, Cloud-Computing oder Industrie 4.0 werden immer mehr Unternehmensprozesse und Daten in die Cloud beziehungsweise ins Internet verlagert, was gleichzeitig das Risiko von Cyber-Angriffen auf Systeme und gespeicherte Daten erhöht. Etwa 69 % der Industrieunternehmen in Deutschland waren in den vergangenen zwei Jahren Opfer von Cyber-Angriffen. Die immer größer werdenden Datenmengen stellen ebenfalls ein Schadensrisiko für Unternehmen dar. Der Diebstahl von Produkt- und Entwicklungsinformationen kann gravierende Auswirkungen für Unternehmen haben. Insbesondere personenbezogene Daten wie Kundendaten oder Informationen von Zulieferern stellen ein besonders Risiko dar, da diese dem Datenschutz unterliegen. Werden zu schützende Daten Dritter veröffentlicht oder missbraucht, drohen Schadensansprüche der Dateninhaber. Unternehmen sollten daher, so die Position der Versicherungswirtschaft, regelmäßig ihre eigene Risikolandschaft auf Cyber-Risiken analysieren und ihren Versicherungsschutz gegebenenfalls bedarfsgerecht anpassen, um Deckungslücken zu identifizieren und anpassen zu können.

### Grundstruktur einer Cyber-Versicherung

Cyber-Versicherungen sind fakultative Zusatzversicherungen, die die bereits vorhandenen Industrieverversicherungen um weitere Deckungen in Belangen der Sicherheit von Informationssystemen erweitern sollen. Die Anatomie von Versicherungspaketen und deren Deckungselementen können sich im Laufe der Zeit durch die dynamischen Cyber-Risiken zum Teil stark verändern. Jedoch hat sich inzwischen eine grundlegende Struktur einer Cyber-Versicherung etabliert. Sie wird in zwei grundlegende Bereiche unterteilt. So wird unterschieden zwischen einer Eigenschadenversicherung und einer Drittschadenversicherung (Haftpflicht). Die Eigenschadenversicherung deckt Schäden an Vermögenswerten der Versicherungsnehmer ab, während die Drittschadensversicherung oder Haftpflicht Schäden an Vermögenswerten Dritten abdeckt. Letzterer Fall würde eintreten, wenn ein Cyber-Sicherheitsvorfall beim Versicherten einen Schaden bei einem Dritten verursacht und der Dritte infolgedessen Schadensersatz verlangt. Das können Kunden, Zulieferer oder Geschäftspartner sein. Zusätzlich werden noch weitere Dienstleistungen aus einem umfassenden Dienstleistungsnetzwerk angeboten.

**Zusätzliche Kostenpositionen im Schadensfall**

- Ursachenerkennung durch IT-Forensik-Unternehmen
- Krisenmanagement mithilfe von Kommunikationsberatern und PR-Fachleuten
- Rechtsberatung durch Rechtsanwälte

**Eigenschaden**

- Umsatzverluste bei Betriebsunterbrechungen
- Mehrkosten zur Aufrechterhaltung des Betriebes
- Reputationsschäden
- Wiederherstellungskosten bei Verlust oder Beschädigung der Integrität von Daten
- Kosten bei Erpressungen

**Drittshäden**

- Verletzung von Datenschutz- oder Vertraulichkeitspflichten
- Schadenersatzansprüche von Kunden
- Bußgelder wegen Vertragsstrafen
- Verstöße gegen Gesetze und Regularien

Viele Versicherungsunternehmen bieten einen individuell gestaltbaren Versicherungsumfang an. So können oft vordefinierte Versicherungspakete für verschiedene Unternehmensgrößen um optionale Deckungselemente beziehungsweise Leistungsbausteine reduziert oder erweitert werden. Die Ausmaße des kompletten Versicherungsumfangs hängen oft folglich von den Anforderungen des Versicherungsnehmers ab. Wichtige Faktoren bei der Auswahl einer Cyber-Versicherung sind:

- die Unternehmensgröße
- die Branchenzugehörigkeit
- die Frage nach der Verarbeitung sensibler oder personenbezogener Daten
- und die wirtschaftlichen Tätigkeitsfelder des Unternehmens

**Zusätzliche Kostenpositionen im Schadensfall**

Bei der Bewältigung von Vorfällen kann es unter Umständen dazu kommen, dass zusätzlich qualifizierte externe Dienstleister zur Krisenbewältigung hinzugezogen werden müssen. Dadurch kann ein zusätzliches finanzielles Risiko für ein Unternehmen entstehen. So könnten zertifizierte IT-Forensiker zur Vorfallaufklärung und Wiederherstellung des Betriebs erforderlich werden. Des Weiteren werden für das Krisenmanagement und die Unternehmenskommunikation Kommunikationsberater und PR-Fachleute benötigt. Zusätzlich können Kosten für eine Rechtsberatung durch spezialisierte Anwälte entstehen. Eine Cyber-Versicherung kann die Kosten für Sachverständige abdecken und damit das finanzielle Risiko beherrschbar machen und somit erheblich zur Krisenbewältigung beitragen.

## IT-Forensik

Die anwachsende Vernetzung und Digitalisierung hat aus der ursprünglichen Spezialwissenschaft für Ermittlungsbehörden einen neuen professionellen Dienstleistungssektor gemacht. Die IT-Forensik umfasst kriminaltechnische Analysen und Vorgehensweisen zur Aufklärung von Vorfällen im Zusammenhang mit Cyber-Risiken und IT-Ausfällen von informationstechnischen Systemen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt die IT-Forensik in seinem Leitfaden als „die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung insbesondere aus der Sicht des Anlagenbetreibers eines IT-Systems“. Folglich beinhaltet das Aufgabenfeld der IT-Forensik die forensische Untersuchung und Aufklärung von Auswirkungen durch Cyber-Angriffe, als auch Betriebsstörungen oder Ausfälle der Unternehmens-IT-Systeme und Infrastruktur durch interne Quellen.

Eine der ersten Aufgaben der IT-Forensik besteht darin zu erkennen, ob überhaupt ein Vorfall vorliegt. Ist ein Vorfall aufgetreten, so muss dieser identifiziert werden. Eine zeitnahe Bestätigung und Identifizierung eines Vorfalls ist eine Voraussetzung für die Einleitung von Maßnahmen. Die Maßnahmen sollen zur Begrenzung von möglichen Schäden und zur Eindämmung der Auswirkungen des Vorfalls führen. Eine kurze Reaktionszeit kann sich positiv auf die Reduzierung von Schäden auswirken. Es müssen bei der Aufklärung des Schadenshergangs die Bereiche des Unternehmens identifiziert werden, die betroffen sind. Ferner muss überprüft werden, ob Dritte in der Reichweite der Auswirkungen des Vorfalls waren. Nur mit einer präzisen Analyse lassen sich die Gesamtauswirkungen eines Vorfalls für das Unternehmen und Dritte so gut wie möglich abschätzen. So kann auch der entstandene Schaden erst bemessen werden.

Zusammengefasst kann der Ablauf in folgenden Punkten festgehalten werden:

- klären, ob ein Vorfall vorliegt
- Vorfall lokalisieren und durch Maßnahmen eindämmen
- Bereiche und Elemente identifizieren, die betroffen sind
- Auswirkungen des Vorfalls einschätzen
- einen möglichen entstandenen Schaden benennen und quantifizieren

Die Bearbeitung eines Cyber-Vorfalls ist nur ein Teilbereich der IT-Forensik. Das Ziel ist, neben der Aufklärung des Schadenshergangs, die Wiederherstellung der IT-Systeme und IT-Infrastruktur. Folglich sollen Maßnahmen für das betroffene Unternehmen getroffen werden, um einen Notbetrieb einleiten zu können und Folgeschäden zu verhindern oder zu begrenzen. Das betroffene Unternehmen soll in einen Zustand versetzt werden, in dem es dringende Aufgaben mit hoher Priorität weiter bearbeiten kann und Zeit für die Wiederherstellung des Normalbetriebs bereitstellt. Sofern das möglich ist, sollen auch Informationen zur Herkunft des Angriffs gesammelt und ausgewertet werden. Zusätzlich ist es für ein

Unternehmen oder eine Organisation entscheidend zu wissen, welche Daten bei einem Angriff verändert, gestohlen oder gelöscht wurden.

**Wichtig** Mit Cyber-Versicherungen können Restrisiken, die nicht direkt durch Cyber-Sicherheitslösungen abgedeckt werden können, abgesichert werden.

### Voraussetzungen

Der Versicherungsschutz deckt das Restrisiko ab. Im Vordergrund steht jedoch ein angemessener Grundschutz als Folge unterschiedlicher Cyber-Sicherheitsmaßnahmen, für die das Unternehmen selbst sorgen muss. Dazu gehören etwa tägliche Datensicherungen, zeitnahe Aufspielen von sicherheitsrelevanten Software-Updates, starke Passwörter oder Multifaktor-Authentifikation (MFA), Schutz vor unbefugtem Zugriff auf personenbezogene und andere sensible Daten sowie Berechtigungsmanagement und Verschlüsselungen. Welcher IT-Schutz angemessen ist, das variiert von Unternehmen zu Unternehmen, typischerweise sind die Anforderungen an Konzerne höher als an Klein- und mittelständische Betriebe.

---

## 1.12 Zusammenfassung

Cyber-Sicherheit ist eine Aufgabenstellung, die mit der immer größer werdenden Nutzung von IT und dem Internet sowie der weiteren Digitalisierung bedeutsamer wird. Die konkreten Cyber-Sicherheitsprobleme und Herausforderungen sind gewaltig und die Sichtweisen auf die Cyber-Sicherheit vielfältig. Die Kenntnisse der Wirkung von Cyber-Sicherheitssystemen, Cyber-Sicherheitsstrategien, Cyber-Sicherheitsbedürfnissen, das Pareto-Prinzip, Cyber-Versicherungen sowie die Motivation von Angreifern helfen, geeignete Cyber-Sicherheitsmaßnahmen umzusetzen.

Das Erlangen einer angemessenen Cyber-Sicherheit ist eine sehr anspruchsvolle und komplexe Aufgabe.

In den weiteren Kapiteln werden ein Vielzahl von Cyber-Sicherheitskonzepten, -Sicherheitsmechanismen, -Prinzipien usw. beschrieben, die alle helfen können, einen höheren Level einer Cyber-Sicherheit zu erlangen und damit Risiken zu minimieren.

---

## 1.13 Übungsaufgaben

### Übungsaufgabe 1 (Softwarequalität)

Sie sind Leiterin eines großen Projekts, das Software für selbstfahrende Autos entwickelt. Einer Ihrer Entwickler stellt Ihnen das fertige Entertainment-Programm des Autos vor. Sie fragen ihn, wie die Qualität der Software sichergestellt

wurde. Er antwortet, dass er unterschiedliche Szenarien an Teilen des Entertainment-Systems getestet hat und bei dieser Untermenge alle Tests einwandfrei funktioniert haben. Sind die Tests ausreichend? Begründen Sie die Antwort!

### Übungsaufgabe 2 (Stärke eines Cyber-Sicherheitsmechanismus)

Betrachten Sie die folgenden Fälle und ordnen Sie die Stärken der Cyber-Sicherheitsmechanismen ein!

#### *Fall 1:*

Sie betreiben einen Blog, der politische Ereignisse kommentiert. Sie bieten ebenfalls einen Newsletter an, über den Sie Ihren Lesern wichtige Informationen mitteilen. Sie merken aber, dass bei der Anmeldung, anscheinend automatisch, tausende falsche Angaben gemacht werden, indem keine korrekten E-Mail-Adressen eingegeben werden. Daher implementieren Sie eine Prüfung, die erkennt, ob die eingegebene E-Mail-Adresse das korrekte Format hat. Sie speichern eine E-Mail-Adresse nur dann, wenn diese das korrekte Format hat.

Wie beurteilen Sie die Stärke dieses Sicherheitsmechanismus und warum?

niedrig  mittel  hoch

#### *Fall 2:*

Nachdem sich ein Nutzer auf Ihrer Webseite authentifiziert hat, ordnen Sie dem Nutzer eine Nummer zu, die den Nutzer für die Dauer der Sitzung identifiziert („Session ID“) und angibt, dass er sich bereits erfolgreich authentifiziert hat. Diese Session IDs laufen bei Inaktivität nach 15 min ab. Bisher wurde diese Nummer einfach hochgezählt, was Angreifern erlaubt hat, diese Nummern einfach zu erraten. Nun stellen Sie auf ein System um, das diese Zahlen mit einer Länge von 256 Bit vollkommen zufällig, aber immer noch eindeutig pro Nutzer generiert.

Wie beurteilen Sie die Stärke dieses Cyber-Sicherheitsmechanismus und warum?

niedrig  mittel  hoch

#### *Fall 3:*

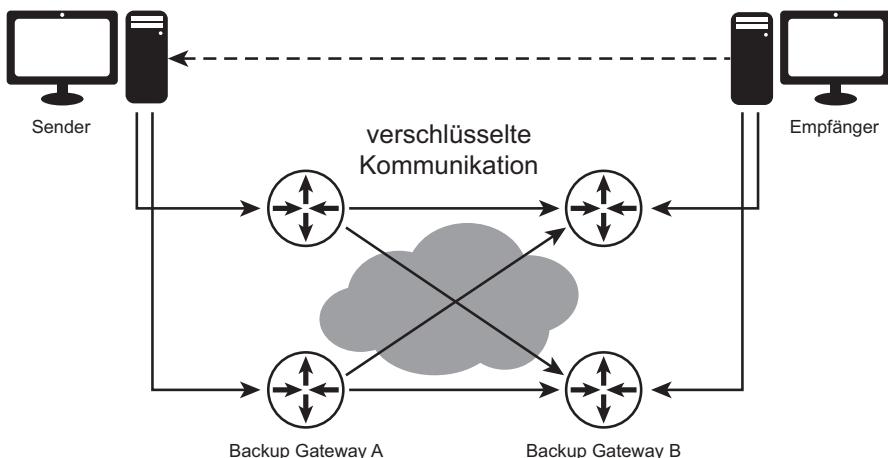
Für Ihr privates Heimnetzwerk nutzen Sie ein 8-stelliges WLAN-Passwort. Sie wissen, dass ein motivierter Angreifer ungefähr 2 Monate braucht, um das Passwort zu knacken.

Wie beurteilen Sie die Stärke dieses Sicherheitsmechanismus und warum?

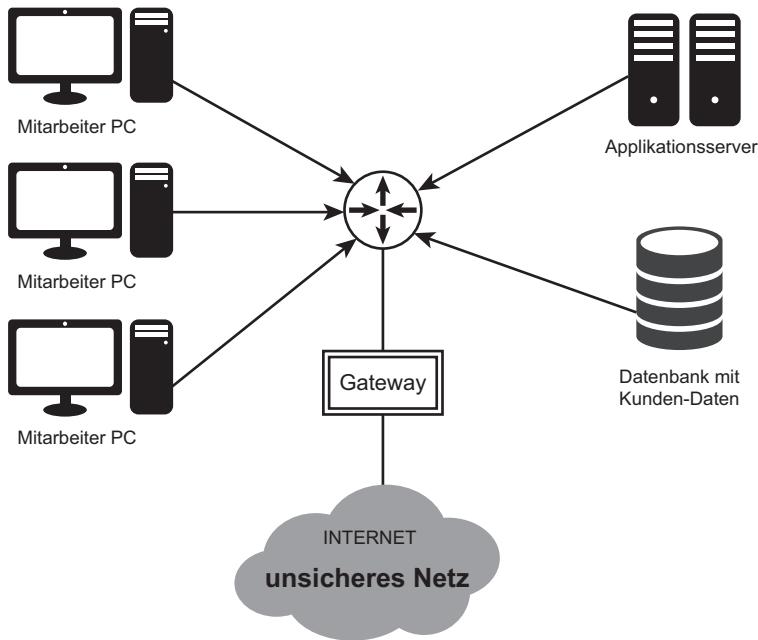
niedrig  mittel  hoch

**Übungsaufgabe 3 (Cyber-Sicherheitsbedürfnisse)**

Gegeben ist das Kommunikationsnetzwerk in der folgenden Abbildung. Vor dem Senden der Daten wird sichergestellt, dass die Daten auch wirklich vom bekannten Kommunikationspartner stammen und nicht verändert oder mitgelesen werden können. Geben Sie an, wo und wie die unterschiedlichen „Cyber-Sicherheitsbedürfnisse“ in dem Kommunikationsnetzwerk umgesetzt werden.

**Übungsaufgabe 4 (Angriffsflächen)**

Gegeben ist der Ausschnitt des Netzwerkplans eines Start-ups im Bereich des Onlinehandels in der folgenden Abbildung. Das junge Unternehmen vertreibt Produkte über einen eigens entwickelten Onlineshop mit zahlreichen innovativen Funktionen, die sie erfolgreich von anderen Marktteilnehmern abgrenzen. Das Frontend des Onlineshops wird überwiegend in einem „Content Delivery Network“ gehostet. Die Geschäftslogik und die Weiterentwicklung der Shop-Software werden auf einem internen Applikationsserver durchgeführt. Identifizieren Sie die IT-Systeme, die aus Sicht des Start-ups besonders schützenswert sind! Wo sollte angesetzt werden, wenn Angriffe frühzeitig erkannt werden sollen? Begründen Sie Ihre Wahl!

**Übungsaufgabe 5** (Cyber-Sicherheitsprobleme)

Welches Cyber-Risiko verursacht eine ungenügende Software-Qualität im Bereich der Cyber-Sicherheit?

**Übungsaufgabe 6** (Cyber-Sicherheitsprobleme)

Warum wird die Erkennungsrate von Anti-Malware-Lösungen tendenziell schlechter?

**Übungsaufgabe 7** (Pareto-Prinzip)

Warum ist die Umsetzung von Cyber-Sicherheitslösungen zusätzlich zur Basis-Sicherheit im Sinne der Reduzierung des Risikos finanziell ineffektiver?

**Übungsaufgabe 8** (Angreifer und deren Motivation)

Welche Typen von Angreifern agieren ohne materielle Gewinnabsichten?

**Übungsaufgabe 9** (Angreifer und deren Motivation)

Welche Motivation von Angreifern ist gesetzlich geregelt?

**Übungsaufgabe 10** (Cyber-Sicherheitsstrategien)

Welche Cyber-Sicherheitsstrategien würden Sie bei den folgenden Gegebenheiten verfolgen?

**Fall 1:**

Sie haben eine verteilte Datenbank, in der zum Beispiel alle Kundendaten auf jedem IT-System der Mitarbeiter gespeichert sind, obwohl diese Informationen nur 1 % der Mitarbeiter des Unternehmens benötigen. Welche Cyber-Sicherheitsstrategie wählen Sie und begründen Sie Ihre Entscheidung.

Vermeiden  Entgegenwirken  Erkennen

**Fall 2:**

Sie haben wichtige Informationen im Unternehmen, die einen sehr hohen Bedarf an Vertraulichkeit haben und auf die regelmäßig zugegriffen werden muss, um die Aufgabenstellung zu erfüllen.

Welche Cyber-Sicherheitsstrategie wählen Sie und begründen Sie Ihre Entscheidung!

Vermeiden  Entgegenwirken  Erkennen

**Fall 3:**

Sie erkennen, dass Sie erfolgreich angegriffen worden sind, können aber die Vorgehensweise des erfolgreichen Angriffes nicht identifizieren. Welche Cyber-Sicherheitsstrategie wählen Sie und begründen Sie Ihre Entscheidung!

Vermeiden  Entgegenwirken  Erkennen

**Übungsaufgabe 11** (Cyber-Sicherheitsbedürfnisse)

Welches Cyber-Sicherheitsbedürfnis kann durch die „Gewährleistung der Vertraulichkeit“ befriedigt werden?

**Übungsaufgabe 12** (Cyber-Sicherheitsbedürfnisse)

Welches Cyber-Sicherheitsbedürfnis kann durch die „Gewährleistung der Authentifikation“ befriedigt werden?

**Übungsaufgabe 13** (Cyber-Sicherheitsbedürfnisse)

Welches Cyber-Sicherheitsbedürfnis kann durch die „Gewährleistung der Verfügbarkeit“ befriedigt werden?

Ergebnisse siehe: <https://norbert-pohlmann.com/cyber-sicherheit/uebungen/>

---

## Literatur

1. Pohlmann N (2014) IT-Sicherheitsherausforderungen im 21. Jahrhundert. Die Polizei – Fachzeitschrift für die öffentliche Sicherheit mit Beiträgen aus der Deutschen Hochschule der Polizei 9:255–260
2. Pohlmann N (2011) Bugs, die Nahrung für Malware – Von guter, schlechter und böser Software. IT-Sicherheit Manage Prax 4:32–34

3. Pohlmann N (2013) Daten gegen Diebstahl sichern. *Wirtschaftsspiegel*, 2:12–21
4. Petersen D, Pohlmann N (2014) Wiederaufbau – Verschlüsselung als Mittel gegen die Überwachung. *iX Mag Prof Informationstech* 5:82–86
5. Pohlmann N, Spogahn N (2011) Bauchladen – Wie man Googles Dienste umsichtig nutzt. *iX Mag Prof Informationstech* 7:98–101
6. Heidisch M, Pohlmann N (2013) Aktive informationelle Selbstbestimmung in der Online-Welt – Privacy Service macht das Internet vertrauenswürdiger. *IT-Sicherheit – Manage Prax* 1:64–67
7. Linnemann M, Pohlmann N (2010) Sicher im Internet: Tipps und Tricks für das digitale Leben, ISBN: 978-3-280-05381-2. orell füssli, Zürich
8. Pohlmann N, Speier A (2013) Eine Diskussion über Trusted Computing – Sicherheitsgewinn durch vertrauenswürdige IT-Systeme. *IT-Sicherh Manage Prax* 5:55–58
9. Heibel N, Linnemann M, Pohlmann N (2008) Mehr Vertrauenswürdigkeit für Anwendungen durch eine Sicherheitsplattform. In: Pohlmann N, Reimer H (Hrsg) *Trusted Computing – Ein Weg zu neuen IT-Sicherheitsarchitekturen*. Vieweg, Wiesbaden, S 73–85
10. Commission of the European Communities, Directorate-General XIII (1994) *Information Technology Security Evaluation Manual (ITSEM)*. ECSC-EEC-EAEC, Brüssel



# Kryptografie

2

Im Kapitel Kryptografie werden Kenntnisse über den Aufbau, die Prinzipien, die Architektur und die Funktionsweise von grundlegenden kryptografischen Verfahren vermittelt. Kryptografische Verfahren spielen eine besondere Rolle bei vielen wichtigen Cyber-Sicherheitssystemen zur Gewährleistung der Cyber-Sicherheitsbedürfnisse, wie zum Beispiel Vertraulichkeit, Authentifikation, Authentizität, Integrität und Verbindlichkeit.

Die Kryptografie prägt in immer stärkerem Maß das Alltagsleben [1]. Das gilt nicht bloß für das Online-Banking oder den Remote-Zugriff auf Firmennetze, die ohne die Nutzung von Techniken wie TLS/SSL und IPSec praktisch nicht mehr vorstellbar sind: Selbst dort, wo Kryptografie zunächst nicht vermutet wird, sind heutzutage kryptografische Verfahren im Einsatz, zum Beispiel bei den elektronischen Wegfahrsperren in Autos, wenn das Smartphone eingeschaltet wird oder jemand sich beim Mobilfunknetz des Providers anmeldet oder bei Blockchain, Fernsehen, dem neuen Personalausweis, Fernbedienungen, Datenschutz usw.

## 2.1 Grundlagen der Kryptografie

Kryptografie ist eine moderne, mathematisch geprägte Wissenschaft, die für Informatiker eine wichtige Rolle spielt, um IT-Systeme, Anwendungen, Informationen und die Infrastruktur des Internets angemessen zu schützen. Die Kryptografie ist aus der Wissens- und Informationsgesellschaft nicht mehr wegzudenken, und jeder, der sich darin zurechtfinden will, sollte zumindest einige ihrer Grundprinzipien und Funktionsweisen kennen, um eine optimale und richtige Nutzung zu gewährleisten.

**Wichtig** Kryptografie ist heute Bestandteil des Alltagslebens; ihre Prinzipien und Funktionsweisen zu kennen, hilft, sie optimal und richtig anzuwenden.

### 2.1.1 Grundlagen der Verschlüsselung

Das Ziel der Verschlüsselung besteht darin, Daten in einer solchen Weise einer mathematischen Transformation zu unterziehen, dass es einem Unbefugten unmöglich ist, die Originaldaten aus den transformierten, verschlüsselten Daten zu rekonstruieren. Damit die verschlüsselten Daten für ihren legitimen Nutzer dennoch verwendbar bleiben, muss es diesem aber möglich sein, durch Anwendung einer inversen Transformation aus ihnen wieder die Originaldaten zu generieren. Die Originaldaten werden als Klartext (clear text, plain text, message) bezeichnet, die transformierten Daten werden Schlüsseltext (Chiffertext, Chiffrat, Kryptogramm, cipher text) genannt. Die Transformation heißt Verschlüsselung (Encryption), ihre Inverse Entschlüsselung (Decryption).

**Wichtig** Verschlüsselung dient zur Übertragung und Speicherung geheimer Informationen, die nur dem legitimen Empfänger/Besitzer zugänglich sein sollen.

Das generelle Ziel der Verschlüsselung kann folgendermaßen formuliert werden: Die Entschlüsselung darf nur den legitimen Empfängern/Besitzern der übermittelten/gespeicherten Informationen möglich sein, nicht jedoch anderen Personen – im Extremfall nicht einmal den Absendern/Initiatoren selbst, die eine Information verschlüsselt haben.

Dieses Ziel lässt sich offensichtlich genau dann erreichen, wenn nur die legitimen Empfänger/Besitzer die zur Entschlüsselung benötigten Informationen kennen und es ohne diese Kenntnis nicht möglich ist, die ursprüngliche Information aus dem Schlüsseltext zu bestimmen. Es wäre also auf den ersten Blick ausreichend, wenn Sender und Empfänger eine nur ihnen bekannte Transformation untereinander absprechen und die Kenntnisse darüber geheim halten, siehe Abb. 2.1. Mit Transformation ist die Verschlüsselung und Entschlüsselung eines bestimmten Verschlüsselungsalgorithmus gemeint.

Dieser Ansatz ist jedoch aus drei Gründen nicht praktikabel:

1. Definition und Realisierung eines Verschlüsselungsalgorithmus erfordern einen erheblichen Aufwand. Dieses Argument wiegt umso schwerer, als es von Zeit zu Zeit notwendig ist, den Verschlüsselungsalgorithmus zu wechseln. In diesem Fall müsste ein neuer Verschlüsselungsalgorithmus entwickelt werden.



**Abb. 2.1** Einfachste mögliche Vorgehensweise bei einer Verschlüsselung

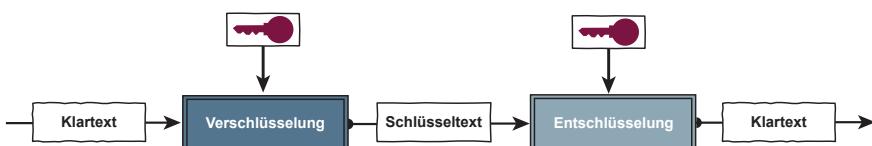
**Wichtig** Die Eigenentwicklung von Verschlüsselungsverfahren erfordert großen Aufwand sowie große Expertise und führt meist zu mangelhaften Resultaten.

2. Es besteht das Risiko, dass es einem Angreifer möglich ist, aus der Struktur der verschlüsselten Daten den Klartext oder die zur Verschlüsselung beziehungsweise Entschlüsselung verwendete Transformation abzuleiten, also die Verschlüsselung zu „brechen“. Da es sehr aufwendig ist, den Nachweis zu führen, dass ein neues Verschlüsselungsverfahren gegen derartige Angriffe durch „Kryptoanalyse“ sicher ist, und da ad hoc bestimmte Verschlüsselungsalgorithmen mit hoher Wahrscheinlichkeit unsicher sind, ist der Einsatz eigener Verfahren für jede einzelne Kommunikation praktisch unmöglich.

**Wichtig** In der Praxis werden nur Verschlüsselungsalgorithmen eingesetzt, die etabliert und die nachweislich sicher sind. Ebenfalls muss der Algorithmus im Laufe der Zeit gewechselt werden, um die Aktualität des Verfahrens sicherzustellen.

3. Als letztes ist der untragbare Aufwand bei wechselnden Kommunikationspartnern zu nennen, da für jeweils zwei Partner ein separater Verschlüsselungsalgorithmus zur Verfügung stehen muss. Der mit dessen Entwicklung, Übermittlung, Aufbewahrung und Geheimhaltung verbundene Aufwand ist organisatorisch kaum zu bewältigen und wirtschaftlich nicht vertretbar.

Als Lösung dieser Probleme bietet sich an, zur Verschlüsselung nur einige wenige Verschlüsselungsalgorithmen einzusetzen, deren Sicherheit aktuell erwiesen ist. Um dennoch die Forderung nach einer Vielzahl von Verschlüsselungsverfahren zu erfüllen, kann das Verschlüsselungsverfahren zusätzlich von einem Parameter abhängig gemacht werden, dem sogenannten **Schlüssel**, der den Ablauf der Transformation so stark beeinflusst, dass ohne seine Kenntnis keine Entschlüsselung möglich ist, siehe Abb. 2.2.



**Abb. 2.2** Schlüsselabhängige Verschlüsselung

Bleibt dieser Schlüssel geheim, so kann der Verschlüsselungsalgorithmus selbst durchaus öffentlich gemacht werden; dies sollte sogar der Regelfall sein, da sich dessen Sicherheit nur in einer öffentlichen Diskussion hinreichend beweisen lässt.

### 2.1.2 Definition eines kryptografischen Verfahrens

Ein kryptografisches Verfahren wie ein Verschlüsselungsalgorithmus ist als 6-Tupel  $(M; C; K_E; K_D; E; D)$  beschreibbar:

**M = Menge der Klartext-Nachrichten m** (messages, clear text, plain text), zum Beispiel  $M = \{0, 1\}$ , also die Menge der endlichen 0,1-Folgen

**C = Menge der Schlüsseltext-Nachricht c** (verschlüsselte Nachrichten, cipher text, Chifferrat), zum Beispiel  $C = \{0, 1\}$ , also die Menge der endlichen 0,1-Folgen

**$K_E$  = endliche, nicht-leere Menge des Verschlüsselungs-Schlüssels,**  
zum Beispiel  $K_E = \{0, 1\}^X$  ( $X$ : Anzahl der Bits, zum Beispiel 256 Bit)

**$K_D$  = endliche, nicht-leere Menge des Entschlüsselungs-Schlüssels**  
mit:  $k_d = f(k_e)$ ,  $k_d \in K_D$ ,  $k_e \in K_E$

**E = Verschlüsselungsverfahren**  $E: M \times K_E \rightarrow C$  (umkehrbar)

**D = Entschlüsselungsverfahren**  $D: C \times K_D \rightarrow M$   
mit für  $m \in M$ :  $D(E(m, k_e), k_d) = m$  mit  $k_e \in K_E$ ,  $k_d \in K_D$  und  $f(k_e) = k_d$

### 2.1.3 No Security by Obscurity

„No Security by Obscurity“ hat unter Mathematikern, die sich wissenschaftlich mit Verschlüsselung befassen, eine lange Tradition und geht zurück auf den niederländischen Linguisten und Kryptologen Auguste Kerckhoffs von Nieuwenhof, der 1883 in seiner Abhandlung „*La Cryptographie militaire*“ einige Grundsätze für schlüsselbasierte Verfahren entwickelte, von denen einer noch heute als Kerckhoffs Prinzip bekannt ist:

**Wichtig** Die Sicherheit von kryptografischen Verfahren darf nur von der Geheimhaltung der Schlüssel, aber nicht von der Geheimhaltung der Verfahren abhängig sein.

Dennoch sind noch immer wesentliche Einsatzfelder von Kryptografie durch den gegenteiligen Ansatz geprägt, der oft mit „Security by Obscurity“ (Sicherheit durch Geheimhaltung) bezeichnet wird, von dem sich die Entwickler entsprechender Verfahren eine stärkere Sicherheit erhoffen.

Ein Beispiel für geheime Verfahren stellen die Kryptoalgorithmen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) dar, die zum Schutz der geheimen Informationen der Bundesrepublik Deutschland genutzt werden.

Ein recht kritisches Beispiel waren die bei der Mobilfunktechnik GSM eingesetzten Algorithmen A3, A8 und A5 oder Verschlüsselungsverfahren beim Pay-TV. Diese galten schon lange nicht mehr als sicher und waren mit moderner Technik leicht zu brechen.

Ob geheime Verschlüsselungsalgorithmen einer Überprüfung Stand halten, darf mit einem Recht bezweifelt werden: Denn die Entwicklung neuer kryptografischer Verfahren ist äußerst schwierig, weswegen die wenigen auf diesem Gebiet tätigen Fachleute ihre Arbeit in der Regel einem fachkundigen Publikum vorstellen.

Dieses bewertet zunächst die theoretische Stärke des vorgestellten Verfahrens, also die Wahrscheinlichkeit, dass es durch eine der im nächsten Abschnitt beschriebenen Methoden, der sogenannten Kryptoanalyse, gebrochen (kompromittiert) wird. Erst wenn ein kryptografisches Verfahren einige Jahre nicht durch Krypto-Experten gebrochen wurde, gilt es als sicher und darf sich dann praktisch bewähren.

#### **2.1.4 Die wichtigsten Begriffe in Kurzdefinition**

In diesem Abschnitt werden die wichtigsten Begriffe im Bereich der Kryptografie kurz definiert:

---

**Kryptografie**

ist die Wissenschaft von den Methoden der Ver- und Entschlüsselung.

---

**Kryptoanalyse**

ist die Wissenschaft von den Methoden der unbefugten Entschlüsselung von Daten zum Zweck der Rückführung der ursprünglichen Information.

---

**Kryptosystem**

dient zur Geheimhaltung von übertragenen oder gespeicherten Informationen gegenüber Dritten. Ein Kryptosystem ist ein kryptografisches Verfahren.

---

**Kryptoanalyse**

ist die Analyse eines Kryptosystems zum Zwecke der Bewertung seiner kryptografischen Stärke.

---

**Kryptologie**

ist die Wissenschaft der Geheimhaltung von Informationen durch Transformation der Daten. Sie umfasst Kryptografie und Kryptoanalyse.

---

**Steganografie**

ist eine Methode zum Verbergen der Existenz einer Information.

### 2.1.5 Begriffe aus der Kryptoanalyse

Angriffe gegen Kryptosysteme können folgendermaßen unterschieden werden:

#### Black Box-Modelle

Der Angreifer sieht nur, was er in den Verschlüsselungsalgorithmus hineinsteckt und was herauskommt. Es gibt mehrere Modelle für Black Box-Angriffe, die im Folgenden aufgezählt und kurz erläutert werden:

##### 1. Ciphertext-only attack

Der Kryptoanalytiker kennt außer dem verwendeten Kryptoverfahren nur den Schlüsseltext. Der Angreifer kann selber weder Ver- noch Entschlüsselungen anstoßen, er ist völlig passiv.

##### 2. Know-plaintext attack

Hier stehen dem Kryptoanalytiker Klartext/Schlüsseltext-Paare zur Verfügung. Diese Paare können zum Beispiel dadurch erlangt werden, dass bestimmte Zeichenfolgen bekannt sind, die im Klartext vorkommen (zum Beispiel HTTP-Header-Informationen, wie Codierung, User-Agent usw.).

##### 3. Chosen-plaintext attack

Der Kryptoanalytiker hat Zugang zum Verschlüsselungsgerät, nicht aber zum Schlüssel und kann somit beliebige Klartexte verschlüsseln. Durch gezielte Wahl des Klartextes lässt sich unter Umständen der Schlüssel mit wesentlich niedrigerem Aufwand als bei den beiden anderen Verfahren bestimmen, sodass der Angreifer mit ausgewähltem Klartext die höchsten Anforderungen an die Sicherheit des Verschlüsselungsverfahrens stellt!

##### 4. Chosen-ciphertext attack

Der Angreifer kann verschlüsseln und entschlüsseln. Dieses Modell wird häufig verwendet, um den exakten Schlüssel herauszufinden und zu verteilen, beispielsweise beim Umgehen des Kopierschutzes von Video-Portalen. Hier reicht es nicht, eine Entschlüsselung durchzuführen, sondern es wird der exakte Schlüssel benötigt, um das Ganze zu verteilen.

### 2.1.6 Strategien der Analyse eines Kryptosystems

Der Verschlüsselungsalgorithmus und der Schlüssel bilden zusammen ein sogenanntes Verschlüsselungs- oder Kryptosystem. Für die Analyse derartiger Verschlüsselungssysteme gibt es verschiedene grundlegende Strategien, aus denen sich Anforderungen an die Qualität ableiten lassen. Im Folgenden werden vier Strategien der Analyse eines Kryptosystems vorgestellt.

## 1. Vollständige Suche

Die vollständige Suche (Brute-Force-Methode) besteht im Wesentlichen im Ausprobieren aller möglichen Schlüsselkombinationen. Bei einem Know-Plaintext-Angriff wird der bekannte Klartext mit allen möglichen Schlüsselkombinationen verschlüsselt und der entstehende Schlüsseltext mit dem bekannten Schlüsseltext verglichen.

Bei einer Schlüssellänge von 128 Bits gibt es  $2^{128}$  ( $3,4 * 10^{38}$ ) verschiedene Kombinationen, die ausprobiert werden müssen. Unter der Voraussetzung, dass eine Operation  $1 * 10^{-9}$  s benötigt, dauert die vollständige Suche  $1,08 * 10^{22}$  Jahre, das heißt, solche Verfahren sind praktisch sicher gegen vollständige Suchangriffe.

**Forderung:** Der Schlüssel muss immer lang genug gewählt werden, damit eine vollständige Suche praktisch mit den verfügbaren Ressourcen nicht umgesetzt werden kann.

## 2. Trial-and-Error-Methode

Bei der Trial-and-Error-Methode wird die vollständige Suche dadurch reduziert, dass aus dem gesamten Schlüsselraum Teilräume herausgegriffen werden, in denen der gesuchte Schlüssel vermutet wird. Dies ist etwa der Fall, wenn es viele äquivalente Schlüssel mit übereinstimmenden Eigenschaften gibt (zum Beispiel Vornamen, Spitznamen, Firmenname usw.).

Beispiel: Es werden als Schlüssel nur darstellbare ASCII-Zeichen verwendet, also die Ziffern 0 bis 9 sowie alle Klein- und Großbuchstaben des lateinischen Alphabets – insgesamt 62 verschiedene ASCII-Zeichen, die in 5 Bit codiert werden können. Damit reduziert sich die Zahl der möglichen Kombinationen von  $2^{128}$  auf  $2^{80}$  und damit die Entschlüsselungszeit erheblich.

**Forderung:** Eine qualitativ hochwertige Schlüsselgenerierung, die den vollständigen Schlüsselraum ausnutzt, ist sehr wichtig, damit eine Reduzierung der vollständigen Suche nicht möglich ist.

## 3. Statistische Methoden

Bei den statistischen Methoden versucht der Analytiker, statistische Strukturen, wie zum Beispiel Buchstaben- oder Worthäufigkeiten einer Sprache, im Schlüsseltext wiederzufinden, um dadurch an den Klartext zu gelangen.

**Forderung:** Ein Verschlüsselungsverfahren muss solche Angriffe prinzipiell ausschließen.

## 4. Strukturanalyse des Kryptosystems (Short-Cut-Methode)

Die Strukturanalyse des Kryptosystems, oder auch Short-Cut-Methode genannt, ist immer nur auf ein spezielles Kryptosystem zugeschnitten. Sind alle Parameter außer dem Schlüssel bekannt, versucht der Analytiker, mit ihrer Hilfe eine Funktion aufzustellen, mit der sich der Klartext berechnen lässt. Das kann zum Beispiel dann schnell zum Erfolg führen, wenn er den Schlüsseltext, den verwendeten Algorithmus und die Struktur des Originaldokuments kennt.

$m = \text{Kyptoanalyse}(c, \text{Design}, \text{Struktur}, \text{sonstige Parameter})$

**Forderung:** Ein Verschlüsselungsverfahren muss mindestens fünf Jahre öffentlich von den Fachleuten diskutiert werden, damit die Wahrscheinlichkeit des Findens einer Short-Cut-Methode sehr klein ist.

### 2.1.7 Bewertung der kryptografischen Stärke

In der Regel werden die kryptografischen Verfahren, die entwickelt werden, der Kryptologen-Gemeinde (mehrere 100 Krypto-Spezialisten in diesem besonderen Fachgebiet aus der ganzen Welt) zur Verfügung gestellt, damit die Kryptoanalyse beginnen kann. Vorgestellt werden die kryptografischen Verfahren mit allen Design-Aspekten auf öffentlichen Konferenzen, wie zum Beispiel Eurocrypt, Crypto, Asiacrypt usw. und/oder bei Wettbewerben der Jury, in der die entsprechenden Kryptografie-Spezialisten sitzen.

Erst wenn es nach ca. fünf Jahren nachweisbar viele Kryptografie-Spezialisten nicht geschafft haben, das neue kryptografische Verfahren zu brechen, gilt ein kryptografisches Verfahren als praktisch sicher. Allerdings werden immer wieder solche Verfahren auch nach den fünf Jahren von Mathematikern gebrochen. Eine Garantie für die Sicherheit des kryptografischen Verfahrens ist damit nicht gegeben, allerdings minimiert sich so die Gefahr, dass kryptografische Verfahren genutzt werden, die nachweislich unsicher sind.

#### Konsequenzen aus der prinzipiellen Möglichkeit der vollständigen Suche

Prinzipiell lässt sich die vollständige Schlüsselsuche (Brute-Force-Methode) gegen jedes Kryptoverfahren einsetzen. Sie führt aber nur dann zum Erfolg, wenn genügend Rechnerzeit und Speicherplatz zur Verfügung stehen. Daher lässt sich ein Kryptosystem in zwei Sicherheitskategorien einteilen.

#### 1. Absolute Sicherheit

Absolute Sicherheit liegt vor, wenn es theoretisch unmöglich ist, das Verschlüsselungssystem zu brechen. Diese Anforderung erfüllt zurzeit nur das Einmal-Schlüssel-Verfahren mit definierten Eigenschaften, siehe dazu den Abschn. 2.3 „Der Einmal-Schlüssel“.

#### 2. Rechnerische, praktische Sicherheit

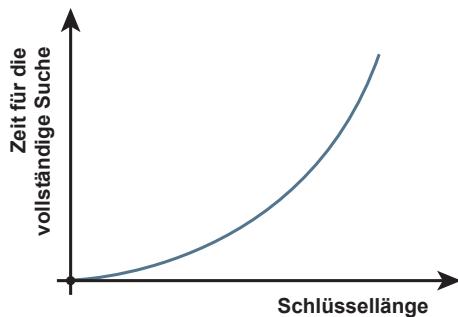
Bei der rechnerischen oder praktischen Sicherheit ist es zwar theoretisch möglich, das Kryptosystem zu brechen, praktisch wird dazu jedoch so enorm viel Rechnerzeit beziehungsweise Speicherplatz benötigt, dass dieser Weg einem jeden Kryptanalytiker aussichtslos erscheint und deswegen nicht umgesetzt werden kann. Die rechnerische, praktische Sicherheit kann durch eine mathematische Analyse der Komplexität festgestellt werden. Wichtig ist, dass sich die rechnerische, praktische Sicherheit im Laufe der Zeit durch die Verbesserung der IT-Systeme verändert.

#### Aufwand für den Angreifer

In Tab. 2.1 wird der Aufwand der vollständigen Schlüsselsuche in Abhängigkeit der Schlüssellänge aufgezeigt. Je länger der Schlüssel ist, umso aufwendiger wird das Durchprobieren aller möglichen Schlüssel. Je länger der Schlüssel ist, umso sicherer ist das kryptografische Verfahren.

**Tab. 2.1** Aufwand für den Angreifer

Schlüssellänge in Bits	Anzahl der möglichen Schlüssel	Aufwand, den richtigen Schlüssel zu finden, in Jahren. (Annahme dieser Betrachtung: 1.000.000.000 Versuche in der Sek.)
8	256	0,00000
40	1.099.511.627.776	0,00002
56	72.057.594.037.927.900	1,14
64	1,84E + 19	292,47
128	3,40E + 38	5.391.448.762.278.160.000.000 (länger als das Universum bisher existiert)
192	6,27E + 57	9,95E + 40
256	1,16E + 77	1,83E + 60

**Abb. 2.3** Komplexität der vollständigen Suche

### Abhängigkeit der vollständigen Suche von der Schlüssellänge

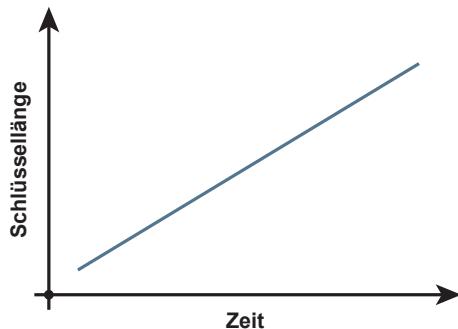
$m = \text{Brute-Force-Funktion } (c) \rightarrow \text{Komplexitätsklasse exponentiell } O(2^n)$

$m = \text{Klartext}, c = \text{Schlüsseltext}, n = \text{Schlüssellänge in Bit}$

Die exponentielle Komplexitätsklasse bedeutet, dass jedes zusätzliche Bit im Schlüssel eine Verdoppelung der notwendigen Rechnerleistung für einen erfolgreichen (Brute-Force-)Angriff verursacht, siehe Abb. 2.3.

**Wichtig** Je länger der Schlüssel ist, umso sicherer ist das kryptografische Verfahren, wenn das Verfahren an sich als sicher gilt.

**Abb. 2.4** Die Schlüssellänge wird mit der Zeit immer größer



### Ein Wettlauf um die Sicherheit

Für die Sicherheit einer Verschlüsselung sind vier Faktoren ausschlaggebend:

1. Der verwendete Verschlüsselungsalgorithmus,
2. die Schlüssel- und Zufallszahlengenerierung,
3. die Schlüssellänge sowie
4. die Aufbewahrung des Schlüssels.

Bei symmetrischen Verschlüsselungsverfahren wird heute davon ausgegangen, dass die praktische Sicherheit gegeben ist, wenn die Schlüssellänge mindestens 128 Bit beträgt. Um einen solchen Schlüssel durch eine vollständige Suche zu ermitteln, sind  $2^{128}$  Versuche nötig. Damit entsteht ein praktisches Problem, denn mit den derzeitigen Ressourcen ist die Berechnung in einer angemessenen Zeit nicht möglich. Da aber die Rechenleistung von IT-Systemen ständig wächst, müssen auch die Schlüssellängen von Zeit zu Zeit angepasst werden, siehe Abb. 2.4. Gegenüber den vor 20 Jahren gebräuchlichen Verfahren wie DES mit 64-Bit-Schlüssel hat sich diese inzwischen verdoppelt, und die meisten Anwendungen nutzen heute schon den AES mit 256-Bit-Schlüssel, um den AES für die nächsten Jahre nutzen zu können.

Alle 10 bis 20 Jahre ist ein Wechsel von kryptografischen Verfahren notwendig, die mit einem längeren Schlüssel arbeiten! Daher muss bei allen Cyber-Sicherheitssystemen, die mit kryptografischen Verfahren arbeiten, mit eingeplant werden, dass kryptografische Verfahren im Laufe der Zeit ein Update brauchen oder gewechselt werden müssen. Das Wechseln kann einen großen Aufwand verursachen.

**Wichtig** Da IT-Systeme immer mehr Rechnerleistung und Speicherplatz zur Verfügung haben, sind vor allem die verwendeten Schlüssellängen regelmäßig anzupassen.

## 2.1.8 Unterstützung bei der Einschätzung von Verfahren und Schlüssellängen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt jedes Jahr die Technische Richtlinie „kryptografische Verfahren: Empfehlungen und Schlüssellängen“ heraus. Mit dieser Technischen Richtlinie legt das BSI eine Bewertung der Sicherheit ausgewählter kryptografischer Verfahren vor und ermöglicht damit eine längerfristige Orientierung bei der Wahl jeweils geeigneter Methoden. Dabei wird kein Anspruch auf Vollständigkeit erhoben, das heißt, nicht aufgeführte Verfahren werden vom BSI nicht unbedingt als unsicher beurteilt. Die Richtlinie richtet sich in erster Linie an Entwickler, die die Einführung neuer kryptografischer Infrastrukturen planen.

Siehe: [https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index\\_htm.html](https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html).

**Wichtig** Für die Einschätzung, welche kryptografischen Verfahren und Schlüssellängen als sicher gelten, gibt das BSI regelmäßig die Technische Richtlinie „kryptografische Verfahren: Empfehlungen und Schlüssellängen“ heraus.

## 2.1.9 Zusammenfassung: Grundlagen der Kryptografie

Es gibt viele Aspekte, die erfüllt sein müssen, damit kryptografische Verfahren sicher genutzt werden können.

Ausreichende Wirkung	Beschreibung
	Wenn alle Design-Aspekte von kryptografischen Verfahren bekannt sind, die Fachleute diese ausreichend genug analysiert haben und die Schlüssellänge lang genug ist, haben die kryptografischen Verfahren eine ausreichende Wirkung, um digitale Werte angemessen zu schützen

## Elementare Verschlüsselungsverfahren

In der Geschichte haben elementare Verschlüsselungsverfahren über die Schicksale von Menschen und Gesellschaften entschieden [2]. Heute spielen sie in ihrer klassischen Form nur noch beim Austausch von Nachrichten unter Freunden oder als Denksportaufgaben eine unterhaltsame Rolle. In diesem Abschnitt wird auf diese Verfahren tiefer eingegangen, um damit die Übungsaufgaben im entsprechenden Abschnitt und den Zugang zu grundlegenden Ideen der Kryptografie zu erleichtern.

Zu den elementaren Verschlüsselungsverfahren gehören zunächst alle Verfahren der Textverschlüsselung, bei denen Buchstaben oder Zeichen durch jeweils andere Buchstaben oder Zeichen ersetzt werden. Ein Beispiel aus der Geschichte liefert das Babington-Komplott von 1586, der Versuch, die protestantische englische Königin Elisabeth I. zu stürzen und durch ihre katholische Rivalin Maria Stuart, die schottische Throninhaberin, zu ersetzen, die zu dieser Zeit in einem Gefängnis in Derbyshire saß. Babington, ein ehemaliger Page Stuarts, und seine Mitverschwörer sendeten ihr verschlüsselte Briefe, die jedoch abgefangen und von dem Chiffrierungsexperten Thomas Phelippes entschlüsselt wurden, was zum Todesurteil über die schottische Königin und ihre Unterstützer führte.

Ein weiteres populäres Beispiel für elementare Verschlüsselungsverfahren und Basis für Hollywood-Filme ist die deutsche Enigma-Maschine aus dem Zweiten Weltkrieg. Diese elektromechanische Rotor-Schlüsselmaschine ver- und entschlüsselte mithilfe von Walzen. Bis zu ihrer endgültigen Kompromittierung durch den britischen Mathematiker Alan Turing 1940 verrichtete Enigma ihre Dienste besonders für die deutsche U-Boot-Flotte, danach profitierten die Alliierten. Die Entschlüsselung war von entscheidender Bedeutung für den weiteren Kriegsverlauf.

### 2.1.10 Monoalphabetische Substitution

Als erstes elementares Verfahren wird die Substitution betrachtet. Die monoalphabetische Substitution ist eine recht einfache Methode, um einen Klartext zu verschlüsseln. Dabei wird jedes Zeichen des Klartextes nach einem festgelegten Schema, der Verschlüsselungsvorschrift, durch ein anderes, ihm zugeordnetes Zeichen ersetzt (substituiert).

Die Verschlüsselungsvorschrift im Beispiel sieht vor, jeden Buchstaben des lateinischen Alphabets durch genau einen anderen zu ersetzen: I durch U, T durch Q, S durch P usw. Aus dem Klartext „ITSICHERHEIT“ wird der Schlüsseltext „UQPUXKLYKLUQ“. Bei einer anderen Verschlüsselungs-, also Zuordnungsvorschrift sieht auch der Schlüsseltext anders aus. Für dieses Verfahren lassen sich auch verschiedenartige Alphabete einsetzen, so können etwa lateinische Buchstaben und 26 ausgewählte chinesische Schriftzeichen verwendet werden.

#### Beispiel Verschlüsselungsvorschrift einer Monoalphabetischen Substitution

(1)	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
(2)	G W X V L O A K U B C N D R M F H Y P Q T Z E I J S

#### Beispiel einer Verschlüsselung

Klartext	ITSICHERHEIT
Schlüsseltext	UQPUXKLYKLUQ

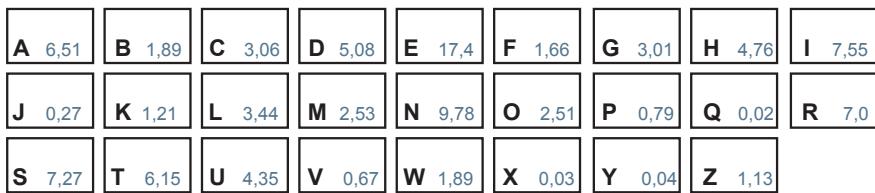


Abb. 2.5 Häufigkeit der Buchstaben des deutschen Alphabets

### 6-Tupel ( $M; C; K_E; K_D; E; D$ ) für die monoalphabetische Substitution

- E und D: Monoalphabetische Substitution
- $K_E$  und  $K_D$ : Verschlüsselungsvorschrift (Tabelle)
- M und C: Klartext und Schlüsseltext

### Kryptoanalyse: Monoalphabetische Substitution

Eine monoalphabetische Substitution ist sehr leicht zu brechen. Der Schlüssel dazu liegt in der charakteristischen Häufigkeit, mit der Buchstaben in natürlichen Sprachen auftauchen. Abb. 2.5 zeigt diese Verteilung für das deutsche Alphabet.

Nach der Statistik kommt im Deutschen das E am häufigsten vor (17,4 %), gefolgt von N (9,78 %), I (7,55 %), S (7,25 %), R (7 %) usw. Diese Verteilung bleibt auch nach der monoalphabetischen Substitution (Verschlüsselung) erhalten, und mit ihrer Hilfe können Kryptoanalytiker aus dem Schlüsseltext den Klartext berechnen, vorausgesetzt, dass dieser in deutscher Sprache verfasst wurde.

### 2.1.11 Homofone Substitution

Die homofone Substitution ist eine Verbesserung der monoalphabetischen Substitution. Die Verbesserung wird durch eine Verschleierung der Häufigkeit erreicht. Das heißt, die Verschlüsselungsvorschrift wird so gestaltet, dass alle Schlüsseltextzeichen mit der gleichen Wahrscheinlichkeit auftreten: Jedem Buchstaben ist eine Menge von Zeichen zugeordnet, und zwar so, dass die Anzahl der Schlüsseltextzeichen, die zu ihm gehören, seiner Häufigkeit entspricht. Demnach existieren für das E die meisten Zeichen, während für Raritäten wie X oder Y ein einzelner Ersatz ausreicht. Bei der Verschlüsselung wird der Klartextbuchstabe zufällig einem passenden Schlüsseltextzeichen zugeordnet. Da Letztere zufällig gewählt werden, kommt jedes Zeichen gleich häufig vor.

### Beispiel Verschlüsselungsvorschrift einer homofonen Substitution

#### Klartext    Schlüsseltext

A	(10, 21, 52, 59, 71)
B	(20, 34)
C	(28, 06, 80)
D	(19, 58, 70, 81, 87)

- 
- E (09, 18, 29, 33, 38, 40, 42, 54, 55, 60, 66, 75, 85, 86, 92, 93, 99)  
F (00, 41)  
G (08, 12, 97)  
H (01, 07, 24)  
I (14, 39, 50, 65, 76, 88, 94)  
J (57)  
K (23)  
L (02, 05, 82)  
M (27, 11, 49)  
N (30, 35, 43, 62, 67, 68, 72, 77, 79)  
O (26, 53)  
P (31)  
Q (25)  
R (17, 36, 51, 69, 74, 78, 83)  
S (15, 16, 45, 56, 61, 73, 96)  
T (13, 32, 90, 91, 95, 98)  
U (03, 04, 47)  
V (37)  
W (22)  
X (44)  
Y (48)  
Z (64)

### **Beispiel einer Verschlüsselung**

Klartext: K R Y P T O L O G I E

Schlüsseltext: 23 69 48 31 90 26 05 53 08 94 33

Beispiel: Der Klartext werde aus den 26 Großbuchstaben gebildet, der Schlüsseltext aus den Zahlen 1 bis 99 bestimmt. Die Zuordnung der Zahlen zu den Großbuchstaben hängt von der Häufigkeit der Buchstaben ab.

In dem Beispiel werden die einzelnen Buchstaben durch zufällig ausgewählte Schlüsseltextzeichen substituiert, die ihnen zugeordnet sind: K durch 23, R durch 69 (möglich wären auch 17, 36 etc.), Y durch 48 usw.

### **6-Tupel ( $M$ ; $C$ ; $K_E$ ; $K_D$ ; $E$ ; $D$ ) für die homofone Substitution**

- E und D: Homofone Substitution
- KE und KD: Verschlüsselungsvorschrift (Tabelle)
- M und C: Klartext und Schlüsseltext

### **Kryptoanalyse: Homofone Substitution**

Natürlich können auch homofone Substitutionen gebrochen werden. Ein Ansatz dafür basiert auf der Beobachtung, dass nicht nur einzelne Buchstaben, sondern auch bestimmte Buchstabenpaare statistisch gesehen häufiger vorkommen als andere, wie aus Abb. 2.6 hervorgeht. Diese Vorgehensweise ist natürlich noch längst keine vollständige Kryptoanalyse. Sie zeigt aber deutlich, dass auch ein auf

**Abb. 2.6** Häufigkeit von Buchstabenpaaren der deutschen Sprache

EN 3,88	ER 3,75	CH 2,75	TE 2,26	DE 2,00
ND 1,99	EI 1,88	IE 1,79	IN 1,67	ES 1,52

den ersten Blick „praktisch unknackbares“ Verfahren sich bei näherem Hinsehen als durchaus angreifbar entpuppt. Dies ist ein weiteres Beispiel dafür, dass die Entwicklung von Kryptosystemen sehr komplex ist und erklärt, warum nur wenige Experten sie erfolgreich betreiben.

### 2.1.12 Polyalphabetische Substitution

Weitere Chiffriermethoden verschleiern die Häufigkeit noch stärker. Dazu zählen alle polyalphabetischen Substitutionsverfahren mit ihrer bekanntesten Methode, der Vigenère-Verschlüsselung. Diese arbeitet mit einem Schlüssel, der aus einer Zeichenfolge besteht. Mithilfe der darin verwendeten Zeichen wird eine bestimmte Zeile einer Tabelle „angewählt“; darin wiederum ist jedem Klartextzeichen eine bestimmte Spalte zugeordnet. Der Kreuzungspunkt von Zeile und Spalte enthält dann das zugehörige Schlüsseltextzeichen. Ist der Schlüssel kürzer als das zu chiffrierende Klartextwort, wird er wiederholt. Die Entschlüsselung erfolgt auf umgekehrtem Weg und setzt die Kenntnis des Schlüssels voraus. Es folgt ein Beispiel für eine solche Verschlüsselungsvorschrift.

Klartext:	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Schlüsseltext:	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z B C D E F G H I J K L M N O P Q R S T U V W X Y Z A C D E F G H I J K L M N O P Q R S T U V W X Y Z A B D E F G H I J K L M N O P Q R S T U V W X Y Z A B C E F G H I J K L M N O P Q R S T U V W X Y Z A B C D F G H I J K L M N O P Q R S T U V W X Y Z A B C D E G H I J K L M N O P Q R S T U V W X Y Z A B C D E F H I J K L M N O P Q R S T U V W X Y Z A B C D E F G I J K L M N O P Q R S T U V W X Y Z A B C D E F G H J K L M N O P Q R S T U V W X Y Z A B C D E F G H I K L M N O P Q R S T U V W X Y Z A B C D E F G H I J L M N O P Q R S T U V W X Y Z A B C D E F G H I J K M N O P Q R S T U V W X Y Z A B C D E F G H I J K L N O P Q R S T U V W X Y Z A B C D E F G H I J K L M O P Q R S T U V W X Y Z A B C D E F G H I J K L M N P Q R S T U V W X Y Z A B C D E F G H I J K L M N O Q R S T U V W X Y Z A B C D E F G H I J K L M N O P R S T U V W X Y Z A B C D E F G H I J K L M N O P Q S T U V W X Y Z A B C D E F G H I J K L M N O P Q R T U V W X Y Z A B C D E F G H I J K L M N O P Q R S U V W X Y Z A B C D E F G H I J K L M N O P Q R S T V W X Y Z A B C D E F G H I J K L M N O P Q R S T U W X Y Z A B C D E F G H I J K L M N O P Q R S T U V X Y Z A B C D E F G H I J K L M N O P Q R S T U V W Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
Schlüssel:	G E H E I M G E H E I
Klartext:	D A T E N S C H U T Z
Schlüsseltext:	J E A I V E I L B X H

In diesem Beispiel werden die einzelnen Klartext-Zeichen schlüsselabhängig substituiert: D durch J, da das erste Zeichen des Schlüssels (G) dafür die entsprechende (siebte) Zeile (G) bestimmt; A durch E, da das zweite Zeichen des Schlüssels die fünfte Zeile (E) vorgibt – und so weiter bis zum letzten Buchstaben.

#### **6-Tupel ( $M$ ; $C$ ; $K_E$ ; $K_D$ ; $E$ ; $D$ ) für die polyalphabetische Substitution**

- E und D: Polyalphabetische Substitution
- KE und KD: Verschlüsselungsvorschrift (Tabelle) und der Schlüssel
- M und C: Klartext und Schlüsseltext

#### **Kryptoanalyse: Polyalphabetisches Substitutionsverfahren**

Obwohl es aufwendiger statistischer Analyse bedarf, können auch polyalphabetische Verfahren gebrochen werden. Ein genügend langer Schlüsseltext weist viele statistisch erfassbare Regelmäßigkeiten auf, die es ermöglichen, den Schlüssel zu ermitteln.

Methoden, die die Länge des benutzten Schlüssels für **Polyalphabetische Substitutionen** bestimmen:

Ist der Abstand der beiden Klartextbuchstaben ein Vielfaches der Schlüssellänge, dann ist „gleicher Klartext = gleicher Schlüsseltext“. Wenn der Klartext genauso lang wie der Schlüssel ist, arbeitet das Verfahren wie eine monoalphabetische Substitution.

#### **2.1.13 Transpositionsverfahren**

Als letzte Gruppe elementarer Verschlüsselungsoperationen wird eine Methode betrachtet, bei der einzelne Zeichen des Klartextes nach einer bestimmten Regel permutiert, das heißt vertauscht werden. Diese Methode wird als Transpositionsverfahren bezeichnet und spielt in modernen Kryptosystemen eine Rolle.

In Abb. 2.7 wird als Beispiel das Zickzack-Verfahren vorgestellt. Der Klartext wird hierbei in einer Zickzack-Kurve, zum Beispiel über fünf Zeilen verteilt,

Schlüssel Klartext		Tiefe der Zickzack-Kurve (hier 5)												
		D A T E N M A N A G E M E N T												
1	D							A						
2		A						N		G				
3			T				A				E			T
4				E	M						M		N	
5				N							E			

**Schlüsseltext      D A A N G T A E T E M M M N N E**

**Abb. 2.7** Zickzack-Kurve

aufgeschrieben und anschließend zeilenweise von oben nach unten ausgelesen (der Schlüsselwert beträgt 5).

In dem Beispiel werden die einzelnen Klartext-Zeichen permutiert: Das erste Zeichen D bleibt erhalten, das zweite Zeichen ist nun das neunte (A), das dritte Zeichen ist das zweite (erneut A), das vierte das achte (N) usw.

Auch für die Permutationsverfahren gilt, dass sie prinzipiell mithilfe der Kryptoanalyse entschlüsselt werden können. Dennoch ist klar, dass diese elementaren Verschlüsselungsoperationen in der modernen Kryptografie immer noch eine Rolle spielen.

#### 6-Tupel ( $M; C; K_E; K_D; E; D$ ) für das Transpositionsverfahren

- E und D: Zickzack-Kurve
- KE und KD: Tiefe der Zickzack-Kurve
- M und C: Klartext und Schlüsseltext

#### Lernprogramm: CrypTool

Für diejenigen, die tiefer in das Thema einsteigen wollen, wird das frei erhältliche Lernprogramm CrypTool empfohlen, das bei der Kryptoanalyse und dem Verständnis von Verschlüsselungsverfahren hilft. Dieses Tool ist unter [www.cryptool.de](http://www.cryptool.de) zu finden.

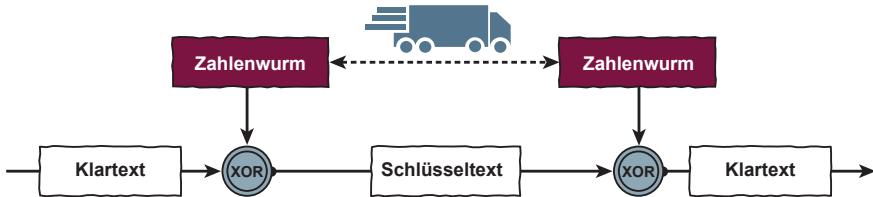
### 2.1.14 Zusammenfassung: Elementare Verschlüsselungsverfahren

Die elementaren Verschlüsselungsverfahren spielen heute in ihrer ursprünglichen Form keine Rolle mehr. Aber sie werden in Kombination und iterativ in modernen Kryptografie-Verfahren verwendet.

Unzureichende Wirkung	Beschreibung
	Die elementaren Verschlüsselungsverfahren sind rechnerisch/praktisch nicht sicher genug, um in der Praxis Anwendung zu finden. Ihre Wirkung alleine ist unzureichend, um die digitalen Werte zu schützen.

#### Der Einmal-Schlüssel

Das Einmal-Schlüssel-Verfahren wird auch individuelle Wurmverschlüsselung, Zahlenwurm oder One-Time-Pad genannt.



**Abb. 2.8** Einmal-Schlüssel-Verfahren

Das Einmal-Schlüssel-Verfahren zählt zu den „absolut sicheren“ Verschlüsselungsverfahren.

Das Verfahren benötigt für jede Nachricht einen Zahlenwurm, das heißt einen Schlüssel, der mindestens die Länge des zu übermittelnden Klartextes haben muss. Wichtig ist auch, dass der Zahlenwurm aus echten gleichverteilten Zufallszahlen bestehen muss. Es darf kein Teil des Schlüssels wiederverwendet wird.

Der Zahlenwurm/Schlüssel muss für jede Nachricht neu durch Zufallskriterien erzeugt werden und sicher zwischen den Kommunikationspartnern verteilt werden. Der Schlüssel und die Nachricht werden bitweise modulo 2 addiert, das heißt XOR verknüpft, siehe Abb. 2.8.

Da jede Nachricht mit einem gleich langen Schlüssel verknüpft wird, geht im Schlüsseltext jede Struktur verloren, sodass der Schlüsseltext für die Kryptoanalyse keinerlei Ansatzpunkte bietet. Wichtig ist die hohe Qualität der Zufallszahlen des Zahlenwurms!

Obwohl dieses Verfahren für den „heißen Draht“ zwischen Washington und Moskau genutzt wurde oder vielleicht in bestimmten Fällen auch noch genutzt wird, ist dieses Verfahren für den kommerziellen Einsatz nicht geeignet, da anstelle des absolut geheimen Schlüssels ebenso gut die zu übertragene Nachricht selbst auf dem sicheren Weg übermittelt werden könnte.

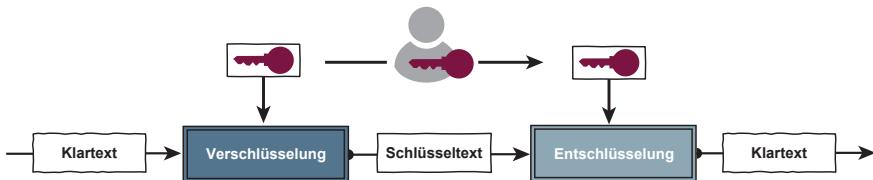
**6-Tupel ( $M; C; K_F; K_D; E; D$ ) für das Einmal-Schlüssel-Verfahren**

- E und D: XOR-Verknüpfung
  - KE und KD: Zahlenwurm
  - M und C: Klartext und Schlüsseltext

**Wichtig** Das Einmal-Schlüssel-Verfahren zählt zu den „absolut sicheren“ Verschlüsselungsverfahren. Aber, da der Schlüssel aus echten Zufallszahlen bestehen und mindestens die Länge des zu übermittelnden Klartextes haben muss, spielt dieses Verfahren in der Praxis keine besondere Rolle.

## Symmetrische Verschlüsselungsverfahren

Die vorgestellten elementaren Verfahren im Abschn. 2.2 gehören ohne Ausnahme zur Gattung der sogenannten symmetrischen Verschlüsselungen [3]. Deren Hauptkennzeichen besteht darin, dass alle an einer Verschlüsselung beteiligten Instanzen



**Abb. 2.9** Symmetrische Verschlüsselungsverfahren

den gleichen Schlüssel kennen und einsetzen. Diese elementaren Verfahren sind aber relativ leicht zu brechen und können damit heute keinen ausreichenden Schutz mehr bieten.

### Produktverschlüsselung

Um diesen Nachteil auszugleichen, werden im praktischen Einsatz mehrere elementare Verfahren mit verschiedenen kryptografischen Eigenschaften zu sogenannten Produktverschlüsselungen verknüpft.

**Wichtig** Ziel der Produktverschlüsselung ist es, kryptografisch stärker, das heißt, schwerer zu brechen zu sein als jede ihrer Einzelverschlüsselung.

Eine der gängigsten Methoden ist dabei die iterative (wiederholte) Verknüpfung nichtlinearer Substitutionen und Permutationen. Bekannteste Vertreter dieser Gattung sind der alte Data Encryption Standard (DES) und der neuere Advanced Encryption Standard (AES).

Neben den DES- und AES-Verfahren gibt es noch IDEA, RC5, Blowfish, CAST usw., die aber keine relevante Rolle spielen. Die Produktverschlüsselungsverfahren sind schlüsselabhängige Verschlüsselungen, bei denen der Schlüssel sicher ausgetauscht werden muss, siehe Abb. 2.9.

#### 2.1.15 Data Encryption Standard

Der DES stellt eine Block-Produkt-Verschlüsselung aus nichtlinearer Substitution und Permutation dar, die schlüsselgesteuert in einer Iterationsschleife 16 Mal durchlaufen wird. Kleine Änderungen im Klartext oder Schlüssel führen dabei zu großen Änderungen im Schlüsseltext – ein Verhalten, das alle als sicher gelgenden kryptografischen Verfahren aufweisen müssen. Entwickelt wurde der Algorithmus bereits Mitte der 70er-Jahre von einem IBM-Forscherteam um Horst Feistel, Walter Tuchman und Don Coppersmith, das mit der US-Standardisierungsbehörde NBS (heute NIST) und der National Security Agency (NSA) zusammenarbeitete. Als lizenzkostenfreies Verfahren, das überdies von vornherein für eine Hardware-Implementierung optimiert war, konnte sich DES sehr bald auch

international etablieren. Auf Kritik stieß allerdings von Anfang an die Kooperation zwischen IBM und der NSA, die unter anderem zur Reduzierung der ursprünglich geplanten Schlüssellänge von 128 auf 56 Bit führte, wodurch der Algorithmus für Brute-Force-Angriffe anfällig wurde. Heute gilt diese Schlüssellänge praktisch (rechnerisch) als unsicher, da moderne IT-Systeme (auch Smartphones) die insgesamt  $2^{56}$  möglichen Schlüsselkombinationen in zu kurzer Zeit durchspielen und damit das Verfahren „knacken“ können. Aufgrund seiner weiten Verbreitung und der bereits erwähnten guten Eignung für die Realisierung in Hardware wurde es jedoch beständig weiterentwickelt und ist noch relativ lange als Triple-DES-Verfahren mit einer Schlüssellänge von 168 Bit verwendet worden. Heute spielt das DES-Verfahren keine Rolle mehr und sollte nicht verwendet werden!

### 2.1.16 Advanced Encryption Standard

Als weitere Folge dieser Entwicklung sah sich die NIST im September 1997 veranlasst, abermals einen Wettbewerb zur Einführung eines neuen Verschlüsselungsstandards abzuhalten. Der Algorithmus musste vor allem zwei Kriterien erfüllen, nämlich erstens mindestens für die nächsten zwei Jahrzehnte als rechnerisch sicher und zweitens lizenzkostenfrei sein. Weitere Anforderungen betrafen Leistungsfähigkeit, Effizienz, Flexibilität und Implementierbarkeit: Die erforderlichen Operationen sollten schnell erfolgen, Speicher und CPU des eingesetzten IT-Systems nicht zu sehr belasten und sich sowohl für den Einsatz in Embedded-Geräten als auch als „reine“ Software-Lösung (etwa fürs Online-Banking) eignen.

Von den ursprünglich eingereichten 21 Vorschlägen genügten 15 diesen Mindestanforderungen. Im Verlauf der weiteren Auswertung blieben schließlich fünf Verfahren für die „letzte Runde“ übrig. Das Wettbewerbskomitee entschied sich schließlich für den sogenannten Rijndael-Algorithmus, den ein Kryptologen-Team der belgischen Universität Leuven um Vincent Rijmen vorgelegt hatte. Den Ausschlag gab dabei einerseits, dass das Verfahren von vornherein für den Einsatz mit variablen Schlüssellängen von 128, 192 und 256 Bit ausgelegt war und andererseits im Gegensatz zu den Alternativvorschlägen in Hard- wie Software-Implementierungen gleichermaßen schnell funktionierte. Praktische Einsatzbeispiele für den mit dem NIST-Entscheid in Advanced Encryption Standard „umgetauften“ Algorithmus sind unter anderem die E-Mail-Verschlüsselung mithilfe von S/MIME und Übertragungsprotokolle, wie IPSec und SSL/TLS für den Datenaustausch im Internet.

#### Funktionsweise von AES

Wie sein Vorgänger ist auch AES ein Produktverschlüsselungsverfahren, welches in mehreren Runden die Bits transformiert. Dazu wird zunächst der Klartext in Blöcke fester Bitlängen eingeteilt, die 128, 192 oder 256 Bit betragen können. Die Anzahl der Transformationsrunden hängt dabei von der Block- und der Schlüssellänge ab und beträgt 10, 12 oder 14, siehe Abb. 2.10.

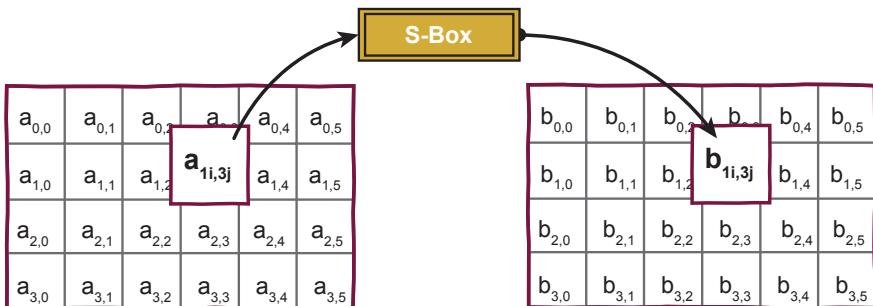
**Abb. 2.10** Schlüssellänge/  
Blocklänge

Schlüssellänge (Bit)	Blocklänge (Bit)		
	128	192	256
128	10	12	14
192	12	12	14
256	14	14	14

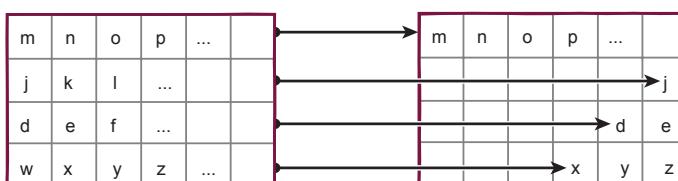
Jede Runde besteht aus einer Reihe byteorientierter Transformationen, welche die Stärken vieler anderer Verschlüsselungsalgorithmen kombinieren. Im ersten Schritt werden die in einem zweidimensionalen Array abgelegten Zeichen des Klartext-Blocks der sogenannten ByteSub-Transformation unterworfen. Es handelt sich also um eine monoalphabetische Substitution der einzelnen Bytes, die über eine Tabelle (die sogenannte Rijndael S-Box, die öffentlich bekannt ist) festgelegt wird, siehe Abb. 2.11.

Den zweiten Schritt stellt die ShiftRow-Transformation dar, eine Permutation, bei der alle Zeilen des Arrays außer der ersten abhängig von der Zeilen- und Blocklänge um maximal vier Spalten nach links verschoben werden. Überlaufende Zeilen werden von rechts fortgesetzt, siehe Abb. 2.12.

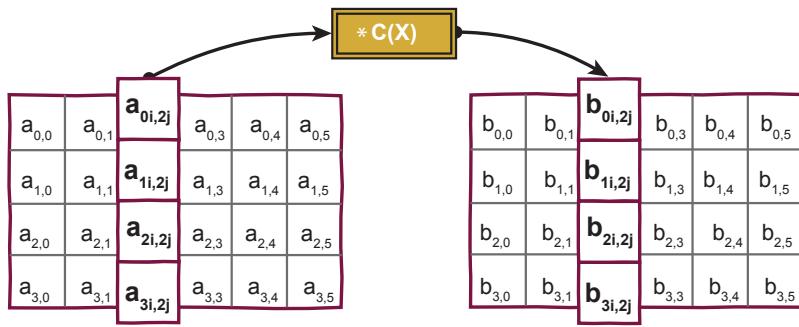
Der dritte Schritt ist die MixColumn-Transformation, bei der jede Spalte des Arrays mit einem festen Polynom multipliziert wird, siehe Abb. 2.13. Die



**Abb. 2.11** ByteSub-Transformation



**Abb. 2.12** ShiftRow-Transformation



**Abb. 2.13** MixColumn-Transformation

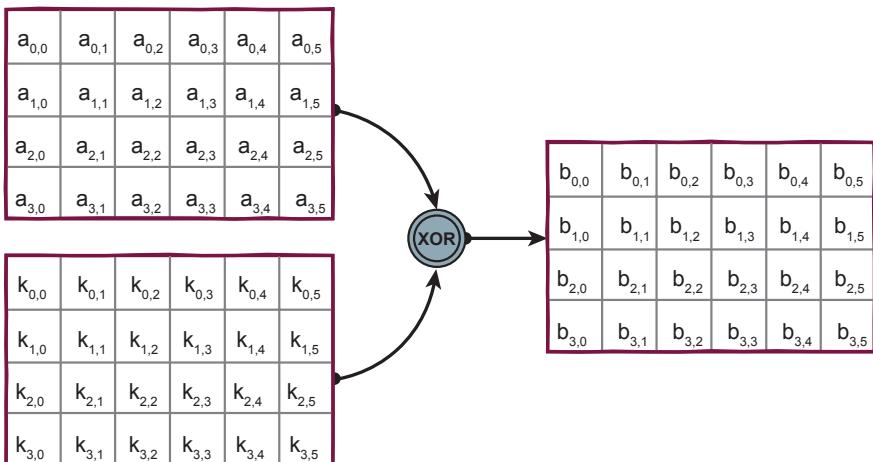
MixColumn-Transformation wird in der letzten Runde von AES überschlagen, und es folgt dann direkt der nächste Schritt.

In der abschließenden AddRoundKey-Transformation wird der aus dem geheimen Schlüssel ermittelte Rundenschlüssel mit dem Array durch ein bitweises XOR verknüpft, siehe Abb. 2.14.

Die in den einzelnen Runden benutzten Rundenschlüssel werden aus dem originalen Schlüssel durch eine sogenannte Expansions-Funktion berechnet. Diese berechnet die Rundenschlüssel mit XOR, zyklischen Shifts und einem Tabellen-Lookup. Dabei wird zum Beispiel ein Puffer der Länge

$$(\text{Blocklänge in Bit}) * (\text{Anzahl der Runden} + 1)$$

gefüllt, dem dann die jeweiligen Rundenschlüssel entnommen werden. Die ersten  $n$  Bit ( $n = \text{verwendete Schlüssellänge}$ ) des Puffers entsprechen dem Schlüssel in



**Abb. 2.14** AddRoundKey-Transformation

unverfälschter Form, alle anderen jeweils  $n$  Bit entstehen aus den vorherigen durch zyklische Permutation und eine Substitution, die der Byte-Sub-Transformation ähnelt. Vor Beginn der ersten Runde erfolgt eine initiale AddRoundKey-Transformation, die den Klartext mit dem ersten Rundenschlüssel verknüpft. Die Entschlüsselung erfolgt analog zur Verschlüsselung mit den jeweiligen inversen Funktionen.

Insgesamt kombiniert der AES-Algorithmus also eine Reihe von Elementarverschlüsselungen in besonders geschickter Anordnung. Die relative Einfachheit macht das Verfahren besonders schnell und flexibel, sodass es zurzeit keine echte Alternative gibt. Ohne die Kombination dieser Verfahren wäre AES nicht sicher. Jedes Verfahren steuert zur Sicherheit von AES bei. Ohne die Key Expansion würden beispielsweise alle Runden denselben Schlüssel  $k$  verwenden und AES wäre gegen Slide-Angriffe verwundbar. SubBytes sorgt für nicht lineare Eigenschaften von AES, wodurch es kryptografische Stärke erhält.

Als Verschlüsselungs-Standard wird der AES-Algorithmus heute in nahezu allen Anwendungen für die Verschlüsselung verwendet.

### Statistische Eigenschaften von Verschlüsselungsverfahren

**Lawineneffekt bei kryptografischen Verfahren** Als Lawineneffekt wird in der Kryptografie die Eigenschaft eines kryptografischen Verfahrens bezeichnet, durch die Änderungen im Klartext oder im Schlüssel große Änderungen im Schlüsseltext hervorrufen und somit einen lawinenartigen Vorgang auslösen. Wenn die Eingabe auch nur geringfügig, zum Beispiel ein Bit, geändert wird, soll sich jedes Ausgabebit mit der Wahrscheinlichkeit von 50 % ändern. Diese Eigenschaft müssen alle kryptografischen Verfahren besitzen!

**Sehr hohe Entropie im Schlüsseltext** Jeder Schlüsseltext hat nach der Verschlüsselung eine sehr hohe Entropie, wie echte Zufallszahlen. Die Entropie ist das Maß für den Informationsgehalt und Zufälligkeit einer Information (Schlüsseltext). Besitzt eine Information einen vollkommen zufälligen Inhalt und nutzt die volle Bandbreite eines Informationsraumes aus, beträgt die Entropie 1. Gibt es aber innerhalb einer Information statistische Regelmäßigkeiten, Wiederholungen oder gar fest definierte Bestandteile, wird die Entropie kleiner und geht bis auf 0, wenn eine Information überhaupt keine zufälligen Bestandteile mehr besitzt. Wenn ein Klartext verschlüsselt wird, hat der Schlüsseltext immer eine sehr hohe Entropie. Damit kann auch relativ einfach ein verschlüsselter Text – der Schlüsseltext – gefunden werden. Dieses Kriterium ist aber nicht eindeutig, da auch komprimierter Text oder Zufallszahlen diese Eigenschaft haben.

Aus diesem Grund müssen Klartexte immer zuerst komprimiert und dann verschlüsselt werden. Zufallszahlen können nicht komprimiert werden, da sie keine Redundanz besitzen!

**Wichtig** Den Klartext immer erst komprimieren und dann verschlüsseln.

Indirekter Angriff	Beschreibung
	<p>Wenn das kryptografische Verfahren sicher ist und eine hohe Wirkung hat, versuchen Angreifer zum Beispiel bei der Verwaltung der Schlüssel anzugreifen. Der Angreifer versucht, an den Schlüssel zu gelangen und damit eine Entschlüsselung durchzuführen. Angriffspunkte sind: Schlüssel- und Zufallszahlengenerierung, Speicherung von Schlüsseln, Schlüsselwechsel und Schlüsselverteilung.</p> <p>Aus diesem Grund muss die Verwaltung der Schlüssel auch sehr sicher umgesetzt werden, um insgesamt eine hohe Wirkung der kryptografischen Verfahren erzielen zu können</p>

### 2.1.17 Verwaltung von Schlüsseln (Key Management)

Komplexere Anforderungen als an die Verschlüsselungsverfahren selbst werden an die Verwaltung der benötigten Schlüssel gestellt. Komplexer deshalb, weil an dieser Stelle des Verfahrens der „Unsicherheitsfaktor Mensch“ ins Spiel kommt: Erzeugung, Speicherung, Wechsel und Verteilung von Schlüsseln sind meist entweder Sache des Anwenders oder werden zumindest von diesem angestoßen. In jedem Stadium dieses Zyklus lauern bestimmte Gefahren. Wenn das Verschlüsselungsverfahren sicher ist, versuchen die Angreifer, bei der Verwaltung der Schlüssel anzugreifen, siehe Abb. 2.15.

**Wichtig** Höhere Anforderungen als an die Verschlüsselungsverfahren werden an Erzeugung, Speicherung, Wechsel und Verteilung der benötigten Schlüssel gestellt.

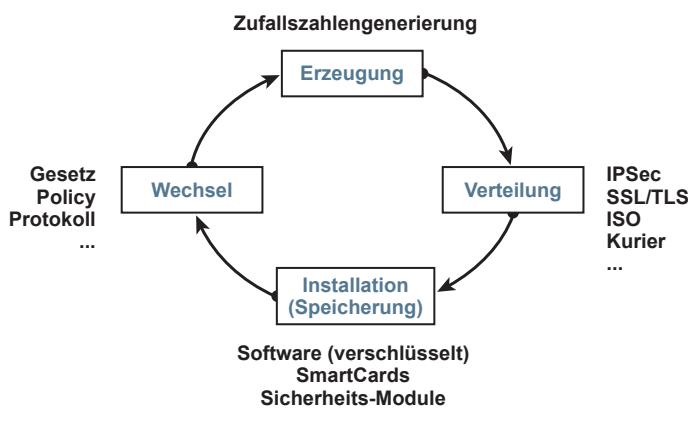


Abb. 2.15 Lebenslauf eines Schlüssels

**Zufallszahlengenerierung** Bei der Erzeugung des Schlüssels besteht das Risiko, dass der Nutzer einen zu einfachen Schlüssel wählt. Wird zum Beispiel der eigene Vorname als Schlüssel verwendet, können selbst ungeübte Angreifer dies leicht erraten. Aus diesem Grund sollten die Schlüssel immer mithilfe von echten Zufallszahlengeneratoren berechnet und der vollständige Schlüsselraum ausgenutzt werden. Darüber hinaus sind Aspekte wie Streuung, Periodizität und Gleichverteilung zu beachten.

**Schlüsselverteilung** Das schwierigste und daher wichtigste Problem jedoch besteht in der Verteilung des oder der Schlüssel an mögliche Kommunikationspartner. Sind Anwendungen mit höchsten Sicherheitsanforderungen betroffen, wird dafür selbst heute oft noch ein vertrauenswürdiger Bote eingesetzt, der den auf einem physikalischen Medium (Papier oder Datenträger) fixierten Schlüssel vom Ort der Erzeugung zu den Einsatzorten bringt, siehe Abb. 2.9.

Speziell in sehr großen Umgebungen erfordert dies jedoch einen kaum vertretbaren Zeit- und Geldaufwand. Zudem ist selbst bei dieser Methode weder theoretisch noch praktisch auszuschließen, dass der Schlüssel bei der Übermittlung in die Hände Unbefugter gelangt – wodurch automatisch das gesamte Verfahren ausgehebelt wird. Daher sind für diese Zwecke unterschiedliche Key-Management-Protokolle entwickelt worden, die sich ihrerseits wiederum eigener, asymmetrischer Verschlüsselungsverfahren bedienen (siehe Abschn. 2.2 „Asymmetrische Verschlüsselungsverfahren“).

**Sichere Speicherung von Schlüsseln** Auch die Schlüsselverwahrung- und Speicherung ist nicht ganz trivial: Schlüssel sind als Zufallszahlen aufgrund ihrer Entropie-Eigenschaft leicht im Speicherbereich eines IT-Systems aufzufinden. Daher sind sie selbst zusätzlich durch eine Verschlüsselung zu schützen oder, besser noch, in einer Sicherheitsumgebung zu verwahren. Dabei haben sich Hardware-Sicherheitsmodule (HSMs) wie Smartcards, USB-Token, TPMs und High-Level-Sicherheitsmodule bewährt (siehe Kap. 3). Der geheime Schlüssel wird auf ihnen gespeichert und verlässt zu keiner Zeit die sichere Umgebung. Zugriff hat nur der legitime Nutzer, der sich gewöhnlich zusätzlich durch PIN-Eingabe authentifiziert. Die Hardware-Sicherheitsmodule enthalten neben den Schlüsseln auch die Algorithmen, die für die Verschlüsselungsoperationen benötigt werden. Auch wenn die Angreifer keinen direkten Zugriff auf den Schlüssel haben, muss zusätzlich verhindert werden, dass die Schlüssel von Angreifern im HSM unberechtigt verwendet werden können.

**Schlüsselwechsel** Damit ein eingesetztes Kryptoeverfahren auch sicher bleibt, ist zudem von Zeit zu Zeit ein Schlüsselwechsel erforderlich. Wie häufig dieser erfolgt, hängt vom Einsatzzweck beziehungsweise der Anwendung und der Umgebung ab – von täglich bis einmal im Jahr ist alles denkbar. Festgelegt wird dieser Zeitraum in einer eigenen Policy, die im laufenden Management- und Sicherheitsprozess zu erarbeiten und regelmäßig an die Bedürfnisse des Anwenders anzupassen ist, siehe zum Beispiel auch Kap. 10 „IPSec-Verschlüsselung“.

## Blockverschlüsselung/Mode of Operation

Das Verschlüsselungsverfahren AES gehört zur Familie der Blockverschlüsselung, bei dem in einem Ver- beziehungsweise Entschlüsselungsvorgang jeweils ein ganzer Block von 128/192/256 Bits (AES) verändert wird.

Diese Blockverschlüsselungs-Algorithmen können in verschiedenen Betriebsarten oder Modes of Operation ausgeführt werden.

Die verschiedenen Betriebsarten bieten eine unterschiedliche Sicherheit sowie verschiedene Eigenschaften, die auf der anderen Seite aber auch verschiedenen Aufwand erforderlich macht.

Im Folgenden werden die sechs verschiedenen Betriebsarten beschrieben:

- ECB-Mode (Electronic Code Book Mode)
- CBC-Mode (Cipher Block Chaining Mode)
- CFB-Mode (Cipher Feedback Mode)
- OFB-Mode (Output Feedback Mode)
- CTR-Mode (Counter Mode Mode)
- GCM-Mode (Galois/Counter Mode).

### 2.1.18 Betriebsart: Electronic Code Book Mode (ECB-Mode)

Der ECB-Mode stellt die Standardverschlüsselung dar, die jeweils auf einem Block zum Beispiel von  $n$  Bits (Länge des Blockes) operiert und diesen unabhängig von anderen Blöcken verschlüsselt. Die Nachricht wird in  $n$ -Bit Blöcke (zum Beispiel  $n=256$  Bit) zerlegt, die dann einzeln hintereinander verschlüsselt werden, siehe Abb. 2.16.

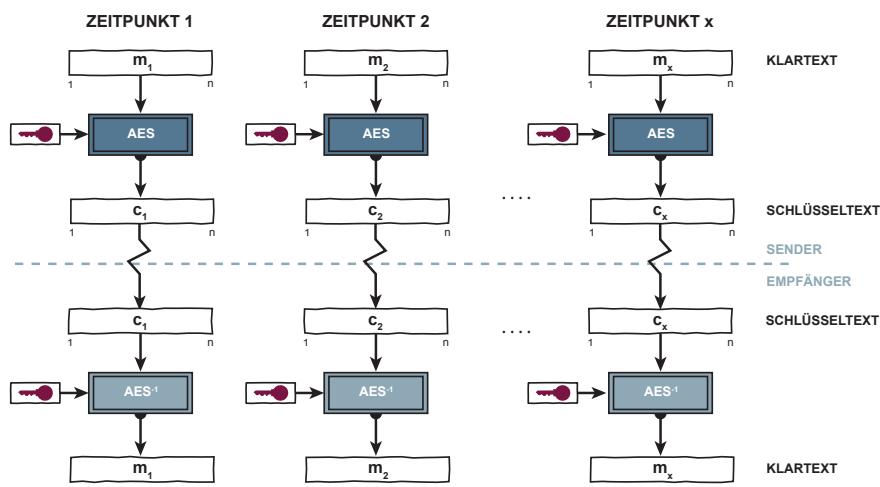


Abb. 2.16 Electronic Code Book Mode (ECB-Mode)

### Eigenschaften des ECB-Modes

Falls innerhalb einer Klartext-Nachricht ein gleicher n-Bit Klartext-Block  $m_x$  auftritt, ergibt dies auch einen gleichen n-Bit Schlüsseltext-Block  $c_x$ . Aufgrund dieser Eigenschaft ist die ECB-Betriebsart nur für spezielle Anwendungen sinnvoll, bei denen Wiederholungen oder häufig auftretende Folgen nicht vorkommen.

Falls die Blockgrenze zwischen Ver- und Entschlüsselung verloren geht (zum Beispiel durch den Verlust eines Bits), so geht die Synchronisation zwischen Verbeziehungsweise Entschlüsselung verloren, bis die richtige Blockgrenze wiederhergestellt wird. Die Ergebnisse aller Entschlüsselungsoperationen sind dann fehlerhaft.

**Wichtig** Beim ECB-Mode führen identische Klartext-Blöcke innerhalb einer Nachricht zu gleichen Schlüsseltext-Blöcken.

### 2.1.19 Betriebsart: Cipher Block Chaining Mode (CBC-Mode)

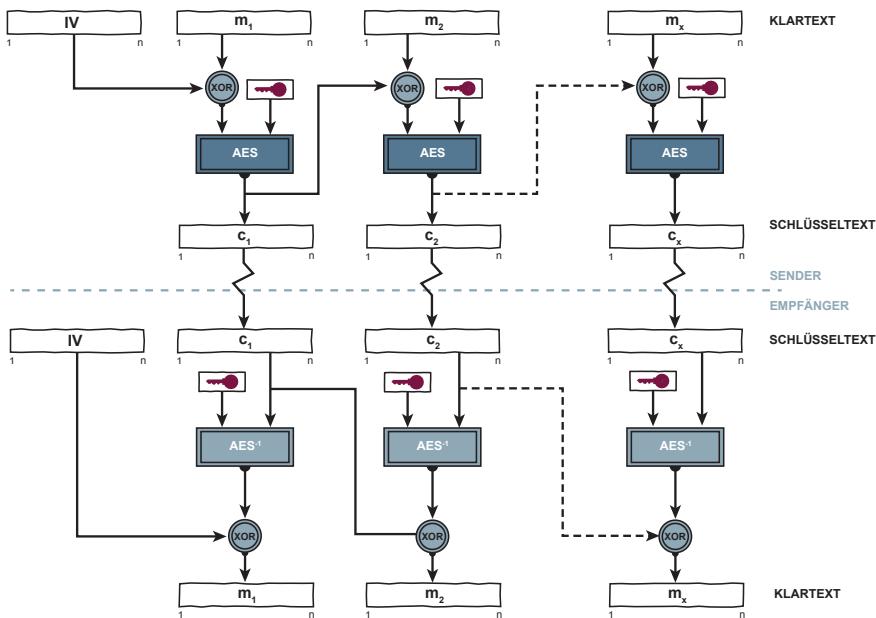
Der Cipher Block Chaining Mode verschlüsselt einen Block, der vor der Verschlüsselung jeweils mit dem verschlüsselten Vorgängerblock mithilfe einer XOR-Operation verknüpft wird. Diese Art der Verschlüsselung heißt Blockverkettung. Dies erfordert für den ersten Klartext-Block einer Nachricht  $m_1$  einen bei Sender und Empfänger verfügbaren Startwert oder Initialisierungsvektor (IV). Der Initialisierungsvektor, oder auch „nonce“ (von dem englischen „for the nonce“ = „für dieses eine Mal“) ist meist eine Zufallszahl oder ein Zeitstempel, der nur einmal genutzt werden sollte, siehe Abb. 2.17.

### Eigenschaften des CBC-Mode

Der CBC-Mode erzeugt denselben Schlüsseltext, wenn derselbe Klartext mit gleichem Schlüssel und Initialisierungswert verschlüsselt wird. Mithilfe eines variablen Initialisierungsvektors oder ausgetauschten Zufallszahlen kann dieses verhindert werden.

Identische Klartext-Blöcke innerhalb einer Klartext-Nachricht führen zu verschiedenen Schlüsseltext-Blöcken (Blockverkettung). Dies verhindert „Known-Plain-Text“-Angriffe.

Beim CBC-Mode beeinflussen ein oder mehrere Bitfehler in einem einzigen Schlüsseltext-Block die Entschlüsselung von zwei Blöcken, und zwar in dem Block, in dem der Fehler auftritt und in den folgenden Blöcken. Wenn die Fehler im i-ten Schlüsseltextblock auftreten, beträgt die durchschnittliche Bitfehlerrate im i-ten Klartextblock 50 %. Im (i+1)-ten Klartextblock sind nur die Bitfehlerhaft, die direkt den fehlerhaften Bitpositionen im i-ten Schlüsseltext-Block entsprechen.



**Abb. 2.17** Cipher Block Chaining Mode (CBC-Mode)

Wie bei dem ECB-Mode: Falls die Blockgrenze verloren geht, geht auch die Synchronisation verloren, bis die richtige Blockgrenze wiederhergestellt wird. Die Ergebnisse aller Entschlüsselungsoperationen sind dann fehlerhaft.

**Wichtig** Beim CBC-Mode führen identische Klartext-Blöcke innerhalb einer Nachricht zu verschiedenen Schlüsseltext-Blöcken (Blockverkettung).

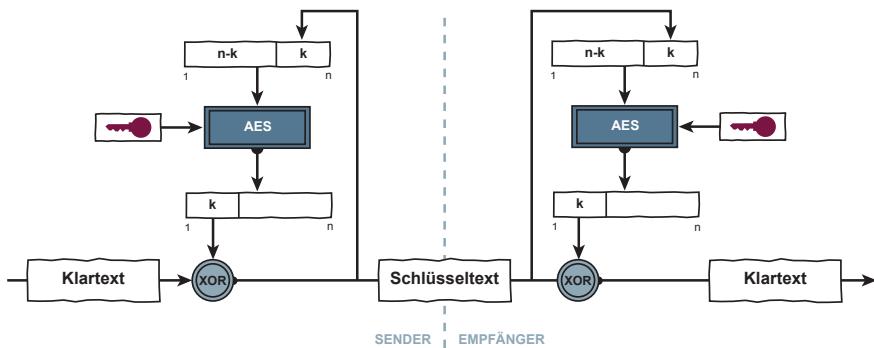
### 2.1.20 Betriebsart: Cipher Feedback Mode (CFB-Mode)

Eine Methode, eine Folge von Zeichen oder Bits einzeln zu verschlüsseln, ist der Cipher Feedback Mode. Durch die Betriebsart wird eine Blockverschlüsselung zu einer kontinuierlichen Verschlüsselung, die auf Klartexteinheiten  $k$ -Bit Länge operiert.

Sowohl sender- als auch empfängerseitig arbeitet die Blockverschlüsselung im Verschlüsselungsmodus und erzeugt eine pseudozufällige Bitfolge, die modulo 2 (XOR) zu dem Klartextzeichen beziehungsweise empfängerseitig zu den Schlüsseltextzeichen addiert wird.

Zu Beginn einer Verschlüsselung muss der Input der Blockverschlüsselung mit einem Initialisierungsvektor sender- und empfängerseitig geladen werden.

Für jedes zu verschlüsselnde Zeichen ist eine Blockverschlüsselung erforderlich, sodass diese Betriebsart bei einem kleinen  $k$  nicht so effizient ist. Ist  $k$  gleich 1, muss für jedes Bit die Blockverschlüsselung umgesetzt werden, siehe Abb. 2.18.



**Abb. 2.18** Cipher Feedback Mode (CFB-Mode)

### Eigenschaften des CFB-Modes

Beim CFB-Mode beeinflussen Fehler in einem  $k$ -Bit-Block des Schlüsseltextes die Entschlüsselung des unmittelbaren verstümmelten und des folgenden Schlüsseltextes so lange, bis die fehlerbehafteten Bits aus dem CFB-Eingabeblock herausgeschoben sind.

Der erste betroffene  $k$ -Bit-Block des Klartextes ist in genau den Bitpositionen fehlerhaft, in denen der Schlüsseltext fehlerhaft ist. Der nachfolgende entschlüsselte Klartext hat eine durchschnittliche Bitfehlerrate von 50 %, und zwar so lange, bis alle Fehler aus dem Eingangsblock herausgeschoben sind.

Sind bis dahin keine zusätzlichen Fehler aufgetreten, so erscheint danach wieder der richtige Klartext. Diese Eigenschaft wird mit „begrenzte Fehlerfortpflanzung“ oder mit „Selbstsynchronisation“ bezeichnet.

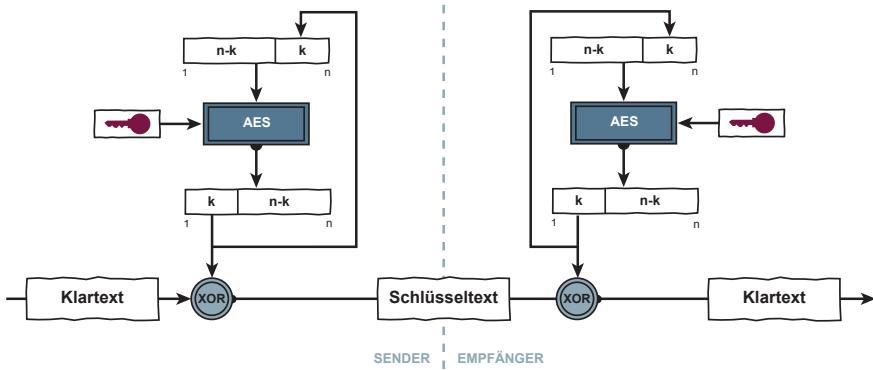
Wenn die Grenzen der  $k$ -Bit-Blöcke während der Entschlüsselung verloren gehen, so geht auch die kryptografische Synchronisation verloren, bis eine erneute Initialisierung (Reinitialisierung) durchgeführt wird.

Nach Wiederherstellung der richtigen Grenzen der  $k$ -Bit-Blöcke sind höchstens noch die folgenden  $n$ -Bit fehlerhaft.

**Wichtig** Der CFB-Mode ermöglicht eine begrenzte Fehlerfortpflanzung und kann sich selbst synchronisieren.

### 2.1.21 Betriebsart: Output Feedback Mode (OFB-Mode)

Der Output Feedback Mode arbeitet ähnlich wie der CFB-Mode, nur mit dem Unterschied, dass hier nicht das Schlüsseltextzeichen, sondern das Outputzeichen der Blockverschlüsselung in das Inputregister zurückgeführt wird, siehe Abb. 2.19.



**Abb. 2.19** Output Feedback Mode (OFB-Mode)

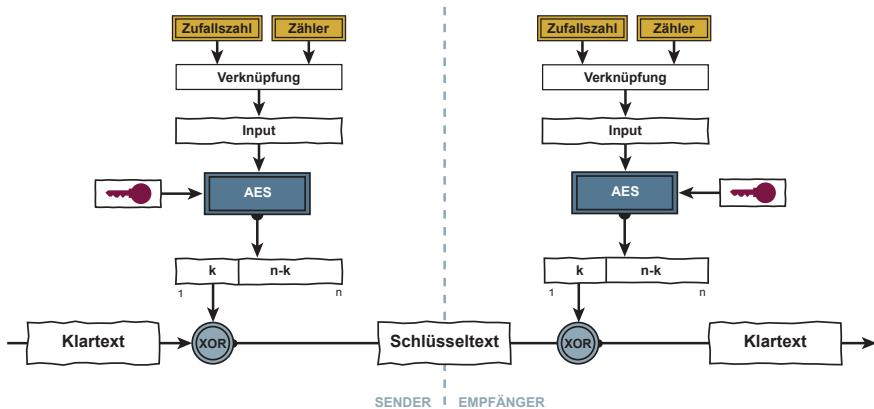
### Eigenschaften des OFB-Mode

Der OFB-Mode führt zur keiner Fehlerfortpflanzung in der resultierenden Klartextausgabe. Ein fehlerhaftes Bit im Schlüsseltext hat nur ein fehlerhaftes Bit im entschlüsselten Klartext zur Folge. Der OFB-Mode ist nicht selbst-synchronisierend. Wenn die beiden Operationen Verschlüsselung und Entschlüsselung aus der Synchronisation geraten, muss das System wieder neu initialisiert werden. Eine Re-Initialisierung kann mit einem neuen Startwert bei gleichem Schlüssel durchgeführt werden.

**Wichtig** Der OFB-Mode ist für störungsanfällige Übertragungswege wie Satellitenverbindungen gedacht, bei denen eine Fehlerfortpflanzung nicht erwünscht ist.

### 2.1.22 Betriebsart: Counter Mode (CTR-Mode)

Mithilfe des Counter Modes kann wie beim CFB- und OFB-Mode eine Blockverschlüsselung zu einer kontinuierlichen Verschlüsselung, die auf Klartexteinheiten  $k$ -Bit Länge operiert, umgesetzt werden. Bei dieser Betriebsart wird der Input für die Verschlüsselung aus einer Zufallszahl  $r$  und einem Zähler  $c$  verknüpft. Die Verknüpfung kann durch die Konkatenation, Addition oder XOR-Operation erfolgen, siehe Abb. 2.20.



**Abb. 2.20** Counter Mode (CTR-Mode)

### Eigenschaften des CTR-Mode

Ein fehlerhaftes Bit im Schlüsseltext hat nur ein fehlerhaftes Bit im entschlüsselten Klartext zur Folge.

Wie beim OFB-Mode, wenn die beiden Operationen Verschlüsselung und Entschlüsselung aus der Synchronisation geraten, muss das System wieder neu initialisiert werden.

Der besondere Vorteil des CTR-Mode ist der wahlfreie Zugriff auf jeden verschlüsselten Block und die Möglichkeit, sämtliche Ver- und Entschlüsselungsoperationen parallel durchzuführen.

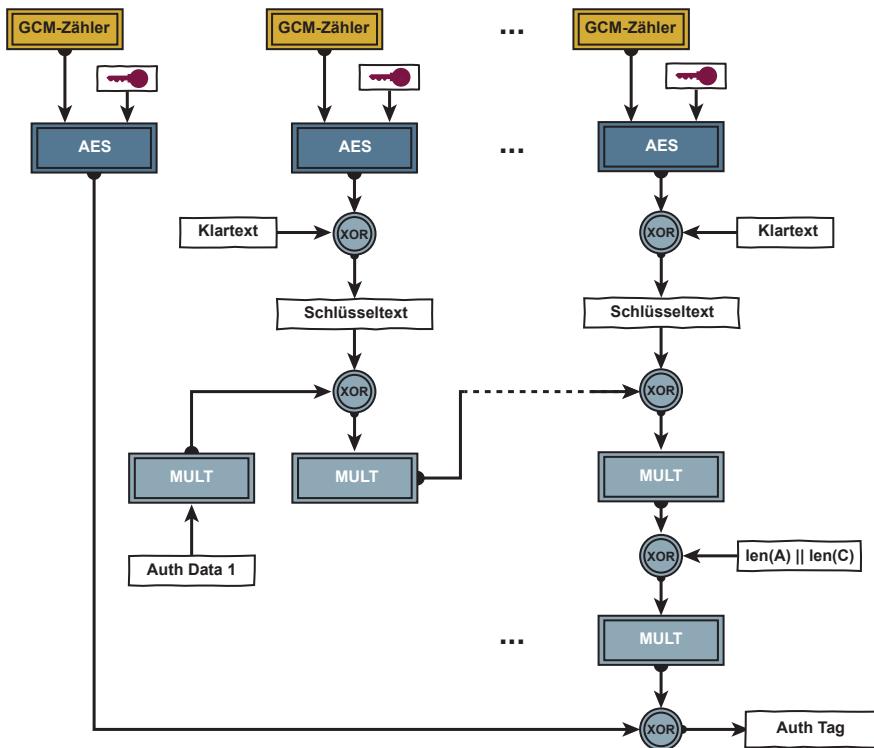
**Wichtig** Der CTR-Mode ist besonders geeignet für Massen-Daten wie Festplatten und ZIP-Archive.

### 2.1.23 Betriebsart: Galois/Counter Mode (GCM-Mode)

Der GCM-Mode gehört zu der Kategorie Authenticated Encryption with Associated Data (AEAD), bei der neben der eigentlichen Verschlüsselung auch Daten authentisiert werden können. Beim GCM-Mode wird als Input für die Verschlüsselung ein eindeutiger Zähler verwendet. Die Blockgröße ist auf 128 Bit festgelegt.

### Eigenschaften des GCM-Mode

Der GCM-Mode hat einen hohen Durchsatz und eignet sich zur parallelen Verarbeitung. Daher ist der GCM-Mode bei der Echtzeitverschlüsselung von Kommunikationsdaten und Festplattenverschlüsselung im Einsatz. Der GCM-Zähler wird in jedem Schritt erhöht. In der Darstellung bezeichnet „MULT“ die Multiplikation im Galoiskörper GF(2<sup>128</sup>). In der NIST Special Publication 800-38D wird die zugehörige Funktion als GHASH bezeichnet. len(A): 64-bit ist die



**Abb. 2.21** Galois/Counter Mode (GCM-Mode)

Repräsentation der Bit-Länge der Authentifizierten Daten und  $\text{len}(C)$ : 64-bit ist die Repräsentation der Bit-Länge der verschlüsselten Daten, siehe Abb. 2.21.

Wird der Schlüsseltext nicht genutzt, reduziert sich der GCM-Mode auf die Authentifizierung der Klartextdaten und wird GMAC (Galois Message Authentication Code) genannt.

**Wichtig** Der GCM-Mode kombiniert die Verschlüsselung mit der Authentifizierung der Daten und ist geeignet für die parallele Verarbeitung.

#### 2.1.24 Modes of Operation: Zusammenfassung

Über die Auswahl des Modes of Operation wird in Abhängigkeit von Performance, die benötigt wird und vorhanden ist (Software/Hardware), der Fehlerfortpflanzung, die gewünscht oder ungewünscht ist und der Selbstsynch�onisation, die eventuell notwendig ist, entschieden.

Diese Anforderungen können unterschiedlich sein bezogen auf die Kommunikationsebene, auf der verschlüsselt werden soll (Schicht 1 bis 7 OSI-Kommunikationsmodells) sowie auf die Qualität des Übertragungskanals.

Die Modes of Operation werden typischerweise schon in den entsprechenden Standards festgelegt.

<b>Standards</b>	<b>Modes of Operation</b>
WinZip	CTR-Mode
TLS 1.2	CTR-Mode, GCM-Mode
IPSec	GCM-Mode
TLS/SSL	GCM-Mode
IEEE 802.11ad	GCM-Mode
SSH	GCM-Mode

### **Anwendungen von symmetrischen Verschlüsselungsverfahren**

Symmetrische Verschlüsselungsverfahren werden überwiegend für die Erreichung des Cyber-Sicherheitsbedürfnisses Vertraulichkeit verwendet.

Die Anwendungsfelder sind vielfältig:

- E-Mail-Verschlüsselung (zum Beispiel bei S/MIME, PGP, ...)
- Datenverschlüsselung innerhalb von Netzwerken (zum Beispiel bei IPSec, TLS/SSL, ...)
- Datei-, Verzeichnis- oder Plattenverschlüsselung
- Anwendungen (ec-Cash, Streaming usw.)

### **Nachteil von symmetrischen Verschlüsselungsverfahren**

Ein Nachteil von symmetrischen Verschlüsselungsverfahren ist, dass bei der Kommunikationsverschlüsselung beide Kommunikationspartner den gleichen geheimen Schlüssel nutzen. Dieser geheime Schlüssel muss gesichert zwischen den Kommunikationspartnern ausgetauscht werden, was sehr aufwendig sein kann, zum Beispiel mithilfe eines vertrauenswürdigen Boten. Erschwerend kommt hinzu, dass dieser geheime Schlüssel regelmäßig gewechselt werden muss.

Eine weitere Herausforderung ist, dass bei n verschiedenen Kommunikationspartnern

$$n*(n - 1)/2$$

verschiedene Schlüssel benötigt werden.

Das sind zum Beispiel bei 12 Partnern 66 Schlüssel und bei 1.000 Partnern 499.500 Schlüssel.

Dieser Nachteil wird mithilfe von asymmetrischen Verschlüsselungsverfahren kompensiert.

## Steganografie

In diesem Abschnitt wird die Kryptografie von der Steganografie abgegrenzt.

Bei der Kryptografie werden Klartext-Daten für alle unberechtigten Dritte durch die Verschlüsselung unverständlich gemacht, aber offen als Schlüsseltext übermittelt oder gespeichert.

Die Steganografie ist die Wissenschaft der verborgenen Speicherung oder Übermittlung von vertraulichen Daten.

Wie bei der Kryptografie soll mithilfe der Steganografie Vertraulichkeit erzielt werden.

Anders als bei der Kryptografie, bei der ein unberechtigter Dritter von der Existenz von Klartext-Daten weiß, aber aufgrund der Verschlüsselung nicht in der Lage ist, die Klartext-Daten aus dem Schlüsseltext zu extrahieren, werden bei der Steganografie die Daten im Klartext gelassen, aber so „versteckt“, dass ein unberechtigter Dritter diese nicht identifizieren und damit nicht lesen kann.

Da mithilfe der Protokollerkennung von Verschlüsselungsstandards, wie IPSec, TLS/SSL usw., oder der Entropie des Schlüsseltextes die Verschlüsselung identifiziert und damit die Nutzung verhindert werden kann, ist es mit der Steganografie möglich, eine vertrauliche Übertragung zu ermöglichen, die nicht identifiziert werden kann.

Klassische Beispiele der Steganografie sind: Unsichtbare Tinte, Mikrofilm, Semagramme: Informationen in Bildern verstecken, verdeckte Kommunikationskanäle usw.

Moderne Beispiele der Steganografie sind: Verstecken von Bits in Textdateien, Bilddateien, Audiodateien, Videokonferenzen usw.

Abb. 2.22 zeigt ein Beispiel von Steganografie. Die schmalen Stangen stellen einen Text im Morsealphabet dar.

Erste Zeichen „kurz, kurz, kurz“=S, das zweite Zeichen „kurz“=E, das dritte „lang, kurz, lang, kurz“=C, das vierte „kurz, kurz, lang“=U, das fünfte „kurz, lang, kurz“=R und das sechste „kurz, kurz“=I, das siebte „lang“=T und acht „lang, kurz, lang, lang“=Y.

Insgesamt steht dort „SECURITY“.



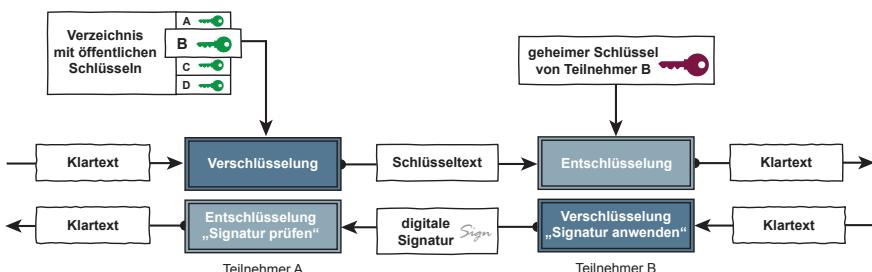
**Abb. 2.22** Steganografie

## 2.2 Asymmetrische Verschlüsselungsverfahren

Um das klassische Problem der Kryptografie, die Schlüsselverteilung, zu erleichtern, wurden Verfahren entwickelt, die mit sogenannten *öffentlichen Schlüsseln* oder *Public-Keys* arbeiten. Das wichtigste Kennzeichen asymmetrischer Verschlüsselungsverfahren ist, dass die Kommunikationspartner dabei, anstelle eines einzelnen geheimen Schlüssels, zwei verschiedene, aber trotzdem zusammengehörige Schlüssel nutzen [4]. Von diesen ist einer öffentlich bekannt, der sogenannte *Public Key*, und kann von einem beliebigen Absender zur Verschlüsselung einer Klartext-Nachricht verwendet werden. Anders als bei der symmetrischen Verschlüsselung ist es aber nicht möglich, den Klartext mit diesem öffentlichen Schlüssel zu entschlüsseln. Dazu benötigt der Empfänger einen zweiten Schlüssel, den nur er allein kennt, den sogenannten *Private Key* oder geheimen Schlüssel. Damit dieses Verfahren auch wirklich sicher funktioniert, darf der geheime Schlüssel nicht aus dem öffentlichen Schlüssel ableitbar sein. Auch muss das Verfahren Angriffen mithilfe der Known-Plaintext- beziehungsweise Chosen-Plaintext-Methode widerstehen. Erfüllt das Public-Key-Verfahren beide Bedingungen, gibt es keinen Grund mehr, den Schlüssel für die Verschlüsselung geheim zu halten.

Verfahren mit zwei unterschiedlichen Schlüsseln, die nicht voneinander ableitbar sind, werden als Public-Key-Verfahren gekennzeichnet. Der Schlüssel zur Verschlüsselung wird als *öffentlicher Schlüssel* bezeichnet und der Schlüssel zur Entschlüsselung *privater* oder *geheimer Schlüssel* genannt.

Will Alice (A) eine vertrauliche Nachricht an Bob (B) senden, so entnimmt sie den öffentlichen Schlüssel von B einem Verzeichnis mit öffentlichen Schlüsseln, verschlüsselt den Klartext damit und sendet diesen als Schlüsseltext an B. Da nur B den zugehörigen geheimen Schlüssel kennt, und da dieser Schlüssel weder aus dem öffentlichen Schlüssel noch aus der verschlüsselten Nachricht, dem Schlüsseltext, bestimmt werden kann, ist B tatsächlich der Einzige, der den Schlüsseltext wieder zum Klartext entschlüsseln kann. Damit ist also eine sichere Kommunikation möglich, ohne dass dazu vorher eine geheime Schlüsselübermittlung zwischen A und B oder von dritter Seite an beide notwendig wäre, siehe Abb. 2.23.



**Abb. 2.23** Prinzip der asymmetrischen Verschlüsselung

**Wichtig** Alle asymmetrischen Verschlüsselungsverfahren arbeiten mit einem Schlüsselpaar, dem öffentlichen und dem geheimen Schlüssel.

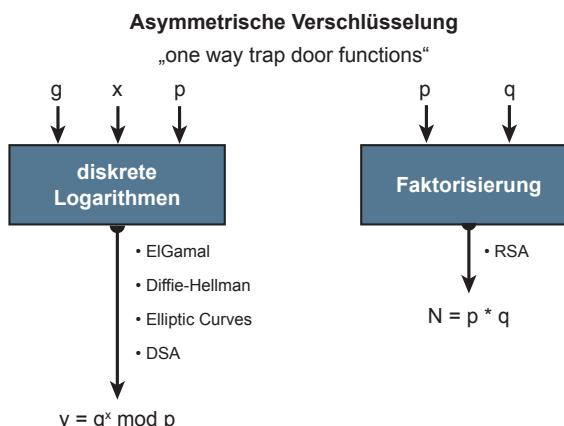
### Einwegfunktionen mit Parameter

Beide Bedingungen – der geheime Schlüssel darf nicht aus dem öffentlichen Schlüssel ableitbar sein und das Verfahren muss der Chosen-Plaintext-Methode widerstehen – sind allerdings nicht so einfach einzuhalten. Das liegt zum einen daran, dass der geheime Schlüssel vom Prinzip her immer aus dem öffentlichen Schlüssel ableitbar ist, da zwischen beiden eine mathematische Relation besteht. Daher werden für Public-Key-Verfahren Algorithmen gewählt, die auf der Lösung von schweren Problemen der Komplexitätstheorie beruhen. Idealerweise handelt es sich um Funktionen, bei denen die Verschlüsselung „leicht“ zu berechnen, aber die Entschlüsselung ohne den geheimen Schlüssel unendlich komplex, das heißt praktisch „unmöglich“ ist. Die Begriffe „leicht“ und „unmöglich“ sollen den rechnerischen Aufwand beschreiben und hängen somit vom Entwicklungsstand der jeweiligen Computergeneration ab.

Ein einfaches Beispiel hierfür ist die Primzahlenzerlegung. Es ist leicht, die Primzahlen 1237 und 2251 zu multiplizieren. Hingegen ist die Frage: „Welche beiden Primzahlen ergeben multipliziert die Zahl 2.100.457?“ deutlich schwerer zu bestimmen. Grundlegend basiert die Sicherheit des bereits genannten RSA-Verfahrens auf dieser Fragestellung. Die beiden Primzahlen sind 1627 und 1291.

Die Lösung von schweren Problemen der Komplexitätstheorie ist zum Beispiel bei Exponentialfunktionen und diskreten Logarithmen oder dem Problem der Faktorisierung von Produkten zweier großer Primzahlen der Fall, siehe Abb. 2.24.

Derartige Funktionen werden auch als One-Way- oder Einwegfunktionen bezeichnet. Die dabei eingesetzten Schlüssel sind insgesamt deutlich länger als bei symmetrischen Verschlüsselungsverfahren.



**Abb. 2.24** Einwegfunktionen der asymmetrischen Verschlüsselung

Ein besonderer Fall ist gegeben, wenn für die benutzte Einwegfunktion ein Parameter beziehungsweise Schlüssel existiert, mit dem sich die inverse Transformation „leicht“ berechnen lässt. Derartige Funktionen werden **one-way trap door functions** (Einwegfunktionen mit Falltür oder Hintertür) genannt. Wie der geheime Schlüssel darf auch die „Hintertür“ ausschließlich dem legitimen Nutzer bekannt sein.

Als Analogie kann ein Schnapp-Schloss betrachtet werden, jeder kann die Tür zu schlagen, aber derjenige, der den passenden Schlüssel hat, kann die Tür wieder aufschließen.

### Digitale Signatur

Eine wichtige Anwendung des Public-Key-Verfahrens ist die digitale Signatur. Sie nutzt beide Komponenten – sowohl den öffentlichen als auch den geheimen Schlüssel –, um mit ihrer Hilfe ein elektronisches Äquivalent zur eigenhändigen Unterschrift zu erzeugen, das ebenso rechtsverbindlich und im juristischen Sinn beweiskräftig ist wie eine eigenhändige Unterschrift.

Klartext-Daten, die mit einem bestimmten geheimen Schlüssel „verschlüsselt“ wurden, können nur mithilfe des dazugehörigen öffentlichen Schlüssels wieder „entschlüsselt“ werden.

Hat nun eine Person die Klartext-Daten mit ihrem geheimen Schlüssel digital signiert, kann mithilfe des öffentlichen Schlüssels überprüft werden, ob es wirklich diese Person war, die die Klartext-Daten digital signiert hat. Die erfolgreich durchgeführte Überprüfung der digitalen Signatur ist der Beweis für die Authentizität des Absenders und Integrität der Nachricht, dem Klartext, siehe Abb. 2.23.

Mit dem Prinzip der digitalen Signatur steht somit ein Äquivalent zur eigenhändigen Unterschrift zur Verfügung. Das bekannteste Public-Key-Verfahren, mit dem gleichzeitig signiert und verschlüsselt werden kann, ist der RSA-Algorithmus.

### Authentische Schlüssel

Ein offenes Problem bei Public-Key-Verfahren ist die Frage, wie der öffentliche Schlüssel zum Kommunikationspartner gelangt? Wie kann überprüft werden, dass ein öffentlicher Schlüssel in einem Verzeichnis wirklich der echte ist? Selbst im Fall der Verwendung öffentlicher Schlüssel müssen diese authentisch ausgetauscht werden.

Eine elegante Möglichkeit, öffentliche Schlüssel authentisch auszutauschen, ist die Einrichtung eines Zertifizierungssystems, eines Trustcenters oder einer Public-Key-Infrastruktur. Der öffentliche Schlüssel jedes Nutzers wird von einer Public-Key-Infrastruktur (Zertifizierungssystem) in Form eines „digitalen Zertifikates“ zur Verfügung gestellt, siehe Kap. 4 „Digitale Signatur, elektronische Zertifikate sowie Public Key Infrastruktur (PKI) und PKI-enabled Application (PKA)“.

#### 2.2.1 Das RSA-Verfahren

Das RSA-Verfahren wurde 1978 von Ron Rivest (Massachusetts Institute of Technology – MIT), Adi Shamir (Weizmann-Institut für Wissenschaften) und Leonard Adleman (Stanford University) entwickelt und findet seine Verwendung bei

Verschlüsselung, digitalen Signaturen und beim Key Management. Der Algorithmus basiert auf dem Problem, dass das Produkt zweier großer Primzahlen nur schwer in seine Faktoren zu zerlegen ist. Dazu ein Beispiel: 377 ist das Produkt aus 13 und 29, mit anderen Worten: das Ergebnis der Multiplikation der sechsten mit der zehnten Primzahl. Sind die Primzahlen bekannt beziehungsweise wie hier klein genug, ist die Operation einfach. Werden die Faktoren dagegen hinreichend groß gewählt, kann die Zerlegung eine praktisch unlösbare Aufgabe darstellen, was bedeutet, dass das Verfahren für einen definierten Zeitraum als „sicher“ gelten kann. Kryptografie-Experten empfehlen derzeit eine Länge zwischen 2048 und 3072 Bit in binärer Darstellung für den RSA-Modulus, wobei der erste Wert bis Ende des Jahres 2022 und der zweite darüber hinaus gilt.

### RSA-Schlüsselgenerierung

Um einen Schlüssel nach RSA zu erzeugen, wird zunächst nach zwei großen Primzahlen  $p$  und  $q$  gesucht. Dann wird das Produkt  $n = p \cdot q$  berechnet. Als nächstes wird eine zu  $((p - 1) * (q - 1))$  teilerfremde Zahl  $e$  ausgewählt. Diese bildet mit dem Produkt  $n$  den öffentlichen Schlüssel  $(e, n)$ . Dann wird der erweiterte Euklidische Algorithmus verwendet, um eine Zahl  $d$  zu berechnen, wobei  $e \cdot d \bmod ((p - 1) * (q - 1)) = 1$  gilt. Die Zahl  $d$  ist der geheime Schlüssel, der es ermöglicht, die Trap-Door-Eigenschaften des Verfahrens auszunutzen. Die Qualität des so erstellten Schlüssels und damit die Sicherheit des RSA-Verfahrens hängen von den verwendeten Primzahlen ab.

Es gibt zum Beispiel Faktorisierungsmethoden, die mithilfe der Faktoren in  $p-1$  und  $q-1$  zu viel besseren Ergebnissen kommen.

Aus diesem Grund sollen die Primzahlen für das RSA-Verfahren noch besondere Eigenschaften aufweisen, die mit **starken Primzahlen** bezeichnet werden.

Die Eigenschaften sind für die Primzahlen  $p$  und  $q$ :

- $p$  ist eine große Zahl (zum Beispiel 1500 Bit)
- $p$  ist eine Primzahl (kann sehr unterschiedlich nachgewiesen werden)
- $p$  wurde zufällig ausgewählt (Zufallszahlengenerator)
- $p$  hat eine vorher festgelegte Länge (zum Beispiel zwischen 1480 und 1520 Bit)
- $p - 1$  hat einen großen Primteiler  $r$
- $p + 1$  hat einen großen Primteiler  $s$
- $r - 1$  hat einen großen Primteiler
- $s - 1$  hat einen großen Primteiler

### RSA-Verschlüsselungsvorschrift

Eine Klartextnachricht  $m$  soll in einen Schlüsseltext  $c$  durch Verschlüsselung umgewandelt werden. Aus der Schlüsselgenerierung steht der öffentlichen Schlüssel  $(e, n)$  zur Verfügung, bestehend aus der zu  $((p - 1) * (q - 1))$  teilerfremden Zahl und dem Produkt der Primzahlen  $n$ . Außerdem steht der geheime Schlüssel  $d$  zur Verfügung.

Für die Verschlüsselung wird folgende Berechnung durchgeführt:

$$c = m^e \bmod n.$$

Die Entschlüsselung erfolgt jedenfalls mit der Berechnung von:

$$m = c^d \bmod n.$$

**Öffentlicher Schlüssel** (ÖS) ist das Zahlenpaar (**e**, **n**)

**Geheimer Schlüssel** (GS) ist die Nummer **d**

### 6-Tupel (**M; C; K<sub>E</sub>; K<sub>D</sub>; E; D**) für das RSA-Verfahren

$$E \quad m^e \bmod n$$

$$D \quad c^d \bmod n$$

$$KE \quad e$$

$$KD \quad d$$

$$M \quad m$$

$$C \quad c$$

Anschaulicher lässt sich diese abstrakte Berechnung anhand eines Beispiels erklären, für das abermals sehr kurze Primzahlen gewählt wurden.

### Beispiel RSA-Verschlüsselung

$$p=61 \quad \text{erste Primzahl}$$

$$q=53 \quad \text{zweite Primzahl}$$

$$n=p*q=3233 \quad \text{Modulus – (Teil des öffentlichen Schlüssels)}$$

$$e=17 \quad \text{öffentlicher Exponent – (Teil des öffentlichen Schlüssels)}$$

$$d=2753 \quad \text{geheimer Exponent – (der geheime private Schlüssel)}$$

$$c=m^{17} \bmod 3233 \quad \text{Verschlüsselungsoperation}$$

$$d=c^{2753} \bmod 3233 \quad \text{Entschlüsselungsoperation}$$

### Aufgabe 1

Verschlüssele die Zahl  $m = 123$

Ergebnis 1

$$c = 123^{17} \bmod 3233 = 337587917446653715596592958817679803 \bmod 3233 = 855$$

### Aufgabe 2

Entschlüssle die Zahl  $c = 855$

Ergebnis 2

$$d = 855^{2753} \bmod 3233 = 5,043288895841606873442289912739e+8071 \bmod 3233 = 123$$

Asymmetrische Verschlüsselungsverfahren sind im Vergleich zu symmetrischen Verfahren leider sehr rechenintensiv, weswegen die Ver- und Entschlüsselung deutlich langsamer vor sich geht. Die verwendeten Algorithmen müssen daher mit Blick auf Rechenleistung und Speicherplatz des verwendeten IT-Systems sowie die zur Verfügung stehende Zeit angepasst werden, um eine effektive Lösung zu realisieren.

### 2.2.2 Das Diffie-Hellman-Verfahren

Das Diffie-Hellman-Verfahren (kurz DH) war der erste Public-Key-Algorithmus und wurde 1976 vorgestellt. Das Verfahren dient jedoch nicht der Verschlüsselung, sondern wurde entwickelt, um geheime Schlüssel (Diffie-Hellman Shared Secret) gesichert über einen unsicheren Kommunikationskanal auszutauschen. Dazu bedienten sich die Autoren Whitfield Diffie und Martin E. Hellman des Problems der diskreten Logarithmen.

#### Das Diffie-Hellman-Verfahren funktioniert folgendermaßen

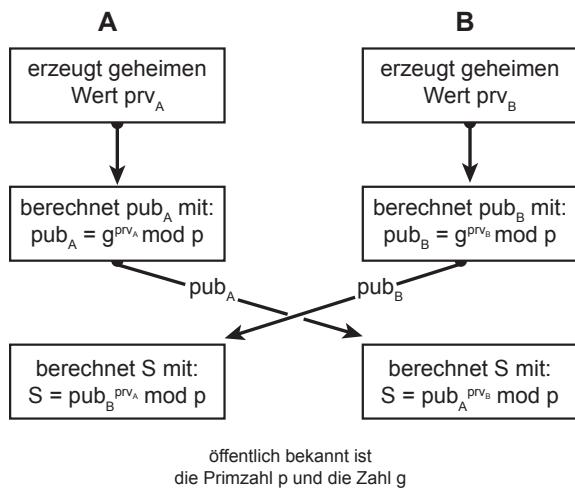
Das Schlüsselpaar des Kommunikationspartners A besteht aus einem geheimem Schlüssel  $prv_A$  und einem öffentlichen Schlüssel  $pub_A$ .  $pub_A$  errechnet sich aus dem geheimen Schlüssel  $prv_A$  mittels der Formel:

$$pub_A = g^{prv_A} \bmod n$$

Jeweils öffentlich bekannt für alle Kommunikationspartner sind  $g$  und  $n$ , wobei  $n$  eine lange Primzahl ist und  $g$  eine zu  $n$  teilerfremde Zufallszahl.

Der Kommunikationspartner B errechnet analog sein Schlüsselpaar mit dem geheimen Schlüssel  $prv_B$  und dem öffentlichen Schlüssel  $pub_B$ . Die Zahlen  $prv_A$  und  $prv_B$  sind jeweils Zufallszahlen. Ziel des Diffie-Hellman-Verfahrens ist die Vereinbarung eines geheimen Schlüssels  $S$  (Diffie-Hellman Shared Secret), ohne dass zuvor Parameter zwischen den Kommunikationspartnern ausgetauscht werden müssen, siehe Abb. 2.25.

**Abb. 2.25** Diffie-Hellman-Verfahren



Die Kommunikationspartner berechnen nun jeweils ihren öffentlichen Schlüssel nach der vorgestellten Formel und schicken diesen an den Partner.

Der gemeinsame Schlüssel S (Diffie-Hellman Shared Secret) errechnet sich dann als

$$s = \text{pub}_B^{\text{prvA}} \bmod p$$

für Kommunikationspartner A und

$$s = \text{pub}_A^{\text{prvB}} \bmod p.$$

für Kommunikationspartner B.

Dabei ist das errechnete S (geheimer Schlüssel – Diffie-Hellman Shared Secret) jeweils identisch. Eingesetzt wird das Diffie-Hellman-Verfahren unter anderem bei SSL/TLS und IPSec.

Auf den ersten Blick scheinen damit alle Schlüsselaustauschprobleme beseitigt. Bei näherer Betrachtung wird allerdings klar, dass auch das Diffie-Hellman-Verfahren eine Schwachstelle hat: Eine Authentifizierung der Kommunikationspartner untereinander wird nicht realisiert, was die Methode anfällig für einen sogenannten Man-in-the-Middle-Angriff macht. Bei dieser Attacke leitet der Angreifer den gesamten Kommunikationsvorgang über sein eigenes IT-System um und sitzt so quasi zwischen seinen Opfern. Der eigentlich zwischen A und B auszuhandelnde Schlüssel S wird also tatsächlich jeweils zwischen den Opfern und dem Angreifer ausgehandelt. Die Authentifikation der Kommunikationspartner muss beim Diffie-Hellman-Verfahren mithilfe weiterer Verfahren umgesetzt werden!

**Wichtig** Das Diffie-Hellman-Verfahren ist kein Verschlüsselungsalgorithmus und es gewährleistet auch keine Authentifizierung der Kommunikationspartner. Es dient dem gesicherten Austausch eines geheimen Schlüssels S über einen unsicheren Kommunikationskanal.

### 2.2.3 Elliptische Kurven

Auf elliptischen Kurven basierende Kryptografie, auch bekannt als EC (Elliptic Curve) beziehungsweise ECC (Elliptic Curve Cryptography), wird als Ersatz für RSA, DSA und Diffie-Hellman-Schlüsselaustausch genutzt. Es sind asymmetrische Kryptosysteme, die Operationen auf elliptischen Kurven über endlichen Körpern verwenden.

Vorteile von elliptischen Kurven sind:

- kürzere Schlüssel (256 Bit statt 2048 Bit)
- schnellere Verarbeitung, da kleinere Schlüssel
- geringerer Speicherbedarf, da kleinere Schlüssel
- schnellere Kommunikation, da kleinere Schlüssel

Elliptische Kurven sind besonders interessant für Smartcards und werden zum Beispiel im deutschen elektronischen Personalausweis verwendet.

## 2.2.4 Hybride Verschlüsselungsverfahren

Die vorgestellten symmetrischen Verfahren sind zwar deutlich schneller und effizienter als asymmetrische Verfahren. Problematisch ist bei ihnen aber das Schlüsselmanagement.

Für den praktischen Einsatz werden daher die positiven Eigenschaften beider Methoden (symmetrisch und asymmetrisch) zu hybriden Verfahren kombiniert. Dabei verschlüsselt ein Absender eine Nachricht zuerst mit einem zufällig erzeugten symmetrischen Schlüssel. Dieser wird in der Regel nur dieses eine Mal verwendet und daher als Sitzungsschlüssel (Session Key) bezeichnet. Um den Sitzungsschlüssel sicher an den Kommunikationspartner zu übermitteln, nutzt er dessen öffentlichen Schlüssel des Public-Key-Verfahrens. So können verschlüsselte Nachrichten und der seinerseits verschlüsselte Sitzungsschlüssel zusammen über einen unsicheren Transportkanal übertragen werden. Dieser entschlüsselt mithilfe des Public-Key-Verfahrens unter Verwendung des geheimen Schlüssels zunächst den Sitzungsschlüssel und dann mithilfe des eigentlichen symmetrischen Verschlüsselungsverfahrens die Nachricht. Beispiele für den Einsatz hybrider Verfahren sind PGP oder S/MINE, siehe auch Abschn. 4.6.1 „E-Mail-Sicherheit“.

**Wichtig** Hybride Verschlüsselungsverfahren vereinen die Vorteile von symmetrischen und asymmetrischen Verfahren.

---

## 2.3 Quantencomputer: Das Damoklesschwert der Verschlüsselung

Die Einführung von leistungsfähigen Quantencomputern hätte für die Kryptografie zur Folge, dass alle zurzeit gebräuchlichen asymmetrischen Verschlüsselungsverfahren, wie beispielsweise das RSA-Verschlüsselungsverfahren, unsicher wären [5]. Alle Verschlüsselungsprotokolle, mit denen die Internet-Kommunikation verschlüsselt wird, wie zum Beispiel SSH, TLS, IPSec, PGP, S/MINE wären von da an unbrauchbar. Verschlüsselter oder signierter E-Mail-Verkehr sowie sicheres Surfen im Internet wären nicht mehr möglich. Dies hätte zur Folge, dass sämtliche Geschäftsprozesse im E-Commerce nicht mehr vertraulich und somit jegliche Formen von Onlinehandel effektiv nicht mehr möglich wären.

### Hintergrund

Im Jahre 1994 entwickelte der Mathematiker Peter Shor einen Algorithmus, mit dem es theoretisch möglich ist, die Primfaktoren einer Zahl N mithilfe von Quantencomputern zu bestimmen [6]. Das Besondere dieser Methode ist, dass das Problem somit erheblich schneller gelöst werden kann als mit dem schnellstmöglichen konventionellen Faktorisierungsalgorithmus. Die Sicherheit vieler

asymmetrischer Verschlüsselungsverfahren heutzutage basiert auf der Annahme, dass kein Verfahren existiert, das sehr hohe Zufallszahlen in Polynomialzeit in deren Primfaktoren zerlegen kann. Ein Quantencomputer mit genügend Qubits und dem Shor-Algorithmus würde jedoch in der Lage sein, genau das zu tun. Experten schätzen, dass ein 2048-Bit RSA Schlüssel von einem Quantenrechner mit 4000 Qubits gebrochen werden kann.

In den vergangenen 15 Jahren gab es schon eine Handvoll experimenteller Realisierungen von Shors Algorithmus. 2012 wurde die Zahl 21 in ihre Primfaktoren zerlegt [7]. Diese Realisierungen werden noch keinem Verschlüsselungsverfahren gefährlich werden können, doch sie kennzeichnen den Start für einen Umschwung auf diesem Gebiet der Verschlüsselung.

Heutige symmetrische Verschlüsselungsverfahren, wie beispielsweise AES, würde ein Quantencomputer mit Shors Algorithmus nicht brechen können. Doch mithilfe einer anderen Methode, dem sogenannten Grover Algorithmus, wäre ein Quantenrechner in der Lage, die Sicherheit dieser Verfahren effektiv zu halbieren. AES-256 wäre folglich nur noch so sicher wie AES-128 für einen Quantenrechner mit Grover Algorithmus [8]. Um dieser Gefahr vorzubeugen, würde eine Verdopplung der Schlüssellänge reichen. Bei asymmetrischen Verfahren sieht es nicht so einfach aus.

Zwar gibt es auch heute schon Algorithmen, die wahrscheinlich Angriffen von Quantencomputern widerstehen könnten, doch die absolute Mehrheit dieser existiert lediglich in der Theorie. Es wird hierbei von **Post-Quanten-Kryptografie** gesprochen.

Diese Herausforderung wird auf allen Ebenen durch hohe Forschungsgelder in diesem Bereich gerade an vielen Hochschulen und Forschungseinrichtungen bearbeitet.

**Wichtig** Quantencomputer sind für Public-Key-Verfahren das Damokles-schwert.

### Post-Quanten-Kryptografie

Doch Quanten-Computing wird nicht nur Nachteile für die Sicherheit von kryptografischen Verfahren mit sich bringen. So können bestimmte quantenmechanische Phänomene, wie das No-Cloning Theorem, genutzt werden, um Verbindungen wirklich sicher zu machen. Hierbei wird von Quanten-Kryptografie gesprochen. So kann zwar unter der Annahme, dass aktuell keine Computer mit genug Rechenleistung existieren, um bestimmte Schlüssel zu knacken, behauptet werden, dass aktuelle Verfahren praktisch sicher sind. Mithilfe von Quanten-Kryptografie können allerdings Kommunikationswege aufgebaut werden, die „absolut sicher“ sind. Es wurden bereits Verfahren entwickelt, bei denen die Sicherheit nicht auf der Rechenleistung von Großrechnern beruht, sondern vielmehr auf den Gesetzen der Physik. Und diese können von keinem noch so starken Computer gebrochen werden.

Spezieller geht es bei einem solchen Verfahren um den sicheren Austausch eines Schlüssels über einen öffentlichen Kanal, genauer gesagt, einen Quantenkanal. Hier werden Qubits beispielsweise in Form von Photonen benutzt. Diese bieten sich an, weil sie sich relativ einfach durch Fasern oder in der Luft übertragen lassen. Die Information kann auf die Photonen anhand ihrer Polarisation codiert werden. Versucht ein Angreifer nun, diesen öffentlichen Kanal abzuhören, so ist dies nicht möglich, ohne dass er dabei die ursprüngliche Nachricht verändert und somit verfälscht. Das hätte zur Folge, dass die beiden Kommunikationsteilnehmer erfahren würden, dass sie abgehört werden und dass es zu keinem Schlüsselaustausch kommen würde. Der offensichtliche Vorteil einer solchen Verbindung ist die bewiesenermaßen sichere Kommunikation. Die Nachteile werden jedoch schnell ersichtlich, wenn betrachtet wird, welcher Aufwand nötig ist, um einen solchen Quantenkanal praktisch umzusetzen. So wird diese Methode auch heute schon genutzt, allerdings war sie bisher nur über kleine Strecken von etwas über hundert Kilometern anwendbar. Zwar lassen sich Photonen relativ einfach versenden, doch eine solche Kommunikation ist sehr anfällig für Störungen. So wird die Versendungsdistanz in Kabeln durch deren Dämpfung stark begrenzt. Eine Übertragung durch die Luft über weite Strecken wird von der Atmosphäre verhindert [5].

---

## 2.4 One-Way-Hashfunktionen

Die eigenhändige Unterschrift ist seit Jahrhunderten bewährt. Anders als in der elektronischen Welt sind bei einem Vertragsabschluss die Parteien zugegen und können den Vertragspartner persönlich einschätzen und überprüfen. Dies grenzt auf natürliche Weise den Aktionsradius für Betrüger erheblich ein. In der elektronischen Welt kann auf diese bewährten Mechanismen nicht zurückgriffen werden, da über das Internet lediglich indirekt kommuniziert wird. Daher müssen grundlegende Cyber-Sicherheitsbedürfnisse anders befriedigt werden als in der realen Welt.

### Prüfsummenbildung und One-Way-Hashfunktionen

Auch wenn sich die digitale Signatur im elektronischen Geschäftsverkehr nur sehr zögerlich durchsetzt, bietet sie gegenüber der eigenhändigen Unterschrift doch einige entscheidende Vorteile. Der wichtigste darunter ist, dass die digitale Signatur – anders als ihr „analoges“ Gegenstück – benutzt werden kann, um die Integrität, also die Unverletztheit des unterzeichneten Dokuments, zu prüfen und zu bestätigen. Mit anderen Worten: Manipulationen lassen sich schnell und mit verhältnismäßig geringem Aufwand feststellen. Leider sind die dabei verwendeten asymmetrischen Operationen sehr aufwendig und damit langsam in der Ausführung. Außerdem wird noch einmal genau so viel Speicherplatz für die Signatur benötigt wie für den Klartext.

In der Praxis wird daher nicht die eigentliche Nachricht signiert, sondern lediglich eine charakteristische, kryptografische Prüfsumme (Hashwert), die gleichsam deren „Fingerabdruck“ bildet. Dazu wird die Nachricht an eine One-Way-Hashfunktion übergeben, welche die Prüfsumme bildet, siehe Abb. 2.26.

**Abb. 2.26** Berechnung einer kryptografischen Prüfsumme



Die One-Way-Hashfunktion berechnet aus einer beliebig umfangreichen Nachricht eine kryptografische Prüfsumme (Hashwert) mit einer zuvor festgelegten Länge. Dabei gilt die Formel

$$h_M = H(M),$$

wobei  $h_M$  die kryptografische Prüfsumme (Hashwert),  $H$  die One-Way-Hashfunktion und  $M$  die Nachricht bezeichnet.

### 2.4.1 Besondere Eigenschaften von Hashfunktionen

Eine One-Way-Hashfunktion muss bestimmte Eigenschaften aufweisen, damit sie für den kryptografischen Einsatz geeignet ist.

#### 1. $H$ ist eine öffentliche bekannte Einwegfunktion

Wie für jeden Verschlüsselungsalgorithmus gilt auch für One-Way-Hashfunktionen, dass sie öffentlich bekannt sein muss: Das ist einerseits notwendig, da sie auf allen, an einem Datenaustausch beteiligten Systemen verfügbar sein müssen, andererseits garantiert nur die öffentliche Bekanntheit ihre genaue Begutachtung durch Experten. Jede Hashfunktion muss einer öffentlichen Diskussion von Experten standgehalten haben, damit sie als sicher genutzt werden kann.

#### 2. $h_M = H(M)$ , $h$ ist ein eindeutiger „Fingerabdruck“ von $M$

Die Hashfunktion zählt zur Gruppe der kontrahierenden Einwegfunktionen, mit deren Hilfe sich die Länge der kryptografischen Prüfsumme (Hashwert) auf eine definierte, feste Länge reduzieren lässt, zum Beispiel 256 Bit. Außerdem kann  $M$  beliebig lang sein, aber die kryptografische Prüfsumme bleibt immer gleich.

#### 3. $H(M)$ ist eine One-Way Funktion (Einwegfunktion)

$H(M)$  ist einfach zu berechnen, bei gegebenem  $M$ .

Die One-Way-Hashfunktion stellt sicher, dass nicht von der kryptografischen Prüfsumme  $h$  auf den Klartext geschlossen werden kann. Es existiert also keine

Funktion  $H^{-1}(h_M)$ , mit der der Inhalt der Nachricht M aus dem Hashwert  $h_M$  wiederhergestellt werden kann. Mit gegebenem  $h_M$  ist es praktisch unmöglich, M zu berechnen, sodass  $M = H^{-1}(h_M)$  ist!

#### **4. $H(M)$ ist kollisionsresistent**

Weiterhin muss eine One-Way-Hashfunktion kollisionsresistent sein, das heißt, es darf nicht möglich sein, systematisch eine bestimmte kryptografische Prüfsumme  $h_M = H(M')$  zu erzeugen, die derjenigen der ursprünglichen Nachricht entspricht. Anders ausgedrückt: Es muss praktisch unmöglich sein, zu einer gegebenen Nachricht M eine weitere Nachricht  $M'$  mit der identischen kryptografischen Prüfsumme  $h_M$  zu finden.

Die Gleichung  $H(M) = H(M') = h$  darf nie zutreffen.

Die Kollisionsresistenz verhindert, dass Signaturen für beliebige Nachrichten gelten beziehungsweise diese systematisch so gestaltet werden, dass eine gewollte kryptografische Prüfsumme entsteht. Andernfalls ließe sich eine vorhandene signierte Nachricht gezielt ersetzen oder manipulieren, ohne dass dies nachgewiesen werden könnte. Ferner spielt hier die Prüfsummenlänge eine wichtige Rolle: Zwar sollte ein Hashwert kurz sein, allerdings darf es nicht zu leicht sein, Kollisionen zu finden. Aufgrund der ständig zunehmenden Rechenleistung moderner IT-Systeme ist jedoch abzusehen, dass solche Kollisionen für derzeit verwendete Prüfsummenlängen in einigen Jahren gezielt errechnet werden können. Daher müssen auch die One-Way-Hashfunktionen regelmäßig an die Gegebenheiten angepasst werden.

Neben SHA-3 und SHA-256 Verfahren gibt es noch MD5, RIPEMD, SHA-1, SHA-2 usw., die aber als unsicher einzustufen sind und nicht mehr genutzt werden sollten.

#### **2.4.2 SHA-3 (SHA = Secure Hash Algorithm)**

Im Oktober 2012 ist die Hash-Funktion Keccak vom National Institute of Standards and Technology (NIST) zum Standard ausgewählt worden.

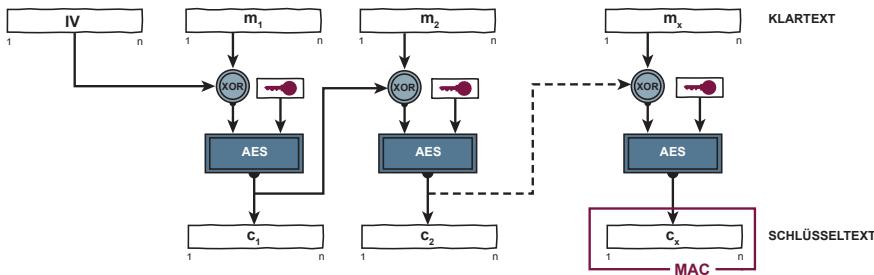
SHA-3 ist ein Algorithmus mit verschiedenen Parametern wie Wortlänge und Rundenzahl. Die Ausgabelänge kann 224, 256, 384 und 512 Bit lang sein.

#### **2.4.3 Message Authentication Code (MAC)**

Ein Message Authentication Code oder MAC ist eine Einweg-Hashfunktion, die einen Schlüssel verwendet, mit nur diesem der Hashwert verifiziert werden kann. Damit kann eine Authentizität ohne Geheimhaltung erreicht werden.

Mithilfe von MACs können mehrere Nutzer ihre Dateien authentifizieren und einzelne Nutzer können mit MACs überprüfen, ob ihre Dateien verändert wurden, zum Beispiel von Malware.

Im Gegensatz zu Einweg-Hashfunktionen ist der geheime Schlüssel des MACs zur Berechnung des Hashwertes (MAC) nur dem Nutzer bekannt, und der



**Abb. 2.27** Message Authentication Code (MAC)

Hashwert (MAC) kann nicht unbemerkt verändert werden. Eine einfache Möglichkeit zur Umwandlung einer Einweg-Hashfunktion in einen MAC besteht darin, den Hashwert mit einem symmetrischen Algorithmus zu verschlüsseln.

Jeder MAC kann in eine Einweg-Hashfunktion umgewandelt werden, indem der Schlüssel veröffentlicht wird.

CBC MAC ist ein weit verbreiteter NIST-Standard. Die Idee ist die Verwendung von einem symmetrischen Verfahren, wie AES im CBC-Modus und die anschließende Verwendung des letzten Blocks des Schlüsseltext-Blockes als Prüfsumme (in diesem Fall MAC), siehe Abb. 2.27.

#### 2.4.4 Keyed-Hashing for Message Authentication (HMAC)

Keyed-Hashing for Message Authentication (HMAC) ist ein Internet-Standard (RFC 2104) und wird zum Beispiel bei IPSec (siehe Kap. 10 „IPSec-Verschlüsselung“) verwendet.

Der HMAC ist eine Einweg-Hashfunktion, die mit einem Schlüssel arbeitet, aber Hashfunktionen statt Verschlüsselungsverfahren verwendet. Das HMAC-Verfahren soll mit möglichst vielen Hashfunktionen zusammenarbeiten, ohne dass diese modifiziert werden müssen. Die Sicherheit der Hashfunktion darf durch die Manipulation mit geheimen Schlüsseln nicht verringert werden.

##### HMAC-Verfahren

$$\text{HMAC} = \text{KH}(\text{K} \text{ XOR } \text{opad}, \text{H}(\text{K} \text{ XOR } \text{ipad}, \text{M}))$$

ipad  $0 \times 36, 0 \times 36, 0 \times 36, \dots$

(gleiche Länge wie die Blocklänger der Hashfunktion)

opad  $0 \times 5c, 0 \times 5c, 0 \times 5c, \dots$

(gleiche Länge wie die Blocklänger der Hashfunktion)

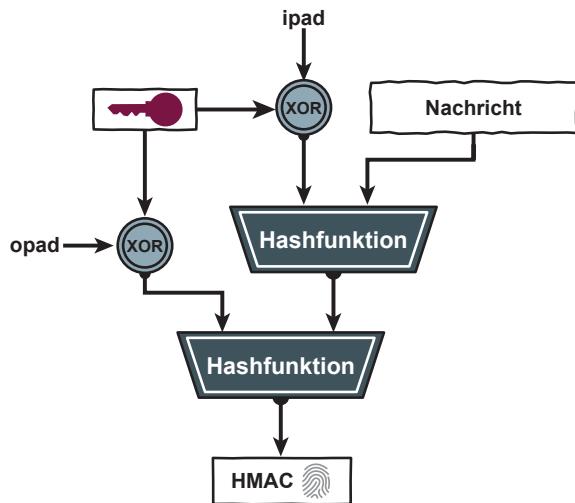
K geheimer Schlüssel

M Input (Nachricht)

XOR bitweise modulo 2 addieren

KH „Keyed-Hashing for Message Authentication“-Verfahren – HMAC-Verfahren

**Abb. 2.28** Keyed-Hashing for Message Authentication (HMAC)



Die beiden konstanten Felder  $\text{ipad}$  und  $\text{opad}$  haben eine Länge, die der Blockgröße  $B$  der eingesetzten Hashfunktion entspricht. Der Schlüssel  $K$  wird durch das Anhängen von Nullen ebenfalls auf die Länge  $B$  gebracht. Verknüpfe den auf die Länge  $B$  gebrachten geheimen Schlüssel  $K$  mittels XOR mit dem Feld  $\text{ipad}$ ! Stelle das Ergebnis dieser Operation vor die Nachricht und berechne mit der Hashfunktion den Hashwert aus diesem Input! Der Hashwert hat die Länge  $L$ . Verknüpfe den auf die Länge  $B$  gebrachten geheimen Schlüssel  $K$  mittels XOR mit dem Feld  $\text{opad}$ ! Dann stelle das Ergebnis dieser Operation (Länge  $B$ ) vor den Hashwert (Länge  $L$ ) und berechne mit der Hashfunktion den HMAC-Hashwert. Der HMAC-Hashwert hat die Länge  $L$ , siehe Abb. 2.28.

### Zusammenfassung

Kryptografische Verfahren sind nur ein kleiner Teil im Puzzle der Cyber-Sicherheitsmechanismen. Aber kryptografische Verfahren sind sehr wichtig und stellen die Basis der meisten Cyber-Sicherheitssysteme dar, verursachen aber oft auch die größten Cyber-Sicherheitsprobleme.

Wichtig ist, dass die Sicherheit eines kryptografischen Verfahrens niemals von der Geheimhaltung der Algorithmen abhängt, sondern ausschließlich auf der Geheimhaltung des geheimen Schlüssels basiert. Daher müssen kryptografische Verfahren immer öffentlich bekannt sein und durch eine intensive öffentliche Diskussion der Krypto-Experten die Sicherheit bestätigt werden.

Symmetrische Verschlüsselungsverfahren bieten eine sehr hohe Performance für die Verschlüsselung von Daten. Der Nachteil ist, dass für die geheimen Schlüssel ein gesicherter Schlüsselaustausch notwendig ist.

Bei der Nutzung von asymmetrischen Verschlüsselungsverfahren ist kein vertraulicher Schlüsselaustausch notwendig. Es muss aber sichergestellt werden, dass der öffentliche Schlüssel authentisch ist, das heißt, dem echten Nutzer gehört. Der Nachteil ist, dass die Performance eher schlecht ist.

Mithilfe von One-Way-Hashfunktionen können kryptografische Prüfsummen einer festen Länge von Nachrichten beliebiger Länge generiert werden.

Besonders wichtig bei kryptografischen Verfahren ist, dass die Sicherheit der Verfahren öffentlich diskutiert und bestätigt wird. Ebenso muss die Implementierung richtig sein, die Zufallszahlen- und Schlüsselgenerierung allen notwendigen Anforderungen genügen und die geheimen Schlüssel sicher gespeichert sein und nicht durch Unberechtigte genutzt werden können.

## Übungsaufgaben

### Übungsaufgabe 1 (monoalphabetische Substitution)

Entschlüsseln Sie den Schlüsseltext, der mithilfe einer monoalphabetischen Substitution mit der folgenden Verschlüsselungsvorschrift verschlüsselt wurde!

Schlüsseltext L N L D L R Q G Y Z L Y P X K N T L P P L N T R A

### Verschlüsselungsvorschrift

- (1) A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
- (2) G W X V L O A K U B C N D R M F H Y P Q T Z E I J S

### Übungsaufgabe 2 (monoalphabetische Substitution)

Der folgende Schlüsseltext ist mithilfe einer monoalphabetischen Substitution verschlüsselt worden. Ihre Aufgabe ist es, den Text zu entschlüsseln beziehungsweise die Verschlüsselungsvorschrift mithilfe einer statistischen Analyse (siehe Häufigkeit der Buchstaben) des Schlüsseltextes oder durch Ausprobieren zu erhalten. Der Originaltext (Klartext) ist in deutscher Sprache.

Schlüsseltext:

Rq efy Gaseysrtl tiun yftys Wfypjinp wat  
Wyszunprzypprlzwysginsyt  
ysgrypypt jr oayttw oitt qit efyzy Iplasfdnqyt jrziydjpfu wat  
yftyq Visiqydys ikniytlf qunyt eys eyt Ikpirg eys  
Dsitzgasqidfat za zdiso kyyftgprzzd eizz anty zyfty Oytdtfz  
oyfty Ytdzunprzypprl qaylpfun fz

### Übungsaufgabe 3 (homofone Substitution)

Der Schlüsseltext, der mithilfe einer homofonen Substitution verschlüsselt wurde, soll mit der unten aufgeführten Verschlüsselungsvorschrift entschlüsselt werden.

Schlüsseltext 34 75 61 47 80 01 93 78 41 51 93 25 04 29 72 64

### Verschlüsselungsvorschrift

Klartext	Schlüsseltext
A	(10, 21, 52, 59, 71)
B	(20, 34)
C	(28, 06, 80)
D	(19, 58, 70, 81, 87)
E	(09, 18, 29, 33, 38, 40, 42, 54, 55, 60, 66, 75, 85, 86, 92, 93, 99)
F	(00, 41)
G	(08, 12, 97)
H	(01, 07, 24)
I	(14, 39, 50, 65, 76, 88, 94)
J	(57)
K	(23)
L	(02, 05, 82)
M	(27, 11, 49)
N	(30, 35, 43, 62, 67, 68, 72, 77, 79)
O	(26, 53)
P	(31)
Q	(25)
R	(17, 36, 51, 69, 74, 78, 83)
S	(15, 16, 45, 56, 61, 73, 96)
T	(13, 32, 90, 91, 95, 98)
U	(03, 04, 47)
V	(37)
W	(22)
X	(44)
Y	(48)
Z	(64)

### Übungsaufgabe 4 (polyalphabetische Substitution)

Sie können den Schlüsseltext einer Nachricht abfangen, von der Sie bereits den Klartext kennen (polyalphabetischen Substitution – siehe nächste Übungsaufgabe). Sie gehen davon aus, dass auch zukünftige Nachrichten mit diesem Schlüssel übertragen werden. Wie lautet der Schlüssel, mit dem diese Nachricht verschlüsselt wurde?

Klartext                    D A T E N S C H U T Z  
Schlüsseltext            V I V L R J J L C M R

## Verschlüsselungsvorschrift

<b>Klartext:</b>	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
<b>Schlüsseltext:</b>	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z B C D E F G H I J K L M N O P Q R S T U V W X Y Z A C D E F G H I J K L M N O P Q R S T U V W X Y Z A B D E F G H I J K L M N O P Q R S T U V W X Y Z A B C E F G H I J K L M N O P Q R S T U V W X Y Z A B C D F G H I J K L M N O P Q R S T U V W X Y Z A B C D E G H I J K L M N O P Q R S T U V W X Y Z A B C D E F H I J K L M N O P Q R S T U V W X Y Z A B C D E F G I J K L M N O P Q R S T U V W X Y Z A B C D E F G H J K L M N O P Q R S T U V W X Y Z A B C D E F G H I K L M N O P Q R S T U V W X Y Z A B C D E F G H I J L M N O P Q R S T U V W X Y Z A B C D E F G H I J K M N O P Q R S T U V W X Y Z A B C D E F G H I J K L N O P Q R S T U V W X Y Z A B C D E F G H I J K L M O P Q R S T U V W X Y Z A B C D E F G H I J K L M N P Q R S T U V W X Y Z A B C D E F G H I J K L M N O Q R S T U V W X Y Z A B C D E F G H I J K L M N O P R S T U V W X Y Z A B C D E F G H I J K L M N O P Q S T U V W X Y Z A B C D E F G H I J K L M N O P Q R T U V W X Y Z A B C D E F G H I J K L M N O P Q R S U V W X Y Z A B C D E F G H I J K L M N O P Q R S T V W X Y Z A B C D E F G H I J K L M N O P Q R S T U W X Y Z A B C D E F G H I J K L M N O P Q R S T U V X Y Z A B C D E F G H I J K L M N O P Q R S T U V W Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Z A B C D E F G H I J K L M N O P Q R S T U V W X Y

## Übungsaufgabe 5 (polyalphabetische Substitution)

Ein Schlüsseltext wurde mithilfe einer polyalphabetischen Substitution unter Verwendung eines Schlüssels verschlüsselt. Wie lautet der dazugehörige Klartext? Verschlüsselungsvorschrift siehe Übungsaufgabe 4.

Schlüsseltext    W Q R F V E N I Q I Q G Y G X B U M I Z  
Schlüssels       E I P Y R N G

## Übungsaufgabe 6 (Permutation – Zackzack-Verfahren)

Sie wissen, eine Nachricht wurde mit dem Zackzack-Verfahren verschlüsselt. Es gelingt Ihnen, den Schlüsseltext abzuhören. Wie lautet der Klartext?

Hinweis: Die Tiefe der Zackzack-Kurve kennen Sie nicht, das heißt, Sie müssen mehrere Tiefen ausprobieren, um ein sinnvolles Ergebnis zu erzielen.

Schlüsseltext=I T E N A I L I S L O N T T L N A U G A S N

## Übungsaufgabe 7 (Public-Key-Verfahren – RSA)

Gegeben sind der öffentliche Schlüssel ( $e=5$ ,  $n=21$ ) und der private Schlüssel ( $d=17$ ).

- Sie wollen die Zahl „5“ vor einer Übertragung mit dem öffentlichen Schlüssel verschlüsseln. Wie lautet das Ergebnis der Verschlüsselung?

- b) Sie erhalten die mit dem öffentlichen Schlüssel verschlüsselte Zahl „11“. Wie lautete die ursprüngliche Nachricht?
- c) Sie erhalten eine Nachricht mit der Zahl „3“, die mit der digitalen Signatur des Absenders ausgestattet wurde. Die Signatur lautet „12“. Kommt die Nachricht vom richtigen Absender?  
Sie erhalten eine weitere Nachricht mit der Zahl „4“ und der Signatur „15“. Wie sieht es in diesem Fall mit der Authentizität des Absenders aus?
- d) Wir nehmen an, Sie kennen den geheimen Schlüssel nicht und wollen diesen berechnen, um alle Nachrichten mitlesen zu können. Dazu benötigen Sie die Primzahlen p und q, die Sie durch die Zerlegung von n erhalten können. Wie lauten die verwendeten Primzahlen?

### Übungsaufgabe 8 (One-Way-Hashfunktionen)

- a) Gegeben ist die folgende Funktion:

```
private static byte[] one_way_hashfunction_1(byte[] input)
```

```
{
byte hash_key=(byte) 0xFF; //Schlüssel zum Hashen der Eingabe
byte[] hash=new byte[input.length]; //Array zum Speichern des Hash-Werts
for (int i=0; i<input.length; i++)
{ //Iteration über das Eingabe-Array
hash[i]=(byte) (input[i] ^ hash_key); //Jede Stelle im Array mit dem Schlüssel XORn
}
return hash;
}
```

Beispiele:

Eingabe	Ausgabe	
Daten	Byte-Repräsentation	Hash-Wert
Hallo Welt	[72, 97, 108, 108, 111, 32, 87, 101, 108, 116]	[-73, -98, -109, -109, -112, -33, -88, -102, -109, -117]
Cyber-Security	[67, 121, 98, 101, 114, 45, 83, 101, 99, 117, 114, 105, 116, 121]	[-68, -122, -99, -102, -115, -46, -84, -102, -100, -118, -115, -106, -117, -122]
Norbert Pohlmann	[78, 111, 114, 98, 101, 114, 116, 32, 80, 111, 104, 108, 109, 97, 110, 110]	[-79, -112, -115, -99, -102, -115, -117, -33, -81, -112, -105, -109, -110, -98, -111, -111]

Warum handelt es sich bei der gegebenen Funktion *nicht* um eine One-Way-Hashfunktion?

- b) Gegeben ist die folgende Funktion:

```
private static int one_way_hashfunction_2(String input)
{
    int hash=1; //Initialer Hash-Wert
    for (int i=0; i<input.length(); i++)
    { //Über die Eingabe iterieren
        char c=input.charAt(i); //Zeichen an Stelle i auslesen
        hash=hash*Character.getNumericValue(c); //Hash-Wert berechnen
    }
    return hash;
}
```

Eingabe	Ausgabe
Hallo Welt	-1274889216
Cyber-Security	-265940992
Norbert Pohlmann	-931899904

Warum handelt es sich bei der gegebenen Funktion *nicht* um eine One-Way-Hashfunktion?

### Übungsaufgabe 9 (Symmetrische Verschlüsselung)

Sie haben die folgende „verschlüsselte“ HTTP Kommunikation (Bytes) mitgeschnitten. Bei näherem Betrachten erkennen Sie aber, dass diese gewisse Muster aufweist. Finden Sie den Klartext zu der Kommunikation!

HTTP-Anfragen:

Die gesamten Anfragen sind online zu finden.

Anfrage 1:

[120, 5, 21, 98, 108, 37, 53, 54, 104, 60, 33, 47, 38, 41, 62, 97, 33, 63, 35, 48, 54, 38, 33, 123, 39,...]

Anfrage 2:

[120, 5, 21, 98, 108, 37, 53, 54, 104, 60, 33, 47, 38, 41, 62, 97, 33, 63, 35, 48, 54, 38, 33, 123, 39,...]

Anfrage 3:

[120, 5, 21, 98, 108, 37, 53, 54, 104, 60, 33, 47, 38, 41, 62, 97, 33, 63, 35, 48, 54, 38, 33, 123, 39,...]

Anfrage 4:

[120, 5, 21, 98, 108, 37, 53, 54, 104, 61, 57, 38, 36, 45, 41, 61, 96, 98, 97, 99, 100, 123, 100, 102,...]

Anfrage 5:

[120, 5, 21, 98, 108, 37, 53, 54, 104, 61, 57, 38, 36, 45, 41, 61, 96, 98, 97, 99, 101, 123, 101, 111,...]

### Übungsaufgabe 10 (Allgemeine Fragen)

Beurteilen Sie die folgenden Situationen, jeweils mit Begründung.

Situation 1:

Sie wollen vertrauliche Daten einer Wahl über das Internet der dafür zuständigen Behörde übermitteln. Dazu hat Ihr Chef-Entwickler einen sehr komplexen Kryptografie-Algorithmus geschrieben, der die Daten effizient verschlüsselt und anschließend übermittelt. Wie beurteilen Sie die Situation?

- Das Vorgehen ist nicht akzeptabel.
- Ja, das geht in Ordnung

Begründung:

Situation 2:

Sie haben einen neuen Praktikanten in Ihrem Unternehmen. Nach einiger Zeit kommt der Praktikant und teilt Ihnen mit, dass er bemerkt hat, dass Bilder in Ihr Netzwerk übertragen werden, die am Ende der Bilder (Bild-Datei) nicht lesbare Daten enthalten, die nicht zu dem Bild gehören. Zu welchem Experten schicken Sie den Praktikanten?

- Steganografen
- Kryptoanalytiker
- Firewall-Experten
- Datenschutzbeauftragter

Situation 3:

Sie haben geheime Informationen erhalten, die Sie aufgrund ihrer Brisanz vertraulich mit einer Journalistin teilen möchten. Problematisch dabei ist, dass Sie sich nicht persönlich mit der Journalistin treffen können, sondern die Daten über das Internet übertragen müssen. Welche Verschlüsselungsart wählen Sie?

- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung

**Situation 4:**

Sie sind Entwicklerin in einem aufstrebenden Start-up-Unternehmen. Ihre angebotene App soll um eine Funktion erweitert werden, die es erlaubt, Daten, die in der App anfallen (Bilder, Videos,...), sicher auf dem Gerät zu speichern. Sie entscheiden sich aus Performance-Gründen für eine symmetrische Verschlüsselung. Daher generieren Sie einen 100-stelligen vollkommen zufälligen Schlüssel, den Sie im Quell-Code der App hinterlegen.

Wo liegt das Problem in diesem Design? Was könnten Sie besser machen?

**Übungsaufgabe 11** (Allgemeine Fragen)

Sie wollen einen Text sowohl verschlüsseln, als auch komprimieren. Welche Aktionen führen Sie als erstes aus? Begründen Sie die Reihenfolge!

**Übungsaufgabe 12** (Allgemeine Fragen)

Wie oft müssen Sie maximal unterschiedliche Schlüssel durchprobieren, wenn Sie einen Brute-Force-Angriff auf einen Schlüsseltex durchführen wollen, bei dem eine Schlüssellänge von 256 Bit genutzt worden ist?

**Übungsaufgabe 13** (Allgemeine Fragen)

Welchen Vorteil hat ein Angreifer, wenn er den IV des CBC-Modes kennt?

**Übungsaufgabe 14** (Allgemeine Fragen)

Eine kontinuierliche Kommunikation wird auf Bit-Ebene wahlweise mit dem CFB-Mode oder OFB-Mode bitweise, bei einem Blockverschlüsselungs-Output von n-Bit, verschlüsselt. Dann wird ein Bit manipuliert (von 0 auf 1 oder von 1 auf 0). Kann sich die Verschlüsselung bei den beiden Modes wieder synchronisieren? Wenn ja, nach wie vielen Bits?

**Übungsaufgabe 15** (Allgemeine Fragen)

Eine kontinuierliche Kommunikation wird auf Bit-Ebene wahlweise mit dem CFB-Mode oder OFB-Mode bitweise, bei einem Blockverschlüsselungs-Output von n-Bit, verschlüsselt. Dann geht ein Bit verloren (Sender und Empfänger sind nicht mehr synchron). Kann sich die Verschlüsselung bei den beiden Modes wieder synchronisieren? Wenn ja, nach wie vielen Bits?

**Übungsaufgabe 16** (Allgemeine Fragen)

Bitte kreuzen Sie Ihre Antworten an!

	Cyber-Sicherheitsmechanismen				
	Symmetrische Verschlüsselung	One-Way-Hashfunktion	Public-Key-Verschlüsselung	Public-Key-Verschlüsselung	Stenografie
Gewährleistung von Cyber-Sicherheitsbedürfnissen	Vertraulichkeit Authentifikation Authentizität Integrität Verbindlichkeit Verfügbarkeit Anonymisierung/ Pseudonymisierung				
Cyber-Sicherheitsstrategien	Vermeiden von Angriffen Entgegenwirken von Angriffen Erkennen von Angriffen				

**Übungsaufgabe 17** (Allgemeine Fragen)

Welche Eigenschaften muss ein Schlüssel für symmetrische Verschlüsselungsverfahren haben, damit er eine maximale Sicherheit bieten kann?

Ergebnisse siehe: <https://norbert-pohlmann.com/cyber-sicherheit/uebungen/>.

---

**Literatur**

1. Hesse M, Pohlmann N (2006) Kryptographie (I): Von der Geheimwissenschaft zur alltäglichen Nutzanwendung. IT-Sicherh Datenschutz Z Rechts Prüfungssicheres Datenmanag 6:405–419
2. Hesse M, Pohlmann N (2006) Kryptographie (II): Von der Geheimwissenschaft zur alltäglichen Nutzanwendung – Elementare Verschlüsselungsverfahren. IT-Sicherh Datenschutz Z Rechts Prüfungssicheres Datenmanag 7:430–439
3. Hesse M, Pohlmann N (2006) Kryptographie (III): Von der Geheimwissenschaft zur alltäglichen Nutzanwendung – Symmetrische Verschlüsselungsverfahren. IT-Sicherh Datenschutz Z Rechts Prüfungssicheres Datenmanag 8:464–473
4. Hesse M, Pohlmann N (2006) Kryptographie (IV): Von der Geheimwissenschaft zur alltäglichen Nutzanwendung – Asymmetrische Verschlüsselungsverfahren. IT-Sicherh Datenschutz Z Rechts Prüfungssicheres Datenmanag 9:495–505
5. Fischer J, Pohlmann N (2017) Ein Quantum Bit. Quantencomputer und ihre Auswirkungen auf die Sicherheit von morgen. IT-Sicherh Fachmag Informationssicherh Compliance 1
6. Shor PW (1996) Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J Sci Statist Comput 26(1)
7. Martín-López E, Laing A, Lawson T, Alvarez R, Zhou X, O'Brien J (2012) Experimental realization of Shor's quantum factoring algorithm using qubit recycling. Nat Photonics 6(11):773–776
8. Leurent G, Leverrier A, Naya-Plasencia M (2015) On the security of symmetric key ciphers against quantum adversaries. M. Kaplan 9



# Hardware-Sicherheitsmodule zum Schutz von sicherheitsrelevanten Informationen

3

Immer mehr sicherheitsrelevante Informationen, wie zum Beispiel geheime Schlüssel und Transaktionsdaten, werden durch Bezahlsysteme sowie Verschlüsselungs- und Authentifikationslösungen im Internet genutzt. In diesem Kapitel werden Hardware-Sicherheitsmodule (HSMs) beschrieben, die helfen, besonders sensible sicherheitsrelevante Informationen angemessen zu schützen.

---

## 3.1 Einleitung

Das Ziel eines Hardware-Sicherheitsmoduls ist ein hoher Schutz vor Auslesen und Manipulation von besonders sensiblen sicherheitsrelevanten Informationen innerhalb eines besonders geschützten Hardware-Bereiches [1].

Besonders sensible sicherheitsrelevante Informationen, die in einem Hardware-Sicherheitsmodul geschützt werden sollen, sind zum Beispiel:

- geheime Schlüssel für Verschlüsselung, Authentifizierung, Signaturen usw.
- Programme, die nicht kopiert oder modifiziert werden sollen, im Sinne eines Softwareschutzes.
- Daten, die besondere Werte darstellen, wie zum Beispiel Transaktionsdaten, Coins usw.

Alle sicherheitsrelevanten Operationen, wie zum Beispiel „Verschlüsseln“, „Signieren“, „Zufallszahlen und Schlüssel generieren“ usw. finden direkt im besonders geschützten Hardware-Sicherheitsmodul statt, siehe Abb. 3.1. Geheime Schlüssel können so benutzt werden, ohne sie zu kennen. Geheime Daten, digitale Werte und Software sind manipulationssicher im Hardware-Sicherheitsmodul gespeichert.

**Abb. 3.1** Idee eines  
Hardware-Sicherheitsmoduls



In der Praxis haben sich unterschiedliche Umsetzungskonzepte von Hardware-Sicherheitsmodulen mit verschiedenen Sicherheitswirkungen und Einsatzumfeldern etabliert.

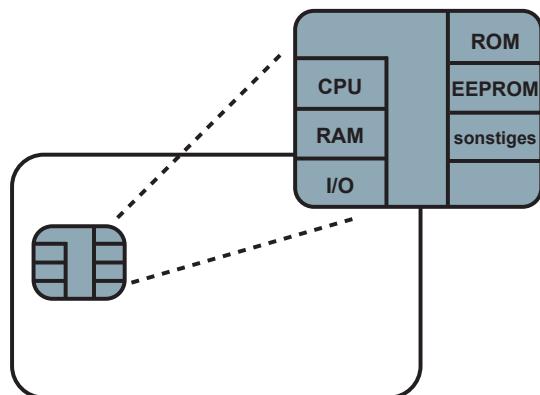
**Wichtig** Hardware-Sicherheitsmodule (HSMs) schützen sicherheitsrelevante Informationen besonders wirkungsvoll.

### 3.2 Hardware-Sicherheitsmodul: Smartcards

Eine Smartcard oder intelligente Chipkarte ist ein IT-System in der genormten Größe der EC-Karte ( $86 \times 54 \times 0,76$  mm), das Personen IT-Sicherheitsdienstleistungen zur Verfügung stellt.

Eine Smartcard (siehe Abb. 3.2) enthält einen Sicherheitschip mit CPU, RAM- und ROM-Speicher, ein „schlankes“ und sicheres Betriebssystem im ROM, eine I/O-Schnittstelle, über die die gesamte Kommunikation stattfindet (Kontaktflächen oder kontaktloses Interface) und ein EEPROM, auf dem die geheimen Schlüssel, wie ein geheimer RSA-Schlüssel oder andere symmetrische Schlüssel sowie persönliche Daten (Passwörter etc.) sicher gespeichert sind. „Sonstiges“ ist beispielsweise ein Co-Prozessor, der symmetrische oder asymmetrische Verschlüsselung sehr schnell durchführt (Krypto-Prozessor) [2].

**Abb. 3.2** Smartcard



Der Sicherheitschip der Smartcard bietet zum Beispiel die folgenden Hardware-Sicherheitsmechanismen zum Schutz der sicherheitsrelevanten Informationen: Unter- und Überspannungsdetektion, Erkennung niedriger Frequenzen. Diese Sicherheitsmechanismen sorgen dafür, dass der Sicherheitschip immer in einem definierten Zustand arbeitet (Strom, Frequenz) und nicht bei einer Manipulation die sicherheitsrelevanten Informationen nach außen sendet.

Weitere Sicherheitsmechanismen im Sicherheitschip sind: Verwürfelte Busse, Sensoren für Licht, Temperatur usw. Passivierungs- beziehungsweise Metallisierungsschichten über Bus- und Speicherstrukturen oder über der gesamten CPU, Zufallszahlengenerator in der Hardware, spezielle CPU-Befehle für kryptografische Funktionen und Speicherschutzfunktionen.

Auch die Smartcard-Software bietet Software-Sicherheitsmechanismen an, wie Zugriffskontrolle auf Objekte und Zustandsautomaten, die in Abhängigkeit von Identifikations- und Authentisierungsmechanismen auf der Smartcard Befehle zulassen.

Die Sicherheit einer Smartcard beruht in der Regel auf zwei Faktoren: Wissen (PIN) und Besitz (Karte).

Geheime Schlüssel verlassen den Sicherheitschip der Smartcard nie. Alle Operationen mit sicherheitsrelevanten Informationen finden direkt im Sicherheitschip der Smartcard statt. Geheime Schlüssel können benutzt werden, ohne sie zu kennen. Geheime Daten sind manipulationssicher im Sicherheitschip gespeichert.

Smartcardbasierte Sicherheitschips werden in Form von Smartcards, aber auch in der Form von USB-Token, NFC-Token usw. realisiert und genutzt. Die Nutzung der IT-Sicherheitsdienste kann dann aber performanter und ohne zusätzliches Lesegerät über USB und NFC vorgenommen werden.

Die Aktivierung mithilfe einer PIN hat einige praktische Herausforderungen. In der Regel werden nur vier bis sechs Zeichen für die Aktivierung gefordert, was die Anzahl der möglichen Kombination sehr einschränkt. Oft benutzen die Nutzer für alle Smartcards die PIN ihrer EC-Karte, was selbstverständlich ein Sicherheitsrisiko darstellt.

Wird das Fingerabdruckverfahren anstelle der üblicherweise verwendeten PIN zur Aktivierung einer Smartcard verwendet, ist „Match on Card“ ein notwendiges und passendes Sicherheitskonzept. Dabei erfolgt der Vergleich des aktuellen Fingerabdrucks mit dem gespeicherten Referenzwert direkt im Sicherheitschip der Smartcard. In der Regel werden mehrere Fingerabdrucktemplates im Sicherheitschip der Smartcard abgelegt, damit der Nutzer unterschiedliche Finger nutzen kann, zum Beispiel, wenn er eine Verletzung am Zeigefinger hat.

Die Vorteile des *Match-on-Card*-Verfahrens bezüglich Biometrie liegen vor allem in der hohen Sicherheit, da die Referenzwerte niemals den geschützten Bereich des Sicherheitschips der Smartcard verlassen und nicht ausgelesen werden können. Die sichere Speicherung des Referenzwerts nur im Sicherheitschip der Smartcard ist besonders datenschutzfreundlich, weil die personenorientierten Daten nicht zentral gespeichert werden müssen. Darüber hinaus ermöglicht ein direkt auf dem Sicherheitschip gespeicherter Referenzwert auch die Verwendung an verschiedenen Standorten (Roaming) oder auf offline betriebenen IT-Systemen.

### Anwendungsfelder für Smartcards

Sehr bekannte Anwendungsfelder für Smartcards mit Sicherheitschips sind: EC-Karte, Kreditkarten, der neue Personalausweis, Dienstausweise, Banken-Signaturkarten, die neue Gesundheitskarte, der Heilberufsausweis, Authentifikations-token, Verschlüsselungstoken, Bitcoin-Wallet usw.

**Wichtig** Smartcards schützen sicherheitsrelevante Informationen für Personen.

**Diskussion über den Level an IT-Sicherheit**, der mit einem smartcardbasierten Hardware-Sicherheitsmodul erzielt werden kann:

Die IT-Sicherheit soll in der Wirkung so stark sein, dass erst mit einem Aufwand von mehr als 1. Mio. EUR ein erfolgreicher Angriff auf die sicherheits-relevanten Informationen umgesetzt werden kann.

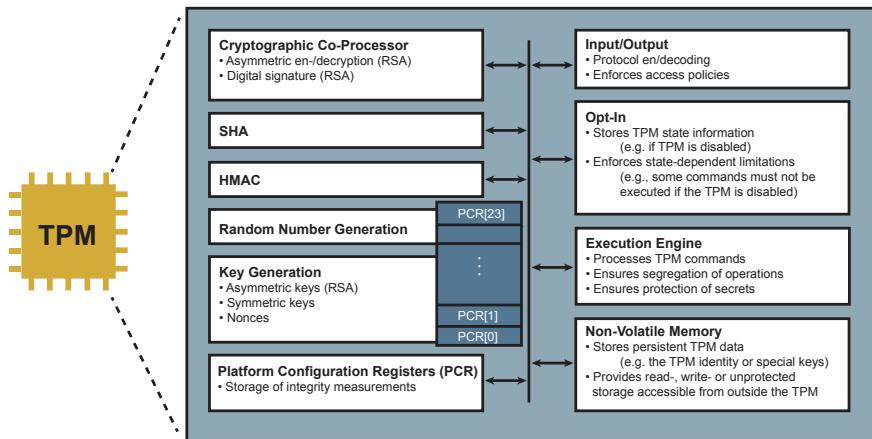
Daher werden in der Regel nur abgeleitete Schlüssel auf der Smartcard gespeichert. Das bedeutet, bei einer Bankkarte, wenn die Smartcard geknackt wurde, kann nur der geheime Schlüssel des Bankkunden ausgelesen und damit auch nur das Konto des betroffenen Bankkunden mit einem begrenzten Schaden ausgeraubt werden. Die gesamte Sicherheit des Bankensystems und aller anderen Bankkunden bleibt bestehen.

**Wichtig** Eine Smartcard hat in der Regel nur personenorientierte, abgeleitete Schlüssel und keine Masterschlüssel gespeichert.

---

### 3.3 Hardware-Sicherheitsmodul: Trusted Platform Module (TPM)

Trusted Computing ist der Begriff für die Idee, IT-Systeme grundsätzlich vertrauenswürdiger zu gestalten. Forciert werden die damit einhergehenden Sicherheitstechnologien von einem Industriekonsortium mit sehr vielen internationalen Mitgliedern [3] siehe auch Kap. 7 „Trusted Computing“. Die Ergebnisse dieser Zusammenarbeit sind offene Spezifikationen, die grundsätzlich zum Ziel haben, die Basis für die vertrauenswürdige IT zu bilden. Insbesondere die Sicherheit verteilter Anwendungen soll mit wirtschaftlich vertretbarem Aufwand verbessert werden, das heißt, es soll keine massive Veränderung existierender Hard- beziehungsweise Software notwendig sein. Eine der Hauptideen ist die Nutzung einer manipulationssicheren Hardware-Komponente, das sogenannte Trusted Platform Module (TPM). Es soll softwarebasierten Angriffen entgegenwirken. Die TPM-Spezifikationen wurden bereits von vielen Herstellern umgesetzt. Fast jedes aktuelle Notebook beinhaltet einen solchen Sicherheitschip. Ein TPM ist im Prinzip und vom Sicherheitslevel her ein Smartcard-Sicherheitschip mit ein paar Erweiterungen, wie das Platform Configuration Register (PCR), siehe Abb. 3.3.



**Abb. 3.3** Trusted Platform Module (TPM)

TPM ist ein kleines Hardware-Sicherheitsmodul für alle IT-Systeme (PC, Notebook, Smartphones, PDSs, Drucker, Router, Kühlschrank usw.).

Das TPM wirkt als vertrauenswürdiger Anker in einem IT-System (Root of Trust). Beginnend mit dem Startvorgang werden alle Hardwareelemente und Softwarekomponenten (BIOS, Betriebssystem, Anwendungsprogramme etc.) mithilfe von Hashfunktionen gemessen und ihre Zustände im Platform Configuration Register (PCR) des TPM gespeichert. Die Systemkonfiguration des IT-Systems ist also jederzeit komplett mess- und damit auch überprüfbar.

In der Automobilindustrie entspricht das der Arbeit eines Kontrolleurs, der die gesamte Montage eines Wagens protokolliert und hinterher anhand einer zertifizierten Liste mit Kontrollnummern aller Teile (zum Beispiel des Fahrgestells) die „Integrität“ des Autos beweisen kann. Wird ein Teil ersetzt, wäre das Auto nicht mehr im Originalzustand und im Vergleich mit der Liste nicht mehr vertrauenswürdig. Die Systemkonfigurationsüberprüfung durch das TPM erfolgt in identischer Weise. Damit können sich IT-Systeme gegenüber einem Nutzer oder anderen IT-Systemen hinsichtlich ihrer Systemkonfiguration „ausweisen“. Dieser Vorgang wird Attestation genannt. Dies bietet ein hohes Maß an Vertrauenswürdigkeit der genutzten Software.

Außerdem bietet das TPM die Möglichkeit, Daten zu versiegeln und vertraulich zu speichern. Dabei werden die Daten während der Verschlüsselung an die Systemkonfiguration gebunden. Dieser Vorgang wird Sealing genannt. Er stellt sicher, dass auf versiegelte Daten nur wieder zugegriffen werden kann, wenn sich das IT-System in einem bekannten Zustand (Systemkonfiguration) befindet. Dem entspricht im übertragenen Sinn die Möglichkeit, genau zu prüfen, ob zum Beispiel das Bremssystem eines Autos unverändert und damit funktionsfähig ist, siehe auch Kap. 7.

Was sind die großen Vorteile von TPMs?

- Das TPM bietet eine sehr hohe Sicherheit bei geringer Investitionssumme, da ein TPM nicht mehr als ein Euro kostet.
- Da IT-Systeme wie Notebooks in den meisten Fällen Microsoft ready sind, ist ein TPM auf dem überwiegenden Teil der IT-Systeme verfügbar.
- Die TPMs sind in eine Sicherheitsinfrastruktur (PKI, etc.) eingebunden und daher einfach im Sicherheitsmanagement zu behandeln.

Es gibt auch Vorbehalte gegen die TPM-Nutzung, zum Beispiel

- Das Konsortium, die Trusted Computing Group, welches das TPM spezifiziert, handelt nicht immer transparent und der Zugang zu den Spezifikationen könnte insbesondere für kleinere Unternehmen einfacher sein.
- TPMs sind in der Lage, über Hintertüren im Chip-Design, auf die sicherheitsrelevanten Informationen zuzugreifen, wenn sie physikalischen Zugriff auf das IT-System mit dem TPM haben

### Anwendungsfelder für TPMs

Die Sicherheitswirkung des Schutzes der sicherheitsrelevanten Informationen von TPMs eignet sich, wie bei Smartcards, für abgeleitete Schlüssel im IT-System-orientierten und lokalen Umfeld. Das Einsatzgebiet von TPMs ist typischerweise die Sicherheit von sicherheitsrelevanten Informationen für kleinere IT-Systeme (zum Beispiel PCs, Notebooks, Drucker, Netzwerkkomponenten, Autos und andere Dinge).

**Diskussion über den Level an IT-Sicherheit:** Da ein TPM auf der Basis eines Smartcard Sicherheitschip arbeitet, ist auch der Level an IT-Sicherheit gleich mit dem Sicherheitschip einer Smartcard.

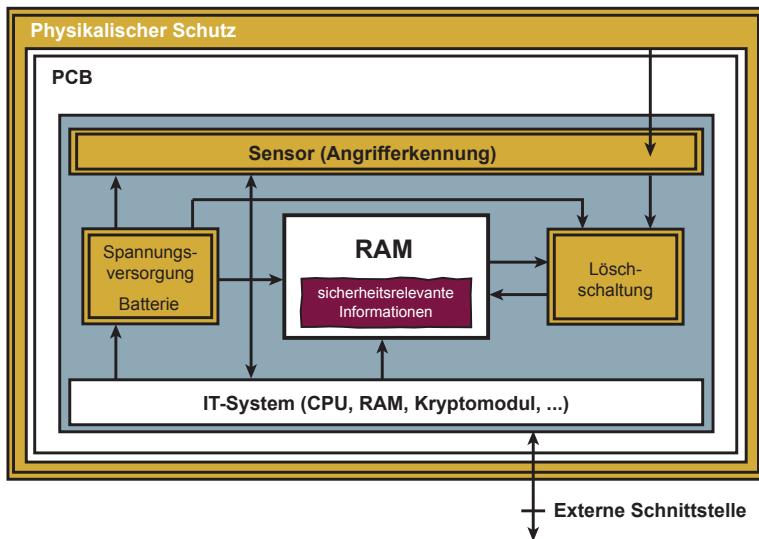
**Wichtig** Das Hardware-Sicherheitsmodul TPM speichert in erster Linie abgeleitete Schüssel von IT-Systemen und Personen.

Eine neue Entwicklung von vertrauenswürdigen Ausführungsumgebungen ist unter dem Begriff „Trusted Execution Environment“ bekannt und wird insbesondere im Bereich von mobilen Geräten Neuerungen bringen. Hier bieten die vorhandenen Chip-Sätze der Hersteller von CPUs die Möglichkeit, sogenannte „Trusted Apps“ in einer sicheren Umgebung ohne zusätzliche Hardware laufen zu lassen.

---

### 3.4 Hardware-Sicherheitsmodul: High-Level Security Module (HLSM)

Ein High-Level Security Module (HLSM) ist für besonders wertvolle sicherheits-relevante Informationen (Master-Keys, Schlüssel von globaler Bedeutung etc.) und für sehr hohe Performance-Anforderungen konzipiert. Ein besonderer Unterschied



**Abb. 3.4** High-Level Security Module (HLSM)

zur Smartcard-Sicherheit ist, dass wenn ein Angriff vom High-Level Security Module erkannt wird, die zu schützenden sicherheitsrelevanten Informationen innerhalb des Sicherheitsmoduls sofort aktiv und sicher gelöscht werden können. Dazu ist ein HLSM typischerweise physikalisch gekapselt und mit einer aktiven Sensorik ausgerüstet, die Angriffe erkennt und dann Aktionen auslösen kann. Ein HLSM ist in der Regel ein Vielfaches sicherer und leistungsfähiger als eine Smartcard, aber auch sehr viel teurer (mehrere tausend Euro, in Abhängigkeit der Leistung).

Die Grundidee eines HLSM ist ein physikalisch geschütztes IT-System mit einem gepufferten RAM, in dem alle sicherheitsrelevanten Informationen gespeichert sind, siehe Abb. 3.4. Alle Sicherheitsdienstleistungen des Security Module werden über eine definierte externe Schnittstelle zur Verfügung gestellt [4].

Mithilfe eines physikalischen Schutzes wird der Inhalt des RAMs so geschützt, dass es einem Angreifer nicht möglich ist, es auszulesen oder zu manipulieren. Ein physikalischer Schutz ist zum Beispiel eine komplex aufgebaute, flexible Leiterplatte mit vielen Layern und unterschiedlich verlaufenden Leiterbahnen, die das RAM mit den sicherheitsrelevanten Daten schützen. Der physikalische Schutz ist mit Sensorik untermauert, sodass jeder denkbare Angriff sofort erkannt wird. Es gibt eine Löschschaltung, die den Inhalt des RAM aktiv und sicher löscht, wenn ein Angriff erkannt wurde. Eine interne Stromversorgung sorgt dafür, dass die Löschschaltung und die Sensorik immer funktionsfähig sind. Außerdem überwacht die Sensorik die Stromversorgung. Bevor die Energie der internen Stromversorgung zu Ende geht, wird der Löschevorgang aus Sicherheitsgründen aktiv und löscht alle sicherheitsrelevanten Informationen nachhaltig sicher. Die

Sensorik hat die Aufgabe, mögliche Angriffe zu erkennen, wie Durchleuchten, Temperatur-Angriffe, mechanische Attacken auf das RAM, chemische Attacken gegen den physikalischen Schutz und Manipulation des ordentlichen Betriebs über Spannung und Frequenzen. Wird ein Angriff durch die Sensorik erkannt, wird ein Löschtorgang ausgelöst und damit können die sicherheitsrelevanten Informationen nicht mehr erfolgreich angegriffen werden.

Bei dieser wichtigen Sicherheitsfunktion wird deutlich, dass es einen verlässlichen und sicheren Backup-Prozess geben muss, der die sicherheitsrelevanten Daten wiederherstellen kann. Somit bleibt die eigentliche und gewollte Anwendung mit den besonders sensiblen sicherheitsrelevanten Informationen verfügbar.

Die Leistungsfähigkeit der verwendeten CPU bei einem HLSM ist in der Regel sehr hoch, und die Kommunikationsgeschwindigkeit mit einem HLSM ist sehr schnell. Auch Lösungen, die eine hohe Parallelität für eine höhere Performance sowie gute Verfügbarkeit zur Verfügung stellen, sind in sehr vielen Anwendungsfällen notwendig [5].

Dabei werden mehrere HLSM in einem IT-System angeboten und/oder mehrere HLSM in IT-Systeme parallel über Kommunikationsschnittstellen parallel und redundant genutzt.

Die Vorteile eines HLSM sind seine hohe Leistungsfähigkeit und die hohe Sicherheit, im Vergleich zu Smartcard-Sicherheitschips und TPMs.

### Anwendungsfelder für High-Level Security Module

Ein Hardware-Sicherheitsmodul für das Hoch-Sicherheitsumfeld ist in der Umsetzung meist ein High-Level Security Module (HLSM). Die Sicherheitswirkung eines HLSM zum Schutz der sicherheitsrelevanten Informationen eignet sich für Master-Keys und Schlüssel von globaler Bedeutung. Die Einsatzgebiete sind typischerweise Sicherheitskomponenten für größere IT-Systeme im Hoch-Sicherheitsumfeld.

Anwendungsfälle von HLSMs sind: Public Key-Infrastruktur (Schlüsselgenerierung, Zeitstempeldienste), Bankenumfeld (Autorsierungsstationen für die Freigabe von Geld, wie bei EC-Cash, Speicherung von Wallets, wie für Bitcoins usw.), Sicherheit für die Netzbetreiber (im Bereich EC-Cash mit Mineralölunternehmen usw.) und Industrie (Schlüsselgenerierung für Autoschlüssel, Abrechnung in Maut-Systemen, Authentifikation im Mobilfunknetz, digitale Signatur von zentralen Prozessen, wie Rechnungen, Archivierungssystemen usw.), im behördlichen Umfeld (IT-Sicherheitsdienste des neuen Personalausweises, Speicherung von Schlüsseln für die Verschlüsselung, ...).

### Diskussion über den Level an IT-Sicherheit, der mit einem High-Level Security Modul erzielt werden kann:

Die Wirkung gegen Angriffe auf die sicherheitsrelevanten Daten im High-Level Security Modul kann nur mit einem Aufwand von weit über 5. Mio. EUR umgesetzt werden. Daher werden in dem High-Level Security Modul auch Master-Schlüssel und Schlüssel von globaler Bedeutung gespeichert.

Das bedeutet, wenn das High-Level Security Modul einer Bankanwendung geknackt wurde, ist die ganze Bankenanwendung kompromittiert und das ganze Banksystem kann nicht mehr sicher genutzt werden.

**Wichtig** High-Level Security Module (HLSM) bieten eine sehr hohe Wirkung gegen Angriffe auf die sicherheitsrelevanten Informationen und eignen sich für den Schutz von Master-Keys.

### 3.5 Zusammenfassung: Kategorien von Hardware-Sicherheitsmodulen

Bei Hardware-Sicherheitsmodulen ist es wichtig, dass die Software eine hohe Qualität hat und vertrauenswürdig ist, um die Angriffe zu minimieren. Es ist zudem besonders wichtig, dass die Software nur das tut, was sie soll, weil die sicherheitsrelevanten Informationen die Basis der Sicherheitsmechanismen darstellen.

Die Software in Hardware-Sicherheitsmodulen hat in der Regel eine geringe Anzahl von Zeilen Code, ca. 90.000 Lines of Code plus/minus 10 %. Durch die geringe Anzahl von Zeilen Code ist eine sehr vertrauenswürdige Basis vorhanden, die in der Regel auch schon semiformal verifiziert werden kann.

#### Restrisiko der unautorisierten Nutzung der Schlüssel im HSM

Alle sicherheitsrelevanten Operationen, wie zum Beispiel „Verschlüsseln“, „Signieren“, „Zufallszahlen und Schlüssel generieren“ usw. finden direkt im besonders geschützten Hardware-Sicherheitsmodul statt. Geheime Schlüssel können so benutzt werden, ohne dass sie das Hardware-Sicherheitsmodul verlassen müssen. Damit kann ein hoher Level an IT-Sicherheit erreicht werden.

Indirekter Angriff	Beschreibung
	Der Angreifer kann zwar die Schlüssel nicht auslesen, er könnte den Angriff aber so organisieren, dass er die angebotenen Sicherheitsfunktionen des Hardware-Sicherheitsmoduls unberechtigt nutzt. Dies kann zum Beispiel durch eine Malware erfolgen, die bei der Verwendung einer Smartcard oder eines USB-Sicherheitstokens nach der Aktivierung des HSMs die Sicherheitsdienste unberechtigt für Angriffe nutzt. Eine andere Möglichkeit ist, dass der Angreifer sich Zugang zu einem Server schafft, um ein aktiviertes HSM unberechtigt zu nutzen. Diese unberechtigte Nutzung muss aktiv durch weitere Cyber-Sicherheitsmechanismen verhindert werden.

### **3.6 Evaluierung und Zertifizierung für eine höhere Vertrauenswürdigkeit von Hardware-Sicherheitsmodulen**

Vertrauenswürdigkeit hat etwas mit Vertrauen zu tun. Aber welche Kriterien zur Beurteilung der Vertrauenswürdigkeit sollten bei Hardware-Sicherheitsmodulen angewendet werden?

Im Folgenden werden ein paar Prinzipien aufgezeigt, wie eine höhere Vertrauenswürdigkeit von Hardware-Sicherheitsmodulen erzielt werden kann.

#### **Evaluierung/Zertifizierung**

Hardware-Sicherheitsmodule werden in der Regel nach den folgenden Standards evaluiert und zertifiziert: FIPS 140–1 und 140–2, DK (Die Deutsche Kreditwirtschaft) oder Common Criteria (CC). Speziell für HSMs, die von Zertifizierungsdienstanbietern für die Erzeugung von digitalen Signaturen verwendet werden, wurde das CC Schutzprofil CWA 14167–2 entwickelt.

In der Praxis ist es so, dass die Hard- sowie die Software-Sicherheit durch eine Evaluierung/Zertifizierung nachgewiesen werden kann.

Bei der Evaluierung und Zertifizierung müssen unabhängige und qualifizierte Organisationen die Qualität und Vertrauenswürdigkeit von IT und IT-Sicherheit in Produkten und Lösungen prüfen.

Das Problem bei IT-Sicherheit, insbesondere Kryptografie, ist, dass diese nur von Experten evaluiert werden kann, weil es nicht um die Funktionalität geht, sondern um eine sichere Umsetzung der IT-Sicherheitsmechanismen. Dass eine Funktion ver- und entschlüsseln kann, heißt noch lange nicht, dass der dahinterliegende Algorithmus sicher ist. Weitere Fragestellungen sind: Erfüllt ein Zufallszahlengenerator alle notwendigen Eigenschaften, wie zum Beispiel Gütekriterien, Streuung, Periodizität, Gleichverteilung? Sind die Sicherheitsprotokolle sicher implementiert?

**Wichtig** Bei der Evaluierung und Zertifizierung müssen unabhängige und qualifizierte Organisationen die Qualität und Vertrauenswürdigkeit von IT und IT-Sicherheit in Produkten und Lösungen prüfen.

---

### **3.7 Key-Management von Hardware-Sicherheitsmodulen**

Das Besondere an Hardware-Sicherheitsmodulen für die Umsetzung eines Key-Managements sind die folgenden Aspekte:

- Keiner hat direkten Zugriff auf die geheimen Schlüssel.
- Nur autorisierte Entitäten sind in der Lage, die unterschiedlichen Krypto-Funktionen mit den geheimen Schlüsseln im Hardware-Sicherheitsmodul zu nutzen.
- Die Software im Hardware-Sicherheitsmodul kann nur von Autorisierten in ihrer Funktionalität definiert und verändert werden.

### 3.7.1 Das Management von TPMs

Der Hersteller von TPMs personalisiert diese in einer sicheren Umgebung mit einer sogenannten TPM-Identität. Die TPM-Identität ist ein Zertifikat mit einem Schlüsselpaar, dem Endorsement Key (EK), das das TPM niemals verlässt und die Eindeutigkeit und Einzigartigkeit des TPMs definiert.

Das Zertifikat mit dem öffentlichen Schlüssel wird von einer öffentlichen Public-Key-Infrastruktur verwaltet und ist damit direkt kryptografisch nutzbar.

Durch dieses Prinzip können Sicherheitssysteme, die auf der Basis von TPMs aufgebaut sind, sehr einfach aus der Ferne für bestimmte Anwendungen, wie zum Beispiel VPN-Systeme, sicher und vertrauenswürdig übernommen und individuell personalisiert werden. Das spart das übliche Personalisieren an einer gemeinsamen zentralen Stelle oder das Einbringen von Schlüsseln vor Ort durch vertrauenswürdiges Personal, was in der Regel sehr umständlich und teuer ist.

### 3.7.2 Vier-Augen-Prinzip

Das Vier-Augen-Prinzip besagt, dass kritische Tätigkeiten nicht von einer einzelnen Person durchgeführt werden dürfen. Ziel ist es, das Risiko von Fehlern und Missbrauch zu reduzieren.

Im Bereich von Key-Management kann dieses Prinzip mithilfe von Hardware-Sicherheitsmodulen unterstützt werden.

Anwendungsbeispiel: Electronic Cash System. Beim Electronic Cash System gibt es neben der Deutschen Kreditwirtschaft unterschiedliche Electronic Cash-Netzbetreiber mit eigenständiger Verantwortung. Diese betreiben Electronic Cash-Netze mit eigenen POS-Kartenterminals und HLSMs für den Übergang ins Netz der Deutschen Kreditwirtschaft.

Die Electronic Cash-Netze werden mit unterschiedlichen Schlüsselsystemen betrieben, um das Risiko bei einer Kompromittierung zu minimieren. Aus diesem Grund müssen an den Grenzen der Electronic Cash-Netze die verschlüsselten Transaktionen in die verschiedenen Schlüsselsysteme umverschlüsselt werden. Dazu treffen sich die Verantwortlichen der Electronic Cash-Netze, um jeweils die dazu notwendigen Schlüssel im Sinne des Vier-Augen-Prinzips einzugeben. Dadurch, dass der Sicherheitsmechanismus des Vier-Augen-Prinzips im HSM implementiert ist, kann dieser nicht manipuliert und das Risiko eines Missbrauchs kann deutlich reduziert werden.

---

## 3.8 Zusammenfassung

Die Nutzung der Kryptografie in der modernen Gesellschaft steigt ständig. Bezahl-systeme, zunehmend über das Internet, Verschlüsselung von Daten auf Datenträgern und während der Kommunikation, Mobilfunkverschlüsselung und Authentifikation, Wegfahrsperren im Auto usw. sind nur einige Beispiele dieses Trends.

Die dazu notwendigen Schlüssel, Software und Transaktionsdaten können in normalen IT-Systemen nicht angemessen geschützt werden. Aus diesem Grund werden Hardware-Sicherheitsmodule (HSMs) benötigt, die diese besonders sensiblen sicherheitsrelevanten Informationen angemessen schützen. Smartcards, TPMs und HLSM sind in der Lage, auf sehr unterschiedliche Art und Weise und mit unterschiedlichen Wirkungen des Schutzes, diese Aufgabe zuverlässig umzusetzen. Da Nutzer nicht in der Lage sind, die komplexen Aspekte des physikalischen Schutzes der sicherheitsrelevanten Informationen, die Kryptografie, die Generierung von Schlüsseln, die Implementierung der kryptografischen Algorithmen und ein sicheres Key-Management zu beurteilen, ist es unbedingt erforderlich, dass eine professionelle Zertifizierung der Hardware-Sicherheitsmodule auf einem angemessenen Evaluierungsniveau umgesetzt wird.

**Wichtig** Hardware-Sicherheitsmodule schützen sensitive sicherheitsrelevante Informationen angemessen und besonders sicher.

### 3.9 Übungsaufgaben

#### Übungsaufgabe 1

Entscheiden Sie für die folgenden Fälle, ob ein Trusted Platform Module (TPM), eine Smartcard, oder ein High-Level Security Modul (HLSM) eingesetzt werden sollte.

##### *Fall 1:*

In Ihrem Unternehmen haben Angestellte keinen festen Arbeitsplatz, da diese oft auf Dienstreise sind, und nutzen für ihre Arbeiten ein Notebook. Auf welchem Hardware-Sicherheitsmodul würden Sie die Schlüssel speichern, die Mitarbeiter für die Verschlüsselung von E-Mails verwenden?

Trusted Platform Module (TPM)  SmartCard  High-Level Security Modul (HLSM)

##### *Fall 2:*

Sie sind Sicherheitschef bei einer deutschen Bankengruppe. Die Bank nutzt zum Einsenden von sensiblen Kundendaten ein asymmetrisches Verschlüsselungsverfahren. Wo würden Sie den geheimen Schlüssel der Bank speichern, der für die Entschlüsselung der Dokumente genutzt wird?

Trusted Platform Module (TPM)  SmartCard  High-Level Security Modul (HLSM)

**Fall 3:**

In Ihrem Start-up arbeiten Ihre Mitarbeiter sehr flexibel und oft von unterwegs. Da die Mitarbeiter wichtige Firmendaten auf dem Notebook speichern, haben Sie sich entschlossen, die Festplatten der Notebooks zu verschlüsseln. Wo würden Sie den Schlüssel zur Entschlüsselung der Festplatte speichern?

Trusted Platform Module (TPM)  SmartCard  High-Level Security Modul (HLSM)

**Fall 4:**

Bei der Planung eines neuen Firmenstandorts sollen elektronische Schlüssel für alle Türen verwendet werden. Wo sollten die Schlüssel der Nutzer gespeichert werden, mit denen sie die Türen öffnen können?

Trusted Platform Module (TPM)  SmartCard  High-Level Security Modul (HLSM)

**Übungsaufgabe 2**

Welche Kategorie von Hardware-Sicherheitsmodul würde sich für ein Challenge-Response-Verfahren für Nutzer eignen?

Trusted Platform Module (TPM)  SmartCard  High-Level Security Modul (HLSM)

**Übungsaufgabe 3**

Welche Kategorie von Hardware-Sicherheitsmodul würde sich für ein Enterprise-Rights-Management-System auf Endsystemen eignen?

Trusted Platform Module (TPM)  SmartCard  High-Level Security Modul (HLSM)

**Übungsaufgabe 4**

Welche Kategorie von Hardware-Sicherheitsmodul würde sich für die Umsetzung einer Fernsignatur einer Bank eignen?

Trusted Platform Module (TPM)  SmartCard  High-Level Security Modul (HLSM)

**Übungsaufgabe 5**

Welcher Sicherheitsmechanismus eignet sich für das Aufbringen von sicherheitsrelevanten Informationen bei besonders kritischen Systemen?

## Übungsaufgabe 6

Bitte kreuzen Sie Ihre Antwort an!

	Cyber-Sicherheitsmechanismen
	Hardware-Sicherheitsmodul
Gewährleistung von Cyber-Sicherheitsbedürfnissen	Vertraulichkeit
	Authentifikation
	Authentizität
	Integrität
	Verbindlichkeit
	Verfügbarkeit
	Anonymisierung/ Pseudonymisierung
Cyber-Sicherheitsstrategien	Vermeiden von Angriffen
	Entgegenwirken von Angriffen
	Erkennen von Angriffen

Ergebnisse siehe: <https://norbert-pohlmann.com/cyber-sicherheit/uebungen/>.

---

## Literatur

1. Pohlmann N (2014) Hardware-Sicherheitsmodule zum Schutz von sicherheitsrelevanten Informationen. DuD Datenschutz Datensich – Recht und Sicherh in Informationsverarbeitung Kommun 38:661–665
2. Pohlmann N (1994) Security-API eines Sicherheits-Moduls für den Einsatz in heterogen Rechnerumgebungen. In Fumy W, Meister G, Reitenspiß M, Schäfer W (Hrsg) Proceedings der GI-Fachgruppe Verlässliche IT-Systeme Konferenz – Konzepte, Anwendungen und Einsatzbeispiele, Deutscher Universitätsverlag, 1994
3. Pohlmann N, Reimer H (2008) Trusted Computing – Ein Weg zu neuen IT- Sicherheitsarchitekturen. Vieweg, Wiesbaden
4. Pohlmann N (1995) Bausteine für die Sicherheit: Chipkarten und Sicherheits-Module, KES – Kommunikations- und EDV-Sicherheit, SecMedia, 05/1995
5. Pohlmann N (2001) Aktivierung von Smartcards durch Biometrie, KES – Kommunikations- und EDV-Sicherheit, SecMedia, 03/2001



# Digitale Signatur, elektronische Zertifikate sowie Public Key-Infrastruktur (PKI) und PKI-enabled Application (PKA)

4

In diesem Kapitel werden die Themen digitale Signatur, elektronische Zertifikate sowie Public Key-Infrastrukturen und PKI-enabled Application (PKA) behandelt. Diese Cyber-Sicherheitsprinzipien und Cyber-Sicherheitsmechanismen sind in einer modernen Informations- und Wissensgesellschaft von enormer Wichtigkeit und unterstützen dabei, zentrale Vertrauensdienste und ein modernes Schlüsselmanagement aufzubauen.

---

## 4.1 Digitale Signatur

In diesem Abschnitt werden die grundsätzliche Idee und die notwenigen Funktionen einer digitalen Signatur behandelt.

### Eigenhändige Unterschrift als Äquivalent zur digitalen Signatur

Um die grundsätzliche Idee der digitalen Signatur zu verstehen, sollen als erstes die Funktionen der eigenhändigen Unterschrift betrachtet werden.

Welche Bedeutung hat die eigenhändige Unterschrift, die Analogie zur digitalen Signatur? In Abb. 4.1 ist eine schriftliche Bestellung einer Waschmaschine zu finden.

#### Fragen, die bei einer eigenhändigen Unterschrift gestellt werden, sind:

- Welchen Wert hat eine eigenhändige Unterschrift?
- Wer hat etwas davon?
- Welche Bedeutung hat die eigenhändige Unterschrift?
- Welche Bedingungen müssen erfüllt sein, damit die Unterschrift einen Vorteil hat?

**Abb. 4.1** Schriftliche Bestellung einer Waschmaschine

<p>Dr. Gerd Müller Sonnenallee 100a 1000 Wohlfühlstadt</p> <p>Fachgroßhandel für Waschmaschinen Aachener Str. 70 50674 Köln</p> <p>Sehr geehrter Herr Maier,</p> <p>hiermit bestelle ich, auf der Grundlage Ihres Angebotes (Nr.345/11/17) vom 13.11.2017, bei Ihnen eine Waschmaschine im Wert von 650 Euro.</p> <p>Mit freundlichen Grüßen</p>  <p>Gerd Müller</p>	<p>02.01.2018</p>
---	-------------------

### Funktionen einer eigenhändigen Unterschrift

Die eigenhändige Unterschrift hat unterschiedliche Funktionen:

1. **Abschlussfunktion – Vollendung einer Erklärung – hebt sich vom Entwurf ab**  
Wenn etwas unterschrieben wird, ist das Dokument in der Regel vollendet, das heißt, die Inhalte sind ausgehandelt, gegenseitig bestätigt usw. Mit der eigenhändigen Unterschrift wird der Abschluss dieser Aktivitäten dokumentiert.
2. **Identitätsfunktion – Unterschrift macht die Identität des Ausstellers kenntlich**  
Die Unterschrift macht deutlich, welche Person unterschrieben hat und dafür verantwortlich zeichnet, was mit der eigenhändigen Unterschrift vereinbart wurde.
3. **Echtheitsfunktion – Dokument stammt vom Aussteller**  
Die Unterschrift dokumentiert den Aussteller und damit die Herkunft. Außerdem wird eine Überprüfung der eigenhändigen Unterschrift ermöglicht, was auch deren Echtheit beweist. Wenn es möglich ist, ergibt es Sinn, den Akt der eigenhändigen Unterschrift aktiv zu verfolgen, weil dann die Identitäts- und Echtheitsfunktionen einfach zu verifizieren sind. Wenn der Unterschriftenprozess schon mal durchgeführt wurde, kann die Unterschrift mit einer alten verglichen werden, oder es kann auch ein Gutachten angefertigt werden, das die Echtheit beweist.

**4. Warnfunktion – Schutz des Unterzeichners vor Übereilung**

Eine Unterschrift hat etwas Verbindliches, und aus diesem Grund leistet jemand nur eine Unterschrift, wenn er oder sie sich wirklich sicher ist. Jeder sollte sich bewusst sein, dass eine Unterschrift rechtsverbindlich ist und vorher gründlich abwägen, ob eine Unterschrift geleistet wird oder nicht.

**5. Beweisfunktion (Urkundenbeweis) – erleichtert die Beweisführung im Streitfall**

Eine eigenhändige Unterschrift gilt in Deutschland nach § 415 ZPO als Beweisfunktion und erweitert daher die Beweisführung im Streitfall.

**Digitale Signatur mithilfe eines Public Key-Verfahrens**

Im Folgenden werden die Funktionen betrachtet, die für die Erstellung und Verifikation einer digitalen Signatur notwendig sind:

**Signaturerstellung zu einer Nachricht m:**

$$s = S(m, GSA)$$

S Signaturfunktion, zum Beispiel RSA-Verfahren

m Nachricht, die signiert werden soll

s Signatur, zum Beispiel 3000 Bit Zeichenkette

GSA geheimer Schlüssel des Nutzers A, der die Nachricht signiert

**Verifikation der Signatur der Nachricht m:**

$$V(m, s, \ddot{O}SA) = \text{true?}$$

V Verifikationsfunktion

ÖSA öffentlicher Schlüssel des Nutzers A, der die Nachricht signiert hat

**One-Way-Hashfunktion: Was wird sonst noch für die digitale Signatur benötigt?**

Es wird eine einfache Möglichkeit benötigt, lange Nachrichten einfach signieren zu können. Die Gründe dafür sind vielfältig:

**1. Public Key-Verfahren haben eine relativ hohe Verarbeitungszeit für eine Operation**

Wenn eine Nachricht von 100 M Byte signiert werden soll und das RSA-Verfahren mit einer Schlüssellänge von 2048 Bit verwendet wird, müssen ca. 400.000 Operationen durchgeführt werden. Dies ist notwendig, da die in einem Schritt zu signierende Nachricht m kleiner als der Schlüssel sein muss (2048 Bit) und die eigentliche Nachricht 100 M Byte groß ist.

Wenn eine RSA-Operation 0,1 s dauern würde, werden ca. 11 h dafür benötigt.

## 2. Die Zusammengehörigkeit von Einzelsignaturen ist nicht gegeben

Wenn 400.000 Signatur-Operationen mit 2000 Bit-Teilen der Nachrichten durchgeführt werden, sind im Prinzip als Ergebnis nur Einzelsignaturen vorhanden, deren Zusammenhang nicht nachgewiesen werden kann.

Als Lösung dieser Herausforderung wird eine **One-Way-Hashfunktion** (siehe Abschn. 2.4) genutzt, mit der ein Hashwert der ganzen Nachricht berechnet wird und anschließend wird nur dieser Hashwert signiert, siehe die angepasste Verifikationsfunktion AV:

$$\text{AV} (h_m = H(m), s, \ddot{\text{O}}\text{SA}) = \text{true}$$

$h_m$  Hashwert der Nachricht m

H One-Way-Hashfunktion

AV Angepasste Verifikationsfunktion

Die Vorteile dieser Vorgehensweise sind:

1. Es können beliebig lange Nachrichten einfach signiert werden, es ist immer nur eine Signatur von einem Hashwert notwendig.
2. Die notwendige Zeit für eine Signatur über längere Nachrichten wird deutlich kleiner.
3. Die Bindung der Nachricht mithilfe der Hashfunktion an die digitale Signatur gewährleistet die Integrität der ganzen Nachricht, das heißt, jedes Bit der Nachricht ist in die digitale Signatur eingeschlossen!

Dies hat gegenüber der eigenhändigen Unterschrift auf der letzten Seite eines langen Dokumentes den Vorteil, dass alle Informationen immer eingeschlossen sind und eine Manipulation nicht möglich ist.

**Wichtig** Jedes Bit einer Nachricht ist mithilfe einer One-Way-Hashfunktion in die digitale Signatur eingeschlossen.

## Elektronische Zertifikate: Was wird zusätzlich noch für die digitale Signatur benötigt?

Ein Problem mit öffentlichen Schlüsseln ist, dass sie zwar tatsächlich öffentlich sein können und in der Regel auch sind, sich aber „mit bloßem Auge“ nicht feststellen lässt, ob sie wirklich vom angegebenen Nutzer stammen [1].

Für die Verifikation der Signatur ist noch die Gewährleistung der Authentizität des öffentlichen Schlüssels unabdingbar. Die Gewährleistung der Authentizität des öffentlichen Schlüssels und weiteren, dem Nutzer zugeordneten Eigenschaften und Attribute werden mithilfe von elektronischen Zertifikaten umgesetzt, deren Funktionsweise im nächsten Abschnitt beschrieben wird.

## 4.2 Elektronische Zertifikate/digitale Zertifikate

Zur Gewährleistung der Authentizität des öffentlichen Schlüssels und weiteren Attributen, helfen elektronische Zertifikate, mit denen genau überprüft werden kann, ob ein öffentlicher Schlüssel und weitere Attribute zu einem bestimmten Nutzer gehören.

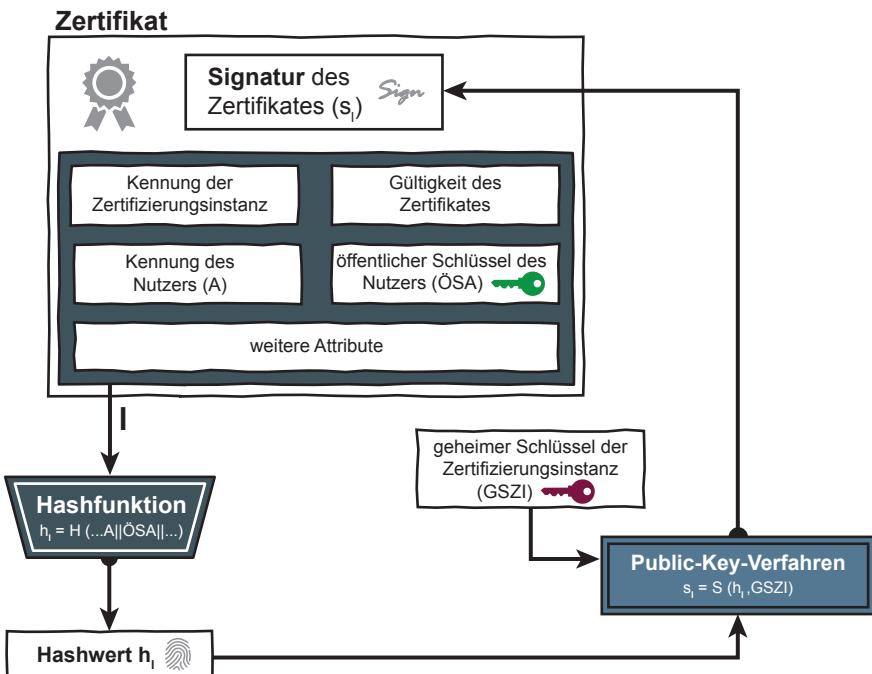
Bei elektronischen Zertifikaten handelt es sich um elektronische Dokumente, die den Public Key des Nutzers sowie weitere Angaben wie Kennung des Nutzers, Gültigkeit des Zertifikates, Kennung einer Zertifizierungsinstanz und andere Attribute, wie zum Beispiel Ausbildung, Kreditrahmen usw., enthalten. Ein Zertifikat ist demnach „das Äquivalent“ zu einem Personalausweis oder Reisepass in der realen Welt, mit dessen Hilfe der Staat die Identität und weitere Attribute der Bürger bestätigt.

**Wichtig** Mithilfe von elektronischen Zertifikaten können Attribute von Nutzern überprüfbar nachgewiesen werden.

Ausgestellt werden elektronische Zertifikate durch eine Zertifizierungsinstanz. Diese prüft die Angaben des Nutzers, seine Identität und weitere Attribute bei Vorlage von Ausweisen und Urkunden. Als Zertifizierungsinstanz kommen spezialisierte Anbieter für Vertrauensdienste infrage oder Berufsverbände, wie zum Beispiel von Notaren, Steuerberatern/Wirtschaftsprüfern, Ärzten/Krankenschwestern/Hebammen usw., aber auch Personal- und IT-Abteilungen von Unternehmen oder einer Behörde. Es werden alle Attribute des Zertifikats, aber auch die Informationen über den Aussteller signiert. Zweck ist, die Authentizität der Inhalte zu gewährleisten und das Zertifikat vor Manipulation zu schützen. Als allgemeinverbindlicher Standard hat sich der ITU-Standard X.509 für Zertifikate durchgesetzt.

### Erstellung und Verifizierung von Zertifikaten

Der öffentliche Schlüssel (Public Key) eines jeden Nutzers wird in Form eines elektronischen Zertifikats zur Verfügung gestellt. Das elektronische Zertifikat enthält mindestens die Kennung der Zertifizierungsinstanz (ZI), die Kennung des Nutzers (A), den öffentlichen Schlüssel des Nutzers (ÖSA) und eine Angabe zur Gültigkeitsdauer sowie Lebensdauer des elektronischen Zertifikates. Weitere Attribute können sein: Position und Rechte in einem Unternehmen, Ausbildungen wie Bachelor- und Masterabschlüsse usw., siehe Abb. 4.2.



**Abb. 4.2** Inhalt und Erstellung eines Zertifikats für den Nutzer A

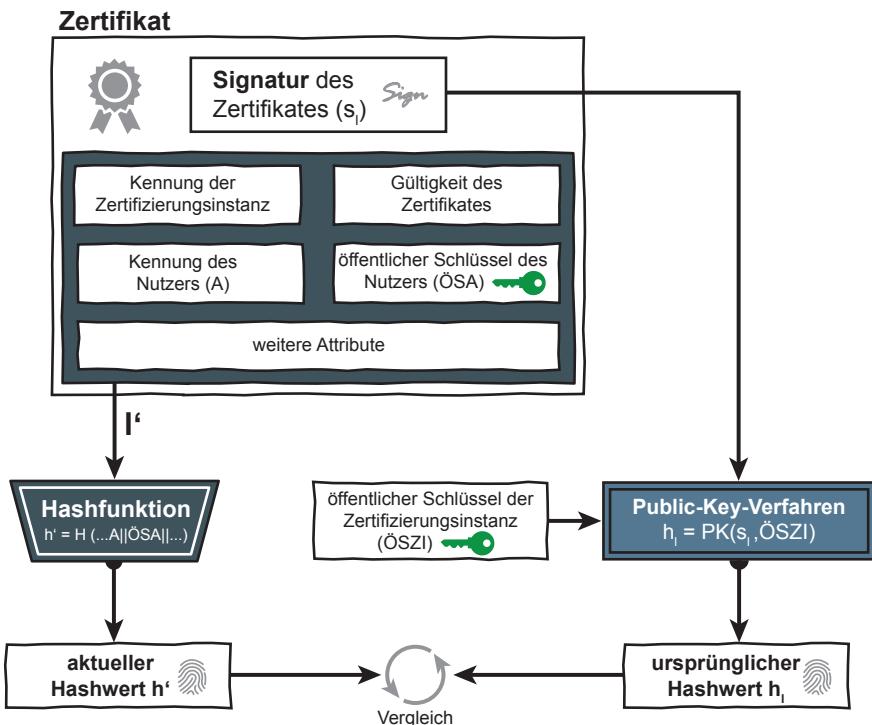
H: One-Way-Hashfunktion, S: Signaturfunktion

Das elektronische Zertifikat ist von der erstellenden Zertifizierungsinstanz digital signiert. Die Signatur des Zertifikates ist  $s_i = S(h_i, GSZ)$ .  $h_i$  ist der gerade berechnete Hashwert über alle Informationen des Zertifikates. GSZ ist der geheime Schlüssel der Zertifizierungsinstanz.

**Wichtig** Die Zertifizierungsinstanz bestätigt mithilfe eines Zertifikates, dass ein öffentlicher Schlüssel und die weiteren Attribute tatsächlich zu einem bestimmten Nutzer gehören.

Jeder, der den öffentlichen Schlüssel der Zertifizierungsinstanz besitzt (ÖSzi), kann überprüfen, ob der öffentliche Schlüssel eines Nutzers (ÖSA) und weitere Attribute wirklich von der Zertifizierungsinstanz bestätigt worden sind. Mit anderen Worten: Die Zertifizierungsinstanz bestätigt mithilfe eines Zertifikates, dass ein öffentlicher Schlüssel (ÖSA) und die weiteren Attribute tatsächlich zu einem bestimmten Nutzer gehören.

Zur Verifikation des Zertifikates wird zum einen der aktuelle Hashwert  $h' = H(\dots A || ÖSA || \dots)$  über den aktuellen Inhalt des Zertifikates berechnet. Wenn das Zertifikat nicht mehr das Original ist, ist der aktuelle Hashwert auch



**Abb. 4.3** Verifikation eines Zertifikates; H: One-Way-Hashfunktion, PK: Public Key-Verfahren

nicht mehr gleich mit dem ursprünglichen Hashwert  $h_i$ . Daher wird zum anderen aus der Signatur des Zertifikats und dem öffentlichen Schlüssel der Zertifizierungsinstanz (ÖSzi) unter Verwendung des Public Key-Verfahrens der ursprüngliche Hashwert  $h_i = PK(s_i, ÖSzi)$  berechnet. Stimmen beide Hashwerte überein, sind die Unversehrtheit des Zertifikates und die Echtheit des öffentlichen Schlüssels des Nutzers bewiesen, siehe Abb. 4.3.

Voraussetzung ist, dass alle Nutzer des Sicherheitssystems der Zertifizierungsinstanz vertrauen. Daher muss eine Zertifizierungsinstanz bestimmten Sicherheitsanforderungen genügen. Dazu zählen unter anderem vertrauenswürdiges Personal, zertifizierte Sicherheitskomponenten und eine vertrauenswürdige Systemumgebung usw.

Um die Verifikation eines Zertifikates durchführen zu können, wird der authentische öffentliche Schlüssel der Zertifizierungsinstanz (ÖSzi) benötigt. In der Praxis stellt die Beschaffung des öffentlichen Schlüssels der Zertifizierungsinstanz (ÖSzi) eine große Aufgabenstellung dar.

Eine Möglichkeit ist die Nutzung eines sogenannten Wurzelzertifikats (engl. Root Certificate). Dabei handelt es sich um ein selbst signiertes Zertifikat, das den öffentlichen Schlüssel der Zertifizierungsinstanz enthält. Wurzelzertifikate sind besonders sensibel und haben einen hohen Schutzbedarf. Gelänge es einem Angreifer, auf einem IT-System ein falsches Wurzelzertifikat unterzubringen,

wären die Nutzer dieser Systeme Betrügern, die sich dies zunutze machen, schutzlos ausgeliefert. Daher werden Betriebssysteme und Webbrower bereits mit den gängigsten Wurzelzertifikaten ausgeliefert. Die Anbieter haben Auflagen zu erfüllen, die die Vertrauenswürdigkeit festigen.

Eine andere Möglichkeit ist, dass der Zertifizierungsanbieter den eigenen öffentlichen Schlüssel zum Beispiel mithilfe eines Sicherheitsmoduls, Smartcard, USB-Token usw. bei einem persönlichen Treffen übergibt.

### Fazit

Digitale Signaturen sollen im elektronischen Geschäftsverkehr die eigenhändige Unterschrift ersetzen. Dabei bieten sie zweierlei Vorteile: Sie bestätigen zum einen die Identität eines Nutzers und zum anderen schützen sie auch die Nachricht selbst gegen nachträgliche Manipulationen. Damit das funktioniert, müssen sie sich in der Praxis jederzeit auf ihre Echtheit kontrollieren lassen. Dabei helfen einerseits One-Way-Hashfunktionen, mit denen sich für jede Nachricht spezifische Hashwerte bilden lassen, und andererseits elektronische Zertifikate, die bestätigen, dass der mit der Signatur übermittelte öffentliche Schlüssel auch tatsächlich zum entsprechenden Nutzer gehört. One-Way-Hashfunktionen und Zertifikate sind daher zentrale Bestandteile moderner Cyber-Sicherheitssysteme.

**Wichtig** Digitale Signaturen stellen die Integrität und Authentizität einer Nachricht sicher.

## 4.3 Public Key-Infrastrukturen

Eine Public Key-Infrastruktur (PKI) ist eine Infrastruktur zur Verwaltung von Identitäten, Schlüsseln, Zertifikaten, Attribute usw. [2].

Zertifikate sind eine von einer Ausgabestelle signierte Sammlung, bestehend aus persönlichen Informationen/Attributen über Nutzer und deren öffentliche Schlüssel. Darüber hinaus enthalten sie Angaben zu den für die Signatur verwendeten kryptografischen Algorithmen und One-Way-Hashfunktionen sowie zu ihrer eigenen Gültigkeit und zum Herausgeber. Mithilfe des öffentlichen Schlüssels einer Zertifizierungsstelle kann die Echtheit eines Zertifikats und seiner Inhalte verifiziert werden. Dadurch lässt sich in modernen IT-Systemen im Prinzip ein einfaches und organisationsübergreifendes Key Management realisieren. Durchgesetzt haben sich Zertifikate nach dem Standard X.509 der International Telecommunication Union (ITU).

**Wichtig** Mithilfe von PKIs lässt sich in modernen IT-Systemen ein einfaches und organisationsübergreifendes Key Management realisieren.

### 4.3.1 Idee und Definition von Public Key-Infrastrukturen

Public Key-Infrastrukturen (PKI) dienen zum Verwalten von Zertifikaten mit öffentlichen Schlüsseln und weiteren Attributen über deren gesamten Lebenszyklus, von der Erstellung über die Aufbewahrung und Verwendung bis hin zur Löschung. Dabei kommt es, außer auf die sichere Erstellung und Speicherung gültiger Schlüssel, auch auf die Verifizierung der ursprünglichen Identität ihrer Inhaber – der PKI-Nutzer – an.

Public Key-Infrastrukturen bestehen aus Hardware, Software und einem abgestimmten Regelwerk, der Leitlinie. Diese definiert, nach welchen Sicherheitsregeln die Dienstleistungen um die Zertifikate erbracht werden. Dazu zählen das Betriebskonzept der PKI, die Nutzerrichtlinien sowie Organisations- und Arbeitsanweisungen.

Im Allgemeinen ist es üblich, die Registrierung der Nutzer und die Zertifizierung der Schlüssel voneinander zu trennen und zum Teil auch an unterschiedlichen Orten vorzunehmen.

#### Standesamt und Einwohnermeldeamt als Analogie zu Public Key-Infrastrukturen

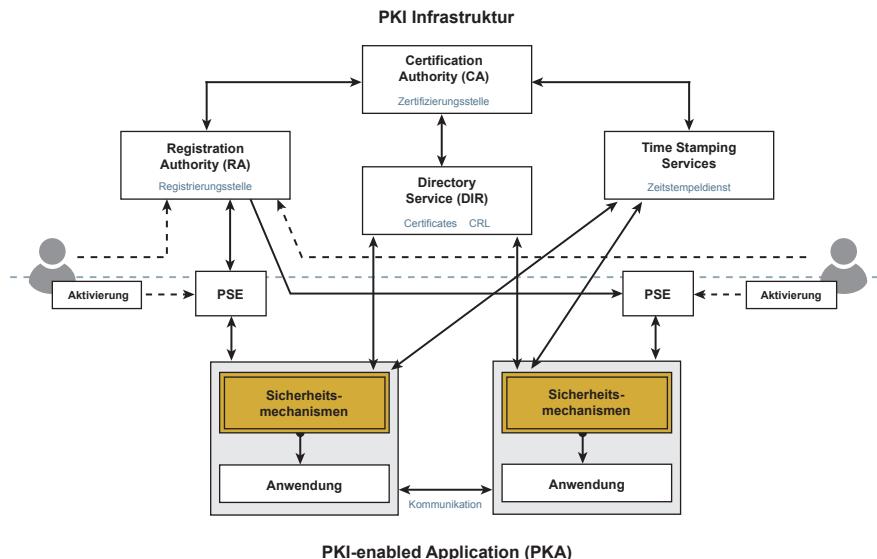
Standes- und Einwohnermeldeämter sichern die eindeutige und überprüfbarre Identität von Personen. Sie fungieren demnach als dritte Instanz, der vertraut wird. Das Standesamt sorgt dafür, dass über Vor- und Nachnamen, den Geburtsort und das Geburtsdatum jede Person eindeutig weltweit identifizierbar ist, erledigt also die Aufgaben einer Registrationsstelle. Das Einwohnermeldeamt gibt Ausweise heraus, die es ermöglichen, diese eindeutige Identität zweifelsfrei zu beweisen und fungiert mit hin als Zertifizierungsstelle.

#### Einsatz und Anwendungsformen

Eine PKI stellt zentrale Sicherheitsdienste beziehungsweise Vertrauensdienste zur Verfügung, schafft also die Voraussetzungen dafür, dass eine Anwendung dadurch vertrauenswürdig realisiert werden kann. Abb. 4.4 zeigt im oberen Teil den prinzipiellen Aufbau einer Public Key-Infrastruktur sowie einige Kommunikationskanäle, die dabei benutzt werden. Im unteren Bereich ist schematisch eine Anwendung abgebildet, deren Sicherheitsmechanismen die Public Key-Infrastruktur-Dienste nutzen.

Im Folgenden werden die Funktionseinheiten und Dienste einer PKI beschrieben:

**Registration Authority (RA)** Die Registration Authority (RA) oder auch Registrierungsstelle kann als private oder öffentliche Einrichtung betrieben werden, das heißt, es kommen Berufsverbände, Unternehmen, Behörden und öffentliche Dienstanbieter infrage. Die Hauptaufgabe einer RA besteht darin, die Anträge auf Zertifizierung zu erfassen und die Identität der Antragsteller entsprechend der Leitlinie zu prüfen. Dies kann sehr einfach erfolgen, indem sie zum Beispiel um die Verifikation einer E-Mail-Adresse bittet, oder auch aufwendiger



**Abb. 4.4** Aufbau und Funktionsweise einer Public Key-Infrastruktur (Schema)

und sicherer, indem sie vom Antragsteller persönliches Erscheinen und die Vorlage des Ausweises verlangt. Weitere Möglichkeiten der Verifizierung von Nutzern sind die Nutzung der eID-Funktion des elektronischen Personalausweises oder mithilfe von VideoIdent-Verfahren. Die RA bildet die Schnittstelle zwischen dem PKI-Nutzer und der Certification Authority (CA), an die sie dessen Anträge weiterleitet.

**Wichtig** Eine Registration Authority (RA) bildet die Schnittstelle zum Nutzer und hat die Aufgabe, die Identität des Nutzers zu verifizieren.

**Certification Authority (CA)** Die Certification Authority (CA) oder auch Zertifizierungsstelle vergibt eindeutige digitale Identitäten, erzeugt die Zertifikate und verwaltet für jeden Nutzer ein oder mehrere Schlüsselpaare mit den dazugehörigen Zertifikaten. Jedes von ihr erzeugte Zertifikat verbindet den öffentlichen Schlüssel des Nutzers mit dessen Namen und zusätzlichen Daten (Gültigkeitszeitraum, Seriennummer, eventuell weiteren Attributen). Die Certification Authority gibt die Zertifikate aus und verwaltet sie, damit die öffentlichen Schlüssel und Attribute der Nutzer (Position im Unternehmen, Ausbildungen, Kreditrahmen usw.) möglichst einfach verifiziert werden können.

**Wichtig** Eine Certification Authority (CA) erzeugt und verwaltet die Zertifikate für die Nutzer.

**Directory Service (DIR)** Zur Verwaltung der Zertifikate unterhält jede PKI einen Directory Service (DIR) oder auch Verzeichnisdienst. Hier werden die gültigen zertifizierten öffentlichen Schlüssel der Nutzer als Zertifikate veröffentlicht und sind damit für jeden, der die Inhalte überprüfen möchte, abrufbar.

**Certificate Revocation List (CRL)** Zurückgezogene oder kompromittierte Schlüssel/Zertifikate hält der Verzeichnisdienst in einer Sperrliste oder auch Certificate Revocation List (CRL) zum Abruf bereit. Die Zertifikate haben zwar eine Lebensdauer, wenn aber innerhalb dieser Lebensdauer ein Problem auftritt, kann das Zertifikat in der Sperrliste aufgeführt werden. Daher sollte vor jeder Verifikation eines Zertifikates überprüft werden, ob dieses nicht gesperrt worden ist.

**Time Stamping Service** Ein Time Stamping Service oder auch Zeitstempeldienst dient dazu, gesicherte Zeitsignaturen gemäß der Leitlinie zu erstellen. Dabei wird ein Dokument oder eine Transaktion, zum Beispiel der Eingang einer E-Mail, mit der aktuellen Zeitangabe verknüpft und diese Gesamtinformation anschließend digital signiert. Mit dem Zeitstempeldienst kann dann zum Beispiel ein zu spät eingereichtes Angebot über E-Mail rechtssicher dokumentiert werden.

**Personal Security Environment (PSE)** Das Personal Security Environment (PSE) ist die Sammlung aller sicherheitsrelevanten Daten eines Teilnehmers. Dazu gehören der geheime Schlüssel des Nutzers, der öffentliche Schlüssel der Zertifizierungsinstanz und eventuell auch die Zertifikate seiner Kommunikationspartner. Die folgenden Formen kann ein Personal Security Environment annehmen: Software, Smartcards, USB-Token, allgemeine Sicherheits-Module, SIM-Karte im Smartphones, TPM usw., siehe auch Kap. 3.

Indirekter Angriff	Beschreibung
	<p>Wenn eine PKI sicher und vertrauenswürdig umgesetzt wird, kann eine hohe Wirkung der darauf aufbauenden Anwendungen erzielt werden. Der Angreifer kann aber versuchen, an den Schlüssel zu gelangen, wenn dieser nicht sicher gespeichert ist. Aus diesem Grund werden in der Regel Smartcards oder USB-Sicherheitstokens verwendet. Auch wenn der Angreifer die Schlüssel nicht auslesen kann, könnte er den Angriff so organisieren, dass er die angebotenen Sicherheitsfunktionen der Smartcards oder des USB-Sicherheitstokens unberechtigt nutzt. Dies kann zum Beispiel durch eine Malware erfolgen, die er bei der Verwendung einer Smartcard oder eines USB-Sicherheitstokens nach der Aktivierung die Sicherheitsdienste unberechtigt für Angriffe nutzt. Aus diesem Grund sollte für die Smartcard oder USB-Sicherheitstoken ein externes Lesegerät und eine externe Tastatur verwendet werden, um solche Angriffe zu verhindern.</p>

## **Lesegeräte für Smartcards**

Es können drei Kategorien an Lesegeräten unterschieden werden, die einen unterschiedlichen Level an Sicherheit und damit an Wirkung gegen Angriffe zur Verfügung stellen:

### **1. Basisleser**

Der Basisleser hat keine Tastatur und auch keine Anzeige. Die Anzeige und Eingabe wird über das IT-System, zum Beispiel Notebook des Nutzers umgesetzt. Damit kann mithilfe einer Malware die PIN abgehört und die Sicherheitsfunktionen nutzbar gemacht werden.

Ein Basisleser kann nur dann verwendet werden, wenn sichergestellt werden kann, dass über das IT-System nicht angegriffen werden kann.

### **2. Standardleser**

Der Standardleser hat eine Tastatur und auch eine Anzeige. Dadurch kann die PIN im Standardleser und muss nicht auf einem potenziell unsicheren Notebook eingegeben werden.

Voraussetzung für die Höhe der Sicherheit ist die Vertrauenswürdigkeit der Software im Standardleser.

### **3. Komfortleser**

Der Komfortleser ist wie der Standardleser, nur wird hier eine Zertifizierung umgesetzt, um einen höheren Level an Sicherheit garantieren zu können.

## **PKI-enabled Application (PKA)**

Als PKI-enabled Application (PKA) wird eine Anwendung bezeichnet, die auf Grundlage der durch die PKI zur Verfügung gestellten Sicherheitsdienste (Zertifikate, Verzeichnisdienst, Zeitstempeldienst etc.), eine vertrauenswürdige Umsetzung ermöglicht. Eine PKA enthält selbst unterschiedliche Sicherheitsmechanismen (für Authentisierung, Verschlüsselung, Signatur usw.), mit denen Vertrauenswürdigkeit (Authentizität, Integrität, Verbindlichkeit, Einmaligkeit und Vertraulichkeit) erzielt wird.

Eine PKI bildet die Sicherheitsgrundlage für die vertrauenswürdige Nutzung von Anwendungen (PKI-enabled Application) wie:

- E-Mail,
- Dokumentverschlüsselung (Word, Excel, PowerPoint, ...),
- Transaktionen (in EDIFACT, XML oder andere Formate)
- Programme für Online-Banking und Online-Broking,
- SSL/TLS-Kommunikation,
- IPSec-Kommunikation,
- Identifikations- und Authentisierungsprozesse,
- Zahlungssysteme,
- Sicherheitsdomänen, die auf Trusted Computing aufbauen,
- der elektronische Personalausweis
- und weitere.

**Tab. 4.1** Gegenüberstellung von Cyber-Sicherheitsbedürfnissen und Cyber-Sicherheitsmechanismen

Cyber-Sicherheitsbedürfnisse		Cyber-Sicherheitsmechanismen
Authentizität	→	Signatur
Integrität	→	Signatur
Verbindlichkeit	→	Signatur
Einmaligkeit	→	TimeStamp
Vertraulichkeit	→	Verschlüsselung

### Ziele von PKIs und PKAs

Mit der Hilfe von PublicKey-Infrastrukturen (PKIs) und PKI-enabled Application (PKAs) soll mehr Vertrauenswürdigkeit in den Geschäftsprozessen umgesetzt werden.

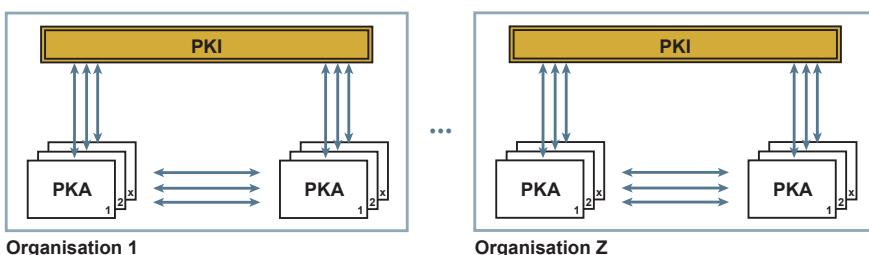
In Tab. 4.1 werden die IT-Sicherheitsbedürfnisse und IT-Sicherheitsmechanismen gegenübergestellt.

### 4.3.2 Offene und geschlossene PKI-Systeme

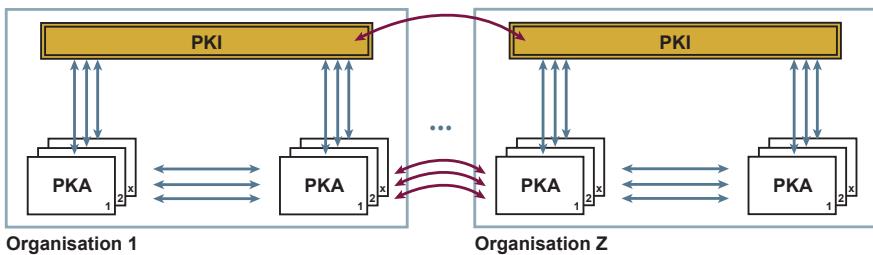
In diesem Abschnitt werden offene und geschlossene sowie dezentrale und zentrale Public Key-Infrastrukturen (PKIs) diskutiert.

**Geschlossene und dezentrale PKI-Systeme** Ein geschlossenes und dezentrales PKI-System betreibt eine Organisation, wenn sie ihre PKI für eine oder mehrere Anwendungen (PKAs) nutzt, die vollständig in ihrem eigenen Verantwortungsbereich liegen, siehe Abb. 4.5.

Cyber-Sicherheitsdienste, wie zum Beispiel gesicherte Kommunikation oder Authentisierung, stehen dann nur innerhalb der eigenen Infrastruktur zur Verfügung.



**Abb. 4.5** Geschlossene PKI-Systeme



**Abb. 4.6** Offene PKI-Systeme

**Offene und dezentrale PKI-Systeme** Im Alltag werden offene PKI-Systeme bevorzugt: Dabei betreiben mehrere Organisationen jeweils eigene PKIs für eine oder mehrere Anwendungen, die in ihren Verantwortungsbereichen liegen, siehe Abb. 4.6.

So ist zum Beispiel die gesicherte Kommunikation zwischen den Nutzern des offenen Systems möglich. Der Austausch beruht auf gegenseitigem Vertrauen sowie auf kompatiblen Technologien und Verfahren.

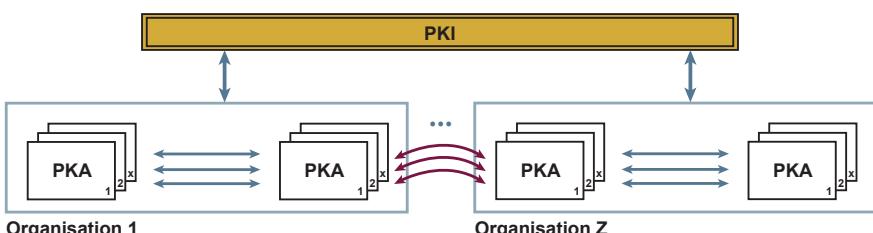
**Offene, zentrale PKI-Systeme** Ein PKI-Anbieter betreibt die PKI für eine oder mehrere Anwendungen, die in den jeweiligen Verantwortungsbereichen der darauf zurückgreifenden Organisationen liegen. Wenn die verschiedenen Organisationen der zentralen PKI vertrauen und kompatible Technologien beziehungsweise Verfahren verwenden, kann eine vertrauenswürdige Kommunikation zwischen den Organisationen realisiert werden, siehe Abb. 4.7.

**Probleme in der Praxis** Bei der Nutzung von PKI-Systemen gibt es immer wieder Herausforderungen, die im Folgenden diskutiert werden.

#### A) Probleme bei geschlossenen PKI-Systemen

Ein geschlossenes PKI-System bedeutet, dass die PKI-Dienstleistungen nur innerhalb einer Organisation verwendet und nicht für die Kommunikation nach außen genutzt werden können.

Da jedoch in der Praxis viele organisationsübergreifende Prozesse stattfinden, schränkt dies ihren Nutzen sehr stark ein.



**Abb. 4.7** Zentral administriertes PKI-System

**B) Probleme bei offenen PKI-Systemen**

Bei offenen PKI-Systemen muss zum Aufbau einer organisationsübergreifenden Kommunikation ein Abgleich der verschiedenen organisationspezifischen Leitlinien erfolgen. Ziel ist die Schaffung einer gemeinsamen, verbindlichen Vertrauensbasis (Level of Trust). Hier sind geeignete Instrumente zu implementieren, um die unterschiedlichen organisatorischen und infrastrukturellen Konzeptionen zu bewerten, zu analysieren und zu gewichten. Gerade bei der Nutzung für personenbezogene organisationsübergreifende Prozesse ist es aus ökonomischer Sicht und aus den tatsächlichen Anforderungen heraus sehr gut, dass die eIDAS-Verordnung die Grundlage und Rahmenbedingungen für Vertrauensdienst bereitstellen.

Es ist auch zu berücksichtigen, dass viele organisationsübergreifende Prozesse automatisiert sind und somit nicht mehr personenbezogen ablaufen. Eine weitere Herausforderung ist, dass eine Vielzahl unterschiedlicher, teilweise sehr komplexer Standards für den Aufbau von PKIs existiert, die ständig weiterentwickelt werden. Die Ursache hierfür liegt in der großen Vielfalt der Anwendungen (SSL/TLS, E-Mail etc.), die mit ihrer Hilfe abgesichert werden, und den daraus resultierenden Anforderungen.

**C) Unterschiedliche Verantwortung für PKIs und PKAs in Unternehmen**

Ein weiteres Problem, dem insbesondere große Organisationen gegenüberstehen, besteht darin, dass die PKAs und PKIs zwar voneinander abhängig sind, die Zuständigkeit für Entwicklung und Verwaltung der PKI und der PKAs aber häufig organisatorisch getrennt wird. In solchen Fällen müssen sich dann verschiedene Abteilungen auf gemeinsame Ziele und Vorgehensweisen verstndigen, um die entsprechenden technischen Grundlagen zu erarbeiten.

**D) Henne-Ei-Problem**

Public Key-Infrastrukturen sind nur dann ökonomisch sinnvoll, wenn der Einsatz dieser Strukturen und damit der vertrauenswürdige Ablauf von Geschäftsprozessen so umfassend wie möglich realisiert werden, das heißt, wenn die gesicherte Kommunikation mit so vielen Partnern wie möglich stattfinden kann. Voraussetzung dafür ist der konsequente Einsatz der bestehenden Technologien und die Umsetzung der Security-Leitlinien.

Die Realität ist aber, dass sich die beteiligten Organisationen nur schwer auf den Abgleich ihrer individuellen Cyber-Sicherheitskonzepte einigen können. Dadurch gestaltet sich der Aufbau eines gemeinsamen „Level of Trust“ langwierig, und längst fällige Entscheidungen werden nicht getroffen.

**E) Hoher personeller und organisatorischer Aufwand**

Die Einführung und der Betrieb einer Public Key-Infrastruktur erfordern neben der technischen Umsetzung auch einen hohen personellen und organisatorischen Aufwand. Gerade in der Einführungsphase einer PKI sind die Sensibilisierung der Nutzer für die Cyber-Sicherheit, die Schulung der Nutzer für die Produkte und die Planung und Durchführung des Rollout nicht zu vernachlässigende Faktoren.

## F) Key-Recovery bei der Verschlüsselung

Wenn Unternehmenswerte verschlüsselt werden, muss ein Verfahren realisiert werden, das bei technischen Defekten, bei einem PSE-Verlust oder beim Ausscheiden eines Mitarbeiters aus dem Unternehmen garantiert, dass die Unternehmenswerte sicher wieder entschlüsselt werden können.

### 4.3.3 Umsetzungskonzepte von Public Key-Infrastrukturen

Neben der Bereitstellung der notwendigen Technologien und der weitgehenden Lösung der Interoperabilitäts-Problematik sollte der Blick konsequent auf die tatsächlichen Anforderungen gerichtet werden. Pragmatische Ansätze sind gefragt, um die Einführung von Public-Key-Infrastrukturen zu beschleunigen.

Die folgenden vier Kernsätze können als Grundlage für die erfolgreiche Realisierung eines PKI-Systems gelten:

1. Verschiedene Anwendungen haben unterschiedliche Cyber-Sicherheitsbedürfnisse.
2. Unterschiedliche Cyber-Sicherheitsbedürfnisse lassen sich isoliert einfacher verwirklichen.
3. Isolierte Lösungen haben einen klaren Fokus.
4. Ein klarer Fokus verringert die auftretenden Probleme und ermöglicht eine schnellere, einfachere und kostengünstigere Umsetzung.

Im Folgenden werden einige Umsetzungskonzepte exemplarisch dargestellt.

**Umsetzungskonzept „TLS/SSL“** Bei nahezu allen Webanwendungen lautet eine explizite Vertrauensanforderung, die Kommunikation zwischen Client und Server vertraulich zu gestalten, damit die ausgetauschten Daten weder mitgelesen noch manipuliert werden können.

Alle hierfür notwendigen Voraussetzungen sind gegeben, die technische Infrastruktur ist bereits vorhanden: Web-Server sind für die TLS/SSL-Verschlüsselung vorbereitet, Clients (Browser) unterstützen den Standard und mehrere hundert PKIs stehen zur Verfügung. Dem Markt stehen etablierte TLS/SSL-Bibliotheken als Open Source zur Verfügung und auch TLS/SSL-Accelerator-Lösungen für die Beschleunigung der gesicherten Verbindung stehen bereit. Diese PKI-Anwendung hat sich etabliert, 2018 wurden schon mehr als 80 % der IP-Pakete mit TLS/SSL im Internet verschlüsselt, siehe auch Kap. 11 „Transport Layer Security (TLS)/Secure Socket Layer (SSL)“.

**Umsetzungskonzept „E-Mail-Sicherheit“** Zu schützende Unternehmensdaten sollen personenorientiert und vertraulich ausgetauscht werden. Das bedeutet, dass das gegenseitige Wissen um die Identität der Kommunikationspartner von zentraler Bedeutung ist. Insbesondere wenn via E-Mail Prozesse mit nachfolgenden Kosten (Bestellungen, Wareneinkauf, ...) ausgelöst werden, liegt die Verbindlichkeit im Interesse der Unternehmen.

Mailprogramme sind den Nutzern bekannt und vertraut. Sicherheitsrelevante Funktionen müssen so eingepasst werden, dass der Nutzer sich nur einem Mindestmaß an neuen Funktionalitäten gegenübersieht und jederzeit Klarheit über die nötigen Arbeitsschritte und ihre Folgen hat. Die Anwendung der Nutzer, das heißt, die Einhaltung der Cyber-Sicherheitskonzepte, sollte so einfach wie möglich gehalten werden. Dies ist eine Voraussetzung dafür, dass der Nutzer seine aktive Rolle (im Gegensatz zur passiven Rolle bei der gesicherten SSL-Kommunikation) konsequent wahrnehmen kann, siehe auch Kap. 13 „E-Mail-Sicherheit“.

**Umsetzungskonzept „Verbindlicher Austausch von Transaktionsdaten“** Transaktionsdaten stellen insofern „besondere“ Kommunikationsdaten dar, weil sich aus ihnen in der Regel Aktionen ableiten, die kostenrelevant sind. Für den Empfänger wie für den Sender steht die Verbindlichkeit im Mittelpunkt.

Diese Anwendungen sind meist firmen- beziehungsweise gerätebezogen und basieren auf geschlossenen Systemen (zum Beispiel der Austausch von Rechnungsdaten zwischen Telekommunikationsanbietern und ihren Partnerunternehmen). Die Bandbreite reicht von kleinen Datenmengen pro Monat bis hin zu einer hohen Anzahl von Transaktionen pro Minute. Hier liegt der Fokus auf der möglichst nahtlosen Integration in bestehende Workflows, um zu einer praktikablen Lösung zu gelangen.

Ein Alternativkonzept stellt die Blockchain-Technologie dar, siehe auch Kap. 13 „Blockchain-Technologie“.

---

## 4.4 Vertrauensmodelle von Public Key-Infrastrukturen

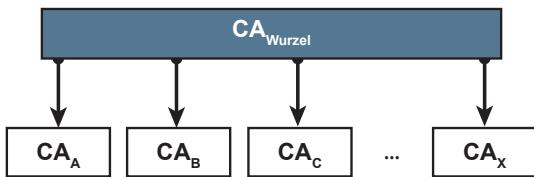
Für offene PKI-Systeme, mit deren Hilfe mehrere Organisationen mit je eigener PKI über ihre Grenzen hinweg vertrauenswürdig mit anderen Organisationen kommunizieren, werden Vertrauensmodelle benötigt [2].

Dazu sind die verschiedenen organisationsspezifischen Leitlinien der beteiligten Public Key-Infrastrukturen miteinander abzugleichen. Die Leitlinien beschreiben neben den verwendeten Technologien, Verfahren und Schnittstellen unter anderem den für die Nutzer-Registrierung notwendigen Prozess, insbesondere Maßnahmen zur initialen Identifizierung und Authentifikation der Nutzer, die zum angestrebten Schutzniveau der PKI passen. So kann es in einem Fall notwendig sein, dass die Personalausweise überprüft und Kopien für die Unterlagen gemacht werden, während in einem anderen die Stammdaten aus der Personalverwaltung für die Zertifikaterstellung ausreichen. Wichtig ist, dass die Geschäftspartner sich auf einen Mindeststandard einigen.

### Zertifizierungshierarchie und Vertrauensmodelle

Mit der zunehmenden Verbreitung von PKI-basierten Dienstleistungen erhalten die Nutzer eine Vielzahl von verschiedenen Zertifikaten für spezielle Applikationen. Zusätzlich gibt es sehr viele unterschiedliche Public Key-Infrastrukturen. In der Praxis ist daher sicherzustellen, dass sich die unterschiedlichen Zertifikate auf ihre Gültigkeit und Richtigkeit sowie den passenden Level of Trust überprüfen lassen,

**Abb. 4.8** Vertrauensmodell einer Wurzel-CA



damit die angestrebte vertrauenswürdige Kommunikation stattfinden kann. Dies wiederum lässt sich durch verschiedene Vertrauensmodelle für die Zusammenarbeit von Public Key-Infrastrukturen erreichen.

**Wichtig** Der organisationsübergreifende Einsatz von Public Key-Infrastrukturen erfordert verbindliche Vertrauensmodelle, für die prinzipiell drei Ansätze existieren.

#### 4.4.1 Vertrauensmodell: Übergeordnete CA (Wurzel-CA, Root CA)

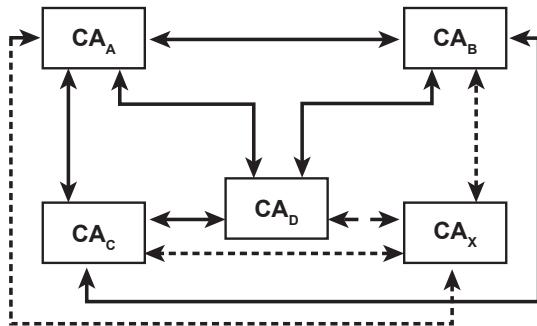
Eine Methode ist die Schaffung einer übergeordneten Certification Authority (CA), welche die Wurzelzertifikate der untergeordneten CAs aufnimmt, siehe Abb. 4.8.

Wurzelzertifikate sind Zertifikate mit den öffentlichen Schlüsseln der CAs ( $CA_A$  bis  $CA_X$ ).

**Ablauf** Die Wurzel-CA generiert Zertifikate der öffentlichen Schlüssel der untergeordneten CAs. Der öffentliche Schlüssel der Wurzel-CA ist im Personal Security Environment (zum Beispiel auf einer Smartcard) untergebracht oder wird für einen einfachen Abruf als Zertifikat der untergeordneten CAs zur Verfügung gestellt. Damit ist jeder Nutzer einer speziellen untergeordneten CA in der Lage, die öffentlichen Schlüssel einer anderen untergeordneten CA zu verifizieren und auch die Zertifikate mit den öffentlichen Schlüsseln der Nutzer der entsprechenden untergeordneten CAs zu überprüfen.

**Bewertung** In den meisten Fällen akzeptieren Unternehmen, Organisationen oder Länder keine derartige Unterordnung, da sie zu große Abhängigkeiten von einer zentralen Autorität schafft: Im Extremfall würde eine für alle verbindliche „Welt-CA“ eingerichtet. Da dieses Maß an Zentralisierung meist weder nötig noch realisierbar ist, hat sich das Modell der Wurzel-CA nur in großen, geschlossenen PKI-Systemen etabliert, die nicht für eine organisationsübergreifende Kommunikation konzipiert wurden.

**Abb. 4.9** Vertrauensmodell einer n:n-Cross-Zertifizierung



#### 4.4.2 Vertrauensmodell B: n:n-Cross-Zertifizierung

Ein weiterer Ansatz ist, dass jede Certification Authority (CA) ihre öffentlichen Schlüssel selbstständig mit jeder anderen CA austauscht, siehe Abb. 4.9.

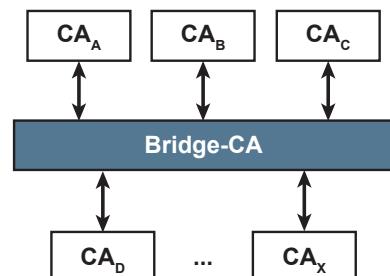
**Ablauf** Jede CA stellt jeder anderen ihre eigenen öffentlichen Schlüssel zur Verfügung und übernimmt deren Zertifikate beziehungsweise erkennt sie an. Dieser Prozess ist sehr aufwendig, weil der authentische Austausch der öffentlichen Schlüssel in der Regel ein persönliches Treffen der beteiligten PKI-Betreiber notwendig macht.

**Bewertung** Dieses Vertrauensmodell erfordert multiple Vertragsverhandlungen und ermöglicht abweichende Verträge und Vereinbarungen zwischen den beteiligten PKI-Betreibern. Bei einer Vielzahl von Beteiligten wird die daraus entstehende Infrastruktur jedoch schnell sehr komplex und lässt sich nur schwer verwalten. Daher hat sich dieses Vertrauensmodell nur bei kleinen Gruppen unabhängiger PKI-Betreiber durchgesetzt, und auch dort nur in abgegrenzten Geschäftsprozessen.

#### 4.4.3 Vertrauensmodell: 1:n Cross-Zertifizierung (Bridge CA)

Ein vielversprechendes Konzept stellt der Bridge-CA-Ansatz dar, weil er zum einen den Verwaltungsaufwand klein hält, zum anderen den angeschlossenen CAs die Entscheidungsfreiheit über die passende Vertrauenskette lässt. Erreicht wird dies durch eine sehr einfach gehaltene Struktur, bei der alle CAs authentisch ihre öffentlichen Schlüssel an die Bridge Certification Authority (Bridge CA) übergeben, die ihrerseits als eine zentrale Vermittlungsinstanz zwischen den beteiligten Organisationen fungiert, siehe Abb. 4.10.

**Abb. 4.10** Vertrauensmodell einer 1:n-Cross-Zertifizierung am Beispiel einer Bridge CA



**Ablauf** Die CAs ( $CA_1$  bis  $CA_X$ ) übergeben authentisch ihre öffentlichen Schlüssel an eine zentrale Bridge CA. Diese signiert eine Tabelle der öffentlichen Schlüssel aller beteiligten CAs. Die eigene CA stellt dann all ihren Nutzern den öffentlichen Schlüssel der Bridge CA als Zertifikat zur Verfügung.

**Bewertung** Bei der 1:n-Cross-Zertifizierung gibt es für jede CA nur einen Vertragspartner, die Bridge-CA. Das reduziert den Abstimmungsaufwand und ermöglicht es dennoch, in jedem Fall ein passendes Vertrauensmodell einzuführen. Die Kunst einer erfolgreichen Bridge CA besteht darin, eine Policy zu erarbeiten, die möglichst viele PKI-Betreiber politisch wollen und technisch erfüllen können.

Ein Beispiel für dieses Vertrauensmodell ist die von Bundesverband IT-Sicherheit – TeleTrusT betriebene European Bridge CA, die sich zum Ziel gesetzt hat, eine „Brücke des Vertrauens“ zwischen verschiedenen PKIs weltweit herzustellen. Zu diesem Zweck hat TeleTrusT pragmatische Leitlinien-Anforderungen und technische Vorbedingungen definiert, die eine vertrauenswürdige Kommunikation über organisatorische Grenzen hinweg erlauben. Gleichzeitig gilt es, bei allen Beteiligten ein gemeinsames Verständnis für den Nutzen und den korrekten Einsatz digitaler Signaturen herzustellen. Die Praktikabilität, die Flexibilität der vereinbarten Lösungen und der Schutz der getätigten Investitionen in die Sicherheitsinfrastruktur stehen im Vordergrund.

Die European Bridge CA stellt eine allgemeine Plattform dafür zur Verfügung, die die teilnehmenden CAs auf eine vertrauenswürdige, aber einfache Weise verbindet. Ein standardisiertes technisches und organisatorisches Regelwerk erleichtert die Integration neuer CAs in die Infrastruktur. Sobald sich eine neue CA (PKI) anschließt, können alle Mitglieder seiner PKI mit allen Mitgliedern der anderen Bridge-CA-Partner vertrauenswürdig kommunizieren. Eine einheitliche formale Registrierungsprozedur stellt dabei sicher, dass alle PKIs den Mindestanforderungen gerecht werden (siehe dazu die Webseite [www.bridge-ca.org](http://www.bridge-ca.org)).

**Wichtig** In der Praxis hat sich das Modell der 1:n-Cross-Zertifizierung durchgesetzt, das den PKI-Betreibern die größtmögliche Entscheidungsfreiheit bei der Wahl der Vertrauenskette lässt.

## 4.5 Gesetzlicher Hintergrund

Die EU-Verordnung 910/2014 [1] über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS – electronic identification and trust services) hat die vorher geltende EG-Richtlinie 1999/93/EG [2] über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen aufgehoben. eIDAS gilt für alle in der EU niedergelassenen Vertrauensdienstanbieter (VDA), mit Ausnahme von Vertrauensdiensten innerhalb geschlossener Nutzergruppen wie zum Beispiel interne Unternehmenslösungen.

Die 1999/93/EG-Richtlinie wurde in Deutschland mit dem Signaturgesetz (SigG) [5] und der Signaturverordnung (SigV) [5] in nationales Recht umgesetzt. EU-Verordnungen gelten, anders als EG-Richtlinien, direkt und müssen nicht erst durch nationales Recht umgesetzt werden.

### **Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS)**

Die Europäische Kommission verfolgt bei der eIDAS Verordnung einen offenen und technologieneutralen Ansatz. Das Hauptaugenmerk liegt auf der Gleichstellung, Interoperabilität und gegenseitigen Anerkennung der Vertrauensdienste der Mitgliedsstaaten. Bürger, Unternehmen und öffentliche Verwaltung sollten dazu ermuntert werden, die Vorteile des integrierten digitalen Binnenmarktes voll auszuschöpfen. Ganz oben auf der Prioritätsliste steht deshalb die Schaffung von Vertrauen in die vom Vertrauensdienstanbieter (VDA) erbrachten Dienste. Untrennbar mit Vertrauen verbunden ist ein Anspruch auf Rechtssicherheit, ganz gleich aus welchem Mitgliedsstaat der Dienst erbracht wird. Ein elektronisches Dokument soll in der EU den gleichen Stellenwert erhalten wie ein analoges. Durch diese Rechtssicherheit ist es möglich, Unternehmen und öffentliche Verwaltungen durch den Wegfall von analogen Dokumenten deutlich effizienter zu gestalten und ganz nebenbei für Unionsbürger Hemmnisse bei der Ausübung ihrer Bürgerrechte aus dem Weg zu räumen.

Mit eIDAS geht eine Vereinfachung des Systems einher. eIDAS sieht nur noch qualifizierte und nicht-qualifizierte VDA vor. Dies heißt jedoch nicht, dass sich ein qualifizierter VDA keiner Überprüfung mehr unterziehen muss. Aktuell können sich qualifizierte ZDA freiwillig alle drei Jahre akkreditieren lassen (§ 11, Abs. 2, SigV). In Zukunft muss sich jeder qualifizierte VDA alle zwei Jahre einer Überprüfung unterziehen, welche auf europäischer Ebene nicht eine Akkreditierung, sondern Konformitätsbewertung ist (Artikel 19, eIDAS). Der Konformitätsbewertungsbericht wird dabei jedoch von einer akkreditierten Konformitätsbewertungsstelle ausgestellt (Art. 3, Nr. 18, eIDAS). Ein qualifizierter VDA musste bis 1. Juli 2016 einen Konformitätsbewertungsbericht vorlegen, sofern er seinen Status nicht verlieren wollte (Art. 51, Abs. 3, eIDAS).

Da die Anforderungen beider Überprüfungen nahezu gleich sind und das Prüfungsintervall zudem verkürzt wurde, ist somit kein Sicherheitsverlust zu erwarten. Für den Kunden wurde zudem die Auswahl eines VDA durch die unnötig komplizierte Unterscheidung von fortgeschrittenen, qualifizierten und sowohl qualifizierten als auch akkreditierten VDA deutlich vereinfacht [4].

### **EU-Vertrauenssiegel (Art. 23)**

VDA können in Zukunft freiwillig mit einem EU-Vertrauenssiegel darauf aufmerksam machen, dass sie ein auf europäischer Ebene qualifizierter VDA sind. Das EU-Vertrauenssiegel verfolgt dabei einen ähnlichen Ansatz wie zum Beispiel das „IT Security made in Germany“ Qualitätssiegel der TeleTrusT, mit dem ein Anbieter dem Kunden auf einen Blick über den praktizierten Qualitätsstandard informieren kann. Dies ist insbesondere für ausländische Anbieter und Start-ups wichtig, da sie dem Kunden in der Regel weniger geläufig sind, was instinktiv

mit einer niedrigen Vertrauenswürdigkeit assoziiert wird. Das Siegel schafft die Möglichkeit der Vertrauensbildung, was gerade im e-Commerce-Umfeld eine essenzielle Voraussetzung ist. Alle VDA mit EU-Vertrauenssiegel werden zudem in einer zentralen Liste aufgeführt, was die Findung eines VDA erleichtert.

#### Suspendierung von qualifizierten Zertifikaten (Art. 28)

Bislang konnten Kunden nach SigG nur neue Zertifikate ausstellen oder diese endgültig sperren lassen. Nicht berücksichtigt wurde der Anwendungsfall, dass ein Kunde sein Zertifikat (zum Beispiel in Form einer Smartcard) kurzfristig verlegt, dann aber doch wiederfindet, was nach alter Regel bedeuten würde, dass die alte Smartcard wertlos wäre.

Für genau diesen Anwendungsfall ist in eIDAS die Möglichkeit der zeitlichen Suspendierung von Zertifikaten geschaffen worden (Artikel 28, Abs. 5, eIDAS; Erwägungsgrund 53). Das Zertifikat verliert dabei nur während der Aussetzung die Gültigkeit, kann aber nach der Reaktivierung wiederverwendet werden. Die Dauer der Aussetzung muss dabei klar in der Zertifikatsdatenbank angegeben werden.

#### Elektronische Siegel (Art. 35–40)

Das SigG sieht nur elektronische Signaturen für natürliche Personen vor (§ 2 Nr. 2a, SigG).

Diese Beschränkung ist für Organisationen jedoch eher hinderlich, wie das Beispiel eines Angebotes deutlich macht: Ein Angebot, welches mit einer FES beziehungsweise QES signiert wurde, beinhaltet implizit die Identität des Verfassers des Angebotes. Der Mitarbeiter kann das Unternehmen jedoch wechseln, wodurch das Zertifikat gesperrt wird. Dem Empfänger ist ab diesem Zeitpunkt nicht mehr klar, ob das Angebot gültig ist. Natürlich wäre es möglich, das Angebot mit einem Pseudonym zu signieren (§ 5, Abs. 3, SigG), jedoch wirkt ein Pseudonym im Geschäftsverkehr nicht sonderlich vertrauenserweckend.

Elektronische Siegel stellen jetzt mit eIDAS das Pendant zu elektronischen Signaturen dar, mit dem Unterschied, dass elektronische Siegel auch von Organisationen verwendet werden können. Elektronische Siegel beinhalten ein großes Potenzial zur Bekämpfung von Cyber-Kriminalität. Jedes Jahr gibt es tausende von Fällen, in denen Verbraucher auf gefälschte Rechnungen und Mahnungen hereinfallen. Würden alle Firmen in der EU ausnahmslos ihren Geschäftsverkehr mit elektronischen Siegeln versehen, so wäre es für Verbraucher deutlich einfacher, Phishing-E-Mails als solche zu entlarven.

#### Elektronische Fernsignaturen

Qualifizierte Signaturen nach SigG setzen voraus, dass der Kunde selbst eine sichere Signaturerstellungseinheit (SSEE) besitzen muss (§ 5, Abs. 6, SigG). In Zeiten, in denen immer mehr Dienste über die Cloud, Tablets, Smartphones und andere weit verbreitete Gadgets benutzt werden, wirkt eine lokale Signaturerstellungseinheit jedoch eher bremsend auf eine weitere Verbreitung von QES.

Genau hier setzt in eIDAS die Fernsignatur an. Die Idee ist, dass die SSEE beim qualifizierten VDA bleibt und nur der eigentliche Auslöser der Signatur

mit technischen Mitteln verlängert wird. Der VDA hat dafür zu sorgen, dass unter anderem durch abgesicherte elektronische Kommunikationskanäle eine vertrauenswürdige Umgebung zur Erstellung elektronischer Signaturen hergestellt wird und muss gewährleisten, dass die Umgebung unter alleiniger Kontrolle des Unterzeichners ist (Erwägungsgrund 52, eIDAS).

In Österreich, Finnland und Estland sind mit der „Handy-Signatur“ bereits seit längerem ähnliche Lösungen im Einsatz. Zum Schutz der Kunden dürfen Fernsignaturen nur von einem qualifizierten VDA angeboten werden (Anhang II, Abs. 3, eIDAS).

#### Haftung und Beweislast (Art. 11, 13)

Bei einem qualifizierten VDA wird vom Vorsatz oder Fahrlässigkeit ausgegangen, es sei denn er kann nachweisen, dass der Schaden auf andere Weise entstanden ist. Im Beispiel von Fernsignaturen muss also der VDA nachweisen, dass er sichere Systeme zur Verfügung gestellt hat. Bei nicht-qualifizierten VDA liegt die Nachweispflicht hingegen beim Kunden.

In jedem Fall haftet der VDA, wenn er die in der eIDAS-Verordnung genannten Pflichten nicht eingehalten hat, beispielsweise wenn er nicht Dienste nach dem neuesten Stand der Technik anbietet (Art. 19, Abs. 1, eIDAS). Der VDA hat jedoch im Vorfeld die Möglichkeit, seine Haftung zu beschränken, indem er die Verwendungszwecke der vom ihm erbrachten Dienste beschränkt.

#### Elektronisches Einschreiben (Art. 43–44)

Elektronische Einschreiben sind ein weiterer Weg, um den analogen Schriftverkehr überflüssig zu machen. Die Anforderungen an qualifizierte Dienste für die Zustellung elektronischer Einschreiben nach eIDAS sind:

- Identifizierung des Absenders mit hohem Maß an Vertrauenswürdigkeit.
- Identifizierung des Empfängers vor Zustellung der Daten.
- Absenden und Empfang ist durch fortgeschritten elektronische Signatur oder ein fortgeschrittenes elektronisches Siegel eines qualifizierten VDA vor Veränderung geschützt.
- Jede Veränderung von Daten wird deutlich angezeigt.
- Zeit und Datum von Versand, Empfang oder Änderung der Daten wird durch qualifizierte elektronische Zeitstempel angezeigt.

Auf nationaler Ebene existiert in Deutschland mit der De-Mail bereits ein ähnlicher Dienst. Es existieren jedoch einige kleine Unterschiede:

- Bei De-Mail versieht nach De-Mail-Gesetz (De-Mail-G) immer der akkreditierte Anbieter selbst die Nachrichten mit einer qualifizierten Signatur (§ 5, Abs. 7, De-Mail-G). Es ist also nur eine Art Fernsignatur zulässig.
- Überall wo in eIDAS qualifizierte Zeitstempel vorgesehen sind, benutzt De-Mail Prüfsummen und qualifizierte Signaturen.
- De-Mail schreibt zwingend eine Transportverschlüsselung zwischen den Anbietern vor (§ 5, Abs. 3, Satz 1, De-Mail-G).
- De-Mail überlässt es den Anbietern, eine sichere Dokumentenablage anzubieten (§ 8, De-Mail-G).

- De-Mail ist aktuell also nicht vollständig eIDAS-konform. Laut einem Zwischenbericht der Bundesregierung soll De-Mail aber ab Geltung der Regelungen zu elektronischen Zustelldiensten den Anforderungen der eIDAS-Verordnung entsprechen und auf dieser Grundlage mit elektronischen Zustelldiensten anderer Mitgliedstaaten interoperabel werden.

#### Sicherheitsanforderungen an Vertrauensdienstanbieter (Art. 19)

Alle qualifizierten und nicht-qualifizierten VDA müssen unter Berücksichtigung des jeweils neuesten Standes der Technik gewährleisten, dass das Sicherheitsniveau der Höhe des Risikos angemessen ist. Besteht ein Sicherheitsvorfall, so muss der VDA innerhalb von 24 h die zuständige nationale Stelle beziehungsweise Datenschutzbehörde sowie die betroffenen natürlichen oder juristischen Personen informieren. Betreffen Sicherheitsverletzungen oder Integritätsverlust mehrere Mitgliedsstaaten, so müssen die Aufsichtsstellen der betroffenen Mitgliedsstaaten und die ENISA davon in Kenntnis gesetzt werden. Besonders heikel für VDA ist jedoch, dass die Aufsichtsstelle entscheiden kann, ob bei einem Sicherheitsvorfall oder Integritätsverlust die Öffentlichkeit informiert wird, falls dies im öffentlichen Interesse ist. Für jeden VDA stellt schließlich ein Vertrauensverlust den höchsten denkbaren Wertverlust dar.

#### Fazit

Die größten Probleme bei der flächendeckenden Einführung von PKI-Systemen ergeben sich bei der Umsetzung geeigneter Vertrauensmodelle. Konzepte wie die European Bridge CA können helfen, diese zu lösen. Allerdings werden auch in Zukunft weitere Anstrengungen nötig sein, um einen verbindlichen, organisations-, länder- und kulturübergreifenden Level of Trust zu schaffen, der die Einführung international verbindlicher Modelle gestattet.

**Wichtig** PKIs sind eine wichtige Cyber-Sicherheitsinfrastruktur für sehr viele Cyber-Sicherheitssysteme.

---

## 4.6 PKI-enabled Application

PKI-enabled Application nutzen PKI-Dienste für die Umsetzung von Cyber-Sicherheitsdiensten.

### 4.6.1 E-Mail-Sicherheit

Der Austausch von E-Mails ist eine sehr häufig genutzte Anwendung im Internet. Dabei werden mithilfe von E-Mails und ihren Attachements Informationen übermittelt, die hohe Werte darstellen können, wie zum Beispiel Vertragsentwürfe. Bei

Fusionsverhandlungen kann es unter Umständen sogar um Milliardensummen gehen.

In diesem Abschnitt wird beschrieben, wie mithilfe einer Public Key-Infrastruktur (PKI) das Schlüsselmanagement sowie die Verschlüsselung und Signatur von E-Mails prinzipiell umgesetzt werden können [1].

### Idee und Definition von E-Mail-Sicherheit

Eine Information wurde früher entweder auf einer Schreibmaschine getippt oder mithilfe eines Textverarbeitungssystems in ein IT-System eingegeben und anschließend ausgedruckt. Der Ausdruck wurde unterschrieben, in einen Briefumschlag gesteckt und vertraulich an den gewünschten Empfänger gesendet. Der Empfänger erkannte an der Unversehrtheit des Umschlags, dass die Information vertraulich übermittelt worden war. Nach dem Öffnen des Briefes konnte der Empfänger an der eigenhändigen Unterschrift die Echtheit des Absenders oder des Autors überprüfen. Die eigenhändige Unterschrift ist zudem eine rechtsgültige Unterschrift.

E-Mail-Sicherheit bedeutet, die gleiche Sicherheit bei Mails zu haben, die auch für Briefe gilt.

Die Funktionen der E-Mail-Sicherheit bieten hierzu das Verfahren der digitalen Signatur in Verbindung mit einem digitalen Zeitstempel an, das in seiner Vertraulichkeit einer echten Unterschrift gleichkommt. Die Verschlüsselung des Dokuments hat die gleiche Wirkung wie der zugeklebte Briefumschlag.

### Funktionen von E-Mail-Sicherheit

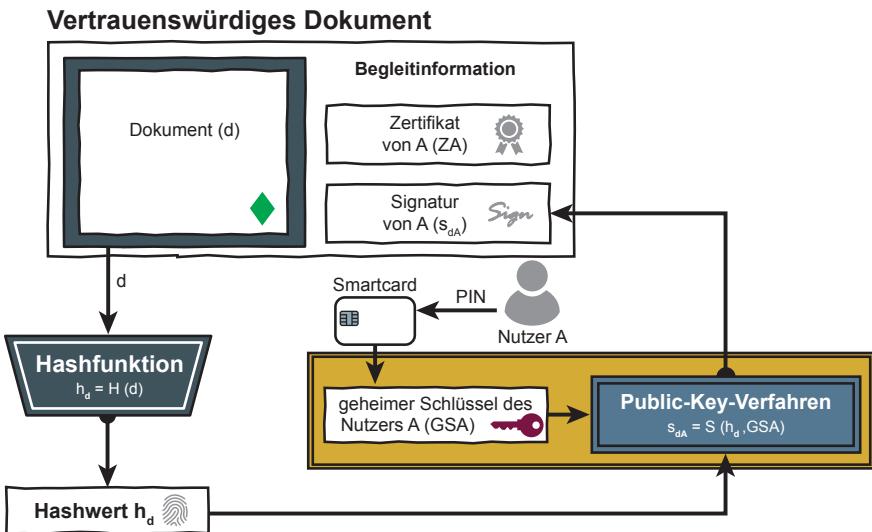
Ein Beispiel soll die prinzipielle Arbeitsweise eines Sicherheitssystems zum Schutz von elektronischen Dokumenten erläutern. Damit das vorgestellte IT-Sicherheitssystem funktioniert, wird das normale Kommunikationssystem um eine Zertifizierungsinstanz, eine Public-Key-Infrastruktur erweitert, die für die Nutzer personalisierte Hardware-Sicherheitsmodule wie Smartcards ausgibt und das Cyber-Sicherheitssystem mit Zertifikaten versorgt.

#### 1. Signatur eines Dokuments

Ein Nutzer erstellt mit einem Editor (Textverarbeitungssystem, Browser, Mail-Programm, ...) eine elektronische Information, die er vertrauenswürdig versenden will.

Anschließend ruft der Nutzer die Signatur-Funktion auf. Als erstes muss der Nutzer mithilfe seiner PIN die Smartcard, auf der ein geheimer Schlüssel des Nutzers (GSA) gespeichert ist, aktivieren. Die Signatur-Funktion in der Smartcard berechnet mithilfe der One-Way-Hashfunktion ( $H$ ) aus dem vom Nutzer A angegebenen Dokument ( $d$ ) einen Hashwert  $h_d$ , siehe Abb. 4.11.

Dieser Hashwert (kryptografische Prüfsumme) wird mit dem Public Key-Verfahren unter Verwendung des auf der Smartcard des Nutzers A gespeicherten geheimen Schlüssels (GSA) mithilfe der Signaturfunktion ( $S$ ) digital signiert. Das Ergebnis ist eine Signatur ( $s_{dA}$ ), die dem Dokument als Begleitinformation hinzugefügt wird. Außerdem schreibt die Signatur-Anwendung noch das Zertifikat des



**Abb. 4.11** Signatur-Funktion

Nutzers A (ZA) in die Begleitinformationen. Eine wichtige Sicherheitseigenschaft ist, dass der geheime Schlüssel (GSA) des Nutzers die Smartcard nie verlässt.

Wenn ein Dokument (wie im täglichen Büroleben) von mehreren Nutzern unterschrieben werden muss, kann auch eine digitale Signatur von mehreren Nutzern generiert werden. Alle digitalen Signaturen eines Dokuments stehen in der Begleitinformation des entsprechenden Dokuments.

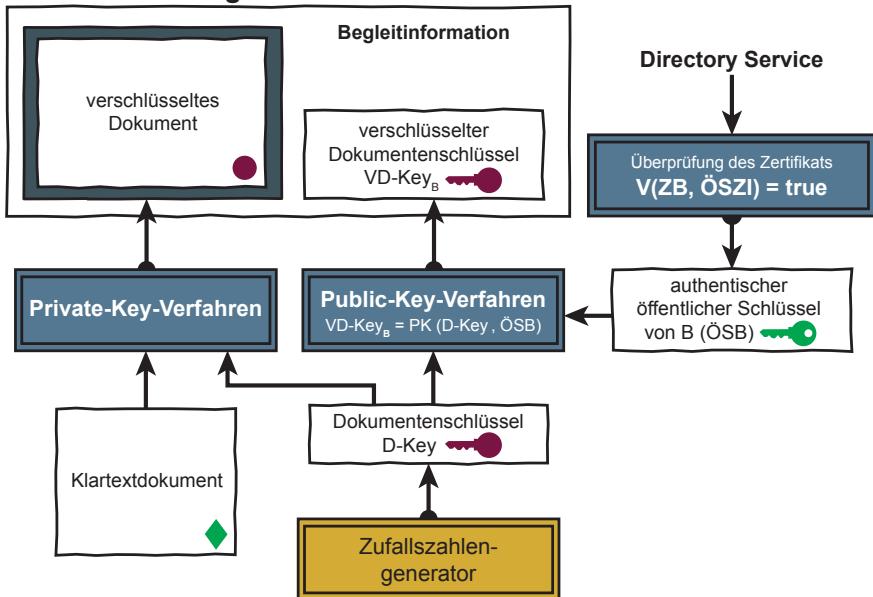
**Wichtig** Die digitale Signatur ist das Äquivalent einer eigenhändigen Unterschrift.

### Digitaler Zeitstempel

Die Beweiskraft eines elektronischen Dokuments hängt häufig zusätzlich auch vom Zeitpunkt seiner Erstellung ab. Da sich die Uhren und Zeitfunktionen in handelsüblichen IT-Systemen und Betriebssystemen ohne Probleme verstehen lassen, kann die Uhrzeit nicht für eine vertrauenswürdige Zeitangabe bei der digitalen Signatur angegeben werden. Ein Zeitstempel benötigt eine digitale Bescheinigung einer Zertifizierungsstelle. Sie bestätigt, dass ihr das Dokument zum angegebenen Zeitpunkt vorgelegen hat, indem sie den Zeitstempel digital signiert.

**Wichtig** Ein digitaler Zeitstempel dient dazu, ein Dokument mit der vertrauenswürdigen aktuellen Zeitangabe zu verknüpfen und diese Gesamtinformation anschließend digital zu signieren.

## Vertrauenswürdiges Dokument



**Abb. 4.12** Verschlüsselung des Dokuments

## 2. Verschlüsselung eines Dokuments

Nachdem eine oder mehrere Nutzer das Dokument signiert oder auch nicht signiert haben, kann mithilfe der Verschlüsselungs-Funktion das Dokument für die Übertragung verschlüsselt werden, siehe Abb. 4.12.

Dazu wird vom Cyber-Sicherheitssystem als Dokumentenschlüssel (D-Key) eine qualitative Zufallszahl berechnet. Das Klartext-Dokument wird dann unter Verwendung des Dokumentenschlüssels mit dem Private Key-Verfahren (symmetrisches Verschlüsselungsverfahren), zum Beispiel AES, verschlüsselt (verschlüsseltes Dokument). Der Dokumentenschlüssel wird unter Verwendung des öffentlichen Schlüssels des Empfängers B (OSB) mit dem Public Key-Verfahren (PK) verschlüsselt und der Begleitinformation hinzugefügt (verschlüsselter Dokumentenschlüssel VD-Key<sub>B</sub>).

Um sicherzustellen, dass der öffentliche Schlüssel des Empfängers B auch authentisch ist, wird vorher noch das Zertifikat des Empfängers B auf dessen Richtigkeit verifiziert (Verifikationsfunktion V). ZB ist das Zertifikat von B und ÖSZI ist der öffentliche Schlüssel der Zertifizierungsinstanz, die das Zertifikat erstellt und signiert hat.

Der Dokumentenschlüssel kann mithilfe des Cyber-Sicherheitssystems für mehrere Empfänger verschlüsselt werden, es stehen dann aber mehrere verschlüsselte Dokumentenschlüssel für die verschiedenen Empfänger in den Begleitinformationen (zum Beispiel für C, D, ...). Das vertrauenswürdige Dokument wird nun an den/die Empfänger gesendet.

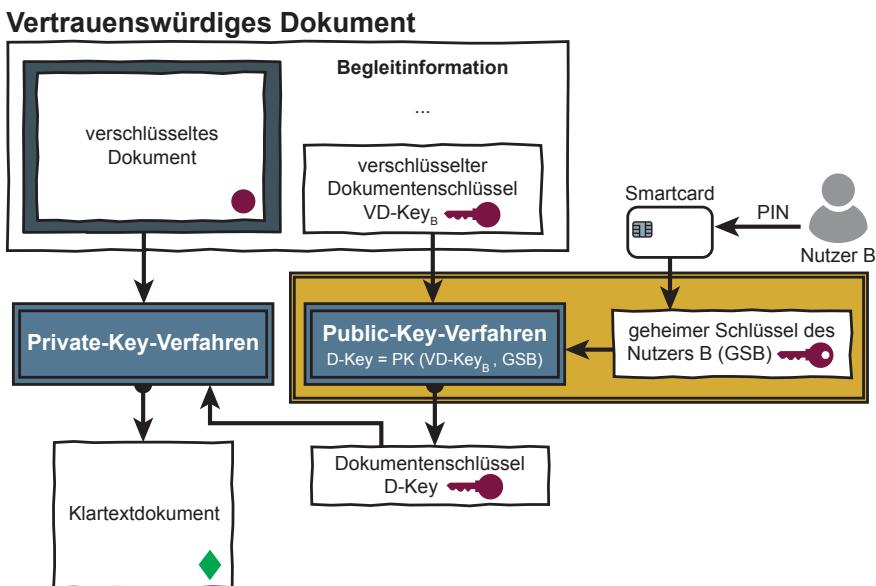
Das vertrauenswürdige Dokument kann dann mithilfe der E-Mail-Infrastruktur über das unsichere Internet übertragen werden.

### 3. Prüfung der Vertrauenswürdigkeit des Dokuments und seine Entschlüsselung

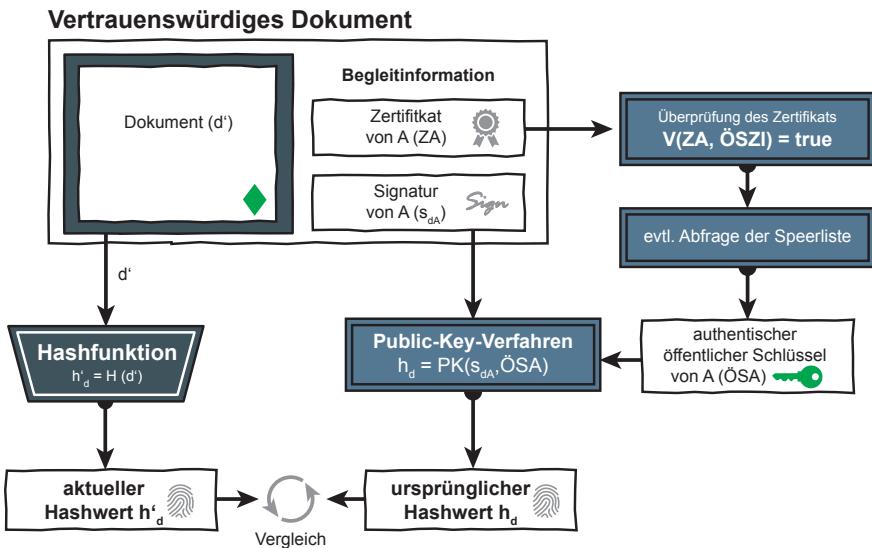
Nachdem das Dokument beim Empfänger eingetroffen ist, kann dieser mithilfe der Begleitinformation erkennen, ob und von wem das Dokument digital signiert worden ist. Außerdem ist erkennbar, ob das Dokument verschlüsselt wurde und wer in der Lage ist, es zu entschlüsseln (hier Nutzer B).

Mithilfe der Entschlüsselungs-Funktion kann das Dokument entschlüsselt und anschließend im Klartext gelesen werden, siehe Abb. 4.13.

Zuerst wird der Empfänger B aufgefordert, mithilfe seiner PIN seine Smartcard zu aktivieren. Zur Entschlüsselung wird der für den Empfänger B verschlüsselte Dokumentenschlüssel ( $VD\text{-Key}_B$ ) aus den Begleitinformationen entnommen und mit dem geheimen Schlüssel (GSB), der sich auf der Smartcard des Empfängers B befindet, mithilfe des Public Key-Verfahrens (PK) entschlüsselt. Anschließend wird das Dokument unter Verwendung des Private Key-Verfahrens (symmetrisches Verschlüsselungsverfahren) mit dem Dokumentenschlüssel (D-Key) entschlüsselt und steht im Klartext zur Verfügung.



**Abb. 4.13** Entschlüsselung eines Dokuments



**Abb. 4.14** Überprüfung von Signaturen

#### 4. Verifikation von Signaturen

Liegt das Dokument im Klartext vor, können mithilfe der Verifikations-Funktion die digitale Signatur oder die digitalen Signaturen überprüft werden. Im Beispiel wurde das Dokument vom Nutzer A digital signiert, siehe Abb. 4.14.

Zur Überprüfung der Signatur wird mithilfe der One-Way-Hashfunktion ( $H$ ) der aktuelle Hashwert ( $h'_d$ ) über das Dokument ( $d'$ ) berechnet. Das Dokument wird als  $d'$  bezeichnet, weil noch unklar ist, ob es tatsächlich das originale Dokument  $d$  ist.

Danach wird die Signatur ( $s_{dA}$ ) den Begleitinformationen entnommen, um mithilfe des Public Key-Verfahrens (PK) unter Verwendung des öffentlichen Schlüssels (ÖSA) des entsprechenden Nutzers A den ursprünglichen Hashwert ( $h_d$ ) zu erlangen.

Sind beide kryptografischen Prüfsummen gleich, so ist das empfangene Dokument unversehrt und der Nutzer A, der die Signatur durchgeführt hat, ist authentisiert.

Um sicherzustellen, dass der öffentliche Schlüssel des Absenders (Nutzer A) auch authentisch ist, wird vorher noch das Zertifikat des Absenders A auf dessen Richtigkeit verifiziert (Verifikationsfunktion  $V$ ). ZA ist das Zertifikat von A und ÖSzi ist der öffentliche Schlüssel der Zertifizierungsinstanz, die das Zertifikat erstellt und signiert hat.

Außerdem kann/sollte noch eine Sperrlistenabfrage durchgeführt werden, um zu prüfen, ob das Zertifikat des Nutzers A nicht gesperrt worden ist.

### Sicherheitsdienste des E-Mail-Sicherheitssystems

Nach erfolgreicher Überprüfung der Signatur ist sichergestellt, dass das Dokument unversehrt übertragen worden ist. Das bedeutet:

1. Niemand hat das Dokument manipuliert (Gewährleistung der Datenunversehrtheit).
2. Die angegebene Zeit der Signatur im Dokument wurde nicht geändert. Hierdurch kann erkannt werden, ob abgefangene Dokumente zu einem späteren Zeitpunkt wieder eingespielt wurden.
3. Nur die Nutzer, die in den Begleitinformationen angegeben sind, konnten die entsprechende Signatur durchführen, da nur diese über die entsprechenden Smartcards mit dem passenden geheimen Schlüssel verfügen.

Diese Funktionen machen die digitale Signatur zum elektronischen Äquivalent der eigenhändigen Unterschrift. Als zusätzliche Sicherheitsfunktion steht die Verschlüsselung des Dokuments zur Verfügung, die seine Vertraulichkeit garantiert. Vertraulichkeit bedeutet, dass keiner, außer den in den Begleitinformationen explizit angegebenen Nutzern des IT-Sicherheitssystems, das Dokument entschlüsseln und im Klartext lesen kann.

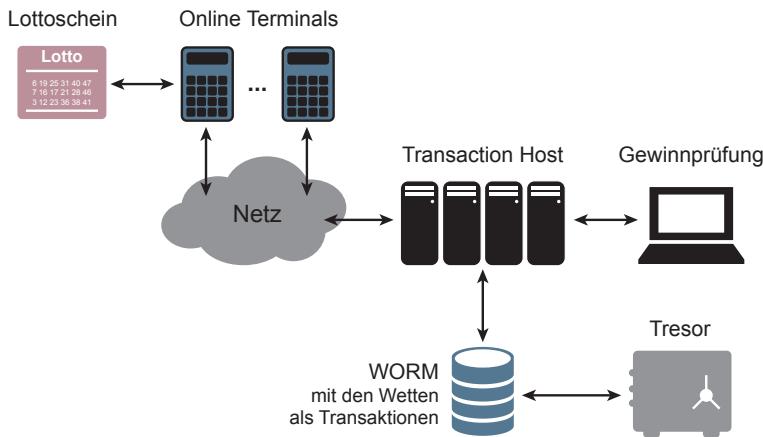
### E-Mail-Sicherheit aus Sicht des Nutzers?

Die Sicherheitsfunktionen: digitale Signatur und Objektverschlüsselung, werden in die Anwendungen integriert, die der Nutzer verwendet. Das sind zum Beispiel Mailsoftware (Outlook, Thunderbird usw.), Browser und andere Software. Der Nutzer kann dabei durch einfachen Mausklick die Sicherheitsfunktionen aufrufen und die entsprechende Dienstleistung nutzen. Je einfacher die Nutzbarkeit der Sicherheitsfunktionen ist, desto höher wird die Akzeptanz der Nutzer sein.

Außerdem ist es denkbar, dass ein Gateway als zentrale E-Mail-Annahmestelle fungiert und eingehende E-Mails entschlüsselt und intern verteilt, oder ausgehende E-Mails signiert, damit die Empfänger sicher sein können, dass diese Mails wirklich von der entsprechenden Organisation stammen.

### Zusammenfassung E-Mail-Sicherheit

Der Austausch von E-Mails ist eine wichtige Anwendung im Internet, gerade hier sollte die Sicherheit an allerster Stelle stehen. Doch die E-Mail-Sicherheit wird immer noch viel zu oft vernachlässigt, dabei ist es heute möglich, die gleiche Sicherheit wie bei der Übermittlung eines Briefes zu gewährleisten. Adressat und Empfänger können durch digitale Signaturen und Zeitstempel für diese Sicherheit sorgen. Die Dokumente werden verschlüsselt übertragen, auf ihre Vertrauenswürdigkeit überprüft und anschließend entschlüsselt, wobei die Funktionen der E-Mail-Sicherheit auf unterschiedliche Art und Weise realisiert sind, siehe auch Kap. 13 „E-Mail-Sicherheit“.



**Abb. 4.15** Altes Verfahren der Manipulationssicherung von Wetten

#### 4.6.2 Lotto – Online-Glückspiel

In diesem Abschnitt werden die grundsätzliche Idee und die notwenigen Funktionen eines Zeitstempeldienstes für Transaktionsdaten beschrieben. Die Idee wird anhand eines „Online“-Glückspiels dargestellt.

In Abb. 4.15 ist ein alter Ablauf des Lottospieles dargestellt. Der Kunde stellt einen Lottoschein aus und gibt diesen in einer Lotto-Annahmestelle ab. Dort wird dieser Lottoschein in einen Online-Terminal eingescannt und über das Netz an den Transaktionshost gesendet.

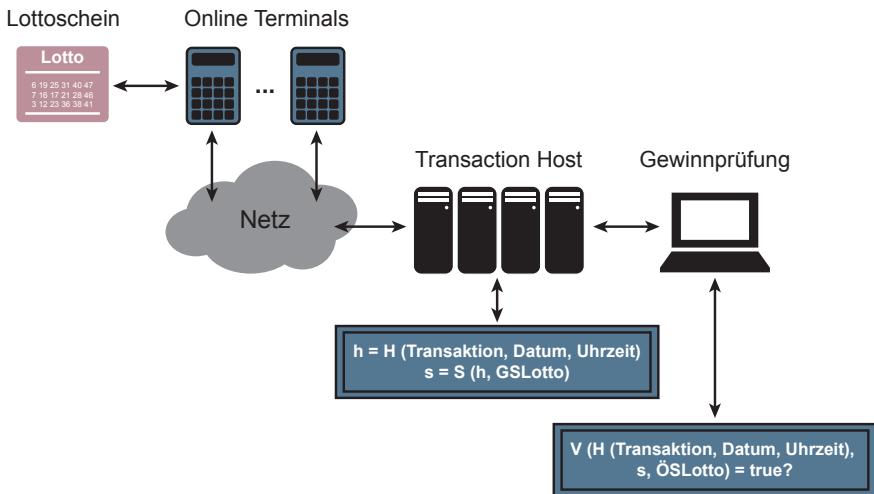
Der Transaktionshost speichert die Transaktion ab. Wenn um 18 Uhr die Wette geschlossen wurde, sind alle Transaktionen mit den Wettanträgen auf einem externen Speichermedium (WORM) gespeichert worden. Eine WORM ist die Abkürzung für „write once read many“. Es bezeichnet ein Speichermedium, das das Löschen, Überschreiben und Ändern von Daten dauerhaft ausschließt. Diese WORM wurde dann unter der Aufsicht eines Notars während der Ziehung in einem Tresor manipulationssicher aufbewahrt.

Anschließend fand die Ziehung statt. Später wurde dann die WORM wieder unter der Aufsicht eines Notars aus dem Tresor geholt und eine Gewinnprüfung durchgeführt.

Dieses Verfahren hat dafür gesorgt, dass keine Manipulationen nach der Ziehung durchgeführt werden konnten.

#### Neue Herausforderungen

Mit neuen Gewinnspielen, wie Sportwetten, die sehr viel schnellere Lebenszyklen haben, wurde eine neue Idee gesucht, das Verfahren des Wegschließens einer WORM in einem Tresor zu modernisieren.



**Abb. 4.16** Neus Verfahren der Manipulationssicherung von Wetten

### Nutzung eines Zeitstempeldienstes für Manipulationssicherung von Transaktionsdaten

In den neuen Verfahren wurde ein Zeitstempeldienst für eine moderne Manipulationssicherung von Wetttransaktionen eingeführt, siehe Abb. 4.16.

Bei diesen Verfahren werden die über das Netz angekommenen Transaktionen mit Datum und Uhrzeit erweitert und ein Hashwert daraus berechnet:

$$h = H(\text{Transaktion, Datum, Uhrzeit}).$$

Datum und Uhrzeit werden von einem vertrauenswürdigen Zeitdienst genommen.

Anschließend wird dann dieser Hashwert mit dem geheimen Schlüssel von Lotto ( $GS_{\text{Lotto}}$ ) digital signiert.

$$s = S(h, GS_{\text{Lotto}})$$

Dadurch werden die Wetttransaktionen als digital signierte Transaktionen mit Zeitangaben manipulationssicher auf dem Transaktionshost gespeichert. Die eigentliche „Tranaktion“ und die passende Signatur „s“.

Da es nicht mehr möglich ist, die digital signierten Wetttransaktionen zu manipulieren, können sie auf dem „Transaction Host“ gespeichert bleiben. Die Zeitangabe in der digitalen Signatur gewährleistet, dass keine Transaktion rückdatiert werden kann.

Wenn die Ziehung vorbei ist, kann die Gewinnprüfung umgesetzt und jede Transaktion verifiziert werden.

$V(H(\text{Transaktion, Datum, Uhrzeit}), s, OS_{\text{Lotto}}) = \text{true?}$

V	Verifikationsfunktion
H	Hashfunktion
S	Signaturfunktion
s	Signatur der Transaktion
$OS_{\text{Lotto}}$	Öffentlicher Schlüssel von Lotto

### Zusammenfassung: Lotto – Online-Glückspiel

Das Lotto-Beispiel zeigt sehr schön, wie mit einem Zeitstempeldienst, digitale Signatur und Datum/Uhrzeit die digitale Transformation des Wettgeschäfts vertrauenswürdig umgesetzt werden kann.

---

## 4.7 Zusammenfassung

Digitale Signatur, elektronische Zertifikate und Public Key-Infrastrukturen sind wichtige Cyber-Sicherheit-Prinzipien, -Mechanismen und -Konzepte für die Realisierung von Cyber-Sicherheitslösungen und -Diensten.

Public Key-Infrastrukturen stellen die Basis für organisationsübergreifende Cyber-Sicherheitssysteme dar und haben über eIDAS in Europa eine rechtliche Grundlage.

Die Beispiele der PKI-enabled Application zeigen sehr schön auf, dass mit den Vertrauensdiensten einer PKI interessante und hilfreiche Cyber-Sicherheitssysteme für sicherheitsrelevante Anwendungen umgesetzt werden können.

---

## 4.8 Übungsaufgaben

### Übungsaufgabe 1 (digitale Signatur)

Was ist der Unterschied zwischen einer eigenhändigen Unterschrift und einer digitalen Signatur bezüglich der Verifizierung des Inhaltes?

### Übungsaufgabe 2 (elektronische Zertifikate)

Welche Cyber-Sicherheitsbedürfnisse können mithilfe von elektronischen Zertifikaten umgesetzt werden?

### Übungsaufgabe 3 (PKI)

Mit welchem PKI-Dienst wird das Sperren von eigentlich gültigen Zertifikaten umgesetzt?

### Übungsaufgabe 4 (PKI)

Die digitale Signatur wird mit einem Public Key-Verfahren unter Verwendung des geheimen Schlüssels durchgeführt. Kann ein Angreifer die Nachricht „entschlüsseln“, das heißt, im Klartext lesen?

**Übungsaufgabe 5 (E-Mail-Sicherheit)**

Welche Sicherheitsfunktion wird bei der E-Mail-Sicherheit als erstes durchgeführt und warum?

**Übungsaufgabe 6 (E-Mail-Sicherheit)**

Welche Cyber-Sicherheitsbedürfnisse können mit der E-Mail Sicherheit befriedigt werden?

**Übungsaufgabe 7 (Lotto)**

Mit welchem Sicherheitsdienst kann die Ankunftszeit einer Transaktion manipulationssicher bewiesen werden?

**Übungsaufgabe 8 (Vertrauensmodelle)**

Welches PKI-Vertrauensmodell würden Sie in den folgenden Situationen vorschlagen?

*Fall 1:*

Sie beraten einen Verband, der für seine Mitglieder eine PKI zur Verfügung stellen möchte. Welches Vertrauensmodell würden Sie für den Verband vorschlagen?

*Fall 2:*

In einem Forschungsvorhaben mit drei teilnehmenden Unternehmen, von denen keines mehr Rechte haben sollte als die anderen, soll eine PKI aufgebaut werden. Welches Modell würden Sie wählen?

*Fall 3:*

Sie wollen ein Geschäftsmodell aufbauen, bei dem sehr viele Unternehmen mit sehr vielen Nutzern Daten vertrauenswürdig austauschen wollen. Alle Unternehmen haben schon eine PKI. Zukünftig werden noch weitere Unternehmen dazukommen. Welches Vertrauensmodell würden Sie wählen?

Ergebnisse siehe: <https://norbert-pohlmann.com/cyber-sicherheit/uebungen/>.

---

**Literatur**

1. Hesse M, Pohlmann N (2007) Kryptografie: Von der Geheimwissenschaft zur alltäglichen Nutzanwendung (V) – Prüfsummen, Zertifikate und die elektronische Signatur, IT-Sicherheit & Datenschutz. Suppl in DuD Datenschutz Datensch – Recht und Sicherh in Informationsverarbeitung Kommun 31(3):218–221
2. Hesse M, Pohlmann N (2007) Kryptografie: Von der Geheimwissenschaft zur alltäglichen Nutzanwendung (VI) – Public Key Infrastruktur (PKI), IT-Sicherheit & Datenschutz. Suppl in DuD Datenschutz Datensch – Recht und Sicherh in Informationsverarbeitung Kommun 31(4):300–302
3. Pohlmann N (2003) Firewall-Systeme – Sicherheit für Internet und Intranet, E-Mail-Security, Virtual Private Network, Intrusion Detection System, Personal Firewalls, 5. aktualisierte u. erweiterte Aufl. MITP-Verlag, Bonn

4. Hesse M, Pohlmann N (2007) Kryptografie: Von der Geheimwissenschaft zur alltäglichen Nutzanwendung (VII) – Vertrauensmodelle von Public-Key-Infrastrukturen, IT-Sicherheit & Datenschutz. Suppl in DuD Datenschutz Datensich – Recht und Sicherheit in Informationsverarbeitung Kommun 31(5):380–384
5. Niessen G, Pohlmann N (2015) Der Aufschwung der Vertrauensdienste!? Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt – eIDAS. IT-Sicherheit – Manage Prax 2015(4):51–55



# Identifikation und Authentifikation

5

Die Identifikation und Authentifikation spielen in der modernen IT und im Internet eine besondere Rolle.

Bei den meisten IT-Anwendungen ist es wichtig zu wissen, wer gerade auf einem IT-System arbeitet oder einen IT-Dienst nutzen möchte. Aus diesem Grund muss verifiziert werden können, welche Person oder welches IT-System hinter einem Zugriff steckt.

**Wichtig** Nur wenn identifiziert und authentifiziert werden kann, welche Person oder welches IT-System wirklich hinter einem Zugriffswunsch steckt, kann ein Zugriff zugelassen werden.

## 5.1 Was ist eine Identifikation und Authentifikation?

Wenn ein Nutzer Zugang zu einem IT-System haben möchte, muss er sich diesem gegenüber identifizieren und authentisieren, damit er den Zugang gewährt bekommen kann [1].

### 5.1.1 Identifikation

Die Identifikation ist die Überprüfung eines vorgelegten, kennzeichnenden Merkmals, zum Beispiel des Nutzernamens oder der Identität. Eine Person wird weltweit eindeutig durch die Angabe von Vorname, Nachname, Geburtsort und Geburtstag identifiziert. In Deutschland wird die Eindeutigkeit der Identifikation durch die Regularien von den Standesämtern garantiert.

In der digitalen Welt wird in der Regel der Nutzernname als kennzeichnendes Merkmal verwendet.

Eine Identifikation muss immer innerhalb eines Systems (Organisation) abgesprochen sein, damit sie eindeutig ist. Ein System kann die Weltbevölkerung sein, die Bürger in Deutschland, die Kunden eines Webshops, die Mitglieder eines sozialen Netzwerkes wie Facebook usw.

Damit eine solche Absprache mit verschiedenen Nutzern zustande kommt, müssen klar definierte Regeln bezüglich der Identifikation eingehalten werden. Als Beispiel hierfür kann die CCITT Recommendation X.509 beziehungsweise ISO 9594-8 betrachtet werden. Hierbei handelt es sich um ein standardisiertes Konzept eindeutiger, kennzeichnender Namen oder „Distinguishing Identifier“.

Weitere Beispiele:

**E-Mail-Adresse** Bei vielen IT-Anwendungen und IT-Diensten wird als Nutzernname eine E-Mail-Adresse verlangt und verwendet. Dies hat den Vorteil, dass von aktiven E-Mail-Adressen international keine Doppelungen auftreten können. Das heißt, dass die E-Mail-Adresse einer Person weltweit ein eindeutiges kennzeichnendes Merkmal ist. Die E-Mail-Adressen mit ihren entsprechenden Domänen werden als Baumstruktur verwaltet und sind daher eindeutig. [rainer.maier@gmx.de](mailto:rainer.maier@gmx.de) gibt es nur ein Mal. Möchte ein zweiter Rainer Maier eine E-Mail-Adresse bei GMX haben, könnte er zum Beispiel [rainer.maier2@gmx.de](mailto:rainer.maier2@gmx.de) wählen.

**Freie Wahl** Der Nutzer kann selbst einen Nutzernamen auswählen. Das IT-System muss dann prüfen, ob der gewählte Nutzernname in diesem IT-System nicht schon vergeben ist. Wenn ja, muss der Nutzer einen anderen Namen finden, der noch nicht vergeben ist.

**Das IT-System bestimmt** Es ist aber auch möglich, dass das IT-System den Nutzernamen bestimmt und dem Nutzer mitteilt.

### 5.1.2 Authentifikation

Authentifikation bezeichnet einen Prozess, in dem überprüft wird, ob „jemand“ oder „etwas“ echt ist. Daher bedeutet Authentifikation die Verifizierung (Überprüfung) der Echtheit beziehungsweise der Identität. Die Überprüfung des Personalausweises einer Person ist eine solche Authentifikation in der realen Welt:

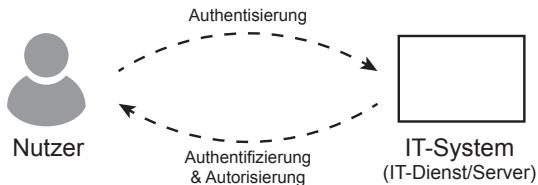
Was muss und kann identifiziert und authentisiert werden?

- **Nutzer**, wie Personen, Prozesse, Instanzen und weitere Entitäten.
- **Medien**, wie Notebooks, Smartphones, Smartwatches, Serversysteme, Cyber-Sicherheitssysteme, Security Token usw.
- **Nachrichten**, wie E-Mails, Dateien, Java-Applets, Datenpakete usw.

### Grundsätzliche Architektur der Identifikation und Authentifikation

In Abb. 5.1 möchte der Nutzer Zugriff auf ein IT-System (Server, IT-Dienst, ...) erhalten.

**Abb. 5.1** Authentisierung, Authentifizierung und Autorisierung



Aus der Sicht des Nutzers und des IT-Systems werden IT-Sicherheitsfunktionen umgesetzt, die verschiedene Sicherheitsdienste erbringen.

**Authentisierung:** (Sichtweise Nutzer)

Der Nutzer authentisiert sich gegenüber einem IT-System (IT-Dienst, Server, ...), indem er einen Nachweis über seine Identität, den Nutzernamen, erbringt.

**Authentifizierung:** (Sichtweise IT-System)

Das IT-System (IT-Dienst, Server, ...) überprüft den Nachweis der Echtheit der Identität eines Nutzers im Rahmen der Authentifizierung.

**Autorisierung:** (Sichtweise IT-System)

Wenn die Echtheit der Identität eines Nutzers erfolgreich verifiziert werden konnte, kann das IT-System (IT-Dienst, Server, ...) dem Nutzer definierte Rechte für den IT-Dienst/Server einräumen.

**Wichtig** Erst wenn bekannt ist, wer auf ein IT-System zugreifen will, können die entsprechenden Rechte dieser Identität zugeordnet werden.

### 5.1.3 Klassen von Authentifizierungsverfahren

Es werden verschiedene Klassen von Authentifizierungsverfahren unterschieden, bei denen unterschiedliche Aspekte eine Rolle spielen und diverse Charakteristika berücksichtigt werden müssen.

#### 1. Wissen

Bei dieser Klasse von Authentifizierungsverfahren wird über einen Nachweis der Kenntnis von Wissen die Echtheit eines Nutzers überprüft.

Beispiele von Wissen:

Passwort, PIN, Antwort auf eine bestimmte Frage (Sicherheitsfrage) usw.

Charakteristika von Wissen:

- Das Wissen kann vergessen werden (insbesondere nach einer Feier).
- Das Wissen kann dupliziert, verteilt, weitergegeben und verraten werden.
- Das Wissen kann in vielen Fällen erraten werden (Sozial Engineering, Wörterbuchangriff, ...).
- Die Preisgabe von Wissen kann kompromittiert werden (Androhung von Gewalt).
- Die Mitführung von Wissen erfordert in der Regel keine praktischen Hilfsmittel.

## 2. Besitz

Verwendung eines Besitztums für das Authentifizierungsverfahren ist eine weitere Klasse.

Beispiele für Besitz:

Neuer Personalausweis, SIM-Karte im Smartphone, Hardware-Sicherheitsmodule (Smartcard, USB-Stick, ...) usw.

Charakteristika von Besitz:

- Das Besitztum ist mit Kosten verbunden (Hardware).
- Das Besitztum muss mitgeführt werden (umständlich).
- Das Besitztum kann verloren gehen (kein Zugang mehr).
- Das Besitztum kann gestohlen werden (kein Zugang mehr).
- Das Besitztum kann übergeben oder weitergereicht werden (jemand anderes kann zugreifen).

## 3. Sein

Bei dieser Klasse von Authentifizierungsverfahren muss der Nutzer gegenwärtig sein.

Beispiele von Sein:

Biometrische Merkmale wie Iris, Fingerabdruck, Gesichtsgeometrie, DNA, Tippverhalten usw.

Charakteristika von Sein:

- Biometrische Merkmale werden durch Personen immer mitgeführt.
- Biometrische Merkmale können nicht an andere Personen weitergegeben werden.
- Verfahren zu Erkennung von biometrischen Merkmalen können keine 100 %-Aussagen treffen, sondern nur mit einer gewissen Wahrscheinlichkeit die Echtheit von Personen abschätzen.
- Eine Lebenderkennung kann erforderlich sein (damit zum Beispiel ein künstlicher Fingerabdruck oder abgeschnittener Finger zurückgewiesen wird)
- Ein biometrisches Merkmal ist im Laufe der Zeit oder durch Unfälle veränderlich und damit schlechter erkennbar.
- Bestimmten Personengruppen fehlt das biometrische Merkmal.
- Ein biometrisches Merkmal kann nicht ersetzt werden (Problem, wenn diese „gestohlen“ werden können).

## 5.2 Identifikationsverfahren

Bei Identifikationsverfahren handelt es sich um einen Vorgang, der es einem Prüfer ermöglicht, eindeutige, kennzeichnende Merkmale einer zu identifizierenden Person zu überprüfen. Im Folgenden werden mögliche Identifikationsverfahren mit ihren Möglichkeiten und Grenzen vorgestellt [2].

**Wichtig** Für viele Prozesse und Aktivitäten ist es wichtig, dass die Identitäten der Kommunikationspartner vertrauenswürdig und eindeutig sind.

### 5.2.1 Vorlage eines Personalausweises

Eine natürliche Person identifiziert sich in der Bundesrepublik Deutschland durch das Mitführen und das Vorzeigen des deutschen Personalausweises, siehe Abb. 5.2.

Hierbei kann der Prüfer die Identitätsdaten, wie Namen und Geburtsdatum, einsehen und das Aussehen der natürlichen Person mit dem Lichtbild auf dem Ausweisdokument vergleichen. Bei Grenzkontrollen wird dieser Prozess schon mithilfe von Kameras und dem gespeicherten digitalen Foto im Personalausweis automatisiert. Voraussetzung für dieses Verfahren ist, dass die zu überprüfende natürliche Person vor Ort sein und der Prüfer Erfahrungen bei der Echtheitsüberprüfung des Ausweises haben muss.

### 5.2.2 Fernidentifizierung – Allgemeine Aspekte

Neben der persönlichen Anwesenheit und dem Vorzeigen des Identifikationsdokuments beim Prüfer, der die Identitätsfeststellung verlangt, ist es auch möglich, eine sogenannte Fernidentifizierung durchzuführen.

Bei der Fernidentifizierung ist eine physische Anwesenheit der zu identifizierenden natürlichen Person zur Identitätsfeststellung nicht notwendig. Die nicht erforderliche physische Anwesenheit der zu identifizierenden Person hat einige Vorteile. So kann die zu identifizierende Person die Identifizierung von zu Hause aus durchführen. Dabei kann gerade bei Online-Geschäften eine Medienbruchfreiheit erzielt werden, da die Identifizierung auch direkt online, bestenfalls integriert in den aktuellen Prozess, durchgeführt werden kann. Neben dem besonderen Vorteil der Medienbruchfreiheit bietet sich die Fernidentifizierung daher in besonderem Maße für Personen an, die nicht mehr mobil sind oder deren Anreise zum Dienstleister einen enormen Aufwand bedeuten würde. Zusätzlich

**Abb. 5.2** Vorlage eines Personalausweises



kann, wenn es sich bei der Fernidentifizierung um eine Online-Identifizierung handelt, auch eine enorme Verkürzung der Wartezeit bis zur Möglichkeit der Identitätsfeststellung erreicht werden.

Für den Dienstleister einer Identitätsüberprüfung bietet sich die Fernidentifizierung an, da er in diesem Fall normalerweise nicht selbst für die Identifizierung zuständig ist, beispielsweise durch Sichtkontrolle in einer Filiale, sondern diese durch eine dritte Stelle übernommen wird. Letztgenannte hält dafür entsprechend geschultes Personal bereit. Dadurch kann der Dienstleister seinem Kerngeschäft nachgehen und ist nicht verantwortlich für die Bereitstellung der Infrastruktur, der Personalschulungen und der Kontrolle der Einhaltung gesetzlicher Vorgaben der Identitätsfeststellung.

### 5.2.3 Videoidentifikation

Beim VideoIdent-Verfahren handelt es sich um ein Fernidentifizierungsverfahren, das über einen Online-Videochat durchgeführt wird. Das VideoIdent-Verfahren wird dabei von Banken für die Kontoeröffnung, aber auch vermehrt durch Mobilfunkanbieter vor der Ausstellung einer SIM-Karte, eingesetzt. Im Gegensatz zu einer Sichtprüfung bei physischer Anwesenheit findet die Sichtprüfung beim VideoIdent-Verfahren über das Live-Videobild statt, siehe Abb. 5.3.

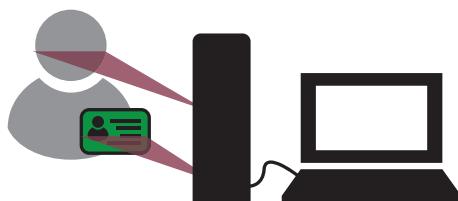
Hierbei führt der Prüfer den zu Identifizierenden durch den Identifikationsvorgang. Dabei hat der Prüfer zu verifizieren, dass es sich um ein echtes Ausweisdokument und um den legitimen Besitzer dieses Ausweisdokuments handelt.

#### Anforderungen an die Nutzung von Videoidentifizierungsmaßnahmen

Die Anforderungen für Videoidentifizierungen, wie sie von Dienstleistern für Unternehmen, die dem Geldwäschegesetz unterliegen, durchgeführt werden, sind im „Rundschreiben 3/2017 (GW) – Videoidentifizierungsverfahren“ [3] der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), das am 15.06.2017 in Kraft trat, geregelt. Gemäß des vorgenannten Dokuments ist die Videoidentifizierung nur für natürliche Personen und nicht für juristische Personen möglich.

Das BaFin Rundschreiben stellt dabei zuerst Anforderungen an die Prüfer, die die Identifikation über das Videochat-System durchführen. Dabei ist sicherzustellen, dass es sich um einen, für den Identifikationsvorgang mittels VideoIdent geschulten Mitarbeiter handelt. Die Schulung gewährleistet, dass der Mitarbeiter

**Abb. 5.3** VideoIdent-Verfahren



die über einen Videochat verifizierbaren Sicherheitsmerkmale des Ausweisdokuments erkennen und auf Legitimität überprüfen kann. Zusätzlich muss der Mitarbeiter Kenntnisse über häufig durchgeführte Fälschungsmöglichkeiten, die Vorgaben des BaFin Rundschreibens, sowie der datenschutz- und geldwäscherechtlichen Bestimmungen besitzen. Die Schulungen zur Erlangung dieser Kenntnisse sind dabei vor Aufnahme der Tätigkeit und danach in regelmäßigen Abständen durchzuführen. Durch eine Softwareunterstützung kann die Verifikation der Ausweismerkmale und der Inhalte des Ausweises deutlich vereinfacht und verbessert werden [2].

Die Videoidentifikation auf Mitarbeiterseite muss zudem in einem Raum stattfinden, der ausschließlich für Zutrittsberechtigte erreichbar ist. Des Weiteren müssen sämtliche für dieses Aufgabenfeld bestimmte Räume so voneinander abgetrennt sein, dass sich während des Identifikationsvorgangs jeweils nur der hierfür zuständige Mitarbeiter in diesen aufhält. Eine technische Anforderung an den Videochat ist eine vorhandene Ende-zu-Ende-Verschlüsselung.

Außerdem muss die Ton- und Videoqualität ausreichend sein, um für den Mitarbeiter eine zweifelsfreie Identifikation des Ausweisinhabers und des Ausweisdokuments zu ermöglichen. Da während des Identifikationsvorgangs auch Bilder der Person, sowie der Ausweisvorder- und -rückseite aus dem Videobild extrahiert werden müssen, muss zudem auch eine ausreichende Qualität dieser Standbilder gewährleistet sein. Es wird zudem ein Mechanismus vorausgesetzt, der eine Manipulation bei der Zuteilung der zu identifizierenden Personen zu einem bestimmten Mitarbeiter verhindert.

Bevor der eigentliche Identifikationsvorgang beginnt, muss die zu identifizierende Person ihr Einverständnis für die Durchführung des Identifikationsvorgangs abgeben. Im Folgenden überprüft der Prüfer, ob die auf dem im Videochat vorgezeigten Ausweisdokument visuell sichtbaren Sicherheitsmerkmale vorhanden und so platziert sind, wie es auf einem originalen Ausweisdokument zu erwarten ist.

### Kategorien von Sicherheitsmerkmalen

Die BaFin nennt dazu vier Kategorien von Sicherheitsmerkmalen, die optisch überprüfbar sind:

„beugungsoptisch wirksame Merkmale:

- Hologramme
- Identigram
- Kinematische Strukturen

Personalisierungstechnik:

- Laserkippbilder
- Ausfüllschrift

**Material:**

- Fenster (zum Beispiel personalisiert)
- Sicherheitsfaden (personalisiert)
- Optisch variable Farbe

**Sicherheitsdruck:**

- Mikroschrift
- Guillochenstruktur“

Hieraus sollen mindestens drei Sicherheitsmerkmale aus unterschiedlichen Kategorien zufällig ausgewählt und auf Legitimität verifiziert werden. Der Prüfer muss hierfür bei Bedarf den zu identifizierenden Nutzer auffordern, durch Kippen des Ausweises bestimmte Variationen der Merkmale, beispielsweise der Hologramme oder des Laserkippbildes, sichtbar zu machen. Zusätzlich muss vom Prüfer auch untersucht werden, ob Auffälligkeiten bzgl. der Typografie, der Größe oder den Abständen der Textdaten bestehen. Weiter sind die Textdaten auf Plausibilität zu überprüfen. Hier ist zu kontrollieren, ob das Ausstellungs- und Gültigkeitsdatum in diesem Kontext Sinn ergeben. Zusätzlich ist die maschinenlesbare Zone (Machine Readable Zone, MRZ) auf Korrektheit zu überprüfen. Bei allen Prüfungen, die das Ausweisdokument betreffen, muss sich der Prüfer davon überzeugen, dass es sich um ein unbeschädigtes Dokument handelt und zudem nichts auf diesem Ausweisdokument zusätzlich, mit Ausnahme eines eventuell vorhandenen offiziellen Adressaufklebers bei Umzug, aufgebracht ist. Um technischen Manipulationen, wie Simulationen von Sicherheitsmerkmalen, vorzubeugen, muss der Mitarbeiter die zu identifizierende Person auffordern, bestimmte Merkmale wie Hologramme mit einem Finger teilweise zu verdecken und wieder offen zu legen, während diese sichtbar sind. Eine Untersuchung der Übergänge zwischen zugedecktem und noch sichtbarem Sicherheitsmerkmal soll eventuell vorhandene Manipulationen erkennbar machen. Die Dokumentennummer des Ausweisdokuments ist dem Prüfer von der zu identifizierenden Person zudem akustisch mitzuteilen.

Neben der Überprüfung des Ausweisdokuments findet eine Kontrolle der zu identifizierenden Person statt. Diese Kontrolle umfasst dabei vor allem die Sichtprüfung von der aktuellen Erscheinung der Person zum vorgezeigten Lichtbild auf dem Ausweisdokument. Der Prüfer hat sich hierbei zu vergewissern, dass es sich um die Person handelt, die durch das Lichtbild auf dem Ausweisdokument abgebildet ist. Des Weiteren muss der Prüfer während der Durchführung des Identifikationsvorgangs Fragen an den Nutzer richten. Diese sollen zum einen nochmal zur Verifikation der Legitimität der zu identifizierenden Person dienen, indem nach dem Alter und dem Geburtsdatum gefragt wird. Zum anderen muss durch das Gespräch aber auch verifiziert werden, dass der zu identifizierende Nutzer sich im Klaren darüber ist, wofür die Identifikation vorgenommen wird und dass dieser auch tatsächlich aus eigenem und freiem Willen handelt und nicht durch eine andere Person unter Druck gesetzt wurde, die

Identifikation vorzunehmen. Sollte der Prüfer durch schlechte Bild- oder Tonverhältnisse, dem Zustand des Ausweisdokuments sowie durch das Verhalten der zu identifizierenden Person Zweifel an der Legitimität des Identifikationsvorgangs haben, ist dieser sofort abzubrechen. In solch einem Fall kann der Mitarbeiter die zu identifizierende Person auf weitere, nach dem Geldwäschegesetz zulässige Identifikationsmöglichkeiten hinweisen. Falls bis dahin keine Zweifel an der Legitimität aufgetreten sind, wird die zu identifizierende Person abschließend dazu aufgefordert, diesen Identifikationsvorgang mittels einer über einen zweiten logischen oder physikalischen Kanal übermittelten Transaktionsnummer (TAN) zu bestätigen. Sollte die bestätigte TAN mit der tatsächlich übermittelten TAN übereinstimmen, ist der Identifikationsvorgang erfolgreich abgeschlossen.

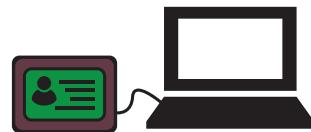
### Eigenschaften des VideoIdent-Verfahrens

Das VideoIdent-Verfahren bietet den Vorteil der Medienbruchfreiheit bei Online-Dienstleistungen, da dieses nahtlos in den Prozess mit eingebunden und direkt online am Kunden-Endgerät durchgeführt werden kann. Eine Anreise zur Filiale des Dienstleisters oder zu einem anderen Standort, an dem eine Identifikation durchgeführt werden kann, entfällt. Zur Durchführung des VideoIdent-Verfahrens ist der Kunde auf die Arbeitszeiten der Prüfer, die die Identifikation durchführen, angewiesen. Das bedeutet, dass das VideoIdent-Verfahren nur zu den vom mit der Durchführung des VideoIdent-Vorgangs betrauten Unternehmen vorgegebenen Zeiten durchgeführt werden kann. Für den Identifikationsvorgang entstehen beim Kunden in der Regel keine Kosten, da diese üblicherweise vom Dienstleister übernommen werden. Der Kunde muss nur über ein internethfähiges Endgerät mit einer Kamera, wie ein Notebook oder ein Smartphone, verfügen. Für den Dienstanbieter entstehen entweder Kosten für den selbstständigen Betrieb der Infrastruktur, sowie für die Bezahlung eigener Mitarbeiter, die die Identifikation durchführen, oder der Dienstleister greift auf Anbieter zurück, die den Identifizierungsvorgang für diesen durchführen und die Infrastruktur inklusive den Mitarbeiter stellt.

#### 5.2.4 Das eID Verfahren des elektronischen Personalausweises

Beim eID-Verfahren des elektronischen Personalausweises (ePA) handelt es sich um ein Identifikationsverfahren, bei dem sich der Besitzer des Ausweisdokuments gegenüber einem Dienstanbieter identifizieren und als legitimer Eigentümer authentifizieren kann. Damit dieser Prozess auf Seiten des Nutzers und Dienstanbieters möglich ist, sind auf beiden Seiten einige technische Voraussetzungen zu erfüllen [4]. Auf der Seite des Nutzers müssen ein ePA mit aktivierter eID-Funktion und festgelegter eID-PIN sowie ein Kartenlesegerät vorhanden sein, das mindestens zur Gerätekategorie B (Basis) gehört [5]. Darüber hinaus benötigt der Nutzer die sogenannte AusweisApp als Client-Anwendung auf seinem Endgerät.

**Abb. 5.4** eID-Verfahren  
des elektronischen  
Personalausweises



Auf der Seite des Dienstanbieters werden ein sogenannter eID-Server und ein Berechtigungszertifikat für die Durchführung der Identifikation benötigt. Der Dienstanbieter kann den eID-Server selber betreiben oder als Service von einem entsprechenden Anbieter nutzen. Der eID-Server steuert dabei auf Dienstanbieterseite die Durchführung des Identifikationsprozesses [14]. Die Berechtigung zum Erhalt eines Berechtigungszertifikats kann der Dienstanbieter bei der Vergabestelle für Berechtigungszertifikate (VfB) des Bundesverwaltungsamtes beantragen. Das eigentliche Berechtigungszertifikat erhält der Dienstanbieter mit der Berechtigung der VfB bei einem Berechtigungszertifikatanbieter (BerCA). Gleichzeitig erhält dieser hierdurch die Möglichkeit, bestimmte Daten des ePA, die für den Identifikationsprozess benötigt werden, auszulesen, siehe Abb. 5.4.

### Der Ablauf des eID-Verfahrens

Wenn die technischen Erfordernisse auf Nutzer- und Dienstanbieterseite gegeben sind, gliedert sich der Identifikationsvorgang grundsätzlich in folgende Schritte:

1. Aufbau einer Verbindung zwischen Nutzer (Client) und Dienstanbieter (Server).
2. Übermittlung des Berechtigungszertifikats und der dienstanbieterspezifischen Informationen an die AusweisApp des Nutzers (inklusive Darstellung innerhalb dieser).
3. Annehmen oder Ablehnen der Berechtigungen gemäß Berechtigungszertifikat beziehungsweise Einschränkung der Berechtigungen.
4. Bestätigung der erteilten Berechtigungen durch Eingabe der eID-PIN.
5. Durchführung des Authentifikations- und Autorisierungsvorgangs von Client und Server.
6. Auslesen der freigegebenen Daten des ePA.
7. Beendigung des Identifikations- und Authentifikationsvorgangs.

### Eigenschaften der eID-Funktion des ePA als Verfahren zur Fernidentifikation

Das Fernidentifikationsverfahren mittels eID-Funktion des ePA bietet sowohl für den Nutzer, als auch für den Dienstleister einige Vorteile. Zum einen entsteht eine sehr geringe Terminbindung, die das Verfahren vor allem auszeichnet. Dies bedeutet, dass die Identifikation zu jeder Tages- und Nachtzeit durchgeführt werden kann, weil diese unabhängig von Mitarbeitern des Dienstanbieters oder Drittspielstellers ist. Dadurch entsteht eine reibungslose Einbindung des Identifikationsprozesses in die Dienstleistung des Dienstanbieters, der eine Identifikation vorsieht. Zum anderen erwarten den Nutzer keine Wartezeiten bis zur Möglichkeit der Durchführung des Identifikationsprozesses. Weiter entstehen für

den Nutzer und den Dienstleister pro Identifikationsvorgang keine Kosten. Der Vollständigkeit halber darf dabei allerdings nicht außer Acht gelassen werden, dass für den Nutzer einmalige Kosten für die Beschaffung des Kartenlesegeräts anfallen. Falls der Nutzer die eID-Funktion nicht bei Ausstellung des ePA aktiviert hat, fallen ebenfalls einmalige Kosten für die nachträgliche Aktivierung an. Ferner entstehen für den Dienstleister Kosten für die Ausstellung des Berechtigungs-Zertifikats und dem eigenständigen Betrieb des eID-Servers beziehungsweise der Anmietung eines eID-Service eines Drittanbieters.

### 5.2.5 Das PostIdent-Verfahren der Deutschen Post AG

Das PostIdent-Verfahren der Deutschen Post AG basiert darauf, dass Mitarbeiter in den Postfilialen oder auch Postboten geschult werden, eine Identifikation einer natürlichen Person innerhalb einer Postfiliale oder beim Kunden vor Ort durchzuführen. Dies bietet vor allem Online-Dienstanbietern, die kein Filialnetz betreiben, die Möglichkeit, einen standardisierten Identifikationsprozess in ihre Dienstleistung einzubinden.

Im Folgenden wird das PostIdent-Verfahren innerhalb einer Postfiliale betrachtet, da dieses GwG-konform ist [6]. Beim PostIdent-Verfahren in der Postfiliale wird der Identifikationsvorgang durch einen Mitarbeiter der Postfiliale durchgeführt. Zur Vorbereitung des Identifikationsvorgangs benötigt der Kunde vom Dienstleister nur einen sogenannten PostIdent-Coupon, der Daten des Auftraggebers enthält.

Zusätzlich muss der Kunde zur Durchführung des Identifikationsvorgangs innerhalb der Postfiliale ein gültiges Ausweisdokument vorzeigen. Neben der Ausstellung des PostIdent-Coupons muss der Dienstleister keine weiteren Dienste einbinden, um die Identifikationsfeststellung mittels PostIdent nutzen zu können.

#### Der Ablauf des PostIdent-Verfahrens innerhalb einer Postfiliale

Sobald der Prozess beim Dienstleister abgeschlossen ist, der eine Identifizierung erfordert, und der Kunde den PostIdent-Coupon erhalten hat, kann der Identifikationsprozess innerhalb der Postfiliale beginnen:

1. Der Kunde erscheint während der Öffnungszeiten innerhalb der Postfiliale.
2. Der Kunde legt dem Mitarbeiter den PostIdent-Coupon vor.
3. Das Ausweisdokument wird durch einen Ausweisscanner eingelesen. Dabei werden die auf dem Ausweisdokument vorhandenen Sicherheitsmerkmale verifiziert.
4. Die Daten des Ausweisdokuments werden automatisch in das, später an den Dienstleister übermittelte, Formular übernommen.
5. Die übernommenen Daten werden vom Mitarbeiter noch einmal manuell auf Richtigkeit verifiziert und im Anschluss auf ein sogenanntes PostIdent-Formular gedruckt.
6. Die Richtigkeit der Daten auf dem PostIdent-Formular wird durch eine Unterschrift des Kunden und des Mitarbeiters bestätigt.
7. Das PostIdent-Formular wird an den Dienstleister versendet.
8. Nach Erhalt des PostIdent-Formulars ist die Identifizierung abgeschlossen.

### Eigenschaften des PostIdent-Verfahrens in der Postfiliale zur Fernidentifikation

Die Durchführung des PostIdent-Verfahrens innerhalb einer Postfiliale bietet, wie andere Fernidentifizierungsmaßnahmen, für den Kunden und den Dienstleister den Vorteil, dass der Identifikationsvorgang unabhängig von einer eventuell vorhandenen, aber weit entfernten Filiale des Dienstleisters durchgeführt werden kann. Zusätzlich ist eine Identifikation auch dann möglich, wenn der Dienstleister ausschließlich ein Online-Geschäft betreibt. Durch rund 14.000 Filialen mit Postdienstleistung, die 2010 in Deutschland existierten, ist es dem Kunden in der Regel möglich, ohne lange Anreise eine Filiale zu besuchen und so den Identifikationsprozess durchführen zu können. Anders als beim eID-Verfahren findet bei Online-Dienstleistungen durch die Identifikationsfeststellung ein Medienbruch statt, da die Identifikation offline in der Postfiliale stattfindet. Zusätzlich entsteht eine höhere Terminbindung, da der Kunde sich an die Öffnungszeiten der Postfiliale halten muss. Kosten für den Identifikationsvorgang werden durch die Post an den Dienstleister und nicht an den Kunden weitergegeben. Die Post berechnet dem Dienstleister dafür eine festgelegte Pauschale pro Identifikationsvorgang, die sich nach der Gesamtzahl der für den Dienstleister durchgeführten Identifikationsvorgänge pro Monat richtet. Ob der Dienstleister die Kosten auf den Kunden umlegt, bleibt diesem selbst überlassen.

#### 5.2.6 Vergleich der verschiedenen Identifikationsverfahren

Im Folgenden werden die mit dem GwG konformen Fernidentifizierungsmaßnahmen VideoIdent, eID-Funktion und PostIdent in der Postfiliale und die Vorlage eines Personalausweises miteinander verglichen. Gegenübergestellt werden dabei die folgenden vier Kriterien:

- Medienbruchfreiheit
- Terminbindung
- Kosten auf Kundenseite
- Nutzerkreis

Die Kategorie **Medienbruchfreiheit** bewertet, wie gut das Identifikationsverfahren in einen Online-Prozess eingebunden werden kann. Volle Medienbruchfreiheit bedeutet in diesem Fall also, dass das Verfahren online durchführbar ist.

Die zweite betrachtete Kategorie ist die **Terminbindung**. In dieser Kategorie wird dargestellt, ob das Verfahren zu jeder Zeit oder nur zu bestimmten Zeiten, wie nur werktags, durchführbar ist.

Die Kategorie **Kosten** betrachtet die Kosten auf der Kundenseite, die durch die Durchführung eines Identifikationsvorgangs für diesen entstehen. Hierbei wird bei allen Verfahren vorausgesetzt, dass der Kunde die technischen Voraussetzungen, falls erforderlich, zur Durchführung der Verfahren besitzt. Es wird daher bewertet, inwiefern ein durchzuführender Identifikationsvorgang Kosten beim Kunden verursacht.

Die letzte Kategorie betrachtet die Ausdehnung des **Nutzerkreises**. Hierbei wird bewertet, wie groß der mögliche Nutzerkreis für das Verfahren ist, siehe Tab. 5.1.

**Tab. 5.1** Vergleich der Identifizierungsmaßnahmen

	Personal- ausweis	Videoident	PostIdent Postfiliale	eID
Medienbruchfreiheit	-	+	-	+
Terminbindung	-	+ -	-	+
Kosten	+ -	+	+	+
Nutzerkreis	+	+	+	-

**Medienbruchfreiheit** Die Medienbruchfreiheit ist bei den Verfahren VideoIdent und eID zu 100 % gegeben, da beide Verfahren komplett online durchgeführt werden können. Das PostIdent-Verfahren in der Postfiliale setzt hingegen die Anwesenheit des Kunden während des Identifikationsvorgangs innerhalb der Filiale voraus. Das Verfahren ist daher nur offline durchführbar, was einen Medienbruch zur Folge hat. Die Vorlage eines Personalausweises kann nur offline durchgeführt werden.

**Terminbindung** Die geringste Terminbindung ist beim eID-Verfahren zu verzeichnen. Solange der Service verfügbar ist und keine Störungen auftreten, ist das eID-Verfahren jeden Tag 24 h nutzbar. Bei den Verfahren VideoIdent und PostIdent ist dagegen eine Terminbindung vorhanden. Im Falle der Servicezeiten der Deutschen Post, die zur Vergleichbarkeit herangezogen werden, weil diese neben dem PostIdent-Verfahren auch die Möglichkeit bieten, das VideoIdent-Verfahren durchzuführen, ist die Terminbindung beim VideoIdent-Verfahren geringer als beim PostIdent-Verfahren. Als Zeiten, in denen das VideoIdent-Verfahren genutzt werden kann, wird eine tägliche Servicezeit von 08:00 bis 22:00 Uhr angegeben. Die Öffnungszeiten einer großen Deutsche Post Filiale in Gelsenkirchen-Buer, die die Durchführung des PostIdent-Verfahrens anbietet, sind dagegen montags bis freitags von 08:30 bis 18:00 Uhr und samstags von 09:00 bis 13:00 Uhr.

**Kosten** Bei den drei Fernidentifizierungsverfahren fallen in der Regel keine Kosten beim Nutzer für die Durchführung einer Identifikation an. Stattdessen entstehen hierbei Kosten beim Dienstleister, wenn das Verfahren mithilfe eines spezialisierten Identifizierungsdienstleisters im Namen des Dienstleisters durchgeführt und die Infrastruktur von diesem genutzt wird. Diese Kosten werden aber typischerweise nicht auf den Kunden umgelegt. Bei der Vorlage eines Personalausweises hat der Nutzer in der Regel keine Gebühren, muss aber einen Aufwand betreiben, um physisch vor Ort zu sein.

**Nutzerkreis** Der mögliche Nutzerkreis, auf den die Dienstleister aktuell zurückgreifen können und damit das Maß an Erreichbarkeit und Wirtschaftlichkeit, sind beim PostIdent- sowie VideoIdent-Verfahren praktisch nicht eingeschränkt. Das Vorhandensein eines videofähigen Gerätes wie ein Smartphone oder ein Notebook mit integrierter Webcam kann heutzutage in vielen deutschen Haushalten als gegeben vorausgesetzt werden. Die Anzahl der Postfilialen ist zwar tendenziell abnehmend, aber immer noch durch ein Netz von rund 14.000 Filialen in Deutschland vertreten. Der Nutzerkreis des eID-Verfahrens ist dagegen aktuell noch stark eingeschränkt. So bietet zwar theoretisch jeder ePA prinzipiell die Möglichkeit, die eID-Funktion zu nutzen, praktisch ist aber bislang nur auf einem Drittel der Ausweisdokumente die eID-Funktion aktiviert und spielt international keine Rolle. Dies liegt daran, dass es bis vor kurzem jedem Bürger freistand, die eID-Funktion bei Ausstellung zu aktivieren oder nicht. Durch einen aktuellen Gesetzesbeschluss werden ab Juli 2017 nur noch Personalausweise mit aktivierter eID-Funktion ausgegeben.

### 5.2.7 Weitere Identifikationsverfahren

Im Folgenden werden eine paar weitere mögliche und zukunftsorientierte Identifikationsverfahren dargestellt.

#### Social-Ident

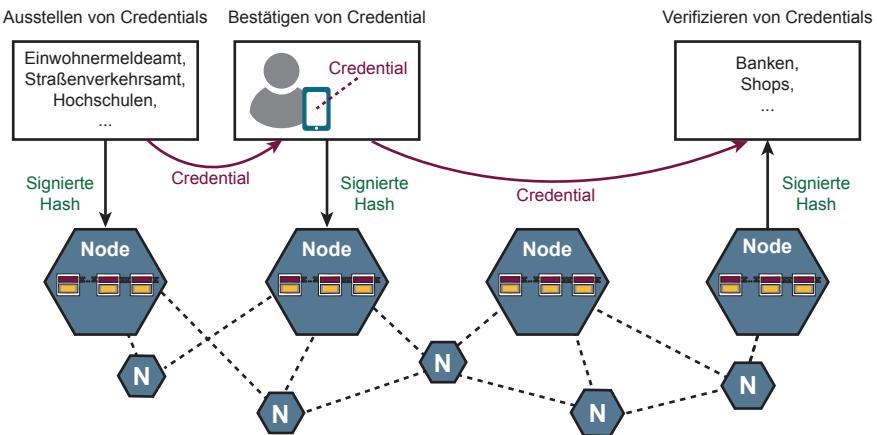
Ein Social-Ident-Verfahren identifiziert Personen anhand des Namens und eines Fotos der Person und basiert dabei auf den Informationen von den sozialen Netzwerken wie Facebook, LinkedIn und XING. Soziale Netzwerke beinhalten viele Informationen über Personen und wurden bisher bei der Identitätsverifikation nicht berücksichtigt. Das Social-Ident-Verfahren zeigt auf, welchen Wert soziale Netzwerke bei Verifikationsverfahren haben können. Es gibt viele Bereiche, in denen das Social-Ident-Verfahren zum Einsatz kommen kann, wie an Grenzübergängen oder bei polizeilichen Einsätzen bei Nichtvorhandensein eines Ausweises. Da auch viele Geflüchtete bei der Einreise keinen Ausweis besitzen, kann das Verfahren auch in diesen Fällen der Identitätsverifikation dienen [7]. Social-Ident kann auch für die Härtung von weiteren Identifikationsverfahren wie zum Beispiel Fernidentifizierung verwendet werden.

#### Self-Sovereign Identity

Bei Self-Sovereign Identity kontrolliert und besitzt ein Nutzer die Identitäten und sonstige Credentials.

Ein Credential ist eine Bescheinigung der Identität, Qualifikation, Befähigung oder Befugnis, die einer Einzelperson von einem Dritten, zum Beispiel Einwohnermeldeamt, Straßenverkehrsam, Hochschule usw. ausgestellt wurde.

Im Gegensatz zum Ansatz der „Enterprise-Centric-Identity“ erlaubt die „User-Centric-Identity“ den Nutzern die Kontrolle ihrer digitalen Identität. Die Nutzer selbst bestimmen, welche Attribute (persönliche Daten) bei einem Authentifizierungsvorgang übermittelt werden. Die Nutzer erhalten somit mehr Rechte, aber auch Verantwortlichkeit hinsichtlich ihrer persönlichen Informationen, siehe Abb. 5.5.



**Abb. 5.5** Self-Sovereign Identity

Beispiel:

Das Einwohnermeldeamt stellt Credentials über verschiedene Attribute einer Person aus. Attribute sind zum Beispiel Nachname, Vorname, Geburtsort, Geburtstag, Wohnort, Alter usw.

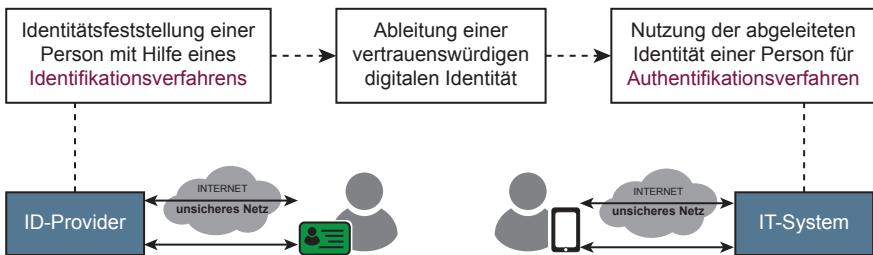
Das Einwohnermeldeamt übergibt die Credentials an die entsprechende Person und gleichzeitig werden Signaturen von Hashwerten der Credentials in einer „Self-Sovereign Identity“-Blockchain verfestigt.

Möchte ein Webdienst das Alter der Person verifizieren, dann kann diese Person das entsprechende Credential an den Webdienst versenden.

Der Webdienst kann dann aus der entsprechenden „Self-Sovereign Identity“-Blockchain den signierten Hashwert der ausstellenden Stelle entnehmen und das Credential mit der Altersangabe, zum Beispiel älter als 18 Jahre, verifizieren, siehe auch Kap. 14 „Blockchain-Sicherheit“.

### 5.2.8 Abgeleitete Identitäten

Die Identität einer Person ist einmalig und unverwechselbar. Sie wird anhand charakteristischer Eigenschaften definiert, der Identitätsattribute. Das können persönliche Daten wie Name, Geburtsort und Geburtsdatum sein. Mit einem hoheitlichen Dokument, beispielsweise dem Personalausweis, kann jede reale Person mithilfe von Identifikationsverfahren nachweisen, dass sie genau die ist, die sie zu sein behauptet [11].



**Abb. 5.6** Abgeleitete Identitäten – Zusammenhang zwischen Identifikations- und Authentifikationsverfahren

Bei Online-Diensten, wie Online-Banking, Webshops, sozialen Netzwerken oder E-Mail-Accounts, authentisiert sich ein Nutzer mit unterschiedlichen Authentifizierungsverfahren. Auch hier greifen Cyber-Sicherheitsmechanismen, die individuelle Attribute einer bestimmten Person zuordnen. Ein Beispiel ist die Verbindung von Nutzernamen und Passwort: Der Nutzernname beschreibt eine Person, die sich mit dem Passwort eindeutig authentisiert. Das IT-System ordnet das korrekte Passwort der Person zu und authentifiziert sie dadurch. Eine vertrauenswürdige digitale Identität liegt dann vor, wenn die zugehörige natürliche Person mithilfe eines Identifikationsverfahrens verifiziert werden konnte. Die klassische Nutzernamen/Passwort-Authentifikation beruht in der Regel auf einer Selbstauskunft des Nutzers und reicht bei sehr vielen Anwendungen nicht aus.

Der Begriff „Abgeleitete Identität“ wird mit der Umsetzung einer Identitätsfeststellung und der Authentifizierung einer Person verwendet, siehe Abb. 5.6.

Der Sinn einer abgeleiteten Identität – vertrauenswürdigen digitalen Identität – besteht darin, die starke Identitätsfeststellung einer realen Person zu nutzen, um diese vertrauenswürdige digitale Identität für die Authentifizierung in der virtuellen, digitalen Welt zu nutzen.

Da eine Identitätsfeststellung immer aufwendiger ist als ein Authentifikationsverfahren, ist diese Vorgehensweise ein pragmatischer Ansatz für die Verifikation von realen Personen für die Nutzung von IT-Systemen und -Diensten.

### 5.3 Authentifikationsverfahren

Für die Authentifizierung der Nutzer durch IT-Systeme sind prinzipielle unterschiedliche Authentifizierungsverfahren möglich. Im Folgenden werden das Konzept und die Prinzipien der grundsätzlichen Möglichkeiten von Authentifizierungsverfahren beschrieben.

## Generelle Authentifikationsverfahren

- Passwort-Verfahren
- Einmal-Passwort-Verfahren
- Challenge-Response-Verfahren
- Biometrische Verfahren

### 5.3.1 Passwort-Verfahren

Das einfachste und prinzipiell unsicherste, aber meist verwendete Authentifizierungsverfahren ist das Passwort-Verfahren. Hierbei werden ein Nutzernname und ein Passwort zwischen dem Nutzer und dem IT-System im Vorfeld abgesprochen.

Der Nutzer weist dann beim Zugriff auf das IT-System seine Identität (Nutzernname) nach, indem er das abgesprochene Passwort sendet. Das Passwort-Verfahren ist eine Authentifikation mit dem Nachweis der Kenntnis von Wissen – des Passworts.

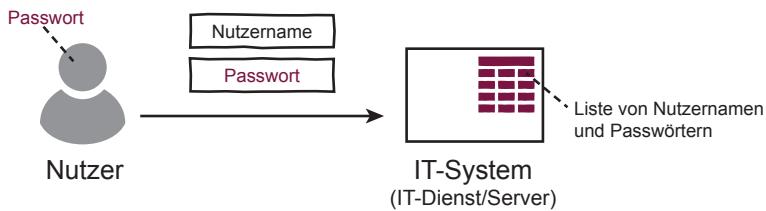
Falls das Passwort falsch war, wird der Zugang abgelehnt. Passt das Passwort zum Nutzernamen, wird der Zugang zum IT-System gewährt.

Das IT-System hat dazu eine Liste von Nutzernamen und Passwörtern von allen zugreifenden Nutzern zur Verfügung, um den Nachweis des Wissens überprüfen zu können.

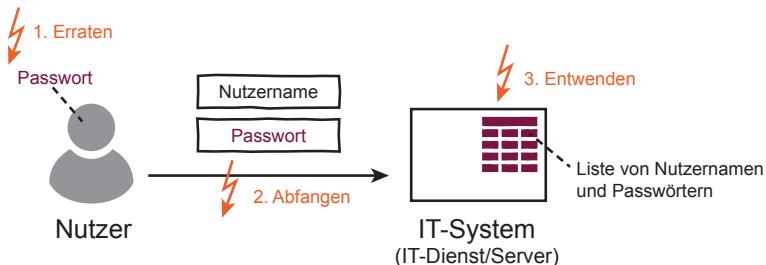
```
If (Check_Passwort (Nutzenname, Passwort, Liste mit Nutzernamen und Passworte))
    - suche Nutzername in der Liste
    - überprüfe, ob das gegebene Passwort mit dem Passwort in
      der Liste übereinstimmt
    return OK
  else
    return ERROR
```

Die Stärke dieses Authentifizierungsverfahrens beruht letztlich auf der Geheimhaltung und der Qualität des Passwortes. Eine besondere Schwäche des Passwortverfahrens ist unter anderem, dass gestohlene Zugänge, die durch Dritte missbraucht werden, von einem IT-System nicht direkt als Angriff erkannt werden können.

**Wichtig** Die Sicherheit des Passwortverfahrens beruht auf der Qualität und Geheimhaltung der genutzten Passworte, beim Nutzer, im IT-System und während der Übertragung/Eingabe.



**Abb. 5.7** Übersicht: Passwort-Verfahren



**Abb. 5.8** Angriffsvektoren bei Passwort-Verfahren

### Übersicht: Passwortverfahren

Wie in der Abb. 5.7 zu sehen ist, kennt der Nutzer sein Passwort und sendet dieses mit dem Nutzernamen zum IT-System, das den Nutzer authentifizieren möchte. Das IT-System kann mithilfe der Liste von Nutzernamen und Passwörtern überprüfen, ob der Nutzer das richtige Passwort eingegeben hat. Nutzernname und Passwort wurden vorher zwischen dem Nutzer und dem IT-System abgesprochen.

### Die prinzipiellen Angriffsvektoren bei der Authentifizierung mittels Passwort (siehe Abb. 5.8.) sind

1. Erraten des Passwortes durch Social Engineering oder Ausprobieren
2. Abfangen von Nutzernamen und Passwort während der Eingabe oder Übertragung
3. Entwenden der Liste von Nutzernamen und Passwörtern auf dem IT-System

#### 1. Angriffsvektor: Erraten des Passwortes durch Social Engineering oder Ausprobieren

Bei diesem Angriff versucht der Angreifer, das Passwort durch unterschiedliche Methoden zu erraten.

Der Angreifer kann unterschiedliche Angriffsmethoden durchführen:

- Er kann versuchen, das Passwort mithilfe der Kenntnis des persönlichen Umfeldes der entsprechenden Person zu erraten (Fußballfan in Gelsenkirchen = Passwort „Schalke04“).
- Er kann Passwörter, die oft genutzt werden, ausprobieren (Wörterbuchangriff).
- Er kann durch systematisches Durchprobieren aller möglichen Kombinationen (Brute-Force-Angriff) das richtige Passwort ermitteln.

a) Erraten des Passwortes durch Social Engineering

Der Angreifer kann mithilfe von Social Engineering das Umfeld einer Person ausspionieren. Er stellt über die sozialen Netzwerke fest, welches Auto die Person fährt, ob er einen Partner hat und wie der Partner mit Vornamen heißt, welchen Verein (Fußballverein, Handballverein, ...) er gut findet, wie der Hund und die Katze heißen usw. Aus diesen Umfeld-Informationen überlegt der Angreifer sich ein mögliches Passwort und probiert dieses aus. Die Wahrscheinlichkeit des Erratens des Passwortes eines bestimmten Nutzers auf der Basis von Social Engineering ist hoch. Aber auch das direkte Fragen des Nutzers nach seinem Passwort, zum Beispiel mit der Begründung, der Administrator zu sein, gehört zum Social Engineering.

b) Erraten des Passwortes durch Ausprobieren

Bei Erraten des Passwortes durch Ausprobieren gibt es zwei Varianten, die unterschieden werden.

### **Wörterbuchangriff**

Eine Variante des „Erratens des Passwortes durch Ausprobieren“ ist der sogenannte Wörterbuchangriff.

Bei einem Wörterbuchangriff oder auch „Dictionary Attack“ wird ein unbekanntes Passwort mithilfe einer vorhandenen Passwörterliste ermittelt. In der Passwortliste stehen Passwörter (Wörter, Phrasen, Zeichenketten, ...), die oft von Personen genutzt werden. Das sind gängige Wörter (Schalke04, Porsche911, Sabine906090, ...), aber auch neu kreierte sinnvolle Buchstabenkombinationen. Für einen Angriff werden alle Passwörter in der Passwörterliste nacheinander automatisch ausprobiert.

Bei dieser Angriffsmethode wird davon ausgegangen, dass das Passwort aus einer sinnvollen Zeichenkombination besteht. Dies ist erfahrungsgemäß viel zu oft der Fall. Die Verwendung einer Passwortliste ist erfolgsversprechend, da viele Nutzer im Internet dieselben unsicheren Passwörter verwenden und die Anzahl der möglichen Passwortkandidaten im Vergleich zu einem Brute-Force-Angriff (siehe nachfolgend) deutlich geringer ist. Häufig werden Passwortlisten verwendet, die aus geklauten/geleakten Datensätzen (Zuordnung von Nutzernamen und Passwörtern) von Online-Plattformen extrahiert werden.

Eine Möglichkeit, einen erfolgreichen Wörterbuchangriff zu verhindern, ist, keine leicht zu erratenden Passwörter zu verwenden. Es wäre zum Beispiel auch möglich zu überprüfen, ob ein ausgewähltes Passwort eines Nutzers in einem bekannten und verfügbaren Wörterbuch steht, das von Angreifern verwendet wird. Wenn ja, muss ein neues Passwort gesucht werden.

Aber auch ein Fehlbedienungszähler bei der Eingabe von Passwörtern hilft, den Angriff zu verhindern.

Der Wörterbuchangriff kann gegen unbekannte Passwörter, aber auch gegen unbekannte Nutzernamen durchgeführt werden.

### Brute-Force-Angriff

Eine weitere Variante des „Erratens des Passwortes durch Ausprobieren“ ist der sogenannte Brute-Force-Angriff. Bei diesem Angriff probiert der Angreifer jede mögliche Kombination eines Passwortes einfach aus. Alle Kombinationen von möglichen Passwörtern werden nacheinander automatisch ausprobiert, bis das richtige Passwort gefunden ist. Diese Verfahren führen immer zum Erfolg, wenn nicht die Anzahl der möglichen Kombinationen, die ausprobiert werden müssen, zu groß sind und daher praktisch nicht in einer angemessenen Zeit umgesetzt werden kann. Daher sollte die Anzahl der möglichen Zeichen des verwendeten Alphabets so groß wie möglich sein und das Passwort eine bestimmte Länge haben, damit dieser Angriff nicht erfolgreich umgesetzt werden kann.

Aber auch ein Fehlbedienungszähler bei der Eingabe von Passwörtern hilft, den Angriff zu verhindern.

### Sicherheitsmerkmal: Verwendetes Alphabet und die Länge von Passworten

Die Anzahl der möglichen unterschiedlichen Zeichen des verwendeten Alphabets definiert die nutzbaren Zeichen in einem Element, siehe Tab. 5.2. In der Tabelle sind es 10, 62 oder 86 Zeichen. Die Länge des Passwortes beschreibt die Anzahl der Elemente, die ausgewählt genutzt werden, wie 6, 8 oder 10. Die Anzahl der möglichen Kombinationen beschreibt die Komplexität der vollständigen Suche.

$$\text{Mögliche Kombinationen} = \text{Zeichenanzahl}^{\text{Passwortlänge}}$$

Hinweis:

Es wird davon ausgegangen, dass 1 Mio. Versuche in der Sekunde umgesetzt werden können.

**Tab. 5.2** Mögliche Zeichen des verwendeten Alphabets und die Länge von Passworten

Verwendetes Alphabet	Anzahl der möglichen Zeichen	Länge des Passwortes	Anzahl der möglichen Kombinationen (vollständiger Schlüsselraum)	Zeit der vollständigen Suche
0-9	10	6	$10^6 = 1.000.000$	1 s
		8	$10^8 = 100.000.000$	100 s
		10	$10^{10} = 10.000.000.000$	2,8 h
A-Z, a-z, 0-9	62	6	$62^6 = 56.800.235.584$	0,66 Tage
		8	$62^8 = 218.340.105.584.896$	6,9 Jahre
		10	$62^{10} = 839.299.365.868.340.224$	26.614 Jahre
A-Z, a-z, 0-9 (){}?!\$%&/= *+~,.;:>-_-	86	6	$86^6 = 404.567.235.136$	4,68 Tage
		8	$86^8 = 2.992.179.271.065.856$	94,9 Jahre
		10	$86^{10} = 22.130.157.888.803.070.976$	701.743 Jahre

Diese Tabelle zeigt deutlich, dass sowohl die Länge des Passwortes sowie die Anzahl der möglichen Zeichen des verwendeten Alphabets eine wichtige Rolle bei der Verhinderung eines Passwortangriffes spielen.

Außerdem spielt es eine Rolle, ob ein einfaches IT-System für einen Passwort-Angriff verwendet wird, der Webservice von Amazon dafür angemietet und genutzt wird oder die NSA mit spezieller Hardware diesen Angriff durchführt.

### Sicherheitsmechanismus: Passwortregeln

Im Folgenden werden Passwortregeln aufgestellt, die helfen, die Wahrscheinlichkeit von erfolgreichen Angriffen zu reduzieren:

- **Das Passwort nirgends notieren und niemandem mitteilen**  
*(Verhinderung eines Social-Engineering-Angriffes)*
- **Das Passwort darf nur dem Nutzer bekannt sein**  
*(Verhinderung, dass jemand anders mit dem Passwort zugreifen kann)*
- **Mindestlänge: zehn Stellen, besser zwölf Stellen**  
*(Verhinderung des Brute-Force-Angriffes)*
- **Es sollen Klein- und Großbuchstaben in Kombination mit Zahlen und Sonderzeichen verwendet werden**  
*(Verhinderung des Brute-Force-Angriffes)*
- **Die verwendeten Zeichen sollen auf den ersten Blick eine sinnlose Zusammensetzung sein**  
*(Verhinderung des Wörterbuchangriffes)*
- **Ein Passwort nur für einen Dienst verwenden**  
*(Verhinderung, dass der Diebstahl eines Passwortes die Sicherheit aller IT-Dienste betrifft)*
- **In angemessenen Zeitabständen ändern**  
*(Verhinderung des Brute-Force-Angriffes)*

Obwohl die Passwortregeln im Prinzip allen Nutzern bekannt sein sollten, werden immer noch schlechte Passwörter verwendet. Hier sind die „Top Ten“ deutscher Passwörter aus dem Jahre 2017 [8], die alle sehr leicht über Wörterbuchangriffe geknackt werden können.

1. 123456
2. 123456789
3. 1234
4. 12345
5. 12345678
6. hallo
7. passwort
8. 1234567
9. 111111
10. hallo123

### Sicherheitsmechanismus: Fehlbedienungszähler

Gegen Brute-Force-Attacken hilft eine Limitierung bei der Eingabe der Passwörter. Echte Nutzer geben ihr Passwort in der Regel spätestens im dritten Versuch richtig ein. Danach sollten IT-Systeme eine Pause vor der nächsten Eingabe erzwingen. Diese kann zunächst wenige Sekunden betragen, sollte aber immer länger werden. Nach einer unrealistischen Zahl von falsch eingegebenen Passwörtern sollte der Zugang gesperrt werden.

### Sicherheitsmechanismus: Passwörter überprüfen

Immer dann, wenn ein Passwort erstellt wird, werden als erstes die Passwortregeln überprüft. Danach wird zusätzlich noch ein Wörterbuchangriff durchgeführt, da auch Passwörter, die alle Regeln erfüllen, trotzdem in einem Wörterbuch gespeichert sein können und daher ein erfolgreicher Angriff durchgeführt werden kann.

## 2. Angriffsvektor: Auffangen von Nutzernamen und Passwort während der Übertragung

Bei diesem Angriff versucht der Angreifer, das Passwort während der Übertragung im Klartext mitzulesen. Dies ist prinzipiell immer dann möglich, wenn das Passwort von dem IT-System des Zugreifenden zu einem IT-System, auf dem der Zugriff stattfinden soll, über ein Kommunikationsnetz übertragen werden muss.

Aus diesem Grund darf ein Passwort nie im Klartext übertragen werden, weil sonst der Angreifer dieses mitlesen und missbräuchlich verwenden kann.

Der Angreifer kann das Mitlesen im Klartext an Übertragungsleitungen und Router im Gebäude oder im Internet umsetzen. Eine weitere Möglichkeit ist ein sogenannter Man-in-the-Middle-Angriff. Der Angreifer steht dabei physisch oder logisch zwischen den beiden Kommunikationspartnern und hat die vollständige Kontrolle über den Datenverkehr und kann die Passwörter mitlesen. Auch dieser Angriff muss erkannt und verhindert werden.

### Sicherheitsmechanismus: Verschlüsselung

Um das Mitlesen der Passwörter zu verhindern, wird die Kommunikation zwischen dem IT-System des zugreifenden Nutzers und des IT-Systems, auf dem der Zugriff stattfinden soll, SSL/TLS verschlüsselt.

Die SSL/TLS-Verschlüsselung sorgt zum einen für die Verifizierung der richtigen Domäne, das heißt, der Nutzer kann mithilfe des Domänen-Zertifikats einer Webseite sicher überprüfen, auf welche Webseite er zugreift, siehe auch Kap. 11 „Transport Layer Security (TLS)/Secure Socket Layer (SSL)“.

Durch die dynamische Verschlüsselung kann verhindert werden, dass das Passwort im Klartext gelesen werden kann.

Eine weitere Möglichkeit für den Schutz eines Remote-Zugriffes ist die Nutzung von Secure Shell (SSH).

**Tab. 5.3** Liste mit Nutzernamen und Passwort

Nutzername	Passwort
rainer.maier@gmx.de	Schalke04
peter.hop@gmail.com	Ulrike2003
klaus.mueller@t-online.de	X23y9gl!\$0_R

### 3. Angriffsvektor: Entwenden der Liste von Nutzernamen und Passwörtern auf dem IT-System

Bei diesem Angriff hat der Angreifer die Möglichkeit, auf die Liste von Nutzernamen und Passwörtern auf dem IT-System zuzugreifen. Danach kann er sich mit jedem Nutzernamen und dem entsprechenden Passwort erfolgreich anmelden.

Tab. 5.3. zeigt ein Beispiel einer Liste mit Nutzernamen und Passwörtern. In diesem Beispiel stehen Nutzername und Passwort im Klartext in der Liste auf dem IT-System. Wenn der Angreifer die Liste kennt, kann er sofort die entsprechenden Nutzerzugriffe erlangen. Wenn zum Beispiel Amazon die Passwörter in einer derartigen Liste speichern würde und Angreifer Zugriff darauf erlangen würden, wäre der mögliche Schaden sehr hoch. Aus diesem Grund werden die Passwörter nie im Klartext auf dem IT-System gespeichert.

### Sicherheitsmechanismus: Passwort-Hash-Verfahren

Eine etablierte Möglichkeit, einen Angriff auf die Passwörter zu erschweren, ist, nicht die Passwörter, sondern die entsprechenden Hashwerte der Passwörter auf dem IT-System zu speichern.

$$\text{Passwort-Hash} = H(\text{Passwort})$$

H	One-Way-Hashfunktion
Passwort-Hash	Hashwert des Passwortes

Wenn der Nutzer das Passwort eingibt, wird der entsprechende aktuelle Passwort-Hash im IT-System berechnet und mit dem richtigen Passwort-Hash in der Liste verglichen.

Sind beide Werte gleich, hat der Nutzer das richtige Passwort eingegeben.

```

if (Check-Passwort (Nutzername, Passwort, Liste mit Nutzernamen und Passwort-Hashes))
    - suche nach Nutzernamen in der Liste
    - berechne: Passwort-Hash = H (Passwort)
    - überprüfen, ob der Passwort-Hash mit dem in der Liste übereinstimmt
return OK
else
return ERROR

```

**Tab. 5.4** Liste mit Nutzernamen und Passwort-Hashes

Nutzername	Passwort-Hashes
rainer.maier@gmx.de	3C CB 4D A8 26 66 1D ... BF
peter.hop@gmail.com	87 30 28 B3 43 A3 17 ... 15
klaus.mueller@t-online.de	3C CB 4D A8 26 66 1D ... BF

Tab. 5.4. zeigt ein Beispiel einer Liste mit Nutzernamen und Hashwerten von Passwörtern (Passwort-Hashes). Wenn der Angreifer Zugriff auf diese Liste hat, muss er durch das Ausprobieren aller möglichen Passwörter und dem Vergleich mit dem Passwort-Hash auf das Passwort kommen, was sehr aufwendig ist und einer vollständigen Suche gleich kommt.

### Angriff auf Passwort-Hashes mithilfe von Rainbow-Table

In einer Rainbow-Table stehen bereits im Voraus errechnete und optimierte Passwort-Hash-Tabellen (Hashwerte und die zugehörigen Klartext-Passwörter), was dem Angreifer einen enormen Zeitvorteil verschafft, da das Suchen des Passwortes mit einer schnellen Suchanfrage in der Rainbow-Table umgesetzt werden kann. Aus dem Grund sollte der Rainbow-Table-Angriff durch die Einführungen von weiteren Sicherheitsmechanismen erschwert werden.

### Sicherheitsmechanismus: Salts

Ein Sicherheitsmechanismus, der den Rainbow-Table-Angriff unwirtschaftlich macht, ist der Einsatz von Salt. Beim Sicherheitsmechanismus „Salt“ wird an das Passwort vor dem „Hashen“ ein zufällig generierter Wert, das Salt, angehängt. Das Salt wird zusammen mit dem Passwort-Hash gespeichert, um das Passwort später überprüfen zu können.

$$\text{Passwort-Hash} = H(\text{Passwort} \mid\mid \text{Salt})$$

H	One-Way-Hashfunktion
Passwort-Hash	Hashwert des Passwortes
Salt	Zufallszahl, die in der Liste steht

Tab. 5.5. zeigt ein Beispiel einer Liste mit Nutzernamen, Passwort-Hashes und Salt. Wenn der Angreifer diese Liste kennt, muss er durch Ausprobieren aller möglicher Passwörter sowie aller möglichen Salt-Werte durch den Vergleich mit dem Passwort-Hash auf das Passwort kommen, was deutlich aufwendiger ist und den Rainbows-Table-Angriff verhindert.

**Tab. 5.5** Liste mit Nutzernamen, Passwort-Hashes und Salt

Nutzername	Passwort-Hashes	Salt
rainer.maier@gmx.de	15 A2 C7 39 F1 ... C9	FA 9C 13 0D 66 ... 1D
peter.hop@gmail.com	36 94 19 A1 5B ... 5A	10 29 C6 EC A3 ... 17
klaus.mueller@t-online.de	7C 91 38 C9 71 ... 1A	02 EE 74 1B 66 ... 1D

---

```

if (Check-Passwort (Nutzername, Passwort, Liste mit Nutzer-
namen, Passwort-Hashes, Salts))
    - suche nach Nutzername in der Liste
    - berechne: Passwort-Hash = H (Passwort || Salt)
    - überprüfen, ob der Passwort-Hash mit dem in der Liste
      übereinstimmt
return OK
else
return ERROR

```

### Randbedingungen für die Nutzung von Salt

- Salt muss eine hochwertige Zufallszahl sein.
- Salt muss für jeden Nutzer zufällig und unabhängig gewählt werden.
- Faustregel: Salt soll so groß sein wie die Ausgabegröße der Hashfunktion (SHA3: 256-Bit Hashwert).
- Ein n-Bit Salt verlangsamt einen Angriff um den Faktor  $2^n$ .

### Sicherheitsmechanismus: Pepper

Pepper basiert auf der gleichen Idee wie Salt. Pepper ist ein Sicherheitsmechanismus, der das Passwort mit einer geheimen Zeichenfolge kombiniert, bevor der Hash-Wert berechnet wird. Die Zeichenfolge „Pepper“ ist geheim und wird nicht in einer Liste gespeichert. Stattdessen wird die Zeichenfolge „Pepper“ sicher gespeichert. Die Zeichenfolge „Pepper“ ist für alle Passwörter gleich. Kennt der Angreifer die Zeichenfolge „Pepper“, so bringt der Sicherheitsmechanismus keinerlei Vorteile. Salt und Pepper können kombiniert werden.

**Passwort-Hash = H (Passwort || Salt || Pepper)**

H	One-Way-Hashfunktion
Passwort-Hash	Hashwert des Passwortes
Salt	Zufallszahl, die in der Liste steht
Pepper	Zufallszahl, die geheim ist

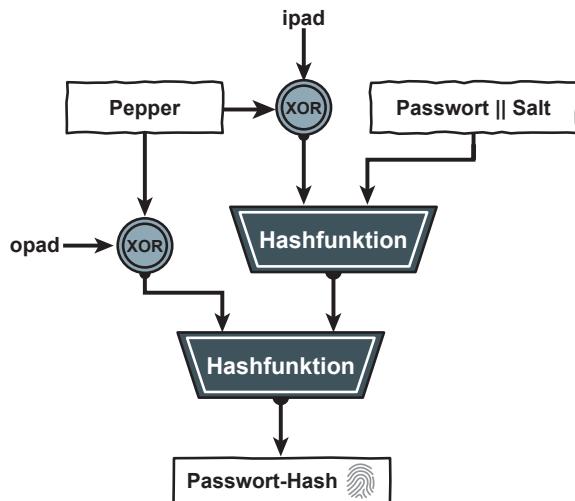
```

if (Check-Passwort (Nutzername, Passwort, Pepper, Liste mit
Nutzernamen, Passwort-Hashes, Salts))
    - suche nach Nutzername in der Liste
    - berechne: Passwort-Hash = H (Passwort || Salt || Pepper)
    - überprüfen, ob der Passwort-Hash mit dem in der Liste
      übereinstimmt
return OK
else
return ERROR

```

Eine andere Variante ist, Pepper als Schlüssel für den HMAC zu verwenden, siehe Abb. 5.9.

**Abb. 5.9** Berechnung des Passwort-Hash mit HMAC mit Salt und Pepper



```

If (Check-Passwort (Nutzername, Passwort, Pepper, Liste mit
Nutzernamen, Passwort-Hashes, Salts))
- suche nach Nutzername in der Liste
- berechne: Passwort-Hash = HMAC (Pepper, Passwort || Salt)
- überprüfen, ob der Passwort-Hash mit dem in der Liste übereinstimmt
return OK
else
return ERROR

```

## Weitere Angriffsvektoren bei Passwortverfahren

### Keylogger

Eine Keylogger-Funktion in Malware speichert alle Informationen, die über die Tastatur vom Nutzer in das eigene IT-System eingegeben werden. Diese Informationen sind hauptsächlich Nutzernamen und Passwörter. In regelmäßigen Abständen werden von der Malware die gespeicherten Informationen in sogenannte Drop-Zonen im Internet gesendet. Drop-Zonen sind Speicherbereiche von beliebigen Servern im Internet, von denen sich die Angreifer die Informationen unentdeckt holen können und damit Angriffe auf die Internet-Dienste der Opfer durchführen.

### Phishing

Mit einem Phishing-Angriff wird versucht, mithilfe von gefälschten Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Nutzers zu gelangen und damit Identitätsdiebstahl zu begehen. Es handelt sich dabei um eine Form

des Social Engineerings, bei dem die Gutgläubigkeit des Opfers ausgenutzt wird. Beim klassischen Phishing werden große Mengen von E-Mails wahllos an Empfänger verschickt, um sie dazu zu bringen, auf schädliche Links zu klicken oder vertrauliche Informationen preiszugeben.

Eine Phishing-Webseite sieht aus wie eine Original-Webseite, ist jedoch eine vom Angreifer präparierte Webseite. Nichts ahnende Nutzer werden auf einer präparierten Webseite aufgefordert, persönliche Daten einzugeben, die der Angreifer dann für sich nutzen kann.

Typisch ist dabei die Nachahmung einer vertrauenswürdigen Webseite, etwa einer Bank. Um keinen Verdacht zu erregen, wird das Corporate Design der betroffenen Stelle nachgeahmt, so werden etwa dieselben Firmenlogos, Schriftarten und Layouts verwendet. Der Nutzer wird dann auf einer solchen gefälschten Seite dazu aufgefordert, Nutzernname und Passwort einzugeben. Diese Daten werden dann vom Angreifer missbräuchlich für unautorisierte Zugriffe verwendet.

### **Spear-Phishing**

Beim Spear-Phishing werden die Empfänger sorgfältig recherchiert und ausgewählt und erhalten E-Mails, die auf sie persönlich zugeschnitten sind und viel glaubwürdiger wirken. Spear-Phishing richtet sich in der Regel gegen Mitarbeiter einer konkreten Organisation und zielt darauf ab, nicht autorisierten Zugriff auf vertrauliche Daten zu erhalten. Beispiele sind ein gezielter Angriff auf Banken, um Finanzbetrug umzusetzen oder ein Angriff auf eine Firma, um Geschäftsgeheimnisse zu erzielen.

### **Whaling**

Whaling ist ein Spear-Phishing-Angriff, der gezielt gegen hohe Führungskräfte gerichtet ist.

### **Über die Schulter schauen**

Vielen Nutzern ist nicht bewusst, wie einfach die Einsicht in oder das Erlangen von vertraulichen Informationen, wie Passwörter in öffentlichen Bereichen (beispielsweise im Flugzeug, im Zug oder im Cafe), sein kann. Es reicht zum Teil schon, wenn der Interessierte einen Blick über die Schulter wagt. Das Beobachten der Eingabe eines Passwortes ist für geübte Angreifer eine gute Möglichkeit, an Passwörter zu kommen.

### **Mit Social Engineering Nutzer motivieren, Passwörter zu nennen**

Mithilfe von Social Engineering werden Menschen so beeinflusst, dass sie Passwörter freiwillig nennen. „Social Engineers“ spionieren das persönliche Umfeld ihres Opfers aus, täuschen Identitäten vor oder nutzen Verhaltensweisen, wie Autoritätshörigkeit aus, um an Passwörter zu gelangen. Häufig dient Social Engineering oder auch Social Hacking dem Eindringen in ein fremdes IT-System, um vertrauliche Daten einzusehen und/oder Aktionen auslösen zu können.

### **Ein bekanntes Passwort auf einem anderen IT-System ausprobieren**

Falls ein Angreifer Nutzernamen und Passwort von einer Person hat, kann er versuchen, mit diesen Informationen weitere Zugänge zu anderen IT-Systemen zu erlangen. Hintergrund dieser Vorgehensweise ist, dass viele Nutzer den gleichen Nutzernamen und das gleiche Passwort für verschiedene Zugänge nutzen.

### **Sicherheitsfragen/Reset-Mechanismus/Passwort Recovery**

„Passwort vergessen“-Funktionen erlauben, ein Passwort zurückzusetzen. Eine oft genutzte Variante ist, Fragen, zu denen vorher Antworten hinterlegt worden sind, zu beantworten. Wenn die Frage richtig beantwortet ist, wird das Passwort zurückgesetzt, der Nutzer bekommt die Gelegenheit, ein neues Passwort einzugeben.

Typische Fragen sind:

- Wie lautet der Name Ihres ersten Haustieres?
- Welches war Ihre erste Telefonnummer?
- In welcher Stadt sind Sie geboren?

Da diese Fragen mithilfe von Social Engineering und sozialen Netzwerken leicht beantwortet werden können, ist dieses Verfahren nicht besonders sicher.

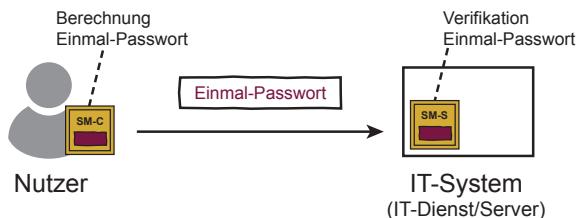
### **5.3.2 Einmal-Passwort-Verfahren**

Ein Einmal-Passwort (engl. One-Time Password – OTP, siehe Abb. 5.10) ist ein Authentifikationsverfahren, bei dem ein Passwort nur einmal für eine Session benutzt werden kann.

Damit wird ausgeschlossen, dass ein Angreifer ein Passwort abhören und erneut verwenden kann (Replay-Attacken). Man in the Middle-Attacken sind aber immer noch möglich.

Die Einmal-Passwörter werden in der Regel in einem Hardware-Sicherheitsmodul (SM-C) des Nutzers generiert. Die Verifikation findet in einem Hardware-Sicherheitsmodul (SM-S) des IT-Systems statt. Das Einmal-Passwort ist nur für eine bestimmte Zeit nach der Generierung gültig.

**Abb. 5.10 Einmal-Passwort**



Es gibt unterschiedliche Methoden, das Einmal-Passwort-Verfahren umzusetzen:

1. Die Einmal-Passwörter werden im Vorfeld bestimmt und verteilt

Das IT-System, auf das der Nutzer zugreifen möchte, generiert die Einmal-Passwörter und stellt diese den Nutzern vertraulich, vorher über einen sicheren Kanal, zur Verfügung. Bei dieser Methode kann eine Limitierung der möglichen Anmeldevorgänge vorgenommen werden, indem nur eine begrenzte Anzahl an Einmal-Passwörtern zur Verfügung gestellt werden. Wenn die Einmal-Passwörter zu Ende sind, muss der Nutzer neue beantragen.

Ein Beispiel für diese Methode sind TANs des PIN/TAN-Verfahrens (TAN-Liste). Bei dieser Methode werden keine Sicherheitsmodule für die Berechnung und Verifikation der Einmal-Passwörter gebraucht.

2. Der Nutzer kann Einmal-Passwörter nach einem definierten Verfahren berechnen

Nutzer und das IT-System berechnen nach einem definierten Verfahren das Einmal-Passwort während des Authentisierungsprozesses. Für das Verfahren können kryptografische Hash-Funktionen zur Generierung von nur kurzzeitig gültigen Einmal-Passwörtern oder zeitgesteuerte Generatoren verwendet werden. Ein bekanntes Beispiel für einen zeitgesteuerten Generator ist SecurID von der Firma RSA Security.

$$\text{Einmal - Passwort} = f(\text{Zeit} \mid\mid G_x)$$

f	Kryptografische Funktion (One-Way-Hashfunktion, Verschlüsselungsverfahren)
Zeit	Eine relative oder absolute Zeitangabe
G <sub>x</sub>	Geheimnis des Nutzers (X)

Voraussetzungen:

Beide Seiten kennen die Funktion f und das Geheimnis.

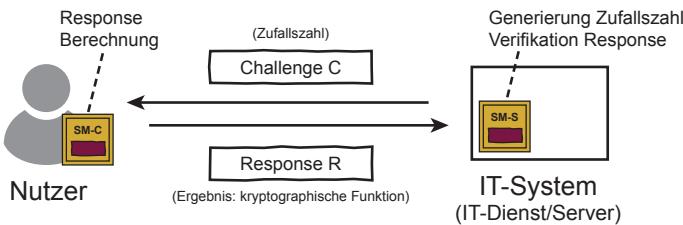
Damit auf der überprüfenden Seite nicht für jeden Nutzer (X) ein Geheimnis (G<sub>x</sub>) gespeichert werden muss, wird dieses in der Regel auf der Basis eines Master-Schlüssels berechnet.

$$G_x = H(\text{Nutzername} \mid\mid \text{Master-Schlüssel})$$

Durch Einmal-Passwörter können Nachteile des Passwort-Verfahrens überwunden werden. In der Praxis ist aber der Aufwand für das Verfahren hoch und wird nur für wichtige Anwendungen akzeptiert.

### 5.3.3 Challenge-Response-Verfahren

Beim Challenge-Response-Verfahren wird festgelegt, dass ein Nutzer sich gegenüber dem IT-System kryptografisch beweisen muss. Bei diesem Verfahren besitzt der Nutzer ein Geheimnis, zum Beispiel einen geheimen Schlüssel, mit



**Abb. 5.11** Challenge-Response-Verfahren

dem er als Beweis dafür, dass er den geheimen Schlüssel besitzt, spontan eine kryptografische Operation durchführen muss. In der Regel sendet das IT-System dem Nutzer eine Zufallszahl, die Challenge, die dann spontan kryptografisch verarbeitet und dem IT-System als Response gesendete wird. Das IT-System überprüft, ob der Nutzer die kryptografische Operation richtig durchgeführt hat. Falls ja, war die Authentisierung erfolgreich. Ansonsten gilt die Echtheit nicht als nachgewiesen und eine Kommunikation über das IT-System wird nicht zugelassen, siehe Abb. 5.11.

Aufgezeichnete Informationen können kein zweites Mal verwendet werden, da immer neue Zufallszahlen als Challenge gesendet werden. Bei einer Authentifizierung über unsichere Netze müssen Challenge-Response-Verfahren eingesetzt werden, um ein Abhören und daraus resultierende missbräuchliche Verwendung zu verhindern. Für die Speicherung der geheimen Schlüssel und die Berechnung der kryptografischen Verfahren werden auf beiden Seiten Hardware-Sicherheitsmodule verwendet. SM-C ist das Hardware-Sicherheitsmodul des Nutzers und SM-S des IT-Systems.

### Mögliche Methoden der Umsetzung eines Challenge-Response-Verfahrens

Es gibt unterschiedliche Methoden, wie Challenge-Response-Verfahren umgesetzt werden können. Im Folgenden werden drei mögliche Varianten exemplarisch beschrieben.

#### 1. Methode auf der Basis einer Hashfunktion und einem Geheimnis (G)

Challenge = Zufallszahl C

$$\text{Response} = H(C \mid\mid G_x)$$

H One-Way-Hashfunktion

C Zufallszahl (Challenge), die gehasht werden soll

G<sub>x</sub> Geheimnis des Nutzers (X), dessen Besitz bewiesen werden soll

Voraussetzungen:

Beide Seiten kennen die Hashfunktion und das Geheimnis.

Damit auf der überprüfenden Seite nicht für jeden Nutzer (X) ein Geheimnis ( $G_X$ ) gespeichert werden muss, wird die in der Regel auf der Basis eines Master-Schlüssels berechnet.

$$G_X = H(\text{Nutzername} \parallel \text{Master-Schlüssel})$$

## 2. Methode auf der Basis von symmetrischen Verschlüsselungsverfahren, wie AES und einem geheimen Schlüssel (gS)

Challenge = Zufallszahl C

$$\text{Response} = \text{AES}(C, gS_X)$$

AES Symmetrisches Verschlüsselungsverfahren

C Zufallszahl (Challenge), die verschlüsselt werden soll

$gS_X$  geheimer symmetrischer Schlüssel des Nutzers (X), dessen Besitz bewiesen werden soll

Voraussetzungen:

Beide Seiten kennen das Verschlüsselungsverfahren (zum Beispiel AES) und den geheimen Schlüssel ( $gS_X$ ).

Damit auf der überprüfenden Seite nicht für jeden Nutzer (X) ein geheimer Schlüssel ( $gS_X$ ) gespeichert werden muss, wird die in der Regel auf der Basis eines Master-Schlüssels berechnet.

$$gS_X = H(\text{Nutzername} \parallel \text{Master-Schlüssel})$$

## 3. Methode auf der Basis einer PKI und digitalen Signatur

Challenge = Zufallszahl C

$$\text{Response} = S(C, GS_X)$$

S Signaturfunktion, zum Beispiel RSA-Verfahren

C Zufallszahl (Challenge), die signiert werden soll

$GS_X$  geheimer asymmetrischer Schlüssel des Nutzers (X), der die Challenge signiert

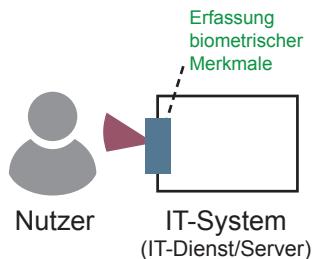
Voraussetzungen:

Beide Seiten kennen die Signaturfunktion und die öffentlichen Schlüssel der Nutzer stehen dem IT-System für die Verifizierung der Response zur Verfügung.

### 5.3.4 Biometrische Verfahren

Biometrie ist die Identifikation und Authentifizierung mittels biologischer Merkmale. Biometrische Authentisierung verwendet physiologische oder verhaltens-typische, also personengebundene Charakteristika. Der prinzipielle Vorteil von

**Abb. 5.12** Biometrische Verfahren



biometrischen Verfahren für die Identifikation und Authentifizierung liegt darin, dass biometrische Merkmale nicht unmittelbar gestohlen und im Allgemeinen nur schwer kopiert werden können [1], siehe Abb. 5.12.

Biometrische Merkmale können auf viele Arten gemessen werden. Die unterschiedlichen Verfahren messen das Tippverhalten an einer Tastatur, die Fingergeometrie, das Fingerlängenverhältnis oder die Handgeometrie. Weitere Möglichkeiten sind die Stimmanalyse, die Gesichtserkennung, die Erfassung der Unterschriftendynamik, des Netzhautmusters, des Irismusters oder des genetischen Codes (DNA-Analyse). Diese Verfahren können auch in unterschiedlichen Kombinationen zum Einsatz kommen.

### Eigenschaften des verwendeten biometrischen Merkmals

In der Praxis werden biometrische Merkmale in passive und aktive Merkmale aufgeteilt, siehe Tab. 5.6.

Es werden auch Kombinationen von aktiven und passiven Merkmalen verwendet, zum Beispiel die Erfassung des Gesichts und der Gesichtsdynamik beim Sprechen kombiniert mit der Stimmerkennung.

**Tab. 5.6** Biometrische Merkmale

Aktive Merkmale	Passive Merkmale
Unterschriftendynamik	Gesichtserkennung
Schreibverhalten	Retinamuster
Tippverhalten an der Tastatur	Irismuster
Stimmerkennung	Fingerabdruck (Daktylogramm)
Lippenbewegung beim Sprechen	Form des Ohres
Gestik/Mimik beim Sprechen	Handgeometrie
Bewegung (Gangartzyklus)	Venenmuster auf dem Handrücken
	Geruch
	DNA
	Thermogramm

## Nutzbarekeit von biometrischen Merkmalen

Damit ein Merkmal für ein biometrisches Verfahren verwendet werden kann, muss es die folgenden Eigenschaften besitzen [12]:

### 1. Universalität

Jede Person muss dieses biometrische Merkmal besitzen.

### 2. Einzigartigkeit/Einmaligkeit

Das biometrische Merkmal muss einzigartig in dem Sinne sein, dass es bei verschiedenen Menschen hinreichend verschieden ist. Keine zwei oder mehr Personen mit gleichem Merkmal dürfen existieren (Zwillinge).

### 3. Konstanz

Das Merkmal sollte sich im Laufe der Zeit möglichst wenig ändern. Kleinere Veränderungen können durch adaptive biometrische Verfahren ausgeglichen werden.

### 4. Merkmalsverbreitung

Ein Merkmal sollte, um für biometrische Verfahren geeignet zu sein, bei möglichst vielen der potenziellen Nutzer vorhanden sein. Kleine Bevölkerungsgruppen weisen jedoch gewisse Merkmale nicht auf beziehungsweise für sie sind bestimmte Verfahren nicht geeignet. So besitzt zum Beispiel ein kleiner Bevölkerungsanteil keine ausgeprägten Fingerabdruckstrukturen. In diesem Fall muss ein alternatives Verfahren zur Verfügung gestellt werden.

Besteht die Gefahr des Verlustes oder der Nichtverwendbarkeit eines biometrischen Merkmals, sollte ebenfalls ein Ersatzsystem vorgesehen werden.

### 5. Erfassbarkeit

Das verwendete biometrische Merkmal muss quantitativ messbar sein.

### 6. Möglichkeit zur willentlichen Beeinflussung durch den Nutzer

Einige biometrische Merkmale bieten die Möglichkeit, neben dem Hauptmerkmal eine zusätzliche Information zu übermitteln. So besteht beim Fingerabdruckverfahren die Möglichkeit, mehrere Finger zu registrieren und je nach Wahl des entsprechenden Fingers dem System eine Zusatzinformation zu geben. Bei der Stimmenkennung, die typischerweise mit einem festen, frei wählbaren Schlüsselwort verbunden ist, besteht diese Möglichkeit durch Anlernen und Speichern verschiedener Schlüsselwörter ebenfalls. Diese Eigenschaft gewinnt besondere Bedeutung in Anwendungsszenarien, in denen mit einer Erpressung des Merkmalsträgers gerechnet werden muss. Der Erpresser kann auf diese Weise einen stillen Alarm abgeben, ohne dass der Erpresser das erkennt.

## Falschakzeptanz und Falschrückweisung

Die wichtigsten Fehlerfälle bei biometrischen Verfahren sind die Falschakzeptanz und die Falschrückweisung.

**1. Falschakzeptanzrate** (FAR – engl. False Acceptance Rate) bezeichnet den Fall, dass eine nicht berechtigte Person aufgrund ähnlicher biometrischer Charakteristika akzeptiert wird. Die Falschakzeptanz stellt damit ein Sicherheitsmerkmal der biometrischen Verfahren dar.

FAR = fälschlich akzeptierte Zugriffe/unberechtigte Zugriffsversuche

**2. Falschrückweisungsrate (FRR – engl. False Rejection Rate)** bedeutet entsprechend, dass einer berechtigten Person der Zugang verweigert wird, weil die Übereinstimmungserfordernisse biometrischer Charakteristika zu rigide gehandhabt werden. Die Falschrückweisung stellt damit ein Komfortmerkmal der biometrischen Verfahren dar.

FRR = fälschlich zurückgewiesene Zugriffe/berechtigte Zugriffsversuche

Die Übereinstimmungserfordernisse bei biometrischen Merkmalen müssen immer einen gewissen Spielraum offen halten. Der Fingerabdruck zum Beispiel kann durch äußere oder physiologische Temperaturschwankungen oder unterschiedliche Stimmungen der Person (Schwitzen, Aufregung) geringfügige Abweichungen zeigen, die toleriert werden sollten. Ebenso müssen Rückstände von Staub, Schmutz oder Fett auf der Haut berücksichtigt werden. Die Wahrscheinlichkeit der Falschakzeptanz und der Falschrückweisung müssen in eine akzeptable Relation zum Sicherheitslevel gebracht werden. Aus diesem Grund kann aus biometrischen Merkmalen kein kryptografischer Schlüssel abgeleitet werden. Ein solcher beruht immer auf einer genauen mathematischen Berechnung, die keine Schwankungen zulässt.

### Diskussion der Akzeptanzraten

Bei der Diskussion der unterschiedlichen Akzeptanzraten können die praktischen Herausforderungen von biometrischen Verfahren dargestellt werden.

Die Betrachtung der Werte der Falschakzeptanzrate (FAR) in Abb. 5.13 beginnt ganz rechts (100 %). In diesem Zustand wird vom biometrischen Verfahren jeder Nutzer akzeptiert.

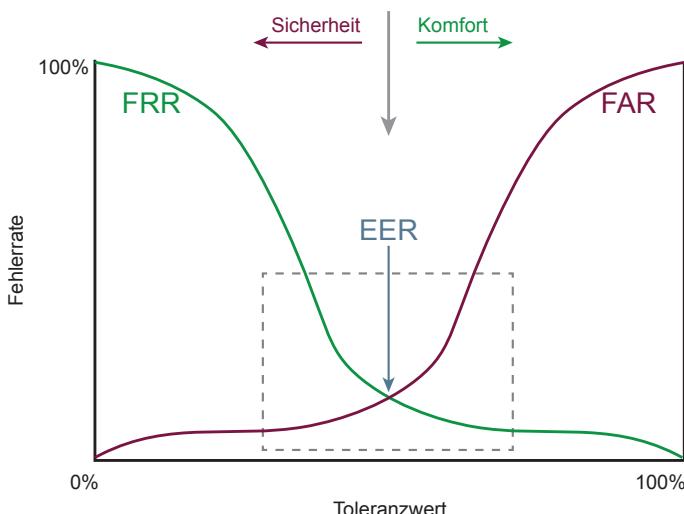


Abb. 5.13 Akzeptanzraten

Da kein autorisierter Nutzer abgewiesen wird, liegt die Falschrückweisungsrate (FRR) bei 0 %. Da jeder unautorisierte Zugriff akzeptiert wird, liegt die FAR bei 100 %. Je weiter der Toleranzwert verkleinert wird, desto seltener werden unautorisierte Zugriffsversuche akzeptiert – die FAR sinkt – und desto häufiger kann es vorkommen, dass autorisierte Nutzer abgewiesen werden – die FRR steigt. Bei einem Toleranzwert von 0 % geht die FRR gegen 100 % und die FAR gegen 0 %.

Wie hoch die Toleranz eines biometrischen Verfahrens eingestellt wird und welche der Fehlerraten somit minimiert wird, hängt von der Anwendung ab, in der das biometrischen Verfahren eingesetzt werden soll. Je kritischer die Sicherheit für ein IT-System ist, desto eher kann von einem Nutzer erwartet werden, eine fälschliche Abweisung hinzunehmen, wie im Hochsicherheitsbereich. Dagegen ist bei IT-Systemen, die als Massenanwendung eingesetzt werden sollen, die Nutzerakzeptanz, die bei häufiger fälschlicher Rückweisung sinkt, von größerer Bedeutung bezüglich des Komforts.

### 3. Equal Error Rate (EER)

Ein gutes Konzept ist, wenn die Akzeptanz und Rückweisung gleich groß sind, Equal Error Rate (EER).

Je niedriger die Equal Error Rate (EER), desto besser die Leistung des biometrischen Verfahrens und desto geringer die Gesamtfehlerrate. In Tab. 5.7 sind einige Fehlerraten von typischen biometrischen Verfahren dargestellt.

### Nutzerakzeptanz

Ein weiterer wichtiger Punkt bei der Verwendung biometrischer Verfahren ist die Akzeptanz bei den Nutzern. Die folgenden Aspekte sind hier entscheidend:

#### 1. Komfort/Praktikabilität

Hier spielen die Einfachheit der Handhabung, der Zeitaufwand bei der Registrierung, der Zeitaufwand im Normal- und im Sonderfall (False Rejection), die Häufigkeit der Aktualisierung des Musters, der Aufwand zur Referenzdatenerfassung, die Möglichkeiten einer zeitweiligen Ersatzlösung und der Aufwand dieser Ersatzlösung für den Nutzer eine wichtige Rolle.

#### 2. Vertrautheit/Transparenz

Hier ist entscheidend, ob die Vertrautheit mit bereits bekannten und etablierten Vorgängen und die Bereitschaft zur Kooperation beim Nutzer vorhanden sind. Dazu muss der Nutzer die Zusammenhänge und Abläufe verstehen.

**Tab. 5.7** FAR- und FRR-Werte für verschiedene biometrische Verfahren [9]

Biometrisches Verfahren	FAR in %	FFR in %
Fingerabdruck	0,001 ... 2	0,1 ... 5
Iriserkennung	0,0001 ... 1	0,1 ... 2
Gesichtserkennung	0,5 ... 2	1 ... 3
Handgeometrie	1 ... 4	1 ... 5

### 3. Belästigung

Für eine hohe Nutzerakzeptanz spielen die Hygiene und das Eindringen in die persönliche Schutzsphäre des Nutzers eine wichtige Rolle.

### 4. Vorurteile und Ängste

Vorurteile gegen den Vorgang der Registrierung im System oder der Anwendung, die Angst vor Missbrauch und die Frage, ob die Methode auch erkennungsdienstlich verwendet wird, sind hier entscheidend. Bei der Methode des Netzhaut-Scannings könnten die Nutzer beispielsweise Angst vor Verletzungen haben.

### Vergleich der verschiedenen biometrischen Verfahren

Die dargestellten Kriterien der Nutzerakzeptanz, der Einzigartigkeit, Konstanz und Verbreitung des Merkmals sowie der technischen und finanziellen Aufwendungen müssen in Relation zur Sicherheit des Verfahrens gesetzt werden [15] (Tab. 5.8).

Die linke Spalte zeigt die Rangfolge der biometrischen Verfahren in Bezug auf ihre Sicherheit (Accuracy). Das sicherste Merkmal ist der „genetische Fingerabdruck“ (DNA). Allerdings ist ein ausschlaggebender Nachteil die Nicht-Akzeptabilität: Für die tägliche Arbeit oder die häufige Anwendung ist dieses Verfahren nicht geeignet, es findet allenthalben bei der Fahndung nach Schwerverbrechern wie Gewalt- und Sexualstraftätern Anwendung. Die Iris- und Retina-Erkennungen bieten eine hohe Sicherheit, erfordern aber einen hohen technischen Aufwand. Sie können deshalb nur für Hochsicherheitsanwendungen eingesetzt werden. Für die alltäglichen Sicherheitsanforderungen in Industrie und Wirtschaft ist das Fingerabdruckverfahren sehr gut geeignet, da es hinreichend sicher und komfortabel ist.

**Tab. 5.8** Bewertung biometrischer Verfahren nach Sicherheit, Nutzerkomfort und Kosten

Rank	Accuracy	Convenience	Cost	MOC integration
1	DNA	Voice	Voice	Finger
2	Iris	Face	Signature	Voice
3	Retina	Signature	Finger	
4	Finger	Finger	Face	
5	Face	Iris	Iris	
6	Signature	Retina	Retina	
7	Voice	DNA	DNA	

## Anwendungen von biometrischen Verfahren

Biometrische Verfahren können unterschiedlich verwendet werden [12].

### 1. Identifikation: Feststellung der Identität

Eine Art der Nutzung ist die Feststellung der Identität. Bei der Personenidentifikation wird festgelegt, um welche Person es sich handelt. Dazu werden bei der Identifikation die aktuellen biometrischen Daten einer Person erfasst und mit den im Vorfeld erfassten biometrischen Referenzdaten einer Vielzahl von Individuen verglichen (1:n-Vergleich). Diese Referenzdaten sind beispielsweise in einer zentralen Datenbank gespeichert. Es findet somit eine Vielzahl von Vergleichen statt. Die Person wird als dasjenige Individuum identifiziert, dessen biometrischer Referenzdatensatz mit dem aktuellen biometrischen Datensatz der Person innerhalb der gewählten Toleranzgrenzen übereinstimmt.

### 2. Verifikation: Bestätigung der Identität

Verifikation bedeutet „Bestätigung der Identität“. Die Personenverifikation entscheidet die Frage, ob es sich bei einer Person um diejenige handelt, für die sie sich ausgibt.

Dazu werden bei der Verifikation die aktuellen biometrischen Daten einer Person erfasst und mit den im Vorfeld erfassten biometrischen Referenzdaten desjenigen Individuums verglichen, als das sich die Person ausgibt (1:1-Vergleich). Es findet ein Vergleich zweier Datensätze statt. Stimmen die beiden Datensätze innerhalb der gewählten Toleranzgrenzen miteinander überein, so wird bestätigt, dass es sich bei der Person um diejenige handelt, für die sie sich ausgibt.

## Angriffe auf Biometrie-Verfahren

Angreifer, die sich als jemand anderes ausgeben wollen, haben eine Vielzahl an Möglichkeiten, Biometrie-Verfahren zu überlisten. Im Folgenden werden zwei exemplarisch aufgezeigt.

- Vorzeigen eines Fotos  
Der Angreifer zeigt ein Foto der Person, für die er sich ausgeben möchte, mit dem Ziel damit positiv identifiziert zu werden.
- Generierung eines künstlichen Fingers  
Der Angreifer erstellt mit einem vorhandenen Fingerabdruck der Person, für die er sich ausgeben möchte, einen künstlichen Finger, mit dem Ziel, damit positiv identifiziert zu werden.

Durch die Erweiterung der Biometrie-Verfahren mit einer Lebendanalyse kann solchen Angriffen entgegengewirkt werden.

---

## 5.4 Mehrfaktor-Authentifizierung

Eine Multifaktor-Authentifizierung dient der Verifizierung der Identität eines Nutzers mittels der Kombination verschiedener unterschiedlicher und insbesondere unabhängiger Klassen von Authentifizierungsverfahren.

### Zweifaktor-Authentifizierung (2FA)

Eine häufige Variante ist die Zweifaktor-Authentifizierung (2FA) mit Besitz und Wissen, zum Beispiel Hardware-Sicherheitsmodul (Smartcard, USB-Token, ...) plus PIN zur Aktivierung des Hardware-Sicherheitsmoduls.

### Multifaktor-Authentifizierung (MFA)

Mit einer Multifaktor-Authentifizierung (MFA) kann noch flexibler reagiert und mit einer höheren Vertrauenswürdigkeit authentifiziert werden.

Die Klassen der Multifaktor-Authentifizierung sind:

- etwas, das der Nutzer besitzt, wie zum Beispiel ein Hardware-Sicherheitsmodul
- etwas, das der Nutzer weiß, wie zum Beispiel ein Passwort oder PIN
- etwas, das als körperliches Charakteristikum untrennbar zum Nutzer gehört (das Sein), wie zum Beispiel ein Fingerabdruck oder die menschliche Stimme

#### **Beispiele:**

Es wird ein Challenge-Respons-Verfahren mithilfe eines Hardware-Sicherheitsmoduls umgesetzt, das mit einem Passwort oder PIN aktiviert werden muss. Um den Nutzerbezug zu verstärken, muss der Nutzer noch mithilfe eines Fingerabdrucks oder Gesichtserkennung seine Identität zusätzlich verifizieren lassen.

#### **Weitere Informationen/Faktoren, die die Stärke einer Authentifikation beeinflussen, sind:**

Das IT-System, mit dem der Authentifikationsprozess umgesetzt werden kann:

- eigenes Notebook
- eigenes Smartphone
- fremdes IT-System
  - bei dem die Vertrauenswürdigkeit positive eingeschätzt werden kann
  - bei dem die Einschätzung der Vertrauenswürdigkeit nicht durchgeführt werden kann

Mit welcher **IT-Technologie** das IT-System, mit dem der Authentifikationsprozess umgesetzt wird, arbeitet:

- aktuelle IT-Technologie mit den neusten Patches
- altes Betriebssystem und alte Anwendungen
- Browser Fingerabdruck
  - Betriebssystem
  - Plug-ins
  - Schriftarten
  - Bildschirmgröße
  - Zeitzone
  - Hardware
    - Grafikkarte
    - Soundkarte

**Ort**, an dem der Authentifikationsprozess umgesetzt wird:

- im eigenen geschützten Büro
- am Flughafen, Bahnhof, ...
- in einem Cafe, Restaurant, ...
- auf einem öffentlichen Platz
- im Zug, im Flugzeug, ...
- ...

### **Rollout von Faktoren für die Authentifikation**

Die Faktoren für die Authentifikation sind nur so stark, wie die Kanäle über die sie verteilt wurden.

Zum Beispiel kann die MFA-Stärke nur gewährleistet werden, wenn durch Personalisierung des Smartphones über Wissensanteil (Transport-PIN), Besitz eines QR-Codes, Geheimnis per SMS (Bindung an SIM-Karte) usw. ein Missbrauch verhindert wird.

---

## **5.5 Konzept der risikobasierten und adaptiven Authentifizierung**

Die adaptive Authentifizierung entscheidet auf der Basis der Vertrauenswürdigkeit des zugreifenden Nutzers, der Kritikalität der konkreten Anwendung/Aktion und den Rahmenbedingungen des aktuellen Zugriffes, welche Authentifikationsverfahren zum Einsatz kommen sollen. Dieser risikoorientierte Ansatz erhöht das allgemeine Sicherheitsniveau und vermindert die Anzahl nicht notwendiger starker Authentifizierungen. Es wird das Optimum zwischen Sicherheit und Komfort angestrebt. Umgesetzt werden Konzepte der adaptiver Authentifizierung mithilfe von Mehrfaktor-Authentifizierung (MFA), die flexible, in Abhängigkeit des gerade notwendigen Sicherheitsniveaus, die passenden Authentifikationsverfahren auswählt.

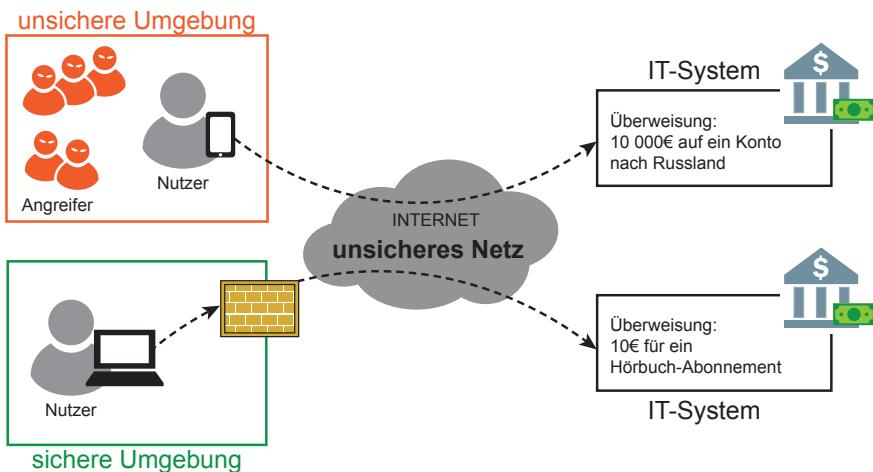
### **Beispiel einer Banküberweisung**

Überweisung eines Betrages von weniger als 25 EUR, was schon mehrfach erfolgreich umgesetzt wurde.

- auf Basis des erfolgreichen Logins zum Online-Banking
- keine weitere Authentifikation der Transaktion

Überweisung eines Betrages von mehr als 1000 EUR auf ein deutsches gut einschätzbares Konto einer vertrauenswürdigen Firma.

- Authentifikation durch Chip-TAN (Besitz) plus
- Authentifikation eines Passwortes (Wissen)



**Abb. 5.14** Risikobasierte und adaptive Authentifikation

Überweisung eines Betrages von mehr als 10.000 EUR auf ein ausländisches nicht einschätzbares Konto zu einer Zeit, in der der Bankkunde noch nie eine Überweisung veranlasst hat.

- Authentifikation durch Chip-TAN (Besitz) plus
- Authentifikation eines Passwortes (Wissen) plus
- Authentifikation mithilfe eines Fingerabdrucks (Sein)

Spannend für Unternehmen ist der Einsatz von Kontextinformationen wie dem Standort. Außendienstmitarbeitern wird in einer als sicher eingestuften Umgebung ein anderes Vertrauensniveau zugewiesen als in einer unsicheren Umgebung. Daran orientieren sich die Anforderungen des Zugriffs auf Unternehmensressourcen, siehe Abb. 5.14.

## 5.6 Modernes Multifaktor-Authentifizierungssystem und Identifikationsverfahren

Ein modernes Multifaktor-Authentifizierungssystem muss das komplexe Umfeld von IT-Eco-Systemen, einen flexiblen Schutz von Nutzerdaten und ein anwendungsspezifisches Vertrauensniveau bei der Authentifizierung des Nutzers berücksichtigen.

Daraus lassen sich die folgenden Anforderungen ableiten:

- hohe Sicherheit bei geringer Komplexität
- adaptive Balance zwischen Sicherheit und Nutzerfreundlichkeit
- einfache Integration
- Interoperabilität und Flexibilität

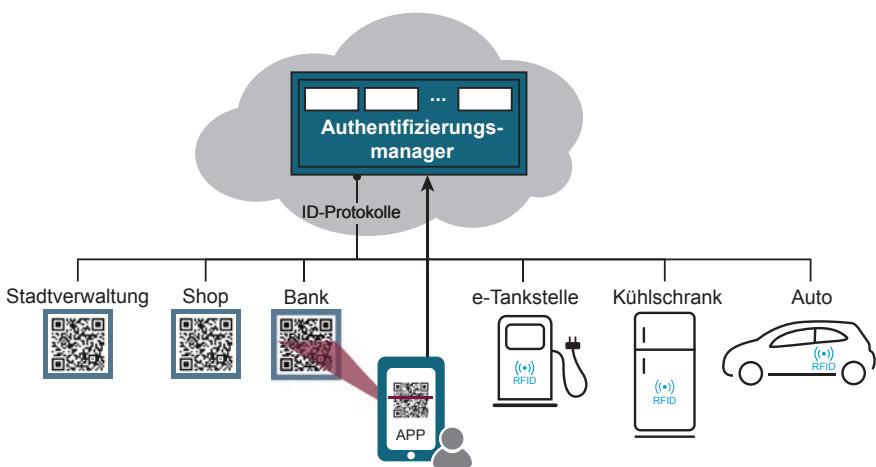
- Datenschutz und -sparsamkeit
- hohe Nutzerakzeptanz durch Verzicht auf Zusatzhardware, Transparenz, informationelle Selbstbestimmung und einfache Verwaltung und Nutzung

Im Folgenden wird eine Lösung einer handhabbaren und modernen Multifaktor-Authentifizierung vorgestellt (XignQR) [10].

Für den Einsatz dieses modernen Multifaktor-Authentifizierungssystems sind grundsätzlich vier Akteure notwendig, die durch eine Public Key-Infrastruktur (PKI) gestützt werden: die Smartphone-App (APP), der Authentifizierungsmanager und die Einbindungskomponente beim Dienstanbieter. Beim Dienstanbieter handelt es sich um ein IT-System, wie eine Webseite (Shop, Behörde, Bank, ...), ein ERP-System oder einen lokalen Arbeitsrechner. Um dem Nutzer den Zugriff auf den Dienst zu ermöglichen, muss er zuvor vom Dienstanbieter authentifiziert werden. Zu diesem Zweck ruft der Dienstanbieter einen QR-Code vom Authentifizierungsmanager ab, der dem Nutzer zum Beispiel auf der Webseite präsentiert wird. Der Nutzer kann dann mit Hilfe der APP den QR-Code einlesen, um die Authentifizierung zu starten. Die APP verarbeitet die darin enthaltenen Informationen und kommuniziert mit dem Authentifizierungsmanager, um den Nutzer schließlich zu authentifizieren, siehe Abb. 5.15.

Das Authentifizierungsergebnis und die angefragten Nutzerdaten werden dann vom Authentifizierungsmanager an den Dienstanbieter übermittelt.

Die Authentifizierung an sich wird über ein PKI-basiertes Challenge-Response-Verfahren unter Verwendung des persönlichen Schlüsselmaterials des Nutzers umgesetzt.



**Abb. 5.15** Einsatz von beteiligten Akteuren in unterschiedlichen Szenarien

### **Authentifizierungsmanager**

Als Trusted Third Party bildet der Authentifizierungsmanager die zentrale Komponente im modernen Multifaktor-Authentifizierungssystem und somit den Vertrauensanker. Als Vermittler zwischen dem Nutzer mit der APP und dem Dienstanbieter ist der Authentifizierungsmanager für die Verteilung der notwendigen Informationen und Ergebnisse während des Authentifizierungsprozesses zuständig.

Zum einen liefert er den QR-Code an den Dienstanbieter aus, während er dem Nutzer über die APP bescheinigt, um welchen Dienstanbieter es sich handelt und welche Informationen für die Erfüllung des Dienstes an den Dienstanbieter übermittelt werden müssen.

Zum anderen versichert der Authentifizierungsmanager dem Dienstanbieter, dass der Nutzer ordentlich und sicher authentifiziert wird.

Die Nutzerdaten werden bei der einmaligen Nutzerregistrierung erfasst und sicher im Authentifizierungsmanager gespeichert. Der Nutzer kann seine Daten jederzeit über den Authentifizierungsmanager verwalten.

Die Trennung von Authentifizierungsmedium, Smartphone inklusive personalisierter APP und Authentifizierungsmanager führt zu einem weiteren Vorteil. Während bei den meisten Authentifizierungssystemen ein großer Eingriff in die bestehende IT-Infrastruktur stattfinden muss, kann das moderne Multifaktor-Authentifizierungssystem, neben dem Betrieb in der eigenen Infrastruktur, auch komfortabel aus der Cloud genutzt werden.

Für die einfache Integration sollten die folgenden ID-Protokolle für die Kommunikation zwischen dem Authentifizierungsmanager und den Dienstanbietern unterstützt werden:

### **ID-Protokolle sind zum Beispiel**

- SAML
- OpenID Connect
- WebSocket-Protokoll mit JSON-Nachrichten
- LDAP
- RADIUS
- ...

### **Smartphone als MFA-fähiges, persönliches Authentifizierungsdevice**

Die APP agiert als vertrauenswürdige Nutzerschnittstelle, Kontrollkanal, QR-Code-Scanner und Token-Lesegerät. Die APP ist mit Schlüsselpaaren und den dazugehörigen Zertifikaten ausgestattet. Mit der Absicherung der APP und dem Schlüsselmaterial, mit der Möglichkeit zur Verwendung einer PIN und der Fähigkeit, das PKI-basierte Challenge-Response-Protokoll zu sprechen, bildet die APP das Softtoken (Software-Token). Hiermit wird das Smartphone zum Personal Authentication Device (PAD).

In Verbindung mit dem QR-Code als Einsprungpunkt für die Authentifizierung kann auf zusätzliche Hardware, wie zum Beispiel Lesegeräte, verzichtet werden. Dadurch ist es möglich, sichere nutzerfreundliche und adaptive Multifaktor-Authentifizierung, bestehend aus Besitz (Smartphone) und Wissen (PIN), oder Sein (Biometrie) oder allen Faktoren, optional auch mehrfach, zur Verfügung zu stellen.

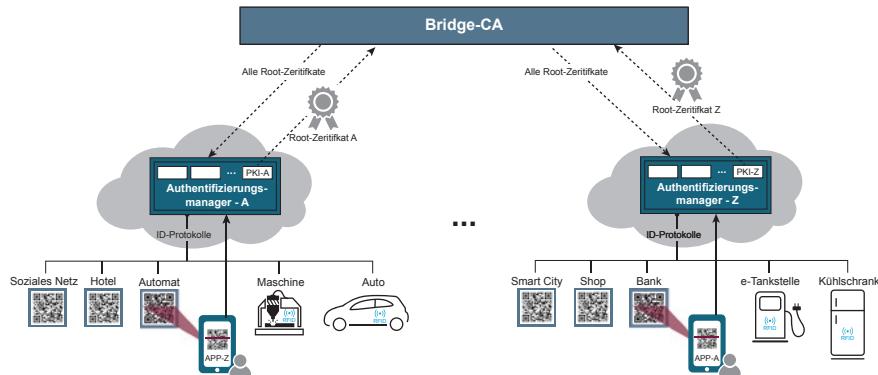
So lassen sich unterschiedliche Vertrauens- und Sicherheitsniveaus realisieren und zudem eine ausgewogene Balance zwischen Nutzerfreundlichkeit und Sicherheit erreichen.

Als Gegenstück zum Authentifizierungsmanager dient die Smartphone-App (APP) zur Anzeige für den Nutzer. Hierüber erhält der Nutzer Transparenz und wird über alle Abläufe und Prozesse informiert. Nach dem Scannen des QR-Codes werden die vom Authentifizierungsmanager übertragenen Daten dem Nutzer zur Gegenkontrolle in der APP angezeigt. Der Nutzer hat nun die Möglichkeit, den Vorgang zu bestätigen oder zu beenden und kann dabei optional verlangte Nutzerdaten ablehnen.

### Bridge-CA für eine organisationsübergreifende Authentifikation

Die Organisationen, die einen Authentifizierungsmanager betreiben, übergeben authentisch ihren öffentlichen Schlüssel in Form eines Root-Zertifikats an eine gemeinsame Bridge-CA.

Wenn das alle umgesetzt haben, dann erstellt die Bridge-CA eine Liste der Root-Zertifikate für alle beteiligten Authentifizierungsmanager. Danach können die Nutzer der Organisation X auch bei der Organisationen erfolgreich authentifiziert werden, siehe Abb. 5.16.



**Abb. 5.16** Bridge-CA

## **Identifizierung, Registrierung, Personalisierung – Basis für vertrauenswürdige Identitäten**

In heutigen IT-Eco-Systemen ist die Vertrauenswürdigkeit einer digitalen Identität für die Nutzung eines Dienstes, besonders für sicherheitskritische und personenbezogene Dienste, entscheidend und muss neben starker Authentifizierung auch eine zuverlässige Identifizierung bei der Nutzerregistrierung aufweisen.

Dazu unterstützt das moderne Multifaktor-Authentifizierungssystem vier grund-sätzliche Vertrauensniveaus. Unterschieden werden dabei die aufgenommenen persönlichen Daten des Nutzers und die Art der Verifizierung dieser Daten.

### **Vertrauensniveau 1: Nicht verifizierte Registrierung**

Der Nutzer gibt seine Daten persönlich ein. Die Daten werden nicht weiter mit einem Vertrauensanker verifiziert und beruhen nur auf der Selbstauskunft des Nutz-ers. Aufgrund des einfachen Vertrauensniveaus werden hier nur wenige Nutzer-daten erfasst, im einfachsten Falle handelt es sich um den Nutzernamen oder ein generiertes Pseudonym.

### **Vertrauensniveau 2: E-Mail verifizierte Registrierung**

Der Nutzer beweist seine Identität, indem er zeigt, im Besitz der angegebenen und funktionierenden E-Mail-Adresse zu sein. Damit wird nur die E-Mail-Adresse verifiziert, was allerdings für viele Dienste, wie zum Beispiel soziale Netzwerke oder Blogs, ausreichend ist.

### **Vertrauensniveau 3: Registrierung per VideoIdent**

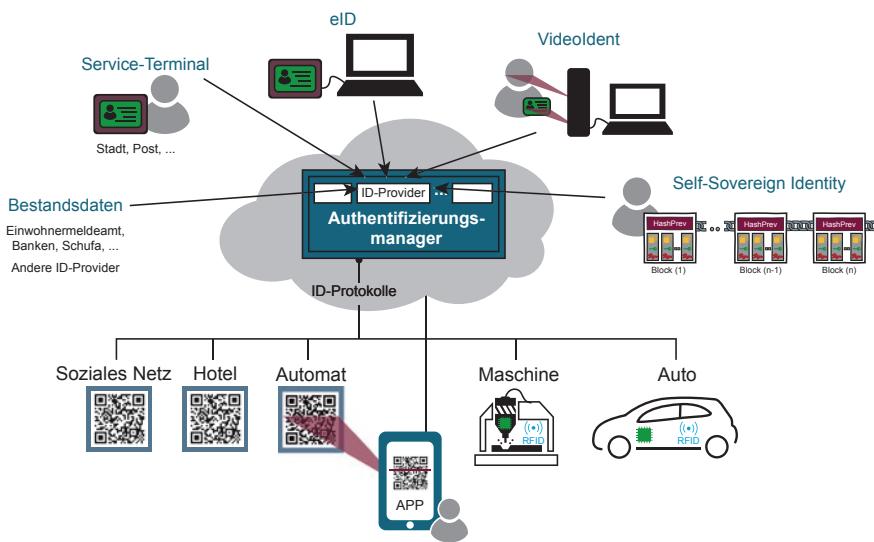
Der Nutzer beweist seine Identität mit dem VideoIdent-Verfahren. Dieses Ver-fahren gibt die Möglichkeit, jederzeit, ohne Zusatzhardware, eine starke Identifi-zierung durchzuführen.

### **Vertrauensniveau 4: Registrierung mit der eID-Funktion des Personalausweises**

Der Nutzer registriert sich mithilfe der Online-Funktion des neuen Personalaus-weses. Die Registrierung per eID resultiert im höchsten Sicherheitslevel. Diese Form des Identitätsnachweises ist besonders sicher, da es sich hier um einen rein elektronischen Nachweis mit einem sehr starken Vertrauensanker handelt. Der Nutzer benötigt für die Verwendung des neuen Personalausweises (nPA) ein Lese-gerät mit zusätzlich aktivierter Online-Funktion des Ausweises – ein Umstand, der nur bei den wenigsten Bürgern zutrifft – und eine spezielle Software auf seinem IT-System, den sogenannten eIDClient (AusweisApp2 oder OpenECardApp).

Aus den erfassten Daten wird eine Kennung (digitale Identität oder abgeleitete Identität) erzeugt, die zur Personalisierung der APP verwendet wird.

Dazu wird dem Nutzer ein sehr kurzlebiger QR-Code angezeigt. Nach dem Scannen des QR-Codes mit der APP, erhält der Nutzer über einen zweiten Kanal, in Abhängigkeit des Vertrauensniveaus, einen Verifizierungscode, der durch die



**Abb. 5.17** ID-Provider

APP verarbeitet wird. Stimmen die Informationen aus dem QR-Code mit den Informationen aus dem zweiten Kanal überein, wird die Registrierung mit dem Generieren der Schlüsselpaare, dem Erstellen und sicheren Speichern der Zertifikate und dem Festlegen der PIN abgeschlossen.

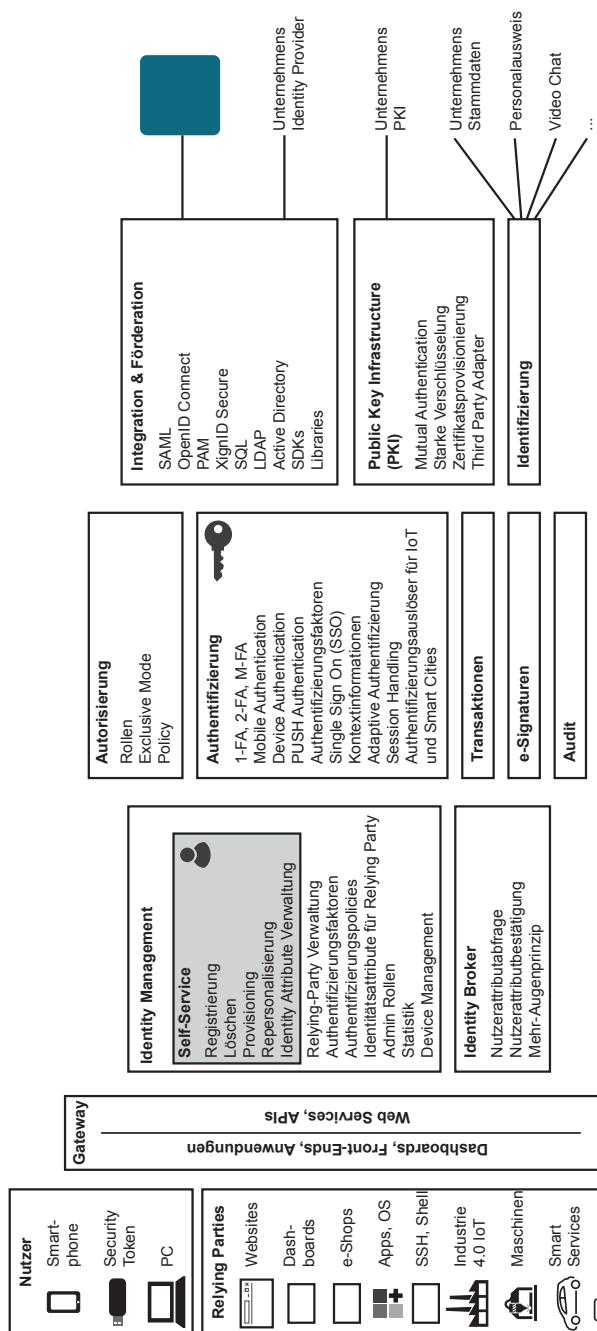
### Nutzung unterschiedlicher verifizierter Identitäten

Moderne Multifaktor-Authentifizierungssystem müssen in der Lage sein, verifizierte Identitäten von unterschiedlichen Quellen aufzunehmen.

In Abb. 5.17 ist zu sehen, dass als Quellen die Verifikation mithilfe der eID-Funktion des neuen Personalausweises (eigenes IT-System oder Service-Terminal), mit VideoIdent, Self-Sovereign Identity, aber auch über Bestandsdaten (Einwohnermeldeamt, Banken, Schufa, usw.) möglich ist.

### Weitere Attribute eines modernen Multifaktor-Authentifizierungssystems

In Abb. 5.18 ist eine Übersicht mit weiteren Attributen eines modernen Multifaktor-Authentifizierungssystems zu sehen, wie unterschiedliche Nutzer, verschiedene Relying Parties und Komponenten des Identity Managements und Identity Broker, verschiedenen Authentifizierungsklassen und -verfahren, die digitale Signatur usw.



**Abb. 5.18** Übersicht der Komponenten eines modernen Multifaktor-Authentifizierungssystems

## 5.7 Fast Identity Online Alliance (FIDO)

FIDO besteht aus einer Reihe von Sicherheitsspezifikationen für starke Authentifizierung. FIDO wird von der FIDO Alliance entwickelt, einer Non-Profit-Organisation, die die Authentifizierung auf Client- und Protokollebene standardisieren möchte. Die FIDO Alliance besteht aus Mitgliedern wie Google, Microsoft, Lenovo, PayPal, Visa, MasterCard, NXP, Nok Nok Lab, Bundesdruckerei usw.

FIDO-Spezifikationen unterstützen Multifaktor-Authentifizierung (MFA) und Kryptografie auf der Basis von Public Key-Verfahren. Im Gegensatz zu Passwortdatenbanken werden im FIDO-Konzept personenbezogene Daten, wie zum Beispiel biometrische Referenzdaten, lokal auf dem Endgerät des Nutzers gespeichert. Die lokale Speicherung biometrischer Referenzdaten und anderer personenbezogener Daten durch das FIDO-Konzept soll die Bedenken der Nutzer hinsichtlich der auf einem externen Server in der Cloud gespeicherten personenbezogenen Daten erleichtern. Durch das Abstrahieren der Protokollimplementierung mit Anwendungsprogrammierschnittstellen (APIs) reduziert FIDO auch die Arbeit, die für Entwickler erforderlich ist, um sichere Anmeldungen für mobile Clients zu erstellen, die unterschiedliche Betriebssysteme auf verschiedenen Arten von Hardware ausführen.

**Wichtig** Die FIDO-Alliance will mithilfe von Sicherheitsspezifikationen eine starke Multifaktor-Authentifizierung flächendeckend motivieren.

### 5.7.1 Ziele der FIDO Alliance

Die Bereitstellung einer starken Multifaktor Authentifikation berücksichtigt die Fähigkeiten des jeweiligen Endgeräts, das die Authentifikation durchführen soll:

- Wahlmöglichkeiten zwischen verschiedenen Authentifikationsmechanismen
- Vereinfachung der Integration neuer Authentifikationsmechanismen
- Erweiterbarkeit
- Verwendung offener Standards (wenn möglich)
- Entwicklung neuer offener Standards (wenn notwendig)
- Datenschutz
- Nutzerkomfort

Zur Erreichung der Ziele stellt die FIDO Alliance zwei Spezifikationen bereit:

- Universal Authentication Framework (UAF)
- Universal 2nd Factor (U2F)

### Universal Authentication Framework (UAF)

Ziel von Universal Authentication Framework (UAF) ist die Bereitstellung passwortloser und Multifaktor Authentifikation für Online-Dienste. Der Nutzer kann einen auf seinem Endgerät vorhandenen Authentifikationsmechanismus wählen und mit einem Online-Dienst registrieren, zum Beispiel Gesichtserkennung, Stimme, PIN oder Fingerabdruck.

Nach der Registrierung kann der entsprechende Authentifikationsmechanismus für die Anmeldung beim Dienst verwendet werden. UAF erlaubt die Auswahl der verwendbaren Authentifikationsmechanismen durch den Online-Dienst (Vertrauen in bestimmte Authentifikationsmechanismen).

### Universal 2nd Factor (U2F)

Das Ziel von Universal 2nd Factor (U2F) ist die Verbesserung der Sicherheit eines Online-Dienstes durch zusätzliche Zwei-Faktor-Authentifikation. Der Nutzer kann sich normal mit seinem gewohnten Authentifikationsmechanismus, wie Nutzernname/Passwort, einloggen.

Der Online-Dienst kann zu jeder Zeit einen zweiten Faktor (zum Beispiel NFC oder USB Hardware-Sicherheitsmodul) für eine weitere Authentifikation vom Nutzer verlangen. Der 2nd Faktor muss dementsprechend registriert werden.

## 5.7.2 Die FIDO-Architektur

### FIDO Client

Der FIDO Client realisiert auf der Client-Seite die FIDO Protokolle auf dem Endgerät des Nutzers. Er interagiert mit der FIDO Komponente „Authenticator“ und „User-Agent“ auf dem Endgerät. Er empfängt UAF-Protokoll-Nachrichten vom FIDO Server, siehe Abb. 5.19.

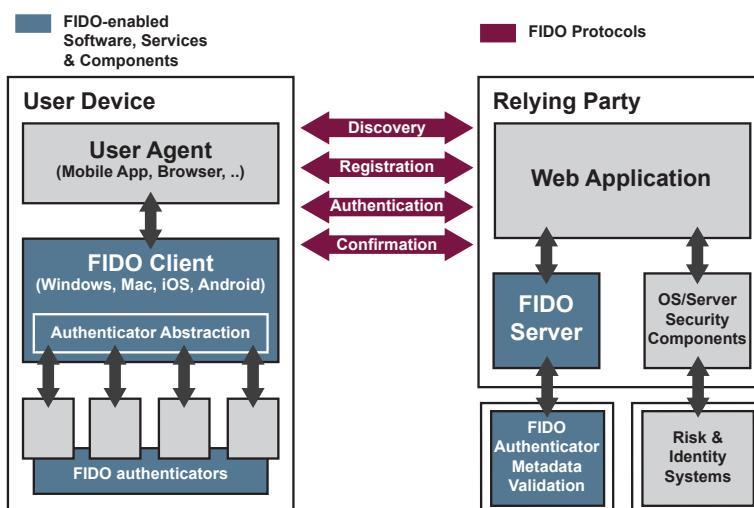


Abb. 5.19 Die FIDO-Architektur

## FIDO Server

Der FIDO Server realisiert die Server-Seite des FIDO Protokolls und interagiert mit Online-Diensten. Er sendet UAF-Protokoll-Nachrichten an den FIDO Client und validiert UAF-Protokoll-Antworten.

Zusätzlich verwaltet er FIDO Nutzerdaten und kennt UserID des Nutzers im Online-Dienst. Er steuert die Auswahl der „Authentikatoren“.

## FIDO Authenticator

Der FIDO Authenticator ist eine sichere Entität, die auf dem Endgerät des Nutzers vorhanden oder entsprechend verbunden ist. Er führt die Authentifizierung des Nutzers auf dem Endgerät durch und kommuniziert mit der Peripherie des Endgeräts (WebCam, NFC-Reader, Fingerabdrucksensor usw.), um den Nutzer zu authentifizieren. Der FIDO Authenticator generiert das Schlüsselmaterial für den Nutzer für das Challenge-Response-Protokoll und signiert die vom FIDO Server übermittelten Challenges.

## Meta-Daten

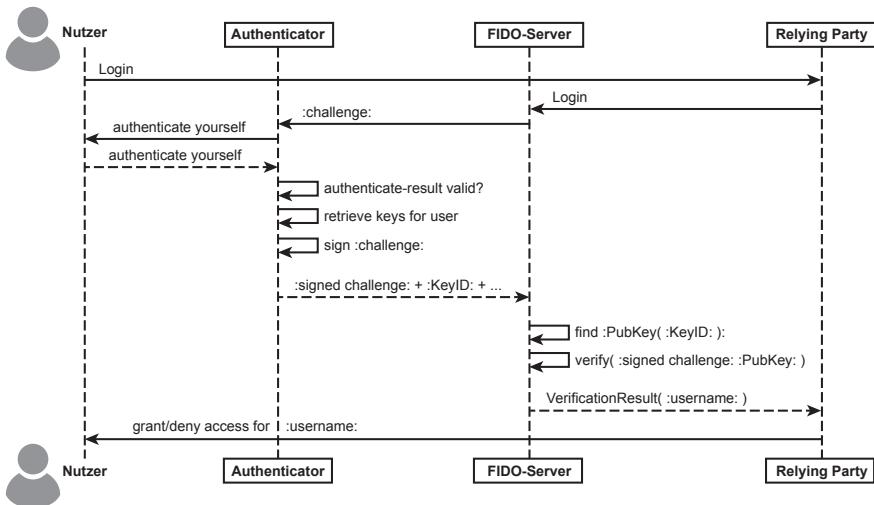
Die Meta-Daten sind Informationen über die bekannten und vertrauten Authentikatoren (IDs, Fähigkeiten usw.). IDs der Authentikatoren werden von der FIDO Alliance vergeben (nur vertraute Authentikatoren können verwendet werden). Die Meta-Daten bilden die Grundlage für die Auswahlmöglichkeiten des Nutzers.

## Identifikation des Nutzers

Während der Registrierung speichert der Authenticator nur die nutzerbezogenen Daten, die wichtig für die spätere Authentifizierung sind:

- KeyID (vom Authenticator generiert)
- Schlüsselmaterial des Nutzers
- je nach Implementierung, die authentikator-spezifischer Daten

KeyID ist in der Datenbank des FIDO Servers mit weiteren Nutzerdaten assoziiert und wird für das Auffinden des Nutzers verwendet. Nutzerdaten enthalten unter anderem die NutzerID des Nutzers im Online-Dienst. Der FIDO Server kann dem Online-Dienst das Authentifikationsergebnis für den entsprechenden Nutzer mitteilen, siehe Abb. 5.20.



**Abb. 5.20** Authentifizierung des Nutzers

### 5.7.3 Authentifizierung des Nutzers

Der Nutzer wird zweimal authentifiziert:

- Lokal durch den Authenticator (Biometrie, Passwort, ...)
- Über Challenge-Response-Verfahren durch FIDO Server

Beim Log-in via FIDO UAF übermittelt der FIDO Server eine Challenge an den FIDO Client. Der Nutzer authentifiziert sich lokal gegen den Authenticator. Bei erfolgreicher Authentifizierung schaltet der Authenticator das Schlüsselmaterial des jeweiligen Nutzers frei und bildet die Signatur zur übermittelten Challenge. Die generierte Signatur, die verwendete KeyID und Challenge werden an den Server übertragen. Der Server lokalsiert über die KeyID den entsprechenden Public Key, verifiziert die Signatur (valide => Auth-Erfolg) und übermittelt das Ergebnis zusammen mit der UserID des Nutzers an den Online-Dienst.

Die eigentliche Authentifikation findet mithilfe eines Authenticators auf dem Endgerät statt und das Ergebnis wird mithilfe eines Challenge-Response-Protokolls dem FIDO Server mitgeteilt, der wiederum den Online-Dienst informiert.

#### Besonderheiten

Die Authentifizierung gegenüber dem FIDO Server und somit des Online-Dienstes ist standardisiert über ein Challenge-Response-Verfahren. Die FIDO Client-/Authenticator-Specific-Module-Funktionalität ist standardisiert. Nur in Spezialfällen ist es wirklich notwendig, spezielle Komponenten mit erweiterter Funktionalität zu implementieren. Die Authentifizierung gegenüber dem Authenticator ist vom Hersteller abhängig. Auf welche Art und Weise der Nutzer vom Authenticator authentifiziert wird, geht über die Spezifikation hinaus.

## FIDO Protokolle

FIDO Protokolle dienen dem Transport der Informationen zwischen den einzelnen Beteiligten. Insgesamt gibt es vier Arten:

- Registration (Auffinden und Registrierung von „Authentikatoren“ bei Online-Diensten)
  - Authentication (Authentifizierung des Nutzers)
  - Confirmation (neben Authentifizierung zusätzliche Bestätigung einer bestimmten Transaktion)
  - Dereistration (De-Registrierung)
- 

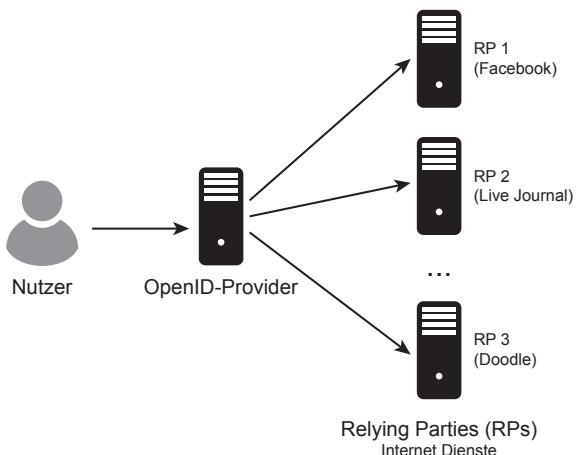
## 5.8 Identity Provider

Ein Identity Provider (Identitätsanbieter) ist ein zentrales Zugangssystem für Service-Provider-Dienste (Dienstanbieter), bei dem sich die Nutzer anmelden können. Identity Provider-Systeme bieten wichtige Cyber-Sicherheitsdienste für Service-Provider, wie die Authentifizierung eines Nutzers für Single-Sign-On (SSO) und die Autorisierung eines Zugriffs auf die Ressourcen der Identität über spezielle APIs. Dazu authentifiziert der Identity Provider den Nutzer und gibt diese Informationen an die Service Provider weiter. Die Kommunikation zwischen Identity Provider und Service-Provider erfolgt über entsprechende Sicherheitsprotokolle, wie zum Beispiel SAML, OpenID oder OAuth. Service-Provider können Dienste von Unternehmen, Webshops usw. sein. Dazu suchen sich Service-Provider vertrauenswürdige Identity Provider aus.

Im Folgenden werden exemplarisch einige Identity Provider-Technologien beschrieben.

### 5.8.1 OpenID

OpenID ist ein offener, dezentraler und URL-basierter Standard für Single Sign-On im Internet. Bei der Technologie Single Sign-On besitzt der Nutzer nur noch einen Identifikator (Nutzernamen) und ein stark gewähltes Passwort oder einen anderen Faktor. Der große Nutzen von SSO ist die einmalige Anmeldung beim Identity Provider (ID-Provider) und die anschließende Nutzung aller angeschlossenen Internetdienste (vgl. Abb. 5.21). Die Zugangsdaten eines Nutzers müssen nicht mehr an vielen Punkten im Internet, bei verschiedenen Internetdiensten, hinterlegt werden, sondern nur noch an einer zentralen und vertrauenswürdigen Stelle – bei dem Identity Provider [13].

**Abb. 5.21** OpenID-Provider

### Das OpenID-Protokoll

OpenID ist ein offener Standard für Single Sign-On im Internet. Der Sicherheitsdienst agiert dezentral und URL-basiert. Das bedeutet, dass ein Nutzer sowohl seine Identität als auch seinen Identity Provider frei wählen kann. Die Identifizierung eines Nutzers erfolgt grundsätzlich über den Beweis des „Besitzes“ einer URL, der sogenannten OpenID-Identität, zum Beispiel <https://openid.internet-sicherheit.de/NorbertPohlmann>. Vor der eigentlichen Nutzung des OpenID-Protokolls muss sich ein Nutzer eine OpenID-Identität erstellen. Hierfür sind grundsätzlich vier Schritte notwendig:

1. Wahl des OpenID-Providers:

Der Nutzer wählt einen vertrauenswürdigen OpenID-Provider (OP), der fortan für die Bestätigung der digitalen Identität zuständig ist. Dieser repräsentiert den Identity Provider im SSO-Gesamtbild, siehe Abb. 5.21.

2. Wahl des Identifikators:

Der Nutzer wählt eine URL, die eigentliche OpenID-Identität. Diese URL repräsentiert die digitale Identität des Nutzers und wird den Internetdiensten anstelle eines Nutzernamens präsentiert. Ein Nutzer hat fortan nicht mehr viele verschiedene Nutzernamen, sondern nur noch einen Identifikator: die OpenID-Identität.

3. Eingabe persönlicher Informationen:

Wenn gewünscht, kann der Nutzer Informationen wie etwa Vor- und Zuname oder E-Mail-Adresse bei dem OP hinterlegen. Da die Eingabe der Informationen dem Nutzer freigestellt ist, kann dieser zum Beispiel lediglich ein Pseudonym hinterlegen oder ein vollständiges Profil. Mittels des OpenID-Protokolls kann ein Internetdienst nicht nur die Authentisierung des Nutzers anfragen, sondern optional auch weitere Informationen. Diese gibt der Nutzer in jedem Fall gesondert frei.

**4. Festlegung der Zugangsdaten:**

Bei der Registrierung der OpenID-Identität hinterlegt der Nutzer seine Zugangsdaten. Das sind für gewöhnlich eine Kombination aus Nutzernamen und Passwort oder weitere Faktoren. Hierüber wird der Nutzer vom OP wiedererkannt. Nachdem ein Nutzer einmalig eine OpenID-Identität angelegt hat, können sämtliche OpenID unterstützenden Internetdienste genutzt werden. Dies kann im Grunde ebenfalls in vier Schritte eingeteilt werden:

**1. Aufruf der Log-in-Seite:**

Der Nutzer möchte einen OpenID-fähigen Internetdienst nutzen und ruft die entsprechende Webseite mit dem Log-in-Formular auf.

**2. Behauptung der Identität:**

Statt wie gewohnt eine Nutzernamen-Passwort-Kombination einzugeben, übermittelt der Nutzer lediglich die OpenID-Identität. Der Nutzer behauptet seine digitale Identität darüber, dass er den Besitz einer URL, der OpenID-Identität, vorgibt.

**3. Beweis der behaupteten Identität:**

Der Internetdienst führt den Beweis der behaupteten Identität nicht selbst durch, sondern leitet den Nutzer zu dem entsprechenden OpenID-Provider weiter. Der Nutzer meldet sich dort, sofern noch

nicht geschehen, an. Wenn der Log-in, das heißt, die Authentisierung beim OP erfolgreich verlief, hat der Nutzer den Besitz der OpenID-Identität und somit auch die eigene digitale Identität bewiesen. Dieses Ergebnis teilt der OP dem Internetdienst mit und leitet den Nutzer zurück.

**4. Nutzung des Internetdienstes:**

Wenn die Antwort des OpenID-Providers positiv ausfällt, so kann der Internetdienst die Identität des Nutzers als bestätigt ansehen und die Nutzung freigeben. Die Bestätigung der Identität wurde faktisch ausgelagert.

**Vor- und Nachteile der Auslagerung der Authentifizierung**

Die Auslagerung der Authentifizierung seitens der Internetdienste hin zu dem OpenID-Provider bringt mehrere Vorteile, birgt aber auch verschiedene Gefahren. Ein Vorteil ist die Zentralisierung der Authentisierung. Der Nutzer kann sich die Instanz für den Beweis der Identität bewusst aussuchen und diese besser sichern. Die Zugangsdaten sind nicht mehr bei vielen Internetdiensten verteilt, sondern liegen nur noch bei dem eingesetzten OP. Für die Internetdienste, die OpenID einsetzen, ergibt sich der Vorteil, dass verschiedene Methoden zur Authentisierung angeboten beziehungsweise genutzt werden können. Ein Internetdienst kann beispielsweise das Log-in mittels Nutzernamen und Passwortanbieten, aber indirekt auch sämtliche Methoden, die der OP des Nutzers anbietet. Der Internetdienst lagert die Authentisierung des Nutzers aus.

Nachteilig an OpenID beziehungsweise an SSO im Generellen ist der Single Point of Failure.

Ein Angreifer kann mittels eines DDoS-Angriffs den zentralen OpenID-Provider lahmlegen und somit die Log-in-Versuche des Nutzers erschweren oder temporär unmöglich gestalten. Schließlich ist OpenID hochgradig anfällig

gegenüber Phishing. Kopiert ein Angreifer die Log-in-Seite und „phisht“ so das Passwort eines Nutzers, kann er diese Identität missbrauchen. Eine Maßnahme gegen die Hauptkritik von OpenID – Phishing – ist der Einsatz einer Multifaktor-Authentisierung.

### 5.8.2 OAuth 2.0

Neben der Identifizierung und Authentifizierung von Nutzern im Internet ist es wichtig, dass Identity Provider geeignete Schnittstellen für die Autorisierung von Zugriffen auf schützenswerte Ressourcen über verschiedene Instanzen hinweg anbieten. Hierfür hat sich das OAuth 2.0 Protokoll im Internet durchgesetzt. Konzeptionell ist das OAuth 2.0-Protokoll lediglich für die Autorisierung zuständig. Abhängig von dem benötigten Sicherheitslevel eines Internetdienstes kann ein erfolgreicher Autorisierungsnachweis mittels OAuth 2.0 ebenfalls als eine Pseudo-Authentifizierung betrachtet werden. Für eine höhere Cyber-Sicherheit sollte OAuth 2.0 jedoch grundsätzlich um ein zusätzliches Protokoll für die Authentifizierung ergänzt werden. Hierfür kann beispielsweise der offene Standard OpenID Connect verwendet werden.

Die Protokollabläufe von OAuth 2.0 sind schematisch in Abb. 5.22 aus Sicht einer nativen Anwendung auf einem Endgerät dargestellt. In dieser Darstellung wird davon ausgegangen, dass die Anwendung auf eine geschützte Ressource auf den Servern einer fremden Instanz zugreifen möchte. Die Autorisierung des Zugriffes erfolgt durch den Besitzer der Ressource. In den „Best Current Practice“ nach RFC 8252 wird für diesen Anwendungsfall aus Gründen der Benutzerfreundlichkeit und Sicherheit empfohlen, dass die Kommunikation über einen externen Browser auf dem Endgerät erfolgt. Bei den beiden Endpunkten „Authorization Endpoint“ und „Token Endpoint“ handelt es sich um berechtigte Instanzen für die

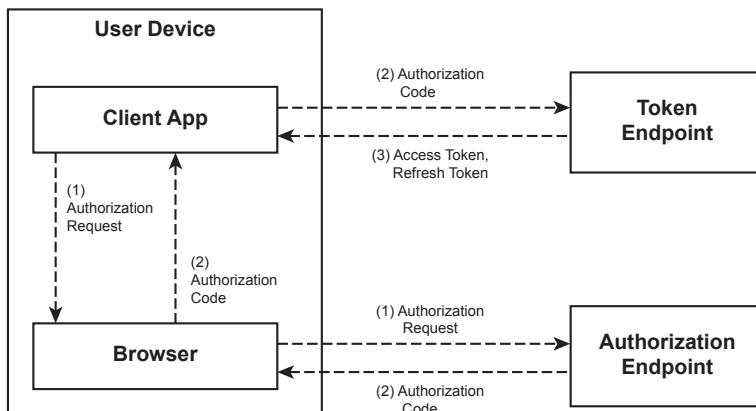


Abb. 5.22 OAuth 2.0 „best current practice“

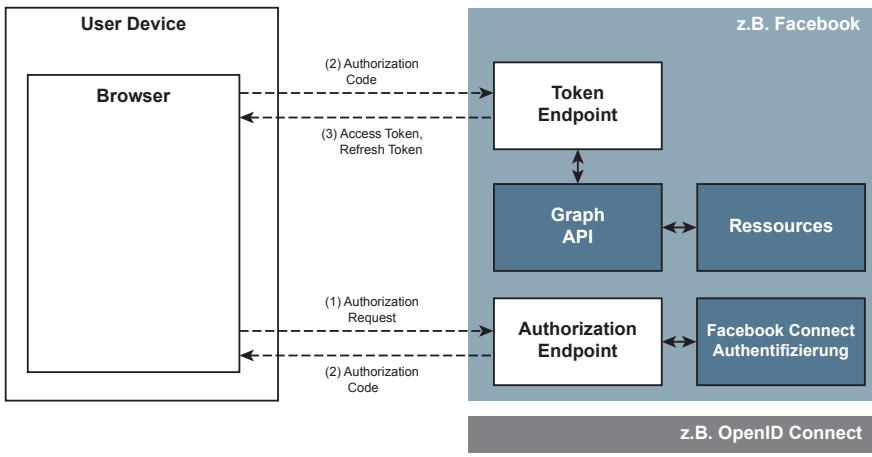
Erteilung des Zugriffs auf die geschützten Ressourcen. Diese beiden Endpunkte können entweder von einer Instanz zusammen oder getrennt voneinander verwaltet werden.

Nachfolgend sind die drei wesentlichen Protokollabläufe von OAuth 2.0 aufgeführt:

1. **Authorization Request:** Die Anwendung auf dem Endgerät öffnet mit den Werkzeugen des zugrunde liegenden Betriebssystems eine Browsersession zwischen der Anwendung und dem Server des „Authorization Endpoints“. Innerhalb dieser Session wird die Autorisierung realisiert. Hierfür sollte der „Authorization Endpoint“ den Nutzer zuerst mittels zusätzlicher Mechanismen authentifizieren, die von OAuth 2.0 nicht weiter spezifiziert werden.
2. **Authorization Code:** Nach erfolgreicher Autorisierung und gegebenenfalls Authentifizierung wird dem Browser ein Autorisierungscode zur Verfügung gestellt. Mit Hilfe dieses Codes kann im weiteren Verlauf nachgewiesen werden, dass eine Autorisierung erfolgreich durchgeführt wurde. Dieser Autorisierungscode wird mit den Werkzeugen des Betriebssystems an die Anwendung weitergegeben.  
Mit dem Autorisierungscode allein kann noch nicht auf die Ressource zugegriffen werden. Die Anwendung ist aber nun in der Lage, mit dem Autorisierungscode einen Zugriffscode, oder auch „Access Token“ genannt, beim „Token Endpoint“ anzufordern.
3. **Access Token, Refresh Token:** Der Autorisierungscode wird beim „Token Endpoint“ zuerst auf Gültigkeit überprüft. Anschließend wird der Anwendung ein Zugriffscode ausgestellt, mit dem der Zugriff auf die Ressource erfolgen kann. Ein „Refresh Token“ wird auf ähnliche Weise immer dann angefordert, wenn der Zugriffscode abgelaufen ist.

### Anwendungsbeispiel: Facebook Connect

Facebook ist mit seiner großen Verbreitung ein potenzieller Identity Provider für viele Nutzer im Internet. Der Log-in-Dienst von Facebook ist grundsätzlich als proprietäre Alternative zu dem offenen Standard OpenID Connect einzurichten. Wesentlicher Bestandteil ist ebenfalls das Autorisierungsprotokoll OAuth 2.0. Nachfolgend werden das Konzept des Log-in-Dienstes von Facebook und die Integration von OAuth 2.0 anhand von Abb. 5.23 erläutert. Als konkretes Anwendungsbeispiel wird die Anmeldung bei dem Internetdienst Stack Overflow mittels Facebook Connect, also mittels Log-in-Daten bei Facebook, betrachtet. In diesem Beispiel ist Facebook sowohl der „Authorization Endpoint“, als auch der „Token Endpoint“. Der Internetdienst Stack Overflow hat sich im Vorfeld bei Facebook registriert, eine eindeutige Client ID erhalten und die benötigten Bibliotheken für die Kommunikation mit den Facebook APIs in seine Webanwendung integriert. In diesem Anwendungsbeispiel sind die schützenswerte Ressource der Account und die damit verbundenen persönlichen Informationen des Nutzers.



**Abb. 5.23** OAuth 2.0 und Facebook Connect

Nachfolgend sind die wesentlichen Protokollabläufe von OAuth 2.0 und ein Ausschnitt zu der zugehörigen HTTP-Kommunikation im Kontext des Anwendungsbspiele aufgeführt:

**1. Authorization Request:** Für die Anmeldung bei dem Internetdienst Stack Overflow mittels Facebook-Account wird der Nutzer zuerst auf die Webanwendung von Facebook umgeleitet. Dem entsprechenden HTTP-Request wird die eindeutige ID der Webanwendung von Stack Overflow angehängt. Zusätzlich wird der OAuth-Schnittstelle von Facebook mitgeteilt, dass die Anwendung Zugriff auf die E-Mail-Adresse des Nutzers benötigt und wie der Nutzer nach einer erfolgreichen Authentifizierung und Autorisierung auf die Webanwendung von Stack Overflow zurückgeleitet werden soll. Für die Wiederherstellung eines Kommunikationszustandes und als Schutz vor CSRG-Angriffen wird zusätzlich ein Zustandsobjekt an den Request angehängt.

```

HTTP/1.1
GET https://www.facebook.com/v2.0/dialog/oauth?
client_id=145044622175352
&scope=email
&redirect_uri=https://stackauth.com/auth/oauth2/facebook
&state=
{
  "sid":1,
  "st":"a7b1972f33fdea4620e3276001a2b33ce9c1d5f9bc63227e-
  cab767c1bd2617bd",
  "ses":"1c2bdda2ed7f4322952baf4ef2cbbd66"
}

```

**2. Authorization Code:** Nach der erfolgreichen Authentifizierung und Autorisierung wird der Nutzer von der Facebook-Webanwendung auf die Webanwendung von Stack Overflow zurückgeleitet. An den entsprechenden HTTP-Request werden der Autorisierungscode und ein aktualisiertes Zustandsobjekt angehängt.

```
HTTP/1.1
GET https://stackauth.com/auth/oauth2/facebook?
code=AQBxewj3LeZBc4NzUJv7FFd0fDFB2UM5jyfeX5Cac2NaaxQMRx-
sfY03TDCcdaj...
state=
{
  "sid":1,
  "st":"2458ff31cc4291023c2c301aa58dd6a4938a0bcfa-
5066d229a77c1f8abc09e51",
  "ses":"d4bda5e797a94c858d8a40edafc431f5"
}
```

Mit dem Autorisierungscode kann anschließend ein Zugriffscode bei der Graph API von Facebook angefragt werden. Hierfür muss wieder die ID der Webanwendung von Stack Overflow an den HTTP-Request angehängt werden. Zusätzlich muss die gleiche Umleitungsadresse wie im ersten Schritt angegeben werden. Da der Zugriffscode nicht clientseitig vom Browser des Nutzers abgefragt wird, sondern serverseitig von der Webanwendung, muss ein spezielles Passwort zu der registrierten ID mit angegeben werden. Damit ein passender Zugriffscode erfolgreich angefragt werden kann, muss der vorher erhaltene Autorisierungscode mit an den Request angefügt werden.

```
HTTP/1.1
GET https://graph.facebook.com/v3.1/oauth/access_token?
client_id=145044622175352
&redirect_uri=https://stackauth.com/auth/oauth2/facebook
&client_secret=<PASSWORD>
&code=AQBxewj3LeZBc4NzUJv7FFd0fDFB2UM5jyfeX5Cac2NaaxQMRx-
sfY03TDCcdaj...
```

**3. Access Token:** Nach der erfolgreichen Validierung des Autorisierungscodes wird der Webanwendung ein Zugriffscode in dem folgenden Format von der Graph API zur Verfügung gestellt:

```
{
  "access_token": "<ACCESS-TOKEN>",
  "token_type": "<TYPE>",
  "expires_in": <SECONDS-TIL-EXPIRATION>
}
```

Mit dem Zugriffscode könnte die Webanwendung nun auf die freigegebenen Ressourcen der Graph API zu dem Nutzer zugreifen. In diesem Anwendungsbeispiel ist das lediglich die bei Facebook hinterlegte E-Mail-Adresse des Nutzers. Diese kann anschließend verwendet werden, um beispielsweise erstmalig einen neuen Account bei Stack Overflow zu dieser E-Mail-Adresse zu erstellen oder um den Log-in durchzuführen.

### 5.8.3 OpenID Connect

Bei OpenID Connect handelt es sich um die dritte und aktuelle Generation des OpenID-Protokolls. Ziel der Weiterentwicklung war es, ein einfache zu verwendendes und interoperables Werkzeug für die aktuellen Anforderungen an die Authentifikation im Internet zu schaffen. OpenID Connect basiert im Wesentlichen auf dem verbreiteten OAuth 2.0-Protokoll und erweitert dieses um fehlende Identity Services, speziell um Protokollabläufe für die Authentifikation.

Aufbauend auf dem OAuth 2.0-Protokoll wird bei OpenID Connect über das Attribut „scope=openid“ im „Authorization Request“ die Authentifikation gestartet. Nachfolgend ist der entsprechende HTTP-Request exemplarisch für die Anmeldung bei der Telekom dargestellt.

```
HTTP/1.1
GET https://accounts.login.idm.telekom.com/oauth2/auth?
client_id=10LIVESAM3000004901VESPAPICTELEKOM0000
&scope=openid
&redirect_uri=https://www.telekom.de/tech/sam/ess/callback
&state=f3a34ae4-80eb-44d9-84f1-a942aafb67f8
&response_type=code
```

Die weiteren Protokollabläufe von OAuth 2.0 erfolgen wie im vorherigen Anwendungsbeispiel zu Facebook Connect beschrieben. Der abschließend erhaltene Access Token enthält jedoch bei der Verwendung von OpenID Connect ein weiteres Attribut.

```
{
"access_token": "<ACCESS-TOKEN>",
"token_type": "<TYPE>",
"expires_in": <SECONDS-TIL-EXPIRATION>
"id_token": "<JSON-WEB-TOKEN>"
}
```

Hierbei handelt es sich um einen JSON Web Token (JWT), der wichtige Informationen zu der durchgeführten Authentifikation des Benutzers enthält.

```
{  
  "sub": "<USER-ID>",  
  "iss": "<ISSUING-AUTHORITY>",  
  "aud": "<AUDIENCE-RESTRICTION>",  
  "nonce": "<ANTI-REPLAY-VALUE>",  
  "auth_time": <AUTHENTICATION-TIME>,  
  "acr": <AUTHENTICATION-CONTEXT>,  
  "iat": <ISSUING-TIME>,  
  "exp": <EXPIRATION-TIME>  
}
```

Basierend auf den enthaltenen Informationen kann eine Client App den zuvor authentifizierten Benutzer identifizieren, einen neuen Account für ihn erstellen oder ihn mit einem bereits bestehenden Account einloggen.

---

## 5.9 Zusammenfassung

Aktuell sorgt jeder Dienstanbieter selber dafür, auf welche Weise ein Nutzer identifiziert und authentifiziert wird. In diesem Zusammenhang stehen ihm verschiedene Formen und Mechanismen zur Verfügung, die von der Identifizierung per E-Mail bis hin zur Nutzung von Onlinefunktionalitäten bestimmter Ausweisdokumente, wie zum Beispiel dem neuen deutschen Personalausweis, reichen.

Die Art, auf die ein Nutzer authentifiziert wird, bestimmt zum einen, wie hoch der Schutz der Nutzerdaten ist und damit auch die Vertrauenswürdigkeit der digitalen Identität, zum anderen bestimmt sie aber auch den Grad der Nutzerfreundlichkeit bei Verwendung des Dienstes. Heutzutage ist eine schwache passwortbasierte 1-Faktor-Authentifizierung (Wissen) sowohl im Internet als auch in Unternehmen immer noch die am häufigsten verwendete Methode zur Authentifizierung.

In der Zukunft werden adaptive und risikobasierte Authentifikationsverfahren genutzt, die ein Höchstmaß an Sicherheit und Nutzerfreundlichkeit gleichzeitig bereitstellen.

---

## 5.10 Übungsaufgaben

### Übungsaufgabe 1

Auf einer Webseite melden sich Nutzer üblicherweise mit Nutzernamen und Passwort an (Passwort-Verfahren). Welcher der beiden Teile übernimmt die Identifikation und welcher die Authentifikation?

**Übungsaufgabe 2**

Warum ist es, wenn Biometrische Verfahren zur Authentifikation genutzt werden, besonders schwerwiegend, wenn das biometrische Merkmal (zum Beispiel der Fingerabdruck) bei einem Hacker-Angriff oder Datenleck gestohlen wird?

**Übungsaufgabe 3**

Sie beraten einen Freund, wie er das Passwort-Verfahren auf seiner Webseite umsetzen sollte. Zurzeit funktioniert das Passwort-System wie folgt: Wenn sich ein Nutzer auf der Webseite anmeldet, gibt der Nutzer einen Nutzernamen und ein Passwort an. Diese werden direkt in die Datenbank auf dem Webserver geschrieben. Wenn sich der Nutzer anmeldet, wird das eingegebene Passwort mit dem Passwort in der Datenbank verglichen.

Wo liegt das Problem? Was würden Sie anders machen?

**Übungsaufgabe 4**

Bei der Analyse von Log-Nachrichten Ihrer Webseite erkennen Sie, dass ein Nutzer tausendfach pro Minute falsche Passworte eingibt. Welche Art von Angriff liegt hier vor? Wie können Sie Ihre Webseite vor einem solchen Angriff schützen?

**Übungsaufgabe 5**

Nennen und beschreiben Sie die Prinzipien der grundsätzlich unterschiedlichen generellen Authentifikationsverfahren!

**Übungsaufgabe 6**

Was ist der Vorteil für den Nutzer, wenn risikobasierte Authentifikation eingesetzt wird?

**Übungsaufgabe 7**

Nennen Sie zwei Identifikationsverfahren, die als Fernidentifikation durchgeführt werden können!

**Übungsaufgabe 8**

Welche Bedeutung haben die Falschakzeptanz- und Falschrückweisungsrate bei biometrischen Authentifikationsverfahren?

Ergebnisse siehe: <https://norbert-pohlmann.com/cyber-sicherheit/uebungen/>.

---

**Literatur**

1. Blumberg H, Pohlmann N (2006) Der IT-Sicherheitsleitfaden. MITP-Verlag, Bonn
2. Widermann R, Ziegler T (2017) Entwicklung eines prototypischen Systems zur teilautomatisierten Durchführung von Fernidentifizierungen mittels Videochat-Technologien, Masterarbeit im Institut für Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen, Dezember

3. Bundesanstalt für Finanzdienstleistungsaufsicht (Hrsg) Rundschreiben 3/2017 (GW) – Videoidentifizierungsverfahren. Bonn, 10.04.2017
4. Bundesamt für Sicherheit in der Informationstechnik (Hrsg) Technische Richtlinie TR-03127: eID-Karten mit eID- und eSign-Anwendung basierend auf Extended Access Control. Bonn, 19.10.2017
5. Bundesamt für Sicherheit in der Informationstechnik (Hrsg) Technical Guideline BSI TR-03119: Requirements for Smart Card Readers Supporting eID and eSign Based on Extended Access Control. Bonn, 02.08.2017
6. Deutsche Post AG. Die POSTIDENT Verfahren im Überblick. <https://www.deutschepost.de/de/p/postident/identifizierungsverfahren.html>. Zugegriffen: 21. Nov. 2017
7. Demir N, Pohlmann N (2018) Identitäts-Check anhand sozialer Netzwerke – Das Social-Ident-Projekt. IT-Sicherheit 2018(2):42–46
8. <https://hpi.de/pressemitteilungen/2017/die-top-ten-deutscher-passwoerter.html>
9. <https://www.itwissen.info/Biometrie-biometrics.html>
10. Hertlein M, Manaras P, Pohlmann N (2016) Die Zeit nach dem Passwort – Handhabbare Multifaktor-Authentifizierung für ein gesundes Eco-System. DuD Datenschutz und Datensicherheit 40(4):206–211
11. Was ist eine digitale Identität? <https://www.bundesdruckerei.de/de/Themen-Trends/Magazin/Was-ist-eine-digitale-Identitaet> Stand: 22.11.18
12. Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren. [https://www.teletrust.de/fileadmin/\\_migrated/content\\_uploads/KritKat-3\\_final.pdf](https://www.teletrust.de/fileadmin/_migrated/content_uploads/KritKat-3_final.pdf) Stand: 22.11.18
13. Feld S, Pohlmann N (2010) Ein OpenID-Provider mit Proxy-Funktionalität für den nPA. In: Horster P, Schartner P (Hrsg) Proceedings der DACH Security Konferenz 2010 – Bestandsaufnahme, Konzepte, Anwendungen und Perspektiven. Syssec, Frechen
14. Dietrich C, Rossow C, Pohlmann N (2012) eID online authentication network threat model, attacks and implications. In: Proceedings des 19. DFN Workshop
15. Pettersson M, Obrink M (2011) Ensuring integrity with fingerprint verification. Precise Biometrics White Paper, Schweden

# Enterprise Identity und Access Management

# 6

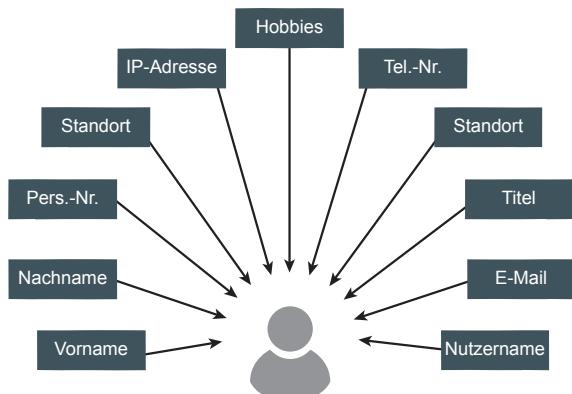
In diesem Kapitel werden Aufgaben, Prinzipien und Mechanismen eines „Enterprise Identity and Access Management-Systems“ dargestellt und erläutert.

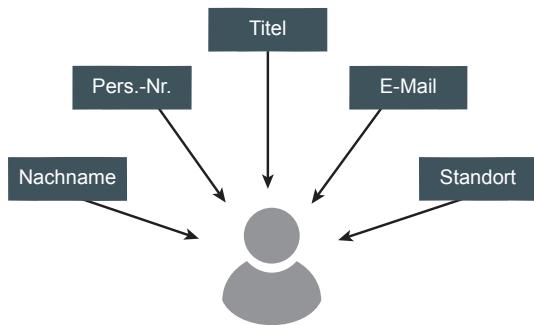
Der Begriff Enterprise Identity and Access Management (EIAM) beschreibt jeglichen Einsatz von digitalen Identitäten, deren Attributen, deren Berechtigungen für IT-Systeme sowie IT-Dienste und schließt die Erzeugung, Nutzung, Pflege und Löschung dieser digitalen Identitäten mit ein. Ziel ist es, vertrauenswürdige, identitätsbezogene und regelkonforme Prozesse durchzusetzen, die unabhängig von Organisationen und Plattformen standardisiert nutzbar sind [1].

Enterprise Identity and Access Management (EIAM) bezieht sich im Kern auf die Kombination von Verfahren der Organisationsführung einerseits und IT-Technologie andererseits, die es Organisationen durch eine breite Palette von Prozessen und Funktionalitäten erlauben, die Einhaltung gesetzlicher Vorschriften sowie die Integrität, Vertrauenswürdigkeit und Verfügbarkeit von Informationen gewährleisten zu können.

Eine Entität (Person, Rechner etc.) setzt sich zusammen aus den sie beschreibenden Attributen, siehe Abb. 6.1.

**Abb. 6.1** Entität



**Abb. 6.2** Digitale Identität

Eine digitale Identität (siehe Abb. 6.2) ist die Teilmenge der Attribute einer Entität, die diese Identität in einem bestimmten Kontext im Unterschied zu anderen Entitäten bestimmbare machen. Eine Entität kann abhängig vom Kontext und den dadurch erforderlichen Attributen auch mehrere digitale Identitäten besitzen. Entitäten sind individuell identifizierbare Personen, IT-System usw.

Der Begriff Identity and Access Management (IAM) wird in den meisten Fällen synonym zu IdM verwendet und soll verstärkt auf den Aspekt der Zugangskontrolle hinweisen. Das Access Management ist in dieser Definition als Teilmenge von IdM zu sehen. Das Wort Enterprise soll deutlich machen, dass das Referenzmodell, das vorgestellt wird, insbesondere für größere Unternehmen und Organisationen gedacht ist.

Enterprise Identity and Access Management (EIAM) erbringen unterschiedliche Mehrwerte für ein Unternehmen. Die Mehrwerte gelten teilweise generell und für das ganze Unternehmen, teilweise auch nur für einzelne Teile. Das liegt daran, dass einzelne Teile eines Unternehmens durchaus widersprüchliche Anforderungen haben können. Es existieren Stellen, an denen eine möglichst hohe Automatisierung (weniger menschliches Personal) und ein reibungsloser Einsatz von oberster Priorität (Nutzerfreundlichkeit) sind. An anderen Stellen wiederum ist ein sehr hohes Maß an Cyber-Sicherheit die wichtigste Vorgabe, worunter unter Umständen die Kosten und die Nutzerfreundlichkeit leiden können.

**Wichtig** Enterprise Identity and Access Management (EIAM) beschreibt jeglichen Einsatz von digitalen Identitäten, deren Attributen, deren Berechtigungen für IT-Systeme sowie IT-Dienste und schließt die Erzeugung, Nutzung, Pflege und Löschung dieser digitalen Identitäten mit ein.

## 6.1 Szenario eines Enterprise Identity and Access Management-Systems

Bei einem typischen Enterprise Identity and Access Management-Szenario innerhalb eines Unternehmens wird der Zeitrahmen von der Einstellung bis zur vollständigen Integration des Mitarbeiters betrachtet. Aber auch das Ausscheiden eines Mitarbeiters mit allen notwendigen Anpassungen und Löschung sind Bestandteil des Szenarios, siehe Abb. 6.3.

Dabei soll das Enterprise Identity and Access Management-System die folgenden Anforderungen umsetzen:

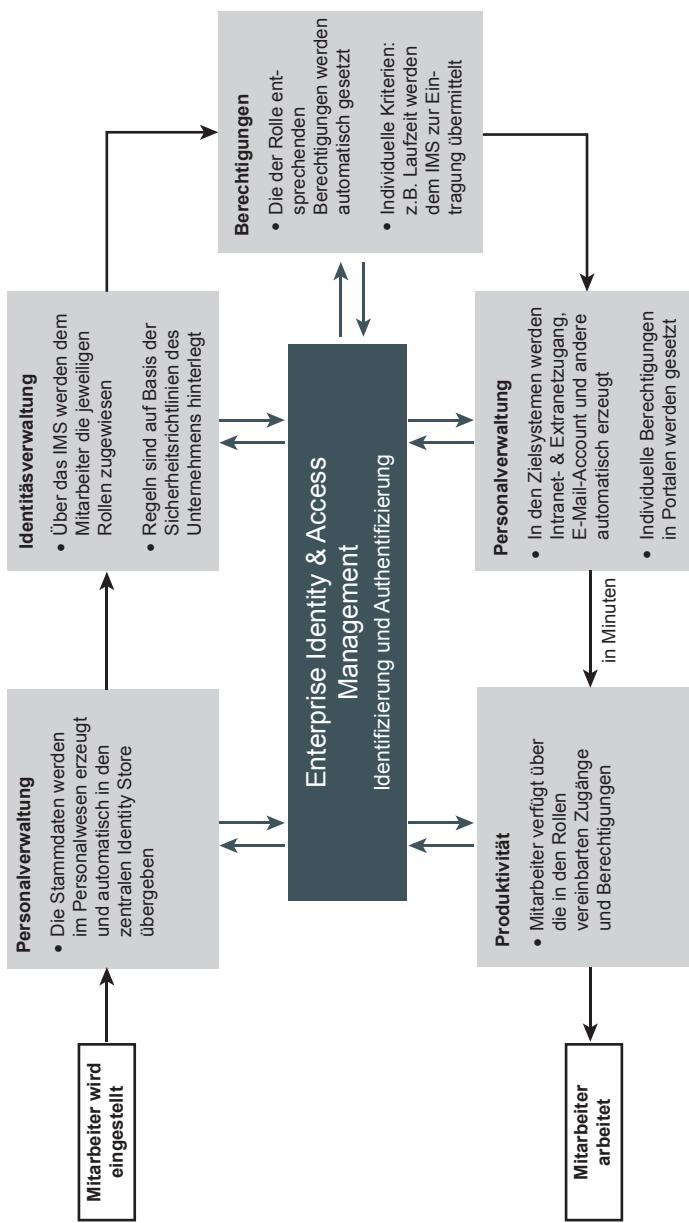
- sichere und komfortable Authentifizierung
  - strukturierte Identitäts-Datenspeicherung und -verwaltung
  - Zusammenführung von Identitätsdaten
  - Identitäten über ihren gesamten Lebenszyklus begleiten
  - Vermeidung von Überberechtigungen
  - Schutz von Informationen und vor nicht berechtigten Zugriffen
  - organisationsübergreifende Nutzung von Identitäten
  - Vertrauen zwischen Dienstanbietern und Partnern herstellen
- 

## 6.2 Enterprise Identity and Access Management-Referenzmodell

In diesem Abschnitt werden die grundlegenden Aufgaben einer Enterprise Identity and Access Management-Lösung in Form eines Enterprise Identity and Access Management-Referenzmodells beschrieben und definiert. Dieses Referenzmodell soll als grundlegendes, allgemein gültiges und anbieterneutrales Enterprise Identity and Access Management-Referenzmodell fungieren. Es besteht aus sieben Modulen, die für sich genommen nur eine beschreibende Rolle übernehmen und selbst keine Funktionalität bieten, siehe Abb. 6.4.

Die Ausprägung eines Moduls sind seine Komponenten, die wiederum auf einen Pool an Funktionen zurückgreifen, mit denen die Aufgaben erfüllt werden. Die gewählte Ordnung und Konstruktion des Modells leitet sich aus bereits etablierten Modellen verschiedener Anbieter im Markt ab und wurde nach wissenschaftlicher Betrachtung der Anforderungen an ein vollständiges Enterprise Identity and Access Management (EIAM), dem heutigen Stand entsprechend, angepasst [2].

Die Komponenten und Funktionen der sieben Module des EIAM-Referenzmodells werden in den folgenden Unterpunkten dargestellt und erläutert:



**Abb. 6.3** Typisches Enterprise Identity and Access Management-Szenario

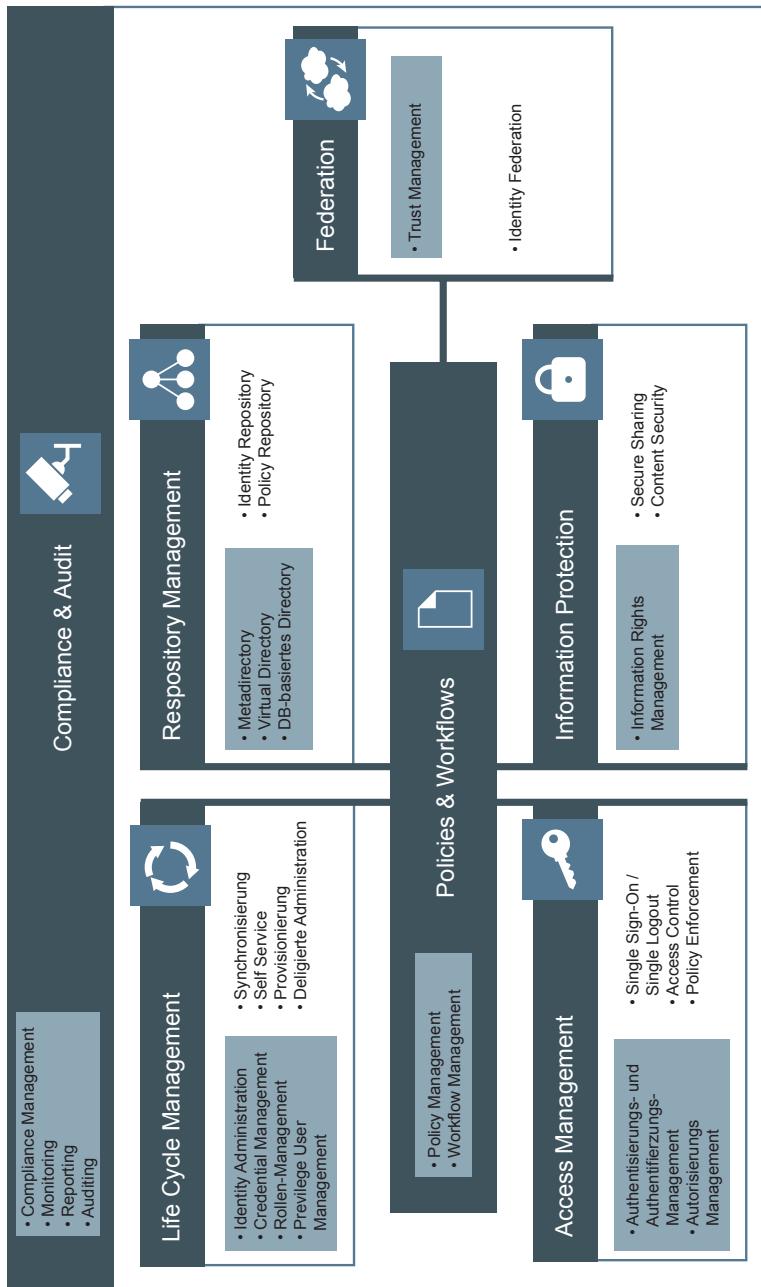


Abb. 6.4 Module, Komponenten und Funktionen des EIAM-Referenzmodells



**Abb. 6.5** Komponenten und Funktionen der Policies & Workflows

### 6.3 Policies & Workflows

Policies (Richtlinien) und Workflows (Arbeitsabläufe) bilden die Basis für einen geregelten Arbeitsprozess, denn mit ihnen werden Voraussetzungen geschaffen, um überhaupt Prozesse zu starten beziehungsweise weiterzuführen, siehe Abb. 6.5.

Eine Policy definiert den Anspruch und die zu erreichenden Ziele eines Unternehmens im Zusammenhang mit Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit, um wertvolle Informationen eines Unternehmens zu schützen. Eine Policy kann entweder als globale Policy für das ganze System oder als servicespezifische Policy für eine bestimmte verwaltete Ressource gelten. Die servicespezifische Policy hat dabei Vorrang vor der globalen Policy. So kann in einem Unternehmen beispielsweise eine servicespezifische Richtlinie für sensible Anwendungen wie die Lohnbuchhaltung erforderlich sein. Policies müssen in einem Repository vorgehalten und den Services zur Verfügung gestellt werden. Jeder Komponente lassen sich Policies zuordnen.

**Wichtig** Eine Policy definiert den Anspruch und die zu erreichenden Ziele eines Unternehmens im Zusammenhang mit Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit, um wertvolle Informationen eines Unternehmens zu schützen.

Ein Workflow bezeichnet die Verwaltung eines Prozesses. Er unterstützt die Erstellung und Verarbeitung von Geschäftsprozessen. Dabei können von den Workflows vordefinierte Ablaufstrukturen festgelegt werden, die die Prozesse zwischen den Entitäten in viele kleine automatische Teilprozesse zerlegen. Dazu gehören auch die Koordination und Fehlerbehandlung beziehungsweise die integrierte Datenverwaltung oder der Transfer von Daten. Workflows sind sehr flexibel und können auch für komplexere Prozesse eingesetzt werden. Damit wird erreicht, dass Arbeitsvorgänge mit Workflows halb-/automatisiert werden können. Workflows sind nicht nur technischer Natur.

**Wichtig** Ein Workflow unterstützt die Erstellung und Verarbeitung von Geschäftsprozessen.

### 6.3.1 Policy Management

Policies beinhalten alle Anforderungen, die Nutzer und Betreiber einhalten müssen, um die Sicherheit und Qualität eines IT-Systems zu gewährleisten. Ein zentrales Policy Management stellt sicher, dass diese Richtlinien eingehalten werden. Es erstellt Policies, deaktiviert sie und weist sie den entsprechenden Bereichen zu.

### 6.3.2 Workflow Management

Das Workflow Management dient zur zentralen Verwaltung aller Workflows. Dies ist notwendig, da Workflows die Komponenten des EIAM-System verbinden und daher übergreifend gestaltete Prozesse darstellen. Workflow Management umfasst jegliche Aufgaben, die notwendig sind, um Workflows zu definieren, zu spezifizieren, zu simulieren, auszuführen und zu steuern. Die Koordination von Workflows erfolgt durch ihren Aufbau. Dabei stellen sich die Fragen der Verantwortlichkeit (wer, was, wann und wie). Des Weiteren werden Workflows auch gerne zur Verwaltung des Dokumentenflusses eingesetzt.

### 6.3.3 Beispiel für Policies & Workflows

Ein Mitarbeiter, definiert als Entität, kommt neu in ein Unternehmen. Eine Richtlinie für die Personalverwaltung regelt, welche Stammdaten zur Erzeugung einer neuen digitalen Identität benötigt werden und wie diese jeweils geprüft werden müssen.

Ein Workflow gibt vor, wie diese Daten in das System der Personalverwaltung eingepflegt werden müssen. Eine weitere Richtlinie regelt, in welchen Abständen die Daten in ein Directory übernommen werden müssen. Zuletzt beschreibt ein Workflow, wie die Daten in das zuständige Directory hinzugefügt/kopiert werden.

---

## 6.4 Repository Management

Das Repository Management hat die Aufgabe, die Informationen in einem EIAM zentral zu speichern und zu verwalten, die für Entitäten in einem Netzwerk von Nutzen sein können. Dadurch kann eine einzige digitale Identität pro Nutzer/Entität erreicht werden.

Zur Datenverwaltung (Client-Server-Prinzip) in einem EIAM-System können Directory Services verwendet werden. Die Daten werden hierarchisch in einer Baumstruktur, dem Directory Information Tree (DIT), gespeichert. Diese Baumstruktur ähnelt oder entspricht oft einer realen organisatorischen oder geografischen Struktur. Die vom Directory Service eingesetzte Datenbank ist im Normalfall für ihre speziellen Aufgaben, die Suche, das Einfügen und Löschen, optimiert. Ein Directory Service ist damit besonders für die Ansprüche eines EIAM-Systems geeignet. Außerdem werden zusätzliche Techniken angewandt, die die verteilte Speicherung und Daten-Replikation unterstützen, siehe Abb. 6.6.

**Abb. 6.6** Komponenten und Funktionen des Moduls Repository Management



**Wichtig** Das Repository Management hat die Aufgabe, die Informationen zentral zu speichern und zu verwalten, die für Entitäten von Nutzen sein können.

#### 6.4.1 Auf einer Datenbank basierendes Directory

Alternativ zu einem Directory Service mit Baumstruktur kann zur Datenspeicherung eine relationale Datenbank verwendet werden. Mögliche Technologien für ein Verzeichnis auf Grundlage einer Datenbank sind zum Beispiel PL/SQL von Oracle, MySQL oder PostgreSQL. Der Zugriff erfolgt mittels jeweiliger Datenbanksprache. Dabei ergeben sich folgende Vorteile gegenüber einem Directory Information Tree (DIT):

- Transaktionsfähigkeit – Änderungen an der Datenstruktur erweisen sich einfacher als in einer Baumstruktur
- Referenzielle Integrität – Verwaltung von Integritätsfähigkeiten zwischen Daten
- Accounting – Datenbank-Sprachen wie SQL nutzen kaufmännische Funktionen, die bei Verwendung von Baumverzeichnissen wegen geringer Typensicherheit nicht einsetzbar sind

Relationale Datenbanken haben den Nachteil, dass ihre Performance nicht in jeder Situation optimal und im Fall von Directories eher schlecht ist, was durch die Art und Weise bedingt wird, wie die Abfragen ausgeführt werden. Des Weiteren fehlt der relationalen Datenbank im Gegensatz zum DIT die Möglichkeit zur Vererbung.

#### 6.4.2 Metadirectory

Das Konzept des Metadirectories, Metaverzeichnisdienst verwendet einen Verzeichnisdienst zur Synchronisierung von Datenbeständen aus verschiedenen Datenquellen (Repositories). Voraussetzung dafür ist, dass alle zu synchronisierenden Daten im Verzeichnisdienst abbildbar sind. Das entsprechende Schema muss standardisiert sein, damit verschiedene Anwendungen darauf zugreifen können.

Durch die Integration von Workflows und Policies wird die Synchronisierung der Einträge und Berechtigungen in den Repositorys geregelt. Daten werden zum Beispiel bei Änderungen automatisch weitergeleitet und aktualisiert.

#### **6.4.3 Virtual Directory**

Virtual Directory ist eine hierarchisch aufgebaute Technologie, die eine Sicht auf digitale Identitäten, ihre Attribute, Daten und die dazugehörigen Berechtigungen bietet, ohne ein komplett eigenes Verzeichnis aufzubauen (im Gegensatz zu einem Metadirectory). Der Aufbau eines Virtual Directory gleicht dem eines normalen LDAP-Directorys, der Datenzugriff erfolgt jedoch per Referenz. Erhält das Virtual Directory eine Anfrage, so werden die Daten beim Zugriff in Echtzeit aus dem jeweiligen Repository (Datensilo) gelesen und an die zuständige Datenquelle weitergeleitet, das heißt, sie werden nur referenziert.

#### **6.4.4 Identity Repository**

Ein Identity Repository, Identitätsspeicher, ist ein Verzeichnisdienst oder eine Datenbank zur Speicherung von digitalen Identitäten. Mittels Synchronisierung, durch ein Metadirectory oder ein Virtual Directory, werden die Einträge unterschiedlicher Identity Repositorys abgeglichen. Die Daten im Identity Repository werden durch die Identity-Administration verwaltet.

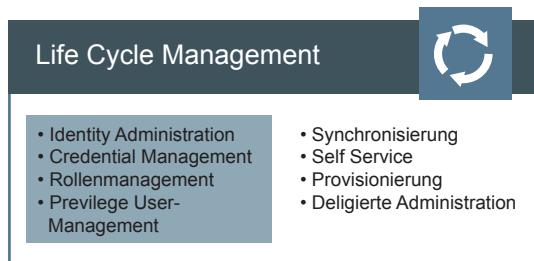
#### **6.4.5 Policy Repository**

Ein Policy Repository dient der zentralen Speicherung von Policies. Es erlaubt IT-Systemen, Policies bei Bedarf abzurufen. Oft ist das Policy Repository mit anderen Repositorys (beispielsweise Role und Entitlement Repository) in einem umfassenden Repository konsolidiert.

#### **6.4.6 Beispiel für Repository Management**

Die digitale Identität eines Mitarbeiters, genauer dessen Attribute, wird beim Zugriff auf Applikationen im Rahmen seiner Tätigkeit im Unternehmen benötigt. Die strukturierte Identitäts-Datenspeicherung und -verwaltung in einem Metadirectory erlaubt eine Authentifizierung anhand der jeweils aktuellen Attributwerte; von jedem Standort im Unternehmen. Ebenso wird die Richtlinie zur Bestimmung der korrekten Stärke einer Authentifizierung aus einem zentralen Repository abgerufen. Dies ermöglicht eine einfache und korrekte Umsetzung in ganzen Unternehmen.

**Abb. 6.7** Komponenten und Funktionen des Moduls Life Cycle Management



## 6.5 Life Cycle Management

Der Life Cycle zeigt die Schritte, die nötig sind, um Entitäten über digitale Identitäten bis zur deren Löschung in ein EIAM-System zu integrieren und zu verwalten. Der Zyklus beginnt mit der Erstellung und Administration von digitalen Identitäten und deren Attributen in entsprechenden Datensätzen sowie deren Zuteilung in entsprechende Repositorys. Die Zugriffsrechte der digitalen Identitäten werden durch eine Rollenverteilung eingeschränkt. Die Änderung beziehungsweise Aktualisierung von identitäts-bezogenen Daten und Credentials erfolgt im Rahmen der Provisionierung, der De- und Reprovisionierung und durch Synchronisierung aller Repositorys mit dem jeweils führenden System (zum Beispiel ein Metadirectory). Durch einen Selfservice haben Nutzer mit einer im System hinterlegten digitalen Identität selbst die Möglichkeit, wenn auch eingeschränkt, zum Beispiel ihre Daten zu aktualisieren und zusätzliche Rechte beziehungsweise Rollen anzufordern. Der Life Cycle einer Entität endet mit der endgültigen Löschung einer digitalen Identität. Eine Reprovisionierung ist dann unmöglich, siehe Abb. 6.7.

**Wichtig** Das Life Cycle Management sorgt dafür, dass Entitäten über digitale Identitäten bis zur deren Löschung integriert und verwaltet werden.

### 6.5.1 Identity-Administration

Der eigentliche Fixpunkt in einem Enterprise Identity and Access Management-System ist die digitale Identität. Sie ist eine Ansammlung von Attributen einer Entität (zum Beispiel einer Person oder einem IT-System), die diese von anderen Entitäten in einem bestimmten Kontext unterscheidbar macht. So ist jede Entität eindeutig identifizierbar und alle Datenanforderungen oder -übermittlungen können einer bestimmten Entität zugeordnet werden. Die Identity-Administration erstellt und verwaltet die digitalen Identitäten. Sie unterstützt deren Erzeugung und Bearbeitung und sorgt für eine Synchronisierung identitätsbezogener Daten.

### 6.5.2 Provisionierung

Die Provisionierung (auch Nutzer-Provisionierung, Provisioning beziehungsweise User-Provisioning) muss die Automatisierung aller Prozesse bezüglich der Erstellung, Verwaltung, Deaktivierung sowie Löschung von digitalen Identitäten und deren Attributen beziehungsweise Berechtigungen ermöglichen. Neben der Provisionierung müssen auch die Abläufe Deprovisionierung und Reprovisionierung von digitalen Identitäten und zugehörigen Daten möglich sein. Durch eine Deprovisionierung werden Berechtigungen einer digitalen Identität und ggf. die gesamte digitale Identität in allen betroffenen IT-Systemen automatisiert deaktiviert, was hohe Sicherheit erzeugt. Dies geschieht zum Beispiel, wenn ein Mitarbeiter das Projekt wechselt oder das Unternehmen verlässt. Der Mitarbeiter hat dann keinen Zugang mehr zu den Projekt- beziehungsweise Organisationsressourcen und den Diensten des EIAM-Systems. Mit Reprovisionierung werden digitale Identitäten, ihnen zugehörige Daten und die jeweiligen Berechtigungen wieder reaktiviert, sofern sie aufgrund bestehender Vorschriften noch vorgehalten wurden.

### 6.5.3 Rollenmanagement

Ein Rollenmanagement wird zur Erstellung und Verwaltung von Rollen benötigt. Es regelt die Zuteilung von Rollen an eine digitale Identität (Nutzer oder IT-Systeme). Eine Rolle ist eine Art Baustein eines Zugriffsmodells und wird benötigt, um digitalen Identitäten Berechtigungen zu erteilen. Die unterschiedlichen Berechtigungen in einem Unternehmen müssen je nach Prozess in entsprechende Rollen zusammengefasst werden. Einer digitalen Identität können mehrere Rollen für verschiedene Teilbereiche zugeordnet werden. Rollen differenzieren sich in Geschäftsrollen und technische Rollen. Eine Geschäftsrolle ist eine Zusammenfassung von technischen Rollen und könnte beispielsweise „Mitarbeiter“ oder „Projektleiter“ heißen. Technische Rollen wiederum sind spezifisch gerichtet, wie zum Beispiel eine Portalrolle „Mitarbeiter Standard“. Die Einstellungen werden per Hand vom Administrator bewilligt und zugewiesen. Im Self-Service hat der Nutzer eine stark eingeschränkte Möglichkeit, Rollen zu verwalten, zum Beispiel einen Antrag für eine neue Rolle zu erstellen. Mithilfe von Genehmigungsworkflows und Separation of Duties kann die Zuweisung an die unternehmensspezifischen Policies und Workflows angepasst werden. Ein Rollenmanagement unterstützt über das Verfahren des Role Minings die Gewinnung von Rollen für eine optimale und sichere Administration, falls bisher keine Rollen genutzt wurden oder falls zusätzliche bereits bestehende Verfahren das EIAM-System nutzen sollen.

### 6.5.4 Privileged User Management

Privilegierte Nutzer, wie zum Beispiel Administratoren von IT-Systemen, besitzen durch ihre weitreichenden Rechte, zum Beispiel Daten und Nutzereigenschaften zu verwalten oder Berechtigungen zu vergeben, die potenzielle Macht, jederzeit und an jedem Ort Veränderungen an diesen Informationen durchführen zu können. Außerdem verfügen diese Nutzergruppen fast immer auch über das notwendige Fachwissen, um diese Macht anzuwenden, was oft auch unbemerkt passieren kann. Aus diesem Grund ist eine genaue Kontrolle der privilegierten Nutzer, verbunden mit zusätzlichen Sicherheitsmaßnahmen, notwendig. Das Privileged User Management (PUM) stellt sicher, dass Personen mit besonders weitreichenden/kritischen Rechten, zum Beispiel Administratoren, nur die Rechte und Zugänge erhalten, die für die Erfüllung ihrer Aufgaben notwendig sind. Ein Privileged User Management ermöglicht die datenschutz- und richtlinienkonforme kontinuierliche Überwachung von Aktivitäten privilegierter Nutzer, integriert in das Monitoring und Reporting des EIAM-Systems. Dies dient der Risikominimierung und hat den Vorteil, dass durch automatisiert versandte Reports bei Verdacht auf kriminelle Handlungen zeitnah eingegriffen werden kann.

### 6.5.5 Delegierte Administration

Mit delegierter Administration werden in einem Enterprise Identity and Access Management-System (EIAMS) Rechte/Privilegien (im Idealfall auf Rollen basierend) nach Bedarf von einer digitalen Identität an eine bisher nicht privilegierte Identität weitergegeben. Dieser Prozess kann auch, gesteuert durch zuvor festgelegte und in einem Policy Repository bereitgestellte Richtlinien, automatisiert ablaufen. So werden Mitarbeitern, abhängig von der erwünschten Zuständigkeit, zum Beispiel als stellvertretender Abteilungsleiter, entsprechende Rollen und Rechte zugeteilt. Die Zuteilung kann auch für einen bestimmten Zeitraum realisiert werden, zum Beispiel bei Urlaub oder Erkrankung. Mit diesem automatisierbaren Prozess soll ein möglichst fortwährender Arbeitsbetrieb gewährleistet werden. Jegliche Weitergabe von Rechten wird zu jedem Zeitpunkt durch das EIAM-System protokolliert und ist somit vollständig nachvollziehbar.

### 6.5.6 Synchronisierung

Bei der Synchronisierung werden Daten jeglicher Art nach einer Veränderung automatisch an alle beteiligten IT-Systeme, zum Beispiel Repositorys beziehungsweise Directory Services, weitergeleitet und abgeglichen. Dieser Vorgang ist zum Beispiel notwendig, um Berechtigungsänderungen im Rahmen der Provisionierung in den betroffenen IT-Systemen durchzuführen oder Inkonsistenzen von Datenbeständen in unterschiedlichen Verzeichnissen zu vermeiden.

### 6.5.7 Self-Service

Die Pflege von Nutzerdaten kann sich als sehr aufwendig herausstellen. Unterstützung erfahren die Verwalter und Administratoren durch einen kontrollierten User Self-Service, bei dem Nutzer die eigenen Daten, im Rahmen der ihnen begrenzt zur Verfügung gestellten Möglichkeiten, selbst verwalten können. Die Funktionen des SelfServices sind:

- Anmeldung an Diensten
- Änderung eigener Daten sowie Passwortbearbeitung
- Zurücksetzen vergessener Passwörter (zum Beispiel anhand von vorher festgelegten Antworten auf definierte Fragen)
- Beantragung von Rollen für sich selbst
- Überprüfen des Status der eigenen Anträge
- Genehmigung sowie Delegation von Zugriffsrechten oder Teilen davon für die Nutzer- und Rollenverwaltung an andere Nutzer

Eine datenschutzkonforme Protokollierung aller Aktivitäten im Self-Service stellt sicher, dass eine Nachvollziehbarkeit gewährleistet ist und jederzeit Prüfungen im Rahmen des Auditings durchgeführt werden können.

### 6.5.8 Credential Management

Ein Credential Management, Management von Berechtigungsnachweisen, ist zuständig für die komplette Verwaltung aller Credentials einer Entität. Credentials sind Nutzernamen, Passwörter, Zertifikate, biometrische Merkmale, kryptografische Schlüssel und weitere Nachweise, die als Authentisierungsmerkmale dienen können. Diverse Kombinationen aus diesen Credentials ergeben wieder eigene Credentials, beispielsweise das Paar Nutzernname + Passwort. Zusätzlich regelt ein Credential Management auch die Nutzung von Hilfsmitteln, die zum sicheren Umgang mit Credentials notwendig sind. Dies kann zum Beispiel eine Smartcard sein, die als sicherer Container für Zertifikate dient, oder ein Security Token mit ähnlicher Funktionalität.

### 6.5.9 Beispiel für Life Cycle Management

Der Mitarbeiter benötigt durch die Zuordnung zu einem neuen Projekt Rechte zum Zugriff auf Applikationen, auf die er zuvor nicht zugreifen konnte. Er beantragt diese Rechte in einem Web-Frontend (Self-Service). Der Projektleiter hat sein Recht zur Genehmigung dieser Rechte an einen Vertreter delegiert. Dieser genehmigt dem neuen Projektmitarbeiter diese Rechte nach Prüfung in seinem Web-Frontend. Das System provisioniert diese Rechte anschließend in die Applikationen.

**Abb. 6.8** Komponenten und Funktionen des Moduls Access Management



## 6.6 Access Management

Das Access Management beinhaltet die Entscheidung über Zugriffsberechtigungen auf der Basis von Nutzeridentitäten, -rollen und Zugriffsrechten. Es beschreibt die notwendigen Sicherheitsmechanismen für den Zugriff auf ein EIAM-System sowie die Kontrolle (Access Control) und das Durchsetzen des Zugriffs (Enforcement). Mögliche Zugangslösungen werden über Sicherheitsprotokolle, firmenspezifische Netzkonfigurationen, durch Virtual Private Networks (VPNs) und die vorhandenen Authentifizierungstechniken realisiert. Standardisierte Verfahren sind Authentisierungs- und Authentifizierungs-Management, Autorisierung, Single Sign-On/Single Log-out, Access Control und Policy Enforcement, siehe Abb. 6.8.

**Wichtig** Das Access Management beinhaltet die Entscheidung über Zugriffsberechtigungen auf der Basis von Nutzeridentitäten, -rollen und Zugriffsrechten.

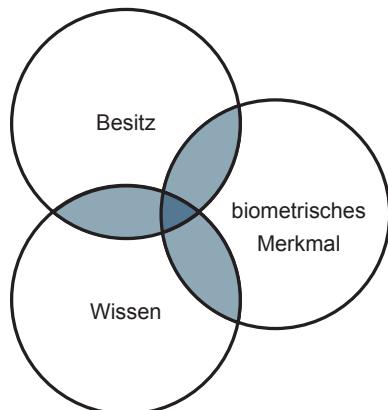
### 6.6.1 Authentisierungs- und Authentifizierungs-Management

Die Authentifizierung beschreibt die Verifizierung der Echtheit der Identität einer Entität, zum Beispiel eines Nutzers oder eines IT-Systems. Sie erfolgt üblicherweise durch ein Passwort (Besitz), ein biometrisches Merkmal wie den Fingerabdruck oder durch Hardware-Sicherheitsmodule (Besitz) (Abb. 6.9).

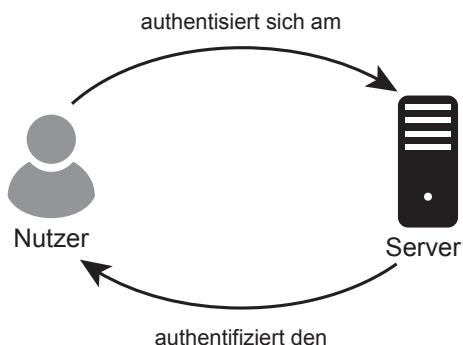
Der Begriff Authentifizierung wird oft synonym zum Begriff Authentisierung verwendet. Sie unterscheiden sich in der „Richtung der Aktion“, siehe Abb. 6.10:

Eine Entität (zum Beispiel ein Nutzer) authentisiert sich an einer Instanz, indem sie den Nachweis der eigenen Identität erbringt. Die Instanz authentifiziert die Entität in der Folge. Das Authentifizierungs-Management definiert und kontrolliert den Vorgang der Verifizierung sowie die zu verwendenden Authentisierungs-techniken. Mit diesem Prozess wird die Datenintegrität und Vertraulichkeit gewahrt, und es wird zum Schutz von Informationen beigetragen. Der Authentifizierung folgt im Normalfall die Autorisierung für definierte und an Rechte gebundene Zugriffe, siehe auch Kap. 5 „Identifikation und Authentifikation“.

**Abb. 6.9** Klassen von Authentifizierungsverfahren



**Abb. 6.10** Authentisierung und Authentifizierung



### 6.6.2 Autorisierungs-Management

Die Autorisierung bestimmt, wer Zugang zu Systemressourcen hat und diese nutzen darf. Für eine mögliche Autorisierung werden eine erfolgreiche Authentifizierung und die damit einhergehende Verifikation einer Identität vorausgesetzt. Im Regelfall werden über bereits vorhandene Prozesse Berechtigungen und Zugriffsrechte definiert, die festlegen, auf welche IT-Ressourcen eine digitale Identität – gemäß den Richtlinien der Organisation – Zugriff hat. Ein EIAM-System muss innerhalb seines Autorisierungs-Managements Richtlinien, Prozesse und Verfahren vereinen, die diese Prozesse sicher, effektiv und effizient steuern und verwalten. Hierzu sollte neben dem eigentlichen Berechtigungsmanagement auch ein Modul zum Review der Berechtigungen für Audits gehören. Mehrwerte vom Autorisierungs-Management sind die Automatisierung der Vorgänge und die Vermeidung von Überberechtigung.

### 6.6.3 Single Sign-On/Single Log-out

Single Sign-On (SSO) ist einer der entscheidenden Faktoren in einem EIAM-System. Nicht nur die Interaktion mit mehreren heterogenen IT-Systemen beziehungsweise Applikationen werden erleichtert und damit die Nutzerfreundlichkeit erheblich verbessert, sondern es wird auch die Sicherheit erhöht. SSO benötigt nur eine einmalige Verifikation der Identität, um auf mehrere Dienste in heterogenen Netzen und Systemen (möglichst domänenübergreifend) zugreifen zu können. Grundsätzlich lässt der Vorgang je nach Sicherheitslevel unterschiedliche Authentifizierungsmechanismen zu. SSO birgt den Nachteil, dass der Schaden bei unbemerkt Verlust der Authentifizierungsdaten an einen Angreifer sehr groß sein kann, weil der Angreifer einen globalen Zugriff in Bezug auf die Autorisierung der betroffenen Identität erlangt. Daher besteht die Notwendigkeit effektiver Maßnahmen und Authentifizierungsmechanismen. Zu einem SSO gehört aus Sicherheits- und Komfortgründen ein Single Log-out (SLO) als Dienst zur zentralen, einmaligen Abmeldung von allen Diensten und Anwendungen im definierten EIAM-Kontext.

### 6.6.4 Access Control

Access Control bezeichnet den netzwerkweiten Zugriffsschutz auf unternehmensspezifische Ressourcen und Services durch Entitäten. Um einen Zugriff auf solch einen Dienst zu gewährleisten, werden vorab technische und organisatorische Vorbereitungen getroffen. Dazu werden Entitäten authentisiert, authentifiziert und autorisiert. Die Kontrolle erfolgt meist durch Passwörter, Gewährung von Privilegien und Bereitstellung von Attributen. Diese Einschränkungen fördern mehr Sicherheit in einem Unternehmen, denn nur zugangsberechtigte Entitäten können auf ihre Dienste zugreifen.

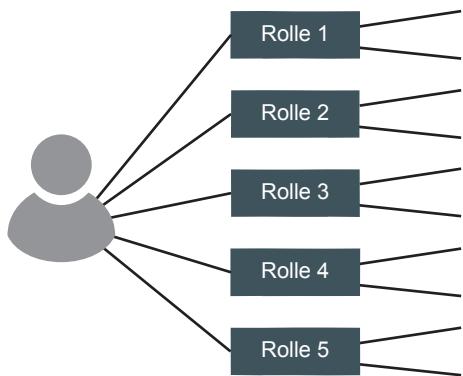
Unterschiedliche Ressourcen erfordern unterschiedliche Zugriffskontrollen. Abhängig von deren Zuständigkeit sind einige wichtige Grundmodelle definiert. Die folgenden Erklärungen beschreiben den Grundsatz, die Funktionalität und den Schutzmechanismus der notwendigsten Grundmodelle in einem EIAM-System.

Im Folgenden werden zwei authentifikationsbasierte Access Control (NBAC)-Modelle dargestellt:

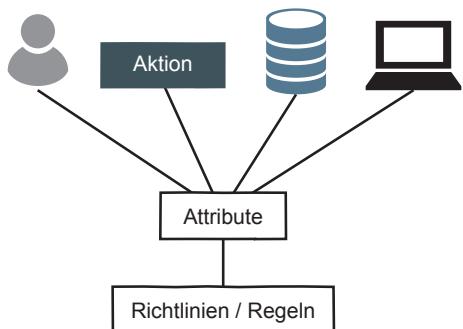
#### **Role-Based Access Control**

Bei der rollenbasierten Zugriffskontrolle werden den Nutzern des IT-Systems oder Netzwerks Rollen zugeordnet, siehe Abb. 6.11. Die Nutzer können dabei mehrere Rollen besitzen. An eine Rolle sind entsprechende Berechtigungen gebunden. Je nach Rollenzuordnung des Nutzers erteilt oder sperrt das IT-System dann das Zugriffsrecht auf Betriebsmittel.

**Abb. 6.11** Role-Based Access Control



**Abb. 6.12** Attribute-Based Access Control



### Attribute-Based Access Control (ABAC)

Bei der attributbasierten Zugriffskontrolle wird der Zugriff auf eine Ressource anhand von Attributen des Nutzers (Entität), der Ressource, dem Zustand der Systemumgebung, sowie auf diese Attribute angewendeten Sicherheitsregeln gesteuert, siehe Abb. 6.12.

### 6.6.5 Remote Access Control

Remote Access beschreibt den Vorgang, aus der Distanz einen Zugang zu einem IT-System oder von außen in ein Netzwerk/ein Intranet zu erlangen. Es wird unterschieden zwischen direkter Punkt-zu-Punkt-Verbindung und Verbindungen über ein öffentliches Netz als Transportmedium, beispielsweise über das Internet.

### 6.6.6 Network Access Control

Unter Network Access Control (NAC) wird eine Technologie verstanden, mit der der Zugang zu einem Unternehmensnetzwerk – abhängig vom Nutzer und der Vertrauenswürdigkeit des zum Zugriff eingesetzten IT-Systems – gesteuert wird.

Dabei wird die Entscheidung nicht nur von den Log-in-Daten des Nutzers, sondern auch vom vertrauenswürdigen Zustand des zum Zugriff genutzten IT-Systems abhängig gemacht. Die Überprüfung basiert auf Messungen der Konfiguration des IT-Systems und einem Vergleich dieser Messung mit Sicherheitsrichtlinien (Policies) des Unternehmens. IT-Systeme mit einer aus Sicht des Unternehmens fehlerhaften, also nicht vertrauenswürdigen Konfiguration können entdeckt und präventiv vom Netzwerk fern gehalten werden, siehe auch Abschn. 7.4 „Trusted Network Connect“.

### 6.6.7 Policy Enforcement

Das Policy Enforcement ist dafür verantwortlich, Anfragen an einen Dienst entgegenzunehmen und basierend auf einem Regelwerk die angefragten Aktionen durchzusetzen oder effektiv zu verhindern. Die technische Umsetzung wird meist als Policy Enforcement Point (PEP) beschrieben. Policy Enforcement ist keine zentrale Funktion, sondern muss in allen IT-Systemen und Anwendungen umgesetzt werden.

### 6.6.8 Beispiel für Access Management

Der Mitarbeiter benötigt Zugriff auf viele unterschiedliche Applikationen. Er bekommt eine Smartcard mit einem Personenzertifikat der unternehmenseigenen PKI. Hiermit meldet er sich morgens an der Domäne und dadurch gleichzeitig an einem Single Sign-On System an. Dieses sorgt dafür, dass er beim Zugriff auf eine Applikation automatisch authentifiziert wird, ohne sich erneut anmelden zu müssen. Am Ende seines Arbeitstages meldet er sich von der Domäne ab, wodurch ihn ein Single Log-out-Mechanismus bei allen Applikationen abmeldet.

## 6.7 Information Protection

Informationen sind das höchste Gut einer jeden Organisation, daher gilt es, diese entsprechend zu schützen. In einigen Unternehmen wird eine Vielzahl von eingestuften Dokumenten erstellt, verarbeitet und verteilt, siehe Abb. 6.13.

**Abb. 6.13** Komponente und Funktion des Moduls Information Protection



Die häufigsten Gefahren in kritischen Informationssystemen sind typischerweise:

- Rückgang oder Verlust der Verfügbarkeit (zum Beispiel Denial of Service)
- Verlust der Vertraulichkeit, zum Beispiel Ausspionieren von Informationen auf Systemen und Ausspionieren der Kommunikation (Netzwerkverkehr)
- Angriffe auf die Kommunikationsverbindung (zum Beispiel ARP Spoofing)
- Angriffe von innen gegen Systeme und Applikationen (zum Beispiel Malware mit den Schadfunktionen Key-Logger, Ransom-Ware, ...)
- Verlust der Integrität durch Verfälschen der übertragenen Information, zum Beispiel bei einer „Man in the Middle“-Attacke

**Wichtig** Information Protection soll Informationen eines Unternehmens immer adäquat vor Angriffen schützen.

Die Technologien und Prozesse hinter dem Begriff der Information Protection gewährleisten, dass Informationen immer auf ihrem angemessenen Schutzlevel gehalten und über Policies nur entsprechenden Nutzern mit entsprechenden Berechtigungen zugänglich gemacht werden. In keiner Phase der Existenz verlässt die Information das Schutzlevel, weder bei der Lagerung noch beim Transport oder der Bearbeitung. Dazu gehört beispielsweise auch, welche Art von Daten für wie lange und unter welchen Voraussetzungen gespeichert werden sollen, wer Verwendung für die Daten hat und wie der Zugriff realisiert werden soll. Ein EIAM-System gewährleistet die beschriebenen Funktionen und belegt das Feld der Nachverfolgbarkeit und damit die Einhaltung von Richtlinien.

Der Mehrwert von „Information Protection“ liegt in der Umsetzung eines angemessenen Cyber-Sicherheitslevels zum Schutz von Informationen (Werte) eines Unternehmens.

### 6.7.1 Secure Sharing

Secure Sharing beschreibt einen Sicherheitsmechanismus, der die schutzlevelkonforme Verarbeitung von Informationen unter dem Zugang von mehreren Identitäten gewährleistet. Eine Information ist bei der Weitergabe innerhalb einer definierten Gruppe über ihren gesamten Lebenszyklus geschützt. Sie ist von Rechten abhängig, wie definierte Identitäten. Rein technisch bedeutet das beispielsweise eine durchgehende Transport- und Ende-zu-Ende-Verschlüsselung von Informationen bei der Verarbeitung eines Dokuments.

### 6.7.2 Information Rights Management

Information Rights Management (IRM) bildet die logische Ergänzung zum Secure Sharing. Information Rights Management bewahrt sicherheitskritische Daten vor unkontrollierten Veränderungen oder Verarbeitungen, indem den Identitäten eindeutige automatisierte Rechte vergeben werden. Die korrekte Zuweisung von Rechten an Nutzer oder Nutzergruppen beziehungsweise Rollen beinhaltet individuell einstellbare Lese-, Schreib- und Ausführungsrechte, immer in Bezug auf eine Identität. Identitäten mit entsprechenden Rechten dürfen die Informationen eventuell verändern und drucken, während andere Identitäten die Informationen lediglich sichten dürfen.

### 6.7.3 Content Security

Content Security beschreibt den Schutz von Informationen durch die Absicherung der Infrastruktur und der verarbeitenden Hard- und Software. Dazu gehören Sicherheitsmaßnahmen wie Anti-Malware-Programme, aber auch Verschlüsselung und Data Leakage Prevention (DLP). Im Grunde bezieht Content Security die Punkte Information Rights Management (IRM) und Secure Sharing mit ein beziehungsweise ergänzt die Prozesse sinnvoll durch Abwehrmaßnahmen gegen potenzielle Angreifer und absichtliches oder versehentliches Fehlverhalten.

### 6.7.4 Beispiel für Information Protection

Ein Mitarbeiter generiert im Rahmen seiner Tätigkeit unternehmenskritische Informationen. Er muss diese Informationen den Mitarbeitern und externen Partnern zugänglich machen und dabei sicherstellen, dass keine unbefugten Personen Zugriff erhalten. In seiner Office-Applikation wählt er bei Abspeicherung des Dokumentes die Personen aus, die dieses später lesen können sollen. Er kann sicher sein, dass das Dokument nun in verschlüsselter Form vorliegt und nur mit Hilfe einer IRM-Infrastruktur von den im Vorfeld definierten Nutzern geöffnet werden kann.

---

## 6.8 Federation

Federation oder Föderation ermöglicht den gesicherten Austausch von Identitäts- beziehungsweise Authentifizierungsinformationen von digitalen Identitäten unterschiedlicher Einheiten oder Organisationen, basierend auf einem zuvor aufgebauten Vertrauensverhältnis. Entscheidend dabei ist, dass nicht direkt alle identitätsbezogenen Daten ausgetauscht werden müssen, sondern logische Beziehungen zwischen den Attributen der Identitäten hergestellt werden können. Dadurch können die realen Daten geschützt beziehungsweise anonymisiert werden. Es werden

**Abb. 6.14** Komponente und Funktion des Moduls Federation



also nur Teilinformationen oder eventuell auch nur Zustände, wie „erlaubt“ oder „verweigert“, ausgetauscht. Der Mehrwert ist ein gemeinsames, sicheres und vertrauenswürdiges Arbeiten auch über Organisationsgrenzen hinweg, siehe Abb. 6.14.

**Wichtig** Federation ermöglicht den gesicherten Austausch von Identitätsbeziehungsweise Authentifizierungsinformationen von digitalen Identitäten unterschiedlicher Einheiten oder Organisationen, basierend auf einem zuvor aufgebauten Vertrauensverhältnis.

### 6.8.1 Trust Management

Da für den Einsatz von Identity Federation ein Vertrauensverhältnis zwischen einer Organisation und ihrem jeweiligen Föderationspartner Voraussetzung ist, muss dieses in organisatorischer und technischer Hinsicht gewährleistet sein. Trust Management dient der Herstellung und dem Erhalt dieser Vertrauensbasis. Der organisatorische Hintergrund setzt sich zusammen aus Policies, Workflows und vertraglichen Aspekten zwischen der föderierenden Organisation und ihrem Partner. Auf der technischen Ebene fordert das Trust Management die Sicherheit der gesamten EIAM-System-Infrastruktur und die Einhaltung von Standards.

### 6.8.2 Identity Federation

Identity Federation ermöglicht den gesicherten Abgleich von Identitätsbeziehungsweise Authentifizierungsinformationen von Entitäten zwischen Infrastrukturen unterschiedlicher Organisationen. Sie unterscheidet sich von der Synchronisierung durch Abgleichungen über Systemgrenzen hinweg, die auch eine Anonymisierung einzelner Informationen ermöglichen. Grundlegend ist die Authentifizierung des Nutzers an der organisationsinternen Domäne, mit der

anschließend Nutzerinformationen (Claims) an die andere Organisation übergeben werden. Neben den grundsätzlichen Authentisierungsinformationen werden auch Rollen, Berechtigungen oder Nutzereigenschaften übergeben. Da nur noch eine digitale Identität transparent verwaltet wird, wird vom Nutzer nur noch ein Authentifizierungsmerkmal benötigt. Die Security Assertion Markup Language (SAML), WS-Federation und Liberty Alliance gehören zu den Standards innerhalb einer Federation-Lösung.

### 6.8.3 Beispiel für Federation

Der Mitarbeiter muss für einige Zeit mit Applikationen eines Projektpartners arbeiten. Bei dem Zugriff auf die Applikationen muss er sich mit seiner Smartcard authentifizieren. Anschließend kann er auf die fremde Applikation zugreifen.

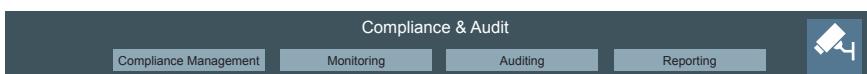
## 6.9 Compliance & Audit

Ein Audit auf Basis von Compliance, Rechtskonformität, fördert durch Überprüfung der Einhaltung von Vorschriften die Stabilität in der Infrastruktur eines Unternehmens. Compliance dient dabei der Einhaltung, während ein Audit die Überprüfung übernimmt. Weitere Techniken, die zu diesem Vorgang zählen, sind Monitoring, Reporting und Auditing, siehe Abb. 6.15.

**Wichtig** Compliance dient der Einhaltung von Vorschriften eines Unternehmens, Audit der Überprüfung.

Ein EIAM-System in einer Enterprise-Umgebung ist dazu aufgefordert, gesetzliche und regulative Vorschriften einzuhalten und umzusetzen. Compliance verfolgt das Ziel, Vorschriften einzuhalten und gegebenenfalls Risiken zu erkennen, auszuwerten und Vorschriften mittels Einsatz technischer Lösungen zu erfüllen (auch als Governance, Risk Management, and Compliance (GRC) bezeichnet). Zur Rechtskonformität zählen zum Beispiel die Dokumentation von Prozessen und (Langzeit-)Archivierung von Vorgängen in IT-Systemen. Compliance dient folgenden Bereichen:

- Schutz unternehmenskritischer Daten
- Revision von Berechtigungen
- Revision von Administrationstätigkeiten
- Einhaltung von rechtlichen und organisatorischen Vorgaben im Datenmanagement



**Abb. 6.15** Komponenten des Moduls Compliance & Audit

Ein Audit dient zum Vergleich eines Soll-Istzustandes. Es urteilt über die getroffenen Maßnahmen im Prüfungsumfeld und gibt an, ob weitere Maßnahmen erfolgen sollen, um den Sollzustand zu erreichen. Der Zustand wird formal festgelegt, indem Compliance eingeführt wird.

Die Mehrwerte von Compliance und Audit liegen in den Bereichen Einhaltung von Vorschriften, Erkennung und Bewertung von Risiken, Vergleich eines Soll-Istzustandes sowie Einhaltung der Rechtskonformität.

### **6.9.1 Compliance Management**

Ein Compliance Management definiert und verwaltet Vorschriften für Prozesse und Prozessergebnisse. Ein Unternehmen kann die Vorgaben festlegen, während Audits tatsächliche oder mögliche Verstöße gegen die Vorgaben identifizieren sowie einschätzen und gegebenenfalls dem Compliance Management berichten.

### **6.9.2 Monitoring**

Ein umfassendes Monitoring realisiert eine systematische Überwachung von Systemen und eine Protokollierung aller relevanten Daten beziehungsweise Vorgänge innerhalb eines EIAM-Systems. Die Daten liegen in Echtzeit beziehungsweise mit Zeitstempel versehen vor, um eine Überschneidung bei gleichzeitigen Zugriffen zu verhindern. Durch ein Monitoring können Fehler bei Konfiguration, Kommunikation und Anwenderaktivitäten erkannt und ausgewertet werden. Das Monitoring kann bei kritischen Vorkommnissen geeignete Gegenmaßnahmen anstoßen. Neben der Protokollierung von Aktivitäten, wie Zugriff, delegierter Administration, Self-Service oder Änderungen von Credentials können zum Beispiel auch Protokolldaten eines Privileged User Managements erfasst werden.

### **6.9.3 Reporting**

Ein Reporting bietet eine kontinuierliche Berichterstellung und Auswertung von vergangenen und aktuellen Aktivitäten im EIAM-System. Die Berichte beinhalten zum Beispiel Informationen über Zustände von Identitätsdaten und Berechtigungen sowie über den Ablauf verschiedenster Vorgänge. Das zuständige Personal erhält eine klare Übersicht über den Zustand verschiedener Prozesse und kann feststellen, ob Aktivitäten vorschriftsmäßig durchgeführt wurden. Das Reporting hat auch die Aufgabe, kritische Vorkommnisse entsprechend zu melden. Dies kann automatisierbar zum Beispiel per E-Mail, Instant-Messenger oder SMS erfolgen.

### 6.9.4 Auditing

Auditing bezeichnet im Identity Management die Bemühungen, aktuelle und vergangene Rechte und Aktionen einer Entität mit Bezug auf die IT-Systeme und IT-Ressourcen nachvollziehen und prüfen zu können. Dabei werden relevante Informationen über den Prozess erstellt, gespeichert und dem Auditor zur Verfügung gestellt. Diese ergeben sich beispielsweise durch folgende Fragen: Welche Aktionen wurden wann und von wem ausgeführt? Welche Anwendungen wurden genutzt und auf welcher Ressource wurden sie ausgeführt? Wer hat wann welche Berechtigungen vergeben? Das Reporting kann das Auditing entsprechend unterstützen. Dabei sind immer die Bestimmungen bzgl. des Datenschutzes zu beachten, die die Möglichkeiten des Auditings in Bezug auf personenbezogene Daten einschränken.

### 6.9.5 Beispiel für Compliance & Audit

Der Mitarbeiter hat während seiner Tätigkeit weisungsgemäß zwei Transaktionen durchgeführt, die eine Verletzung einer Richtlinie bedeuten. Seinem Vorgesetzten fallen diese Vorgänge auf, und er möchte die Gründe hierfür erfahren. Anhand von Logdateien der Applikation, die an einen hierfür vorgesehenen Dienst versendet werden, lässt sich die Situation nachvollziehen und der Vorgang durchgängig verifizieren.

---

## 6.10 Allgemeine Mehrwerte eines Enterprise Identity and Access Management-Systems

In vielen Unternehmen werden bereits an mehreren Stellen Teile von Enterprise Identity and Access Management-Systemen (EIAMS) eingesetzt. Durch die Konzeption und den Einsatz eines umfassenden EIAM-System ist es möglich, die verschiedenen Teilsysteme und Konzepte in das umfassende System zu migrieren. Eingebunden in eine ganzheitliche Struktur bieten die Systeme durch die gewonnene Vernetzung Mehrwerte. Das schließt die Kontrollierbarkeit (Erhöhung der Sicherheit), die Nutzerfreundlichkeit (SSO über mehrere Systeme) und die Kostensparnis mit ein. Bisherige (Teil-)EIAM-System müssen also nicht verworfen, sondern lediglich migriert werden.

### **Erhöhung der Sicherheit**

Durch die Einführung und Anwendung eines umfassenden EIAM-Systems wird mehr Sicherheit und Kontrolle von und im Umgang mit IT-Systemen erreicht. Im Folgenden wird ein kurzer Überblick über die Mehrwerte mit Bezug auf Sicherheit gegeben.

### **Starke Authentifizierungsmethoden**

Bei Systemen mit sicherheitsrelevanten Daten und Informationen ist eine starke Authentifizierung unerlässlich. Eine Möglichkeit ist das Konzept von Wissen und Besitz als Zwei-Faktor-Authentifizierung. Ein zusätzlicher dritter Faktor könnte ein biometrisches Merkmal sein.

### **Vermeiden von Fehlern durch Fehlbedienung (Schwachstelle Mensch)**

Mittels eines EIAM-Systems können die Zugänge zu Ressourcen und Daten grundsätzlich sicherer und auch einfacher gestaltet werden. Beispielsweise wird durch Single Sign-On sichergestellt, dass der Nutzer statt vieler leicht zu erratender Passwörter nur ein entsprechend starkes Passwort wählt, wodurch für den Nutzer die Notwendigkeit zum Aufschreiben von Passwörtern nicht mehr besteht. Durch einen intelligenten User Self-Service kann der Nutzer bei vergessenen Passwörtern schnell und sicher wieder arbeitsfähig werden.

### **Kontrolle von System- und Netzzugängen**

Ein umfassend eingesetztes Enterprise Identity and Access Management-System stellt sicher, dass alle aktivierten Zugänge genutzt werden und autorisiert sind, während verwaiste und nicht autorisierte Zugänge geblockt oder gelöscht werden. Im Falle des Ausscheidens oder Wechsels eines Mitarbeiters werden automatisch und unverzüglich die Zugangsrechte aufgehoben beziehungsweise modifiziert. Besonderes Augenmerk wird auf die Verwaltung von „privilegierten Nutzern“ wie beispielsweise Systemadministratoren gelegt, da hier umfangreiche Befugnisse gesammelt sein können.

### **Automatisierung**

Ein besonderer Mehrwert unter dem Aspekt der Sicherheit, aber auch der Kostenreduktion und der Nutzerfreundlichkeit, ist die Möglichkeit zur Automatisierung von Arbeitsabläufen. So kann realisiert werden, dass potenziell kritische Aktionen nicht mehr manuell und auf Abruf getätigten werden, sondern im Normalfall nur noch automatisch, basierend auf definierten Regeln und Workflows.

### **Nachvollziehbarkeit**

Ein EIAM-System ermöglicht es, alle Aktionen seiner Komponenten nachzuvollziehen. In einer sicherheitskritischen Umgebung muss zu jeder Zeit erkennbar sein, welcher Nutzer aus welchem Grund welche Aktion getätigten hat. Es bestehen aber auch „externe“ Gründe, die das sogenannte Monitoring und Auditing notwendig machen. Einer dieser Gründe ist die sogenannte Compliance.

### **Durchgängige Dokumentensicherheit**

Bei elektronischen Dokumenten ist zum einen die Reglementierung des Zugriffs von Bedeutung, zum anderen sollte bestimmt werden, wie mit dem Dokument verfahren werden darf. Neben der korrekten Arbeitsweise ist auch die Integrität des

eigentlichen Dokuments ein Schutzziel. Ein EIAM-System kann die Dokumentensicherheit über Labeling und Signaturen gewährleisten und zudem zum Beispiel die Grundlage für die Rechtsverbindlichkeit von Dokumenten bieten.

### Gewährleistung von Compliance

Mit Compliance ist die Einhaltung von Gesetzen und Vorschriften sowie eine generell regelkonforme Arbeitsweise des gesamten IT-Systems eines Unternehmens gemeint. So bietet ein EIAM-System einen zusätzlichen Mehrwert, indem die Einhaltung von Sicherheitsrichtlinien und Normen sowie Datenschutzkonformität ermöglicht beziehungsweise gewährleistet werden. Neben der Einhaltung der oftmals vielfältig gegebenen Vorschriften ist insbesondere die Überprüfbarkeit der Einhaltung von Bedeutung. Es ist möglich, eine vorgeschriebene, regelkonforme Arbeitsweise darzulegen und in unterschiedlicher Ausprägung und Tiefe Dritten gegenüber zu beweisen.

### Kostenreduktion

Ein weiterer Mehrwert, der allerdings erst nach der initialen Einführung eines EIAM-Systems entsteht, ist die Kostenreduktion. Dieser Mehrwert ist oft der Hauptbeweggrund, um die Einführung eines EIAM-Systems voranzutreiben. Die Einführung eines EIAM-Systems bringt Kosteneinsparungen mit sich, da die Aufstellung eines modernen Konzepts für die Administration der IT-Infrastruktur zu einer Rationalisierung führt. Das komplexe System zur Verwaltung von Nutzern und Rechten in einem Unternehmen wird maßgeblich vereinfacht. In der nachfolgenden Liste werden nur die wichtigsten Teilbereiche für diese Kosteneinsparung dargestellt.

### Delegated Administration

Dieser Begriff beschreibt die Dezentralisierung des Rechte- und Rollenmanagements eines EIAM-Systems. Die Verwaltung wird an diejenigen Stellen im System delegiert, an denen die Rollen tatsächlich entstehen beziehungsweise eingesetzt werden. Das hat zwei Vorteile. Zum einen kommt es zum Beispiel bei Rollenänderungen nicht mehr zu zeitlichen Verzögerungen, da nicht mehr ein zentrales und unter Umständen überlastetes IT-Team zuständig ist, sondern ein kleineres und organisatorisch leichter zu erreichendes Team mit delegierten Rechten. Zum anderen werden die Rollen mit spezieller Sachkenntnis und Fähigkeit verwaltet, da sich die entsprechende Administration in einem Zuständigkeitsbereich befindet, der mit den verwalteten Rollen in engerer Beziehung steht. Die Kostenreduktion wird einerseits durch die Zeitersparnis erreicht, andererseits durch die vereinfachte Bearbeitung der Änderungen, bei der weniger Fehler oder Nachfragen anfallen.

### Prozessautomatisierung

Die Automatisierung von Prozessen hat mehrere Vorteile, an dieser Stelle soll vor allem die Reduzierung der Opportunitätskosten (auch Alternativkosten, Verzichtskosten oder Schattenpreis genannt) genannt werden. Ein EIAM-System kann

durch Automatisierungen versuchen, dass möglichst wenig Gelegenheiten zur Nutzung von Ressourcen vergeudet werden. Konkret bedeutet dies: Wenn dem Nutzer eines IT-Systems eine Aufgabe übergeben wird – sei es bei der Ersteinstellung der Person oder bei der Bildung von Teams oder Arbeitsgruppen – sollen unmittelbar und automatisiert die korrekten Rollen und Rechte übergeben werden. Dies führt zu einer direkten Arbeitsfähigkeit des Nutzers und verringert die Opportunitätskosten auf ein Minimum.

### **User Help Desk-Reduzierung**

Ein umfassend eingesetztes EIAM-System unterstützt die Verwaltung von Identitäten und der entsprechenden Nutzer und bringt so eine Unterstützung für den User Help Desk mit sich. Durch die geringere Beanspruchung des User Help Desks werden nicht nur Kosten eingespart, sondern es wird gleichzeitig auch die Sicherheit erhöht. Denn wenn weniger Personen mit den sicherheitskritischen Nutzerinformationen umgehen müssen, entsteht weniger Angriffsfläche (Stichwort Social Engineering und Gefahren von innen).

### **Pre-Audit-Checks**

Ein Identity Management-System kann eine „Simulation“ von zum Beispiel Compliance-Audits (Überprüfung der Übereinstimmung mit einem Regelwerk) ermöglichen. Werden potenzielle Unstimmigkeiten und Probleme frühzeitig erkannt und behoben, kann die Wahrscheinlichkeit verringert werden, dass der eigentliche Audit fehlschlägt und eine Nachbearbeitung notwendig wird.

### **Zentralisierung von Aufgaben**

Die zentralisierte Ausführung von Aufgaben steht in direktem Zusammenhang mit der Automatisierung von Prozessen. Die Erfahrung zeigt, dass ein massiver Teil der Aufgaben im Bereich der Nutzer- und Berechtigungsverwaltung automatisiert ablaufen kann. Dies bewirkt eine wesentliche Kosteneinsparung.

---

## **6.11 Zusammenfassung**

Enterprise Identity and Access Management-Systeme (EIAMS) vereinfachen den Umgang mit digitalen Identitäten, ihren Attributen und Berechtigungen enorm. EIAM ist aber ein sehr komplexes Thema, daher hilft das beschriebene Modell, die unterschiedlichen Module in Einklang zu bringen.

---

## **6.12 Übungsaufgaben**

### **Übungsaufgabe 1**

Beantworten Sie die folgenden Fragen zu dem Enterprise Identity and Access Management-Referenzmodell.

1. Welcher Teil des EIAM definiert die Ziele eines Unternehmens im Zusammenhang mit Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit?
2. Wo werden die Entscheidungen über Zugriffsberechtigungen auf der Basis von Nutzeridentitäten, -rollen und Zugriffsrechten getroffen?
3. Welches Modul im EIAM-Referenzmodell ist für den Schutz des Unternehmens vor Angriffen verantwortlich?

### **Übungsaufgabe 2**

Welche Folgen hat es, wenn eine Angreiferin die „Single Sign-Off“-Komponente in einem EIAM-System übernimmt?

### **Übungsaufgabe 3**

Warum ist es wichtig, dass das Löschen einer Entität in das Life Cycle Management übernommen wird?

### **Übungsaufgabe 4**

Sie beraten eine Firma, die mehrere Tochterfirmen betreibt. Innerhalb einer Umstrukturierung sollen die Abteilungen der Tochterfirmen enger zusammen arbeiten. Bisher hat jede Tochterfirma ihr eigenes Entity-Management umgesetzt, was nun zu Problemen führt, da die Firmen die Entitäten der anderen Firmen nicht kennen. Wir würden Sie das Entity-Management umstrukturieren?

### **Übungsaufgabe 5**

Innerhalb eines streng geheimen Forschungsprojekts müssen zwei Wissenschaftler unterschiedlicher Institutionen wichtige Ergebnisse auf einem sicheren Kanal teilen. Welche Teile der EIAM-Systeme der jeweiligen Institutionen sind unmittelbar von diesem Prozess betroffen und warum?

Ergebnisse siehe: <https://norbert-pohlmann.com/cyber-sicherheit/uebungen/>

---

## **Literatur**

1. IdM-Referenzmodell <https://www.internet-sicherheit.de/forschung/identity-management/idm-referenzmodell.html>
2. Achten O, Feld S, Pohlmann N (2010) Identity Management als fortwährender Prozess – Mit Sicherheit zum Ziel. IT-Sicherheit 2010(1):52–54



# Trusted Computing

7

Trusted Computing (TC) ist eine Cyber-Sicherheits- und Vertrauenswürdigkeitstechnologie. Mithilfe von Trusted Computing stehen moderne und intelligente Cyber-Sicherheitsarchitekturen, -konzepte und -funktionen zur Verfügung, mit denen IT-Systeme mit einer höheren Robustheit und einem höheren Cyber-Sicherheitslevel umgesetzt werden können. Der besondere Schwerpunkt liegt dabei auf der Verifikation der Integrität eines IT-Systems.

**Wichtig** Ein IT-System ist vertrauenswürdig, wenn es sich immer in der erwarteten Weise für den beabsichtigten Zweck verhält.

## 7.1 Einleitung

Der Begriff des Trusted Computing wurde primär durch die Trusted Computing Group (TCG) geprägt, die die grundlegenden Spezifikationen für ein vertrauenswürdiges IT-System erarbeitet hat. Die TCG ist ein Industriekonsortium, zusammengeschlossen aus ca. 200 Firmen. Darunter befinden sich Weltmarktführer wie Microsoft, Intel, AMD, HP, IBM, Cisco, HUAWEI, Lenovo und Infineon. Die Gruppe hat sich zur Aufgabe gemacht, offene Spezifikationen für vertrauenswürdige IT-Systeme zu entwickeln, um die Cyber-Sicherheit verteilter Anwendungen mit vertretbarem Aufwand zu erhöhen. Kern aller Bemühungen der TCG ist die Bildung einer „Trusted Platform“, einer sicheren und vertrauenswürdigen Basis für Anwendungen. Die Trusted Platform, in der Form einer Sicherheitsplattform, auf der Basis von intelligenten kryptografischen Verfahren, stellt eine sichere Umgebung zum Schutz von sicherheitskritischen Daten für sicherheitskritische Operationen bereit, die sehr viele heutige Cyber-Sicherheitsprobleme, wie Malware, reduzieren kann.

**Abb. 7.1** „Airbag-Methode“ –  
„Wenn's passiert, soll es  
weniger wehtun“



## Veränderung von reaktiven zu proaktiven Cyber-Sicherheitssystemen

### 1. Reaktive Cyber-Sicherheitssystemen

Bei den heutigen reaktiven Cyber-Sicherheitssystemen, wie Anti-Spam-, Anti-Malware-, Intrusion-Detection-Systemen, ist die grundsätzliche Idee, so gut und schnell wie möglich Cyber-Angriffe zu erkennen. Das bedeutet, wenn die Cyber-Sicherheitslösungen einen Angriff durch eine entsprechende Angriffs-signatur oder eine Anomalie erkennen, dann wird versucht, das IT-System so schnell wie möglich zu schützen, um den Schaden zu reduzieren.

Dies entspricht der „**Airbag-Methode**“ – Wenn's passiert, soll es weniger wehtun! Siehe Abb. 7.1.

### 2. Proaktive Cyber-Sicherheitssysteme

Für die zunehmende Vielfalt und Komplexität der IT-Endgeräte (Wearables, Smartphones, Notebooks, PC, ...), IoT-Geräte, Netzkomponenten und IT-Infrastrukturen werden deutlich verlässlichere, robustere und wirkungsvollere Cyber-Sicherheitskonzepte benötigt. Daher ist es sinnvoll, weniger reaktive und mehr moderne proaktive Cyber-Sicherheitssysteme zu verwenden, die eine Ausführung von intelligenter Malware, eines der größten Cyber-Sicherheitsprobleme zurzeit, verhindern können.

Solche proaktiven Cyber-Sicherheitssysteme arbeiten mit einem kleinen Sicherheitskern (sichere Betriebssysteme) und Virtualisierung, können Software messbar machen und mit einer starken Isolation Anwendungen mit ihren Daten separieren und so nachhaltige und angemessene Cyber-Sicherheit bieten.

Für proaktive Cyber-Sicherheitssysteme muss die Softwarearchitektur der IT-Endgeräte allerdings grundlegend anders aufgebaut sein als bisher. Außerdem müssen Sicherheits-Infrastrukturkomponenten gemeinsam umgesetzt werden, damit diese Cyber-Sicherheits- und Vertrauenstechnologien organisationsübergreifend genutzt werden können.

Dies entspricht der „**ESP-Strategie**“ – Verhindern, dass ein Auto überhaupt ins Schleudern kommt, siehe Abb. 7.2.

**Abb. 7.2** „ESP-Strategie“ –  
Verhindern, dass ein Auto  
überhaupt ins Schleudern  
kommt

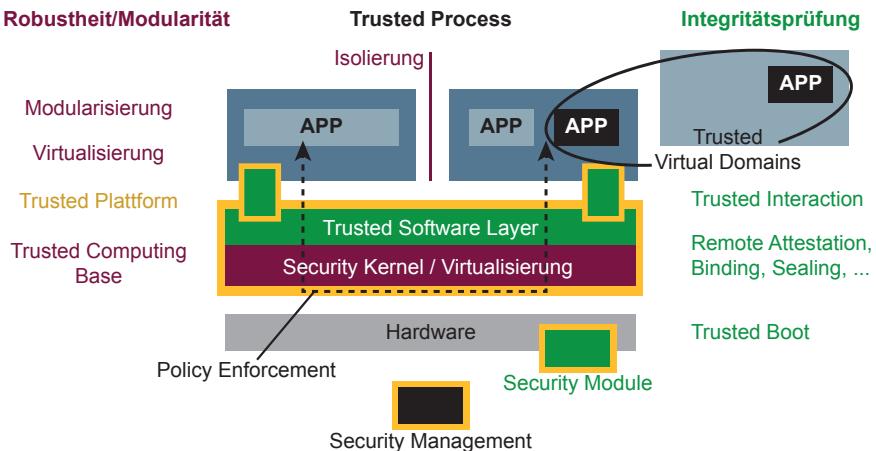


### Das Software-Problem als eine der wichtigsten Herausforderungen

Die Software stellt heute in allen Branchen einen immer größeren Wertschöpfungsanteil dar. Genutzt wird Software in Großrechnern, PCs, Notebooks, Smartphones, aber auch immer mehr in Autos, Industrieanlagen, Kühlschränken usw. Waren zum Beispiel bei Autos in der Vergangenheit nur mechanische Bauteile für die Funktion verantwortlich, steigt der Wertschöpfungsanteil der Software in Autos immer mehr. Heute werden oft die gleichen Motoren in Autos eingebaut und nur über die Software und deren Konfiguration kann entschieden werden, ob das Auto zum Beispiel 100, 130 oder 160 PS nutzen kann. Auch verfügen die Autos über immer mehr Sensoren, die von Software ausgelesen werden, um für mehr Sicherheit und Komfort zu sorgen. Das bedeutet aber auf der anderen Seite, dass die Software eine sehr hohe Qualität aufweisen muss, um verlässlich zu sein. Bei der Software in Autos wurde und wird sehr viel Aufwand in die Qualität und Verifikation von Software gesteckt, um diesem Anspruch zu genügen. Bei vielen Betriebssystemen und Anwendungen für PCs, Notebook, Smartphones usw. ist es noch ein langer Weg, eine qualitativ hochwerte Software nutzen zu können [1].

IT-Sicherheitslücken sind in der Regel keine Absicht der Programmierer oder Hersteller, sondern ein Resultat von heutigen Entwicklungsprozessen. Software wird noch immer von Menschen entwickelt und so bleiben Fehler, trotz vieler Gegenmaßnahmen durch spezielle Programmiermethoden und Softwaregutachten, nicht aus [2]. Die Fehlerdichte einer Software wird anhand der Fehler pro 1000 Programmzeilen (lines of code, kurz: loc) gemessen. Der daraus resultierende Quotient sagt dann in etwa aus, wie anfällig ein Programm potenziell ist, wobei erst bei einer Fehlerdichte <0,5 ein Programm als wirklich stabil gilt. Eine so geringe Fehlerdichte ist vor allem dort Pflicht, wo Menschenleben von einer Anwendung abhängen, wie beispielsweise bei Steuerungssystemen von Flugzeugen. Akzeptanz finden Programme jedoch schon ab einem Fehlerquotienten von 5, obwohl in der Regel stets ein Quotient <2 angestrebt wird. Kommerzielle Software weist eine durchschnittliche Fehlerdichte von 0,76 auf, bei Open Source-Software sogar nur 0,61 [3].

**Wichtig** Mit der Hilfe von Trusted Computing kann das Software-Problem in seiner Wirkung deutlich reduziert werden.



**Abb. 7.3** Sicherheitsarchitektur und Sicherheitsprinzipien eines vertrauenswürdigen IT-Systems

## 7.2 Trusted Computing auf den Punkt gebracht

In Abb. 7.3. und im folgenden Text wird dargestellt, mit welcher Sicherheitsarchitektur und mit welchen Sicherheitsprinzipien sowie Cyber-Sicherheitsmechanismen ein vertrauenswürdiges IT-System prinzipiell aufgebaut werden kann.

### 7.2.1 Robustheit und Modularität

Als erstes werden Sicherheitsaspekte grob beschrieben, die die Robustheits- und die Modularitätsaspekte betreffen.

#### Trusted Computing Base (TCB)

Eine „Trusted Computing Base“ dient als verlässliches Fundament, um darauf weitere Komponenten aufzubauen. Per Definition ist dadurch die „Trusted Computing Base“ der kritische Teil eines IT-Systems. Wenn im TCB eine Schwachstelle vorhanden ist, dann ist das ganze IT-System kompromittiert. Wenn außerhalb der TCB eine Schwachstelle vorhanden ist, dann kann anhand einer Sicherheitspolicy der potenzielle Schaden sehr eingeschränkt und klar beschrieben werden. Aus diesem Grund ist eine TCB sehr sorgfältig designet und implementiert. Eine auf einem Mikrokernel (Security Kernel) basierende TCB hat ca. 20.000 Lines of Code und ist von daher eine sehr vertrauenswürdige Basis, die in der Regel auch schon semiformal oder formal verifiziert werden kann. Mithilfe der formalen Beweisbarkeit wird eine Sicherheitsevaluation auf hohem Niveau möglich.

Es gibt aber auch TCBs, die zum Beispiel aus einem sehr abgespeckten und speziell gehärteten Linux bestehen, das auch schon sehr viel vertrauenswürdiger ist als übliche Betriebssysteme.

### **Virtualisierung**

Ein weiterer wichtiger Sicherheitsaspekt ist die Virtualisierung auf dem Endgerät. Der Vorteil von Virtualisierung besteht darin, dass auftretende Fehler (Schwachstelle, Malware, ...) in einer virtuellen Maschine in einem abgeschlossenen Bereich begrenzt bleibt und nicht eine andere virtuelle Maschine infizieren kann. Es ist auch sehr einfach möglich, die verschiedenen virtuellen Maschinen wieder in einen stabilen Urzustand zu versetzen und von da aus neu zu starten.

### **Isolierung**

Der Sicherheitsaspekt Isolierung sorgt dafür, dass die virtuellen Maschinen zusätzlich weiter stark isoliert und sicher getrennt voneinander laufen und sich nicht gegenseitig beeinflussen können und daher Schwachstellen und „Angreifer“ in einer isolierten virtuellen Maschine keinen Einfluss auf die anderen virtuellen Maschinen hat. Eine solche stark isolierte virtuelle Maschine wird im Bereich von TC auch Compartment genannt.

### **Modularisierung**

Der Sicherheitsaspekt der Modularisierung ist eine Möglichkeit, Anwendungen, die zusammen gehören, in einer virtuellen Maschine laufen zu lassen und Anwendungen, die getrennt sein sollten, in verschiedenen virtuellen Maschinen zu positionieren. Dieser Sicherheitsaspekt offeriert einen interessanten Gestaltungsspielraum, mit dem eine sehr hohe Cyber-Sicherheit erzielt werden kann, weil für verschiedene Sicherheitslevel von Anwendungen unterschiedliche virtuelle Maschinen genutzt werden können.

Eine Beispiel ist: Das Office-Paket läuft in einer virtuellen Maschine, das Design-Paket für die Business-Anwendung in einer anderen und der Browser hat auch eine separate virtuelle Maschine.

## **7.2.2 Integritätsüberprüfung**

Mit dem generellen Sicherheitsaspekt Integritätsüberprüfung kann die Integrität und damit der vertrauenswürdige Zustand eines IT-Systems überprüft sowie die Sicherheit der Schlüssel mithilfe eines TPMs gewährleistet werden.

### **Trusted Software Layer**

Die Trusted Software Layer stellt dazu vertrauenswürdige Sicherheitsdienste zur Verfügung, die helfen, IT-Systeme (Hardware, Software und Konfigurationen) vertrauenswürdig zu gestalten und messbar zu machen.

### **Security Module (TPM)**

Das Security Module (Hardware-Sicherheitsmodul) ist zum Beispiel ein TPM mit intelligenten kryptografischen Verfahren auf dem Level von Smartcard-Sicherheit, aber auch weiteren Sicherheitsdiensten, wie die Platform Configuration Register (PCR), die die sichere Speicherung und Überprüfung von Messdaten sicherstellt.

Das TPM ist ein kleiner passiver Hardware-Sicherheitschip, der fest mit dem Mainboard verbunden ist. Damit steht prinzipiell ein Hardware-Sicherheitsmodul auf jedem IT-Systemen zur Verfügung.

#### Vorteile eines TPMs

- Die Hardware-Sicherheitsmodule bieten eine sehr hohe IT-Sicherheit bei geringer Investitionssumme, da ein TPM nicht mehr als ein Euro kostet.
- Die Hardware-Sicherheitsmodule sind schon auf dem überwiegenden Teil der IT-Systeme verfügbar, das heißt, die flächendeckende Einführung einer Sicherheitsplattform ist einfach! Wenn ein IT-System „Microsoft Ready“ sein soll, muss es ein TPM verbaut haben.
- Die Hardware-Sicherheitsmodule sind in eine Sicherheitsinfrastruktur (PKI, ...) eingebunden und daher einfach im Sicherheitsmanagement zu behandeln.

#### Trusted Boot/Authenticated Boot

Mithilfe von Trusted Boot oder Authenticated Boot kann dafür gesorgt werden, dass ein IT-System nur in einem definierten vertrauenswürdigen Zustand aktiv wird.

#### Remote Attestation

Remote Attestation gibt die Möglichkeit, die Vertrauenswürdigkeit von anderen, auch fremden IT-Systemen zu messen, bevor eine Interaktion mit diesem IT-System begonnen wird.

#### Binding/Sealing

Binding und Sealing sind weitere Trusted Computing-Funktionen, mit denen moderne IT-Sicherheitssystem intelligent und vertrauenswürdig umgesetzt werden können. Bei Binding werden verschlüsselte Daten an ein TPM gebunden. Bei Sealing werden verschlüsselte Daten an die Software- und Hardware-Konfiguration eines IT-Systems sowie an ein TPM gebunden.

#### Trusted Interaction

Unter dem Begriff „Trusted Interaction“ werden Sicherheitsdienste in den Trusted Software Layern zusammengefasst, die dafür sorgen, dass Informationen vertrauenswürdig eingegeben, gespeichert, übertragen und dargestellt werden können.

### 7.2.3 Trusted Process

Trusted Process vereint die Sicherheitsaspekte, die die Abläufe in den und mit den verschiedenen IT-Systemen betreffen.

#### Security Management

Security Management fasst die wichtigen Funktionen zusammen, die notwendig sind, um das proaktive Sicherheitssystem vertrauenswürdig nutzbar zu machen.

### Policy Enforcement

Mithilfe des Policy Enforcements ist eine Trusted Plattform in der Lage, die definierte Regel auf dem eigenen, aber auch auf fremden IT-Systemen vertrauenswürdig umzusetzen.

### Trusted Virtual Domains

Trusted Virtual Domains ist das Umsetzungskonzept, das es einer Trusted Plattform ermöglicht, übergreifende Sicherheitskonzepte vertrauenswürdig umzusetzen.

#### 7.2.4 Trusted Plattform

Die Kombination und das Zusammenwirken aller Sicherheitsaspekte stellt als „Trusted Platform“ die vertrauenswürdige Basis dar! Eine Sicherheitsplattform löst mithilfe von Trusted Computing-Technologien essenzielle IT-Sicherheits-Probleme konventioneller IT-Systeme, wie sie zum Beispiel durch Malware verursacht werden. Darüber hinaus ermöglicht die Sicherheitsplattform die Durchsetzung eigener Sicherheitsregeln bei der Ausführung eigener Inhalte und Dokumente auf fremden IT-Systemen.

**Wichtig** Trusted Computing ist ein Cyber-Sicherheitskonzept, mit dem die Integrität von IT-Systemen verifiziert und die Widerstandsfähigkeit gegen moderne Angriffe deutlich vergrößert werden kann.

---

## 7.3 Trusted Computing – Grundlagen

In diesem Abschnitt werden einige Grundlagen von Trusted Computing beschrieben.

### 7.3.1 Kernelarchitekturen von Betriebssystemen

In diesem Teil wird beschrieben, welche Betriebssysteme für welchen Einsatz aus Sicht der Cyber-Sicherheit geeignet sind.

Ein Kernel ist der zentrale Bestandteil eines Betriebssystems und bildet dessen unterste Softwareschicht ab. Kernel unterscheiden mindestens zwei verschiedene Ausführungsmodi, den User-Modus und den privilegierteren Kernel-Modus. Der Kernel-Modus genießt eine besondere Priorität beim Ausführen von Kommandos und ist daher für unverzichtbare Funktionen geeignet. Zwischen den Kernel-Architekturen selbst bestehen gravierende Unterschiede in der Aufteilung der Modi und damit in der Performance und der Robustheit und Sicherheit der IT-Systeme.

## Monolithischer Kernel

Unix und unixoide Systeme wie Android, GNU Linux, BSD und andere basieren auf einem monolithischen Kernel. In dieser Kernelarchitektur sind neben der Prozesskommunikation und Speicherverwaltung bereits viele wichtige Funktionen, wie Zugriff auf die Hardware durch Treiber, im Kernel-Modus implementiert und benötigen keine zusätzlichen Programme. Gegenüber anderen Kernelarchitekturen bietet die monolithische Architektur daher einen Vorteil in Sachen Performance.

Da alle Module im selben Adressraum laufen, kann ein Fehler in einem Modul das ganze IT-System zum Absturz bringen. Architekturen auf monolithischem Kernel sind anfälliger für Systemausfälle, da fest integrierte, wichtige Teile des Kernels nicht ohne weiteres neu gestartet werden können, falls diese abstürzen.

Die klassische, monolithische Kernelarchitektur eignet sich durch ihre Performance für den Betrieb von Desktop- oder Notebook-Systemen. Dasselbe gilt für mobile Betriebssysteme wie Android, da die Anforderungen durch die hohe Bandbreite an Apps mindestens so hoch sind wie bei einem Notebook oder Desktop-PC. Solche IT-Systeme lassen sich zusätzlich abhärten, in dem bewusst auf Funktionen verzichtet wird, die für den vorgesehenen Einsatz nicht benötigt werden. Betriebssysteme mit monolithischem Kernel sind sehr groß, und selbst gehärtet bestehen sie noch aus mehreren Millionen Zeilen Programmcode.

### Vor- und Nachteile eines monolithischen Kernels

Vorteile:

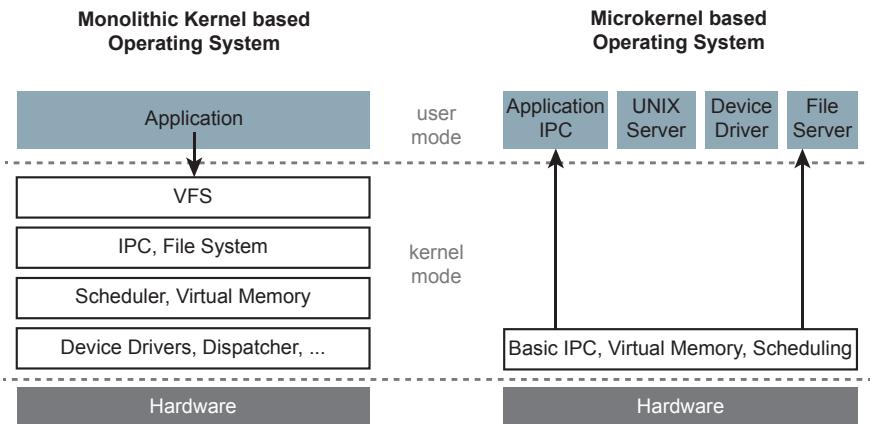
- lange etabliert
- gute Performance

Nachteile:

- alle Treiber vereint im Kernel-Space
- geringere Flexibilität
- höhere Komplexität
- wenig robust
- schlechte Sicherheitsmechanismen

## Mikrokernel

In einem Mikrokernel hingegen laufen nur grundlegende Funktionen im Kernel-Modus, wie Prozess- und Speichermanagement sowie Grundfunktionen zur Synchronisation und Kommunikation. Alle weiteren Funktionen sind durch eigene Prozesse oder Programmbibliotheken im User-Modus implementiert. Einzelne Komponenten des Betriebssystems können im Betrieb ausgetauscht oder neu gestartet werden, ohne dass deren Absturz das gesamte IT-System gefährdet, siehe Abb. 7.4.



**Abb. 7.4** Vergleich von Kernelarchitekturen

Mikrokernels sind vergleichsweise winzig, da viele Funktionen erst durch Programme im User-Modus verfügbar werden. Mikrokernels bestehen beispielsweise aus etwa 20.000 Zeilen Code. Eine so geringe Menge an Codezeilen ist weitaus effektiver zu prüfen und daher qualitativ hochwertiger zu entwickeln, als es bei monolithischen Kernel möglich ist. Daher eignen sich Mikrokernels besonders gut für die Umsetzung einer Trusted Computing Base.

### Vor- und Nachteile eines Mikrokernels

Vorteile:

- höhere Robustheit
- höhere Modularität
- höhere Flexibilität
- höhere IT-Sicherheit ... wegen mehr prozessübergreifender Kommunikation, ...
- weniger benötigter Speicherplatz

Nachteile:

- weniger Leistung durch mehr Kommunikation zwischen den Prozessen

### Sicherheit beginnt bei der Hardware – Sicherheitsanker

Software alleine hat Grenzen bei der vertrauenswürdigen Umsetzung von sicheren IT-Systemen und Anwendungen. Eingebaute Software-Schutzmechanismen können manipuliert werden und dürfen keine Aussage über die Integrität eines IT-Systems tätigen. Die Wahl einer geeigneten Hardware zum Schutz der Software gehört zu den vielversprechenderen Ansätzen im Bereich der Cyber-Sicherheit und ist ein wichtiger Aspekt im Trusted Computing-Konzept. Viele Sicherheitsprobleme können durch spezielle Sicherheitsanker im Vorfeld abgeschwächt oder teilweise sogar verhindert werden. Sicherheitsanker repräsentieren einen stark vertrauensvollen Punkt im IT-System und lassen sich durch autonome Hardwarekomponenten realisieren.

Das Trusted Platform Module (TPM) verfügt über einen kleinen Krypto-Prozessor, der einen Zufallszahlen-, Schlüssel-, One-Way-Hashfunktionsgenerator usw. bereitstellt. Als Hardware-Sicherheitschip ist das TPM fest mit dem Mainboard eines IT-Systems verbunden. Es wird im Rahmen vertrauenswürdiger IT-Systeme dazu benutzt, um Manipulationen an der Hard- und Software aufzudecken, bei denen mit geeigneten Sicherheitsmaßnahmen bis hin zur Sperrung des IT-Systems reagiert wird. Jedes TPM enthält einen speziellen, ihm zugeordneten Basis-Schlüssel (Endorsement Key – EK). Der EK verlässt das Hardware-Sicherheitsmodul nach Erzeugen nicht mehr, sondern kann nur durch Erzeugen eines neuen Schlüssels überschrieben werden. So bleibt sichergestellt, dass der EK des TPM nicht extern missbraucht wird. Das TPM kann auch genutzt werden, um die im Betriebssystem verwendeten Schlüssel zu verwalten. Dazu wird ein weiterer Schlüssel des TPM, der Storage Root Key (SRK), bereitgestellt, um alle im TPM gespeicherten Schlüssel des Nutzers zu verschlüsseln und außerhalb des TPMs sicher zu speichern. Geheime Schlüssel, zum Beispiel für S/MIME oder PGP zur E-Mail-Kommunikation, lassen sich auch auf die Art sicher über das TPM verwalten.

### 7.3.2 Core Root of Trust for Measurement (CRTM)

Eine vertrauenswürdige Basis, eine Trusted Platform, braucht eine Wurzel oder Basis des Vertrauens.

Die Lösung bei der „Trusted Computing Group“ heißt „Basis Root of Trust“, die eine Kette des Vertrauens (Chain of Trust) bildet. Für normale IT-Systeme wurde von der Trusted Computing Group die Komponente „Core Root of Trust for Measurement (CRTM)“ spezifiziert.

Der CRTM ist dabei eine Software, die einen Messvorgang über einzelne Systemzustände (Hard- und Software) außerhalb der Trusted Platform vertrauenswürdig durchführt und dann die Ergebnisse innerhalb der Trusted Platform in die Platform Configuration Register (PCR) des TPMs hinterlegt.

Die Ausführung der CRTM Software beginnt mit dem Bootvorgang. Beim Authenticated Boot werden die Systemzustände der Soft- und Hardware erst mal nur gemessen und in die Platform Configuration Register (PCR) des TPMs gespeichert und können anschließend für die Überprüfung der Integrität des IT-Systems verwendet werden. Dies ist anders als bei einem Secure Boot, bei dem bei Feststellen eines unerwarteten Systemzustands der Bootvorgang sofort gestoppt wird. Technisch wird die CRTM Software in der Regel in das BIOS des IT-Systems integriert.

#### Grundsätzliche Idee von „Chain of Trust for Measurement“

Bei dem Konzept „Chain of Trust for Measurement“ ist das Ziel, das Vertrauen in Entität  $E_n$  zu gewinnen.

Der Ablauf ist so:  $E_0$  startet  $E_1$ ,  $E_1$  startet  $E_2$  usw.



**Abb. 7.5** Chain of Trust

Um E<sub>n</sub> zu vertrauen, muss E<sub>n-1</sub> vertraut werden. Um E<sub>n-1</sub> zu vertrauen, muss E<sub>n-2</sub> vertraut werden usw.

E<sub>0</sub>, E<sub>1</sub> bis E<sub>n</sub> schaffen eine „Vertrauenskette“, siehe Abb. 7.5.

### „Transitives Vertrauen“

Vertrauen ist transitiv von E<sub>0</sub> nach E<sub>1</sub> nach E<sub>2</sub> bis E<sub>n</sub>.

Es wird nicht invertiert: Vertrauen auf E<sub>0</sub> bedeutet NICHT, dass E<sub>2</sub> vertraut werden kann.

Das Vertrauen von E<sub>2</sub> erfordert, dass E<sub>0</sub> und E<sub>1</sub> vertraut werden kann.

### 7.3.3 Identitäten von TPMs

Im Folgenden werden die Identitäten eines TPMs beschrieben.

#### TPM Identität (Endorsement Key)

Die eindeutige TPM-Identität ist der Endorsement Key (EK). Er besteht aus einem RSA-Schlüsselpaar mit geheimem und öffentlichem Schlüssel. Der geheime Schlüssel ist im TPM gespeichert und kann nicht ausgelesen, sondern nur intern im TPM verwendet werden. Der öffentliche Schlüssel ist datenschutzsensitiv, da er ein TPM/eine Plattform identifiziert. Der Endorsement Key wird während des Herstellungsprozesses im TPM erzeugt und muss von der EK erzeugenden Einheit zertifiziert sein, beispielsweise vom TPM-Hersteller. Dieser Prozess und die Einzigartigkeit des EK ist eine wichtige Grundlage für die Vertrauenswürdigkeit des TPM-Systems.

Der TPM-Hersteller hat dazu eine Public Key-Infrastruktur, die insbesondere für das Management von Schlüsseln hilfreich ist.

Eigenschaften des Endorsement Keys:

- steht im nicht flüchtigen Speicher des TPMs
- ist nicht migrierbar
- ist einem TPM eindeutig zugeordnet und einzigartig
- ist von einer Zertifizierungsstelle zertifiziert

#### Endorsement Credential (Endorsement Zertifikat)

Ist ein elektronisches Endorsement-Zertifikat, das besagt, dass der Endorsement Key ordnungsgemäß erstellt wurde und in ein TPM eingebettet ist.

Das Endorsement Credential ist von der Entität ausgestellt, die den Endorsement Key generiert hat, zum Beispiel der TPM-Hersteller.

Das Endorsement Credential enthält:

- TPM-Herstellename
- TPM-Modellnummer
- TPM-Version
- den öffentlichen Schlüssel des Endorsement Keys (datenschutzsensitiv)

### **Plattform-Identität**

Die Plattform-Identität entspricht der TPM-Identität, dem Endorsement Key (EK). Ein TPM muss an nur eine Plattform gebunden sein, entweder durch physikalisches Binden (zum Beispiel an das Motherboard der Trusted Plattform gelötet) oder logische Bindung (zum Beispiel unter Verwendung von Kryptografie).

### **Platform Credential (Plattform-Zertifikat)**

Das Plattform-Zertifikat wird vom Motherboard/IT-System-Hersteller in den TPM eingebracht und bestätigt, dass ein gültiger TPM in eine korrekte Plattform montiert wurde. Ausgestellt wird das „Platform Credential“ vom Plattformhersteller, zum Beispiel IT-System- oder Motherboard-Hersteller. Mit dem Plattform-Zertifikat wird bescheinigt, dass das IT-System eine Trusted Platform darstellt.

Platform Credential enthält:

- Name des Plattformherstellers
- Plattformmodell und Versionsnummer
- Verweise auf die entsprechenden Endorsement and Conformance Credential (bestätigt, dass ein Plattformtyp die Evaluierungsrichtlinien der TCG erfüllt)

### **7.3.4 TPM-Schlüssel und deren Eigenschaften**

In diesem Abschnitt werden die Schlüssel und deren Eigenschaften des TPMs beschrieben.

#### **Migratable and Non-Migratable Keys**

Da über das TPM sowohl plattformbezogene Schlüssel wie auch personenbezogene Schlüssel geschützt werden können, besteht die Notwendigkeit, die personenbezogenen Schlüssel sicher auf andere Plattformen zu transferieren. Die TCG hat dazu unter dem Begriff Migration ein Regelwerk definiert:

1. ***Migratable Keys*** (*sind auf andere Plattformen übertragbar*)

Die Migratable Keys können auf andere TPMs/Plattformen migriert werden, daher kann nicht garantieren werden, dass solche Schlüssel von einem bestimmten TPM generiert wurden. Das sind alle vom Nutzer gespeicherte Schlüssel.

2. ***Non-Migratable Keys*** (*sind an die Plattform gebunden*)

Non-Migratable Keys können nicht auf andere TPMs/Plattformen migriert werden. Dies garantiert, dass der Schlüssel nur in einen TPM genutzt werden kann.

Ein TPM kann ein Zertifikat generieren, das angibt, dass ein Schlüssel nicht migrierbar ist. Beispiele von Non-Migratable Keys sind der Endorsement Key, der Storage Root Key und die Attestation Identity Keys.

### Storage Root Key (SRK)

Ein TPM enthält den sicheren Datenspeicher „Root of Trust for Storage (RTS)“. Dieser sichere Datenspeicher ist als Schlüsselhierarchie implementiert und der Storage Root Key (SRK) ist die Wurzel dieser Schlüsselhierarchie. Der Storage Root Key (SRK) ist ein RSA-Schlüsselpaar (Non-Migratable). Der geheime Schlüssel darf das TPM nie verlassen; damit wird sichergestellt, dass sämtliche anderen Schlüssel nur innerhalb des TPMs entschlüsselt werden können (siehe TPM Schlüsselhierarchie).

Der Storage Root Key wird von TPM während der Installation des TPM-Eigentümers generiert. Der SRK wird gelöscht, wenn der TPM-Besitzer gelöscht wird. Diese Löschung sorgt dafür, dass alle Daten nicht mehr entschlüsselt werden können, die mit Schlüsseln in dieser Hierarchie verschlüsselt sind.

Eigenschaften von Storage Root Keys:

- steht im nicht flüchtigen Speicher des TPMs
- ist nicht migrierbar

### Attestation Identity Keys (AIK)

Der Attestation Identity Keys (AIK) wird verwendet, um die aktuelle Plattformkonfiguration, die Integrität der Plattform zu bestätigen, zum Beispiel die aktuelle Hard- und Softwareumgebung authentisch an eine entfernte Partei oder lokale Instanz melden- siehe Trusted Computing-Funktion „„Attestierung““.

Attestation Identity Keys sind Alias für ein TPM/eine Plattformidentität (Endorsement Key). Die Verwendung von AIKs sollte die Verfolgung von TPMs/Plattformen verhindern. Beispielsweise können die Transaktionen einer Plattform verfolgt werden, wenn der EK in verschiedenen Protokollläufen mit verschiedenen kollidierenden Dienstanbietern verwendet wird.

AIKs sind nicht migrierbare Signaturschlüssel, sie werden vom TPM-Besitzer erstellt und ein TPM/eine Plattform kann mehrere AIKs besitzen, zum Beispiel eine für Online-Banking-Sicherheit, eine für E-Mail-Sicherheit usw.

Eigenschaften von Attestation Identity Keys:

- stehen im nicht flüchtigen Speicher des TPMs
- nicht migrierbar

### Storage Keys

Ein Storage Key wird zum Schutz (Verschlüsselung) von Schlüsseln und Daten außerhalb des TPM, aber innerhalb der TPM-Schlüsselhierarchie, verwendet. Beispielsweise kann ein Storage Key (Speicherschlüssel) verwendet werden, um andere Schlüssel zu verschlüsseln, die auf einer Festplatte gespeichert werden können. Storage Root Key (SRK) ist ein spezieller Speicherschlüssel und bietet

starken Schutz von beliebigen TPM-externen Daten (Versiegelung), zum Beispiel Verschlüsselung von Geheimnissen, die nur wiederhergestellt werden können, wenn die Plattform eine definierte Hard-/Softwareumgebung hat.

Eigenschaften von Storage Keys:

- RSA-Schlüsselpaar
- im Allgemeinen darf die Migration zu anderen TPMs erfolgen

### **Binding Keys**

Ein Binding wird zum Schutz von beliebigen Daten außerhalb des TPM verwendet. Die Bindung entspricht der asymmetrischen Verschlüsselung, die an einen TPM gebunden ist.

Eigenschaften von Binding Keys:

- RSA-Schlüsselpaar (es können auch andere Algorithmen vom TPM unterstützt werden)
- im Allgemeinen darf die Migration zu anderen TPMs erfolgen
- kann nur mit Binding-Befehlen verwendet werden

### **Signing Keys**

Signing wird wie das Binding zum Schutz von beliebigen Daten außerhalb des TPM verwendet. Das Signing bindet aber zusätzlich die Integrität der Plattform mit ein.

Eigenschaften von Signing Keys:

- RSA-Schlüsselpaar (es können auch andere Algorithmen vom TPM unterstützt werden)
- im Allgemeinen darf die Migration zu anderen TPMs erfolgen

### **TPM-Schlüsselhierarchie**

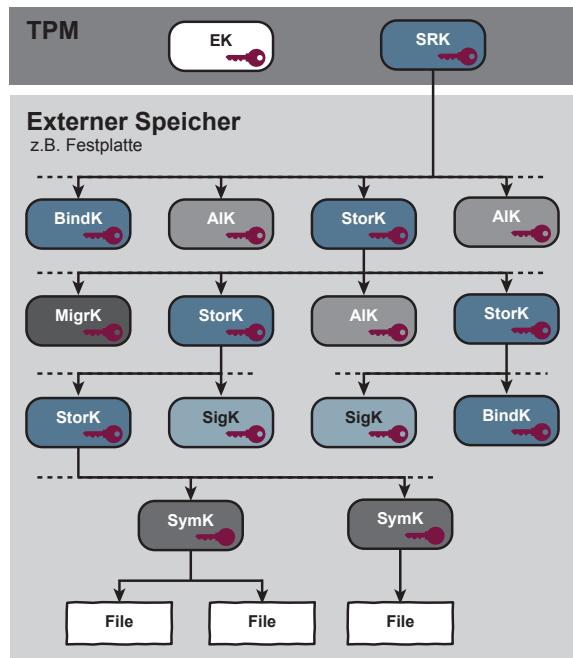
Eine wichtige Aufgabe des Hardware-Sicherheitsmoduls TPM ist die Verwaltung von Schlüsseln. Wie in Abb. 7.6 zu sehen ist, werden alle Schlüssel in eine Schlüsselhierarchie eingeordnet, in der untergeordnete Schlüssel mit dem übergeordneten Schlüssel verschlüsselt gespeichert werden. Dies ermöglicht, dass Schlüssel auch außerhalb des TPMs auf externen Speichern, wie der Festplatte, sicher gespeichert werden können. Die Tiefe der Hierarchie und Anzahl der TPM-geschützten Schlüssel ist nur durch die Größe des externen Speichers begrenzt. Die Wurzel dieser Schlüsselhierarchie ist der Storage Root Key (SRK), der fest an die Plattform gebunden und nicht migrierbar ist.

A → B meint A verschlüsselt B. A ist der übergeordnete und B der untergeordnete Schlüssel.

Der Speicherschlüssel (StoreK) schützt alle anderen Schlüsseltypen:

- Attestation Identity keys (AIK)
- Signing keys (SigK)
- Binding keys (BindK)
- Migration keys (MigrK)
- Symmetric keys (SymK)

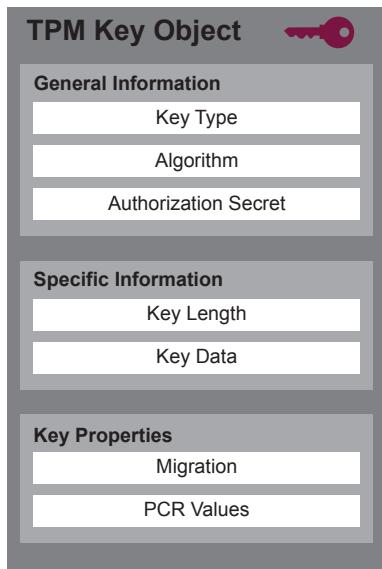
**Abb. 7.6** TPM-Schlüsselhierarchie



### TPM Key Object

Jeder Schlüssel ist in einem „TPM Key Object“ eingebunden, das verschiedene Attribute beinhaltet.

Das Feld „Key Type“ in Abb. 7.7 beschreibt den Typ des Schlüssels, wie zum Beispiel Signing Key, Binding Key, Storage Key, ... Das Feld „Algorithm“ beschreibt das Kryptografieverfahren, wie zum Beispiel RSA, DSA, HMAC, AES, ... Im Feld „Authorization Secret“ steht, dass ein Berechtigungsschlüssel erforderlich ist, um den Schlüssel zu verwenden. Im Feld „Key Data“ steht der öffentliche und geheime Schlüssel, asymmetrischer Schlüssel. Der geheime Schlüssel wird mit dem entsprechenden „übergeordneten Schlüssel“ verschlüsselt. Im Feld „Migration“ steht ein entsprechendes Attribut: migratable, certified mitgratable oder non-migratable. Feld „PCR Values“: Ein Schlüssel kann mit spezifischen PCR-Werten verschlüsselt werden. Dies bedeutet, dass ein solcher Schlüssel nur dann verwendet werden kann, wenn sich die Plattform in einem definierten vertrauenswürdigen Zustand befindet.

**Abb. 7.7** TPM Key Object

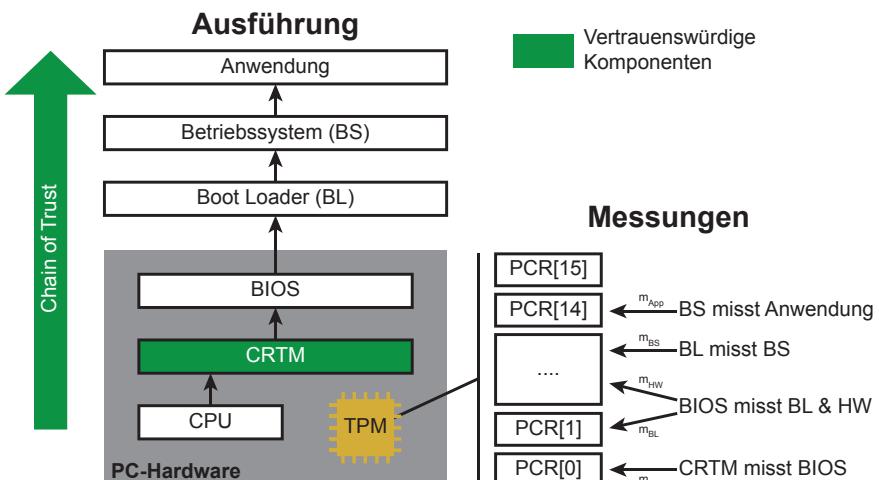
### 7.3.5 Trusted Computing-Funktionen

Mit der Hilfe der folgenden Trusted Computing-Funktionen können moderne IT-Sicherheitssysteme intelligent umgesetzt werden.

#### Authenticated Boot

Beim Authenticated Boot werden die Systemzustände der Soft- und Hardware erst mal nur gemessen und in die Platform Configuration Register (PCR) des TPMs gespeichert.

In Abb. 7.8 ist exemplarisch aufgezeigt, wie eine solche Messung umgesetzt werden kann. Zuerst wird mit der vertrauenswürdigen CRTM Software das BIOS

**Abb. 7.8** Authenticated Boot – Messen und Speichern des Systemzustandes

gemessen und der berechnete Hashwert in ein PCR-Register geschrieben. Danach berechnet das BIOS den Hashwert des Boot Loaders sowie zusätzlich Hashwerte des Hardwarezustandes, wie Mainboard und ROM-Konfiguration und schreibt diese Hashwerte in bestimmte PCR-Register. Anschließend wird vom Boot Loader der Hashwert des Betriebssystems berechnet und in ein weiteres PCR-Register gespeichert. Zum Schluss wird dann vom Betriebssystem der Hashwert der Anwendung berechnet und in ein PCR-Register geschrieben.

Der Gesamtwert kann dann von einer lokalen Instanz wie ein Hardware-Sicherheitsmodul eines USB-Sticks oder aus der Ferne mit „Remote Attestation“ überprüft werden.

#### *Platform Configuration Register (PCR)*

Das Platform Configuration Register (PCR) besteht aus mehreren Registern. Die Register dienen zur Speicherung der Hashwerte bestimmter Systemzustände aktueller Soft- und Hardwarekonfigurationen. Die PCR befinden sich im flüchtigen Speicherbereich des TPM.

Damit ist es auch möglich, erzeugte Schlüssel an spezielle PCR's, spezielle Systemzustände, zu binden (Sealing). Eine Entschlüsselung der mit diesem Schlüssel verschlüsselten Daten ist dann nur mit der exakt gleichen Hard- und Softwarekonfiguration möglich. Beim Einfügen neuer Hashwerte in das PCR im Authenticated Boot-Prozess werden die alten Werte nicht einfach überschrieben, sondern es wird ein neuer Hashwert als Kombination aus altem und neuem Wert gebildet.

#### **Binding**

Binding wird verwendet, um Daten an eine bestimmte TPM/Plattform zu binden. Daten, die mit einem nicht migrierbaren Schlüssel verschlüsselt wurden, können nur von dem entsprechenden TPM wiederhergestellt werden, das den passenden geheimen Schlüssel kennt.

Normalerweise bietet Binding keine Plattformbindung, da die Bindung auch mit migrierbaren Schlüsseln umgesetzt werden kann. Dadurch können verschlüsselte Daten auf eine andere Plattform transferiert und genutzt werden.

#### **Sealing (Erweiterung von Binding)**

Sealing bindet Daten immer an einen bestimmten TPM und zusätzlich auch an die Plattformkonfiguration. Sealing kann nur mit „nicht migrierbaren Schlüsseln“ umgesetzt werden. Damit kann die Soft- und Hardwarekonfiguration der Plattform verifiziert werden. Der Schlüsseltextr enthält implizit auch den Status der Plattform zum Zeitpunkt der Verschlüsselung. Dadurch können mit Sealing Daten an eine bestimmte Plattformkonfiguration gebunden werden. Daten können nur entschlüsselt werden, wenn sich die Plattform in einem vordefinierten Zustand befindet. Die Idee ist, dass der vordefinierte Zustand ein vertrauenswürdiger Zustand ist, mit einer vorgegebenen vertrauenswürdigen Software und Hardware.

### Funktion „Sealing“

#### **Eingabe Parameter**

daten {unverschlüsselte Daten}

#### **Ausgabe Parameter**

cipher	{verschlüsselte Daten}
cryptedKEY	{verschlüsselter Schlüssel}

#### **TPM Interne Funktionen und Daten**

encrypt (key, daten)	{symmetrischer Verschlüsselungsalgorithmus „AES“}
H (daten)	{One-Way-Hashfunktion „SHA-256“}
genKey()	{Schlüsselerzeugung}
SRK	{Storage Root Key}
PCRs	{PCR-0, PCR-1, ...} zum Beispiel aktuell abgespeicherte PCR-Werte

plainKEY=genKEY ()

cipher=encrypt (plainKEY, (daten // H (daten // PCR-0 // ... //PCR-x))

cryptedKEY=encrypt (SRK, plainKEY // H (plainKEY))

### Funktion „Un-Sealing“

#### **Eingabe Parameter**

cipher	{verschlüsselte Daten}
cryptedKEY	{verschlüsselter Schlüssel}

#### **Ausgabe Parameter**

daten	{unverschlüsselte Daten}
-------	--------------------------

#### **TPM Interne Funktionen und Daten**

decrypt (key, daten)	{symmetrischer Verschlüsselungsalgorithmus „AES“}
H (daten)	{One-Way-Hashfunktion „SHA-256“}
checkPCRs (Hash-Value)	{vergleicht PCRs-Inhalte mit Hash-Value}
SRK	{Storage Root Key}
PCRs	{PCR-0, PCR-1, ...}

plainKEY=decrypt (SRK, cryptedKEY)

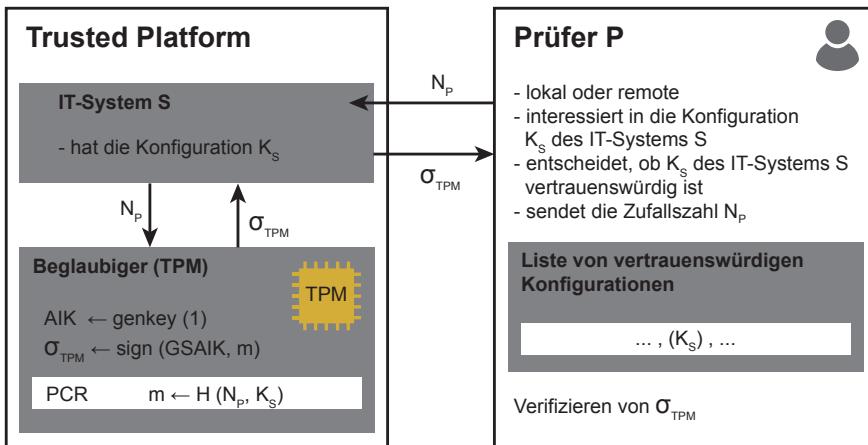
daten // H (daten // PCR-0 // ... //PCR-x)=decrypt (plainKEY, cipher)

if (checkPCRs (Hash-Value))

    return daten

else

    return ERROR

**Abb. 7.9** Attestation

(Remote) **Attestation** (Begläubigung, Überprüfung der Systemkonfiguration eines IT-Systems)

Mit der Attestation ist es möglich, die aktuelle Konfiguration eines IT-Systems zu überprüfen. In Abb. 7.9 ist eine grobe Beschreibung des Attestierungskonzeptes dargestellt. Eine prüfende Instanz kann lokal oder remote überprüfen, ob eine gewünschte vertrauenswürdige Konfiguration eines IT-Systems vorliegt. Dazu hat die prüfende Instanz eine Liste von vertrauenswürdigen Konfigurationen, die ein IT-System haben kann, damit es gestartet werden kann oder eine Interaktion umgesetzt wird.

Dazu sendet die prüfende Instanz eine Zufallszahl ( $N_p$ ) an das IT-System S. Das IT-System S stellt diese Zufallszahl dem TPM zur Verfügung. Dort wird aus der aktuellen Konfiguration der PCRs ein Hashwert berechnet. Dieser Hashwert wird zusammen mit der Zufallszahl unter der Nutzung eines Attestation Identity Keys signiert  $\sigma_{\text{TPM}}$  und an die prüfende Instanz über das IT-System gesendet. Die prüfende Instanz kann jetzt den Wert  $\sigma_{\text{TPM}}$  verifizieren und mit den vertrauenswürdigen Konfigurationen aus der eigenen Liste vergleichen. Findet sich eine passende vertrauenswürdige Konfiguration, wird das IT-System gestartet.

### Signaturfunktion für die Attestierung

#### Eingabe Parameter

random

{Zufallszahl des Prüfers P -  $N_p$ }

#### Ausgabe Parameter

signature//certificate

{Signatur der aktuellen Systemkonfiguration des AIKs}

#### TPM Interne Funktionen und Daten

sign (key, daten)

{RSA-Signatur}

$H(\text{daten})$

{One-Way-Hashfunktion "SHA-256"}

<i>GSAIK</i>	{geheimer AIK-RSA-Schlüssel}
<i>AIK-certificate</i>	{elektronisches Zertifikat des AIKs}
<i>PCRs</i>	{PCR-0, PCR-I, ...} zum Beispiel aktuell abgespeicherte PCR-Werte
$\sigma_{TPM} = \text{sign}(\text{GSAIK}, H(\text{random} // \text{PCR-0} // \dots // \text{PCR-x}))$	

### Verifikationsfunktion für die Attestierung

**Eingabe Parameter**

<i>signature//certificate</i>	{Signatur der Systemkonfiguration des AIKs}
-------------------------------	--

**Ausgabe Parameter**

<i>return value</i>	{Rückgabewert}
---------------------	----------------

**TPM Interne Funktionen und Daten**

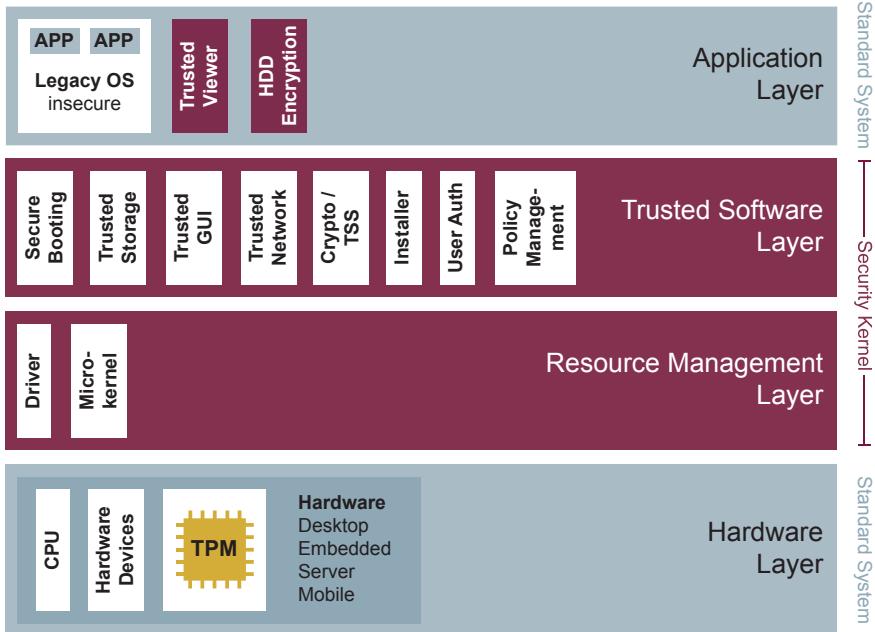
<i>very (key, daten)</i>	{RSA-Signatur-Verifikation}
<i>H (daten)</i>	{One-Way-Hashfunktion "SHA-256"}
<i>ÖSAIK</i>	{öffentlicher AIK-RSA-Schlüssel}
<i>checkPCRs (PCR-Values)</i>	{vergleicht den Inhalt der PCRs mit den gewünschten Werten}
<i>PCRs</i>	{PCR-0, PCR-I, ...}
<i>if (very (ÖSAIK, <math>\sigma_{TPM}</math>)) and</i>	
<i>if (checkCERT (certificate))</i>	and
<i>if (checkPCRs (Hash-Value))</i>	
<i>return ok</i>	
<i>else</i>	
<i>return ERROR</i>	

### Schutz kryptografischer Schlüssel

Schlüssel werden innerhalb des TPMs erzeugt, benutzt und sicher abgelegt. Die Schlüssel müssen dieses also nie unverschlüsselt verlassen. Dadurch sind sie vor Software-Angriffen geschützt. Vor Hardware-Angriffen besteht ebenfalls ein relativ hoher Schutz (Sicherheit ist mit Smartcards vergleichbar), siehe Kap. 3 „Hardware-Sicherheitsmodule zum Schutz von sicherheitsrelevanten Informationen“.

### 7.3.6 Trusted Platform (Security-Plattform, Sicherheitsplattform)

Eine Sicherheitsplattform löst mithilfe von Trusted Computing-Technologien essenzielle IT-Sicherheits-Probleme konventioneller IT-Systeme, wie sie durch Malware verursacht werden. Darüber hinaus ermöglicht die Sicherheitsplattform die Durchsetzung eigener Sicherheitsregeln bei der Ausführung eigener Inhalte und Dokumente auf fremden IT-Systemen. In diesem Abschnitt werden die technische Architektur skizziert und die grundlegenden Eigenschaften dargelegt [4], siehe Abb. 7.10.



**Abb. 7.10** Trusted Platform

### Hardware-Ebene (Hardware Layer)

Die Hardwaerebene besteht aus den herkömmlichen Hardware wie CPU, dem Arbeitsspeicher und anderen Hardwareteilen. Zusätzlich stellt die Hardware Trusted Computing-Technologie zur Verfügung, wie zum Beispiel das Trusted Platform Module (TPM).

### Ressource Management Layer (Hypervisor-Ebene)

Oberhalb der Hardwaereschicht liegt die Ressourcen-Management- oder Hypervisor-Ebene. Die Hauptaufgabe dieser Ebene besteht in der Bereitstellung abstrakter Schnittstellen zu darunter liegenden Hardwareressourcen wie Interrupts, Arbeitsspeicher und anderer Hardware. Sie ist einerseits verantwortlich für die Verteilung der Hardwareressourcen und andererseits für die Durchsetzung der obligatorischen Zugriffsrechte, die auf den zur Verfügung stehenden Hardwareressourcen basieren. Da der Zugriff auf die Hardwareressourcen meist höchst sicherheitskritisch ist, muss die Ebene für das Ressourcen-Management zwei wichtige Bestandteile zur Verfügung stellen: Isolation und das „least privilege“-Prinzip.

Typischerweise wird ein Multi-Server-Ansatz verwendet, bei dem isolierte Dienste im „User-Mode“ auf einem Mikrokern realisiert werden. Um Hardwarekomponenten nutzen zu können, werden Hardwaredriver benötigt, die ebenfalls Teil der Ressourcen-Management-Ebene sind. Da gefährlicher Code mit Zugriff über DMA (direct memory access) jeden Sicherheitsmechanismus umgehen kann,

muss die Ressourcen-Management-Ebene außerdem sicherstellen, dass nur sichere Komponenten DMA nutzen können. Ein wichtiger Vorteil von mikrokernbasierten Systemen ist ihre geringe Anzahl an Lines of Code. Sie sind daher für den Einsatz in kleinen IT-Systemplattformen, zum Beispiel in mobilen Geräten oder eingebetteten Systemen, prädestiniert.

### Trusted Software Layer (Vertrauenswürdige Software)

Durch die Verbindung und Erweiterung der Schnittstellen, die von der darunter liegenden Ressourcen-Management-Ebene zur Verfügung gestellt werden, stellt die Trusted Software-Ebene sicherheitskritische Dienste zur Verfügung, die für eine Sicherheitsplattform benötigt werden:

- **Trusted Storage (Manager)**

Der Trusted Storage-Manager stellt einen vertrauenswürdigen Speicherbereich dar, an den sich Prozesse wenden können, um Daten sicher und integer abzulegen. Es können Daten an die Konfiguration (PCRs), an einen Nutzer, oder an eine Anwendung gebunden werden. Der Trusted Storage-Manager stellt außerdem die Eigenschaft „freshness“ bereit. Das bedeutet, dass Replay-Angriffe erkannt und verhindert werden können.

- **Trusted GUI**

Basierend auf den Grundfunktionen der Ressource-Management-Ebene wird den Nutzern eine nutzerfreundliche, aber sichere Schnittstelle zur Verfügung gestellt, die sicherheitskritische Fehler zu vermeiden hilft. Ein Authentifizierungsmechanismus für Anwendungen hilft Nutzern beispielsweise dabei, Malware zu erkennen. Darüber hinaus ist die sichere Schnittstelle dafür zuständig, dass bestimmte Befehle (z. B. „Kopieren“ und „Einfügen“) nicht gegen Sicherheitsrichtlinien verstößen. Eine weitere Aufgabe der sicheren Nutzerschnittstelle ist es, die Integrität und Vertrauenswürdigkeit sicherheitskritischer Eingaben (zum Beispiel ein Passwort) oder Ausgaben (zum Beispiel Prüfen eines Dokuments) zu sichern. Außerdem werden die Nutzer-Input- und -Output-Geräte (Maus, Tastatur, Grafikkarte, ...) verwaltet. Sie stellt einen sicheren Pfad (trusted path) von der Tastatur-Eingabe bis in die Anwendung sicher, sodass keine Eingaben umgeleitet oder abgefangen werden können.

- **Trusted Network**

Der Dienst „Trusted Network“ wird auch als Trusted Network Connect (TNC) bezeichnet. Er stellt ein vertrauenswürdiges Interface zur Verfügung, das Netzwerkkomponenten prüft und gegebenenfalls die Verbindung verhindert.

- **Crypto/TSS**

Er bildet die zentrale Anlaufstelle für alle Anwendungen, die Funktionen aus der TSS benötigen.

- **Installer**

Der „Installer“ stellt den Loader des IT-Systems dar. Er installiert und startet Dienste aus der TCB oder auch Anwendungen der Nutzer, verwaltet alle laufenden Prozesse und liefert eine vertrauenswürdige Instanz, um Prozesse zu identifizieren.

- **User Auth**

Dies bildet die Nutzerverwaltung für die Nutzer des IT-Systems und stellt diesen Dienst anderen Anwendungen zur Verfügung. Anwendungen können mit diesem Dienst eine Nutzer-Authentifikation anstoßen. Es wird ermöglicht, dass Daten an einen Nutzer gebunden werden.

- **Policy Management**

Dieser Dienst sorgt dafür, dass Regeln durchgesetzt werden. Daten, die nur nach einer bestimmten Regel verarbeitet werden dürfen, sind an das Policy Management verschlüsselt gebunden. Bevor diese Daten verarbeitet werden können, wird die Regel von Policy Management geprüft.

### Anwendungsebene

Oberhalb der Sicherheitsebene können sicherheitskritische und sicherheitsunkritische Anwendungen parallel ausgeführt werden. Herkömmliche Betriebssysteme können als eigenständige Anwendungen auf der Sicherheitsebene laufen, um einen Nutzer die ihm bekannte Schnittstelle zu bieten und eine nach unten kompatible binäre Anwendungsschnittstelle (Application Binary Interface, ABI) bereitzustellen. Der Nutzer kann also auch herkömmliche unkritische Anwendungen und Komponenten weiter verwenden. Beispiele sind:

- **Trusted Viewer**

Der „Trusted Viewer“ stellt nach dem What-you-see-is-what-you-get-Prinzip einen vertrauenswürdigen Dokumenten-Viewer bereit. Anwendungen können Dokumente so ablegen, dass nur der Trusted Viewer in der Lage ist, diese zu öffnen und darzustellen. Ausgaben, die über den Trusted Viewer dargestellt werden, können nicht von anderen Anwendungen überlagert und manipuliert werden.

- **Device Encryption (HDD Encryption)**

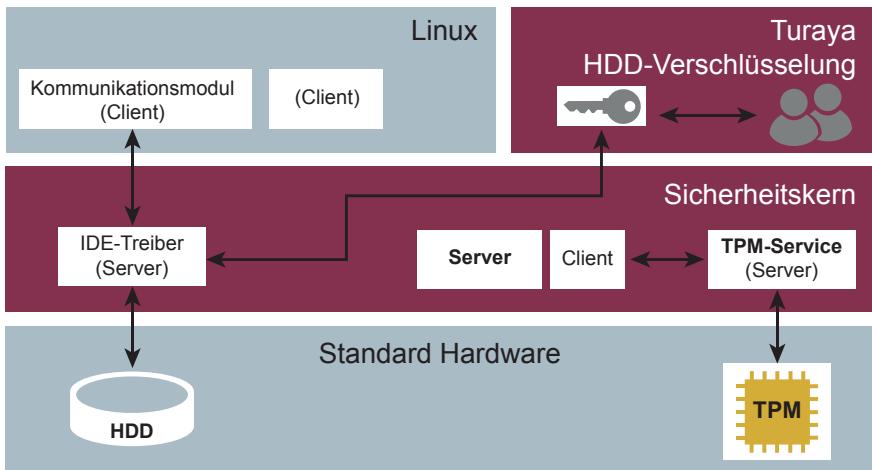
Mit der Device Encryption können blockorientierte Geräte (Festplatte, Memory Sticks, CD/DVD-Medien) verschlüsselt werden. Die Device Encryption ist nach der Konfiguration transparent für den Anwender.

#### 7.3.7 Beispielanwendungen

Auf der Basis der Sicherheitsplattform Turaya werden Beispielanwendungen dargestellt, die aufzeigen sollen, wie groß die Nutzungsmöglichkeiten einer Sicherheitsplattform sind [5].

##### Turaya.Crypt

Eine erste Beispielanwendung ist „Turaya.Crypt“, die eine Festplattenverschlüsselung bietet, die auf der Basis von Trusted Computing läuft. Diese Festplattenverschlüsselung stellt exemplarisch die Möglichkeiten vor, wie Sealings umgesetzt werden können. Daten können direkt mit einer vertrauenswürdigen Systemkonfiguration verbunden werden, um somit nur bei einem per Definition vertrauenswürdigen IT-System verwendet werden zu können.



**Abb. 7.11** Architekturbild Turaya.Crypt

Ziel von Turaya.Crypt ist der Schutz des geheimen Schlüssels, der benötigt wird, um eine verschlüsselte Festplatte oder ein anderes Gerät (Device) wieder entschlüsseln zu können.

Im Linux Compartiment wird durch Nutzerinteraktion die Entschlüsselung einer verschlüsselten Festplatte angestoßen, siehe Abb. 7.11.

Hierzu wird ein spezielles Kernel-Modul geladen, das die Kommunikation über den Sicherheitskern zur Turaya-Festplattenverschlüsselung herstellt. Durch die Nutzung der TrustedGUI, einer vertrauenswürdigen Oberfläche auf Basis der Sicherheitsplattform, erfolgt eine vertrauenswürdige Nutzerauthentifikation. Das eingegebene Passwort ist geschützt, da es nur innerhalb der Sicherheitsplattform verarbeitet wird, sodass die Informationen nicht in das Linux Compartiment gelangen können.

Nach einer erfolgreichen Authentifizierung des Nutzers wird der geheime Schlüssel freigegeben, um die verschlüsselte Festplatte entschlüsseln zu können. Durch die strenge Isolation der einzelnen Compartments bedeutet eine Kompro-mittierung des Linux Compartiments keine Gefahr für den geheimen Schlüssel. Dies gilt nicht für die Inhalte der Daten, da diese nach der Entschlüsselung im Linux Compartiment verfügbar sind. Um den Schutz auf die Daten auszuweiten, wäre es möglich, diese Beispielanwendung dahin gehend zu erweitern, dass ein weiteres Compartiment gestartet wird, die ausschließlich die entschlüsselten Daten erhält. Dort werden die Daten vertrauenswürdig und integer angezeigt beziehungsweise bearbeitet. Ein solches Compartiment wird auch als TrustedViewer oder TrustedEditor bezeichnet.

Als verschlüsseltes Gerät kommen Festplatten/Partitionen, USB-Speicher, CDR/DVD-Medien oder Dateicontainer infrage.

### Turaya.VPN

Die zweite Beispieldienst „Turaya.VPN“ bietet die Möglichkeit, Netzwerkaktivitäten zu steuern, Zertifikate, die hiermit verbunden sind, zu schützen und Automatismen für transparente Sicherheit anzubieten. Das Client-Server-Szenario wird in dieser Pilotanwendung umgesetzt. Um eine vertrauenswürdige Kommunikation herzustellen, müssen der Netzwerkverkehr kontrolliert und sicherheitsrelevante Daten, wie Zertifikate oder Verbindungsdaten vom herkömmlichen Betriebssystem getrennt werden. Die hier verwendete Technologie bietet große Vorteile für sichere Netzwerkverbindungen.

Auf technischer Seite wird diese Pilotanwendung folgendermaßen realisiert:

Ziel von Turaya.VPN ist, wie bei Turaya.Crypt, der Schutz des geheimen Schlüssels in einer unsicheren IT-Systemumgebung. Der Unterschied zu Turaya.Crypt ist, dass der geheime Schlüssel verwendet wird, um einen VPN-Tunnel für die gesicherte Kommunikation aufzubauen. Eine weitere Eigenschaft von Turaya.VPN ist die Kontrolle des gesamten Netzwerkverkehrs. Im Folgenden wird das EMSCB VPN/Firewall Compartment als Turaya.VPN bezeichnet, siehe Abb. 7.12.

Turaya.VPN stellt die physikalische Verbindung zur Netzwerkkarte her und verwaltet diese. Jedes Compartment, das über einen Netzwerkzugang verfügen soll, muss sich über Turaya.VPN für diesen Dienst anmelden und autorisieren. Der gesamte Netzwerkverkehr läuft dabei, transparent für die Nutzer, über Turaya.VPN. Hier können zentral Dienste ausgeführt werden: Unter anderem eine Anonymisierung des Datentransfers, eine Firewall oder ein Malwarescanner.

Hauptaufgabe von Turaya.VPN ist der für den Nutzer transparente Aufbau eines VPN-Tunnels, sobald der Nutzer ein spezielles Ziel aufruft. Die Authentifizierung des Nutzers wird durch die TrustedGUI vom herkömmlichen Betriebssystem isoliert. Durch den TrustedPath, einer abgesicherten Kommunikation zwischen Nutzer und Turaya, wird sichergestellt, dass die Eingabe der Authentifizierungsdaten nur an die dafür zuständige Instanz gelangt.

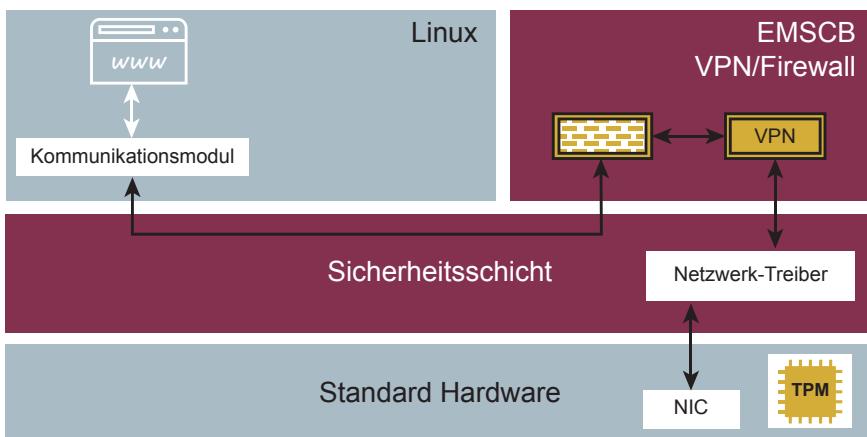
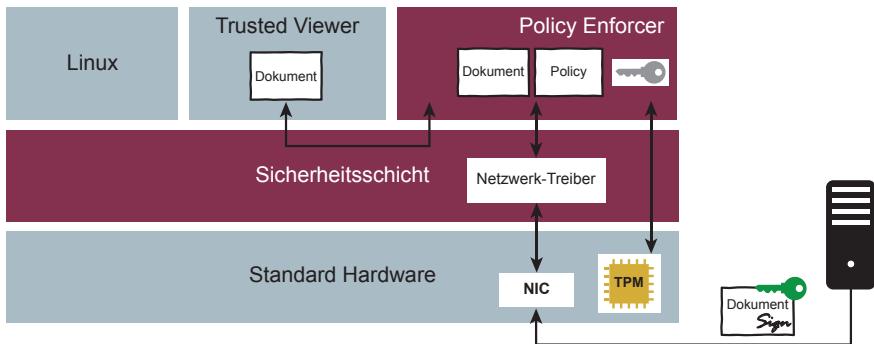


Abb. 7.12 Architekturbild Turaya.VPN



**Abb. 7.13** Architekturbild Turaya.FairDRM

### Turaya.FairDRM

Die ersten zwei Pilotanwendungen zeigen, wie Daten auf einem IT-System vertrauenswürdig gespeichert werden können und wie eine Kommunikation zwischen IT-Systemen vertrauenswürdig geschützt werden kann. Die Pilotanwendungen 3 und 4 stellen vor allem den Schutz von Inhalten sicher. Die dritte Pilotanwendung „Turaya.FairDRM“ legt die Grundlage für den Umgang mit Daten, denen Regeln und Rechte zugewiesen werden können. Es werden Audiodaten mit Regeln versehen, die den Inhalt an eine IT-Systemplattform binden – unter Berücksichtigung der Interessen aller beteiligten Parteien. Auch klassische Mankos von Digital Rights Management-Systemen werden berücksichtigt. So ist der Transfer einer Lizenz auf ein anderes IT-System möglich.

Auf technischer Seite wird diese Pilotanwendung folgendermaßen realisiert:

Turaya.FairDRM besteht aus zwei Compartments: Das Policy Enforcer Compartment bildet die vertrauenswürdige Instanz, die in der Lage ist, das verschlüsselte DRM-Objekt zu entschlüsseln und die entsprechenden Regeln durchzusetzen, siehe Abb. 7.13.

Entsprechen die Regeln der aktuellen Situation, so werden die entschlüsselten Daten an den TrustedViewer übertragen, der diese darstellt.

Der Ablauf des Turaya.FairDRM-Piloten sieht wie folgt aus:

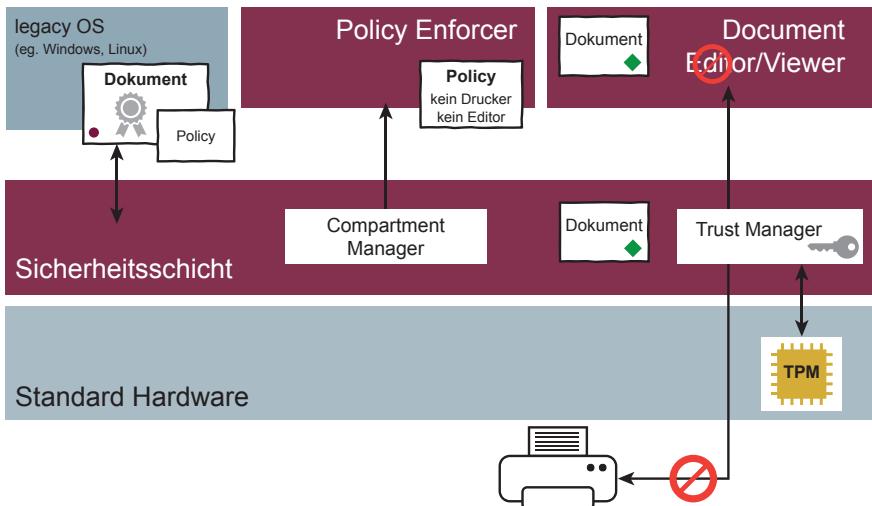
- Der Informationsanbieter sendet eine Auswahl an Media-Daten an den Nutzer. In dem Piloten geschieht dies über eine HTML-Seite.
- Der Nutzer wählt ein Lizenzmodell und eine Media-Datei aus.
- Der Nutzer erstellt ein Zertifikat, das den öffentlichen Schlüssel des TPMs und die aktuelle Konfiguration der Sicherheitsplattform Turaya zertifiziert.

- Zertifikat und ausgewähltes Lizenzmodell werden zusammen mit der Anforderung der Media-Datei an den Informationsanbieter gesendet.
- Der Informationsanbieter prüft das Zertifikat. Vertraut der Informationsanbieter dem Zertifikat und stimmt er dem ausgewählten Lizenzmodell zu, wird die Media-Datei für den Nutzer verschlüsselt und an ihn gesendet.
- Die Sicherheitsplattform Turaya nimmt die verschlüsselte Media-Datei in Empfang (per E-Mail oder Download).
- Solange sich die Konfiguration der Sicherheitsplattform Turaya nicht ändert, ist es nun möglich, die Media-Datei über den TrustedViewer vertrauenswürdig darzustellen.

### Turaya.ERM

Aufbauend auf dem dritten Piloten wird im vierten Piloten ein Enterprise-Rights-Management-System aufgesetzt, das den Umgang mit Inhalten innerhalb eines Firmenumfeldes absichern soll. Das Vorhaben bietet somit die Möglichkeit, Dokumente nur für bestimmte Personen beziehungsweise IT-Systeme lesbar und verwertbar zu machen. Beispielsweise darf ein Dokument auf einem anderen IT-System angezeigt, aber nicht gedruckt werden, da das IT-System nicht die erforderliche Vertrauenswürdigkeit besitzt oder kein privilegierter Nutzer an das IT-System gemeldet ist. Auch hier wird das multilaterale Konzept verfolgt, das beinhaltet, dass alle Beteiligten mit den Regeln und Rechten, die einem Vorgang zugeordnet sind, konform gehen müssen.

Als zusätzliches Element ist ein Policy-Manager beziehungsweise Policy-Enforcer notwendig, der die Rechte auf der einen Seite einem Dokument hinzufügt und auf der anderen Seite die Rechte durchsetzt. Dieser Pilot findet vor allem eine große Anwendung in der Unternehmenskommunikation, sowohl intern als auch extern. Ein typisches Beispiel bieten die bereits angesprochenen „Supply Chains“, wie sie in der Automobil- und Luftfahrtindustrie üblich sind. Die beteiligten Firmen haben jeweils Zugriff auf die IT-Systeme des Partners. Die Zugriffe finden teilweise automatisiert und zwischen einer Vielzahl von IT-Systemen statt. Die Absicherung eines solchen Konstrukts ist nur durch die Integritätsprüfung der Geräte möglich. Firmen tauschen Entwürfe neuer Produkte aus, die im Falle eines Verlusts zu Schäden in Millionenhöhe führen können. Die Sicherheitskonzepte in diesem Umfeld sind nicht in ausreichendem Maße vertrauenswürdig. Mit einer Sicherheitsplattform kann die falsche Verwendung von Inhalten minimiert werden. Die Technologie ermöglicht eine sichere Kommunikation, eine sichere Anzeige (Trusted Viewer) und durch die Integritätsprüfung aller beteiligten IT-Systeme einen vertrauenswürdigen Zustand, siehe Abb. 7.14.



**Abb. 7.14** Architekturbild Turaya.ERM

## 7.4 Trusted Network Connect (TNC)

Da die im Netz befindlichen IT-Systeme nicht auf ihre Systemintegrität und somit ihre Vertrauenswürdigkeit geprüft werden können, ist eine vertrauenswürdige Kommunikation nur bedingt möglich. Besucher oder Außendienstmitarbeiter, die ihre IT-Systeme sowohl außerhalb als auch innerhalb eines zu schützenden Unternehmensnetzes einsetzen, können eine Bedrohung für das Unternehmen darstellen. Durch die Nutzung der IT-Systeme außerhalb des Unternehmensnetzes arbeiten diese auch außerhalb der Schutzmaßnahmen und des Kontrollbereichs der Unternehmens-IT [6]. Diese Lücke wollen Lösungs-Ansätze – wie zum Beispiel Trusted Network Connect (TNC) – durch die Messung der Integrität von Endpunkten schließen. Die Konfigurationen der Endpunkte lassen sich sowohl auf Software- als auch auf Hardwareebene messen und über den Abgleich von definierten Sicherheitsregeln lässt sich eine policygesteuerte Zugriffssteuerung realisieren. Erst durch die Feststellung der Integrität eines IT-Systems ist eine vertrauenswürdige Kommunikation möglich.

### 7.4.1 Problemstellung

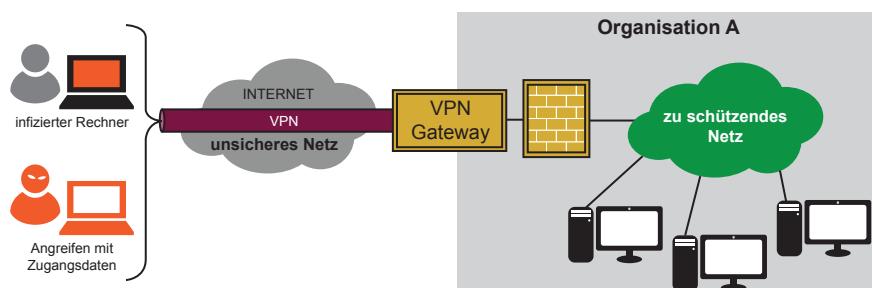
Außendienstmitarbeiter nutzen ihre IT-Systeme in vielen Umgebungen mit unterschiedlichen Cyber-Sicherheitsmechanismen und unterschiedlichem Cyber-Sicherheitsanforderungen. Heimarbeiter verwenden ihre PCs, Notebooks, Smartphones meist auch für private Zwecke. Mitarbeiter nehmen immer häufiger ihre Notebooks mit nach Hause. Durch die zeitweilige oder dauerhafte Auslagerung von

IT-Systemen außerhalb des Unternehmensnetzes, und somit auch außerhalb der lokalen Schutzmaßnahmen, sind diese IT-Systeme weiteren Gefahren ausgesetzt. Kommt es zu einer Kompromittierung durch Malware, erfolgt durch die Reintegration in das Unternehmensnetz (direkt oder über das Internet) eine Umgehung der unternehmenseigenen Cyber-Sicherheitsmechanismen.

Zur sicheren Integration von Heim- und Außendienstmitarbeitern über öffentliche, unsichere Netzwerke werden heute meist Virtual Private Networks (VPNs) in Form von Software-Clients genutzt. Aber auch Verbindungen von ganzen Netzwerken laufen über VPNs, hier in Form von VPN-Gateways an den Zugangspunkten der Netzwerke zum Internet. Die VPN-Technologien setzen meistens auf eine Nutzer-Authentifikation sowie eine verschlüsselte und integritätsge-sicherte Datenübertragung (siehe auch Kap. 10 „IPSec“ und Kap. 11 „TLS/SSL“). Sie bieten aber keine Prüfung der Systemintegrität der zugreifenden IT-Systeme. Deshalb ist keine Aussage über die Vertrauenswürdigkeit der zugreifenden IT-Systeme möglich, was ein Cyber-Sicherheitsrisiko darstellt.

Netzwerkverbindungen über VPNs bieten an ihren Zugangspunkten keinen Schutz vor Angriffen durch die zugreifenden IT-Systeme. Abb. 7.15 zeigt zwei mögliche Gefährdungen eines Netzwerks durch die Nutzung einer durch VPN abgesicherten Kommunikationsverbindung.

- Zum einen ist kein Schutz des zu schützenden Netzes mit seinen angeschlossenen IT-Systemen und Diensten vor einem durch **Malware kompromittierten IT-System** möglich, da eine Überprüfung der Integrität des IT-Systems fehlt.
- Zum anderen kann nicht festgestellt werden, dass das IT-System, mit dem kommuniziert wird, auch wirklich das IT-System ist, das es vorgibt zu sein. Gelangt ein Angreifer an Zugangsdaten eines VPNs, so kann er diese für einen **unberechtigten Zugriff** nutzen.



**Abb. 7.15** Weitere Gefährdungen trotz VPN

### 7.4.2 Anforderungen an heutige Netzwerke

Die Anforderungen an heutige und zukünftige Netzwerke sind vielfältig. Neben Flexibilität in Konfiguration und räumlicher Ausdehnung sollen sie so sicher sein, dass über eine vertrauenswürdige Kommunikation sicherheitskritische Anwendungen stattfinden können.

Wie in der Problemstellung erläutert, bieten Technologien wie VPNs schon heute einen gesicherten Transport von Daten, sowie eine Möglichkeit, Netzwerke flexibel zu erweitern. Sie bieten aber keine Cyber-Sicherheitsmechanismen, die die Vertrauenswürdigkeit der Nutzer von IT-Systemen gewährleisten können.

Ziel neuer Cyber-Sicherheitssysteme muss die Überprüfbarkeit der Vertrauenswürdigkeit der beteiligten IT-Systeme und die Herstellung sicherer Kommunikation sein. Es müssen neben den bekannten Angriffen auf Netzwerke (Netzkomponenten und Leitungen) auch die Angriffe über mit Malware kompromittierte IT-Systeme sowie Angriffe durch Dritte mittels gestohlener Zugangsdaten verhindert werden!

### 7.4.3 Vertrauenswürdige Netzwerkverbindungen

Da vertrauenswürdige Netzverbindungen eine wichtige Voraussetzung sind, werden die Randbedingungen im Folgenden erläutert.

#### Definition: Vertrauenswürdige Kommunikation

Eine Kommunikation kann erst als vertrauenswürdig angesehen werden, wenn die Vertrauenswürdigkeit aller beteiligten Kommunikationspartner gegeben ist. Dabei gilt zu beachten, dass die Vertrauenswürdigkeit für jede Kommunikationsrichtung getrennt betrachtet werden muss. Das heißt, dass mit einem Kommunikationspartner, dem vertraut wird, ein vertrauliches Gespräch geführt werden kann, ohne dass das Gegenüber einem dieses Vertrauen selbst entgegenbringt. Zusätzlich zur persönlichen Vertrauenswürdigkeit muss auch das Umfeld, in dem die Kommunikation stattfindet, vertrauenswürdig sein. Findet die Kommunikation an einem bestimmten Ort statt, so muss der Ort als vertrauenswürdig eingestuft werden, also zum Beispiel frei von Abhöreinrichtungen sein. Findet die Kommunikation über eine größere Distanz statt, so muss der Übertragungsweg, beispielsweise ein Postdienst mit all seinen Mitarbeitern und Räumlichkeiten, vertrauenswürdig sein. Die Anforderungen, die ein Kommunikationspartner an eine vertrauenswürdige Kommunikation stellt, legt er in einer Policy fest. In dieser Policy könnte definiert sein, welchen Botendienst er für vertrauenswürdig hält und wie die Lieferung verpackt sein muss, um kompromittierte Sendungen feststellen zu können.

## Vertrauenswürdigkeit bei Netzwerkverbindungen

Bei einer Kommunikation über unsichere Netzwerke müssen alle an der Kommunikation beteiligten Nutzer und IT-Systeme vertrauenswürdig sein. Dabei handelt es sich neben den beteiligten Nutzern und den eingesetzten IT-Systemen (Endpunkte) auch um sämtliche Netzelemente wie Hubs, Switches, Router und Firewall-Systeme.

Die Vertrauenswürdigkeit eines IT-Systems beziehungsweise Netzelements ist hauptsächlich von seiner Integrität abhängig. Das bedeutet, dass ein Endpunkt nur vertrauenswürdig sein kann, wenn alle Systemkomponenten, das heißt, Hard- und Software (vorhandene Einstekkkarten, Betriebssystem, Anwendungen usw.), in einem unverfälschten und nicht-kompromittierten Zustand sind. Das Problem dabei ist, dass heutzutage eine Kompromittierung nicht direkt, sondern nur indirekt über weitere Software verhindert wird und messbar ist. Dies geschieht zum Beispiel durch die Nutzung einer aktuellen Anti-Malwarelösung und einer Personal-Firewall. Nur solange diese Programme installiert sind und einen aktuellen Datenstand aufweisen, kann die Wahrscheinlichkeit einer Kompromittierung als gering betrachtet werden.

Dabei muss bedacht werden, dass eine vorhandene Integrität keinen standardisierten Zustand eines IT-Systems darstellt. Vielmehr ist die Integrität von den Sicherheitsrichtlinien (Policys) der Kommunikationspartner abhängig. So kann ein Betreiber eines Netzwerkes die Integrität eines IT-Systems durch die Nutzung eines aktuellen Betriebssystems und definierten Anwendungen als bewiesen ansehen, während ein anderer Betreiber zum Beweis der Integrität eine zusätzliche installierte Anti-Malware-Lösung, Personal Firewall usw. verlangt.

Genau hier setzen die neuen Konzepte zur Etablierung vertrauenswürdiger Netzwerkverbindungen an. Sie ermöglichen eine Überprüfung der Konfiguration der Endpunkte schon beim Aufbau einer Netzwerkverbindung. Welche Konfigurationen aus Hard- und Software in einem Netzwerk erlaubt sind, kann vom Netzbetreiber über Policys festgelegt werden. Nur bei Erfüllung der Policys wird einem anfragenden Endgerät ein Zugriff auf das Netzwerk mit seinen Diensten gewährt.

Bei diesen neuen Sicherheitskonzepten kann von einem Wechsel der Schutz-Strategie von Netzwerken und deren Dienste gesprochen werden. Durch die Überprüfung der IT-Systeme **vor** dem Netzzugriff findet ein Wechsel von der Gefahren-Reaktion hin zur Prävention statt. Während heute mit Intrusion-Detection-Systemen (IDS) versucht wird, anhand von abnormalen Messwerten im Netzwerkverkehr kompromittierte IT-Systeme zu erkennen (Reaktion), verhindern die präventiven Sicherheitskonzepte, dass IT-Systeme mit einer fehlerhaften oder unerwünschten Systemkonfiguration und somit einer eventuellen Kompromittierung überhaupt in das Netz gelangen und die dort vorhandenen Dienste nutzen können.

## Umsetzungen

Es existieren mehrere Ansätze, die eine Integritätsprüfung zur Erhöhung der Vertrauenswürdigkeit bieten. Die wohl wichtigsten Vertreter sind Trusted Network Connect (TNC), Microsoft NAP und Cisco NAC.

Mit der Trusted Network Connect-Spezifikation (TNC) entwickelt die Trusted Computing Group einen Ansatz zur Realisierung vertrauenswürdiger Netzwerkverbindungen. Die Entwicklung findet durch die Trusted Network Connect-Subgroup statt. Ziel ist die Entwicklung einer offenen, herstellerunabhängigen Spezifikation zur Überprüfung der Endpunkt-Integrität. Dieser Ansatz wird im Folgenden genauer beschrieben. Die Firma Microsoft entwickelt mit der „Microsoft Network Access Protection“ (Microsoft NAP) eine Lösung einer policybasierten Zugriffssteuerung. Cisco Network Admission Control (Cisco NAC) ist Teil der „Self-Defending Network“-Strategie und gehört ebenfalls zu den policybasierten Zugriffssteuerungen.

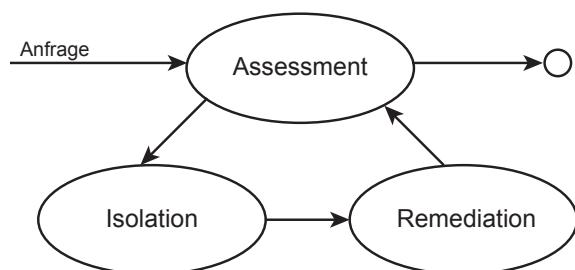
### 7.4.4 Trusted Network Connect (TNC) im Detail

Die durch die Trusted Computing Group vorangetriebene Trusted Network Connect-Spezifikation (TNC) soll als offene und herstellerunabhängige Spezifikation die Realisierung von vertrauenswürdigen Netzwerkverbindungen ermöglichen. TNC versucht dabei nicht, vorhandene Sicherheitstechnologien zu ersetzen, sondern auf diese aufzusetzen. So werden beispielsweise Sicherheitstechnologien für den Netzwerzkzugriff („802.1x“ und „VPN“), für den Nachrichtentransport („EAP“, „TLS“ und „HTTPS“) und für die Authentifizierung („Radius“ und „Diameter“) unterstützt. Durch diese Eigenschaften soll sich TNC leicht in bestehende Netzinfrastrukturen integrieren lassen.

#### Phasen

Alle durch TNC bereitgestellten Funktionen lassen sich in drei Phasen einordnen, siehe Abb. 7.16.

**Abb. 7.16** Zusammenhang der Phasen von TNC



### Assessment-Phase

Die Assessment-Phase umfasst alle Aktionen vom Versuch eines Verbindungsauftaus zu einem TNC-geschützten Netzwerk bis zur Entscheidung über dessen Vertrauenswürdigkeit.

In dieser Phase werden Messwerte vom IT-System an einen Server im Netzwerk gesendet und dort anhand von Policies verglichen. Durch diesen Vergleich ist eine Entscheidung über die Vertrauenswürdigkeit möglich.

### Isolation-Phase

Wird das IT-System, bei Nichterfüllung der Policies, als nicht-vertrauenswürdig eingestuft, gelangt es in die Isolation-Phase. In dieser Phase wird das zugreifende IT-System in einen geschützten Netzwerkbereich isoliert, der vom restlichen Netz abgeschottet ist. Eventuell mit Malware kompromittierte IT-Systeme oder IT-Systeme von Angreifern erlangen so keinen Zugriff auf das Netzwerk und die dort angebotenen Dienste.

### Remediation-Phase

Die Remediation-Phase bietet den isolierten IT-Systemen die Möglichkeit, ihre Integrität, zum Beispiel über die Installation fehlender Sicherheitssoftware, wiederherzustellen, und nach einer erneuten Überprüfung Zugriff auf das Netzwerk mit seinen angebotenen Dienste zu erlangen.

Sowohl die Isolation- als auch die Remediation-Phase sind durch die TNC-Spezifikation nicht vorgeschrieben und müssen somit nicht zwangsläufig implementiert werden.

### Struktur

Grundsätzlich wird in der TNC-Spezifikation zwischen drei Elementen unterschieden, siehe Abb. 7.17.

Das IT-System, mit dem eine Netzwerkverbindung zu einem TNC-Netzwerk aufgebaut werden soll, wird Access Requestor (AR) genannt. Auf dem Access Requestor befinden sich TNC-Komponenten für Verbindungsanfrage, Messwertermittlung und Messwertübermittlung.

Die Messung der einzelnen Komponenten des IT-Systems findet durch sogenannte „Integrity Measurement Collectors“ (IMC) statt. Für jede zu messende sicherheitsrelevante Komponente oder Cyber-Sicherheitslösung existiert dabei ein passender IMC, beispielsweise einer für das installierte Betriebssystem und SW-Anwendungen, für die installierte Hardware, Anti-Malwarelösung und einer für die Personal-Firewall, siehe Abb. 7.17. Zum Systemstart werden die IMCs vom TNC-Client auf dem zugreifenden IT-System initialisiert, um bei einem Verbindungsauftaus Messwerte von den jeweiligen Komponenten sammeln zu können. Die Art der möglichen Messwerte ist dabei zunächst nicht begrenzt. Bei einer Anti-Malware-Lösung können zum Beispiel Informationen über Hersteller und Alter der Malware-Signatur wichtig sein, bei einem angeschlossenen Drucker die Version der Firmware.

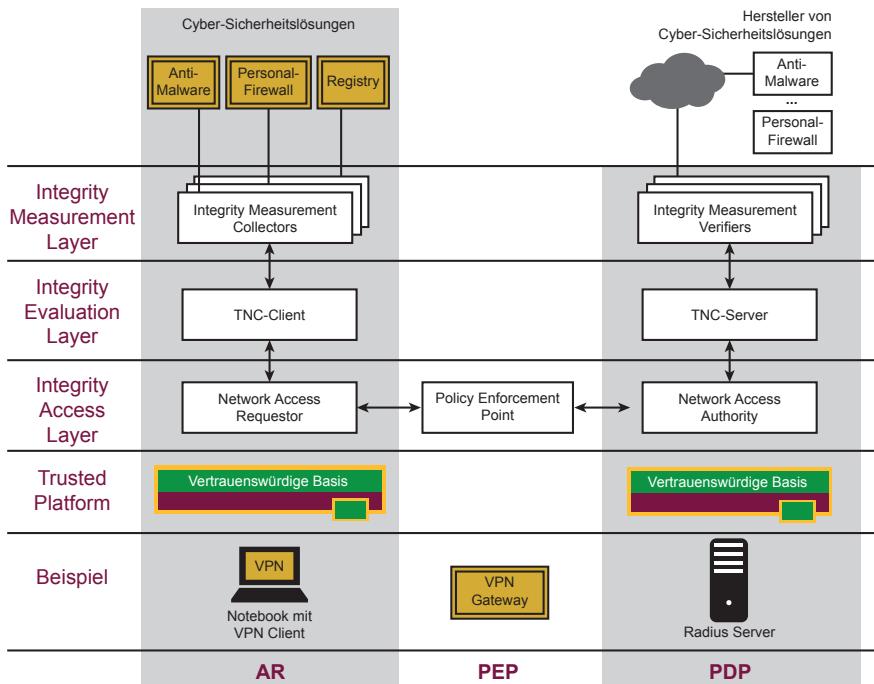


Abb. 7.17 Struktur von TNC

Auf Seiten des Netzwerks existieren zwei TNC-Elemente:

Der Policy Decision Point (PDP) stellt die Gegenseite zum Access Requestor (AR) dar. Es handelt sich dabei um einen Server, der die Aufgabe hat, die Messwerte eines Access Requestors zu sammeln und mithilfe von Policies eine Zugriffsentscheidung zu formulieren. Diese Entscheidung wird anschließend der ausführenden Stelle für den Zugriff mitgeteilt.

Die Network Access Authority (NAA) im Policy Decision Point entscheidet, ob ein AR-Zugriff bekommen soll oder nicht. Dazu fragt der NAA den TNC-Server, ob die Integritätsmessungen des ARs mit der Security Policy übereinstimmen.

Auf dem PDP stellen sogenannte „Integrity Measurement Verifier“ (IMV) das Gegenstück zu den IMCs des AR dar. Auch hier existieren mehrere IMVs für die unterschiedlichen Aspekte und Cyber-Sicherheitskomponenten und Cyber-Sicherheitslösungen. Für jeden zu überprüfenden Aspekt und jede Cyber-Sicherheitskomponente muss es, neben dem IMC, auch einen passenden IMV geben, siehe Abb. 7.17.

Damit ein IMC die richtigen Messwerte sammeln kann, bedarf es einer sehr genauen Kenntnis der zu messenden Hardware/Software. Diese Kenntnis besitzt meist nur der Hersteller von Hardware beziehungsweise Software. Daher ist eine direkte Verbindung zum Hersteller eines IMC sehr hilfreich.

Die IMVs vergleichen die übermittelten Messwerte anhand der in den Policy's festgelegten Regeln und teilen ihr Ergebnis dem TNC-Server im PDP mit. Dieser kann mit diesen Teilergebnissen eine Entscheidung über den Zugriff auf das Netzwerk mit seinen Diensten treffen und diese Gesamtentscheidung dem Policy Enforcement Point über die Network Access Authority (NAA) mitteilen.

Der Policy Enforcement Point (PEP) ist das TNC-Element am Eintrittspunkt des Netzes. Seine Aufgaben sind die Entgegennahme und Weiterleitung von Verbindungsanfragen sowie die Ausführung der Handlungsentscheidung des PDPs.

Der PEP stellt als Eintrittspunkt den zuerst zu adressierenden Verbindungs-  
punkt des Netzwerkes dar. Ankommende Verbindungsanfragen eines AR werden  
direkt an den PDP weitergeleitet. Nachdem ein PDP seine Entscheidung über die  
Vertrauenswürdigkeit des AR getroffen hat, teilt er diese dem PDP mit, der gemäß  
dieser Entscheidung handeln muss.

Ein PEP kann laut TNC-Spezifikation sowohl ein eigenständiges IT-System als  
auch in den PDP oder in ein anderes Netzwerk-Equipment integriert sein. Dadurch  
wird es möglich, den PEP zum Beispiel flexibel direkt in ein VPN-Gateway zu  
integrieren oder, um vorhandene Netzwerkstrukturen unberührt zu lassen, vor  
beziehungsweise hinter diesem Gateway zu platzieren.

Wenn AR und PDP auf einer vertrauenswürdigen Basis arbeiten, kann den  
gemessenen Messwerten eine höhere Echtheit zugesprochen werden, weil diese  
nicht manipuliert werden können. Damit wird der Lying Endpoint-Problematik  
entgegengewirkt.

#### 7.4.5 Anwendungsfelder

Trusted Network Connect soll möglichst flexibel bei vielen Anwendungen zum Einsatz kommen können, weshalb die Spezifikation sehr allgemein gehalten ist. Zwischen den vielfältigen Anwendungsfeldern stechen zwei klassische Einsatzgebiete heraus, die hier genauer betrachtet werden.

##### Schutz des Unternehmensnetzes

TNC kann den Schutz des zu schützenden Netzes vor Angriffen von außen erhöhen. Heimarbeiter und insbesondere Außendienstmitarbeiter, die sich in ständig wechselnden Sicherheitsumfeldern aufhalten, wählen sich heute, zwecks Datenzugriff, meist über VPNs in das eigene Unternehmensnetz ein. Wurde ein IT-System eines Außendienstmitarbeiters kompromittiert, so stellt ein Zugriff über das VPN eine Umgehung der Cyber-Sicherheitsmaßnahmen, beispielsweise einer Firewall, des Firmennetzes dar. Die Malware auf dem kompromittierten IT-System erhält Zugriff auf das Firmennetz und die darin angeschlossenen weiteren IT-Systeme.

Durch eine Erweiterung des VPN-Zugriffs mit TNC-Funktionalität lässt sich die Integrität der IT-Systeme vor dem Zugriff auf das Netzwerk mit seinen Diensten überprüfen, um diesen gegebenenfalls, also bei Nichterfüllung der Sicherheitspolicy, zu unterbinden. Durch die Nutzung der TPM-Funktionen ist es sogar

möglich, einen VPN-Zugang an bestimmte IT-Systeme zu binden, um etwa einen Zugriff mittels gestohlener Zugangsdaten zu verhindern.

### Direkter Schutz des Intranets

Neben dem Einsatz zum Schutz vor Angriffen von außen lässt sich TNC auch zum Schutz vor Angriffen von innen einsetzen. Durch die Ausstattung aller IT-Systeme im zu schützenden Netz mit TNC-Funktionen können Angriffe von innen präventiv abgewendet werden. So können zum Beispiel IT-Systeme von Gästen zuverlässig auf ihre Integrität geprüft werden, bevor sie einen Zugang erlangen.

### Weitere Einsatzfelder

Neben diesen klassischen Einsatzgebieten lässt sich TNC noch viel spezieller einsetzen. Aufgrund der offenen Spezifikation lassen sich auch VPN-Gateways als Endpunkt ansehen. So wird eine sichere Anbindung von Niederlassungen an ein Unternehmensnetz mittels TNC-Mechanismen ermöglicht.

Es ist auch denkbar, dass Diensteanbieter im Internet, zum Beispiel Banken, von ihren Kunden verlangen, eine aktuelle Anti-Malwarelösung sowie eine Personal-Firewall installiert zu haben, um weder den Kunden selbst, noch die angebotenen Dienste zu gefährden.

## 7.4.6 Kritische Diskussion

Im Folgenden werden sowohl einige Aspekte von TNC, wie die Vertrauenswürdigkeit der erfassten Messwerte, die Administration und die Cyber-Sicherheit, als auch die vorgestellten Lösungen im Allgemeinen, wie die Kompatibilität untereinander, kritisch diskutiert.

### Vertrauenswürdigkeit der Messwerte

Die Sicherheit von TNC ist abhängig von der Vertrauenswürdigkeit der Messwerte. Diese müssen korrekt gemessen und unverfälscht an den TNC-Server übermittelt werden können.

Da bei heutigen IT-Systemen keine Möglichkeit besteht, eine korrekte und unverfälschte Messung sowie Übertragung der ermittelten Daten zu garantieren, führt dies zwangsläufig zu einem Paradoxon. Wurden die Hardware oder das Betriebssystem eines IT-Systems kompromittiert, müssen auch die Messwerte als nicht mehr vertrauenswürdig angesehen werden, da diese durch die Malware jederzeit beeinflusst werden können. Da die Messwerte aber zur Entdeckung von fehlender Integrität, und somit eventueller Kompromittierung, genutzt werden sollen, entsteht durch die ständige Gefahr der unbemerkten Fälschung ein dauerhaftes Misstrauen gegenüber den Messwerten.

Die TNC-Spezifikation bietet durch seine optionale und direkte Unterstützung des Trusted Platform Moduls (TPM) grundsätzlich die Möglichkeit, in Verbindung mit einer Sicherheitsplattform Manipulationen der Hardware und Software zu verhindern und die Übertragung der Messwerte durch Signierung vor

Manipulationen zu schützen. Solange aber die Betriebssysteme, die zur Messung genutzt werden, keine vertrauenswürdige Ermittlung der Messwerte ermöglichen, bleibt die erreichte Sicherheit aber weiterhin begrenzt. Erst mit Einführung von geeigneten Sicherheitsplattformen, wie zum Beispiel der Turaya-Sicherheitsplattform des EMSCB-Projektes [7], lassen sich auch die Messwerte aller Sicherheitskomponenten vertrauenswürdig ermitteln.

Dieses Problem ist aber nicht als spezifisches Problem von TNC und ähnlichen Ansätzen zu sehen, sondern als Gesamtproblem heutiger IT-Systeme, das durch die zukünftige Nutzung von Sicherheitsplattformen, die auf Trusted Computing aufbauen, gelöst werden kann.

## Administration

Wie viele Cyber-Sicherheitstechnologien verursachen auch policybasierte Ansätze einen erhöhten Administrationsaufwand vor und während des Betriebs eines Netzwerks. Für alle im Netz befindlichen Endpunkte müssen Zugriffsregeln für jede erdenkliche Konfiguration definiert werden, was besonders in heterogenen Netzwerken, das heißt, in Netzwerken mit vielen verschiedenen IT-Systemen und Konfigurationen, einen hohen Aufwand bedeutet. Dabei ist auch zu beachten, dass Policies für ortsbundene IT-Systeme so gestaltet werden müssen, dass sie in anderen Netzwerken keine Nebeneffekte erzeugen. Schreiben zwei unterschiedliche Unternehmen nicht nur Anti-Malware-Lösungen, sondern unterschiedliche Hersteller vor, so kann dies auf dem Notebook eines Außendienstmitarbeiters, der in beiden Unternehmen tätig ist, zu Inkompatibilitäten führen.

Des Weiteren muss geklärt werden, wie die Daten der Policies optimal aktuell gehalten werden können. So muss zum Beispiel jederzeit bekannt sein, welche Versionsnummer die aktuelle Malwaresignatur einer Anti-Malwarelösung hat, ob die eingesetzte Personal-Firewall aktuell (das heißt, frei von bekannten Sicherheitslücken) ist und welchen Stand die Patch-Datenbank zum eingesetzten Betriebssystem und den verwendeten Anwendungen haben muss. Diese Informationen müssen von den Herstellern der einzelnen Komponenten bereitgestellt und dem Netzbetreiber in geeigneter Form zur Verfügung gestellt werden. Ein Netzbetreiber ist somit nicht nur beim Aufbau des Netzes auf die Hersteller, die ihre Software mit IMC- und IMV-Funktionen ausstatten müssen, angewiesen, sondern auch während des Betriebes. Hier müssen neue Formen der Zusammenarbeit und vertragliche Aspekte zur Haftung geklärt werden.

## Sicherheit

Ein weiteres „Problem“ des TNC-Ansatzes ist die netzabhängige Sicherheit. Das heißt, dass die Messung, und somit auch der Schutz der Daten und Endgeräte, nur bei vorhandener Verbindung zum Netzwerk möglich sind. Wird ein IT-System ohne eine aktive Netzwerkverbindung komromittiert, so ist die Cyber-Sicherheit aller zuvor aus dem Netzwerk kopierten Daten gefährdet.

Dieser Aspekt muss durch andere Cyber-Sicherheitsmechanismen, wie zum Beispiel Enterprise Rights-Management-Systeme, gelöst werden.

## Kompatibilität

Die meisten Lösungen sind grundsätzlich proprietär und deshalb meist inkompatibel zueinander. Ausnahme bietet hier die TNC-Spezifikation, bei der Offenheit zu einer der wichtigsten Anforderungen gehört.

### 7.4.7 Fazit: Trusted Network Connect (TNC)

Im Zuge der immer stärkeren Vernetzung innerhalb und zwischen Unternehmen über unsichere Kommunikationsnetze ist eine Erhöhung der Vertrauenswürdigkeit von Netzwerkkommunikation unabdingbar.

Es existieren verschiedene Lösungsansätze, die die Feststellung der Endpunkt-Integrität ermöglichen und so dazu beitragen können, die Vertrauenswürdigkeit zu erhöhen. Im Gegensatz zu proprietären Lösungsansätzen besitzt TNC durch seine Offenheit einen großen Vorteil. So ist TNC nicht an die Hard- oder Software bestimmter Hersteller gebunden. Dies ermöglicht eine Akzeptanz und Adaption durch alle Hersteller von Systemkomponenten und Netzwerktechnologie, was ein wichtiger Faktor für den Erfolg sein wird.

Es ist aber zu beachten, dass alle Ansätze für sich allein stehend die Vertrauenswürdigkeit nur bedingt erhöhen werden. Erst mit Einsatz sicherer Betriebssystemstrukturen kann die Integrität der Komponenten gewährleistet werden. Da TNC weder ein TPM noch spezielle Betriebssystemstrukturen voraussetzt, lässt es sich aber schon heute schrittweise in vorhandene Netzwerke integrieren und ermöglicht so einen sanften Umstieg in eine vertrauenswürdige Kommunikation.

---

## 7.5 Festlegung einer sicheren und vertrauenswürdigen Systemkonfiguration

Mit Trusted Computing können Hard- und Software-Systemkonfigurationen gemessen und jederzeit überprüft werden. Eine wichtige Frage ist aber, wer definiert, was eine sichere und vertrauenswürdige Systemkonfiguration ist.

### Der Hersteller der IT-Systems?

Der Hersteller kennt die Hardware sehr gut, weil er sie selber baut oder bauen lässt. Er ist für das Betriebssystemen und Basis-Anwendungen verantwortlich. Mit diesem Wissen und Gestaltungsspielraum kann jeder Hersteller genau festlegen, was eine sichere und vertrauenswürdige Systemkonfiguration ist.

### Der Hersteller des Cyber-Sicherheitssystems?

Der Hersteller von Cyber-Sicherheitssystemen kennt sich mit den Cyber-Sicherheitsproblemen und Angriffsvektoren aus und kann auf dieser Basis definieren, was eine sichere und vertrauenswürdige Systemkonfiguration ist.

**Das Anwendungsunternehmen der IT-Systeme?**

Das Anwendungsunternehmen hat Erfahrungen mit der Nutzung der IT-Systeme, kennt die realen Angriffe und die daraus verursachten Schäden. Mit diesen praktischen Erfahrungen kann das Anwendungsunternehmen sichere und vertrauenswürdige Systemkonfigurationen definieren.

**Kooperation der unterschiedlichen Rollen**

Ideal wäre es, wenn sich die Hersteller der IT-Systeme und Cyber-Sicherheitssysteme sowie die Anwendungsunternehmen zusammentreten würden, um eine sichere und vertrauenswürdige Systemkonfigurationen der genutzten IT-Systeme zu definieren.

---

**7.6 Zusammenfassung**

Trusted Computing ist eine Cyber-Sicherheits- und Vertrauenswürdigkeitstechnologie, die auf der Basis eines Hardware-Sicherheitsmoduls, dem TPM, die Integrität von Hard- und Software mess- und überprüfbar macht. Außerdem können durch die Trusted Computing Base, einen Mirokernel und eine Virtualisierung mit dem Gestaltungsfreiraum, Anwendung und Daten zu trennen, die Schäden der Software-Probleme deutlich reduziert werden. Das intelligente und sichere Schlüsselmanagement auf der Basis des TPMs mit den Trusted Computing Funktionen hilft, eine moderne Sicherheitsplattform aufzubauen. Durch den Aufbau einer Sicherheitsplattform ist es möglich, Policies auf fremden IT-Systemen und damit Konzepte wie Digital Rights und Enterprise Rights-Management umzusetzen.

---

**7.7 Übungsaufgaben****Übungsaufgabe 1**

Beschreiben Sie die Motivation für die Umsetzung von Trusted Computing!

**Übungsaufgabe 2**

Beschreiben Sie die Arbeitsweise der Trusted Computing-Funktionen „Trusted Boot“, „Binding“, „Sealing“ und „(Remote) Attestation“!

**Übungsaufgabe 3**

Warum darf der Endorsement Key niemals ein migrierbarer Schlüssel sein?

**Übungsaufgabe 4**

In welcher Phase, innerhalb von Trusted Network Connect, wird bestimmt, ob ein Client Zugriff auf ein Netzwerk erhält. Was geschieht, wenn dem Client der Zugriff verwehrt wird?

### Übungsaufgabe 5

Welchen Vorteil bietet Trusted Boot für den Nutzer?

### Übungsaufgabe 6

Gegeben ist die folgende Chain of Trust. Die Überprüfung der Vertrauenswürdigkeit des dritten Kettengliedes schlägt fehl. Was bedeutet das für die Vertrauenswürdigkeit der anderen Kettenglieder?



### Übungsaufgabe 7

Warum können „migrierbare Schlüssel“ nicht für Sealing, aber für Binding verwendet werden?

Ergebnisse siehe: <https://norbert-pohlmann.com/cyber-sicherheit/uebungen/>.

---

## Literatur

1. Pohlmann N (2011) Bugs, die Nahrung für Malware – Von guter, schlechter und böser Software. IT-Sicherheit 2011(4):32–34
2. Bothe D, Pohlmann N, Speier A (2016) Sicherheitsstandards in der Seitenlage? Proaktive Strategien als Fundament der IT-Sicherheit. IT-Sicherheit 2016(2):46–49
3. Coverity® Scan Open Source Report 2014
4. Alkassar A, Stüble C (2008) Die Sicherheitsplattform TURAYA. In: Pohlmann N, Reimer H (Hrsg) Trusted Computing – Ein Weg zu neuen IT-Sicherheitsarchitekturen. Vieweg-Verlag, Wiesbaden
5. Heibel N, Linnemann M, Pohlmann N (2008) Mehr Vertrauenswürdigkeit für Anwendungen durch eine Sicherheitsplattform. In: Pohlmann N, Reimer H (Hrsg) Trusted Computing – Ein Weg zu neuen IT-Sicherheitsarchitekturen. Vieweg-Verlag, Wiesbaden
6. Jungbauer M, Pohlmann N (2008) Trusted Network Connect Vertrauenswürdige Netzwerkverbindungen. In: Pohlmann N, Reimer H (Hrsg) Trusted Computing – Ein Weg zu neuen IT-Sicherheitsarchitekturen. Vieweg-Verlag, Wiesbaden
7. Linnemann M, Pohlmann N (2007) Turaya – Die offene Trusted Computing Sicherheitsplattform. In: Lutterbeck B, Bärwolff M, Gehring R (Hrsg) Open Source Jahrbuch 2007. Lehmanns Media, Berlin



# Cyber-Sicherheit-Frühwarn- und Lagebildsysteme

8

In diesem Kapitel geht es um die Bedeutung und Grundstruktur eines Cyber-Sicherheit-Frühwarn- und Lagebildsystems. Außerdem werden die notwendigen Prozesse und die Probleme, die durch die Entwicklung eines Cyber-Sicherheit-Frühwarn- und Lagebildsystems entstehen, behandelt.

## 8.1 Einleitung

Alle Organisationen sind zunehmend von der Verfügbarkeit der eigenen und öffentlichen IT-Infrastruktur abhängig. Ausfälle und Störungen der weltweiten Kommunikation, der angebotenen Dienste und digitalen Geschäftsprozesse können zu unkalkulierbaren Schäden führen. Ein Cyber-Sicherheit-Frühwarn- und Lagebildsystem hilft, die Cyber-Sicherheitslage aktuell aufzuzeigen, möglichst früh Angriffs-potenziale und reale Angriffe zu erkennen, um rechtzeitig Warnhinweise zu geben, damit Schäden auf die IT-Infrastruktur minimiert oder verhindert werden können.

**Wichtig** Ein Cyber-Sicherheit-Frühwarn- und Lagebildsystem hilft, Sicherheit und Vertrauenswürdigkeit der IT-Infrastruktur nachhaltig zu erhöhen und widerstandsfähiger zu gestalten.

## 8.2 Angriffe und ihre Durchführung

In diesem Abschnitt werden Grundlagen von Angriffen aufgezeigt, um besser zu verstehen, wie Angriffe und Angriffspotenziale erkannt werden können.

Ein Angriff ist ein Versuch, einen Wert zu stehlen, zu verändern, zu löschen oder sich unbefugten Zugriff auf ein IT-System und deren Ressourcen zu verschaffen, siehe Abb. 8.1.



**Abb. 8.1** Werte

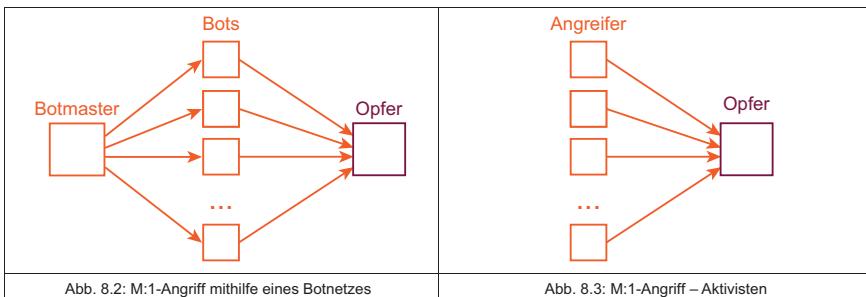
Dies tut der Angreifer in der Regel gezielt und absichtlich, siehe auch Abschn. 1.8 „Angreifer und deren Motivation“.

### Durchführung von Angriffen

Eine Möglichkeit, Angriffe zu unterscheiden, ist Anzahl der Angreifer und Opfer als Kriterium zu verwenden. Im Folgenden werden einige Angriffe diskutiert.

#### A) M:1-Angriff

Bei einem M:1-Angriff gibt es M Angreifer und ein Opfer.



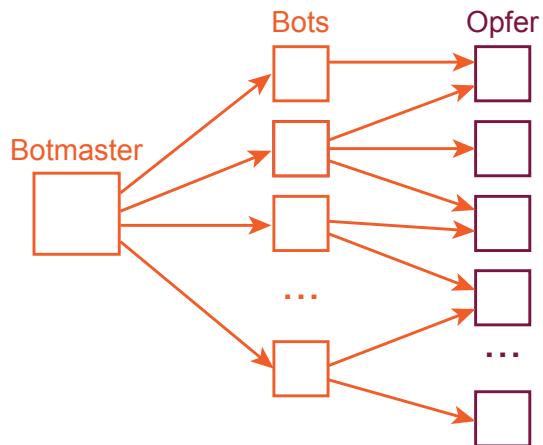
Die M Angreifer sind zum Beispiel

- Bots, das sind kompromittierte IT-Systeme mit Malware und Teil eines Botnetzes, das von einem Botmaster gesteuert wird, siehe Abb. 8.2,

oder/und

- Aktivisten, die sich für einen Angriff abgesprochen haben, siehe Abb. 8.3.

Das Opfer ist zum Beispiel ein Webserver oder ein anderer IT-Dienst im Internet

**Abb. 8.4** M:N-Angriff**Beispiel für ein M:1-Angriffsverfahren:**

## 1. Distributed Denial of Service (DDoS)

Distributed Denial of Service (DDoS) ist ein Beispiel für einen M:1-Angriff. Sehr viele Bots und/oder Aktivisten senden koordiniert spezielle Anfragen mit einer großen Last an ein ausgesuchtes Ziel-IT-System, um durch Erschöpfung der verfügbaren Ressourcen (CPU, RAM, Bandbreite, ...) dieses lahmzulegen, siehe auch Kap. 12 „Cyber-Sicherheitsmaßnahmen gegen DDoS-Angriffe“.

**B) M:N-Angriff**

Bei einem M:N-Angriff gibt es M Angreifer und N Opfer, siehe Abb. 8.4.

Die M Angreifer sind zum Beispiel

- Bots, das sind kompromittierte IT-Systeme mit Malware und Teil eines Botnetzes, das von einem Botmaster gesteuert wird.

Die Opfer sind zum Beispiel Webserver (Click Fraud), E-Mail-Server (Spam), ...

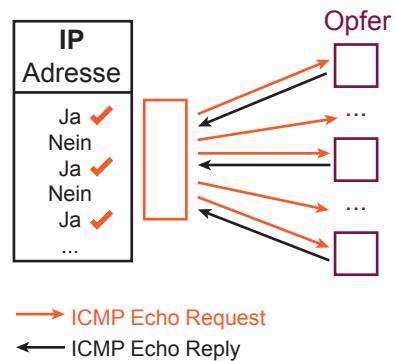
**Beispiele für Angriffsverfahren:**

## 1. Spam-E-Mails

Durch den Botmaster gesteuert werden Spam-E-Mails in einer dosierten Menge mithilfe der kompromittierten IT-Systeme mit Malware (Bots) eines Botnetzes an die Opfer gesendet. Da die Spam-E-Mails von verschiedenen IT-Systemen kommen, ist die Wahrscheinlichkeit des Durchlassens eines Spam-Filters deutlich größer.

## 2. Click Fraud

Mithilfe der kompromittierten IT-Systeme mit Malware (Bots) eines Botnetzes wird, durch den Botmaster gesteuert, automatisiert auf kommerzielle Werbepläne geklickt, um damit die dahinterliegenden Abrechnungssysteme aus monetären Gründen gezielt zu manipulieren. Durch die Verteilung der Klicks auf sehr viele unterschiedliche IT-Systeme, können die Abrechnungssysteme diesen Angriff nicht identifizieren.

**Abb. 8.5** Ping Scan

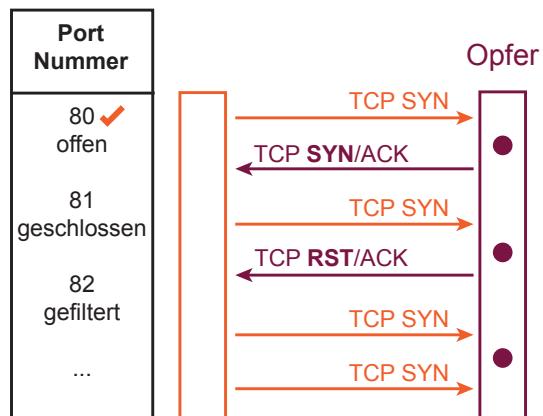
### C) 1:N-Angriff als Vorbereitung von gezielten Angriffen

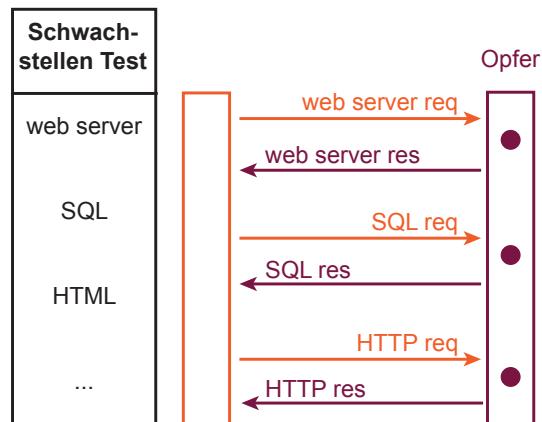
Bei einem 1:N-Angriff gibt es einen Angreifer und N Opfer. Diese Art des Angriffs wird sehr oft für die Vorbereitung von gezielten Angriffen verwendet. Ein Angreifer ist zum Beispiel jemand, der auf der Basis von Tools, Netze, IT-Systemen usw. analysiert, um mit diesen Ergebnissen dann gezielt Angriffe erfolgreich umsetzen zu können. Die Opfer sind IT-Systeme, die angegriffen werden sollen.

Auf der Netzwerkebene wird zum Beispiel eine „Ping Scan“ durchgeführt. Mit „Ping“ wird eine Echo-Request-Nachricht an ein zu testendes IT-System geschickt, siehe Abb. 8.5.

Wird dieses Paket mit einer Echo-Reply-Nachricht beantwortet, ist sichergestellt, dass das IT-System erreichbar ist. Daher soll mit einem Ping Scan überprüft werden, hinter welcher IP-Adresse ein über das Netz erreichbares IT-System angeschlossen ist. Welcher Dienst auf dem IT-System angeboten wird, kann dann mit dem „Port Scan“ gemessen werden.

Auf der Transportebene wird dann für alle erreichbaren IT-Systeme zum Beispiel ein „Port Scan“ durchgeführt, siehe Abb. 8.6.

**Abb. 8.6** Port Scan

**Abb. 8.7** Vulnerability Scan

Der Port Scan überprüft, welche Anwendungsdienste, wie Webserver, E-Mail-Server, SIP-Server usw., auf einem ansprechbaren IT-System angeboten werden. Beim TCP-SYN-Scan wird ein TCP-Paket mit SYN-Flag an das erreichbare Ziel-IT-System gesendet, um einen Verbindungsversuch durchzuführen. Die Antwort des IT-Systems gibt Erkenntnisse über den Port, an den ein TCP-Paket mit SYN-Flag gesendet worden ist: Sendet das IT-System ein SYN/ACK-Paket, akzeptiert der Port Verbindungen und der entsprechende Anwendungsdienst wird auf dem IT-System angeboten. Sendet das IT-System ein RST-Paket, wird auf dem entsprechenden IT-System dieser getestete Anwendungsdienst nicht angeboten.

Sendet das IT-System kein Paket, ist wahrscheinlich ein Firewall-System vorgeschaltet. Dieser Vorgang wird für alle definierten Ports durchgeführt, für die die Verfügbarkeit eines Anwendungsdiensts überprüft werden soll. Port 80/443 für http, Port 25/465 für SMTP, Port 143/993 für IMAP usw.

Nachdem der „Port Scan“ für alle erreichbaren Ziel-IT-Systeme durchgeführt wurde, kann dann gezielt für die verfügbaren Anwendungsdienste und das IT-System ein „Vulnerability Scan“ (Schwachstellentest) umgesetzt werden.

Auf der Anwendungsebene wird zum Beispiel eine „Vulnerability Scan“ durchgeführt. Der Vulnerability Scan probiert über das Senden von Anwendungsnachrichten, ob aktuelle und öffentlich bekannte Sicherheitslücken auf dem zu testenden Ziel-IT-System ausnutzbar sind, siehe Abb. 8.7.

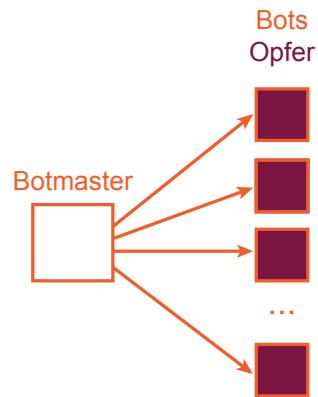
Wenn diese auf dem IT-System noch nicht gepatcht sind, können diese für Angriffe auf dem Ziel-IT-System genutzt werden.

#### D) 1:N-Angriff auf mit Malware kompromittierte IT-Systeme

Bei einem 1:N-Angriff gibt es einen Angreifer und N Opfer.

Der eine Angreifer ist zum Beispiel ein Botmaster, der ein Botnetz unter zentraler Kontrolle hat und dieses für Angriffe nutzt, siehe Abb. 8.8.

Die Opfer sind die komromittierten IT-Systeme (Bots), die mit Malware identifiziert sind und angegriffen werden sollen.

**Abb. 8.8** 1:N-Angriff

**Beispiele, welche Schadfunktionen einer Malware für einen Angriff auf das kompromittierte IT-System genutzt werden können:**

1. Ransom-Ware

„Ransom-Ware“ ist eine Schadfunktion der Malware, die böswillig die Daten auf dem komromittierten IT-System verschlüsselt und Lösegeld für den Erhalt des Schlüssels, der zur Entschlüsselung notwendig ist, fordert.

2. Keylogger

Die Schadfunktion „Keylogger“ liest auf dem komromittierten IT-System über die Tastatur eingegebene Daten wie Nutzernamen, Passwörter und sonstige sicherheitsrelevante Informationen aus und sendet diese in sogenannte Drop Zones. Ein Angreifer kann sich dann in der Drop Zone alle ausgelesenen Daten der komromittierten IT-Systeme holen.

3. Trojanisches Pferd

Mithilfe der Schadfunktion „Trojanischen Pferd“ werden von den komromittierten IT-Systemen zum Beispiel gespeicherte Dateien auf der Festplatte oder sonstigen Speichermedien unberechtigt ausgelesen. Der Angreifer kann diese Dateien dann auswerten und für seine Zwecke verwenden, zum Beispiel wirtschaftliche und politische Spionage.

4. Adware

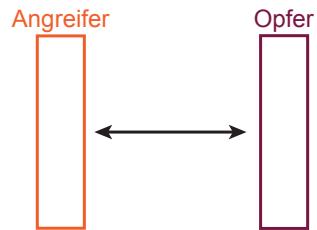
„Adware“ ist eine Schadfunktion einer Malware auf einem komromittierten IT-System, die dem Nutzer unerwünschte Werbung anzeigt und Aktivitäten der Nutzer an die Betreiber dieser illegalen Werbeagenturen sendet.

### E) 1:1-Angriff

Bei einem 1:1-Angriff gibt es einen Angreifer und ein Opfer.

Der eine Angreifer ist zum Beispiel professioneller Hacker, der einen gezielten Angriff durchführen möchte, siehe Abb. 8.9.

Das Opfer ist zum Beispiel ein IT-System einer Person, eines Unternehmens oder der Regierung.

**Abb. 8.9** 1:1-Angriff**Beispiel für ein Angriffsverfahren:****1. Advanced Persistent Threat (APT)**

Mithilfe von komplexen Angriffsmethoden, wie Advanced Persistent Threat (APT), wird das Ziel-IT-System gehackt.

**2. Social Engineering**

Mithilfe von Social Engineering werden Angriffe, wie Spear-Phishing oder Whaling (Führungskräfte) vorbereitet, um dann das Ziel-IT-System anzugreifen.

## 8.3 Idee eines Cyber-Sicherheit Frühwarnsystems

Bei Cyber-Sicherheit Frühwarnsystemen sind zwei relevante Aspekte ausschlaggebend. Zum einen ist es wichtig, Angriffspotenziale früh zu erkennen, um möglichen Schaden zu begrenzen oder im besten Fall sogar ganz zu vermeiden. Die Eingrenzung und Abwehr des Schadens hängt hierbei nach erfolgreicher Erkennung sehr stark von der Initiierung geeigneter Gegenmaßnahmen ab.

Zum anderen ist es nötig, die jeweiligen IT-Infrastrukturen so anzupassen und zu verbessern, dass diese für zukünftige Angriffe gerüstet sind [1].

**Wichtig** Um Angriffspotenziale und Angriffe möglichst früh zu erkennen, müssen die IT-Systeme und deren Kommunikation mithilfe von Sensoren auf sicherheitsrelevante Informationen untersucht werden.

### 8.3.1 Reaktionszeit für die Frühwarnung

Vor dem Hintergrund der beschriebenen Angriffspotenziale wird deutlich, dass im Allgemeinen nur sehr wenig Zeit für eine Frühwarnung zur Verfügung steht und alle beteiligten Komponenten so schnell und effizient wie möglich reagieren müssen. In vielen Fällen ist es sogar unmöglich, eine Warnung auszusprechen, bevor der tatsächliche und konkrete Angriff gestartet wurde.

Leichter ist es hingegen, vor Angriffspotenzialen zu warnen. Besonders bei einem kollaborativen Frühwarnsystem könnten zukünftig betroffene IT-Infrastrukturen rechtzeitig informiert werden, um weiteren Schaden abzuwenden.

### **8.3.2 Definition eines Cyber-Sicherheit Frühwarnsystems**

Ausgehend von den Zielen, IT-Infrastrukturen hinsichtlich Cyber-Sicherheit und Vertrauenswürdigkeit zu verbessern und einen kontinuierlichen Status über die IT-Infrastruktur zu generieren, der in Kooperation mit öffentlichen und privaten Partnern im Sinne einer kollaborativen Frühwarnung durchgeführt wird, könnte eine Definition für ein Cyber-Sicherheit Frühwarnsystem wie folgt lauten:

„Basierend auf verlässlichen Ergebnissen und Resultaten über Angriffspotenziale oder bereits eingetretener Cyber-Sicherheitsvorfälle, die jedoch vorerst nur wenige IT-Infrastrukturen betreffen, wird ein Cyber-Sicherheitslagebild kontinuierlich aktualisiert, und beim Eintreten eines adäquaten und relevanten Vorfalls wird eine qualifizierte Warnung an potenziell Betroffene verbreitet, um deren voraussichtlichen Schaden zu verringern oder ganz zu vermeiden.“

### **8.3.3 Obligatorische funktionelle Anforderungen**

An ein Cyber-Sicherheit Frühwarn-System sind eine Reihe von funktionalen Anforderungen zu stellen:

- Die Angriffserkennung muss zu einem Zeitpunkt erfolgen, bevor konkreter Schaden eingetreten ist und früh genug, um potenzielle Schäden zu minimieren. Hierbei ist wichtig, dass sowohl bekannte als auch unbekannte Angriffe erkannt werden.
- Der Entscheidungsprozess sowie die Entwicklung von Gegenmaßnahmen müssen unterstützt werden. Dies kann zum Beispiel durch Analysetools und Ergebnisvisualisierungen erfolgen. Expertensysteme können bei der Entscheidungsfindung helfen.
- Die Sicherstellung und Sammlung von Beweismitteln für die Forensik müssen gewährleistet werden, um später rechtliche Maßnahmen ergreifen zu können.
- Der aktuelle Status und die Entwicklung des Kommunikationsverkehrs müssen ständig beobachtet werden. Fragen, wie die IT-Infrastruktur erweitert werden muss oder welche IT-Technologien in der Zukunft an Wichtigkeit zu- oder abnehmen, spielen hier eine Rolle.
- Die aktuelle Cyber-Sicherheitslage mitsamt einer Übersicht über alle sicherheitsrelevanten Ereignisse müssen kontinuierlich generiert werden. Hierbei helfen geeignete Visualisierungen für die Lagebetrachtung.
- Weitere Anforderungen ergeben sich direkt aus dem Fakt, dass das Cyber-Sicherheit Frühwarnsystem selbst geschützt werden muss. Es muss dabei auf die Stabilität, die Sicherheit des Cyber-Sicherheit Frühwarnsystems vor Angriffen, die Einhaltung des Datenschutzes, die Wartbarkeit und die Performanz geachtet werden.

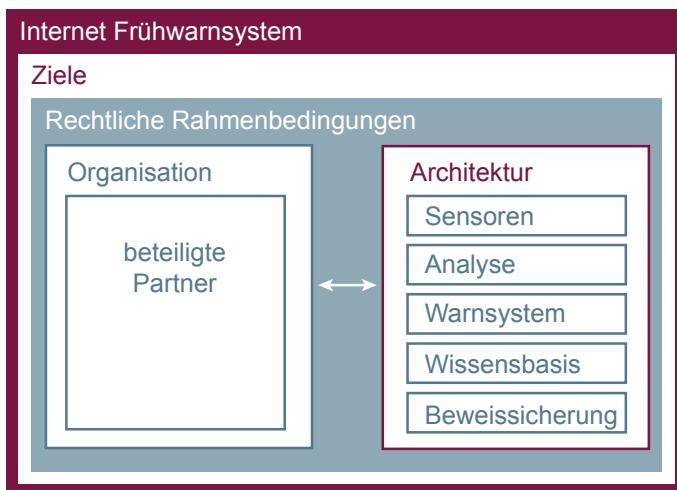
### 8.3.4 Asymmetrische Bedrohungen

Ein weiteres Problem stellen die asymmetrischen Bedrohungen dar. Viele Angriffe werden global durchgeführt und sind nicht auf einen bestimmten Ort ausgerichtet. Das beste Beispiel hierfür stellt ein DDOS-Angriff dar. Die Reaktion auf einen aufgetretenen Sicherheitsvorfall wird derzeit nur lokal initiiert und betrifft demnach auch nur die jeweilige lokale IT-Infrastruktur. Alle Opfer eines globalen Angriffs müssen jedoch die gleichen oder ähnlichen Reaktionen und Gegenmaßnahmen einleiten, um den Schaden zu reduzieren oder abzuwenden. Der Gesamtaufwand für die Angriffsabwehr multipliziert sich somit fast mit der Anzahl der betroffenen IT-Systeme und IT-Infrastrukturen.

**Wichtig** Ziel eines Cyber-Sicherheit Frühwarnsystems muss es also sein, bei Vorfällen effiziente Reaktionen für alle beteiligten IT-Systeme zu initiieren, und dies möglichst auf eine automatisierte Art und Weise.

## 8.4 Aufbau eines Cyber-Sicherheit Frühwarnsystems

Ausgehend von Architektur und Vorgaben der jeweiligen betreibenden Organisation kann ein Modell für ein Cyber-Sicherheit Frühwarnsystem aufgestellt werden, siehe Abb. 8.10.



**Abb. 8.10** Modell eines Cyber-Sicherheit Frühwarnsystems

In erster Linie wird das Cyber-Sicherheit Frühwarnsystem durch die Ziele definiert, die erreicht werden sollen.

### **8.4.1 Rechtliche Rahmenbedingungen**

Gleichermaßen wichtig sind die rechtlichen Rahmenbedingungen, unter denen das Cyber-Sicherheit Frühwarnsystem betrieben werden soll. Je nachdem, wie die rechtlichen Bestimmungen in dem Staat und der Organisation aussehen, kann das Cyber-Sicherheit Frühwarnsystem mehr oder weniger Einschränkungen unterliegen. Relevant sind hierbei vor allem Datenschutzaspekte, die eingehalten werden müssen, der Schutz des Vertrauens und das jeweilige Vertragsrecht. Nicht selten legen die rechtlichen Rahmenbedingungen die Möglichkeiten des Cyber-Sicherheit Frühwarnsystems fest, wie die geforderten Ziele zu erreichen sind.

### **8.4.2 Beteiligte Organisationen**

Anschließend bestimmen die jeweilige Organisation, die das Cyber-Sicherheit Frühwarnsystem betreibt, und die beteiligten Partner das Modell. Die Partner können hierbei zwei verschiedene Rollen (aktiv oder passiv) einnehmen. In der aktiven Rolle sind die Teilnehmer in den Aufbau und Betrieb des Cyber-Sicherheit Frühwarnsystems involviert, zum Beispiel durch das Bereitstellen von Sensoren, den operativen Betrieb eines Lagezentrums oder die Erstellung von Gegenmaßnahmen. Passive Teilnehmer nutzen praktisch ausschließlich die Informationen, die andere Cyber-Sicherheit Frühwarnsysteme ihnen übermitteln. Häufig handelt es sich hierbei um Privatnutzer oder kleine Organisationen.

Die Betreiber eines Cyber-Sicherheit Frühwarnsystems haben in der Regel eine genaue Definition der Organisationseinheiten mit den jeweiligen Beziehungen und klar definierten Verantwortlichkeiten. Um schneller handeln zu können, sind die nötigen Informationsflüsse und Reaktionsmöglichkeiten klar vereinbart. Wichtig ist für ein solches Unternehmen, einen sehr kurzen Entscheidungsprozess, effiziente Pfade für die Informationsverteilung sowie klar definierte Verantwortlichkeiten zu besitzen, um im Notfall früh warnen und reagieren zu können.

---

## **8.5 Technische Realisierung eines Cyber-Sicherheit Frühwarnsystems**

In diesem Abschnitt werden einige technische Aspekte der Realisierung eines Cyber-Sicherheit Frühwarnmodells beschrieben.

### **8.5.1 Architektur**

Die Architektur innerhalb des Cyber-Sicherheit Frühwarnmodells stellt die technischen Komponenten dar, die realisiert werden müssen. Dabei sollten verschiedene

Aspekte berücksichtigt werden, wie Zuverlässigkeit, Wartbarkeit, Komplexität, Leistung, Datenschutz und Vertraulichkeit.

Die Architektur kann zentralisiert oder dezentralisiert umgesetzt werden.

### **1. Zentralisierte Architektur:**

Neben den Sensoren sind alle Komponenten in einer zentralen Betriebseinheit untergebracht.

Vorteile:

- einfache Wartbarkeit
- begrenzte Komplexität

Nachteile:

- könnten zu Leistungsproblemen führen
- zentralisierte Systeme sind leichter anzugreifen, wie zum Beispiel mithilfe von DDoS-Angriffen

### **2. Dezentrale Architektur:**

Nicht nur die Sensoren, sondern auch die Analysekomponenten und die Wissensbasis sind verteilt. Bei Bedarf tauschen die einzelnen Komponenten Informationen aus. Warnungen können von einer zentralen Einheit oder von den verschiedenen verteilten Einheiten verbreitet werden.

Vorteile

- bessere Skalierung der Leistung
- kann nicht so leicht angegriffen zu werden

Nachteile

- komplexer
- Wartbarkeit ist schwieriger.

## **8.5.2 Sensoren**

Die Sensoren, die an jeweils strategischen Positionen in dem zu überwachenden Netzwerk und/oder IT-Systemen verteilt und aufgestellt werden, sammeln Daten, die die Grundlage für den aktuellen Status bilden. Die Verteilung der Sensoren ist abhängig davon, welche Teile des Netzwerks und der IT-Systeme besonders kritisch sind oder wie repräsentativ die Übersicht ausfallen soll. Als Sensoren wurden bereits etliche Typen entwickelt. Möglich sind dabei Sensoren, die eine Abbildung des Gesamtverkehrs erstellen, wie Flow-Daten, paketbasierte Statistiksensoren, Honeypots, Log- und Verfügbarkeitsdaten oder Ansätze, die den kompletten

Verkehr und die Aktivitäten aufzeichnen. Gerade bei den verwendeten Sensoren ist es immens wichtig, gleichermaßen auf den Datenschutz sowie auf die Beweissicherung zu achten. Realisiert werden kann dies durch Methoden der Pseudo- und Anonymisierung.

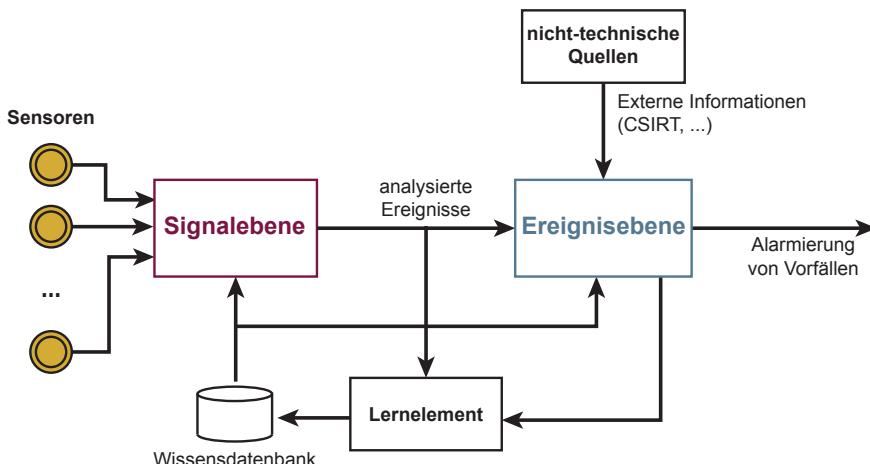
Die Analyse der Sensoren muss sehr performant sein, wenn nicht die gespeicherten Informationen stark reduziert werden sollen. Alternativ kann ein Sampling angewandt werden, bei dem in einer bestimmten Zeit oder nach einer gewissen Anzahl von Paketen nur eine Stichprobe entnommen und ausgewertet wird.

### 8.5.3 Analyse- und Erkennungsmodul

Das Analyse- und Erkennungsmodul (Analysis) bildet die Kernkomponente eines Cyber-Sicherheit Frühwarnsystems. Es ist dafür zuständig, sicherheitsrelevante Vorfälle zu identifizieren und diese in Form von Alarmen geeignet weiterzuleiten. Damit die Erkennung von Angriffspotenzialen und realen Angriffen funktioniert, ist eine Reihe von technischen Komponenten nötig, siehe Abb. 8.11.

Die Messdaten der installierten Sensoren werden an die Signalebene geschickt. Dort werden die Daten nach Relevanz gefiltert und analysiert. Zudem erfolgt hier die Erkennung von anomalen und sicherheitsrelevanten Vorfällen, wie zum Beispiel mit „Erkennen von bekannten sicherheitsrelevanten Aktionen“ und „Erkennen von Anomalien“. Diese Analysekonzepte produzieren Ereignisse, die ein bestimmtes Auftreten samt Informationen, die zu der Erstellung beigetragen haben, darstellen.

Diese Ereignisse werden nun an die Ereignisebene weitergereicht, auf welcher sie miteinander korreliert werden. Hierbei ist es ratsam, weitere Informationen



**Abb. 8.11** Technische Komponenten der Erkennungsverfahren

über Vorfälle oder Sicherheitslücken von externen, nicht-technischen Quellen (zum Beispiel CERTs, CVE) einzubinden, um eine bessere Aussage treffen zu können.

### **Alarmierung**

Gelangt die Analyse zu dem Ergebnis, dass die einzelnen Ereignisse nicht nur eine sicherheits-konforme Anomalie, sondern einen konkreten Vorfall oder Angriff widerspiegeln, wird ein Alarm generiert und an die zuständigen Verantwortlichen in der Organisation geleitet. Die größten Probleme bei der Erkennung stellen zum einen die riesigen Datenmengen dar, die es zu analysieren gilt. Zum anderen besteht die große Herausforderung darin, bislang unbekannte Angriffe und sich langsam entwickelnde Trends zu erkennen.

### **Lernelement**

Um die Erkennungsverfahren stets zu verbessern, muss ein Cyber-Sicherheit Frühwarnsystem ein Lernelement besitzen. Mithilfe der Informationsrückflüsse aus den Ereignissen und den Resultaten aus der Ereignisebene werden die Algorithmen adaptiv und kontinuierlich angepasst. Beispielsweise müssen manche Algorithmen, die den Netzwerkverkehr überwachen, angepasst werden, nachdem ein neuartiger Dienst hinzugefügt wurde, der vorher nicht bekannt war. Die Ergebnisse aus dem Lernelement fließen im Anschluss als modellierte Erkenntnisse in die Wissensdatenbank.

### **Wissensdatenbank**

Einen weiteren wichtigen Aspekt erfüllt die Wissensdatenbank. Sie enthält neben dem Wissen über die Umgebung, in der das Cyber-Sicherheit Frühwarnsystem eingesetzt wird, auch Informationen über das Normalverhalten des Netzwerks und Angriffssignaturen. Im Idealfall befinden sich auch konkrete Gegenmaßnahmen bezüglich bestimmter bereits bekannter Vorfälle sowie Vorgehensweisen für Problemfälle in der Wissensdatenbank. Damit diese auch wirklich unterstützen kann, müssen die enthaltenen Daten stets aktuell gehalten werden. Dies kann zum Beispiel durch die automatische Generierung von Malware- und Angriffssignaturen, das Aktualisieren des Normalzustands des Netzwerkverkehrs oder funktionierende Abläufe, um bis dato unbekannte Probleme zu lösen, erreicht werden.

Die Herausforderung hierbei ist die Akquise und kontinuierliche Speicherung von Wissen. Als Teil eines Expertensystems stellt die Wissensdatenbank nicht nur Hinweise für die Lösung von bereits bekannten Problemen zur Verfügung, sondern leistet auch intelligente Unterstützung beim Bearbeiten von unbekannten Vorfällen, indem sie ähnliche Ereignisse und Entstörungsanweisungen vorschlägt.

### **Beweissicherung (rechtliche Konsequenzen)**

Wurde auf den unterschiedlichen Ebenen der Erkennungsverfahren ein Angriff erkannt und im Idealfall erfolgreich abgewehrt, geht es darum, die Täter auch rechtlich und möglicherweise finanziell zur Verantwortung zu ziehen. Für ein

möglichen Gerichtsverfahren muss die Beweissicherung lückenlos und vertrauenswürdig durchgeführt werden.

Wichtig sind alle Informationen über den Angreifer, seine Vorgehensweise und den Schaden, den der Angriff verursacht hat. Auch hier müssen zwei wichtige Aspekte eingehalten werden. Zum einen muss der Datenschutz gewahrt werden, d. h. der Zugriff auf gespeicherte Daten darf nur bei einem konkret erkannten Vorfall erfolgen. Dies soll etwaige personenbezogene Daten vor Missbrauch schützen. Zum anderen muss die Authentizität der Beweise sichergestellt werden, indem Verfälschungen (zum Beispiel technisch) ausgeschlossen werden können.

## 8.6 Prinzipielle Aspekte von Sensoren

Sensoren sammeln Daten, mit denen der aktuelle Status der IT-Infrastruktur ermittelt wird. Sensoren werden über die gesamte IT-Infrastruktur verteilt, um einen repräsentativen Überblick über die IT-Infrastruktur zu erhalten.

Verschiedene Arten von Sensoren können verwendet werden:

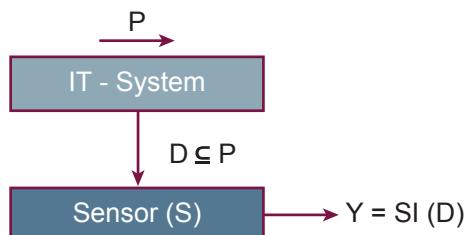
- Vollständige Aufzeichnung des Netzwerkverkehrs (zum Beispiel mit Wireshark)
- Netflow (Router), sFlow (Switch), ...
- Netzwerksensoren (statistischer Ansatz, Deep Packet Inspection, Intrusion Detection System, ...)
- Netzwerkverwaltung (zum Beispiel SNMP)
- Honeyots (Low- oder High-Interaktiv)
- Verfügbarkeit von Diensten, Knoten, Servern und Komponenten
- Logdaten-Analyse (Netzkomponenten (Firewall, Router, ...), ..., IT-Systeme (Anwendungen, Betriebssysteme, Daten, ...), ...).

### 8.6.1 Grundprinzip von Sensoren

Das Sammelsystem hat die Aufgabe, alle Daten (P), Ereignisse usw. zu sammeln. Das Sammelsystem kann ein Router, Switch, Endgeräte, Server oder allgemeines IT-System sein.

Der Sensor hat die Aufgabe, aus den Daten (D) des Sammelsystems sicherheitsrelevante Informationen zu extrahieren, die ein Höchstmaß an Sicherheitsinformationen für die Erkennung von Angriffspotenzialen und Angriffen enthalten, siehe Abb. 8.12.

**Abb. 8.12** Grundprinzip von Sensoren



P = vollständige Daten

Kommunikationsverkehr, Anwendungsverhalten, Datenzustände, Ereignisse, ...

D = Daten, die durch den Sensor gehen.

Hier kann eine erste Reduktion der Information vorgenommen werden. Dies könnte beispielsweise durch einen Router oder einen Switch realisiert werden.

Y = Ergebnis der Verarbeitung des Sensors Y = SI (D)

Der Sensor hat die Aufgabe, sicherheitsrelevante Informationen zu extrahieren, damit bei der Auswertung die Menge der Sicherheitsinformationen so groß wie nur möglich ist. Daher ist es wichtig, dass beim Design des Sensors genau überlegt wird, welche sicherheitsrelevanten Informationen für das Erkennen von Angriffen und Angriffspotenzialen wichtig sind.

Die Ergebnisse werden in der Regel an ein Analysesystem gesendet. Y sind normalerweise die Informationen, die über einen langen Zeitraum gespeichert werden, also sollte es so klein wie möglich sein!

SI (X) = die Menge der Sicherheitsinformationen, die aus X extrahiert werden können.

$$\text{SI (Y)} \leq \text{SI (D)} \leq \text{SI (P)}$$

### Qualität des Sensors

Die Herausforderung besteht also darin, den besten Sensor zu finden, d. h. einen Sensor, der

1. einen sehr hohen Grad an Reduzierung der Bytes aufweist,

$$Y <<< P$$

2. aber eine kleine Reduzierung der Sicherheitsinformationen in Y aufweist – SI (Y),

$$\text{SI (Y)} < \text{SI (P)}.$$

Ein optimaler Sensor hat:

$$\text{SI (Y)} = \text{SI (P)}$$

d. h., obwohl die Anzahl der Bytes eine sehr starke Reduzierung hat, findet keine Reduzierung der Sicherheitsinformationen statt.

**Wichtig** Ein idealer Sensor hat Zugriff auf alle Daten und extrahiert daraus alle sicherheitsrelevanten Informationen so, dass diese für das Erkennen aller Angriffe und Angriffspotenziale genutzt und von der notwendigen Speichergröße langfristig gespeichert werden können.

## 8.6.2 Messmethoden

Bei den Messungen kann zwischen einer aktiven und passiven Messung unterschieden werden.

### Aktive Messung

Der aktive Sensor erzeugt Daten und/oder Aktionen, um ein Verhalten messen zu können., zum Beispiel Ping, Trace-Route, Ausführung von Anwendungen/Diensten, ...

### Passive Messung

Der passive Sensor misst verschiedene Aspekte passiv, wie das Abhören von Kommunikationsleitung oder Messen von Ereignissen in einem IT-System usw.

## 8.6.3 Ort der Messung

Für die Platzierung des Sensors und den Ort der Messungen gibt es verschiedene Möglichkeiten, siehe Abb. 8.13.

Ein Sensor kann die Daten an sehr unterschiedlichen Orten messen.

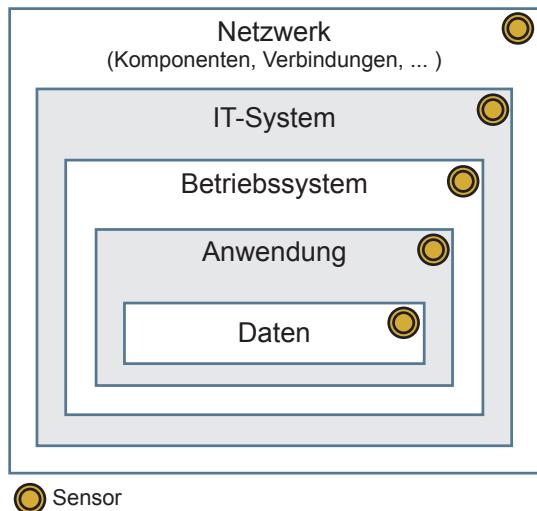
### Datenebene

Auf der Datenebene können zum Beispiel mit One-Way-Hashfunktionen für die Daten entsprechende kryptografische Prüfsummen berechnet werden, mit deren Hilfe die Integrität der Daten überwacht werden kann.

### Anwendungsebene

Auf der Anwendungsebene können Sensoren den ordnungsgemäßen Ablauf der Anwendung kontrollieren.

**Abb. 8.13** Ort der Sensoren



### Betriebssystemebene

Auf der Betriebssystemebene kann überwacht werden, ob nur gewünschte Software in der richtigen Art und Weise auf dem IT-System läuft.

### IT-Systemebene

Auf der IT-Systemebene können zum Beispiel die Daten-, Anwendungs- und Betriebssystemebene zusammengefasst und/oder weitere Elemente, wie zum Beispiel die Auslastung von CPU, RAM, Festplatte, usw. überwacht werden.

### Netzwerkebene

Auf der Netzwerkebene kann die Kommunikation mithilfe von Sensoren auf Anomalien und Angriffssignaturen überprüft werden. Auf der Netzwerkebene würden aber auch Verfügbarkeitssensoren positioniert werden, um die darin liegenden IT-Systeme darauf zu messen.

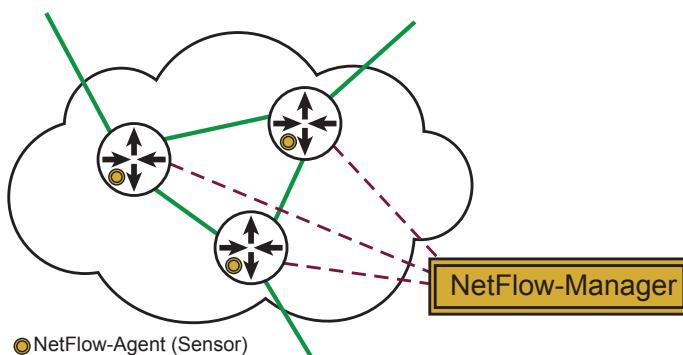
---

## 8.7 Diskussion unterschiedlicher Sensoren

In diesem Abschnitt werden einige mögliche Sensoren exemplarisch diskutiert; erst die grundsätzliche Idee, dann das Prinzip der Sammlung sowie Reduzierung der Datenmenge. Zum Schluss wird eine entsprechende Evaluierung des Sensors durchgeführt.

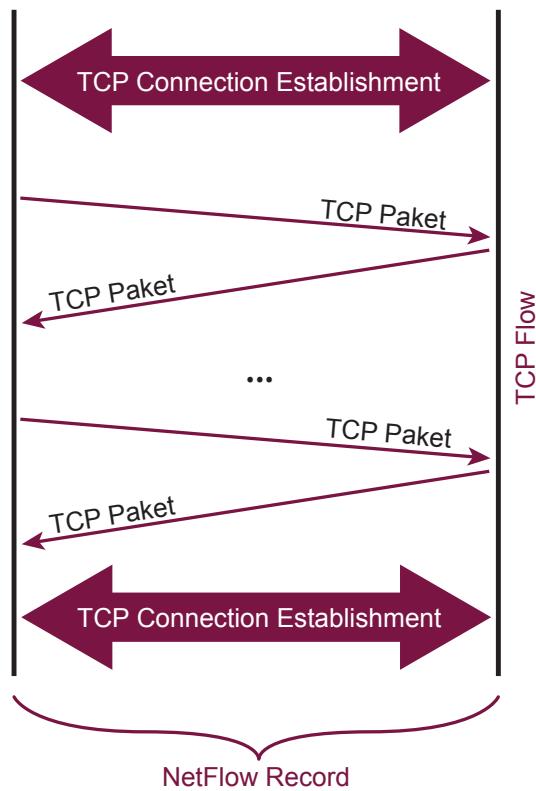
### 8.7.1 NetFlow-Sensor

NetFlow ist ein Standard, der in Routern implementiert ist und Informationen über den IP-Datenverkehr per UDP an einem NetFlow-Kollektor sendet. Im NetFlow-Kollektor werden die Daten in der Regel zur Verkehrsanalyse, zur Kapazitätsplanung oder zur QoS-Analyse verwendet. Es gibt aber auch die Möglichkeit, die NetFlow-Informationen für die Analyse von Angriffen oder für ein Kommunikationslagebild zu nutzen. Netflow ist ein passives Messverfahren, siehe Abb. 8.14.



**Abb. 8.14** NetFlow Sensor und die Integration in die IT-Infrastruktur

**Abb. 8.15** Eingeschlossene TCP-Pakete für die Berechnung eines NetFlow-Rekords



### Aufzeichnung von NetFlow-Rekord

Abb. 8.15 zeigt, welche TCP-Pakete für die Berechnung eines NetFlow-Rekords eingeschlossen sind: alle TCP-Pakete, die zwischen dem Verbindungsauftbau und vor dem Verbindungsabbau ausgetauscht werden.

### NetFlow-Rekord

Im Folgenden werden die Elemente in einem NetFlow-Rekord dargestellt:

- ...
- Zeitstempel (Beginn und Ende)
- Byte- und Paketzähler
- Quell- und Ziel-IP-Adressen
- Quell- und Ziel-IP-Ports (HTTP, SMNP, SIP, ...)
- TOS-Informationen
- AS-Nummern
- TCP-Flags
- Protokoll-Typ (zum Beispiel TCP, UDP oder ICMP)
- ...

**Grundprinzip des Sensors**

P alle IP-Pakete  
D P  
SI (D) Auswahl der NetFlow-Rekords und deren Inhalt  
Y NetFlow-Rekords

Die Analyse der sicherheitsrelevanten Informationen findet im erweiterten NetFlow-Kollektor statt.

**Evaluierung von NetFlow****Genereller Aspekt:**

- Ursprünglich für die Abrechnung des Netzwerkverkehrs konzipiert

**Ort der Messung:**

- Netzwerk, Funktion in Routern

**Sicherheitsinformation: + (wenig)**

Wie dem Inhalt des NetFlow-Rekords zu entnehmen ist, sind dort kaum sicherheitsrelevante Informationen enthalten. Daher können auch nur wenige Sicherheitsinformationen für die Identifizierung von Angriffen und Angriffspotenzialen verwendet werden.

**Vorteile:**

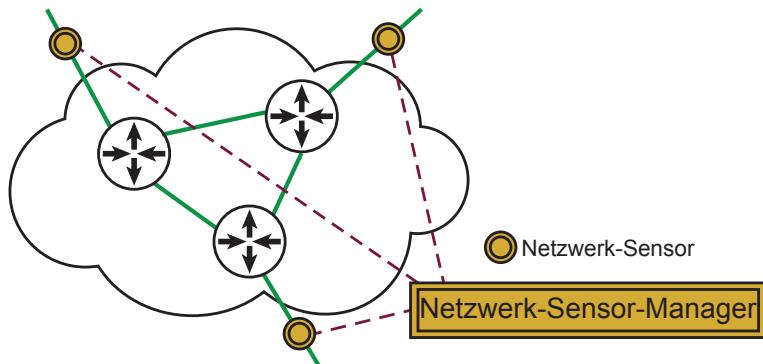
- der Sensor ist bereits als eine Funktion im Router verfügbar
- sehr schnell und keine Probleme mit hoher Bandbreite

**Nachteile:**

- nur wenige Sicherheitsinformationen verfügbar

**8.7.2 Netzwerk-Sensor**

Ein Netzwerk-Sensor ist eine Netzwerkkomponente, die das Netzwerk auf bösartige Aktivitäten oder Richtlinienverletzungen hin überwacht.



**Abb. 8.16** Netzwerk-Sensor

Netzwerksensor könnte sein:

- Intrusion Detection System (IDS) – Netzwerk, oft signaturbasiert, zum Beispiel snort
- Deep Packet Inspection (DPI) – intensive Analyse des Headers und des Datenteils
- statistische Ansätze – nur die Header werden analysiert (keine Datenschutzprobleme), zum Beispiel Internet-Analysesystem (IAS)

Netzwerk-Sensoren (siehe Abb. 8.16) sind passive Messverfahren.

### Grundprinzip des Sensors

P alle IP-Pakete

D P

SI (D) Deep Packet Inspection (erkannte Ereignisse)

oder

Intrusion Detection (erkannte Signaturen)

oder

statistische Ansätze (Statistiken über Kommunikationsparameter)

Y Rohdaten/Sicherheitsereignisse

Analyse von Sicherheitsinformationen im Sensor und/oder Analysesystem

### Evaluierung der Netzwerk-Sensoren

#### Genereller Aspekt:

- Jedes IP-Paket kann analysiert werden

#### Ort der Messung:

- Netzwerk: separater Sensor (Netzwerkkomponente) oder integriert in Netzwerkkomponenten (Router, Switch, ...)

**Sicherheitsinformation:** +++(hoch)

Die Sicherheitsinformationen sind mit hoch bewertet, weil die Sonde Zugriff auf alle Kommunikationsdaten hat, d. h. die Sonde kann daraus die richtigen sicherheitsrelevanten Informationen auswählen.

**Vorteile:**

- unabhängig von Netzwerkkomponenten
- beste Erkennungsfähigkeiten, arbeiten auf allen Kommunikationsebenen

**Nachteile:**

- höhere Kosten, Datenschutzprobleme, sehr hohe Leistungsanforderung

**Herausforderung 1: Nutzung eines Netzwerk-Sensors**

Netzwerk-Sensoren haben noch weitere besondere Herausforderungen:

**A) Kompletter Datenverkehr (P)**

Die Netzwerk-Sensoren wollen im Prinzip den vollständigen Datenverkehr analysieren. Das kann eine besondere Herausforderung darstellen.

Beispiel:

Datenverkehr am größten öffentlichen Austauschpunkt der Welt, DE-CIX. Die Datenrate war 2018 im Peak bis zu 6 T Bit/s und im Durchschnitt ca. 4 T Bit/s. Bei dieser hohen Datenrate kann der vollständige Kommunikationsverkehr nicht analysiert werden.

**B) Es müssen die rechtlichen Bedingungen für den Zugriff beachtet werden.**

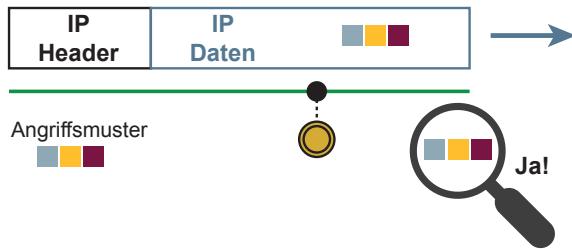
C) Außerdem ist der Datenverkehr, der durch den Sensor geht (D), eine echte Herausforderung. Die Sensoren brauchen eine sehr hohe Leistung (CPU, ...), müssen sehr viel Daten verarbeiten. Bei einem Durchsatz von 100 M Bit/s sind das 1 T Byte in 24 h. Es wird eine Methode der Reduktion notwendig, die die Anzahl der Bytes sehr stark reduziert und gleichzeitig die sicherheitsrelevanten Informationen behält.

**D) Ergebnis durch den Sensor (Y)**

Der Sensor muss wissen, welche sicherheitsrelevanten Informationen benötigt werden, damit ein Angriff erkannt und/oder ein aussagekräftiges Lagebild erstellt werden kann: Welche Kommunikationsparameter? Welche Nutzdaten? usw.

Damit mithilfe der sicherheitsrelevanten Informationen Profile berechnet werden können, müssen diese idealerweise langfristig gespeichert werden können. Daher ist es wichtig, nicht alles zu speichern, sondern nur Sicherheitsrelevantes und das in einer sparsamen Art und Weise.

Wenn die sicherheitsrelevanten Informationen, Personen oder personenbezüglichen Informationen enthalten, müssen diese vor der Speicherung auch noch pseudonymisiert oder anonymisiert werden.



**Abb. 8.17** Angriffserkennung auf der Basis eines Musters (Signatur)

### Herausforderung 2: Advanced Evasion Techniques (AET)

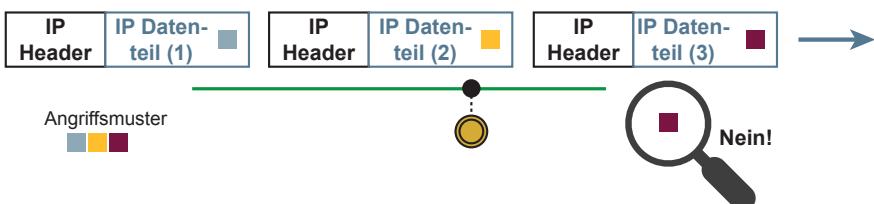
Advanced Evasion Techniques (AET) sind Techniken zum Umgehen eines Netzwerksensors, um einen Angriff auf ein Ziel-Netzwerk oder Ziel-IT-System ohne Erkennung durchzuführen.

In Abb. 8.17 wird ein Angriff anhand eines Angriffsmusters in einem IP-Paket erkannt. Ein Angreifer, der eine solche Erkennungsmethode verhindern möchte, kann das zum Beispiel mit der Nutzung des IP-Fragmentierungsmechanismus als Umgehungstechnik tun. Der IP-Fragmentierungsmechanismus ist Bestandteil der IP-Schicht und wird verwendet, um ein IP-Paket auf mehrere IP-Pakete zu verteilen, falls die Gesamtlänge des Datenpakets größer als die Maximum Transmission Unit der Netzwerkschnittstelle ist.

In diesem Fall nutzt der Angreifer den IP-Fragmentierungsmechanismus, um die Angriffserkennung durch den Netzwerk-Sensor zu verhindern. In dem prinzipiellen Beispiel in Abb. 8.18 wird das IP-Paket künstlich auf drei Pakete durch den IP-Fragmentierungsmechanismus verteilt, damit der Netzwerk-Sensor das Muster nicht erkennen kann. Der IP-Fragmentierungsmechanismus im angegriffenen Ziel-IT-System setzt das IP-Paket wieder zusammen und damit kann der Angriff erfolgreich umgesetzt werden, weil die Möglichkeit der Erkennung umgangen worden ist.

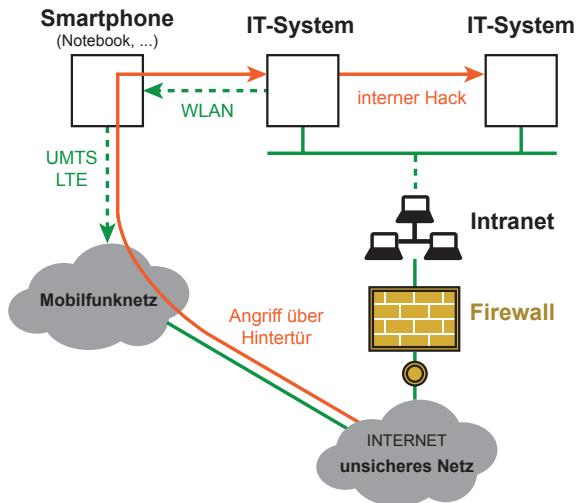
### Herausforderung 3: Nutzung von Hintertüren (Backdoors)

Wenn ein Netzwerk-Sensor an dem zentralen Übergang von dem zu schützenden Netz zum Internet positioniert wird, dann werden auch genau an diesem Übergang Angriffe erkannt.



**Abb. 8.18** Verhinderung der Angriffserkennung mithilfe von Advanced Evasion Techniques

**Abb. 8.19** Nutzung einer Hintertür für einen Angriff



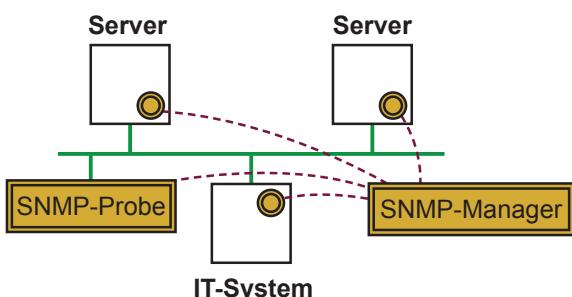
Gibt es Kommunikationsübergänge, wie das Mobilfunknetz, die „als Hintertüren“ an diesem Übergang vorbeigehen, dann kann dort auch kein Angriff erkannt und verhindert werden.

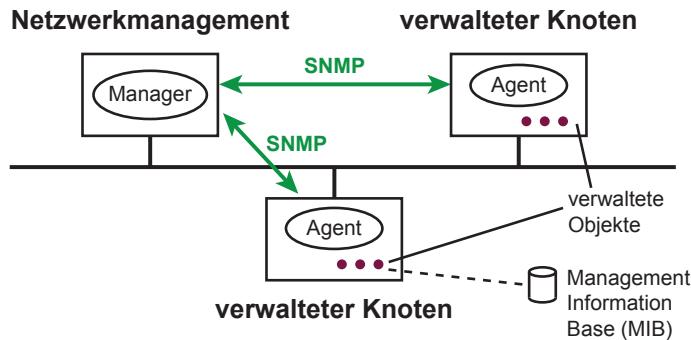
In Abb. 8.19 ist zu sehen, wie ein Angreifer die Kommunikationsverbindung nutzt, um darüber einen internen Angriff durchzuführen.

### 8.7.3 SNMP-Sensor

SNMP ist das Internet-Standard-Protokoll für die Verwaltung von IT-Systemen in IP-Netzwerken. IT-Systeme sind Router, Switches, Server, Workstations, Drucker, Modem-Racks und mehr. Es wird hauptsächlich in Netzwerkverwaltungssystemen verwendet, um an das Netzwerk angeschlossene IT-Systeme unter Bedingungen zu überwachen, die administrative Aufmerksamkeit erfordern. SNMP ist ein passives Messverfahren, siehe Abb. 8.20.

**Abb. 8.20** SNMP-Sensor





**Abb. 8.21** Die Architektur von SNMP

### Das Managementagent-Modell

Die Managementstation ist in der Regel ein einzelnes IT-System, auf dem die Managementapplikation läuft. Die Managementapplikation stellt die Schnittstelle zwischen Netzadministrator und dem Netzmanagementsystem dar. Im einfachsten Fall dient die Managementapplikation zur Aufbereitung und Darstellung der von dem Agent bereitgestellten Informationen. Allerdings können im Manager auch komplexe Managementanwendungen realisiert werden, durch die die Abläufe des Managements automatisiert und der Zustand des Netzes automatisch überwacht werden können [5], siehe Abb. 8.21.

Auf jedem zu verwaltenden Knoten (Managed Node) muss ein Managementagent installiert sein, der Managementinformationen über diesen Knoten für die Managementstation bereit hält und Anfragen von der Managementstation entsprechend bearbeitet. Die Ansammlung von Managed Objects, die ein Agent verwaltet, wird unter dem Begriff Management Information Base (MIB) zusammengefasst. Managementapplikation und Managementagent sind über ein Netzmanagementprotokoll verbunden. Das Protokoll für auf TCP/IP basierende Netzwerk ist das Simple Network Management Protocol (SNMP).

### Grundprinzip des Sensors

- P        alle IP-Pakete  
und/oder  
zusätzliche Daten abhängig von den verwendeten MIBs (Festplatte, CPU, ...)
- D        eine Reduktion von P
- SI (D)    Auswahl der Objekte in der MIB
- Y        SNMP-Nachricht (Inhalt der verwalteten Objekten)

Analyse von Sicherheitsinformationen nur im Analysesystem (SNMP-Manager)

## Evaluierung von SNMP

### Genereller Aspekt:

- Überwachen und/oder Verwalten einer Gruppe von IP-fähigen IT-Systemen in einem Netzwerk.

### Ort der Messung:

- Netzwerk, SNMP-Agent ist eine Anwendung in IP-fähigen IT-Systemen

### Sicherheitsinformation: + (wenig)

Wie dem Inhalt der MIBs von SNMP zu entnehmen ist, sind dort kaum sicherheitsrelevante Informationen enthalten. Daher können auch nur wenige Sicherheitsinformationen für die Identifizierung von Angriffen und Angriffspotenzialen verwendet werden.

### Vorteile:

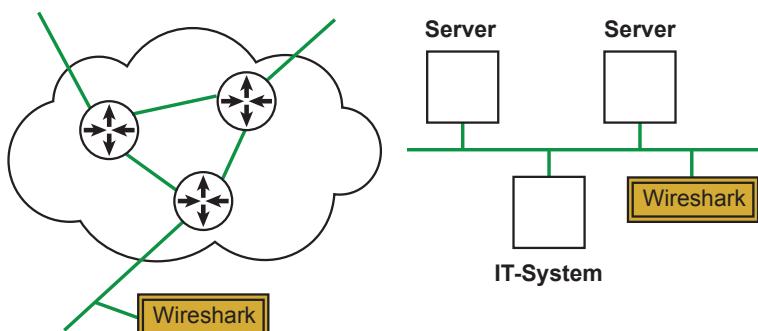
- Der Sensor ist bereits als ein Feature in den IP-fähigen IT-Systemen verfügbar
- perfekt zum Testen der Verfügbarkeit von lokalen Netzwerkgeräten, Servern, Diensten, ...

### Nachteile:

- wenig Sicherheitsinformationen in den MIBs verfügbar
- SNMP ist eher ein Netzwerkmanagement als ein IT-Sicherheits-Tool

### 8.7.4 Wireshark-Sensor

Wireshark ist ein mächtiges Tool zur Analyse und grafischen Aufbereitung von einer Vielzahl von Kommunikationsprotokollen. In Abb. 8.22 ist Wireshark als Sensor für ein Cyber-Sicherheit Frühwarnsystem eingezeichnet. Wireshark ist ein passives Messverfahren.



**Abb. 8.22** Wireshark-Sensor

### Grundprinzip des Sensors

P alle IP-Pakete  
D P  
SI (D) Auswahl der Filter durch den Cyber-Sicherheitsexperten  
Y Interpretation durch einen Cyber-Sicherheitsexperten

Die Analyse der Sicherheitsinformationen erfolgt lokal durch einen Cyber-Sicherheitsexperten mithilfe der Wireshark-Anwendung.

### Evaluierung von Wireshark

#### Genereller Aspekt:

- Wireshark ist sehr nützlich für die detaillierte Analyse eines Angriffs.

#### Ort der Messung:

- Netzwerk, integriert als Anwendungstool in ein IT-System (Notebook, PC)

#### Sicherheitsinformation: +++ (hoch)

Da Wireshark auf alle Paket-Informationen der unterschiedlichen Kommunikationsprotokolle zugreifen kann, werden auch die Sicherheitsinformationen hoch sein können.

#### Vorteile:

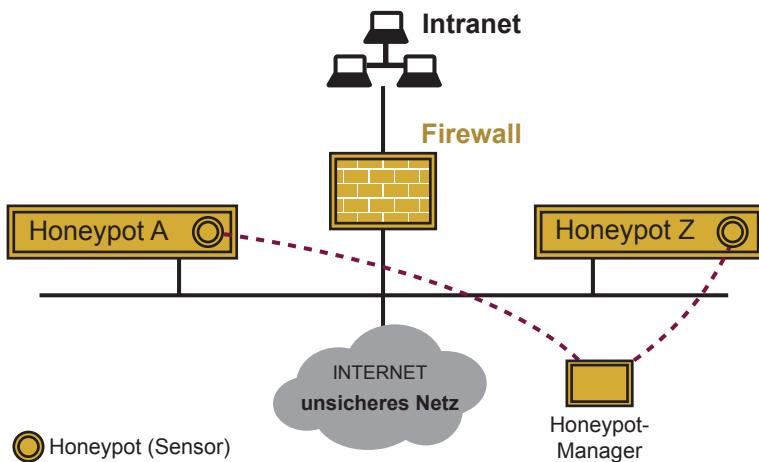
- alle Sicherheitsinformationen verfügbar
- nicht nur IT-Sicherheit, sondern auch Netzwerkinformationen

#### Nachteile:

- zu viele Informationen – Größe der Daten (100 M Bit/s ... ca. 1 T Byte/24 h)
- sehr komplex; nur manuelle Analyse

### 8.7.5 Honeypot-Sensor

Ein Honeypot ist eine Falle für Angreifer zum Erkennen und/oder Lernen von Angriffen. Ein Honeypot täuscht ein IT-System vor, das Informationen oder/und wertvolle Ressourcen für Angreifer enthält. Ein Honeypot-System hilft zu verstehen,



**Abb. 8.23** Honeypot Sensor

welche Arten von Angriffen aktuell umgesetzt werden (Malware, Exploits, Angriffsstrategien, ...). Je nach der notwendigen Interaktion des betreibenden Cyber-Sicherheitsexperten werden bei Honeypot „Low-Interaktion=Emulation“-Lösungen und „High-Interaktion=Full-Service-Stack“-Lösungen unterschieden. Honeypot ist ein passives Messverfahren. Der Anwender nutzt im Beispiel in Abb. 8.23 nicht genutzte öffentliche IP-Adressen, um Honeypots zu betreiben.

### Grundprinzip des Sensors

- P alle IP-Pakete  
und  
Ereignisse im IT-System (Betriebssystem, Anwendung, Daten, ...)
- D Teilmenge der Netzwerkdefinition der Regeln für die Protokollierung
- SI (D) Auswahl der Nutzung und Anzahl der Honeypot-Systeme
- Y detaillierte Angriffsspuren (Netzwerk/Host)

Analyse von Sicherheitsinformationen im Sensor- und Analysesystem

### Evaluierung von Honeypot

#### Genereller Aspekt:

- Alle Interaktionen mit Honeypots als „Fake-Services“ sind Angriffspotenziale, die der Angreifer auch auf einem echten IT-System durchgeführt hätte.

#### Ort der Messung:

- Netzwerk, separater Sensor

### Sicherheitsinformation: ++ (mittel)

Ein Honeypot misst keine realen Angriffe, sondern nur Angriffe auf einem „Fake-Service“. Die Informationen, die dabei gewonnen werden, zeigen aber in der Regel ein gutes Angriffspotenzial auf, daher werden die Sicherheitsinformationen mit mittel bewertet.

### Vorteile:

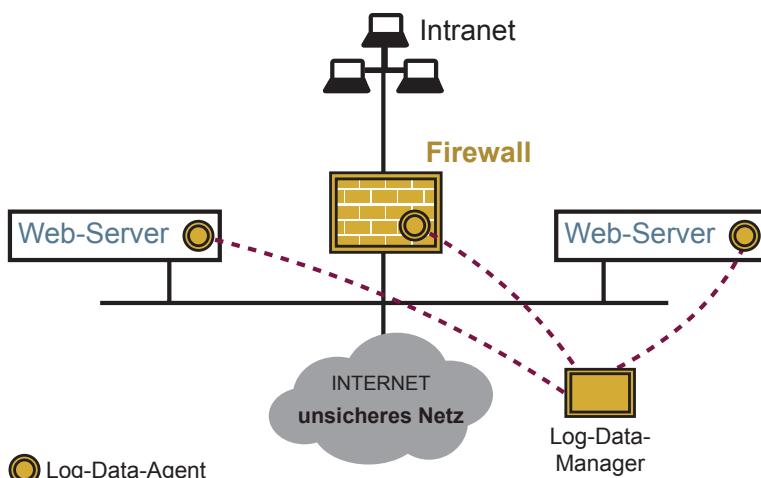
- qualitative Sicherheitsinformationen
- Angriffsmuster werden identifiziert und können genutzt werden, um sich besser zu schützen

### Nachteile:

- wartungsintensiv
- Angreifer sind in der Lage, Honeypots zu erkennen.

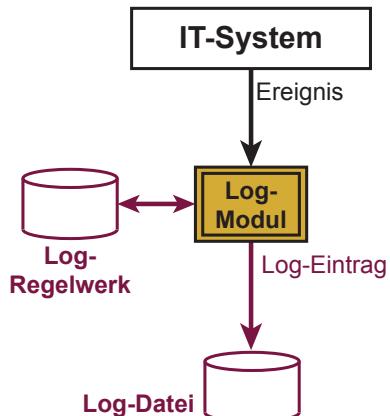
## 8.7.6 Logdaten-Sensor

Mithilfe von Logdaten-Sensoren (siehe Abb. 8.24) werden Ereignisse in einer Logdatei aufgezeichnet. Die Protokollierung von Ereignissen in eine Logdatei bietet einen Nachweis, mit dem die Aktivität und Abläufe eines IT-Systems nachvollzogen werden können. Mithilfe der Logdatei können Diagnosen von Problemen (Prozess, Cyber-Sicherheit, ...) durchgeführt werden. Es kann auch nützlich sein, Logeinträge von unterschiedlichen Quellen zu kombinieren. Beispiele von unterschiedlichen Quellen sind: Netzwerk, Betriebssystem, Anwendung und Daten, Webserver, Mail-Server, Firewall, DNS-Server, VoIP-Server usw.



**Abb. 8.24** Logdaten-Sensor

**Abb. 8.25** Log-Daten-Sensor



### Design einer Protokollierung von Aktivitäten in einem IT-System

Als erstes muss entschieden werden, welche Ereignisse in einem IT-System protokolliert werden können. Für die Protokollierung von sicherheitsrelevanten Informationen ist es wichtig zu definieren, welche Ereignisse hilfreich sind, um Angriffe zu identifizieren, Angriffsabläufe zu speichern, Lagebilder aufzuzeichnen usw. Dann muss dafür gesorgt werden, dass die entsprechenden Komponenten im IT-System diese Ereignisse mit weiteren Informationen auch generieren. Weitere Informationen sind: Welche Komponenten hat das Ereignis generiert, zu welchem Zeitpunkt, was sind die Kriterien, die zu diesem Ereignis geführt haben usw.

Das Log-Modul nimmt das Ereignis entgegen, prüft im Log-Regelwerk, was mit diesem speziellen Ereignis passieren soll, zum Beispiel als Log-Eintrag in die Log-Datei schreiben oder/und eine Alarmierung durch das Log-Modul an einen Cyber-Sicherheitsexperten senden. Im Log-Regelwerk steht die Policy, was mit Ereignissen gemacht werden soll, siehe Abb. 8.25.

### Grundprinzip des Sensors

- P Aktivitäten in den IT-Systemen
- D Ereignisse
- SI (D) Hängt von der Definition des Regelwerks ab  
(signatur- und anomaliebasierte Analyse)
- Y Logdatei (Logeinträge)

Analyse von Sicherheitsinformationen im Sensor- und Analysesystem.

### Evaluierung von Logdaten

#### Genereller Aspekt:

- Erzeugt einen Nachweis und hilft dabei, Aktivitäten (Angriffe) zu identifizieren und zu verstehen.

#### Ort der Messung:

- Netzwerk, Netzwerkkomponenten (Firewall, ...)
- IT-System (Betriebssystem, Anwendungen und Daten)

**Sicherheitsinformation:** +++(hoch)

In den Logdaten sind in der Regel sehr hilfreiche Sicherheitsinformationen enthalten. Daher wird die Bewertung auch mit hoch durchgeführt.

**Vorteile:**

- detaillierte Sicherheitsinformationen
- Angriffspfad kann analysiert werden
- erfolgreiche Angriffe können gespeichert und weiter analysiert werden
- die Logdaten können auch zur Beweissicherung genutzt werden

**Nachteile:**

- schwierige Definition der Ereignisse und ein optimaler Regelsatz
- Problem: in der Praxis sind nur ca. 5 % der Log-Einträge wichtig (sicherheitsrelevant)
- erfolgreiche Angriffe sind bereits umgesetzt, wenn sie protokolliert werden

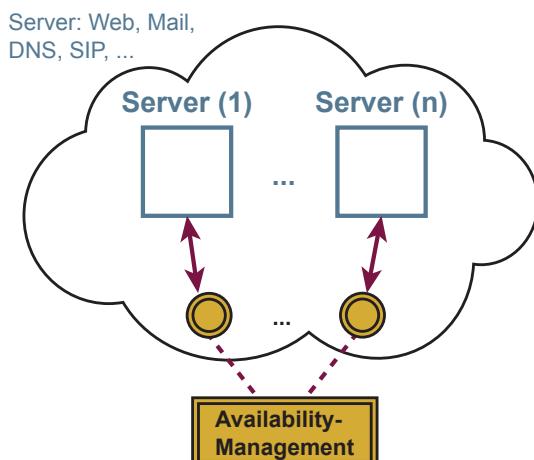
### 8.7.7 Verfügbarkeitssensor

Ein Verfügbarkeitssystem überwacht die Verfügbarkeit von IT-Systemen und -Diensten. Die Eigenschaften, die überwacht werden, sind:

- Quality of Service (Bandbreite, Jitter, Verzögerung, Paketverlustrate)
- Quality of Experience (Empfinden des Nutzer bezüglich der Verfügbarkeit).

Messwerkzeuge sind:

- Ping, Trace-Route, Ausführung von Anwendungen/Diensten, ....
- Der Verfügbarkeitssensor (siehe Abb. 8.26) ist ein aktives Messverfahren.



**Abb. 8.26** Verfügbarkeitssensor

### Grundprinzip des Sensors

- P      Verfügbarkeitsinformationen  
D      Quality of Service (QoS)- und Quality of Experience (QoE)-Parameter  
SI (D) Auswahl der gemessenen Parameter  
Y      Sicherheitsereignisse und/oder QoS/QoE-Parameter?

Analyse von Sicherheitsinformationen im Sensor- und Analysesystem

### Evaluierung von Logdaten

#### Genereller Aspekt:

- hilft, die Verfügbarkeit von IT-Systemen und -Diensten zu bewerten

#### Ort der Messung:

- Sensor im Netzwerk

#### Sicherheitsinformation: ++ (mittel)

Für das Cyber-Sicherheitsbedürfnis „Gewährleistung der Verfügbarkeit“ werden hilfreiche Sicherheitsinformationen zur Verfügung gestellt.

#### Vorteile:

- echte Sicherheitsinformationen für den Aspekt Verfügbarkeit

#### Nachteile:

- Kosten für zusätzlichen Netzwerkverkehr, CPU, ...

---

## 8.8 Analysekonzepte

Im Folgenden werden zwei Analysekonzepte vorgestellt und verglichen [2].

### 8.8.1 Erkennen von bekannten sicherheitsrelevanten Aktionen

Nach diesem Auswertungskonzept wird vorab festgehalten, welche bereits bekannten und hypothetischen sicherheitsrelevanten Ereignisse oder welche Folgen von sicherheitsrelevanten Ereignissen eine Sicherheitsverletzung, zum Beispiel einen Angriff, darstellen. Die unterschiedlichen Analysesysteme suchen dann nach solchen bekannten Ereignissen oder Ereignisfolgen. Diese Art wird auch signaturbasierte Erkennung oder Signaturverfahren bezeichnet.

Das Problem besteht darin, dass zwischen der neuen gefundenen Angriffsaktion und der Signatur, die zur Erkennung der neuen Angriffe verwendet wird, eine Verzögerung auftritt. Während dieser Zeitverzögerung kann die signaturbasierte Erkennung die Angriffe nicht identifizieren, was ein großes Cyber-Sicherheitsrisiko darstellt.

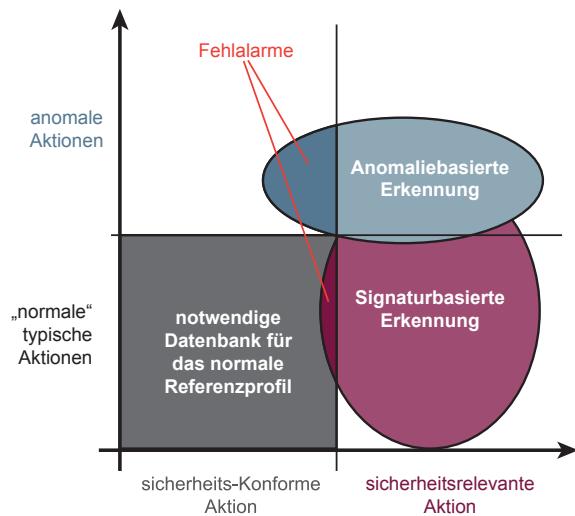
### 8.8.2 Erkennen von Anomalien

Bei diesem Auswertungskonzept sollen über das Erkennen von Anomalien – eine Abweichung vom Normalen – Sicherheitsverletzungen wie Angriffe entdeckt werden. Dieses Analysekonzept basiert auf der Annahme, dass Sicherheitsverletzungen, wie Angriffe anhand gravierender Verhaltensabweichungen erkannt werden können. Daher können mit dem Analysekonzept „Erkennen von Anomalien“ auch neue Angriffe erkannt werden. Solche Verhaltensabweichungen werden auf einzelne Nutzer, auf einzelne Programme, auf bestimmte Dienste oder auch auf Kommunikationsabläufe bezogen erkannt. Grundlage der Anomalie-Erkennung ist die Beschreibung des „normalen“, für einen Aspekt typischen regulären Verhaltens in sogenannten Referenzprofilen. Diese Referenzprofile sind charakteristische Verhaltensmuster, die anhand von objektiv überprüfbaren Merkmalen beschrieben werden. Diese Merkmale können dann entweder mithilfe von Statistiken über das tägliche Verhalten oder aufgrund individueller Erfahrungswerte ausgewählt werden [4].

#### Vergleich der verschiedenen Auswertungskonzepte

Beim Auswertungskonzept „Erkennen von bekannten sicherheitsrelevanten Aktionen“ wird als Ergebnis eine klare Aussage darüber getroffen, ob und welche Sicherheitsverletzung und/oder Angriff auftrat und erkannt wurde. Daraufhin können definierte Reaktionen eingeleitet werden. Das Auswertungskonzept „Erkennen von Anomalien“ hat den großen Vorteil, dass es durch die Art der Analyse gelingen kann, auch bislang unbekannte Sicherheitsverletzungen und Angriffe aufzuspüren, die von der direkten Angriffserkennung als solche nicht klassifiziert werden konnten. Damit kann dem Problem vorgebeugt werden, dass es sehr schwierig sein wird, ständig Informationen über neueste, hochaktuelle Angriffszenarien in Erfahrung zu bringen, diese zu analysieren, und für die direkte Angriffserkennung zu modellieren und eine Angriffssignatur zu definieren sowie den Sponsoren zur Verfügung zu stellen. Ein Nachteil dieses Auswertungskonzeptes ist, dass auch Fehlalarme generiert werden, siehe Abb. 8.27.

**Abb. 8.27** Analysekonzepte



Anomaliebasierte Erkennung bestimmt normale Netzwerkaktivität, insbesondere welche Bandbreite im Allgemeinen verwendet wird, welche Protokolle verwendet werden, welche Ports und IT-Systeme im Allgemeinen miteinander verbunden sind und warnt, wenn Verkehr erkannt wird, der anomaliert ist (nicht normal).

Die Abb. 8.27 zeigt deutlich, dass mehr sicherheitsgefährdende Aktionen erkannt werden, wenn beide Auswertungskonzepte gleichzeitig eingesetzt werden. Es wird ebenfalls dargestellt, wie anomale Aktionen erkannt werden, die keine Gefährdung der IT-Sicherheit bedeuten, aber Fehlalarme auslösen.

## 8.9 Cyber-Sicherheit-Frühwarnprozess

Im Folgenden wird exemplarisch ein Prozess beschrieben, wie ein Alarm einer automatischen Analyse bearbeitet werden kann und welche Tools und Vorgehensweisen dabei sinnvoll sind, siehe Abb. 8.28.

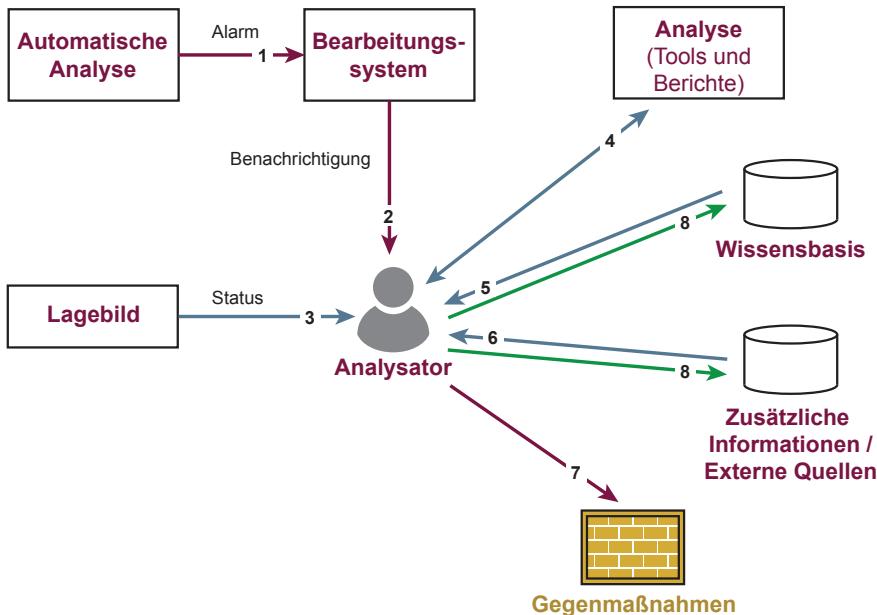


Abb. 8.28 Frühwarnprozess

### **Exemplarischer Ablauf eines Frühwarnprozess**

1. Zuerst wird ein Vorfall mithilfe eines Sensors erkannt und ein Alarm wird generiert.
2. Dann erhält der Cyber-Sicherheitsexperte eine Benachrichtigung mit einigen Hintergrundinformationen, beispielsweise per E-Mail.
3. Danach kann sich der Cyber-Sicherheitsexperte das aktuelle Lagebild ansehen, um einen ersten Überblick über die Lage zu erhalten.
4. Mithilfe zusätzlicher Analysetools kann die Situation genauer analysiert werden.
5. Außerdem ist es möglich, auf die interne Wissensbasis zuzugreifen (Hinweise zur Lösung der Probleme mit positiven Erfahrungen aus der Vergangenheit)
6. Es ist auch möglich, auf weitere Wissensbasen und externe Quellen zuzugreifen. Das ist nötig, wenn lokale Systeme nicht genügend Informationen liefern, um das Problem zu lösen.
7. Nachdem die Ursache analysiert werden konnte, können Gegenmaßnahmen eingeleitet werden.
8. Wenn das Problem gelöst ist, werden die Wissensbasis und andere Informationsquellen aktualisiert. Neu erfahrenes Wissen über Angriffe und/oder pragmatische Lösungen, um diese zu beheben, werden festgehalten und anderen mitgeteilt.

---

## **8.10 Kommunikationslagebild**

Im diesem Abschnitt wird das Thema Kommunikationslagebild behandelt und aufgezeigt, wie dies helfen kann, die Risiken nachhaltig zu reduzieren. Die Herausforderung dabei ist, eine sehr gute Sichtweise über die gesamte Kommunikationslage zu erlangen, Wissen über die eigene Kommunikation und die verwendeten IT-Technologien aufzubauen und zu nutzen, aus der Vergangenheit zu lernen sowie mit anderen zusammenzuarbeiten, um aus den Erkenntnissen angemessene Gegenmaßnahmen einzuleiten.

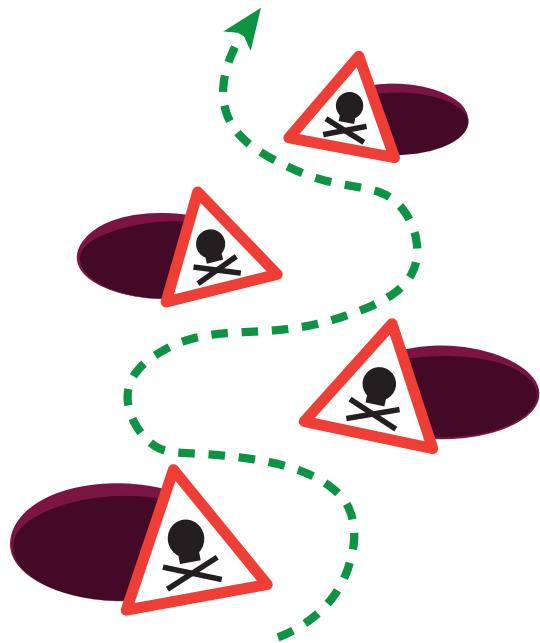
### **Erkennen von Angriffspotenzialen**

Die größte Gefahr besteht immer dann, wenn Angriffspotenziale falsch eingeschätzt werden. Wer die Gefahren hingegen kennt, kann sich und seine Werte besser schützen, siehe die Idee in Abb. 8.29. Mithilfe eines Kommunikationslagebildes sollen Angriffe auf die IT-Systeme und Werte einer Organisation erkannt sowie Schwachstellen der benutzten IT-Technologien und Internet-Protokolle aufgezeigt werden. So lässt sich ein wirkungsvolles und nachhaltiges Schutzkonzept entwickeln.

Dies wird ermöglicht mit den drei wichtigsten Kernaspekten:

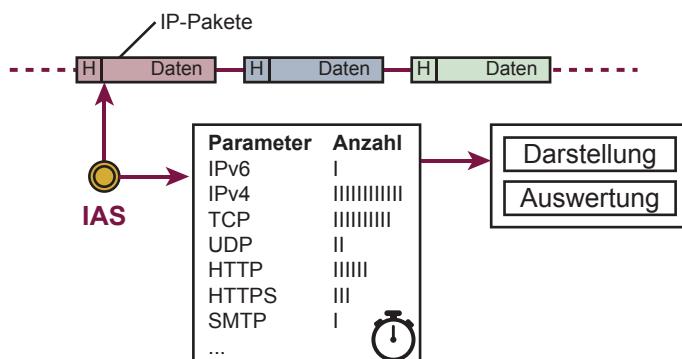
1. Angriffe und Schwachstellen müssen zuerst identifiziert werden.
2. Die daraus resultierenden Angriffspotenziale müssen bewertet werden.
3. Nach Identifikation und Bewertung können Risiken gezielt angegangen und auf ein angemessenes Maß minimiert werden.

**Abb. 8.29** Gefahr erkannt,  
Gefahr gebannt



### Generierung eines Kommunikationslagebildes

Als ein Beispiel wird ein vollständiges Kommunikationslagebild mithilfe des Internet-Analyse-Systems (IAS) unter Verwendung eines speziellen IAS-Sensors ermittelt, der in der Regel zwischen dem Unternehmensnetzwerk und dem Internet positioniert ist. Der Netzwerk-Sensor ist in der Lage, mehr als 4.000.000 potenzielle Kommunikationsmerkmale in den Kommunikationspaketen zu identifizieren und dann zu zählen. Das funktioniert wie bei einer Strichliste. Wenn das Kommunikationsmerkmal vom Netzwerk-Sensor festgestellt wird, dann wird dieses Ereignis mithilfe eines Zählers gezählt. Ein Kommunikationsmerkmal kann ein Kommunikationsparameter oder eine Verknüpfung von verschiedenen Kommunikationsparametern sein. In der Abb. 8.30 sind exemplarisch IPv6,



**Abb. 8.30** Prinzip der Extrahierung der sicherheitsrelevanten Informationen

IPv4, TCP, UDP, HTTP, HTTPS und SMTP, sieben der 4.000.000 möglichen Kommunikationsmerkmale, dargestellt [3].

Mit diesem Prinzip werden die sicherheitsrelevanten Informationen aus dem Datenstrom extrahiert. Wichtig ist, dass so viele sicherheitsrelevante Informationen wie möglich festgehalten werden. Außerdem ist es wichtig, dass der Grad der Reduzierung der Bytes der eigentlichen Kommunikationsdaten und der sicherheitsrelevanten Informationen sehr groß ist, um diese langfristig nutzen zu können. Beim IAS hat sich herausgestellt, dass eine Zählzeit der Strichliste von 5 min ideale Werte erbringt. Bei einer typischen IAS-Sonde werden so ca. 10 G Byte Daten pro Jahr gesammelt. Das Prinzip der Ermittlung der Kommunikationsmerkmale ist dabei datenschutzkonform. Das heißt, es werden keine Nutzerdaten, IP-Adressen oder sonstige personenbezogenen oder -beziehbare Informationen bewertet.

Die Kommunikationsmerkmale zeigen dabei sicherheitsrelevante Informationen über verschiedene Aspekte wie vorbereitende Angriffe (Ports, SYS-ACK usw.), genutzte Technologien (User-Agent, Versionen von Technologien und Standards usw.) und die Nutzung/Verteilung von Protokollen und Anwendungen an. Dadurch erlauben sie, die Kommunikationslage zu ermitteln, darzustellen und zu bewerten. Erst durch diese Maßnahme wird wirklich zu jedem Zeitpunkt live und nachhaltig sichtbar, was im eigenen Netzwerk eigentlich passiert und welche Technologien und Protokolle daran beteiligt sind.

Das Kommunikationslagebild zeigt nicht nur die Cyber-Sicherheitsprobleme, sondern die Gesamtlage, also auch den Anteil sicherer Eigenschaften der IT-Infrastruktur. Aus diesem Grund kann das Kommunikationslagebild auch als Darstellung des Gesundheitszustandes des eigenen Netzwerkes und der daran angeschlossenen IT-Systeme betrachtet werden.

## Ziele des Kommunikationslagebildes

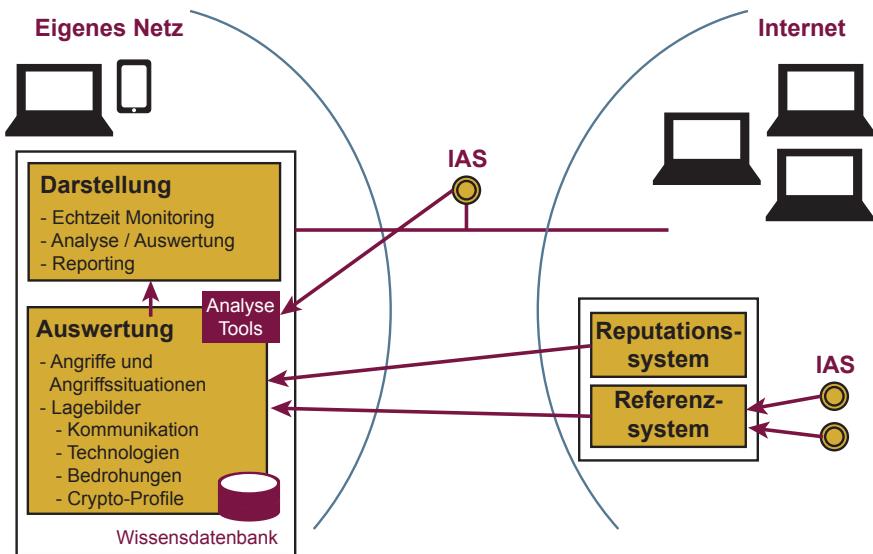
Mit der Hilfe des Kommunikationslagebildes können mehrere Ziele erreicht werden:

### **1. Erkennen von Angriffen und Angriffspotenzialen**

Mithilfe einer Anomalie- oder Angriffssignaturerkennung werden Angriffe und Angriffspotenziale aus den Kommunikationsmerkmalen identifiziert und dargestellt. Dies stellt oftmals den ersten Ansatz dar, um Ursprung und Ziel des Angriffes nach und nach einzugrenzen: Damit können im späteren Verlauf die relevanten Kommunikationsmerkmale zur Auswertung festgelegt werden.

### **2. Analyse und Auswertung der Angriffen und Angriffspotenzialen**

Dank der Analyse und Auswertung der Angriffe und Angriffspotenziale werden weitere Sichtweisen und Hilfestellungen umgesetzt, um ein besseres Verständnis über die Kommunikationslage zu erhalten. Auf Basis detaillierter Analysen bestimmter Angriffe und Angriffspotenziale wird anhand eines Favoriten-systems eine schnelle Übersicht mit den relevanten Kommunikationsmerkmalen erstellt. Das IAS-System ist dank einer Wissensdatenbank lernfähig. Es lässt Erfahrungen und bereits vergangene Angriffe in die Analyse einfließen, um schnell Abweichungen vom Normalzustand festzustellen.



**Abb. 8.31** Funktionsübersicht des Internet-Analyse-Systems

### 3. Übersicht und Bewertung der Kommunikationslage

Um eine effektive Übersicht der Kommunikationslage zu erhalten, wird zum einen ein „Echtzeit-Monitoring“ bereitgestellt, das den Ist-Zustand der Kommunikationslage grafisch darstellt. Zum anderen wird ein „Reporting“ verwendet. Dieses führt eine Bewertung der Kommunikationslage mithilfe eines Reputationssystems durch, bei dem Parameter durch bekannte Reputationsdaten anhand eines Ampelsystems eingeordnet werden.

#### Funktionsübersicht des Internet-Analyse-Systems

In Abb. 8.31 ist eine Funktionsübersicht des Internet-Analyse-Systems dargestellt.

##### 1. Darstellung der Ergebnisse des Internet-Analyse-Systems

Mithilfe des „Echtzeit-Monitorings“ wird der Ist-Zustand der Kommunikationslage dargestellt. Damit ist es immer möglich, einen schnellen, intuitiven Überblick über die aktuelle Kommunikationslage zu bekommen.

Mit der „Analyse und Auswertung“ können Angriffe und Angriffspotenziale analysiert und ausgewertet werden, um die richtigen Entscheidungen treffen zu können.

Das „Reporting“ hilft regelmäßig, eine strukturierte und bewertete Darstellung der Kommunikationslage zu erlangen, um auf dieser Basis mittelfristige Entscheidungen für mehr Sicherheit treffen zu können. Die Reports können in wählbaren zeitlichen Abständen abonniert und per E-Mail verteilt werden. Durch die Art der Verteilung können die intelligenten und übersichtlichen E-Mail-Reports auch einfach weitergeleitet werden.

## **2. Auswertung**

Das Internet-Analyse-System hat vielfältige Analyse-Tools, mit denen die unterschiedlichsten Berechnungen für die Angriffe und Angriffspotenziale, Heuristiken von besonderen Darstellungen usw. umgesetzt werden können. Die Wissensdatenbank repräsentiert die Historie von Mess- und Analyseergebnissen.

## **3. Reputationssystem**

Das Kommunikationslagebild zeigt auf, welche Technologien (Browser, Betriebssysteme, Sicherheitstools, ...), Anwendung von Verschlüsselung (HTTPS, IMAPS, POP3S, SMTPS, IPSec, ...), Verwendung von kryptografischen Profilen (SSL/TLS, ...) usw. verwendet werden. Mithilfe eines Reputationssystems werden diese Aspekte bewertet. Verwendete Browser, die nicht aktualisiert sind oder derzeit kritische Schwachstellen beinhalten, werden rot gekennzeichnet. Verwendete Browser, die aktuell sicher sind, werden grün dargestellt. Protokolle, die bekanntlich überwiegend für Angriffe verwendet werden, sind entsprechend rot gekennzeichnet. Das Gleiche gilt für verwendete Kryptoprofile, Sicherheitstechnologien usw. Damit das Reputationssystem diese Bewertung umsetzen kann, werden die dazu notwendigen Informationen teilautomatisiert beschafft und in das Reputationssystem eingepflegt.

## **4. Referenzsystem (globale Sichtweise)**

Das Kommunikationslagebild zeigt einen klaren Sachverhalt über die Nutzung von Kommunikationsmerkmalen, die für die Bewertung der Sicherheit über den positiven Kommunikationsablauf notwendig sind. Bei der Identifizierung von besonderen Situationen, wie Angriffe, Gefahren und sonstigen Besonderheiten, fällt es aber oft sehr schwer, eine richtige Einschätzung durchführen zu können. Beispiel: Ist die Identifikation von Scan-Angriffen auf Port 80 (HTTP) von 130 % normal oder die Basis eines gezielten Angriffes? Wenn bei solchen Werten Referenzwerte von anderen Organisationen (zum Beispiel insgesamt in Deutschland, in bestimmten Branchen, ...) zur Verfügung ständen, dann könnten eigene Ergebnisse besser bewertet werden. Aus diesem Grund ergibt sich die Idee der globalen Sichtweise: Organisationen tauschen wichtige Kommunikationsmerkmale anonymisiert aus, in einer Zentrale, die diese Werte statistisch berechnet und wieder an alle verteilt. Diese stehen dann als Referenzwerte für die eigene Bewertung zur Verfügung. Dies geschieht immer vollständig anonym.

## **Beispiele für die Bewertung der Kommunikationslage**

### ***Nutzung und Verteilung von aktuell verwendeten Technologien***

Die Kommunikationslage stellt die reale Nutzung von aktuell verwendeten Technologien und Internet-Protokollen dar. Eine große Gefahr entsteht erst durch die Nutzung veralteter oder nicht aktualisierter Software, wie zum Beispiel Betriebssysteme, Browser, Sicherheitstools usw., da sie oft Einfallstore für Angreifer bieten. Gerade für Unternehmen, deren Mitarbeiter ihre eigenen IT-Systeme bei der Arbeit benutzen, ist schwer nachzuhalten, welche Software

**Abb. 8.32** Genutzte TLS/SSL-Technologie

TLS-Version	Pakete	
	Anzahl	%
SSL Version SSL 2.0	0	0,00
SSL Version SSL 3.0	25.989	0,12
SSL Version TLS 1.0	10.154.344	48,42
SSL Version TLS 1.1	608.026	2,90
SSL Version TLS 1.2	10.182.293	48,55
SSL Version Other	0	0,00
<b>Gesamt</b>	<b>20.970.652</b>	<b>100,00</b>

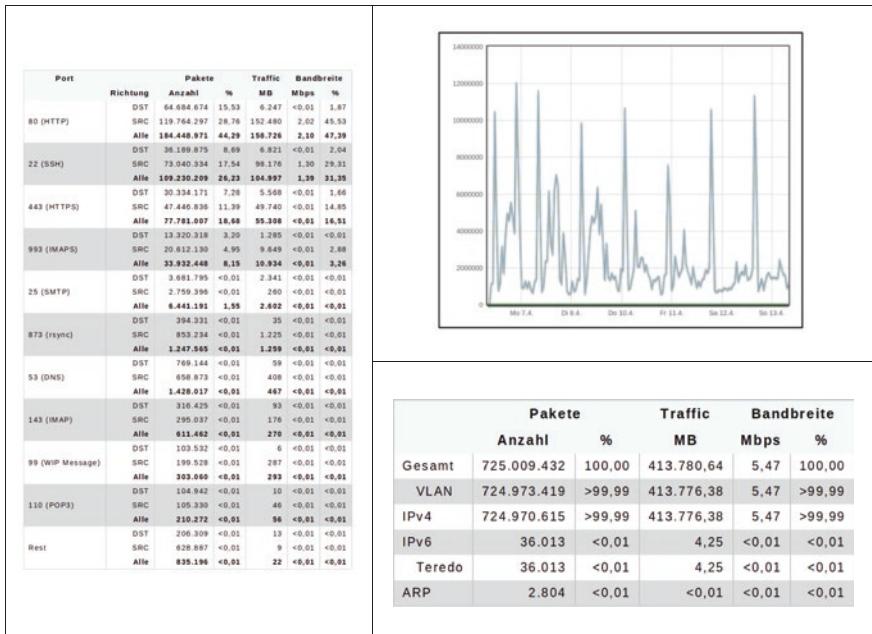
tatsächlich verwendet wird und was sich noch alles für potenzielle Bedrohungen auf diesen IT-Systemen befinden. Das IAS stellt dar, wie viele dieser Lücken an welcher Stelle vorhanden sind. Es wird auch erfasst, ob überhaupt verschlüsselt wird und welche kryptografischen Profile dabei genutzt werden. Dazu wird das Reputationssystem genutzt, welches Aussagen über die Cyber-Sicherheit von Protokollen, Technologien, Crypto-Profilen usw. zur Verfügung stellt.

Das BSI hat zum Zeitpunkt der dargestellten Messungen die Nutzung der TLS/SSL Version 1.2 (Beispiel für eine Referenz). In Abb. 8.32 ist zu sehen, dass bei diesem Netzwerk mehr als 50 % der IT-Systeme diese Sicherheitstechnologie noch nicht nutzen. Mit dieser Information kann die Lage nun definiert und ein Technologiewechsel umgesetzt werden, um das Risiko zu minimieren.

In Abb. 8.33 wird zum Beispiel ersichtlich, dass die „Protocol number 50 (ESP Mode von IPsec“ zu 0,8 % verwendet wird. Dies bedeutet, dass jedes 125. IP Paket IPsec verschlüsselt wird.

IP Protokollnummer	Pakete		Traffic		% Bandbreite
	Anzahl	%	MB	Mbps	
Protocol number 6 (TCP)	468.472.020	64,62	358.462	4,74	86,63
Protocol number 17 (UDP)	237.139.295	32,71	53.729	0,71	12,99
Protocol number 1 (ICMP)	18.914.729	2,61	1.582	0,02	0,38
Protocol number 50 (ESP)	5.799.799	0,8	<1	<0,01	<0,01
Protocol number 2 (IGMP)	4.431	<0,01	2	<0,01	<0,01
Protocol number 132 (SCTP)	12	<0,01	<1	<0,01	<0,01
Protocol number 46 (RSVP)	1	<0,01	<1	<0,01	<0,01
Rest	0	0,00	0	0,00	0,00
<b>Gesamt</b>	<b>724.974.918</b>	<b>100,00</b>	<b>413.776</b>	<b>5,47</b>	<b>100,00</b>

**Abb. 8.33** Verteilung der IP-Portnummern

**Abb. 8.34** Nutzung und Verteilung von Protokollen

### Nutzung und Verteilung von aktuell verwendeten Internet-Protokollen

Mithilfe des Kommunikationslagebildes können wir die Nutzung und Verteilung der Internet-Protokolle darstellen. Abb. 8.34 zeigt einige Beispiele.

In Abb. 8.34 rechts oben ist der sehr dominante Wochenverlauf des Kommunikationsmerkmals IPv4 zu erkennen. Der typische Tagesverlauf ist erkennbar, aber auch, dass der Verkehr am Wochenende geringer ausfällt. Unten rechts ist die Nutzung von IPv4, IPv6 und ARP zu erkennen. Hier werden die Anzahl der identifizierten Pakete, der Traffic in MByte und die Bandbreite dargestellt. Links kann die Verteilung der Anwendungsprotokolle analysiert werden. Port 80 (HTTP) ist mit 47 % das meist genutzte Protokoll. DST und SRC geben einen Hinweis darüber, wie viele Pakete vom Netzwerk in das Internet gesendet worden sind und wie viele vom Internet in das Netzwerk übertragen wurden.

In Abb. 8.35 werden Traffic-Arten mithilfe einer Heuristik berechnet und dargestellt. Server-to-Client zeigt die Angabe vom Server zum Client

Traffic-Art	Pakete		Traffic		Bandbreite	
	Anzahl	%	MB	Mbps	%	
Src >= 1024 and Dst >= 1024 ("P2P") - client-to-client	49.922.825	10,66	23.096	0,31	6,44	
Src < 1024 and Dst < 1024 ("B2B") - server-to-server	326.388	0,07	22	<0,01	<0,01	
Src >= 1024 and Dst < 1024 ("P2B") - client-to-server	152.183.466	32,49	22.752	0,30	6,35	
Src < 1024 and Dst >= 1024 ("B2P") - server-to-client	266.037.102	56,79	312.589	4,13	87,20	
<b>Gesamt</b>	<b>468.469.781</b>	<b>100,00</b>	<b>358.458</b>	<b>4,74</b>	<b>100,00</b>	

**Abb. 8.35** Nutzung und Verteilung von Übertragungsarten

und Client-to-Server die umgekehrte Richtung. Client-to-Client stellt eine Peer-to-Peer-Kommunikation dar. Dies könnte zum Beispiel das illegale Downloaden von Inhalten sein.

### Besondere Eigenschaften des Internet-Analyse-Systems

Die IAS-Sonden liefern eine Übersicht der Netzwerkaktivitäten und werten den Datenverkehr von einer rein passiven Position aus. Zudem ist der Datenschutz von Beginn des Internet-Analyse-Systems ein sehr wichtiges Thema gewesen und Bestandteil der Entwicklung: Es ist nicht möglich, Netzteilnehmer in irgendeiner Form zu überwachen oder Rückschlüsse mithilfe von Profilbildung auf Verhalten oder Metadaten zu ziehen. Das Surfverhalten einzelner Nutzer wird nicht aufgezeichnet, eine Mitarbeiterüberwachung ist ausgeschlossen.

**Wichtig** Die Cyber-Sicherheitsprobleme steigen ständig und damit auch das Risiko eines Schadens. Mithilfe eines Kommunikationslagebildes ist es möglich, den Gesundheitszustand des eigenen Netzwerkes und der daran angeschlossenen IT-Systeme zu analysieren und zu bewerten.

---

## 8.11 Zusammenfassung

In diesem Kapitel wurden Grundstrukturen, Konzepte, Elemente, Prozesse und die Bedeutung Cyber-Sicherheit-Frühwarn- und Lagebildsysteme dargestellt und diskutiert.

---

## 8.12 Übungsaufgaben

### Übungsaufgabe 1

Wozu werden Advanced Evasion Techniques (AETs) verwendet?

### Übungsaufgabe 2

Welches Sicherheitsproblem kann bei dem Analysekonzept „Erkennen von bekannten sicherheitsrelevanten Aktionen“ auftreten?

### Übungsaufgabe 3

Welchen Vorteil hat das Analysekonzept „Erkennen von Anomalien“?

**Übungsaufgabe 4**

Was ist der grundlegende Unterschied zwischen den Daten, die ein Logdaten-Sensor liefert, im Gegensatz zu einem Netzwerk-Sensor?

**Übungsaufgabe 5**

Bewerten Sie die folgenden Situationen in einem Netzwerk. Welche Sensoren hätten geholfen, um diese Situationen zu erkennen/zu verstehen.

*Fall 1:*

Ein Angreifer baut tausende Verbindungen zu Ihrem Web-Server auf und versucht, das Passwort eines Accounts Ihres Mitarbeiters zu erraten.

*Fall 2:*

Auf einem IT-System in einem Unternehmen wurde Schadsoftware gefunden. Sie sollen den Netzwerkverkehr der Schadsoftware im Detail analysieren. Welcher der vorgestellten Sensoren eignet sich hier am besten?

**Übungsaufgabe 6**

Welche beiden besonderen Herausforderungen hat ein Sensor bezüglich der Output-Daten?

**Übungsaufgabe 7**

Betrachten Sie die folgenden Situationen. Warum können Frühwarnsysteme diese Probleme nicht lösen?

*Fall 1:*

Einem Mitarbeiter im Unternehmen wurde das Passwort gestohlen. Der Angreifer loggt sich mit dem gestohlenen Passwort in das E-Mail-Konto ein und stiehlt alle Mails des Mitarbeiters.

*Fall 2:*

Ein Angreifer hinterlegt einen manipulierten USB-Stick in der Lobby eines Unternehmens. Die Mitarbeiterin an dem Empfang findet den USB-Stick und schließt diesen an ihrem IT-System an, um zu prüfen, was auf dem USB-Stick gespeichert ist. Dabei wird Ihr IT-System von einer Malware infiziert.

## Übungsaufgabe 8

Bitte kreuzen Sie Ihre Antworten an!

		Cyber-Sicherheitsmechanismen
		Cyber-Sicherheit Frühwarnsystem
Gewährleistung von Cyber-Sicherheitsbedürfnissen	Vertraulichkeit	
	Authentifikation	
	Authentizität	
	Integrität	
	Verbindlichkeit	
	Verfügbarkeit	
	Anonymisierung/Pseudonymisierung	
Cyber-Sicherheitsstrategien	Vermeiden von Angriffen	
	Entgegenwirken von Angriffen	
	Erkennen von Angriffen	

Ergebnisse siehe: <https://norbert-pohlmann.com/cyber-sicherheit/uebungen/>.

---

## Literatur

1. Petersen D, Pohlmann N (2011) Ideales Internet-Frühwarnsystem. DuD Datenschutz und Datensicherheit 2011(2):241–246
2. Pohlmann N (2003) Firewall-Systeme – Sicherheit für Internet und Intranet, E-Mail-Security, Virtual Private Network, Intrusion Detection System, Personal Firewalls, 5. aktualisierte u. erweiterte Aufl. MITP-Verlag, Bonn
3. Petersen D, Pohlmann N (2015) Die Kommunikationslage. WISU 44(4):476–481
4. Sobirey M (1999) Datenschutzorientiertes Intrusion Detection. Vieweg-Verlag, Wiesbaden
5. Goll, Grüner, Landwehr, Steiner (2000). Netzwerkmanagement: Einführung in das Management verteilter Systeme



Ein Firewall-System ist ein Cyber-Sicherheitsmechanismus, der zwischen verbundenen Netzen Sicherheitsdomänen mit unterschiedlichem Schutzbedarf schafft.

Es wird meist zum Schutz eigener Netze vor Gefahren aus unsicheren Netzen wie dem Internet, aber auch zur Strukturierung eigener Netze in einer Organisation eingesetzt.

Dabei müssen unterschiedliche Aspekte berücksichtigt werden, damit mithilfe eines Firewall-Systems das gewünschte Sicherheitsmaß auch erreicht werden kann [1].

**Wichtig** Mithilfe eines Firewall-Systems kann der Übergang zwischen einem unsicheren und einem zu schützenden Netz sicherer gestaltet werden.

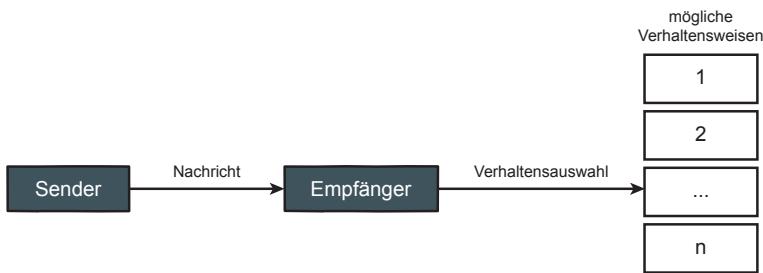
## 9.1 Bedrohungen im Netz

Im folgenden Abschnitt werden die potenziellen Bedrohungen, die in Netzen wie dem Internet wirken, beschrieben. Außerdem werden gezielte Angriffe dargestellt, die auf der TCP/IP-Technologie beruhen, und prinzipielle Möglichkeiten, diesen Angriffen mithilfe von Firewall-Systemen entgegenzuwirken.

### 9.1.1 Angriffsmöglichkeiten in Kommunikationssystemen

Eine starke Bedrohung zielt auf das Kommunikationssystem, das heißt, auf die Nachrichten, die über Kommunikationssysteme wie Internet ausgetauscht werden.

Auf eine Nachricht (ein oder mehrere IP-Pakete) reagiert ein Empfänger mit einem bestimmten Verhalten, siehe Abb. 9.1.



**Abb. 9.1** Reaktionsmöglichkeiten des Empfängers einer Nachricht

Ein Angreifer, der die Kommunikationsverbindung abhört, kann das Verhalten des Empfängers und des Senders interpretieren. Der Angreifer kann die Reaktionen des Empfängers zielgerichtet beeinflussen, wenn er die Möglichkeit hat, die Nachricht zu wiederholen, zu verändern, zu löschen oder zu ergänzen.

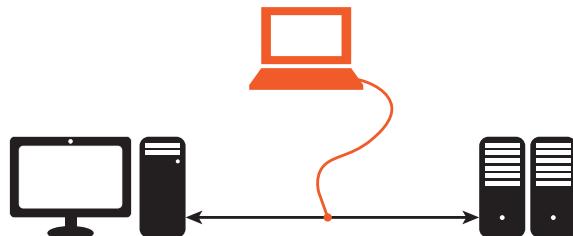
Aus dieser Überlegung heraus werden grundsätzlich zwei Bedrohungarten unterschieden: passive Angriffe und aktive Angriffe.

### 9.1.2 Passive Angriffe

Bei passiven Angriffen werden die übertragenen Nachrichten und der Betrieb des Kommunikationssystems nicht geändert. Passive Angriffe sind Bedrohungen, die vom Angreifer bewusst und gezielt durchgeführt werden, um sich unerlaubt Informationen zu beschaffen.

Passive Angriffe können zum Beispiel durch das Abhören der Leitung oder durch das Abfangen der Signale über die Luft durchgeführt werden. Ein passiver Angreifer bleibt oft gänzlich oder zumindest für lange Zeit unentdeckt und kann so latent über einen längeren Zeitraum großen Schaden anrichten, siehe Abb. 9.2.

**Abb. 9.2** Passive Angriffe auf Nachrichten oder auf das Kommunikationssystem



Es werden die folgenden passiven Angriffsarten unterschieden:

### Abhören von Daten

Ein Abhörende gelangt unmittelbar in den Besitz der Nachricht und kann sie zu seinem Zweck verwerten. Zum Beispiel kann ein Angreifer bei einer unverschlüsselten IP-Verbindung zwischen einem Webserver und einem Client während der Log-in-Prozedur den Nutzernamen und das Passwort eines Nutzers abhören und später mit diesen Zugangsinformationen unerlaubt Zutritt zum Webserver erlangen.

Weitere Beispiele sind das Abhören von vertraulichen Informationen, wie Entwicklungsunterlagen von neuen Produkten, oder das Abhören von Daten, die unter die EU-Datenschutzgrundverordnung fallen. Diese Angriffe sind prinzipiell problemlos durchführbar.

### Abhören der Nutzer-Identitäten

Der Lauscher erfährt, welche Nutzer oder IT-Systeme untereinander eine Datenverbindung aufbauen und Daten austauschen. Allein aus der Kenntnis, wer mit wem zu welchem Zeitpunkt Nachrichten ausgetauscht hat, sind oft Rückschlüsse auf den Inhalt der Nachricht oder das Verhalten der Nutzer möglich. Wenn jemand zum Beispiel auf die WWW-Seiten eines Waschmaschinenherstellers zugreift, kann vermutet werden, dass er eine Waschmaschine kaufen wird.

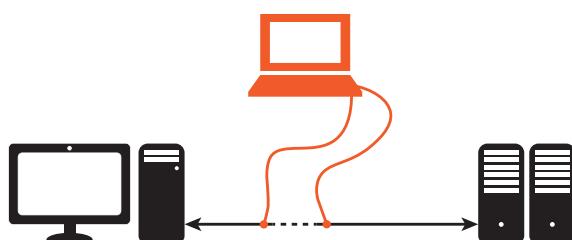
### Verkehrsflussanalyse

Auch wenn die Daten verschlüsselt sind, ist es einem Abhörenden möglich, durch eine „Verkehrsflussanalyse“ gewisse Informationen zu erhalten, wie zum Beispiel Größenordnungen, Zeitpunkte, Häufigkeit und Richtung des Datentransfers. Diese Informationen können für bestimmte spezielle Anwendungen interessant sein, zum Beispiel für Börsen-Transaktionen oder militärische Operationen.

### 9.1.3 Aktive Angriffe

Neben der Gefahr, abgehört zu werden, besteht die Möglichkeit von aktiven Angriffen, die den Nachrichtenstrom und/oder den Betrieb der Kommunikation verfälschen. Aktive Angriffe werden zum Beispiel durch Auf trennen der Übertragungsleitungen oder mithilfe der Emulation von Übertragungsprotokollen durchgeführt, siehe Abb. 9.3.

**Abb. 9.3** Aktive Angriffe



Bei aktiven Angriffen wird grob unterschieden zwischen Bedrohungen durch Dritte und Bedrohungen durch den Kommunikationspartner.

Bedrohungen durch Dritte sind zum Beispiel:

### **Wiederholen oder Verzögern von Informationen**

Durch Wiederholen oder Verzögern von Informationen kann der Empfänger irritiert oder zu einer falschen Aktion veranlasst werden. Beispiel: Mehrfache Überweisung eines Geldbetrages oder Wiederholung eines abgefangenen Log-ins.

### **Einfügen und Löschen bestimmter Daten**

Um ein IT-System zu manipulieren, fügt ein Angreifer bestimmte Nachrichten oder Daten innerhalb der Nachrichten ein oder löscht sie. Ein Empfänger kann durch Unterdrückung oder zusätzlichen Empfang entscheidender Informationen zu einem falschen Verhalten veranlasst werden. Beispiel: In der E-Mail „Kaufen Sie keinesfalls neue Aktien“ wird das Wort „keinesfalls“ während der Übertragung gelöscht, sodass der Empfänger die Instruktion „Kaufen Sie neue Aktien“ erhält.

### **Modifikation von Daten**

Modifikation von Daten bedeutet, dass die Veränderung der Daten von den Kommunikationspartnern nicht erkannt wird. Durch Ändern der Daten während der Datenübertragung ist es dem Angreifer möglich, falsche Aktionen zu veranlassen. Beispiel: Die Veränderung einer Kontonummer bei einer Geldüberweisung führt dazu, dass ein anderer als der intendierte Empfänger das Geld bekommt.

### **Boykott des Kommunikationssystems (Denial of Service)**

Wenn der Umfang von eingefügten oder unterdrückten Daten zu groß wird oder realzeitorientierte Daten zu lange verzögert werden, kann hierdurch das gesamte Kommunikationssystem boykottiert werden. Beispiel: Durch permanenten Verbindungsaufbau zu einem bestimmten Server kann dieser blockiert und isoliert werden (siehe auch Kap. 12 „Cyber-Sicherheitsmaßnahmen gegen DDoS-Angriffe“).

Bedrohungen durch den Kommunikationspartner sind zum Beispiel:

### **Vortäuschung einer falschen Identität (Maskerade-Angriff)**

Wenn sich ein Nutzer für einen anderen ausgibt, kann er sich Informationen erschleichen, die für diesen anderen Nutzer bestimmt waren, oder Aktionen auslösen, die nur der andere Nutzer veranlassen darf. Beispiel: Ein Nutzer verschafft sich unerlaubt Zugang zu einer Datenbank.

### Leugnen einer Kommunikationsbeziehung

Der steigende Einsatz von Datenkommunikation zur Abwicklung vertraglich relevanter Vorgänge erfordert, dass sowohl der Sender einer Nachricht nicht leugnen kann, der Sender zu sein, als auch der Empfänger nicht abstreiten kann, die Nachricht erhalten zu haben.

Beispiele: Bestellung von Waren über das Internet bei einem Händler oder Abschluss von Verträgen über das Internet.

### Trittbrettfahrer (Man in the middle)

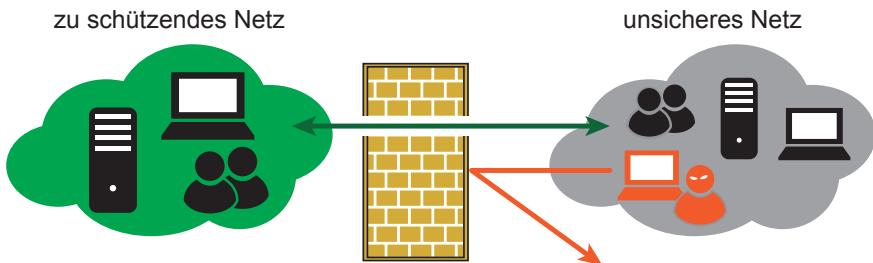
Sogenannte Trittbrettfahrer hängen sich zum Beispiel an einen Knoten (Router oder IT-System) im Internet und verfolgen einen Verbindungsaufbau mit. Die Verbindung wird dann nach der Authentifikation des Nutzers für eigene Zwecke genutzt.

Mit dieser Methode können IT-Systeme, auf die eigentlich kein Zugriff möglich ist, manipuliert und Authentifikationsprozesse (auch kryptografische Methoden) unterlaufen werden.

## 9.2 Idee und Definition von Firewall-Systemen

Ein Firewall-System sichert und kontrolliert den Übergang von einem zu schützenden Netz zu einem unsicheren Netz, wie dem öffentlichen Internet. Ein Firewall-System lässt erlaubte Kommunikation durch (grün) und blockiert nicht gewünschte (orange), siehe Abb. 9.4.

**Wichtig** Firewall-Systeme schotten IT-Bereiche ab, um Schäden zu minimieren.



**Abb. 9.4** Idee eines Firewall-Systems

Dabei muss ein Firewall-System analog zu herkömmlichen Sicherheitseinrichtungen für physikalische Objekte (Gebäude) zwei Aspekte erfüllen:

### 9.2.1 Elektronische Brandschutzmauer

Ein Firewall-System ist dafür zuständig, einen bestimmten IT-Bereich meist in der eigenen Organisation abzuschotten, damit Schäden, die außerhalb von diesem IT-Bereich auftreten, nicht auf die andere Seite übergreifen. Auf Kommunikationsnetze bezogen bedeutet dies, dass das Firewall-System das zu schützende Netz gegen Gefahren aus dem unsicheren Netz abschottet. Es wird nur ein einziger besonders sicherer Übergang zwischen den beiden Teilnetzen realisiert.

### 9.2.2 Elektronischer Pförtner

Ein Firewall-System ist das elektronische Äquivalent zu einem Pförtner. So wie der Pförtner aufpasst, welche Besucher in ein Gebäude hinein dürfen – zum Beispiel solche, die zu Fuß kommen und eventuell noch eine Aktentasche mitbringen, aber nicht solche, die mit dem LKW, Auto oder Fahrrad ins Gebäude der Organisation hineinfahren wollen –, überprüft das Firewall-System, wer aus dem unsicheren Netz auf das zu schützende Netz der Organisation zugreifen darf. Ebenso wie der Pförtner kontrolliert, welche Gegenstände in das Gebäude mit hinein- und hinausgenommen werden, wer in diesem Gebäude wen wann besucht hat, kontrolliert das Firewall-System, über welche Protokolle und Dienste zugegriffen wird und mit welchen IT-Systemen kommuniziert werden darf. Zusätzlich werden alle Ereignisse, die über das Firewall-System umgesetzt werden, protokolliert.

**Wichtig** Mithilfe eines Firewall-Systems wird kontrolliert, ob nur gewollte Nutzer über das Firewall-System gewünschte Aktionen umsetzen.

---

## 9.3 Das Sicherheitskonzept

Ein Firewall-System wird als sicherer und kontrollierter Übergang zwischen dem zu schützenden Netz und dem unsicheren Netz geschaltet, sodass der gesamte Datenverkehr zwischen den beiden Netzen nur über das Firewall-System möglich ist.

Auf dem Firewall-System werden spezielle IT-Sicherheitsfunktionen implementiert, die diesen Übergang sicher und beherrschbar machen. Dazu analysiert das Firewall-System die Kommunikationsdaten, kontrolliert die Kommunikationsbeziehungen und Kommunikationspartner, reglementiert die Kommunikation nach einer Sicherheitsleitlinie, protokolliert sicherheitsrelevante Ereignisse und alarmiert bei wichtigen Verstößen den Security-Administrator.

Ähnlich wie für den Pförtner und die Brandschutzmauer gilt auch für den Einsatz eines Firewall-Systems: Nicht das Firewall-System macht automatisch sicher, sondern mit dem Cyber-Sicherheitsmechanismus-Firewall-System kann, wenn es richtig betrieben wird, eine höhere Cyber-Sicherheit erzielt werden.

Das bedeutet, dass Organisationen, die ihre Netze schützen wollen, vorher genau wissen sollten, wer oder was wovor geschützt werden und was erlaubt beziehungsweise verboten werden soll. Grundsätzlich ist vor dem Einsatz eines Firewall-Systems eine Cyber-Sicherheitsleitlinie zu entwickeln und umzusetzen. Erst wenn die grundlegenden Anforderungen feststehen, kann überprüft werden, wie und mit welchem Firewall-System diese Anforderungen realisiert werden können.

Auch beim Einsatz eines Firewall-Systems muss vorher definiert werden, über welche Protokolle und Hilfsmittel ein Zugriff auf das Netz einer Organisation erlaubt sein soll. Die Reduzierung der Zugriffe, die erlaubt sein sollen, erhöht die Cyber-Sicherheit und erleichtert die Kontrolle und die Administration eines Firewall-Systems.

Wenn auf der organisatorischen, infrastrukturellen und personellen Ebene entsprechende Schutzmaßnahmen ergriffen werden, bleibt der administrative Aufwand für den Betrieb des Firewall-Systems überschaubar, und die Fehlerwahrscheinlichkeit wird stark reduziert. Ein überschaubares Sicherheitsmanagement gewährleistet die übersichtliche Anordnung der notwendigen Sicherheitsdienste.

Ein Firewall-System muss in ein individuelles Cyber-Sicherheitskonzept eingebettet werden. Wird es davon losgelöst installiert, hat es vielleicht eine Alibifunktion, kann aber keine Cyber-Sicherheitsfunktionen garantieren.

**Wichtig** Ein Firewall-System regelt und kontrolliert den Übergang zwischen dem zu schützenden Netz und dem unsicheren Netz, um die Risiken von Schäden zu minimieren.

## 9.4 Aufgaben von Firewall-Systemen

Die allgemeinen möglichen Aufgaben eines Firewall-Systems werden im Folgenden benannt und definiert:

**Zugangskontrolle auf der Netzwerkebene**

Es wird überprüft, welche IT-Systeme über das Firewall-System miteinander kommunizieren dürfen.

**Zugangskontrolle auf Nutzerebene**

Das Firewall-System überprüft, welche Nutzer und IT-Systeme über das Firewall-System eine Kommunikation aufbauen dürfen. Dazu wird die Echtheit (Authentizität) des Nutzers und der IT-Systeme festgestellt.

**Zugangskontrolle auf Datenebene**

Das Firewall-System überprüft, welche Daten eines definierten Nutzers und IT-Systems über das Firewall-System übertragen werden dürfen.

**Rechteverwaltung**

Im Rahmen der Rechteverwaltung wird festgelegt, mit welchen Protokollen und Diensten und zu welchen Zeiten über das Firewall-System eine Kommunikation stattfinden darf.

**Kontrolle auf der Anwendungsebene**

Es wird überprüft, ob Kommandos genutzt oder Dateiinhalte übertragen werden, die nicht zur Anwendung der definierten Aufgabenstellung gehören, generell unerwünscht sind (wie Spam) oder Schaden auf einem IT-System verursachen könnten (wie Malware).

**Entkopplung von Diensten**

Dienste werden entkoppelt, damit Implementierungsfehler, Schwachstellen und Konzeptionsfehler der Dienste nicht die Möglichkeit für Angriffe bieten.

**Beweissicherung und Protokollauswertung**

Verbindungsdaten und sicherheitsrelevante Ereignisse werden protokolliert und können für die Beweissicherung von Handlungen der Nutzer und für die Erkennung von Sicherheitsverletzungen ausgewertet werden.

**Alarmierung**

Besonders sicherheitsrelevante Ereignisse werden an ein Security-Management gesendet, damit bei Sicherheitsverletzungen schnell reagiert werden kann.

**Verbergen der internen Netzstruktur**

Ziel ist es, die Struktur des zu schützenden Netzes gegenüber dem unsicheren Netz zu verbergen. Es soll aus dem unsicheren Netz möglichst nicht sichtbar sein, ob im zu schützenden Netz 10, 100, 1000 oder 10.000 IT-Systeme vorhanden sind oder wie diese strukturiert sind.

## Vertraulichkeit der Nachrichten, wenn zusätzlich eine VPN-Funktion genutzt wird

Nachrichten können nicht im Klartext gelesen werden. Dadurch ist die Vertraulichkeit der Daten bei einer Übertragung über unsichere Netze gewährleistet.

Weitere mögliche Ziele eines Firewall-Systems:

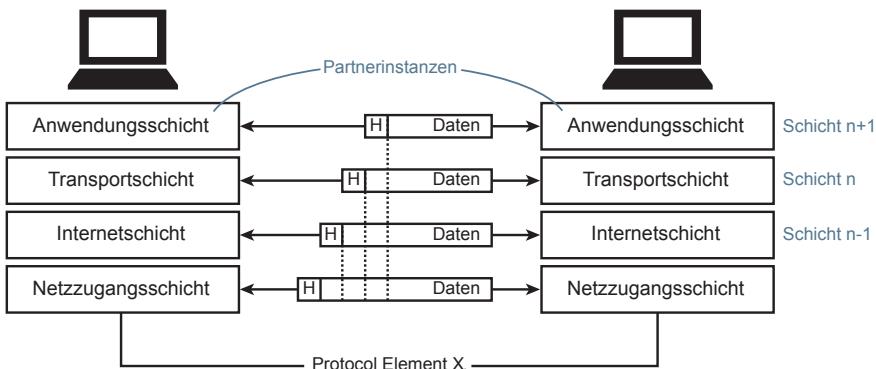
- Das Firewall-System selbst muss gegen Angriffe resistent sein.
- Accounting (IP- und Nutzerorientiert)
- Network Address Translation
- Intrusion Detection
- Network/Traffic Monitoring
- SMTP Whitelisting

## 9.5 Grundlage von Firewall-Systemen

Im Folgenden wird ein Firewall-Modell vorgestellt, mit dessen Hilfe die Definition von einheitlichen Kriterien über die Aussagen der Möglichkeiten und Grenzen im Sinne der Wirkung von Sicherheit und Vertrauenswürdigkeit von Firewall-Systemen abgeleitet und klassifiziert werden kann.

### Definition eines Kommunikationsmodells

Eine Kommunikation ist die Zusammenarbeit von Kommunikationssystemen mit dem Ziel, eine gemeinsame Aufgabe zu bewältigen, wobei jedes Kommunikationssystem Daten in einer für diese Aufgabe spezifischen Weise zu verarbeiten hat. Die Zusammenarbeit erfordert die Einhaltung von Regeln, die in einem Satz von Normen und Standards festgelegt werden, siehe Abb. 9.5.



**Abb. 9.5** TCP/IP-Protokollarchitektur

Ein Kommunikationssystem ist aus mehreren logischen Schichten aufgebaut.

Die TCP/IP-Protokollarchitektur besteht aus vier logischen Schichten:

- In einer Schicht N kommunizieren Partnerinstanzen miteinander.
- Zwischen den Partnerinstanzen werden Protokollelemente ( $x_i$ ) ausgetauscht.
- Protokollelemente bestehen aus Headern (H) und/oder Daten (Daten).
- Header (H) enthalten Steuerinformationen wie Adressen, laufende Nummern, Zähler, Informationen über den Übertragungsweg und Hinweise auf die Verwendung der Daten. Die Header-Informationen (H) können feste Größen, aber auch Variablen sein.
- Jede Schicht hat eigene Header (H), die auch leer sein können.
- In welcher Reihenfolge und zu welchem Zwecke die Protokollelemente ausgetauscht werden, wird im Kommunikationsprotokoll festgelegt.
- Die Implementierung des Kommunikationsprotokolls auf den IT-Systemen und Netzwerkelementen (zum Beispiel Router) ist Sache des Herstellers und nicht festgelegt.

### Schichten der TCP/IP-Protokollarchitektur

In der TCP/IP-Protokollarchitektur bestehen analog zum OSI-Referenzmodell unterschiedliche Kommunikationsschichten, die Daten von der übergeordneten Schicht zur nächsttieferen Schicht weiterreichen. Jede Kommunikationsschicht fügt den Daten eigene Kontrollinformationen hinzu, bis sie über das Netz gesendet werden. Der Empfänger reicht diese Daten dann Schicht für Schicht nach oben weiter, wobei jede Schicht nur die für sie relevanten Daten auswertet und diese aus dem Datenpaket entfernt, bevor sie an die nächsthöhere Schicht weitergegeben werden.

#### Netzzugangsschicht

Die Netzzugangsschicht ermöglicht es einem IT-System, Daten zu einem anderen IT-System über ein Medium (Kupfer- u. Glasfaser-Leitung, Luft, ...) zu übertragen. Protokolle auf der Netzzugangsschicht sind zum Beispiel FDDI, Ethernet, WLAN.

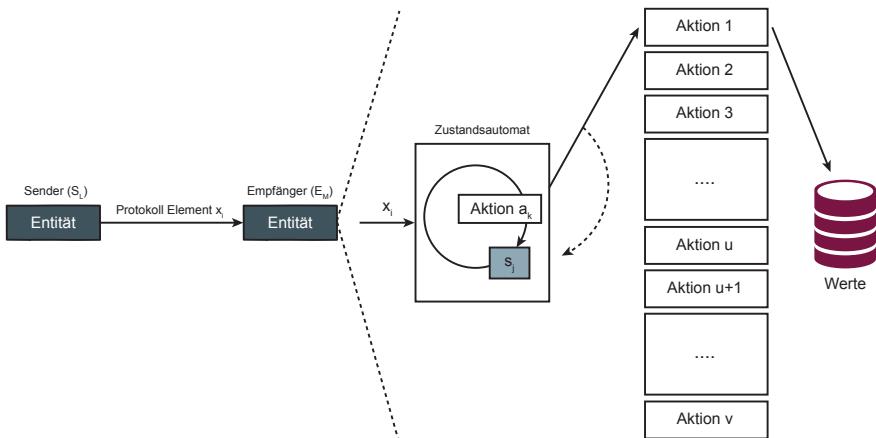
Die Netzzugangsschicht umfasst die zwei unteren Schichten des OSI-Modells und beinhaltet die Kapselung von IP-Paketen in Netzrahmen (Frames und die Zuordnung von IP-Adressen zu physikalischen Netzadressen, zum Beispiel MAC-Adressen), aber auch die Zugriffssteuerung auf das Medium, die Fehlererkennung/Behandlung auf der Netzzugangsschicht.

#### Netzwerkschicht

Die Netzwerkschicht definiert den Aufbau von IP-Paketen und bestimmt, auf welchem Weg die Daten durch das Internet übertragen werden (Routing).

#### Transportschicht

Die Transportschicht stellt eine Verbindung zwischen zwei Endpunkten oder IT-Systemen über das Netzwerk her. Die wichtigsten Protokolle sind TCP und UDP.



**Abb. 9.6** Vereinfachtes logisches Kommunikationsmodell mit Aktionen

### Anwendungsschicht

Die Anwendungsschicht beinhaltet sämtliche Programme und Dienste, die über die Netzwerkverbindung durchgeführt werden sollen. Dazu gehören vor allem Anwendungsprotokolle wie HTTP (World Wide Web, SMTP (E-Mail-Funktionen), FTP (File Transfer Protocol) usw.

### Vereinfachtes logisches Kommunikationsmodell mit Aktionen

Im Folgenden wird ein vereinfachtes logisches Kommunikationsmodell mit Aktionen eingeführt, dass das grundsätzliche Prinzip eines Kommunikationsablaufs darstellen soll. Jede Schicht hat einen eigenen „Zustandsautomat“, der dem jeweiligen Kommunikationsprotokoll der entsprechenden Schicht entspricht, siehe Abb. 9.6.

Zur Bewältigung der spezifischen Aufgabe der Entitäten in einer bestimmten Schicht führt diese in Abhängigkeit vom empfangenen Protokollelement  $x_i$ , vom aktuellen Zustand  $s_j$  und von weiteren Ereignissen (Timerabläufen, Statusmeldungen, ...) eine definierte Aktion  $a_k$  aus. Dabei sind die Header-Informationen mit dem Ablauf der Anwendung für die Aktionen in der Regel entscheidend. Die Schichten sind im Normalfall voneinander unabhängig.

Die Komplexität der jeweiligen Schichten kann sehr unterschiedlich sein. Pro physikalischem Protokollelement können mehrere Schichten beteiligt sein.

### Definition der Transmitter (Sender)

Es gibt eine endliche Menge von Transmittern, die wie folgt definiert werden:

$$\text{Transmitter } (T) = \{t_1, \dots, t_l\}$$

Aufteilung der Transmitter:

$$\text{Erlaubte Transmitter } \{t_1, \dots, t_g\} :$$

Erlaubte Transmitter sind solche Transmitter, die Aktionen beim Receiver veranlassen dürfen. Erlaubte Transmitter stellen ein kalkulierbares Risiko bezüglich der Verwundbarkeit der Werte da.

Nicht erlaubte Transmitter  $\{t_{g+1}, \dots t_l\}$  :

Nicht erlaubte Transmitter sind solche Transmitter, die keine Aktionen beim Receiver veranlassen dürfen. Nicht erlaubte Transmitter (Angreifer, Fremde, Unbefugte) stellen ein sehr hohes Risiko bezüglich der Verwundbarkeit der Werte da.

Welche Transmitter erlaubt sind und welche nicht, wird durch die Sicherheitspolitik festgelegt.

### **Definition der Receiver (Empfänger)**

Es gibt eine endliche Menge von Receivern, die wie folgt definiert werden.

Receiver ( $R$ ) =  $\{r_1, \dots r_m\}$

Aufteilung der Receiver:

Erlaubte Receiver  $\{r_1, \dots r_h\}$  :

Erlaubte Receiver sind solche Receiver, bei denen erlaubte Transmitter erlaubte Aktionen veranlassen dürfen. Erlaubte Receiver stellen ein kalkulierbares Risiko bezüglich der Verwundbarkeit der Werte dar.

Nicht erlaubte Receiver  $\{t_{h+1}, \dots t_m\}$  :

Bei nicht erlaubten Receivern (Unbefugte) dürfen keine Aktionen veranlasst werden.

Welche Receiver erlaubt sind und welche nicht, wird durch die Sicherheitspolitik festgelegt.

### **Definition der Protokollelemente**

Die Protokollelemente, die zwischen Sender und Empfänger ausgetauscht werden, können wie folgt klassifiziert werden, siehe Tab. 9.1: Summe aller Protokollelemente:  $\Sigma = 2^n$

Protokollelemente  $X = \{x_1, \dots x_t, x_{t+1}, \dots x_u, x_{u+1}, \dots x_v, x_{v+1}, \dots x_n\}$

Welche Protokollelemente erlaubt sind und welche nicht, wird durch die Sicherheitspolitik festgelegt.

**Tab. 9.1** Definition der Protokollelemente

$\{x_1, \dots, x_n\}$	Menge der Protokollelemente, die möglich sind (mögliche Codierung der Bits und Bytes)		
mögliche	$\{x_1, \dots, x_u\}$ genormt	Menge der Protokollelemente, die in der Norm definiert sind (ISO, RFC, ...)	
		$\{x_1, \dots, x_t\}$ genormt und erlaubt	Menge der Protokollelemente aus der Norm, die für eine spezielle Aufgabe notwendig und damit erlaubt sind, zum Beispiel die Kommandos „edir“ (Change Directory) und „put“ (Transmit), um mithilfe vom FTP eine Datei vom Sender zu versenden und auf der Empfängerseite zu speichern
	$\{x_{t+1}, \dots, x_u\}$ nicht genormt	$\{x_{t+1}, \dots, x_u\}$ genormt und nicht erlaubt	Menge der Protokollelemente aus der Norm, die für die spezielle Aufgabe nicht notwendig und damit nicht erlaubt sind, zum Beispiel bei FTP das Kommando „del“ (Löschen von Dateien)
		$\{x_{u+1}, \dots, x_v\}$ hersteller-definiert	Menge der Protokollelemente, die nicht in der Norm definiert sind, und für die eigentliche Aufgabe nicht notwendig und damit in der Regel nicht erlaubt sind  Menge der Protokollelemente, die nicht in der Norm definiert sind, aber zusätzliche Dienste anbieten. Hersteller haben bei ihrer Implementierung der Kommunikationsprotokolle oder -dienste weitere, eigene Protokollelemente definiert, um zum Beispiel folgende Aufgaben durchzuführen zu können: Fehleranalyse (Zustand des Protokoll-Automats, Zustand des Betriebssystems, ...). Diese zusätzlichen Dienste werden von den Herstellern angeboten, um aus der Ferne eine Fehleranalyse oder sonstige Servicearbeiten durchzuführen zu können. Trap-Doors, mit denen Angriffe realisiert werden und nicht definierte oder erlaubte Aktionen auf der Empfängerseite unautorisiert durchgeführt werden können. Diese Protokollelemente sind in der Regel nicht erlaubt
	$\{x_{v+1}, \dots, x_n\}$ nicht definiert	Menge der Protokollelemente, die nicht in der Norm und nicht vom Hersteller definiert und damit nicht erlaubt ist. Im Normalfall werden solche Protokollelemente von der Implementierung als Fehler erkannt und entsprechend behandelt. Es werden aber immer wieder Implementierungen bekannt, die beim Empfang von nicht definierten Protokollelementen eine fehlerhafte Aktion durchführen, die für einen Angriff verwendet werden kann	

 $t \leq u$  $u \leq n$  (ist  $u = n$ , dann  $v = n$ , dann gibt es keine undefinierten Protokollelemente) $v \leq n$  (ist  $v = n$ , dann gibt es keine undefinierten Protokollelemente)

Bei der Betrachtung der Sicherheit von Protokollelementen  $\{x_1, \dots, x_n\}$  müssen weitere Aspekte berücksichtigt werden:

- Nicht alle Felder in den Protokollelementen sind sicherheitsrelevant in Bezug auf die Möglichkeiten eines Firewall-Systems (zum Beispiel Laufzähler, Zufallszahlen, ...). Aus diesem Grund reduziert sich die praktische Anzahl der Protokollelemente, die betrachtet werden müssen, sehr stark.
- Bestimmte Protokollelemente sind in Abhängigkeit vom Zustand des Kommunikationsprotokolls erlaubt oder nicht erlaubt. Aus diesem Grund muss der Inhalt der Tab. 9.1 immer in Abhängigkeit vom Zustand des Kommunikationsprotokolls betrachtet werden. Protokollelemente können in einem bestimmten Zustand erlaubt und in einem anderen Zustand nicht erlaubt sein.
- Die Möglichkeit, über verdeckte Kanäle Informationen zu übertragen, wird in diesem Modell nicht betrachtet.
- Erlaubte Protokollelemente  $\{x_1, \dots, x_l\}$  dürfen nur zwischen erlaubten Transmittenern  $\{t_1, \dots, t_g\}$  und Receivern  $\{r_1, \dots, r_h\}$  zu erlaubten Zeiten ausgetauscht werden.

### **Definition der Aktionen**

Die Aktionen auf der Empfängerseite sind wie folgt definiert.

$$\text{Aktion } (A) = \{a_1, \dots, a_f\} :$$

Eine Aktion, die aus einer definierten Anzahl von Teilaktionen besteht, ist zum Beispiel das Schreiben einer Datei auf die Festplatte des Empfängers mithilfe von FTP. Teilaktionen sind zum Beispiel das Selektieren der Subdirectory, das Empfangen von Teildatenmengen, das Abspeichern der Daten usw.

Aufteilung der Aktionen:

$$\text{Erlaubte Aktionen } \{a_1, \dots, a_t\} :$$

Erlaubte Aktionen sind solche Aktionen, die für die erlaubten Anwendungen beziehungsweise Aufgabenstellung notwendig sind. Erlaubte Anwendungen auf definierten „Assets“ stellen ein kalkulierbares Risiko bezüglich der Verwundbarkeit der Werte da.

In den Bereich der erlaubten Aktionen fallen auch die Fehlerbehandlungen bezüglich der nicht definierten Zustände und Ereignisse.

$$\text{Nicht erlaubte Aktionen } \{a_{t+1}, \dots, a_f\} :$$

Nicht erlaubte Aktionen sind solche Aktionen, die zwar die Implementierung eines Kommunikationsprotokolls oder -dienstes auf der Empfängerseite ermöglichen, aber für die eigentliche Aufgabenstellung nicht notwendig und deshalb nicht erlaubt sind, damit das Risiko eines beabsichtigten oder auch unbeabsichtigten Schadens minimiert wird.

Welche Aktionen erlaubt sind und welche nicht, wird durch die Sicherheitspolitik festgelegt.

Erlaubte Aktionen  $\{a_{t+1}, \dots, a_f\}$  dürfen nur durch erlaubte Protokollelemente  $\{x_1, \dots, x_t\}$  ausgelöst werden, die zwischen erlaubten Transmittern  $\{t_1, \dots, t_g\}$  und Receivern  $\{r_1, \dots, r_h\}$  zu erlaubten Zeiten ausgetauscht werden.

### Kommunikationsabläufe

Der Transmitter sendet dem Receiver Protokollelemente ( $x_i$ ) über das Netz. Der Receiver interpretiert die empfangenen Protokollelemente als externe Ereignisse und startet mit diesen und weiteren Informationen seine „protocol-state-machine“.

### Action of the Receiver

$$a_k = \text{protocol-state-machine } (x_i^*, s_j)$$

$a_k$  Teil-Aktion in einer Schicht, die in Abhängigkeit vom empfangenen Protokollelement  $x_i$  und vom aktuellen Zustand  $s_j$  ausgeführt wird

$x_i$  Protokollelement

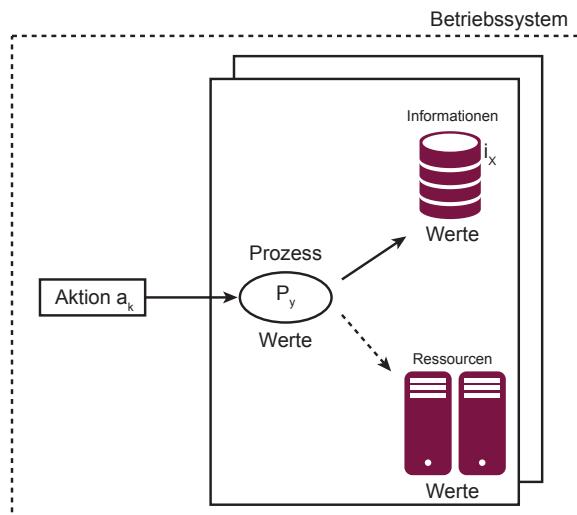
$s_j$  aktueller Zustand (actual state)

Das Protokoll wird als State-Machine betrachtet, in der sich der Zustand  $s_j$  in Abhängigkeit von den empfangenen Protokollelementen und von weiteren Ereignissen (Timerabläufen, Statusmeldungen, ...) verändern kann.

### Ablauf der Aktionen beim Receiver

Mithilfe der Aktionen ( $a_k$ ), die in Abhängigkeit vom empfangenen Protokollelement ( $x_i$ ) sowie von weiteren Ereignissen (Timerabläufen, Statusmeldungen, ...) und vom aktuellen Zustand ( $s_j$ ) ausgeführt werden, werden beim Receiver erlaubte Informationen (Assets) verarbeitet oder Ressourcen (Assets: Drucker, Berechnungen, ...) genutzt. Abb. 9.7 verdeutlicht die Verbindung der Aktionen mit den Informationen und anderen Ressourcen.

**Abb. 9.7** Ablauf der Aktionen beim Receiver



Welche konkreten Informationen oder andere Ressourcen mit einer definierten Aktion genutzt werden dürfen, wird in der Regel mithilfe der Rechteverwaltung des Betriebssystems (Microsoft Windows, LINUX, iOS, Android, ...) und der Rechteverwaltung der Anwendungen (Datenbank, SAP, ...) detailliert definiert.

Aus Sicht des Kommunikationsmodells ist es egal, welche IT-Systeme oder Betriebssysteme der Transmitter (T) oder Receiver (R) nutzt. Beide müssen nur die entsprechenden Kommunikationsprotokolle und -dienste, z. B. TCP/IP-Familie nach den definierten Standards realisieren.

---

## 9.6 Definition eines Firewall-Elements

Ein Firewall-System besteht aus einem oder mehreren Firewall-Elementen, die aktiv in die Kommunikation zwischen dem zu schützenden und dem unsicheren Netz eingreifen sowie einem Security-Management, das für die Verwaltung der aktiven Firewall-Elemente verantwortlich ist.

### Grundsätzliche Aspekte eines Firewall-Elements:

Ein Firewall-Element ist ein separates Kommunikationssicherheitssystem. Es besteht in der Regel keine direkte Verbindung mit den Sicherheitsfunktionen der Betriebssysteme und der IT-Systeme (Receiver, Transmitter). Ein Firewall-Element hat keinen Einfluss (Erweiterung, Veränderung) auf die verwendeten Kommunikationsprotokolle und -dienste. Ein Firewall-Element wird von der Organisation verwaltet, die es betreibt, und ist im Prinzip unabhängig von allen anderen Organisationen in dieser Verwaltung.

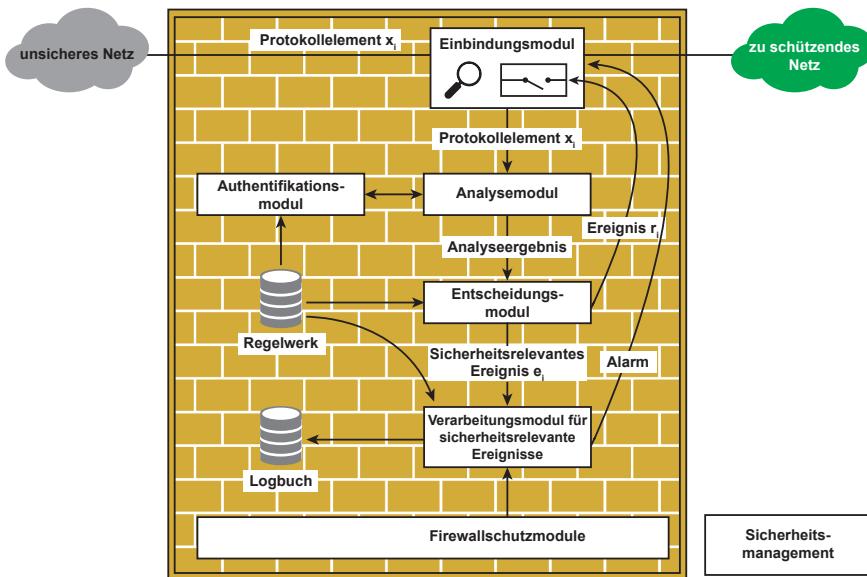
**Wichtig** Ein Firewall-Element ist ein separates Kommunikationssicherheitssystem, das im Prinzip unabhängig von anderen Organisationen arbeitet.

In Abb. 9.8 wird der prinzipielle Aufbau aktiver Firewall-Elemente, die in die Kommunikationsschnittstelle zwischen dem unsicheren Netz und dem zu schützenden Netz eingefügt werden, definiert. Ein so umrissenes Firewall-Element kann Packet Filter, Stateful Inspection, Application Gateway mit Proxys usw. repräsentieren.

### Einbindungs- und Durchsetzungsmodul: -> Funktion: *enforcement* ( $r_i$ )

Das Einbindungs- und Durchsetzungsmodul realisiert die Einbindung des aktiven Firewall-Elements in das Kommunikationssystem sowie die Durchsetzung der im Regelwerk festgehaltenen Sicherheitspolitik.

Die Einbindung in das Kommunikationssystem muss so realisiert werden, dass die Kommunikationsdaten nicht am Einbindungsmodul vorbeifließen können, ohne einer Analyse und einer Entscheidung unterzogen worden zu sein. Aus diesem Grund ist die Einbindung besonders sicherheitskritisch. In Abhängigkeit des



**Abb. 9.8** Aufbau eines aktiven Firewall-Elements

verwendeten Firewall-Elementes (Packet Filter, Stateful Inspection, Application Gateway mit Proxys usw.) wird das Einbindungsmodul an unterschiedlichen Stellen der Protokollarchitektur eingebunden.

#### **Analysemodul -> Funktion: *analysis* ( $x_i$ )**

Im Analysemodul werden die Kommunikationsdaten des Protokollelementes ( $x_i$ ) den Möglichkeiten des aktiven Firewall-Elements entsprechend analysiert. Die Ergebnisse der Analyse werden an das Entscheidungsmodul weitergeleitet. Im Analysemodul können mithilfe von Zustandsautomaten Statusinformationen (zum Beispiel Verbindungsaufbau, Transferzustand oder Verbindungsabbau) der Kommunikation festgehalten werden. Vor allem die Tiefe der Analyse, das heißt, wie weit und umfangreich analysiert wird, ist sicherheitskritisch und stellt ein besonderes Qualitätsmerkmal eines aktiven Firewall-Elements dar. Die unterschiedlichen prinzipiellen aktiven Firewall-Elemente (Packet Filter und Application Gateway) analysieren auf unterschiedlichen Kommunikationsebenen.

#### **Entscheidungsmodul -> Funktion: *result-of-decision* (*analysis* (), *security-management* ())**

Im Entscheidungsmodul werden die Analyseergebnisse ausgewertet und mit den im Regelwerk festgelegten Definitionen der Sicherheitspolitik verglichen. Hier wird anhand von Access-Listen überprüft, ob das ankommende Protokollelement ( $x_i$ ) passieren darf oder nicht ( $r_i = \text{result of the decision}$ ). Falls ja, wird das Einbindungsmodul zum Durchlass aktiviert. Falls nein, wird das Protokollelement ( $x_i$ )

nicht durchgelassen; das Ereignis ( $e_i$ ) wird als sicherheitsrelevant eingestuft und entsprechend weiterverarbeitet.

### **Result of the decision module:**

$$r_i = \text{result-of-decision}(\text{analysis}(x_i), \text{security-management(rules)})$$

$r_i = \text{true}$

das Protokollelement  $x_i$  wird weitergeleitet, eventuell als Beweissicherung der Aktion in einem Logbuch festgehalten

$r_i = \text{false}$

das Protokollelement  $x_i$  wird nicht weitergeleitet und es wird ein sicherheitsrelevantes Ereignis  $e_i$  erzeugt

### **Regelwerk -> Funktion: security-management (rules)**

Das Regelwerk ist die technische Umsetzung der Sicherheitspolitik und wird mit Hilfe eines Security-Managements erstellt.

Im Regelwerk stehen alle Informationen (rules: Schlüssel, Access-Listen, Attribute usw.) über Nutzer, Authentifikationsverfahren, Kommunikationsverbindungen etc., die notwendig sind, um eine Entscheidung für oder gegen eine Übertragung des Protokollelementes ( $x_i$ ) über das aktive Firewall-Element fällen zu können, und wie mit sicherheitsrelevanten Ereignissen ( $e_i$ ) verfahren werden soll.

### **Verarbeitungsmodul für sicherheitsrelevante Ereignisse -> Funktion: event ( $e_i$ )**

In diesem Verarbeitungsmodul werden alle sicherheitsrelevanten Ereignisse ( $e_i$ ) verarbeitet, die im aktiven Firewall-Element erzeugt werden. In Abhängigkeit des Regelwerks wird ein sicherheitsrelevantes Ereignis mit den dazugehörigen Protokolldaten je nach Einstellung in eine Log-Datei geschrieben oder über den Alarmmechanismus als spontane Meldung an ein Security-Management weitergeleitet.

### **Authentisierungsmodul -> Funktion: authentication ( $t_i$ )**

Das Authentisierungsmodul sorgt für die Identifikation und Authentisierung der Instanzen (Prozesse in den IT-Systemen, Nutzer etc.), die über das aktive Firewall-Element kommunizieren möchten. Hier können unterschiedliche Authentisierungsverfahren verwendet werden.

### **Firewall-Schutzmodul -> Funktion: safeguard ()**

Das aktive Firewall-Element muss nicht nur Sicherheitsdienste erbringen, sondern auch selbst gegen Angriffe resistent sein. Im Firewall-Schutzmodul verbergen sich aktive Sicherheitsfunktionen, die für den sicheren Betrieb des aktiven Firewall-Elements selbst sorgen. Dazu gehören zum Beispiel die folgenden Sicherheitsmechanismen:

- **Integritätstest:** Dieser Sicherheitsmechanismus gewährleistet, dass Veränderungen der Software (Betriebssystem, Firewall, Sicherheitsmechanismen etc.), des Regelwerks und des Logfiles erkannt werden. Dies wird zum Beispiel

durch eine regelmäßige und/oder spontane Checksummenüberprüfung der Software und der Daten realisiert.

- **Authentisierungsmechanismus:** Dieser Sicherheitsmechanismus sorgt dafür, dass nur vom (dazu berechtigten) Security-Management das Regelwerk beeinflusst und die Protokolldaten aus dem Logfile ausgelesen werden können.
- **Betriebssicherungsmechanismen:** Hier werden Sicherheitsmechanismen zusammengefasst, die für den sicheren Betrieb der aktiven Firewall-Elemente sorgen. Zu diesen Sicherheitsmechanismen gehören zum Beispiel die Überprüfung des Überlaufs von Logbüchern und Speichermedien (zum Beispiel Festplatte) und die Überprüfung, ob sich die Software in einem definierten Zustand (Automatenzustand) befindet usw.

#### **Logfile -> Funktion: *logfile* (e.)**

Im Logfile stehen alle Protokolldaten der sicherheitsrelevanten Ereignisse, die während des Betriebs eines aktiven Firewall-Elements aufgetreten sind und dem Regelwerk entsprechend registriert werden sollen.

#### **Security Management -> Funktion: *security-management (rules)***

Mithilfe des Security-Managements können die Regeln für die aktiven Firewall-Elemente festgelegt und die Protokolldaten der sicherheitsrelevanten Ereignisse aus den Logbüchern analysiert werden.

---

## **9.7 Designkonzept aktiver Firewall-Elemente**

Im folgenden Kapitel wird ein sicheres Designkonzept für aktive Firewall-Elemente beschrieben. Die Wirksamkeit der Sicherheitsdienste eines aktiven Firewall-Elementes ist umso höher, je mehr die im Folgenden vorgestellten Sicherheitskriterien berücksichtigt werden.

### **Minimale Software**

Zusätzlich zu den Sicherheitsdienstleistungen, die ein aktives Firewall-Element erbringen soll, muss das Firewall-Element selbst gegen Angriffe resistent sein. Daher ist es besonders wichtig, nur fehlerfreie Software einzusetzen. Das Firewall-Element muss klar strukturiert und nachvollziehbar aufgebaut und realisiert werden. Da jedes Programm aber potenziell Sicherheitslücken enthalten kann, sollten nur die für die Erbringung der Firewall-Funktionalität unbedingt notwendigen Programme auf dem aktiven Firewall-Element eingesetzt werden (keine Routerfunktionalität, keine weiteren Anwendungen, ...). Es ist auch möglich, mithilfe einer virtuellen Umgebung eine Separierung und starke Isolierung umzusetzen.

### **Sichere Einbindung in das Kommunikationssystem (Netzwerk-Software, Betriebssystem usw.)**

Die Sicherheit eines aktiven Firewall-Elementes hängt in entscheidendem Maße davon ab, wie gut die Sicherheitsmechanismen in das Kommunikationssystem

eingebunden werden. Es muss sichergestellt werden, dass es nicht möglich ist, die Firewall-Sicherheitsfunktionen über das Betriebssystem oder über die verwendete Kommunikations-Software (TCP/IP-Software, Netzzugangs-Treiber etc.) zu umgehen.

Beispiele: Bei Verwendung von IP-Forwarding (Kernel-Funktionalität) kann die Kommunikation am Firewall-Element vorbeigeleitet werden, ohne dass die Sicherheitsmechanismen wirken können.

### **Getrenntes Security-Management**

Die Forderung, auf den aktiven Firewall-Elementen nur minimale Software zu installieren, bedingt, dass das Security-Management von den eigentlichen Sicherheitsfunktionen des aktiven Firewall-Elementes getrennt realisiert werden muss, damit ein Höchstmaß an Sicherheit auf dem aktiven Firewall-Element gewährleistet werden kann.

Die getrennte Realisierung des Security-Managements kann auf einem separaten IT-System realisiert werden.

### **Einfache, zuverlässige und berechtigte Bedienung des Security-Managements**

Für das Security-Management ist eine einfache und zuverlässige Bedienung erforderlich, damit die Regeln ohne Fehler eingegeben werden können. Außerdem ist eine Überprüfung der Widerspruchsfreiheit der Regeln erforderlich, damit nicht versehentlich sicherheitskritische Eingaben gemacht werden.

Ebenso muss sichergestellt werden, dass nur vom berechtigten Administrator mithilfe des Security-Managements auf die aktiven Firewall-Elemente zugegriffen werden kann, damit das Security-Management nicht von Angreifern genutzt werden kann, um eine Kommunikation über das aktive Firewall-Element zuzulassen.

In diesem Abschnitt wird beschrieben, mit welchen Grundelementen ein Firewall-System aufgebaut werden kann. Das Ziel dieser Darstellung ist aufzuzeigen, wie technische Sicherheitsmechanismen für Firewall-Elemente realisiert werden können, welche konkreten Möglichkeiten bestehen, Sicherheit zu gewährleisten, wie sie wirken und wo ihre Grenzen liegen.

Ein Firewall-System kann aus den folgenden Grundelementen bestehen:

- Packet Filter
- Stateful Inspection
- Application Gateway
- Proxys

Um die konzeptionellen Unterschiede zu verdeutlichen und so das Verständnis zu erleichtern, werden im Folgenden die einzelnen Firewall-Elemente mithilfe von Analogien erläutert.

Eine plastische, leicht fassbare Analogie zu einem Firewall-System ist ein Pförtner. Alle Zugänge zu einem Gebäude sollen vom Pförtner überwacht werden. Hier gilt: Je weniger Zugänge es gibt, desto besser kann der Pförtner den Zugang kontrollieren (Common Point of Trust).

## 9.8 Packet Filter

Das aktive Firewall-Element Packet Filter analysiert und kontrolliert die ein- und ausgehenden Pakete auf der Netzzugangs-, der Netzwerk- und der Transportebene. Dazu werden die Pakete (zum Beispiel Ethernet), die auf dem physikalischen Kabel übertragen werden, aufgenommen und analysiert. Durch den Packet Filter werden die Netze physikalisch entkoppelt. Ein Packet Filter verhält sich wie eine einfache Bridge. Packet Filter sind nicht nur auf TCP/IP-Protokolle beschränkt.

Ein Packet Filter interpretiert den Inhalt der Pakete und verifiziert, ob die Daten in den entsprechenden Headers der Kommunikationsebenen den definierten Regeln entsprechen. Die Regeln werden so definiert, dass nur die notwendige Kommunikation erlaubt ist und bekannte sicherheitskritische Einstellungen vermieden werden, zum Beispiel die IP-Fragmentierung. Die Packet Filter werden transparent in die Leitung eingefügt.

### Analogie zum Pförtner

Wenn der LKW eines Lieferanten am Werkstor mit einer Lieferung vorfährt, schaut der „Packet Filter-Pförtner“ auf das Logo an der Seite des LKWs, um zu überprüfen, ob es ihm bekannt ist und lässt den LKW gegebenenfalls unmittelbar durch das Tor, ohne den Lieferschein zu kontrollieren.

### Allgemeine Arbeitsweise von Packet Filtern

Beim Packet Filter können auf den verschiedenen Kommunikationsebenen unterschiedliche Überprüfungen durchgeführt werden, siehe Abb. 9.9.

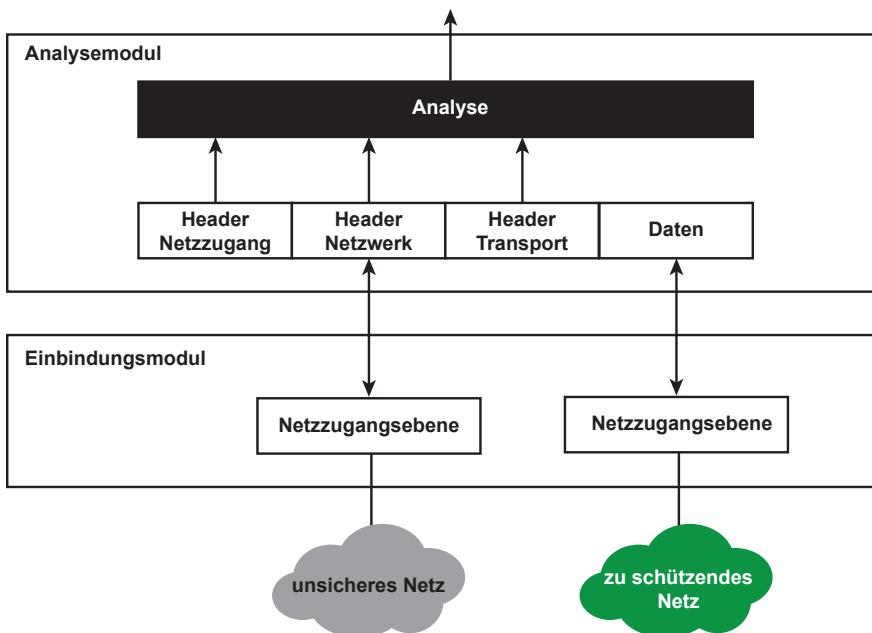


Abb. 9.9 Allgemeine Arbeitsweise eines Packet Filters

- Es wird überprüft, von welcher Seite das Paket empfangen wird (Information aus dem Einbindungsmodul).
- Auf der Netzzugangsebene werden die Quell- und Ziel-Adresse und der verwendete Protokolltyp kontrolliert.
- Auf Netzwerkebene wird je nach Protokoll überprüft:
  - IP-Protokoll: die Ziel- und die Quell-Adresse und das verwendete Schicht-4-Protokoll, aber auch das Optionsfeld und die Flags
  - Das Optionsfeld wird in der Regel nicht durchgelassen.
  - Mithilfe der Flags kann eine Fragmentierung unterbunden werden:
    - ICMP: die ICMP-Kommandos
    - IPX-Protokoll: Network/Node
    - OSI-Protokoll: die OSI-Netzwerkadresse
- Auf Transportebene findet
  - bei UDP/TCP eine Überprüfung der Portnummern (Quell- und Ziel-Port) statt (hierüber werden alle Dienste wie HTTP, FTP, Telnet, definiert);
  - bei TCP findet zusätzlich eine Überprüfung der Richtung des Verbindungsbaus mithilfe der Code Bits statt.
- Zusätzlich kann überprüft werden, ob der Zugriff über den Packet Filter in einem definierten Zeitraum durchgeführt wird (zum Beispiel montags bis freitags von 7 Uhr bis 19 Uhr, samstags von 7 bis 13 Uhr, sonntags nicht).

Die entsprechenden Prüfinformationen werden dem Regelwerk (Accessliste, Rechteleiste) entnommen und mit den Analyse-Ergebnissen verglichen.

Bei Verstoß gegen die Regeln wird dies als sicherheitsrelevantes Ereignis entsprechend protokolliert, und falls diese Option eingerichtet ist, wird eine spontane Meldung mit den Protokolldaten des sicherheitsrelevanten Ereignisses an das Security-Management gesendet, damit schnell reagiert werden kann.

### Anwendungsgebiete von Packet Filtern

Ein Firewall-System, das nur auf Packet Filtern aufbaut, wird sicherlich nicht für die Kopplung eines zu schützenden Netzes an das Internet eingesetzt werden können, da der Schutzbedarf der meisten zu schützenden Netze für die Kontrollmöglichkeiten eines Packet Filter zu hoch ist.

Packet Filter werden zum Aufbau von High-Level-Security-Firewall-Systemen und für die kontrollierte Kommunikation im Intranet verwendet. Für diese Anwendungen sind besonders Packet Filter, die gleichzeitig verschlüsseln, eine wirkungsvolle Sicherheitskomponente, mit der Internet- und Intranet-Anwendungen sicher und beherrschbar realisiert werden können.

Möglichkeiten, Vorteile und besondere Aspekte von Packet Filtern:

- transparent, das heißt, unsichtbar für den Nutzer und die IT-Systeme und ohne ihre aktive Einwirkung tätig
- einfach erweiterungsfähig für neue Protokolle
- flexibel für neue Dienste
- für andere Protokollfamilien verwendbar (IPX, OSI, DECNET, SNA...)
- hohe Performance durch optimale Mechanismen (Betriebssystem, Treiber usw.)
- leicht realisierbar, da geringere Komplexität

Nachteile und Grenzen von Packet Filtern:

- Daten, die oberhalb der Transportebene liegen, werden in der Regel nicht analysiert. Daher kann erfolgreich ein Port-Hopping-Angriff umgesetzt werden.
- Für die Anwendungen (HTTP, FTP, SMTP, ...) besteht keine Sicherheit, zum Beispiel können bei der Freischaltung von SMTP (Port 25) Angriffe über das Mail-Programm „Sendmail“ auf den IT-Systemen des zu schützenden Netzes durchgeführt werden.
- Falsch konfigurierte Programme auf IT-Systemen im zu schützenden Netz können bei erlaubten Kommunikationsverbindungen von außen genutzt werden, da ein direkter Zugriff auf das IT-System besteht.
- Typische Packet Filter können die Struktur des zu schützenden Netzes nicht verbergen.
- Protokolldaten werden nur bis zur Transportebene zur Verfügung gestellt.

## 9.9 Zustandsorientierte Packet Filter (stateful inspection)

Der Leistungsumfang von Packet Filtern kann erweitert werden, indem die Analyse und Interpretation der Pakete auch auf höheren Kommunikationsebenen durchgeführt wird. In diesem Fall werden die Pakete auch auf der Anwendungsebene interpretiert und Statusinformationen für jede aktuelle Verbindung auf den unterschiedlichen Kommunikationsebenen bewertet und festgehalten, siehe Abb. 9.10.

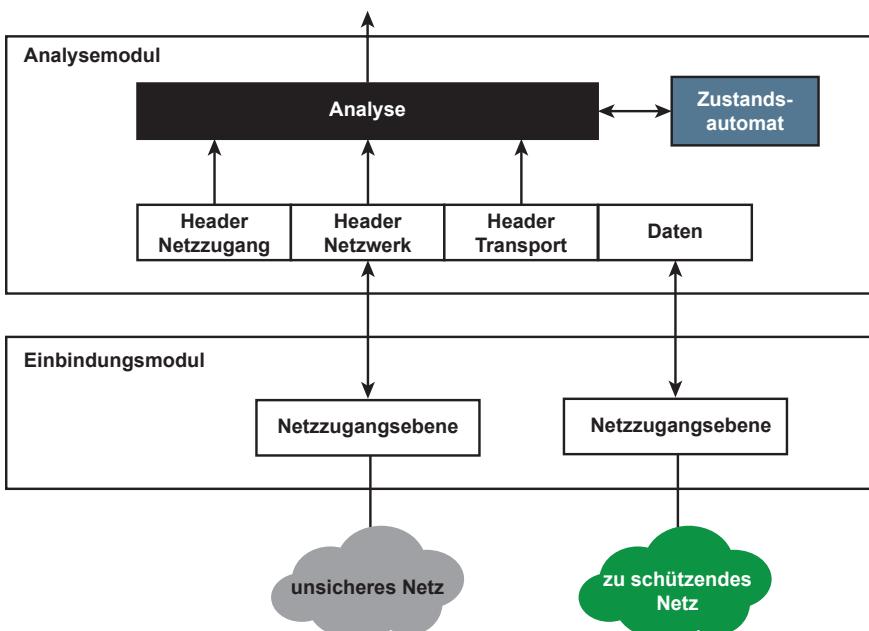


Abb. 9.10 Zustandsorientierte Packet Filter

### Analogie zum Pförtner

Wenn die Lieferung ankommt, dann schaut der Pförtner nicht nur auf die Adressen, sondern er prüft auch den Lieferschein, um zu überprüfen, ob sich in dem Paket etwas Verbotenes befindet. Das ist eine gute Überprüfung, jedoch nicht so sicher, wie das tatsächliche Öffnen des Pakets und die Überprüfung des Inhaltes. Wenn das Paket akzeptabel aussieht, dann öffnet der Pförtner das Tor und gestattet dem Fahrer des LKWs den Zutritt auf das Werksgelände.

Die Statusinformationen können in Form von Zuständen mit den entsprechenden Informationen festgehalten werden. Zustände sind zum Beispiel Verbindungsaufbau, Transferzustand oder Verbindungsabbau für die jeweilige Kommunikationsebene. In jedem Zustand kann dann eine andere Interpretation der Kommunikationsdaten erfolgen.

Mit dieser erweiterten Funktionalität werden sie oft als Stateful Inspection-Firewall angeboten.

Diese zustandsorientierten Packet Filter haben die Vorteile von Packet Filtern, können aber zusätzlich die Anwendungen kontrollieren.

Das gleichzeitige Festhalten und Interpretieren der Kommunikationsdaten auf den verschiedenen Kommunikationsebenen ist sehr komplex. Aus diesem Grund haben zustandsorientierte Packet Filter in der Regel eine geringere Tiefe der Analyse oder sind besonders fehleranfällig. Kommunikationsprotokolle sind aus Gründen der Komplexität extra in Schichten unterteilt. Jede Schicht ist für eine Kernfunktionalität der Kommunikation verantwortlich. Darunterliegende Schichten müssen sich mit diesen Komplexitäten nicht beschäftigen, sondern können sich vielmehr auf deren Funktionalitäten verlassen. Aus diesem Grund ist eine Zusammenführung der Schichten im Rahmen einer Analyse bereits konzeptionell mit großen Hürden behaftet und führt in der praktischen Umsetzung zu Fehlern. Prinzipiell ist es auch nicht möglich, die komplexe Software von zustandsorientierten Packet Filtern so weit auszutesten, dass in nachweislich keinem Betriebszustand Fehler auftreten können. Aus diesem Grund muss auch in Zukunft immer wieder damit gerechnet werden, dass die komplexen Programme potenzielle Sicherheitsrisiken aufweisen, die für Angriffe verwendet werden können.

### Möglichkeiten, Vorteile und besondere Aspekte von zustandsorientierten Packet Filtern:

- wenn keine Authentifikation notwendig ist: transparent, das heißt, unsichtbar für den Nutzer und die IT-Systeme und ohne ihre aktive Einwirkung tätig
- einfach erweiterungsfähig für neue Protokolle
- flexibel für neue Dienste
- eventuell für andere Protokollfamilien verwendbar (IPX, OSI, DECNET, SNA...)

### Nachteile und Grenzen von zustandsorientierten Packet Filtern:

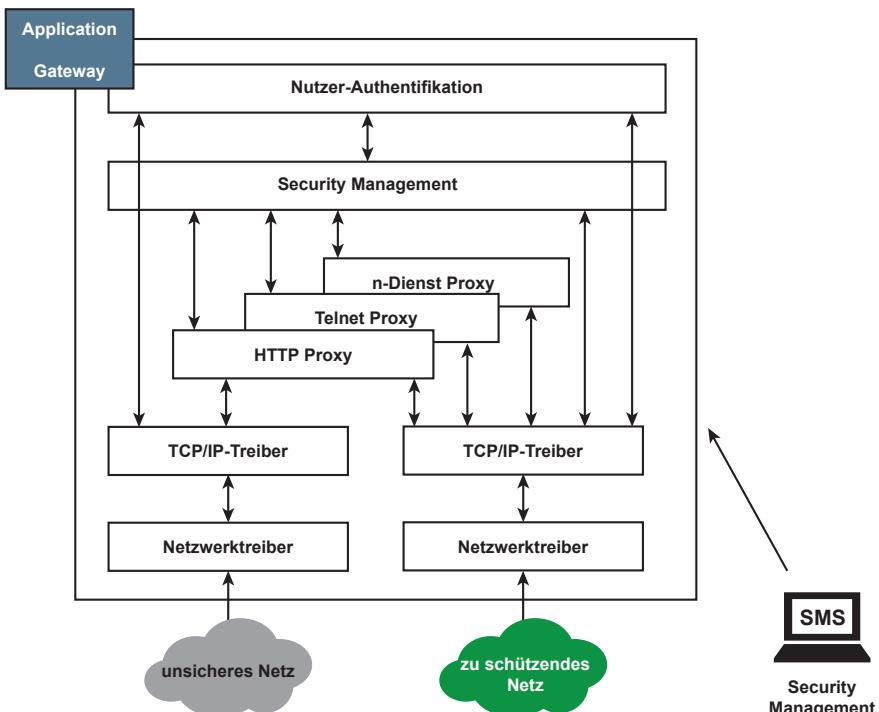
- Komplexität der Lösung
- falsch konfigurierte und fehlerbehaftete Programme auf IT-Systemen im zu schützenden Netz können bei erlaubten Kommunikationsverbindungen von außen genutzt werden, da ein direkter Zugriff auf das IT-System besteht
- typische zustandsorientierte Packet Filter können die Struktur des zu schützenden Netzes nicht verbergen

Ein besseres und sicheres Konzept der Analyse der Anwendungsdaten ist das Konzept von Application Gateways mit Proxys, das im folgenden Abschnitt beschrieben wird.

## 9.10 Application Gateway/Proxy-Technik

Im folgenden Abschnitt wird die Arbeitsweise des aktiven Firewall-Elements „Application Gateway“ beschrieben.

Das Application Gateway zeichnet sich dadurch aus, dass es die Netze sowohl logisch als auch physikalisch entkoppeln kann, siehe Abb. 9.11.



**Abb. 9.11** Application Gateway

Da in einigen Firewall-Konzepten das Application Gateway das einzige vom unsicheren Netz erreichbare IT-System ist, muss das Application Gateway besonders geschützt werden. Aus diesem Grund wird das IT-System, auf dem das Application Gateway realisiert ist, auch als Bastion bezeichnet.

Das Application Gateway – als Dual-homed Gateway realisiert – arbeitet mit zwei Netzwerk-Anschlüssen. Dual-homed bedeutet, dass das Application Gateway die vollständige Kontrolle über die Pakete hat, die zwischen dem unsicheren und dem zu schützenden Netzwerk übertragen werden sollen.

### **Analogie zum Pförtner**

Der Application-Gateway-Pförtner schaut sich nicht nur die Adressen der eingehenden Lieferungen an, er öffnet auch jedes Paket und prüft den kompletten Inhalt und checkt die Arbeitspapiere des Absenders gegen eine klar festgelegte Reihe von Beurteilungskriterien. Nach der erfolgten detaillierten Sicherheitsüberprüfung unterzeichnet der Pförtner den Lieferschein und schickt den LKW weg. Stattdessen bestellt er einen vertrauenswürdigen eigenen Fahrer der Firma, der nun die Pakete zum eigentlichen Empfänger bringt. Die Sicherheitskontrolle ist an dieser Stelle wesentlich zuverlässiger und der Fahrer der Fremdfirma erhält keinen weiteren Einblick in das Firmengelände. Die Überprüfungen nehmen zwar mehr Zeit in Anspruch, dafür können jedoch sicherheitsgefährdende Aktivitäten ausgeschlossen werden.

### **Allgemeine Arbeitsweise des Application Gateways**

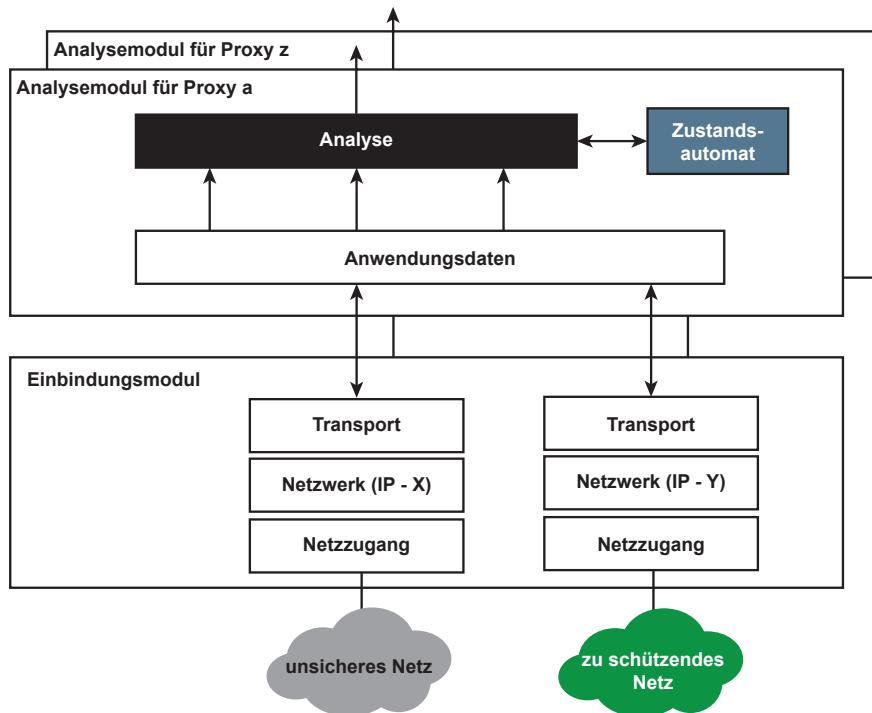
Ein Nutzer, der über das Application Gateway kommunizieren möchte, muss sich zuerst identifizieren und authentisieren. Application Gateways bieten in der Regel unterschiedliche Authentifikationsverfahren an.

Aus diesem Grund baut der Nutzer zuerst eine Verbindung mit dem Application Gateway auf. Der direkte Kommunikationspartner ist nicht sein Ziel-IT-System, sondern das Application Gateway beziehungsweise der entsprechende Proxy für die Anwendung. Nach der Identifikation und Authentifikation arbeitet das Application Gateway aber transparent, sodass der Nutzer den Eindruck hat, direkt auf dem Ziel-IT-System zu arbeiten.

### **Grundsätzlicher Ansatz**

Über die Netzzugangs- und TCP/IP-Treiber empfängt das Application Gateway die Pakete an den entsprechenden Ports. Soll nur ein Dienst über einen entsprechenden Port möglich sein, muss auf dem Application Gateway eine Software zur Verfügung gestellt werden, die das entsprechende Paket von der einen Netzwerkseite zur anderen Netzwerkseite des Application Gateways überträgt und umgekehrt. Eine solche Software, die die Paketübertragung nur für einen speziellen Dienst (HTTP, FTP, Telnet usw.) im Application Gateway durchführt, wird als Proxy bezeichnet.

Der Name Proxy – Stellvertreter – wird verwendet, weil es aus Sicht des zugreifenden Nutzers so aussieht, als würde er mit dem eigentlichen Server-Prozess des Dienstes auf dem Ziel-IT-System kommunizieren, siehe Abb. 9.12.



**Abb. 9.12** Analysemodule für Proxys auf dem Application Gateway

Jeder Proxy auf dem Application Gateway kann speziell für den Dienst, für den er zuständig ist, weitere Sicherheitsdienste anbieten. Bedingt durch den jeweiligen speziellen Proxy und das Wissen um den Kontext eines speziellen Dienstes ergeben sich umfangreichere Sicherungs- und Protokollierungsmöglichkeiten im Application Gateway.

Die Analyse ist auf dieser Kommunikationsebene besonders intensiv möglich, da der Kontext der Anwendungsdaten für den jeweiligen Dienst klar definiert ist. Die Proxys konzentrieren sich auf das Wesentliche. Der Vorteil ist, dass kleine überschaubare Module verwendet werden können, da eine Analyse innerhalb einer Schicht erfolgt. Dadurch wird die Fehleranfälligkeit durch Implementationsfehler reduziert.

### Sicherheitskonzept eines Application Gateways

Für jeden Dienst, der über das Application Gateway möglich sein soll, muss ein spezieller Proxy zur Verfügung gestellt werden.

Sollen bestimmte Dienste generell nicht möglich sein, dann darf für diese Dienste kein Proxy auf dem Application Gateway vorhanden sein, aber auch keine weitere Software, die den Dienst ermöglichen könnte!

Aus diesem Grund ist so wenig Software wie möglich auf dem Application Gateway zu installieren, damit nicht zufällig – oder absichtlich durch einen Angreifer von außen provoziert – eine andere Software die Aufgabe eines Proxys (Paketübertragung im Application Gateway) für einen Dienst übernimmt, der nicht erlaubt sein soll.

Das Security-Management, das dem Nutzer die Arbeit so leicht wie möglich gestalten soll und deshalb mit einer mächtigen Software (X-Terminal, Datenbank, ...) ausgestattet ist, darf aus Sicherheitsgründen nicht auf dasselbe IT-System. Application Gateways sollen aus Sicherheitsgründen keine Routing-Funktionalität haben, damit nicht an den Proxys vorbeigeroutet werden kann.

Da das Application Gateway bei der Kommunikation jeweils zum IT-System des unsicheren Netzes und zu dem des zu schützenden Netzes eine Kommunikationsverbindung hat, bietet das Application Gateway eine „Network Address Translation“. Dazu hat das Application Gateway eine IP-Adresse im unsicheren Netz (zum Beispiel eine offizielle Internet IP-Adresse 194.173.3.1) und eine IP-Adresse im zu schützenden Netz (zum Beispiel eine für diesen Zweck reservierte IP-Adresse 192.168.1.60). Bei der Kommunikation mit den IT-Systemen des unsicheren Netzes verwendet das Application Gateway die IP-Adressen des unsicheren Netzes, und bei der Kommunikation mit den IT-Systemen des zu schützenden Netzes verwendet das Application Gateway die IP-Adressen des zu schützenden Netzes.

## Proxys

Bei der Realisierung von Proxys wird zwischen Application Level und Circuit Level Proxys unterschieden. Application Level Proxys sind für bestimmte Dienste/Anwendungen implementiert. Das heißt, sie kennen die Kommandos der Anwendungsprotokolle und können diese analysieren und kontrollieren. Application Level Proxys arbeiten mit der gängigen, unveränderten Client-Software für FTP, Telnet oder Browser zusammen.

Einige Proxys funktionieren nach dem Store-and-Forward-Prinzip (SMTP), andere interaktiv und nutzerorientiert (Telnet, FTP, HTTP, ...). Da bei Application Gateways ein Routing auf der Netzwerkebene aus Sicherheitsgründen nicht möglich sein darf, könnten für Dienste, für die kein Application Level Proxy zur Verfügung steht, sogenannte Circuit Level Proxys zur Verfügung gestellt werden, wenn eine Kommunikation über das Application Gateway realisiert werden soll. Circuit Level Proxys sind eine Art generische Proxys, die für eine Mehrzahl von Diensten mit verschiedenen Protokollen verwendet werden können. Diese Circuit Level Proxys, die auch als generische Proxys, Port-Relays oder Plug-Gateways bezeichnet werden, können in der Regel für TCP und UDP-Anwendungen verwendet werden.

## Anwendungsgebiete von Application Gateways

Immer dann, wenn es notwendig ist, Schutzmaßnahmen für die Anwendungen zur Verfügung zu stellen, ist ein Application Gateway ein ideales aktives Firewall-Element. Die Möglichkeit der Protokollierung auf der Anwendungsebene

kann ebenfalls ein besonderer Grund sein, das Application Gateway in einem Firewall-Konzept zu berücksichtigen.

Für die Ankopplung an das Internet ist auf jeden Fall ein Application Gateway in der Firewall-Konstellation zu berücksichtigen, wenn die IT-Systeme im zu schützenden Netz einen hohen Schutzbedarf haben.

Außerdem können Organisationseinheiten, die sich abschotten wollen, hiermit einen besonderen Schutz erzielen.

#### **Vorteile und besondere Aspekte eines Application Gateways:**

- sicheres Design-Konzept, da kleine, gut überprüfbare Module (Proxys)
- Konzentration auf das Wesentliche
- Alle Pakete müssen über Proxys übertragen werden, das bedeutet höhere Sicherheit.
- Der Kommunikationspartner der IT-Systeme, die über das Application Gateway kommunizieren, ist der Proxy; dadurch kann eine echte Entkopplung der Dienste erreicht werden.
- Verbindungsdaten und Applikationsdaten können protokolliert werden, wodurch die Handlungen der Nutzer, die über das Application Gateway kommunizieren, festgehalten werden können.
- Verbergen der internen Netzstruktur
- Sicherheitsfunktionen für die Anwendungen werden zur Verfügung gestellt (Kommando-, Datei- und Daten-Filter usw.).
- Eine Network Address Translation findet statt.

#### **Nachteile und Grenzen eines Application Gateways:**

- geringe Flexibilität, da für jeden neuen Dienst ein neuer Proxy zur Verfügung gestellt werden muss
- Die Kosten für ein Application Gateway sind in der Regel höher.
- andere Vorgehensweise bei der Kommunikation über das Application Gateway (ist nicht transparent)
- Bei verschlüsselten Kommunikationskanälen zwischen Server und Client muss das Application Gateway eigene Zertifikate zu der Serveranwendung erzeugen und mit einer eigenen CA signieren. Das entsprechende Root-Zertifikat der CA muss von den Clients im zu schützenden Netz installiert und akzeptiert werden. Hiermit wird das Prinzip von End-to-End-Verschlüsselung und PKIs ausgebahlt. Daraus könnte eine Reduzierung der Cyber-Sicherheit resultieren.

---

## **9.11 Next-Generation-Firewall**

Bei einer Next-Generation-Firewall können die Analyse-Module unterschiedliche Anwendungsdaten in einem Datenstrom unabhängig von der Portnummer erkennen und entsprechend filtern.

Zum Beispiel werden über das Universalprotokoll HTTP fast alle Arten von Informationen transportiert. Aus diesem Grund ist es für den Administrator einer

Firewall nur schwer kontrollierbar, welche Dienste die Mitarbeiter nutzen dürfen und welche nicht. Mit einer herkömmlichen Firewall ist es beispielsweise nicht möglich, den Remotezugriff der Team-Viewer-Software zu blockieren ohne gleichzeitig den gesamten Webseitenzugriff zu blockieren, da Team-Viewer HTTP (Port 80) verwendet. Bisherige Firewalls erlauben es nicht, solche Dienste explizit zu erkennen und ggf. zu blockieren. Ein weiterer Nachteil der herkömmlichen Firewall-Variante ist, dass viele Anwendungen die freigegebenen Standard-Ports durch sogenanntes Port-Hopping ausnutzen, um so eine mühelose Kommunikation zu erlangen. Port-Hopping ist eine Technik, die von vielen Programmen für eine erfolgreiche Kommunikation durch Firewalls genutzt wird. Im Fall eines geblockten Ports wechselt die Software auf einen Standard-Port (zum Beispiel Port 80) und kommuniziert über diesen Weg typischerweise ungehindert weiter.

### Identifizieren von Anwendungen

Die Anwendungserkennung stellt die wesentliche Funktion einer Next-Generation-Firewall dar und ermöglicht einem Administrator eine erhöhte Kontrolle über den Datenstrom. Sie erkennt zum einen, welche Anwendung den Datenstrom erzeugt und zum anderen, welche Funktionen einer Anwendung genutzt werden, siehe Abb. 9.13.

Somit kann ein Administrator zum Beispiel das Telefonieren über Skype erlauben, den Datentransfer über die selbe Software jedoch blockieren. Die Erkennung der Anwendungen verläuft unabhängig vom Port oder Protokoll mittels Analyse durch Erkennungsmuster. Vergleichbar mit Anti-Malware-Lösung besitzt eine Next-Generation-Firewall eine Datenbank mit Signaturen zu den Anwendungen und deren Funktionen beziehungsweise Subanwendungen. Häufig bleiben die Protokolle, die von Anwendungen genutzt werden, viele Jahre unverändert, womit eine Signatur zur Erkennung der Anwendung ausreicht. Auf der anderen Seite werden Webanwendungen häufig angepasst. Damit die Next-Generation-Firewall auch hier die Webanwendungen richtig analysieren kann, sind regelmäßige Aktualisierungen der Signaturen seitens der Next-Generation-Firewall-Hersteller nötig.

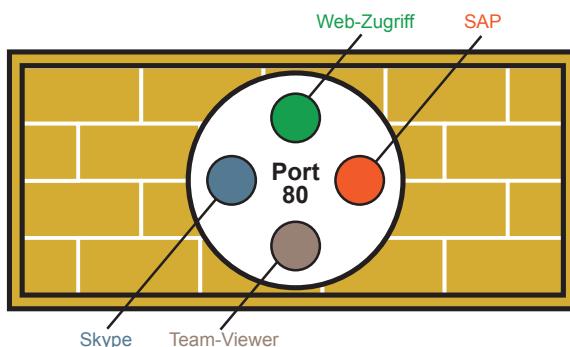


Abb. 9.13 Anwendungserkennung einer Next-Generation-Firewall

Laut einiger Herstellerangaben identifizieren die Next-Generation-Firewalls bis zu 1000 Anwendungen und bis zu 100.000 Subanwendungen, mit denen einzelne Funktionen der Anwendungen gesteuert werden können. Ein weiteres wesentliches Merkmal einer Next-Generation-Firewall ist auch, dass sie Datenströme zu Nutzern zuordnen kann. Dazu wird eine Kombination von Nutzern und IP-Adressen ermittelt. Der Vorteil der Nutzererkennung ergibt sich dadurch, dass den Nutzern Rollen und Gruppenzugehörigkeiten zugeordnet werden können. Damit ist genau erkennbar, welcher Nutzer welche Kommunikation aufbaut und welche Anwendungen dabei verwendet werden. So lässt sich zum Beispiel die Verwendung von sozialen Netzwerken, wie Facebook oder Xing, auf die Personalverwaltung begrenzen, da diese die Netzwerke für die Personalbeschaffung benötigt. Anderen Abteilungen könnte der Zugriff an dieser Stelle verwehrt werden.

---

## 9.12 Firewall-Konzepte

Bei aktiven Firewall-Elementen handelt es sich um Sicherheitskomponenten, die ausschließlich für die Erbringung von Sicherheitsdiensten verantwortlich sind.

Die vorgestellten Firewall-Elemente unterscheiden sich nach dem Maß an Sicherheit, das sie erbringen können, und nach den Einsatzfällen, für die sie sich eignen.

Die verschiedenen Firewall-Elemente können als Firewall-System eigenständig Sicherheit zum Schutz zwischen Netzen erbringen oder mit einer geschickten Kombination der einzelnen Firewall-Elemente ein höheres Maß an Sicherheit erzielen.

### High-Level-Security-Firewall-System

Ein High-Level-Security-Firewall-System fasst mehrere aktive Firewall-Elemente zusammen, sodass ein Höchstmaß an Sicherheit garantiert werden kann, siehe Abb. 9.14.

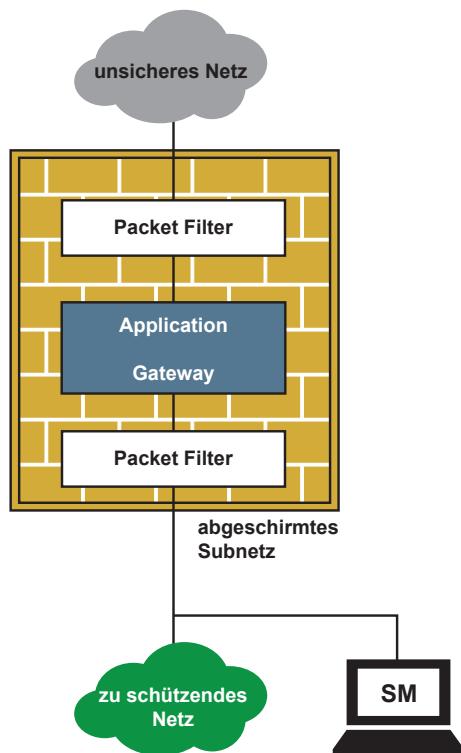
Das High-Level-Security-Firewall-System besteht aus einem Screened Subnet mit einem dual-homed Application Gateway und einem separaten Security-Management. In diesem Firewall-System werden die aktiven Firewall-Elemente Packet Filter und Application Gateway hintereinander geschaltet.

Das dual-homed Application Gateway befindet sich bei diesem Firewall-Konzept im Screened Subnet. Durch die Packet Filter wird das dual-homed Application Gateway vor Angriffen aus dem unsicheren und dem zu schützenden Netz geschützt.

### Bewertung des High-Level-Security-Firewall-System-Konzepts

Die Kommunikation zwischen IT-Systemen im zu schützenden Netz und IT-Systemen aus dem unsicheren Netz wird durch die Packet Filter und das dual-homed Application Gateway kontrolliert. Dieses Konzept lässt keine Möglichkeit zu, das dual-homed Application Gateway zu umgehen.

**Abb. 9.14** High-Level-Security-Firewall-System



Das Maß an Sicherheit, das dieses Firewall-Konzept bietet, addiert sich aus der Sicherheitsleistung des Packet Filters und der Sicherheit des dual-homed Application Gateway, sodass eine besonders hohe Gesamtsicherheit erreicht wird.

Der Grundgedanke und die Zielsetzung eines High-Level-Security-Firewall-Systems lassen sich durch folgende Punkte beschreiben:

- **Einfache Regeln:** Die Anordnung der Elemente ermöglicht eine einfache Definition der Regeln für die einzelnen aktiven Firewall-Elemente. Aus der Sicht des Packet Filters kommuniziert immer nur der Application Gateway mit den IT-Systemen des entsprechenden Netzes.
- **Gegenseitiger Schutz:** Die Packet Filter sorgen dafür, dass nicht jeder auf das dual-homed Application Gateway zugreifen darf, und schützen damit das dual-homed Application Gateway selbst.
- **Geschachtelte Sicherheit:** Wer auf ein zu schützendes Netz zugreifen will, das durch ein High-Level-Security-Firewall-System abgeschottet wird, muss verschiedene Barrieren überwinden: zuerst einen Packet Filter, dann ein dual-homed Application Gateway und zum Schluss wieder einen Packet Filter.

- **Verschiedene Betriebssysteme:** Aus Sicherheitsgründen verwenden High-Level-Security-Firewall-Lösungen für die verschiedenen aktiven Firewall-Elemente verschiedene Betriebssysteme: ein LINUX-Betriebssystem für das dual-homed Application Gateway und ein Real-Time-Betriebssystem für die Packet Filter. Eventuell auftretende Betriebssystemfehler oder Lücken wirken sich dadurch nur jeweils auf ein aktives Firewall-Element aus.
- **Unterschiedliche Einbindungs- und Analysemöglichkeiten:** Außerdem arbeiten die verschiedenen aktiven Firewall-Elemente mit unterschiedlichen Strategien (Sicherheitsansätzen). Die Packet Filter interpretieren die übertragenen Pakete von unten nach oben auf der Netzzugangs-, der Netzwerk- und der Transportebene. Das dual-homed Application Gateway interpretiert die Kommunikation auf der Anwendungsebene. Auch hier können sich mögliche Schwächen der Einbindungs- und Analysemöglichkeiten nur jeweils auf ein aktives Firewall-Element auswirken.
- **Separates Security-Management:** Das separate Security-Management stellt viele eigene Sicherheitsmechanismen wie Zugangskontrolle, Rechteverwaltung, Verschlüsselung und Protokollierung zur Verfügung und sorgt auf diese Weise ebenfalls für High-Level Security.

### **Das Ganze ist mehr als die Summe der Einzelteile!**

Alle diese Sicherheitsmechanismen zusammen garantieren ein höheres Maß an Sicherheit als jeder Sicherheitsmechanismus für sich alleine, so wie bei einem Auto der Sicherheitsgurt, der Airbag, der Seitenauflaufschutz und die Knautschzone zusammen ein Höchstmaß an Sicherheit bieten.

#### Einsatzfall

Der Einsatz eines High-Level-Security-Firewall-Systems empfiehlt sich immer dann, wenn ein zu schützendes Netz an ein unsicheres Netz angekoppelt wird, das ein geringes oder nicht einschätzbares Schutzniveau hat und außerhalb des eigenen Verantwortungsbereiches liegt. Dies ist bei der Ankopplung an das Internet der Fall.

---

## **9.13 Konzeptionelle Möglichkeiten und Grenzen von Firewall-Systemen**

In diesem Abschnitt werden die konzeptionellen Möglichkeiten und Grenzen der Einbindung eines Firewall-Systems dargestellt.

### **9.13.1 Common Point of Trust**

Ein Firewall-System stellt den „Common Point of Trust“ für den Übergang zwischen unterschiedlichen Netzen dar. Das heißt, der einzige Weg zwischen den Netzen führt kontrolliert über das Firewall-System.

Firewall-Systeme werden verwendet, um sich an unsichere Netze wie zum Beispiel das Internet anzukoppeln. Firewall-Systeme werden aber auch eingesetzt, um das eigene Netz zu strukturieren und hier Sicherheitsdomänen mit unterschiedlichem Schutzbedarf zu schaffen.

### **Vorteile des “Common Point of Trust”-Konzepts:**

#### **1. Kosten**

Die Realisierung von Cyber-Schutzmaßnahmen in einem zentralen Firewall-System ist wesentlich effizienter als die Realisierung von Cyber-Schutzmaßnahmen auf jedem einzelnen IT-System, das im zu schützenden Netz steht.

#### **2. Umsetzung der Sicherheitsleitlinie**

Mithilfe eines zentralen Firewall-Systems kann die Sicherheitsleitlinie einer Organisation auf einfache Weise zentral durchgesetzt werden. Zum Beispiel werden die Dienste und Protokolle, die über ein Firewall-System möglich sein sollen, an einer zentralen Stelle für alle Nutzer definiert und überprüft.

#### **3. Möglichkeiten**

Eine kryptografische (starke) Authentisierung von Nutzern und IT-Systemen ist auf einem Firewall-System zu realisieren und nicht auf jedem einzelnen IT-System im zu schützenden Netz, damit die Nutzer sicher identifiziert und authentisiert werden können. Für heterogene IT-Systemlandschaften gibt es zurzeit keine Konzepte und Realisierungen, wie kryptografische Authentisierung auf den unterschiedlichen Betriebssystemen (LINUX, Microsoft Windows, iOS, Android, ...) praktisch realisiert werden kann. Hier können Kosten eingespart werden.

#### **4. Sicherheit durch Abschottung**

Durch die reduzierte Funktionalität, die ein Firewall-System anbietet, existieren weniger Angriffspunkte für Angreifer aus dem unsicheren Netz. Der Aufwand für Schutzmaßnahmen konzentriert sich auf das Firewall-System. Dadurch wird erreicht, dass die IT-Systeme des zu schützenden Netzes nicht mehr von einem IT-System aus dem unsicheren Netz (zum Beispiel Internet) angegriffen werden können, sondern IT-Systeme von außerhalb durch das Firewall-System abgeblockt werden. IT-Systeme können nicht mehr zum Ziel von Angreifern aus dem unsicheren Netz werden, wenn sie falsch installiert oder konfiguriert sind. Alle Schutzmaßnahmen sind in dem Firewall-System konzentriert realisiert.

#### **5. Überprüfbarkeit**

Durch den klaren Übergang (Common Point of Trust) zwischen zwei Netzen ist eine einfache und vollständige Protokollierungsmöglichkeit vorhanden, da die gesamte Kommunikation über das Firewall-System läuft.

### **9.13.2 Konzeptionelle Grenzen eines Firewall-Systems**

Die Firewall-Systeme, die die Sicherheitsdienste für die Kommunikation im Internet und Intranet bereitstellen, sind sehr komplexe technische Sicherheitsmaßnahmen. Dennoch können auch aufwendige Firewall-Systeme keine hundertprozentige Sicherheit gewährleisten.

Im Folgenden werden einige Aspekte aufgezeigt, die beim Einsatz von Firewall-Systemen zu beachten sind:

#### **1. Hintertüren**

Ein Firewall-System schützt genau die Kommunikationsverbindungen, die darüber erfolgen. Gibt es Kommunikationsübergänge am Firewall-System vorbei (backdoors), hat das Firewall-System keine Sicherheitswirkung mehr. Deshalb ist es absolut wichtig, dass keine weitere Verbindung zwischen dem unsicheren Netz und dem zu schützenden Netz besteht, damit das „Common Point of Trust“-Konzept realisiert werden kann. Dafür sind entsprechende personelle und organisatorische Sicherheitsmaßnahmen nötig.

#### **2. Interne Angriffe**

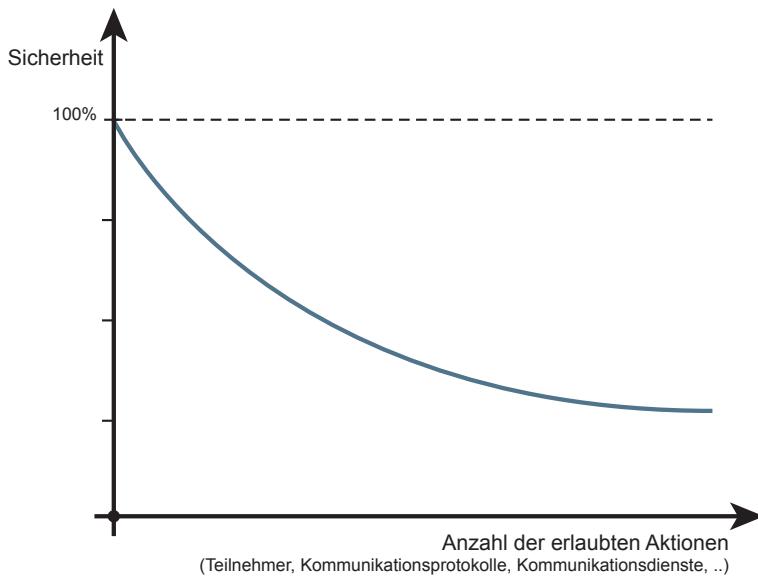
Ein Firewall-System bietet Cyber-Sicherheitsdienste zur Abschottung gegen das unsichere Netz oder zur Kontrolle der Kommunikation zwischen dem unsicheren Netz und dem zu schützenden Netz. Das Firewall-System selbst bietet nur einen sehr geringen Schutz vor internen Angriffen. Um internen Angriffen entgegenzuwirken, müssen weitere, ergänzende Sicherheitsmechanismen (zum Beispiel Intrusion Detection Systeme) eingeführt werden.

#### **3. Wissen und Hypothese**

Mit einem Firewall-System können durch theoretisches Wissen und praktische Erfahrungen Fehlerursachen verhindert werden. Gerade bei innovativen Anwendungen und Technologien, wie dem Internet, wird mit einer Vielzahl von Hypothesen gearbeitet. Daher gibt es einen Bereich des Neuen, Unbekannten und auch Unerwünschten und Unvorhersehbaren, was mithilfe eines Firewall-Systems nicht beherrscht werden kann, weil dieses nur auf Ereignisse reagieren kann, die bereits eindeutig bekannt sind. Hier liegt eine Grenze von Firewall-Systemen. Diesem kann nur mit weiteren, modular ergänzten Sicherheitsmechanismen entgegengewirkt werden.

#### **4. Richtige Sicherheitspolitik und richtige Umsetzung der Sicherheitspolitik**

Ein Firewall-System kann nur die Sicherheitsdienste erbringen, die eingerichtet sind. Deshalb ist es von besonderer Bedeutung, dass eine Sicherheitspolitik erarbeitet wird, die darstellt, welche Ressourcen (IT-Systeme, Kommunikations-einrichtungen, Daten usw.) im zu schützenden Netz einen hohen Schutzbedarf haben und wie sie geschützt werden sollen. Außerdem muss definiert werden, auf welche Weise die Sicherheitsmechanismen für die Aufrechterhaltung des sicheren Betriebs eines Firewall-Systems periodisch überprüft werden.



**Abb. 9.15** Security versus Connectivity

##### 5. security versus connectivity $\Leftrightarrow$ Risiko versus Chance

Je kleiner die Menge erlaubter Aktionen ist, umso geringer ist das Risiko, dass ein Schaden auftreten kann. Jeder Teilnehmer, jedes IT-System, das über ein Firewall-System kommunizieren darf, stellt ein zusätzliches Risiko dar. So stellen zum Beispiel auch die erlaubten Kommunikationspartner ein Risiko dar, falls sie unberechtigte Kommunikationsverbindungen nutzen. Aus diesem Grund ist zu beachten: so wenig wie möglich/nötig über das Firewall-System zulassen, damit ein Höchstmaß an Cyber-Sicherheit erreicht werden kann, siehe Abb. 9.15.

Je mehr erlaubt ist, umso größer ist das Risiko der Verwundbarkeit. Wenn nichts erlaubt ist, kann über das Netz auch kein Schaden auftreten. Hier wird das Spannungsfeld zwischen „security und connectivity“ deutlich. Mithilfe eines Firewall-Systems sollen die Vorteile der Kommunikation nach außen genutzt, aber der mögliche Schaden durch diese Handlungen begrenzt werden.

Die Teilnehmer, die zur Erfüllung ihrer Aufgabenstellung kommunizieren müssen, sollen mit den Kommunikationsprotokollen und -diensten, die sie für ihre speziellen Aufgaben benötigen, dies zu den entsprechenden Zeiten tun dürfen – aber nur so weit, wie es dafür nötig ist.

**Wichtig** Mithilfe eines Firewall-Systems sollen die Vorteile der Kommunikation nach außen genutzt, aber der mögliche Schaden begrenzt werden.

## Vertrauenswürdigkeit des Kommunikationspartners und der empfangenen Daten

Für die Entscheidungen, die ein Firewall-System durchführt, ist die Vertrauenswürdigkeit des Kommunikationspartners und der empfangenen Daten notwendig. Da diese Eigenschaften nicht durch Sicherheitsmechanismen des Firewall-Systems vollständig erbracht werden können, müssen hier weitere, ergänzende Sicherheitsmechanismen wie zum Beispiel Verschlüsselung (VPN) oder digitale Signatur eingesetzt oder schon vorhandene im Firewall-System aktiviert werden.

---

## 9.14 Das richtige Firewall-Konzept für jeden Anwendungsfall

Um eine einschätzbare Aussage über Firewall-Systeme treffen zu können, ist die Sicherheitseinstufung von Firewall-Konzepten sehr hilfreich. Dabei werden folgende Einsatzfälle definiert, die nach den Kriterien Vertrauenswürdigkeit des Netzes und des Kommunikationspartners sowie des Angriffspotenzials in Abhängigkeit betrachtet werden:

1. das unsichere Netz ist innerhalb der eigenen Organisation oder
2. das unsichere Netz ist außerhalb der eigenen Organisation

Die wichtigste Motivation für den Einsatz eines Firewall-Systems ist also die Reduzierung des Risikos der Verwundbarkeit, wenn ein Schutzbedarf der eigenen Werte besteht. Wenn das zu schützende Netz keinen Schutzbedarf hat, muss auch kein Firewall-System eingesetzt werden. Wenn aber ein Schutzbedarf vorliegt, dann muss der Einsatzfall entsprechend berücksichtigt werden und ein angemessenes Firewall-Konzept ist auszuwählen.

Im Folgenden wird eine Methode erläutert, wie dies in der Praxis mit den gewonnenen Erkenntnissen geschehen kann.

### Definition des Einsatzfalles:

In der Tab. 9.2 werden zwei Einsatzfälle von Firewall-Systemen definiert, diskutiert und bewertet.

Tab. 9.3. zeigt, wie in Abhängigkeit des Schutzbedarfs und des Einsatzfalles welches aktive Firewall-Elemente oder eine Kombination aktiver Firewall-Elemente verwendet werden sollen. Die Definition des Schutzbedarfs ist an das Grundschutzhandbuch des BSIs angelehnt.

In Tab. 9.3 ist ein Beispiel für eine Entscheidungsmatrix für das Firewall-Konzept dargestellt.

Falls überhaupt ein Schutzbedarf besteht, ist für die Kommunikation mit einem unsicheren Netz außerhalb des eigenen Verantwortungsbereiches immer ein dual-homed Application Gateway im Firewall-Konzept notwendig.

Dem Schutzbedarf entsprechend kann dann entweder nur ein dual-homed Application Gateway oder ein Gateway in Kombination mit einem Packet Filter beziehungsweise einem Screened Subnet zum Einsatz kommen.

**Tab. 9.2** Einsatzfälle von Firewall-Systemen

	Einsatzfall	
<b>Kriterien</b>	das unsichere Netz ist innerhalb der eigenen Organisation	das unsichere Netz ist außerhalb der eigenen Organisation
Vertrauenswürdigkeit des Netzes	sehr hoch • liegt in der eigenen Verantwortung • wird regelmäßig überprüft	von speziellen, <b>schwer ermessbaren</b> Faktoren abhängig • liegt nicht in der eigenen Verantwortung • es muss mit allen Risiken gerechnet werden
Vertrauenswürdigkeit des Kommunikationspartners	sehr hoch • die Kommunikationsteilnehmer gehören zur gleichen Organisation und arbeiten unter der gleichen Sicherheitspolitik	es wird hier angenommen, dass diese <b>sehr gering</b> ist
Angriffspotenzial	sehr gering • die Kommunikationsteilnehmer gehören zur gleichen Organisation und arbeiten unter der gleichen Sicherheitspolitik	<b>sehr hoch</b> • die Teilnehmer des Netzes haben einen sehr unterschiedlichen Schutzbedarf (Hacker neben professionellen Anwendungen) • zum Beispiel Internet

**Tab. 9.3** Entscheidungsmatrix für das Firewall-Konzept

Schutzbedarf	Risiken	Einsatzfall	Firewall-Konzept
niedrig	<ul style="list-style-type: none"> <li>• geringfügiger Verstoß gegen Gesetze</li> <li>• beschränkte negative Außenwirkung</li> <li>• finanzieller Schaden &lt; 25.000 EUR</li> </ul>	innerhalb der Organisation:	Packet Filter
		außerhalb der Organisation:	Dual homed Applikation Gateway
hoch	<ul style="list-style-type: none"> <li>• erheblicher Verstoß gegen Gesetze</li> <li>• breite negative Außenwirkung</li> <li>• finanzieller Schaden &lt; 5 Mio. EUR</li> </ul>	innerhalb der Organisation:	Packet Filter + Single-homed Applikation Gateway <i>oder</i> Stateful Inspection <i>oder</i> Adaptiv Proxy
		außerhalb der Organisation:	Packet Filter + dual homed Applikation Gateway
Sehr hoch	<ul style="list-style-type: none"> <li>• fundamentaler Verstoß gegen Gesetze</li> <li>• existenzgefährdend negative Außenwirkung</li> <li>• finanzieller Schaden &gt; 5 Mio. EUR</li> </ul>	innerhalb der Organisation:	Screened Subnet mit Packet Filter + Single-homed Applikation Gateway
		außerhalb der Organisation:	Screened Subnet mit Packet Filter + dual homed Applikation Gateway • High-Level Firewall-System

Falls das unsichere Netz innerhalb des eigenen Verantwortungsbereiches liegt, wie zum Beispiel dem Intranet, genügt es, abhängig vom Schutzbedarf, nur Packet Filter oder Kombinationen mit single-homed Application Gateways zu verwenden. Eine Alternative in diesem Anwendungsbereich sind Stateful Inspection- oder Adaptiv Proxy-Lösungen, die auch auf der Anwendungsebene Sicherheitsfunktionen zur Verfügung stellen.

Durch die Kombination eines dual-homed Application Gateways mit Packet Filter oder Screened Subnet ist eine sehr hohe Sicherheit zu erreichen.

Stets muss der Leitsatz sein: „Das passende Firewall-Konzept für den jeweiligen speziellen Anwendungsfall“.

### Sicherheit in der Praxis

In der Diskussion über die Möglichkeiten und Grenzen von Firewall-Systemen ist deutlich geworden, dass es in der Praxis keine 100-prozentige Sicherheit gibt.

Es gibt aber definierte Cyber-Sicherheitsmechanismen und Cyber-Sicherheitskriterien, um das Maß an Cyber-Sicherheit zu erhöhen oder die Unsicherheiten zu verringern. Dabei muss für die konkrete Anwendung ein praxisgerechter Sicherheitsansatz realisiert werden.

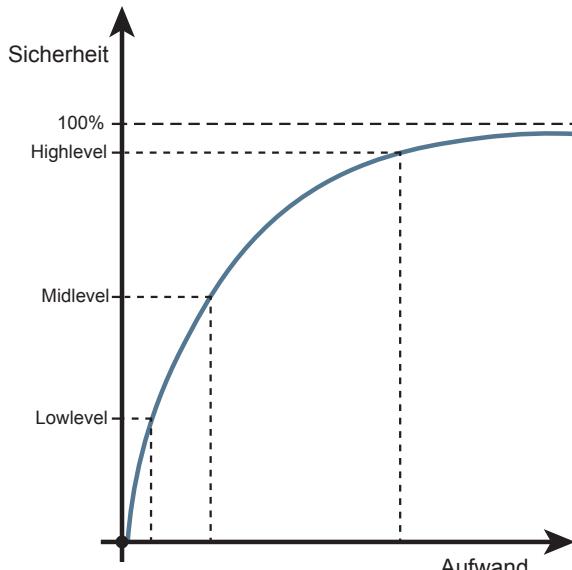
Praxisgerechte Sicherheit von Firewall-Systemen ist dann gegeben, wenn

- mit den verfügbaren Ressourcen
- durch die bekannten Angriffe
- mit vertretbarem Aufwand

das Firewall-System nicht überwunden werden kann.

In Abb. 9.16 wird verdeutlicht, wie die Sicherheit (unterteilt in die Stufen low, mid und high) in Abhängigkeit des Aufwandes betrachtet werden kann.

**Abb. 9.16** Sicherheit versus Aufwand



Für Netze mit hohem Schutzbedarf kann mit sehr hohem Aufwand High Level-Sicherheit erreicht werden.

## 9.15 Definition des Kommunikationsmodells mit integriertem Firewall-Element

Im Folgenden wird das Kommunikationsmodell mit integriertem Firewall-Element definiert. Das Firewall-System soll den Receiver  $\{r_1, \dots r_m\}$  vor Angriffen auf seine Werte aus dem unsicheren Netz schützen. Es wird davon ausgegangen, dass mithilfe eines Security-Managements die Rechte in das Firewall-Element, in Übereinstimmung mit der vorher festgelegten Sicherheitspolitik, eingetragen worden sind, die es ermöglichen sollen, die erlaubten Protokollelemente  $\{x_1, \dots x_l\}$  über das Firewall-Element übertragen zu können. Bei einer fehlerfreien Implementierung des Firewall-Elements und der Kommunikationsprotokolle und -dienste auf der Empfängerseite werden auch nur erlaubte Aktionen  $\{a_1, \dots a_t\}$  beim Receiver  $\{r_1, \dots r_h\}$  ausgeführt. Bei dem Kommunikationsmodell mit integriertem Firewall-Element müssen beliebig viele Transmitter und Receiver berücksichtigt werden.

### Kommunikationsmodell mit integriertem Firewall-Element, siehe Abb. 9.17.

Mithilfe der Betrachtung der möglichen Einflussfaktoren auf die Auswahl und Durchführung der Aktionen beim Receiver sollen Kriterien abgeleitet werden, mit deren Hilfe eine Aussage über die Möglichkeiten und Grenzen im Sinne der Sicherheit und Vertrauenswürdigkeit des Kommunikationsmodells mit integrierten Firewall-Systemen gemacht werden kann.

### Definition der Funktionen für die Auswahl der Aktion auf der Empfängerseite für „ $r_n$ “:

$ak = \text{action-select}(\text{protocol-state-machine}(xi^*, sj), \text{authenticity}(xi),$   
 $\text{result-of-decision}(\text{analysis}(xi^*), \text{security-management(rules)}),$   
 $\text{functionality-of-the-firewall-element}())$

- $a_k$  Teil-Aktion in einer Schicht, die in Abhängigkeit des empfangenen Protokoll-elementes  $x_i$  und des aktuellen Zustandes  $s_j$  ausgeführt wird
- $x_i^*$  Protokollelement, welches vom Sender zum Empfänger gesendet wird
- $x_i$  Protokollelement, welches auf der Empfangsseite ankommt
- $s_j$  aktueller Zustand (actual state)
- rules technische Umsetzung der Sicherheitspolitik (Access-Listen, ...)

Hinweis: Neben „ $r_n$ “ sind in der Regel weitere Empfänger  $\{r_1, \dots r_g\}$  zu berücksichtigen.

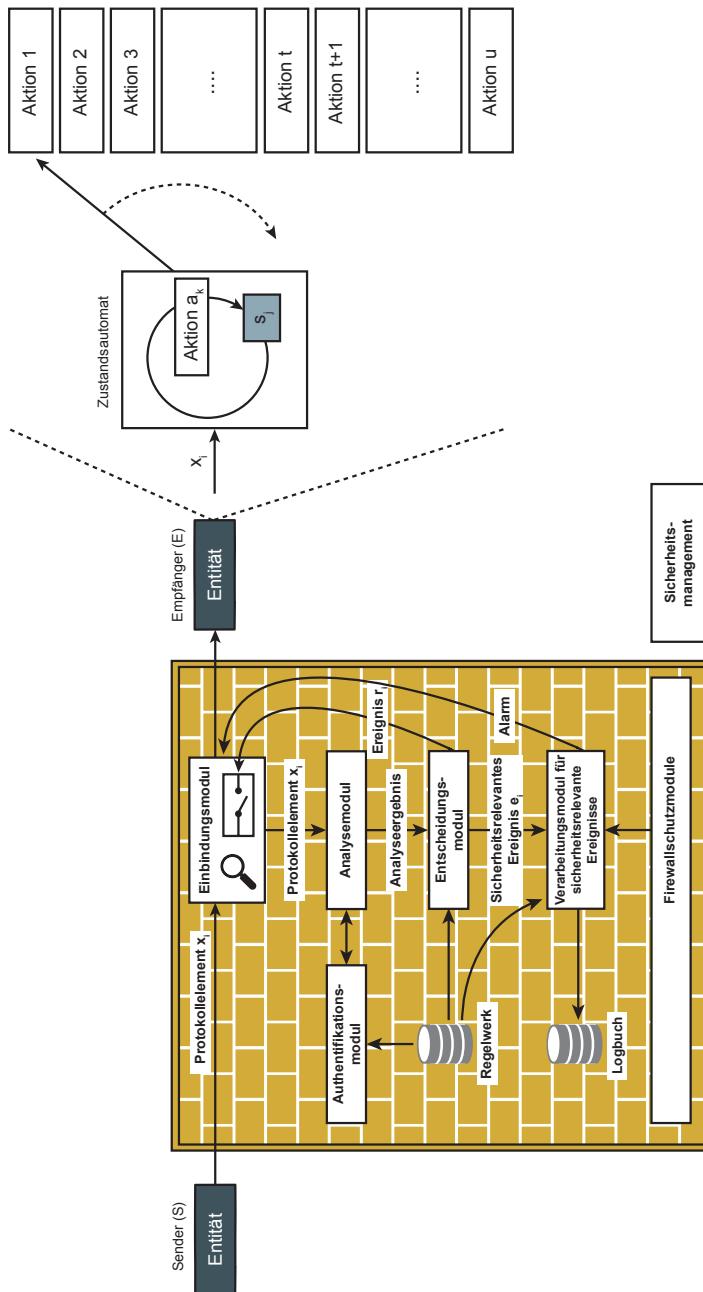


Abb. 9.17 Kommunikationsmodell mit integriertem Firewall-Element

## Grundsätzliche Einflussfaktoren für die Auswahl und Durchführung der Aktion auf der Empfängerseite

Im Folgenden werden die Funktionen und deren grundsätzliche Einflussfaktoren aufgezeigt, die bei der Kommunikation des Kommunikationsmodells mit integriertem Firewall-Element eine Rolle spielen. Es werden die Gründe festgehalten und erläutert, die sich für ein mögliches Fehlverhalten der Kommunikationsabläufe trotz integriertem Firewall-Element herauskristallisiert haben.

### Fehlerquellen durch Angriffe aus dem Netz: Funktion: *authenticity* ( $x_i$ )

Für den richtigen Kommunikationsablauf ist wichtig, dass sowohl der Transmitter( $t_j$ ) authentisch/echt, als auch das Protokollelement  $x_i^*$  authentisch/echt und unversehrt übertragen worden ist.

Einflussfaktoren:

- Vertrauenswürdigkeit des Netzes
  - Vertrauenswürdigkeit des Kommunikationsteilnehmers
- oder/und
- Gewährleistung der Authentifikation des Kommunikationspartners
  - Gewährleistung der Authentifikation des Ursprungs der Daten

### Fehlerquellen der Kommunikationslösung beim Receiver:

Funktion: protocol-state-machine ( $x_i^*, s_j$ )

- Verantwortung des Anwenders
  - Einflussfaktor: **Konfiguration beim Empfänger**  
Die Konfiguration des Kommunikationsprotokolls oder -dienstes haben Fehler, die zur Folge haben, dass trotz erlaubtem Protokollelement ( $x_i$ ) eine nicht erlaubte Aktion auf der Empfängerseite durchgeführt wird.
- Verantwortung des Herstellers
  - Einflussfaktor: **Implementierung beim Empfänger**  
Die Implementierung des Kommunikationsprotokolls oder -dienstes hat Fehler, die zur Folge haben, dass trotz erlaubtem Protokollelement ( $x_i$ ) eine nicht erlaubte Aktion auf der Empfängerseite durchgeführt wird.

### Fehlerquellen des Firewall-Elements

- Verantwortung des Anwenders/Funktion: security-management(rules)
  - Einflussfaktor: Sicherheitspolitik  
Es wird mehr erlaubt, als für die eigentliche Aufgabenstellung der einzelnen Nutzer erforderlich ist.  
Die unbeabsichtigte falsche Eingabe der Regeln führt zu einem Fehlverhalten des Firewall-Elements.

Die beabsichtigte falsche Eingabe der Regeln verfolgt das Ziel, das Firewall-Element zu umgehen.

Die Einschränkung der Protokollelemente kann, zum Beispiel durch Unwissenheit oder nicht richtige Vorgabe, unzureichend sein.

Neue Angriffsmethoden, die dem Verantwortlichen des Firewall-Elements nicht bekannt sind, können daher auch nicht durch eine explizite Einschränkung verhindert werden.

- Verantwortung des Herstellers/**Funktion:** *analysis* ( $x_i$ )

- Einflussfaktor: Tiefe der Analyse

Die Analyse der Protokollelemente kann nicht detailliert genug Aussagen treffen und damit nur eingeschränkt Aktionen verhindern. Dadurch kann die Entscheidung Durchlass oder Sperren zu sehr begrenzt sein. Bei der Analyse der Protokollelemente können wichtige und/oder neue Entscheidungskriterien unberücksichtigt bleiben. Bei der Synthese der Kriterien zu Entscheidungen können Entscheidungsregeln nicht ausgereift oder nicht umfassend umgesetzt sein.

Dieser Punkt geht einher mit der Komplexität der möglichen Einschränkungen.

- **Funktion:** *result-of-decision* ( $\text{analysis}(x_i)$ , rules)

- Einflussfaktor: vertrauenswürdige Implementierung

Unzureichende Qualität der Realisierung des Firewall-Elements:

- Die Qualität der Realisierung eines Firewall-Elements ist derart, dass in bestimmten Situationen ein Fehlverhalten auftritt.
- Folgende Komponenten müssen betrachtet werden:
  - Betriebssystem, auf dem die Firewall-Applikation läuft
  - Firewall-Applikation
  - Security-Management
  - Hardware der Firewall-Elemente und des Security-Managements
  - Authentifikationskomponenten der Kommunikationspartner

## Sicherheitsdienste eines Firewall-Elements

**Funktion:** *functionality-of-the-firewall-element* ()

Tab. 9.4 beschreibt die Standardsicherheitsdienste eines Firewall-Elements. Für jeden Dienst wird aufgelistet, welche Informationen von dem Firewall-Element überprüft werden, welche Festlegungen und Maßnahmen getroffen werden, was geprüft wird und welchen Einfluss das auf Sicherheit und Vertrauenswürdigkeit von Firewall-Elementen hat.

**Tab. 9.4** Sicherheitsdienste eines Firewall-Elements

Sicherheitsdienst	Überprüfung/Festlegung/ Maßnahme	Was wird geprüft?	Einfluss auf Sicherheit und Vertrauenswürdig- keit
Zugangskontrolle auf Netzwerk- ebene	Welche IT-Systeme (Transmitter, Receiver) dürfen über das Firewall-Element miteinander kommunizieren?	<ul style="list-style-type: none"> <li>IP-Adressen der beteiligten IT- Systeme</li> <li>Zeit, zu der eine Aktion zulässig ist</li> </ul>	<ul style="list-style-type: none"> <li>vertrauenswürdige Implementierung</li> <li>Vertrauenswürdigkeit des Netzes</li> <li>Vertrauenswürdigkeit des Kommunikations- partners</li> <li>Sicherheitspolitik</li> </ul>
Zugangskontrolle auf Nutzerebene	Welche Nutzer dürfen über das Firewall-Element eine Kommunikation aufbauen?	<ul style="list-style-type: none"> <li>Identität des Nutzers</li> <li>Authentifikation des Nutzers</li> <li>Zeit, zu der eine Aktion zulässig ist</li> </ul>	<ul style="list-style-type: none"> <li>vertrauenswürdige Implementierung</li> <li>Gewährleistung der Authentifikation des Kommunikations- partners</li> <li>Sicherheitspolitik</li> </ul>
Zugangskontrolle auf Datenebene	Dürfen die Daten eines definierten Nutzers über das Firewall-Element übertragen werden?	<ul style="list-style-type: none"> <li>Identität des Absenders der Daten</li> <li>Authentifikation des Absenders der Daten</li> <li>Integrität der Daten</li> <li>Zeit, zu der eine Aktion zulässig ist</li> </ul>	<ul style="list-style-type: none"> <li>Vertrauenswürdige Implementierung</li> <li>Gewährleistung der Authentifikation des Ursprungs der Daten</li> <li>Sicherheitspolitik</li> </ul>
Rechteverwaltung	Festlegung, mit welchen Protokollen und Diensten und zu welchen Zeiten über das Firewall-Element eine Kommunikation stattfinden darf	<ul style="list-style-type: none"> <li>Header-Informa- tionen auf den verschiedenen Schichten</li> <li>Zeit, zu der eine Aktion zulässig ist</li> </ul>	<ul style="list-style-type: none"> <li>vertrauenswürdige Implementierung</li> <li>Gewährleistung der Datenunversehrtheit</li> <li>Tiefe der Analyse</li> <li>Sicherheitspolitik</li> </ul>
Kontrolle auf Anwendungsebene	Überprüfung, ob Kommandos genutzt oder Dateninhalte übertragen werden, die nicht zur durch die Anwendung definierten Aufgaben- stellung gehören	<ul style="list-style-type: none"> <li>Kommandos und Dateninhalte der verschiedenen Anwendungen</li> <li>Zeit, zu der eine Aktion zulässig ist</li> </ul>	<ul style="list-style-type: none"> <li>vertrauenswürdige Implementierung</li> <li>Gewährleistung der Datenunversehrtheit</li> <li>Tiefe der Analyse</li> <li>Sicherheitspolitik</li> </ul>

(Fortsetzung)

**Tab. 9.4** (Fortsetzung)

Sicherheitsdienst	Überprüfung/Festlegung/Maßnahme	Was wird geprüft?	Einfluss auf Sicherheit und Vertrauenswürdigkeit
Entkoppelung von Diensten	Entkoppeln verhindert, dass Implementierungsfehler, Schwachstellen und Konzeptionsfehler der Dienste Möglichkeit für Angriffe bieten	<ul style="list-style-type: none"> <li>• Kommandos</li> <li>• Zeit, zu der eine Aktion zulässig ist</li> </ul>	<ul style="list-style-type: none"> <li>• vertrauenswürdige Implementierung</li> <li>• Konzept der Entkopplung</li> </ul>
Beweissicherung und Protokollauswertung	Verbindungsdaten und sicherheitsrelevante Ereignisse werden protokolliert und können für die Beweissicherung von Nutzerhandlungen und für die Erkennung von Sicherheitsverletzungen ausgewertet werden	<ul style="list-style-type: none"> <li>• Aktionen und sicherheitsrelevante Ereignisse</li> <li>• Zeit, zu der eine Aktion zulässig ist</li> </ul>	<ul style="list-style-type: none"> <li>• vertrauenswürdige Implementierung</li> <li>• Sicherheitspolitik</li> <li>• Konzept der Beweissicherung und Protokollauswertung</li> </ul>
Alarmierung	Besonders sicherheitsrelevante Ereignisse werden an ein Security-Management gesendet, damit bei Sicherheitsverletzungen schnell reagiert werden kann	<ul style="list-style-type: none"> <li>• Zeit, zu der eine Aktion zulässig ist</li> </ul>	<ul style="list-style-type: none"> <li>• vertrauenswürdige Implementierung</li> <li>• Vertrauenswürdigkeit des Netzes</li> <li>• Sicherheitspolitik</li> </ul>
Verbergen der internen Netzstruktur	Die Struktur des zu schützenden Netzes soll gegenüber dem unsicheren Netz verborgen werden. Es soll nicht sichtbar sein, ob im zu schützenden Netz 10, 100, 1000 oder 10.000 IT-Systeme vorhanden sind	<ul style="list-style-type: none"> <li>• IP-Adressen</li> </ul>	<ul style="list-style-type: none"> <li>• vertrauenswürdige Implementierung</li> <li>• Konzept des Verbergens der internen Netzstruktur (dual-homed Gateway)</li> </ul>

## 9.16 Zusammenfassung

Da die Diskussion über Firewall-Systeme aufzeigt, dass eine 100-prozentige Sicherheit nicht erreicht werden kann, ist es zweckmäßig, die Betrachtung eines Firewall-Systems auf den Schwerpunkt der „Unsicherheit“ zu legen. Ziel muss es sein, diese Rest-Unsicherheit zu minimieren. Denn durch die sinkende Zahl der Unsicherheiten steigt die Resistenz eines Firewall-Systems. Unsicherheiten sind all diejenigen Zustände, welche zu illegalen oder unerwünschten Zuständen eines Firewall-Systems führen.

Auch hier muss einem bewusst sein, dass immer ein Risiko bestehen bleibt, das mit der Hilfe von weiteren – modular zu ergänzenden – Sicherheitsmechanis-

men wie Intrusion Detection, Antivirus-Konzepten und Verschlüsselung weiter reduziert werden muss, um so zu einer praktischen Sicherheit zu gelangen.

Wichtig sind ebenso periodische Audits und Revisionen des Cyber-Sicherheitssystems sowie Überprüfungen der Sicherheitspolitik.

**Wichtig** Ein Firewall-System kann keine 100-prozentige Sicherheit gewährleisten, ein Restrisiko muss immer eingeplant werden und/oder mit anderen Sicherheitsmaßnahmen kompensiert werden.

## 9.17 Übungsaufgaben

### Übungsaufgabe 1

Was ist die grundlegende Idee einer Firewall?

### Übungsaufgabe 2

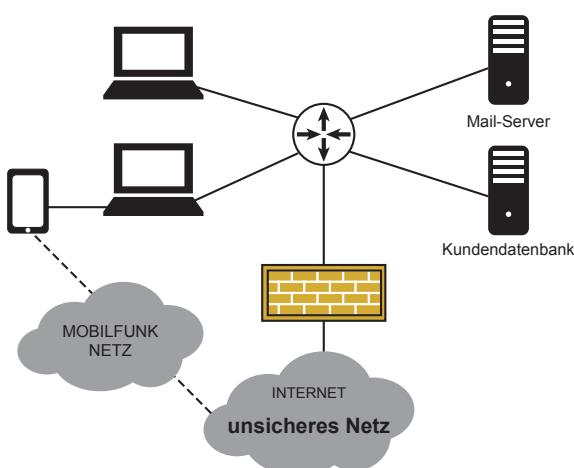
Warum kann ein Paket-Filter nicht ohne besonderen Aufwand erkennen, zu welcher Anwendung gewisse Pakete gehören?

### Übungsaufgabe 3

Beschreiben Sie die Zusammenarbeit zwischen dem „Einbindungs- und Durchsetzungsmodul“, „Analysemodul“ und „Entscheidungsmodul“ in einem Firewall-Element.

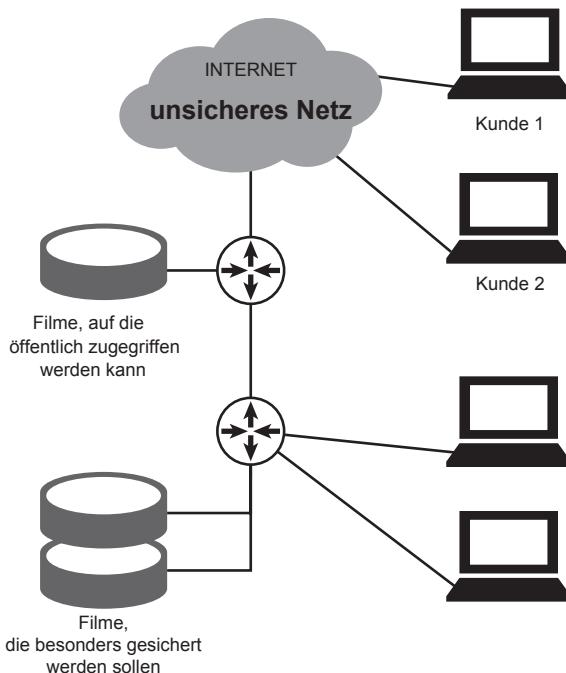
### Übungsaufgabe 4

In der folgenden Abbildung ist ein Unternehmensnetz dargestellt. Können Sie ein Cyber-Sicherheitsproblem erkennen? Wenn ja, welches?



### Übungsaufgabe 5

Sie betreiben eine Firma, die Serien und Filme als Streams im Internet anbietet. Neben den aktuellen Serien, die Ihre Kunden sehen können, haben Sie ebenfalls noch unveröffentlichte Filme, die sie gesondert sichern wollen. Wie können Firewalls eingesetzt werden, um dieses Ziel zu erreichen?



### Übungsaufgabe 6

Die Mitarbeiter in Ihrem jungen Start-up wollen mittels Video-Telefonie mit ihren Kunden kommunizieren. Allerdings haben Sie Sicherheitsbedenken gegenüber der einzusetzenden Software, aber lassen sich letztlich von Ihren Mitarbeitern überzeugen, die Technologie einzusetzen. Nun wollen Sie eine Firewall nutzen, um trotzdem einen hohen Schutz zu garantieren. Welches Firewall-System würden Sie einsetzen?

- Paketfilter
- zustandsorientierter Paketfilter
- Applikation-Firewall

### Übungsaufgabe 7

Einer Ihrer Server weist eine Sicherheitslücke auf, die der Angreifer aus der Entfernung ausnutzen kann. Wenn der Angreifer auf einer gewissen Seite eine spezielle Zeichenkette eingibt, stürzt Ihr System ab. Kann eine Firewall vor einem solchen Angriff schützen?

### Übungsaufgabe 8

In Ihrer Firma kommt es immer wieder zu Problemen, dass Schadsoftware per Mail in Ihr Firmennetzwerk gelangt. Ihr Chef spricht Sie, als Firewall-Experten der Firma, darauf an, dass Sie die Firewalls besser konfigurieren müssen, um das Problem in den Griff zu bekommen.

Was sagen Sie ihm?

### Übungsaufgabe 9

Bitte kreuzen Sie Ihre Antworten an!

		Cyber-Sicherheitsmechanismen
		Firewall-System
Gewährleistung von Cyber-Sicherheitsbedürfnissen	Vertraulichkeit	
	Authentifikation	
	Authentizität	
	Integrität	
	Verbindlichkeit	
	Verfügbarkeit	
	Anonymisierung/ Pseudonymisierung	
Cyber-Sicherheitsstrategien	Vermeiden von Angriffen	
	Entgegenwirken von Angriffen	
	Erkennen von Angriffen	

Ergebnisse siehe: <https://norbert-pohlmann.com/cyber-sicherheit/uebungen/>.

---

### Literatur

- Pohlmann N (2003) Firewall-Systeme – Sicherheit für Internet und Intranet, E-Mail-Security, Virtual Private Network, Intrusion Detection System, Personal Firewalls, 5. aktualisierte u. erweiterte Aufl. MITP-Verlag, Bonn



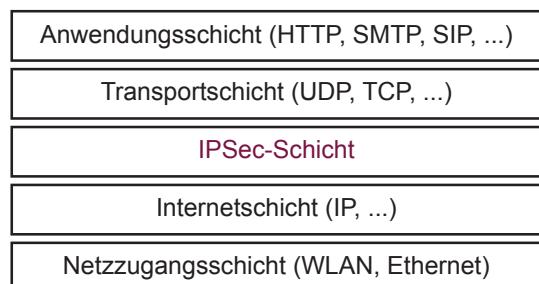
Im Kapitel IPSec-Verschlüsselung werden die Cyber-Sicherheitsarchitektur, Cyber-Sicherheitsprinzipien, Cyber-Sicherheitsmechanismen und Cyber-Sicherheitsprotokolle des IETF Sicherheitsstandards für die Cyber-Sicherheit von IP-Paketen vermittelt.

## 10.1 Einleitung

Das Internet ist eine weltweite und offene Kommunikationsinfrastruktur, über die Unternehmen, Organisationen und deren Niederlassungen miteinander kommunizieren. Besonders für diesen Anwendungsfall wird der IPSec-Standard heute verwendet. IPSec steht für Internet Protocol Security und wurde von der Internet Engineering Task Force (IETF) entwickelt. Die grundsätzliche Idee von IPSec ist, eine offene, kostengünstige und weltweit verfügbare Kommunikationsinfrastruktur wie das Internet zu nutzen und allen Bedrohungen und Risiken möglichst sinnvoll entgegenzuwirken [1].

IPSec arbeitet direkt auf der Vermittlungsschicht und ist eine Weiterentwicklung des IP-Protokolls (IP). IPSec war als Feature in IPv6 gedacht und ergänzt aber auch das bestehende IPv4 Protokoll um wichtige Cyber-Sicherheitsfunktionen, siehe Abb. 10.1.

**Abb. 10.1** IPSec im TCP/IP-Referenzmodell



Ziel ist es, eine Cyber-Sicherheit auf Netzwerkebene bereitzustellen und somit Kommunikation auf der Basis des Internet-Protokolls (IP) zu schützen. Die IP-Pakete werden zwischen definierten Kommunikationsendpunkten geschützt.

Die folgenden Cyber-Sicherheitsfunktionen werden von IPSec angeboten:

- **Verschlüsselung** schützt die Vertraulichkeit der übertragenen Daten (jedes Paket kann verschlüsselt werden).
- **HMAC-Funktion** sorgt für die Authentizität, Unversehrtheit der übertragenen Daten (jedes Paket kann gegen Manipulation geschützt und auf die Echtheit überprüft werden).
- **Anti-Replay Mechanismus** schützt vor unberechtigter Wiedereinspielung von übertragenen Daten (jedes Paket kann vor Wiedereinspielung geschützt werden).
- **Authentifikation** gewährleistet die Eindeutigkeit und Echtheit der Kommunikationspartner (die Kommunikationspartner können authentifiziert werden).
- **Tunneling** verschleiert den Datentransfer für definierte Aspekte (die IP-Kommunikation kann gegen einen gewissen Grad der Verkehrsflussanalyse geschützt werden).

**Wichtig** IPSec schützt IP-Daten auf der Netzwerkebene während der Übertragung.

## 10.2 IPSec Header

IPSec realisiert die zusätzliche Cyber-Sicherheit durch das Einfügen von Erweiterungs-Header in die IP-Pakete. In den IPSec-Headern sind nur minimal notwendige Informationen untergebracht, die auf spezielle Datenbanken verweisen und mit Security Associations das Security-Management zwischen den Kommunikationsendpunkten umsetzen.

Diese zusätzlichen Header sind:

### 1. Authentication Header (AH, RFC 2402)

Cyber-Sicherheitsdienste, die mit den Authentication Header erbracht werden, sind:

- Datenunversehrtheit

- Authentifikation
- Anti-Replay Service (optional)

## 2. Encapsulated Security Payload (ESP, RFC 2406)

Cyber-Sicherheitsdienste, die mit den Encapsulated Security Payload Header erbracht werden, sind:

- Datenunversehrtheit und Authentifikation (optional)
- Anti-Replay Service (optional)
- Verschlüsselung (optional)

Diese zusätzlichen IPSec-Header können in verschiedenen Modi verwendet werden:

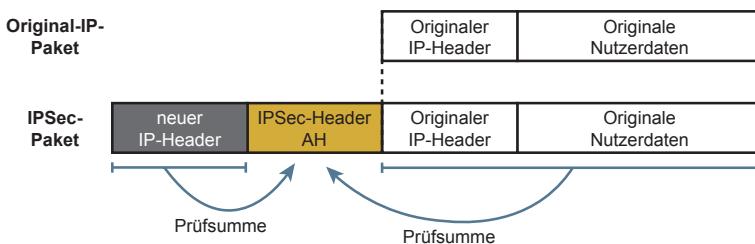
**,Transportmode‘** Verschlüsselung der Nutzdaten

**,Tunnelmode‘** Verschlüsselung des IP-Headers und der Nutzdaten

### 10.2.1 Authentication Header

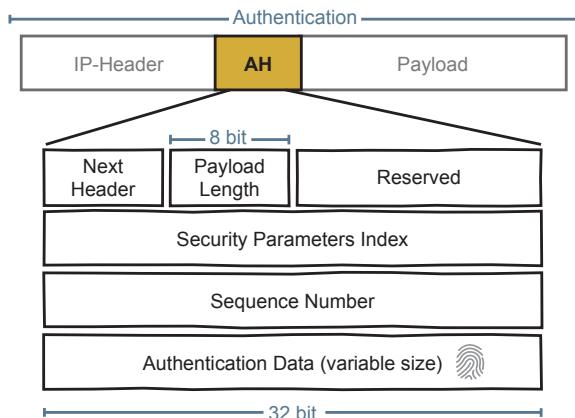
Der Authentication Header (AH) sorgt für eine starke Integrität und Authentizität der IP-Pakete. Dabei wird mit der Hilfe einer HMAC-Funktion über das gesamte IP-Paket und das Authentication-Feld selbst ein HMAC berechnet. Die Felder, die während des Transportes modifiziert werden, wie Time to Live (TTL), TOS, Flags und Header Checksum werden bei der HMAC-Berechnung ausgelassen, damit eine Ende-zu-Ende-Überprüfung möglich ist.

Abb. 10.2 zeigt den „Authentication Header“ im Tunnel-Mode.



**Abb. 10.2** Authentication Header im Tunnel-Mode

**Abb. 10.3** Authentication Header



### Beschreibung des IPSec-Headers „AH“

In Abb. 10.3 ist der IPSec-Header „AH“ dargestellt.

**Next Header** ist ein 8-Bit-Feld, das den Typ der nächsten Daten hinter dem Authentication Header identifiziert (Mechanismus, wie in der IPv6-Spezifikation).

**Payload Length** (8 Bit-Feld) beschreibt die Länge des AH in 32-bit Worten.

**Reserved** ist reserviert für zukünftige Funktionen.

**SPI** ist ein beliebiger 32-Bit Wert, der in Kombination mit der Ziel IP-Adresse und dem IPSec-Header (AH) eindeutig die Security Association für dieses Paket definiert.

**Sequence Number** (32 Bit-Feld) beinhaltet einen Zähler (Replay-Angriff).

**Authentication Data** ist ein Feld, das das Ergebnis vom HMAC erhält. Die Länge ist variabel, aber ein ganzzahliges Vielfaches von 32 Bit.

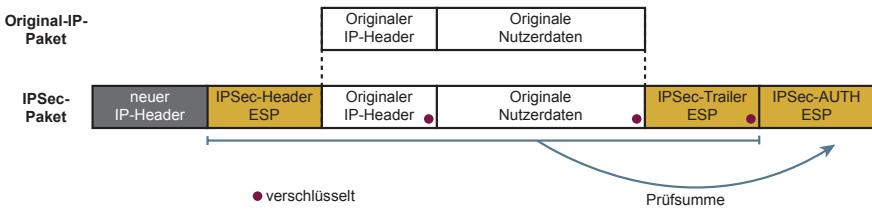
### Zusammenfassung

Mit der AH-Datenstruktur kann gewährleistet werden, dass eine Manipulation von IP-Daten auf dem Weg durch das Netzwerk entdeckt wird. Außerdem findet die Authentizität der Pakete statt. Bei dem ausschließlichen Einsatz des IPSec-Headers AH wird von IPSec keine Verschlüsselung durchgeführt.

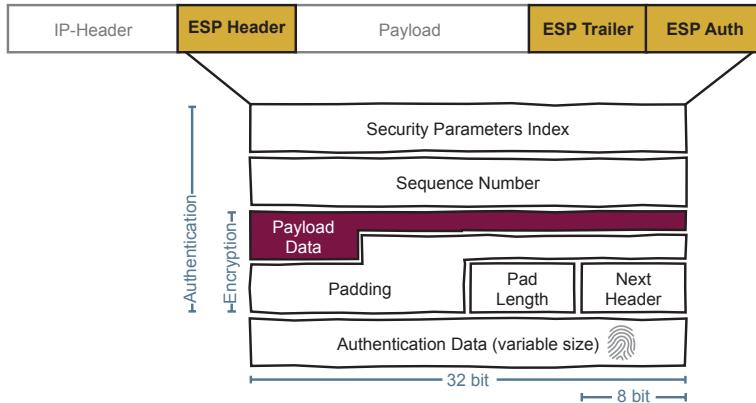
### 10.2.2 Encapsulated Security Payload

Der IPSec-Header ESP sorgt für die Verschlüsselung des IP-Headers und die Nutzdaten mit einem symmetrischen Verschlüsselungsverfahren wie dem AES. Die Integrität und Authentizität der IP-Pakete bezieht sich bei ESP nicht auf den „Outer IP-Header“.

Abb. 10.4 zeigt den „Encapsulated Security Payload“ im Tunnel-Mode.



**Abb. 10.4** Encapsulated Security Payload im Tunnel-Mode



**Abb. 10.5** Encapsulated Security Payload Header

### Beschreibung des IPSec-Headers „ESP“

In Abb. 10.5 ist der IPSec-Header „ESP“ dargestellt.

**SPI** ist ein beliebiger 32-Bit-Wert, der in Kombination mit der Ziel-IP-Adresse und dem IPSec-Header ESP eindeutig die Security Association für dieses Paket definiert.

**Sequence Number** (32-Bit-Feld) beinhaltet einen Zähler (Replay-Angriff).

**Payload Data** ist ein Feld variabler Länge, das das originale IP-Paket beinhaltet (eventuell IV (Initialization Vector) zu Beginn, falls notwendig).

**Padding** wird zum Auffüllen genutzt (0-255 Byte), falls der Verschlüsselungs-Mode dies erfordert.

**Pad Length** beschreibt die Anzahl an Bytes, die für das Padding verwendet wurden.

**Next Header** ist ein 8-Bit-Feld, das den Typ der nächsten Daten hinter dem IPSec-Header ESP identifiziert (Mechanismus, wie in der IPv6 Spezifikation).

**Authentication Data** ist ein Feld, das das Ergebnis vom HMAC erhält. Die Länge ist variabel, aber ein ganzzahliges Vielfaches von 32 Bit.

## Zusammenfassung

Mithilfe von ESP können Vertraulichkeit der Übertragung, Authentifikation des Absenders und Integrität der Daten garantiert werden, da neben der Verschlüsselung auch ähnliche Cyber-Sicherheitsmechanismen wie in AH definiert werden können.

Im Unterschied zu ESP bezieht sich die Authentizität von AH auch auf den IP-Header, sodass die Kombination von AH und ESP Vorteile im Sicherheitsbereich bietet, allerdings mehr Ressourcen auf den beteiligten IT-Systemen benötigt!

---

### 10.3 Cyber-Sicherheitsdienste der IPSec-Header und Realisierungsformen

Im Folgenden werden ein paar Cyber-Sicherheitskonzepte und Cyber-Sicherheitsdienste der IPSec-Header beschrieben.

#### IPSec: Anti-Replay Service

Der Anti-Replay Service wird zum Schutz vor unberechtigter Wiedereinspielung von alten IP-Paketen genutzt. Der Anti-Replay Service kann optional sowohl beim Authentication Header und Encapsulated Security Payload genutzt werden. Standardmäßig ist der Anti-Replay Service aktiviert.

Für den Anti-Replay Service wird die Sequence Number (SN) in den entsprechenden Headern verwendet. Die Sequence Number ist ein 32-Bit-Feld, das einen steigenden Zählerwert enthält.

Der Anti-Replay Service funktioniert folgendermaßen:

Initiator:

- Bei der IPSec-Initialisierung setzt der Initiator SN = 0.
- Das erste Paket wird mit SN = 1 gesendet.
- Das Feld wird vor dem Versand jedes weiteren Paketes um 1 erhöht.

Receiver:

- Überprüft, ob die Sequenznummer in der richtigen Reihenfolge ist, um sicherzustellen, dass während der SA-Lebensdauer keines der empfangenen Pakete dupliziert wird.
- Mithilfe eines „Sliding Windows“ wird entschieden, ob ein Paket mit einer bestimmten Sequenznummer angenommen oder verworfen wird. Die Größe eines Sliding Windows ist zum Beispiel 32.
- Damit wird das unberechtigte Wiedereinspielen von alten Paketen in einer Security Association (AS) unterbunden.

### IPSec: Security Association (SA)

Die beiden IPSec-Header AH und ESP selbst enthalten keine direkten Informationen über die zur Absicherung der eingesetzten Algorithmen und vereinbarten Schlüssellängen, sondern nur einen Verweis auf eine Datenstruktur mit diesen Informationen. Mithilfe eines Security Parameter Index (SPI) und der Ziel-Adresse in den IPSec-Headern wird eindeutig eine Security Association für dieses Paket zugeordnet.

Eine Security Association (SA) legt alle Informationen fest, die zwischen der Verbindung von zwei IPSec-Komponenten (Client/Gateway) benötigt werden.

- Security Parameter Index (SPI)
- genutzter IPSec-Service (AH oder ESP oder beide)
- Modus (Transport oder Tunnel)
- Quell- & Ziel-IP-Adresse, eventuell Adresse des Gateways
- eventuell genutzte Protokolle, Quell- & Zielportnummer
- genutzte Algorithmen & Schlüssel für die Security Association
- Sequenznummer
- Dauer der Gültigkeit der Security Association (kann über einen längeren Zeitraum sein!)
- Statusinformation der Anti-Replay Windows

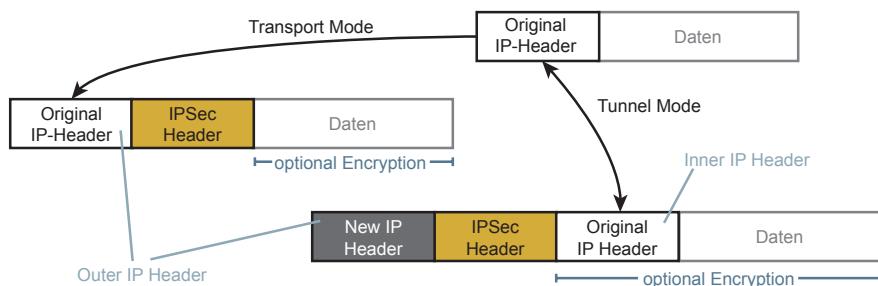
Hinweis:

Es können mehrere Security Associations mit unterschiedlichen Inhalten zum selben Ziel gleichzeitig existieren.

### IPSec: Transport- und Tunnelmodus

IPSec kann im Transport- oder im Tunnelmodus betrieben werden. Im Transportmodus wird der IP-Header des ungesicherten IP-Pakets beibehalten und nur sein Datenteil wird gesichert. Bis auf das Feld „Länge des IP-Paketes“ und die „Prüfsumme“ bleibt der alte IP-Header unverändert.

Im Tunnelmodus hingegen wird das gesamte IP-Paket in die Nutzdaten des IPSec-Pakets übernommen, sodass die alte IP-Adresse bei der Verschlüsselung nicht mehr sichtbar ist, siehe Abb. 10.6.



**Abb. 10.6** Übersicht Transport- und Tunnelmodus

Der **Transportmodus** kann nur mit IPSec-Clients umgesetzt werden. Er ist nicht für IPSec-Gateway verfügbar. Wenn ein IPSec-Gateway im Transportmodus arbeitet, fungiert es als IPSec-Client, das heißt, der Datenverkehr ist dann für sich selbst bestimmt. Im Transportmodus wird der IPSec-Header nach dem IP-Header und vor einem Protokoll der oberen Schicht (z. B. TCP, UDP, ICMP usw.) eingefügt.

Bei 1:n- oder m:n-Verschlüsselung mit IPSec-Client kommt nur der Transportmodus zum Einsatz.

Der **Tunnelmodus** gilt für IPSec-Clients und IPSec-Gateways. Ein IPSec-Gateway unterstützt nur den Tunnelmodus. Die äußeren IP-Quell- und -Zieladressen identifizieren die „Kommunikationsendpunkte“ des Tunnels. Die innere IP-Quell- und -Zieladresse identifiziert den ursprünglichen Absender und Empfänger des Datagramms.

Der IP-Tunneling-Modus ermöglicht die Verwendung öffentlicher IP-Adressen im neuen äußeren IP-Header, während die vorhandenen privaten IP-Adressen des ursprünglichen Pakets beibehalten werden. Das neue Paket wird im Internet gemäß den äußeren öffentlichen Adressen weitergeleitet.

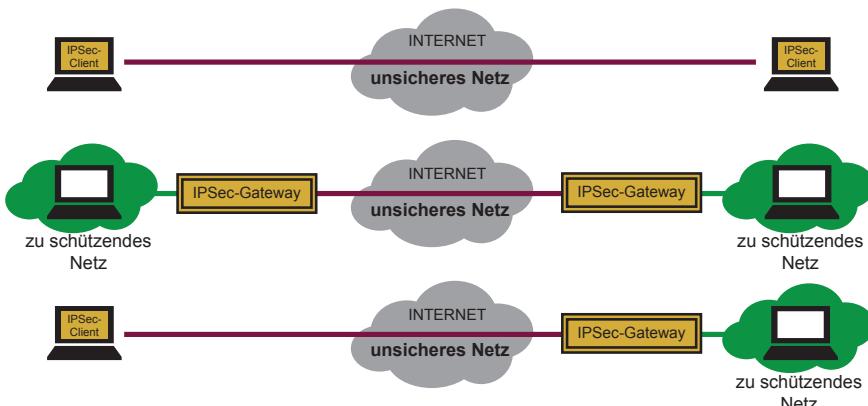
Der öffentliche IP-Header wird dann vom empfangenden IPSec-Gateway gelöscht, und das ursprüngliche Paket wird im Intranet entsprechend dem privaten IP-Header weitergeleitet.

Das ursprüngliche IP-Paket wird am Ende des Tunnels außer dem TTL-Feld, das dekrementiert wird, und dem Checksum-Feld, das aufgrund der TTL-Änderung neu berechnet wird, nicht geändert.

Bei einer 1:1-Verschlüsselung, die beispielsweise zwischen zwei Firewall-Systemen oder sonstigen Security-Gateways eingerichtet wird, wird immer der Tunnelmodus genutzt. Damit bleiben die echten IP-Adressen der Kommunikationspartner einem Angreifer verborgen.

### IPSec: Realisierungsformen

IPSec kann in zwei Realisierungsformen, als IPSec-Client sowie als IPSec-Gateway, implementiert werden, siehe Abb. 10.7.



**Abb. 10.7** IPSec Realisierungsformen

Die IPSec-Sicherheitsdienste können bereitgestellt werden

- zwischen zwei IPSec-Client (End-to-End-Verschlüsselung),
- zwischen zwei IPSec-Gateway (Site-to-Site-Verschlüsselung)
- oder einem IPSec-Gateway und einem IPSec-Client (End-to-Site-Verschlüsselung).

### IPSec-Gateways

Die Konfiguration eines IPSec-Gateways ähnelt in bestimmten Aspekten der einer Firewall. Je Quelladresse, Zieladresse, Schnittstelle, Protokoll, Port und so weiter wird definiert, ob das Paket verworfen oder (verschlüsselt oder entschlüsselt) weitergeleitet wird.

Bei einem IPSec-Gateway kommt als dritte Möglichkeit der Versand durch einen Tunnel infrage. Für diesen Fall müssen die Parameter des Tunnels definiert werden. Der wichtigste Parameter ist die Adresse des Ziel-Gateways.

### Diskussion der verschiedenen Realisierungsformen:

In diesem Abschnitt werden verschiedenen Realisierungsformen diskutiert, nach dem IPSec-Systeme umgesetzt werden können, die zur Sicherstellung einer vertrauenswürdigen Kommunikation genutzt werden.

#### 1. IPSec-Gateway

Mit einer IPSec-Sicherheitsschicht im Kommunikations-Stack eines Gateways kann aus einem unsicheren Netzdienst ein sicherer Netzdienst umgesetzt werden. Hierzu wird in einen IPSec-Gateway eine IPSec-Sicherheitsschicht in die Kommunikationsarchitektur eingeführt, die dann transparent für die IT-Systeme die IPSec-Sicherheitsdienste umsetzt, siehe Abb. 10.8.

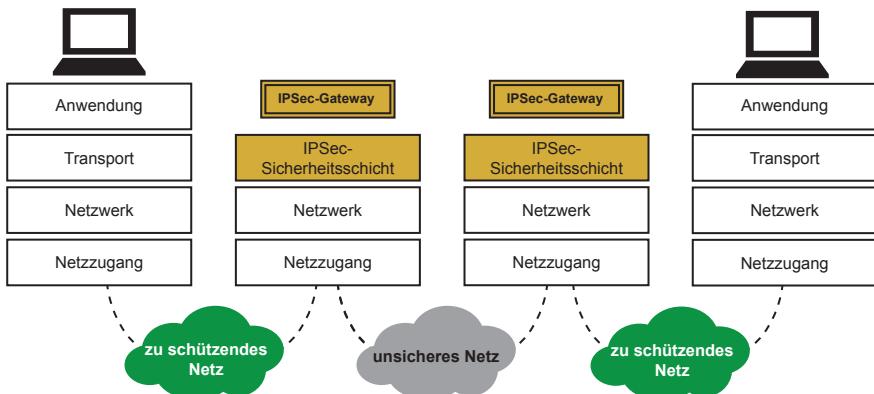


Abb. 10.8 IPSec-Gateway

### Vorteile einer IPSec-Gateway-Lösung

- Die IPSec-Gateway-Lösung ist unabhängig von IT-Systemen (Server, PC, Notebook, Tablets, Smartphone, Wearable, ...) und deren Betriebssystemen (Android, iOS, LINUX, Windows, ...).
- Die IPSec-Gateway-Lösung erlaubt die Einrichtung von Cyber-Sicherheitsfunktionen zwischen IT-Systemen, in die ansonsten keine Cyber-Sicherheitsfunktionen integriert werden könnten (zum Beispiel Terminals).
- Bei heterogenen IT-Systemen (unterschiedliche Hardware, Software, Betriebssysteme, ...) kann immer das gleiche IPSec-Gateway verwendet werden, wodurch sich der notwendige Aufwand verringert.
- IPSec-Gateways sind leichter „sicher“ zu realisieren als spezielle Software-Lösungen in IT-Systemen und sie sind immer ansprechbar, und damit einfacher zu managen.
- Die IPSec-Gateways sind hinsichtlich der Sicherheitsqualität unabhängig von anderen Systemkomponenten. Die Cyber-Sicherheit ist anwendungsunabhängig.

### 2. IPSec-Client

Eine weitere Möglichkeit, die IPSec-Sicherheitsfunktionen bereitzustellen, ist die Integration einer IPSec-Sicherheitsschicht in das IT-System, wie Notebook, Smartphone oder PC. In der Praxis wird eine IPSec-Sicherheitsschicht softwaremäßig als transparenter Netzwerktreiber in das IT-System installiert, siehe Abb. 10.9.

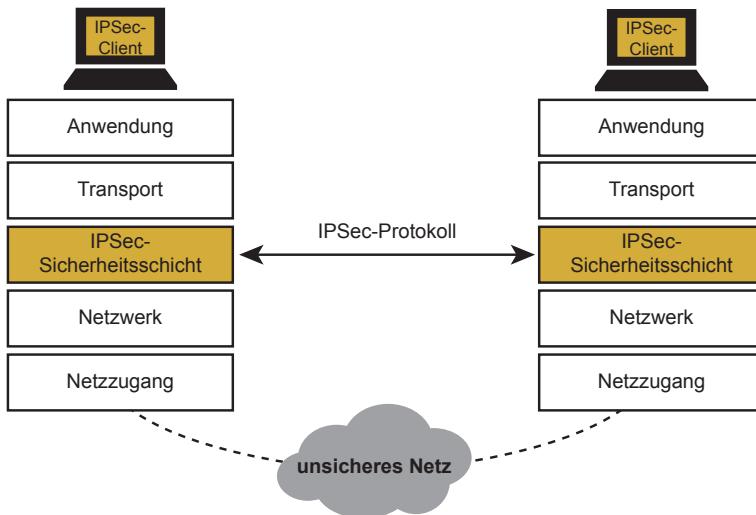
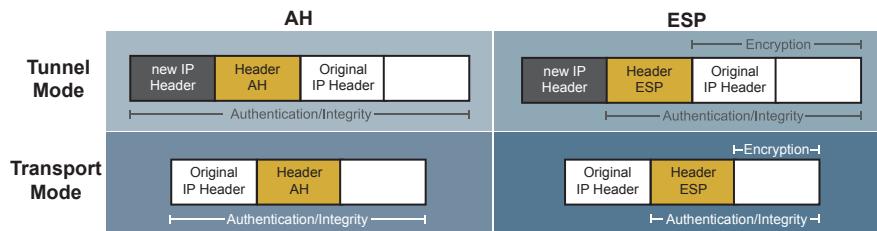


Abb. 10.9 IPSec-Client



**Abb. 10.10** Schutz in Abhängigkeit vom Mode und Header

### Vorteile einer IPSec-Client-Lösung

- Der IPSec-Client ist kostengünstiger als die IPSec-Gateway-Lösung.
- Der IPSec-Client bietet End-to-End-Sicherheit.
- Der IPSec-Client kann mobil und flexibel verwendet werden.
- Bei der IPSec-Client kann eine Person, ein Nutzer, authentifiziert werden.

**IPSec: Schutz der IP-Pakete in Abhängigkeit vom IPSec-Mode und IPSec-Header**, siehe Abb. 10.10.

Mit Tunnelmodus:

Wenn AH verwendet wird, ist der äußere IP-Header geschützt (authentifiziert), ebenso wie das gesamte ursprüngliche IP-Paket.

Im Fall von ESP wird der Schutz nur für das getunnelte IP-Paket umgesetzt, nicht für den neuen äußeren IP-Header.

Mit Transportmodus:

Wenn AH verwendet wird, sind der ursprüngliche IP-Header und die Nutzdaten geschützt (authentifiziert).

Wenn ESP verwendet wird, wird in dem IP-Original-Header kein Schutz umgesetzt, aber die Nutzdaten werden authentifiziert und können verschlüsselt werden.

ESP schützt den äußeren IP-Header nicht, AH schützt das gesamte IP-Datagramm (einschließlich des äußeren IP-Headers und außer veränderbaren Feldern wie TTL und Checksum), bietet jedoch keine Verschlüsselungsdienste an.

---

## 10.4 IPSec-Schlüsselmanagement

Mithilfe des IPSec-Schlüsselmanagements wird das notwendige Schlüsselmanagement bei IPSec-Anwendungen in Organisationen umgesetzt. Dazu gibt es unterschiedliche Realisierungsmöglichkeiten. Einige davon werden in den nächsten Unterkapiteln vorgestellt.

### 10.4.1 Manual Keying

Beim „Manual Keying“ werden die notwendigen Schlüssel entweder von einem der Kommunikationspartner oder einem zentralen Management generiert. Dann werden diese Schlüssel auf einem sicheren Weg zu allen beteiligten Kommunikationspartnern (IPSec-Client und IPSec-Gateways) übertragen und in die IPSec-Komponente neben weiteren Parametern eingefügt. Da der Schlüssel vertraulich sein muss, kann dieser Vorgang sehr aufwendig sein.

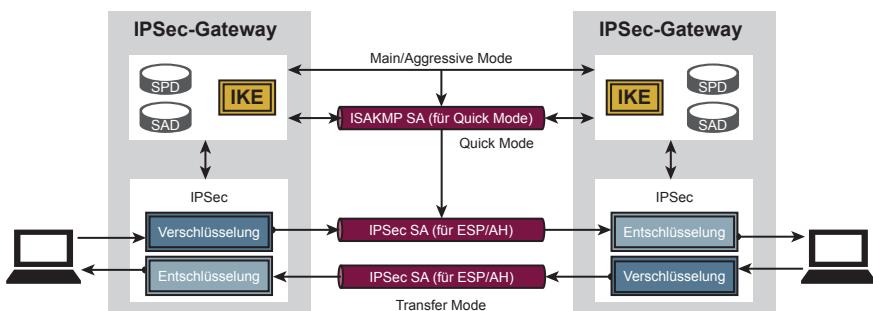
### Nutzung der PKI-Infrastruktur der TPMs

Eine Möglichkeit, das „Manual Keying“ zu vereinfachen, ist gegeben, wenn die IPSec-Lösungen über ein TPM verfügen. Dann kann die PKI-Infrastruktur der TPMs dazu genutzt werden, einfach die notwendigen Schlüssel auf einem sicheren Weg in das TPM zu transferieren. Die Schlüssel werden entsprechend mit den Public Keys verschlüsselt und erst im TPM wieder entschlüsselt, siehe auch Kap. 7 „Trusted Computing“

### 10.4.2 Internet-Key-Exchange-Protocol (IKE)

Das Internet-Key-Exchange-Protokoll (IKE) ist das Schlüsseltransferprotokoll für IPSec. Für IKE brauchen beide Seiten eine identische Passphrase (Pre-Shared Seced). Darauf basierend wird unter dem Einsatz des Diffie-Hellman-Protokolls zum Beispiel ausgehandelt, welche Algorithmen zur Verschlüsselung eingesetzt werden. In diesem Abschnitt werden IKEv1-Spezifikationen beschrieben.

**Übersicht und Zusammenhang zwischen IPSec und IKE (IPSec-Gateway), siehe Abb. 10.11.**



**Abb. 10.11** Übersicht und Zusammenhang zwischen IPSec und IKE

## Übersicht

- **Main Mode/Aggressive Mode:** Aufbau der ISAKMP SA sowie Policy-Ab-sprachen und Authentifikation des Kommunikationspartners
- **Quick Mode:** Aufbau der IPSec SA sowie Mode/IPSec-Header (AH, ESP) Absprache und Key-Management. Der Quick Mode ist geschützt durch die vor-her erstellte ISAKMP SA.
- **Transfer Mode:** Sicherung der IP-Pakete mit AH/ESP und Anti-Replay Service

In den IPSec-Headern sind nur minimal notwendige Informationen untergebracht, die auf Datenbanken verweisen und mit weiteren Security Associations das Secu-rity-Management umsetzen. Bei der Aushandlung der entsprechenden Policy kön-nen mit den Security Associations, für jede Kommunikationsrichtung zwischen den Kommunikationspartnern, unterschiedliche Aspekte ausgehandelt werden.

## Security Policy Database (SPD)

In der Security Policy Database (SPD) ist beispielsweise hinterlegt, wie die Ver-bindung zwischen den Kommunikationsendpunkten, die durch ihre IP-Adressen identifiziert sind, gesichert werden soll. Als Security Protocol werden dann die IPSec-Header AH und ESP oder beide eingesetzt. Zur Aushandlung der Schlüssel wird meist IKE verwendet. Die SPD ist im Vergleich zur SAD (siehe folgender Abschnitt) eher statisch, da ein Eintrag in der SPD „zustandslos“ ist.

Die Security Policy Database definiert den Sicherheitsstandard für ein bestimmtes IPSec-System einer Organisation:

- Quell- & Ziel-IP-Adressen
- Quell- & Zielportnummer
- Protokoll (UDP, TCP, ...)
- eine Liste mit den zugelassenen Algorithmen für das System einer Organisation
- falls notwendig: Beschreibung des Tunnelendpunktes
- Informationen über die Nutzung der Anti-Replay Windows und der maximalen Lebensdauer der SAs

## Security Association Database (SAD)

In der Security Association Database (SAD) werden Security Associations (SA) zwischen den Kommunikationsendpunkten der IPSec-Verbindung verwaltet. Die Einträge in der SAD verändern sich öfter, anders als bei der SPD. Die Einträge der Security Association enthalten die Schlüssel mit der entsprechenden Lebens-dauer. AH und ESP haben eigene Einträge in der Security Association der SAD. Eine Security Association wird über das IKE-Protokoll angelegt und für nur eine Kom-munikationsrichtung genutzt: Sender und Empfänger haben darin die ent-sprechenden Schlüssel und Verfahren. Wenn AH und ESP gleichzeitig verwendet werden, sind vier Einträge in der entsprechenden Security Association vorhanden.

Der Security Parameter Index (SPI) identifiziert zusammen mit der IP-Adresse des Kommunikationsendpunkts die entsprechende Security Association. Diese Infor-mationen stehen im IP- und IPSec-Header.

Für jede SA werden folgende Parameter festgelegt:

- Identifier:
  - Ziel-IP-Adressen oder Ranges
  - IPSec-Header (AH oder ESP)
  - Security Parameter Index (SPI)
- Parameter:
  - Algorithmen für die Authentifikation und Verschlüsselung
  - Lebensdauer der Security Association (SA)
  - Tunnel- oder Transport-Mode
  - Anti-Replay Service
  - Link mit der Policy in der SPDSA´s

### **Verschiedene Modi und Phasen von IKE**

Die verschiedenen Security Association werden mit dem UDP, Port 500 (Quelle und Ziel) umgesetzt.

Es werden zwei Phasen von Security Association durchgeführt:

- Phase 1 – Main Mode/Aggressive Mode
- Phase 2 – Quick Mode

#### **Phase 1: Aufbau der ISAKMP Security Association**

In der Phase 1 wird ein sicherer Kanal (ISAKMP SA) zwischen beiden Kommunikationsendpunkten etabliert. Die Phase 1 wird ISAKMP Security Association oder äußere SA genannt (ISAKMP = Internet Security Association and Key Management Protocol).

In der Phase 1 werden mithilfe des Main Modes/Aggressive Modes

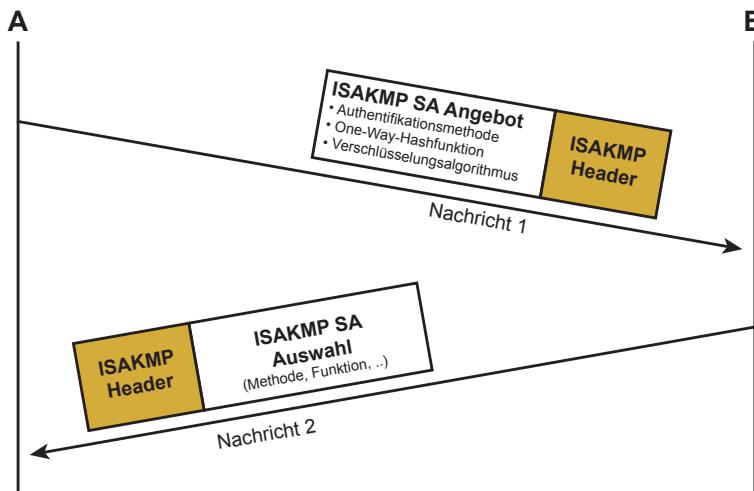
- IKE-Parameter (ISAKMP) ausgehandelt:
  - Authentifikationsmethode (PKI oder PSK)
  - Algorithmen für Authentifikation und Verschlüsselung
  - Schlüsselaustausch (für die SAs)
- und eine Nutzer-Authentifikation durchgeführt.

#### **Phase 1 – IKE Main Mode**

Als erstes wird die Phase 1 mithilfe des Main Modes beschrieben. In dieser Phase wird das „Internet Security Association and Key Management Protocol (ISAKMP)“ umgesetzt.

#### **Schritt 1 – IKE Main Mode – Aushandeln der Basis-Algorithmen**

Im Schritt 1 des Main Modes werden die Basis-Algorithmen (Krypto-Profile) für die Verschlüsselung und Authentifikation der ISAKMP SA ausgehandelt, siehe Abb. 10.12.



**Abb. 10.12** Aushandeln der Basis-Algorithmen

In der Nachricht 1 sendet der Initiator (Kommunikationspartner A) Angebote für Authentifikationsmethoden, One-Way-Hashfunktionen, Verschlüsselungsalgorithmen und den Level des Diffie-Hellman-Verfahrens (Group).

Authentifikationsmethoden sind zum Beispiel auf der Basis einer PKI oder Pre-Shared Key (PSK).

One-Way-Hashfunktionen sind zum Beispiel SHA512, SHA384, SHA256, ... MD5.

Verschlüsselungsalgorithmen sind zum Beispiel AES-256-GCM, AES-256-CBC, ... DES.

DH Group (für p) sind zum Beispiel Group20 (384-Bit Elliptic Curve), Group19, Group14, .... Group1 (768 Bit).

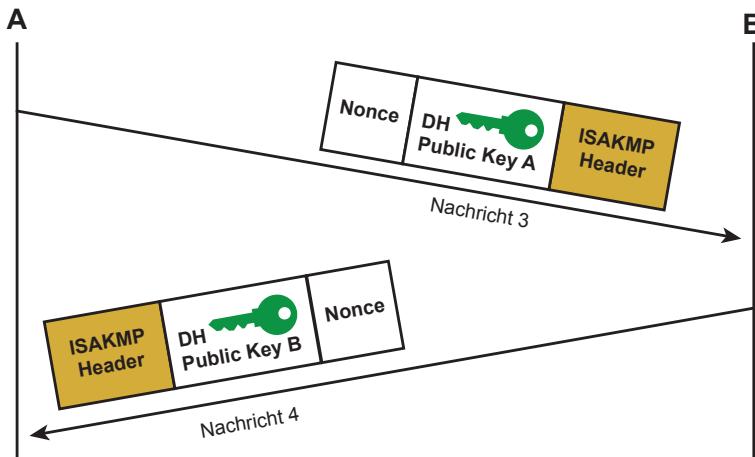
In der Nachricht 2 kann der Kommunikationspartner B daraus ein Krypto-Profil auswählen:

Wenn als Krypto-Profil „PSK, SHA384, AES-256-CBC, Group20“ ausgesucht wird, kann ein hoher Level an Cyber-Sicherheit für die IPSec-Kommunikation erreicht werden. Wenn aber als Krypto-Profil „PSK, MD5, DES, Group1“ gewählt wird, kann keine angemessene Cyber-Sicherheit für die IPSec-Kommunikation erzielt werden, weil das Krypto-Profil nicht den aktuell notwenigen Stand widerspiegelt und dadurch Angreifer in der Lage sind, die Cyber-Sicherheitsfunktionen zu brechen.

Aus diesem Grund sollten vom Initiator nur Methoden für das Krypto-Profil angeboten werden, die sein gewünschtes Cyber-Sicherheitsniveau erfüllen können. Aber auch der Kommunikationspartner sollte nur ein Krypto-Profil auswählen, das sein gewünschtes Cyber-Sicherheitsniveau erfüllt.

### Schritt 2 – IKE Main Mode – Umsetzung des Diffie-Hellman-Verfahrens

Im Schritt 2 des Main Modes werden Zufallszahlen (Nonces) ausgetauscht, die für die Authentifikation im Schritt 3 verwendet wird. Außerdem werden



**Abb. 10.13** Umsetzung des Diffie-Hellman-Verfahrens

die Public Keys des Diffie-Hellman-Verfahrens (DH) ausgetauscht, siehe Abb. 10.13.

Nach diesem Schritt berechnen die beiden Kommunikationspartner A und B jeweils mit dem Diffie-Hellman-Verfahren einen gemeinsamen Diffie-Hellman Shared Secret – DHSS. DHSS ist ein geheimer Schlüssel, den nur die beiden Kommunikationspartner A und B kennen.

#### Berechnungen des Diffie-Hellman Shared Secrets (DHSS):

Kommunikationspartner A:  $DHSS = DH \text{ Public Key B}^{DH \text{ Private Key A}} \bmod p$

Kommunikationspartner B:  $DHSS = DH \text{ Public Key A}^{DH \text{ Private Key B}} \bmod p$

DH Private Key X: Ist der geheime Schlüssel Teil des Kommunikationspartners X

DHSS ist der gemeinsame Shared Secret, geheimer Schlüssel, der genutzt wird, um drei weitere geheime Schlüssel abzuleiten:

#### 1. Derivation Key

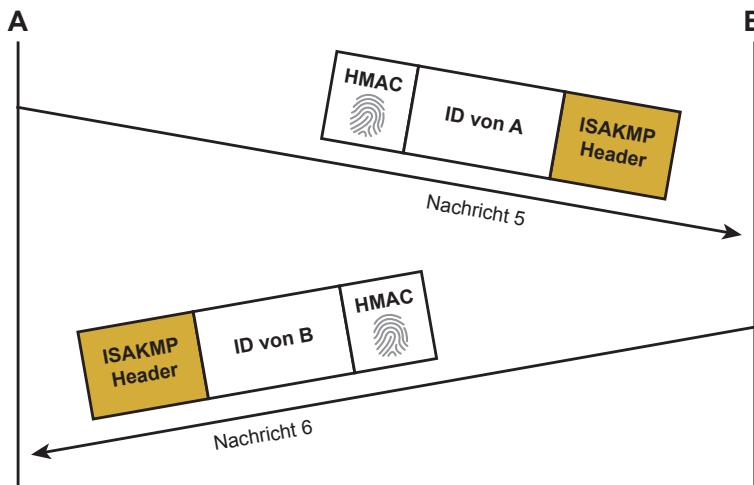
Der Derivation Key wird für die Sicherheit des Quick Modes verwendet.

#### 2. Authentication Key

Der Authentication Key wird als Sitzungsschlüssel für die Authentizität der Protokollelemente im Schritt 3 verwendet.

#### 3. Encryption Key

Der Encryption Key wird als Sitzungsschlüssel für die Verschlüsselung der Protokollelemente im Schritt 3 verwendet.



**Abb. 10.14** Authentifikation der Kommunikationspartner

### Schritt 3 – IKE Main Mode – Authentifikation der Kommunikationspartner

In diesem Schritt 3 werden die Identitäten (IDs) der Kommunikationspartner A und B gegenseitig verifiziert. Da die beiden Pakete verschlüsselt sind, können die IDs nicht mitgelesen werden, siehe Abb. 10.14.

Die Nachrichten 5 und 6 beinhalten die ID des jeweiligen Kommunikationspartners und die HMACs. Die beiden Nachrichten sind mit den schon ausgehandelten Schlüsseln aus dem Vorgänger Handshake verschlüsselt und Integritätsgesichert.

Für die Authentifikation der Kommunikationspartner können zum Beispiel diese zwei unterschiedlichen Methoden verwendet werden.

#### A) Pre-Shard-Secret-Authentifizierung

$$\text{HMAC} = \text{KH}(\text{PSK}, \text{Nonce} \parallel \text{DPHK} \parallel \text{ID} \parallel \text{K-Profil})$$

KH	„Keyed-Hashing for Message Authentication“-Verfahren; HMAC-Verfahren
PSK	Pre-Shared Key (geheimer Schlüssel) der Kommunikationspartner
Nonce	jeweilige Zufallszahl der Kommunikationspartner
DPHK	öffentliche Diffie-Hellman Schlüssel des Kommunikationspartners
ID	ID des Kommunikationspartners (A und B)
K-Profil	ausgewähltes Krypto-Profil (aus Nachricht 2)

Der „Pre-Shared Key“ wird vorher in die IPSec-Gateways oder im IPSec-Clients eingegeben! Wenn alle den gleichen „Pre-Shared Key“ in einer Organisation nutzen, wird „nur“ die Zugehörigkeit zur Organisation verifiziert und nicht der korrekte Kommunikationspartner.

## B) Digitale Signatur-Authentifizierung

$$\text{HMAC} = S(\text{KH}(\text{DHSS}, \text{Nonce} \parallel \text{DHPK} \parallel \text{ID} \parallel \text{K-Profil}), \text{GSX})$$

S	Signaturfunktion (zum Beispiel RSA-Verfahren)
GSX	geheimer Schlüssel des Kommunikationspartners X (A oder B)
KH	„Keyed-Hashing for Message Authentication“-Verfahren; HMAC-Verfahren
DHSS	Diffie-Hellman Shared Secret (geheimer Schlüssel aus Schritt 2)
Nonce	jeweilige Zufallszahl der Kommunikationspartner
DHPK	öffentliche Diffie-Hellman Schlüssel des Kommunikationspartners
ID	ID des Kommunikationspartners (A und B)
K-Profil	ausgewähltes Krypto-Profil (aus Nachricht 2)

Bei der Umsetzung der Authentifikation durch eine digitale Signatur muss die Organisation über eine Public-Key-Infrastruktur (PKI) verfügen. Auf dieser Basis können die Nutzer als Kommunikationspartner bei der Nutzung eines IPSec-Clients authentifiziert werden.

### Phase 1 – IKE Aggressive Mode

Der Aggressive Mode tauscht für die erste Phase des Internet-Key-Exchange-Protocol (IKE) nur drei Protokollelemente aus, siehe Abb. 10.15.

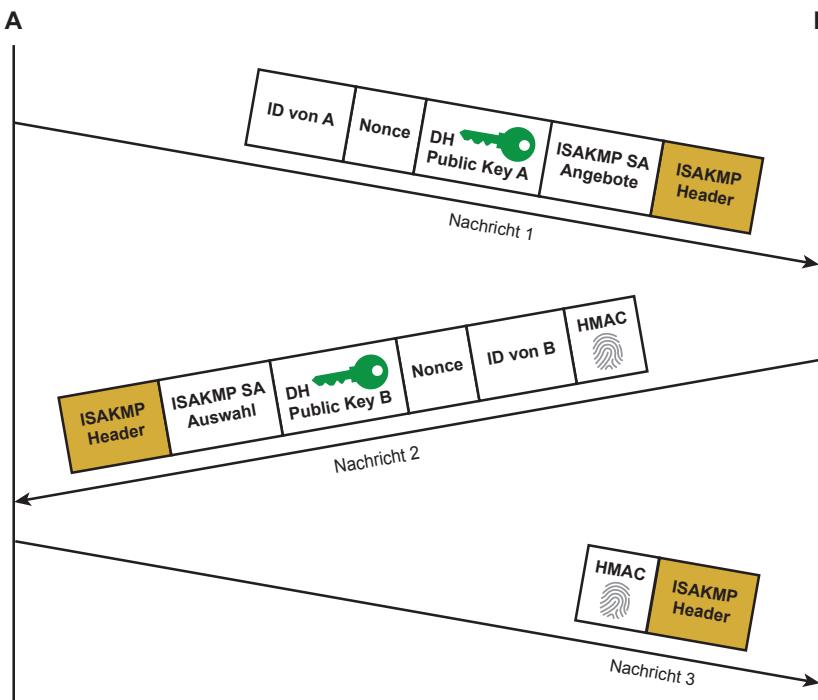


Abb. 10.15 IKE Aggressive Mode

Die Inhalte der ausgetauschten Elemente sind die gleichen wie beim „Main Mode“, nur werden sie im „Aggressive Mode“ mit nur drei Nachrichten ausgetauscht. Daher ist der „Aggressive Mode“ schneller, da er mit nur drei Nachrichten-Paketen auskommt; aber dafür sind die IDs nicht verschlüsselt!

### Aufbau der Phase 2 mit der IPSec Security-Assoziation

Die Phase 2 kann in zwei verschiedenen Varianten umgesetzt werden:

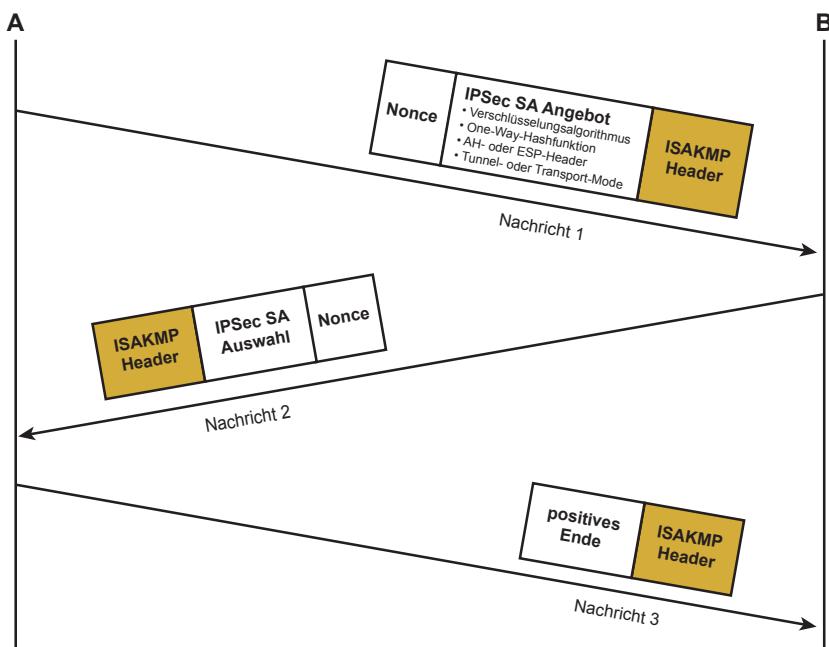
- **Basic Quick Mode**
- **Perfect Forward Secrecy**

### Phase 2: Aufbau der IPSec SA

Phase 2 dient dem Aushandeln der IPSec SA mithilfe des sogenannten Quick Modes innerhalb der sicheren ISAKMP SA (aus der Phase 1):

- Aushandeln der IPSec-Parameter:
  - Security Protocol (AH, ESP)
  - **Algorithmen** (One-Way-Hashfunktion und das Verschlüsselungsverfahren, falls ESP) und **Schlüssel**, die für die Authentisierung und Verschlüsselung der Daten (IP-Pakete) genutzt werden.
  - Modus (Transport oder Tunnel)
- Hinweis: Die Algorithmen können andere sein, als in der Phase 1.
- Alle Pakete der Phase 2 werden durch in der Phase 1 ausgehandelte Algorithmen und Schlüssel (Derivation Key) geschützt.

Ablauf des „Basic Quick Mode“-Protokolls, siehe Abb. 10.16.



**Abb. 10.16** Basic Quick Mode

In der Nachricht 1 sendet der Initiator (Kommunikationspartner A) Angebote für IPSec-Header, One-Way-Hashfunktionen und Verschlüsselungsalgorithmen.

IPSec-Header sind AH und/oder ESP

One-Way-Hashfunktionen sind zum Beispiel SHA512, SHA384, SHA256, ... MD5.

Verschlüsselungsalgorithmen sind zum Beispiel AES-256-GCM, AES-256-CBC, ... DES.

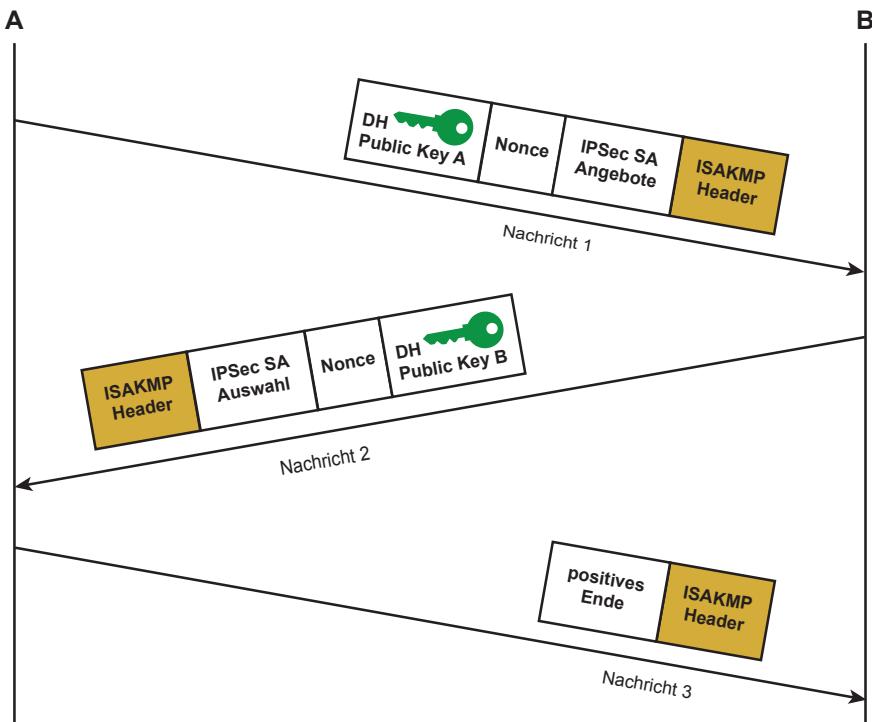
Auch in diesem Mode sollte der Initiator nur Methoden anbieten, die sein gewünschtes Cyber-Sicherheitsniveau erfüllen.

In der Nachricht 2 kann der Kommunikationspartner daraus ein Krypto-Profil auswählen.

Auch der Kommunikationspartner sollte nur Methoden auswählen, die sein gewünschtes Cyber-Sicherheitsniveau erfüllen.

In der Nachricht 3 wird das positive Ende des Quick Mode-Protokolls durch den Initiator bestätigt.

**Ablauf des „Perfect Forward Secrecy“ Protokolls**, siehe Abb. 10.17.



**Abb. 10.17** Perfect Forward Secrecy

Wie Basic Quick Mode, aber zusätzlich mit Diffie-Hellman Verfahren.  
 Beide Kommunikationspartner A und B können jeweils mit dem Diffie-Hellman-Verfahren einen gemeinsamen Diffie-Hellman Shared Secret – DHSS berechnen.

### Berechnungen des Diffie-Hellman Shared Secrets (DHSS):

Kommunikationspartner A:  $DHSS = DH \text{ Public Key B}^{DH \text{ Private Key A}} \bmod p$

Kommunikationspartner B:  $DHSS = DH \text{ Public Key A}^{DH \text{ Private Key B}} \bmod p$

DH Private Key X: Ist der geheime Schlüssel Teil des Kommunikationspartner X

Dieser gemeinsame Diffie-Hellman Shared Secret (DHSS) wird als Input für die Berechnung von KEYMAT verwendet:

### Phase 2 – Berechnung von KEYMAT

KEYMAT ist das Schlüsselmaterial für die Authentizität und Verschlüsselung für die ein- und ausgehenden Kommunikationskanäle im Transfer Mode.

Es gibt zwei Methoden, den Basis-Schlüssel „KEYMAT“ zu berechnen:

- Basic Quick Mode (der Phase-1 „Derivation Key“ wird benutzt)
- Perfect Forward Secrecy (wie Quick Mode aber zusätzlich Diffie-Hellman Shared Secret)

#### A) Basic Quick Mode – Berechnung von KEYMAT

$$\text{KEYMAT} = KM(DK, IPSH \parallel SPI \parallel Nonce)$$

KH	„Keyed-Hashing for Message Authentication“-Verfahren; HMAC-Verfahren
DK	Derivation Key, aus der Phase 1
IPSH	IPSec Header (AH oder ESP)
SPI	Security Parameter Index
Nonce	jeweilige Zufallszahl der Kommunikationspartner

#### B) Perfect Forward Secrecy – Berechnung von KEYMAT

$$\text{KEYMAT} = KM(DK, IPSH \parallel SPI \parallel Nonce)$$

KH	„Keyed-Hashing for Message Authentication“-Verfahren; HMAC-Verfahren
DK	Derivation Key, aus der Phase 1
DHSS	Diffie-Hellman Shared Secret
IPSH	IPSec Header (AH oder ESP)

SPI Security Parameter Index  
Nonce jeweilige Zufallszahl der Kommunikationspartner

Hinweis:

Der „Derivation Key“ kann über einen längeren Zeitraum gültig sein!

Aus dem Schlüsselmaterial „KEYMAT“ werden dann vier weitere Schlüssel erzeugt:

zwei Authentifizierungsschlüssel und zwei Verschlüsselungsschlüssel für eingehende und ausgehende IT-Pakete (Transfer Mode).

### **Perfect Forward Secrecy (PFS)**

Perfect Forward Secrecy (PFS) ist eine kryptografische Charakteristik, die eine Aussage über die Abhängigkeit von Schlüsseln untereinander trifft. Mit aktiviertem PFS sind bei einem kompromittierten Schlüssel (zum Beispiel Derivation Key) alle weiteren nicht gleichzeitig auch kompromittiert, da die Schlüssel nicht voneinander abhängen. Dieses kann durch die zusätzliche Verwendung des Diffie-Hellman-Verfahrens, der Aushandlung des Diffie-Hellman Shared Secret, erreicht werden!

Beispiel eines Angriffes, bei dem PFS eine Rolle spielt:

Ein Angreifer speichert alle Pakete des Quick Modes sowie alle IP-Pakete, die im Transfer Mode verschlüsselt übertragen worden sind, in einer Datenbank. Dann wird der Klartext des „Derivation Keys“ bekannt.

#### **A) Basic Quick Mode**

Mithilfe des „Derivation Keys“ kann der Angreifer für alle vergangenen Security Associations die KEYMAT berechnen und damit alle gespeicherten verschlüsselten IP-Pakete im Nachhinein entschlüsseln.

#### **B) Perfect Forward Secrecy**

Auch wenn der „Derivation Key“ bekannt ist, kann der Angreifer die vergangenen KEYMAT nicht berechnen, weil der Angreifer die entsprechenden „Diffie-Hellman Shared Secret“ nicht kennt.

### **Einbindung von IPSec-Gateways**

Eine besondere Herausforderung ist die Inbetriebnahme von vielen IPSec-Gateways. Wenn ein Unternehmen seine Zentrale mit 1000 Niederlassungen absichern möchte, bedeutet dies, dass 1001 IPSec-Gateways installiert werden müssen. Da die vollständige transparente, gesicherte Kommunikation zwischen der Zentrale und den Niederlassungen sowie zwischen den Niederlassungen nur dann möglich ist, wenn alle IPSec-Gateways installiert sind, brauchen die IPSec-Gateways in der Installationsphase auch die Möglichkeit, die Pakete im Klartext durchzulassen.

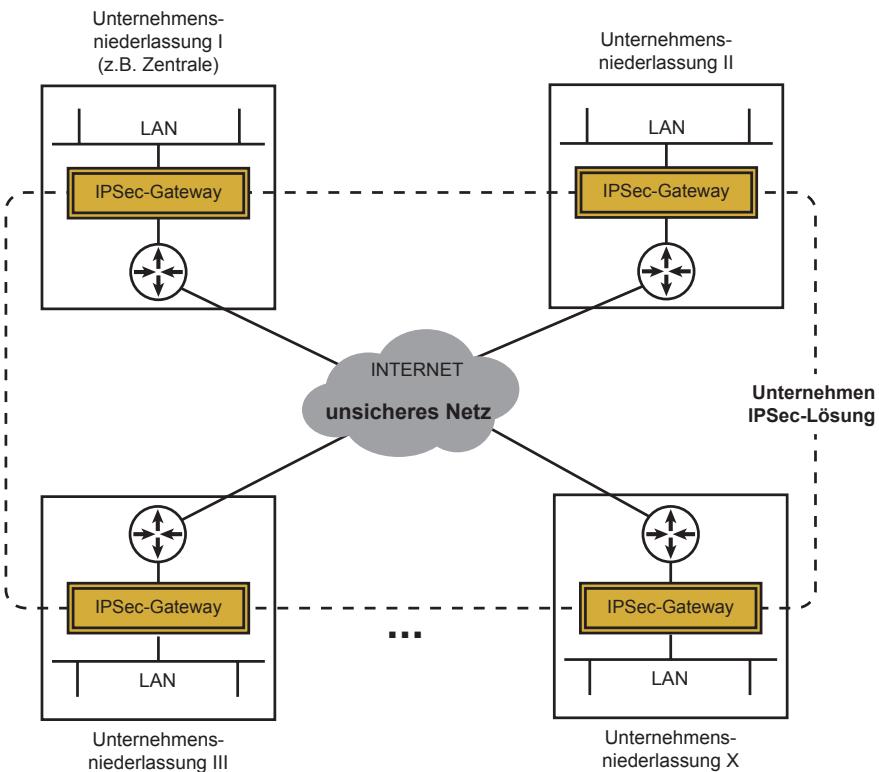
Erst wenn alle IPSec-Gateways installiert sind, kann die vollständige gesicherte Kommunikation umgesetzt werden.

## 10.5 Anwendungsformen von IPSec-Lösungen

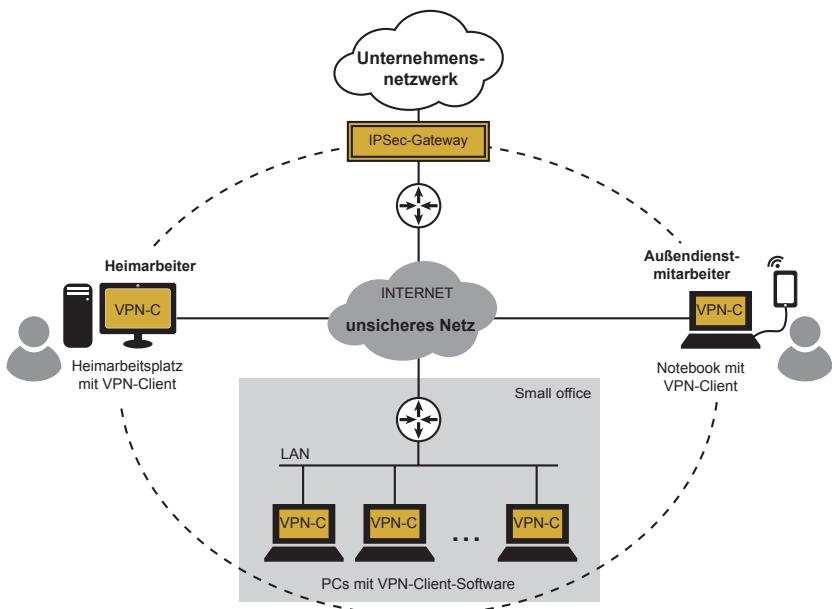
Es gibt verschiedene Anwendungsformen von IPSec-Lösungen, von denen ein paar exemplarisch dargestellt werden.

### Unternehmensweite IPSec-Lösung

Mithilfe einer unternehmensweiten IPSec-Lösung werden zwischen verschiedenen Standorten eines Unternehmens (Zentrale und Niederlassungen) Unternehmensdaten vertrauenswürdig über ein unsicheres Netz, wie das Internet, ausgetauscht. Bei dieser Anwendungsform spielt die Transparenz der Lösung eine wichtige Rolle, siehe Abb. 10.18.



**Abb. 10.18** Unternehmensweite IPSec-Lösung



**Abb. 10.19** Remote-Ankoppelung mithilfe einer IPSec-Lösung

### Sichere Remote-Ankopplung

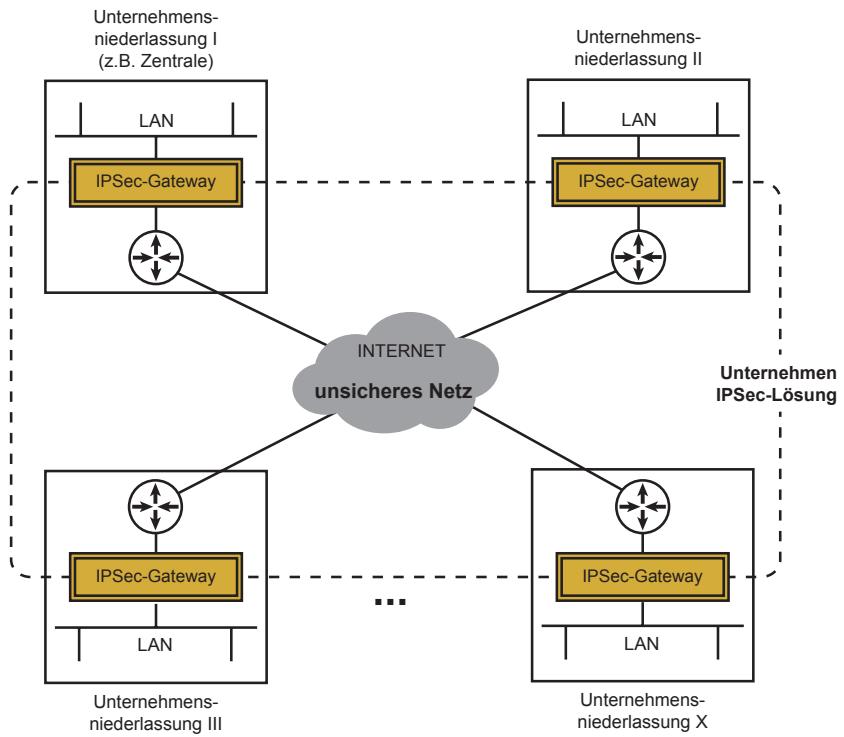
Heim- und/oder Mobil-Arbeitsplätze greifen über ein öffentliches Netzwerk, wie das Internet, geschützt auf die zentral gespeicherten Unternehmensdaten zu. Hier spielen die Identifikation und Authentifikation des Nutzers, der auf die Daten zugreifen möchte, eine besondere Rolle, siehe Abb. 10.19.

Der Zugang zum Unternehmensnetzwerk ist mit einem redundanten, hochverfügbaren IPSec-Gateway aufgebaut, das über ein Directory-Service die Zertifikate und eine **Certificate Revocation List** (CRL) der einzelnen Mobil-Mitarbeiter abrufen kann. Dazu steht zentral eine PKI zur Verfügung.

Die einzelnen Mobil-Mitarbeiter haben auf ihrem IT-System (Notebook, PC, Smartphone, ...) einen IPSec-Client installiert und eine Smartcard oder USB-Stick als Hardware-Sicherheitsmodul für das Challenge-Response-Protokoll der Authentifikation.

### IPSec zwischen verschiedenen Unternehmen

In einer definierten Gruppe von Unternehmen – beispielsweise Automobilhersteller und -zulieferern – können alle Partner miteinander mithilfe der IPSec-Technologie eine vertrauenswürdige, untereinander und nach außen geschützte, Kommunikation realisieren, siehe Abb. 10.20. Hier spielt das unternehmensübergreifende Cyber-Sicherheitsmanagement eine besondere Rolle.

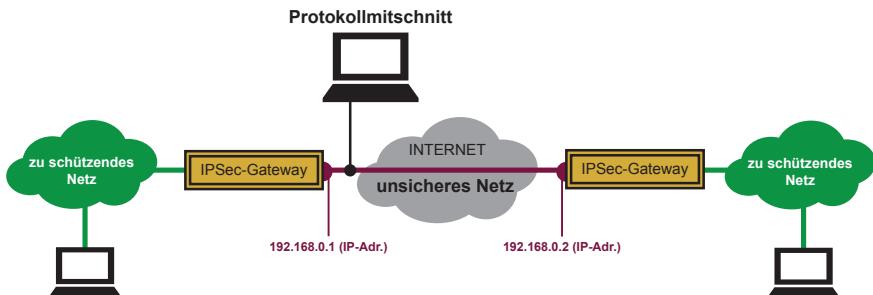


**Abb. 10.20** Kooperative IPSec-Lösung verschiedener Unternehmen

## 10.6 Protokollmitschnitt

In diesem Abschnitt wird ein Protokollmitschnitt beschrieben, der aufzeigen soll, wie das IPSec-Protokoll real umgesetzt sein kann.

In Abb. 10.21 kommuniziert ein IT-System A, mit der IP-Adresse 192.168.0.1, mit einem IT-System B, dessen IP-Adresse 192.168.0.2 ist.



**Abb. 10.21** IPSec gesicherte Kommunikation

## Protokollmitschnitt

### Schritt 1 – IKE Main Mode – Aushandeln der Basis-Algorithmen

**Frame 1:** 222 bytes on wire (1776 bits), 222 bytes captured (1776 bits) on interface 0    **A >>> B**

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2  
User Datagram Protocol, Src Port: 500, Dst Port: 500

**Internet Security Association and Key Management Protocol**

**Initiator SPI:** a93311f793844263  
    **Responder SPI:** 0000000000000000

    Next payload: Security Association (1)  
    Exchange type: Identity Protection (Main Mode) (2)  
    Flags: 0x00

        .... .0 = Encryption: **Not encrypted**  
        .... .0. = Commit: No commit  
        .... .0.. = Authentication: No authentication

    Payload: Security Association (1)

    Payload: Proposal (2) # 0

**Proposal transforms:** 1

        Payload: Transform (3) # 1

            Transform ID: KEY\_IKE (1)

**IKE Attribute (t=1,l=2):** Encryption-Algorithm: AES-CBC  
            **IKE Attribute (t=14,l=2):** Key-Length: 128  
            **IKE Attribute (t=2,l=2):** Hash-Algorithm: SHA2-256  
            **IKE Attribute (t=4,l=2):** Group-Description: Unknown 31  
            **IKE Attribute (t=3,l=2):** Authentication-Method: Pre-shared key  
            **IKE Attribute (t=11,l=2):** Life-Type: Seconds  
            **IKE Attribute (t=12,l=2):** Life-Duration: 3600

...

**Frame 2:** 202 bytes on wire (1616 bits), 202 bytes captured (1616 bits) on interface 0    **A <<< B**

Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1  
User Datagram Protocol, Src Port: 500, Dst Port: 500

**Internet Security Association and Key Management Protocol**

**Initiator SPI:** a93311f793844263  
    **Responder SPI:** 8ec4e54d335d2687

    Next payload: Security Association (1)  
    Version: 1.0  
    Exchange type: Identity Protection (Main Mode) (2)  
    Flags: 0x00

        .... .0 = Encryption: **Not encrypted**  
        .... .0. = Commit: No commit

```
.... .0.. = Authentication: No authentication
Message ID: 0x00000000
Length: 160
Payload: Security Association (1)
Payload: Proposal (2) # 0
Proposal transforms: 1
Payload: Transform (3) # 1
Transform ID: KEY_IKE (1)
IKE Attribute (t=1,l=2): Encryption-Algorithm: AES-CBC
IKE Attribute (t=14,l=2): Key-Length: 128
IKE Attribute (t=2,l=2): Hash-Algorithm: SHA2-256
IKE Attribute (t=4,l=2): Group-Description: Unknown 31
IKE Attribute (t=3,l=2): Authentication-Method: Pre-shared key
IKE Attribute (t=11,l=2): Life-Type: Seconds
IKE Attribute (t=12,l=2): Life-Duration: 3600
...
...
```

### Schritt 2 – IKE Main Mode – Umsetzung des Diffie-Hellman-Verfahrens

```
Frame 3: 214 bytes on wire (1712 bits), 214 bytes captured (1712
bits) on interface 0  A >>> B
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2
User Datagram Protocol, Src Port: 500, Dst Port: 500
Internet Security Association and Key Management Protocol
  Initiator SPI: a93311f793844263
  Responder SPI: 8ec4e54d335d2687
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  .... ..0 = Encryption: Not encrypted
  .... ..0. = Commit: No commit
  .... .0.. = Authentication: No authentication
  Payload: Key Exchange (4)
    Next payload: Nonce (10)
    Payload length: 36
  Key Exchange Data: dea402c4acede7f3deaf139fb9be156fba854c7e17d186bc...
  Payload: Nonce (10)
    Next payload: NAT-D (RFC 3947) (20)
    Payload length: 36
  Nonce DATA: 26c7cbb0b16c80fccf04292800eee2d9066ec853c1c12cea...
...

```

```
Frame 4: 214 bytes on wire (1712 bits), 214 bytes captured (1712
bits) on interface 0  A <<< B
Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1
User Datagram Protocol, Src Port: 500, Dst Port: 500
```

---

**Internet Security Association and Key Management Protocol**

Initiator SPI: a93311f793844263  
 Responder SPI: 8ec4e54d335d2687  
 Exchange type: Identity Protection (Main Mode) (2)  
 Flags: 0x00  
 .... .0 = Encryption: **Not encrypted**  
 .... .0. = Commit: No commit  
 .... .0.. = Authentication: No authentication  
 Message ID: 0x00000000  
 Length: 172  
 Payload: Key Exchange (4)  
 Next payload: Nonce (10)  
 Payload length: 36  
**Key Exchange Data:** 7e04039108ed5b48f2631a8c7dbbc2322875f94ad3ed1358...  
 Payload: Nonce (10)  
 Next payload: NAT-D (RFC 3947) (20)  
 Payload length: 36  
**Nonce DATA:** 290c5cdcbc3f9dd9f754be62f30338fa12af070b6fc3dc5...  
 ...

### **Schritt 3 – IKE Main Mode – Authentifikation der Kommunikationspartner**

**Frame 5:** 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits) on interface 0    A >>> B  
 Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2  
 User Datagram Protocol, Src Port: 500, Dst Port: 500  
**Internet Security Association and Key Management Protocol**

Initiator SPI: a93311f793844263  
 Responder SPI: 8ec4e54d335d2687  
 Exchange type: Identity Protection (Main Mode) (2)  
 Flags: 0x01  
 .... .1 = Encryption: **Encrypted**  
 .... .0. = Commit: No commit  
 .... .0.. = Authentication: No authentication  
 Message ID: 0x00000000  
 Length: 124  
**Encrypted Data (96 bytes)**

**Frame 6:** 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0    A <<< B  
 Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1  
 User Datagram Protocol, Src Port: 500, Dst Port: 500  
**Internet Security Association and Key Management Protocol**

Initiator SPI: a93311f793844263

```
Responder SPI: 8ec4e54d335d2687
Exchange type: Identity Protection (Main Mode) (2)
Flags: 0x01
.... .1 = Encryption: Encrypted
.... .0. = Commit: No commit
.... .0.. = Authentication: No authentication
Message ID: 0x00000000
Length: 92
Encrypted Data (64 bytes)
```

### Aufbau der Phase 2 mit der IPSec Security-Assoziation – „Basic Quick Mode“-Protokoll

**Frame 7:** 230 bytes on wire (1840 bits), 230 bytes captured (1840 bits) on interface 0    A >>> B

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2  
User Datagram Protocol, Src Port: 500, Dst Port: 500

#### Internet Security Association and Key Management Protocol

```
Initiator SPI: a93311f793844263
Responder SPI: 8ec4e54d335d2687
Next payload: Hash (8)
Exchange type: Quick Mode (32)
Flags: 0x01
.... .1 = Encryption: Encrypted
.... .0. = Commit: No commit
.... .0.. = Authentication: No authentication
Message ID: 0x7f1877fd
Length: 188
Encrypted Data (160 bytes)
```

**Frame 8:** 230 bytes on wire (1840 bits), 230 bytes captured (1840 bits) on interface 0    A <<< B

Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1  
User Datagram Protocol, Src Port: 500, Dst Port: 500

#### Internet Security Association and Key Management Protocol

```
Initiator SPI: a93311f793844263
Responder SPI: 8ec4e54d335d2687
Exchange type: Quick Mode (32)
Flags: 0x01
.... .1 = Encryption: Encrypted
.... .0. = Commit: No commit
.... .0.. = Authentication: No authentication
Message ID: 0x7f1877fd
Length: 188
```

**Encrypted Data (160 bytes)**

**Frame 9:** 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0    A >>> B  
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2  
User Datagram Protocol, Src Port: 500, Dst Port: 500  
**Internet Security Association and Key Management Protocol**  
    Initiator SPI: a93311f793844263  
    Responder SPI: 8ec4e54d335d2687  
    Exchange type: Quick Mode (32)  
    Flags: 0x01  
        .... .1 = Encryption: **Encrypted**  
        .... .0. = Commit: No commit  
        .... .0.. = Authentication: No authentication  
    Message ID: 0x7f1877fd  
    Length: 76  
**Encrypted Data (48 bytes)**

**Transfer Mode: Sicherung der IP-Pakete mit ESP inklusiv Anti-Replay Service**

**Frame 10:** 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface 0    A >>> B  
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2  
**Encapsulating Security Payload**  
    ESP SPI: 0xc9e8cf58 (3387477848)  
    ESP Sequence: 1

**Frame 11:** 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface 0    A <<< B  
Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1  
**Encapsulating Security Payload**  
    ESP SPI: 0xca4d2ae5 (3394054885)  
    ESP Sequence: 1

**Frame 12:** 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface 0    A >>> B  
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2  
**Encapsulating Security Payload**  
    ESP SPI: 0xc9e8cf58 (3387477848)  
    ESP Sequence: 2

**Frame 13:** 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface 0    A <<< B  
Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1  
**Encapsulating Security Payload**

**ESP SPI:** 0xca4d2ae5 (3394054885)  
**ESP Sequence:** 2

**Frame 14:** 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface 0   **A >> B**

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2

**Encapsulating Security Payload**

**ESP SPI:** 0xc9e8cf58 (3387477848)  
**ESP Sequence:** 3

**Frame 15:** 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface 0   **A << B**

Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1

**Encapsulating Security Payload**

**ESP SPI:** 0xca4d2ae5 (3394054885)  
**ESP Sequence:** 3

---

## 10.7 Zusammenfassung

IPSec ist der Standard für die Cyber-Sicherheit von IP-Paketen über unsichere Netze wie das Internet. Der Großteil der Anwendungen liegt im Bereich der sicheren Kommunikation zwischen Unternehmen und deren Niederlassungen oder mit anderen Unternehmen. Aber auch die Authentifikation von Mobil-Mitarbeitern für den sicheren Zugang über das Internet in das Unternehmensnetz und seine Dienste ist ein großer Anwendungsbereich von IPSec.

---

## 10.8 Übungsaufgaben

### Übungsaufgabe 1

Bitte kreuzen Sie Ihre Antworten an!

	Cyber-Sicherheitsmechanismen
	IPSec
Gewährleistung von Cyber-Sicherheitsbedürfnissen	Vertraulichkeit
	Authentifikation
	Authentizität
	Integrität
	Verbindlichkeit
	Verfügbarkeit
	Anonymisierung/ Pseudonymisierung

Cyber-Sicherheitsstrategien	Vermeiden von Angriffen	
	Entgegenwirken von Angriffen	
	Erkennen von Angriffen	

### Übungsaufgabe 2

Nennen Sie die Cyber-Sicherheitsdienste, die bei dem AH und ESP Header angeboten werden!

### Übungsaufgabe 3

Beschreiben Sie die Vorteile der Realisierungsformen IPSec-Gateway und IP-Sec-Client!

### Übungsaufgabe 4

Erläutern Sie die zwei unterschiedlichen Modi bei IPSec und deren Anwendungsfelder und zeigen Sie den prinzipiellen Aufbau der IP-Pakete (Original/New-IP-Header, IPSec-Header, Data)!

Name des 1. Modus: \_\_\_\_\_

IP-Paket

Anwendungsfelder: ?

Name des 2. Modus: \_\_\_\_\_

IP-Paket

Anwendungsfelder: ?

### Übungsaufgabe 5

Nennen Sie unterschiedliche Security Associations (SA), Modi in den SAs und deren Aufgaben!

SA: \_\_\_\_\_

Modi: \_\_\_\_\_

Aufgaben:

\_\_\_\_\_

SA: \_\_\_\_\_

Modi: \_\_\_\_\_

Aufgaben:

\_\_\_\_\_

**Übungsaufgabe 6**

Diskutieren Sie die Vor- und Nachteile des Main- und Aggressive Modes!

**Übungsaufgabe 7**

Sie wollen die Kommunikation zwischen einigen Mitarbeitern an zwei unterschiedlichen Arbeitsorten mithilfe von IPSec schützen. Die Verschlüsselung soll End-to-End sein. Welchen Mode wählen Sie dafür?

**Übungsaufgabe 8**

Sie wollen die Kommunikation zwischen einigen Mitarbeitern an zwei Standorten mithilfe von IPSec schützen. Es soll auch verhindert werden, dass ein Angreifer erkennen kann, wer die Kommunikation in den Niederlassungen durchführt. Welchen Mode wählen Sie dafür?

**Übungsaufgabe 9**

Welche Felder im Header des originalen IP-Pakets können beim Authentication Header (AH) nicht für die Integritäts- und Authentizitätsprüfung berücksichtigt werden und warum?

**Übungsaufgabe 10**

Nennen und beschreiben Sie kurz die drei Phasen des Main Modes innerhalb des Internet-Key-Exchange-Protokolls. Welcher zentrale Unterschied besteht zwischen dem Main Mode und dem Aggressive Mode?

**Übungsaufgabe 11**

Beschreiben Sie kurz, wofür der Quick Mode innerhalb des Internet-Key-Exchange-Protokolls verwendet wird. Wovon hängt die Sicherheit des Quick Modes ab und durch welche Funktionalität innerhalb des Quick Modes kann die Cyber-Sicherheit des gesamten Protokolls theoretisch erhöht werden?

**Übungsaufgabe 12**

Sie wollen die Kommunikation zwischen Mitarbeitern an mehreren entfernten Standorten mithilfe von IPSec schützen. Sie haben sich bereits dazu entschlossen, an jedem Standort mindestens ein IPSec-Gateway einzurichten. Mit welcher Methode würden Sie die Authentifikation der Kommunikationspartner innerhalb des Internet-Key-Exchange-Protokolls realisieren? Begründen Sie Ihre Auswahl!

Ergebnisse siehe: <https://norbert-pohlmann.com/cyber-sicherheit/uebungen/>.

---

**Literatur**

1. Campo Ma, Pohlmann N (2003) Virtual Private Network (VPN). MITP-Verlag, Bonn



# Transport Layer Security (TLS)/ Secure Socket Layer (SSL)

11

Im Kapitel „Transport Layer Security (TLS)/Secure Socket Layer (SSL) – TLS/SSL“ werden die Cyber-Sicherheitsarchitektur, Cyber-Sicherheitsprinzipien, Cyber-Sicherheitsmechanismen und Cyber-Sicherheitsprotokolle des IETF Sicherheitsstandards für die Transportebene vermittelt.

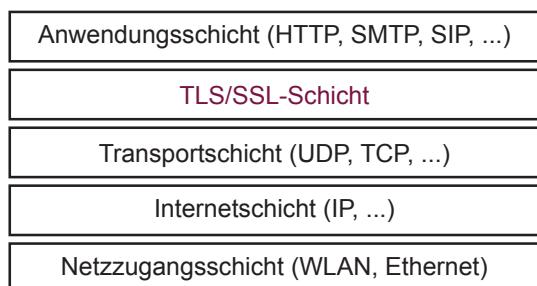
## 11.1 Einleitung

Da das Internet offen ist und die Angriffsmöglichkeiten sowie Angriffswahrscheinlichkeiten sehr groß sind, ist die Nutzung einer verschlüsselten und integritätsgesicherten Kommunikation zwischen Client und Server von besonderer Bedeutung.

Sehr viele Cyber-Sicherheitsaspekte im Web, wie Eingabe von Passwörtern und Kreditkarten-Informationen haben mit der Einrichtung einer vertrauenswürdigen Verbindung zwischen Client und Server zu tun [1].

Der vorherrschende Ansatz für die Transportverschlüsselung im Web ist die Verwendung von TLS (Transport Layer Security)/SSL (Secure Socket Layer) – TLS/SSL (siehe Abb. 11.1). TLS/SSL ist ein anwendungsunabhängiges Cyber-Sicherheitsprotokoll, das logisch auf einem Transportprotokoll aufsetzt.

**Abb. 11.1** TLS/SSL im TCP/IP-Referenzmodell



In diesem Abschnitt werden exemplarisch die Versionen TLS 1.2 und frühere Versionen behandelt.

Die folgenden Cyber-Sicherheitsfunktionen werden von TLS/SSL angeboten:

- **Authentifikation** von Server und Client unter Verwendung von asymmetrischen Verschlüsselungsverfahren und elektronischen Zertifikaten.
- **Vertrauliche Client-to-Server Datenübertragung** mithilfe symmetrischer Verschlüsselungsverfahren unter der Nutzung eines gemeinsamen Sitzungsschlüssels.
- **Sicherstellung der Integrität** der transportierten Daten unter Verwendung des HMAC-Verfahrens.
- TLS/SSL bietet auch die Komprimierung der Daten an.

**Wichtig** TLS/SSL schützt TCP/UDP-Daten auf der Transportebene während der Übertragung.

Hinweis:

Die Idee kam von Netscape, die die erste Version von SSL 1994 veröffentlichte. 1999 wurde SSL von der IETF als Standard festgelegt und umbenannt zu Transport Layer Security (TLS). Da aber heute noch im Sprachgebrauch SSL fest verankert ist, wird im Weiteren immer von TLS/SSL gesprochen.

## 11.2 Einbindung in die Kommunikationsarchitektur

TLS/SSL kann eine Vielzahl höherer Anwendungsprotokolle unterstützen, wie HTTP, SMTP, SIP, IMAP, FTP, Telnet. Die genauen Eigenschaften des TLS/SSL-Kanals werden bei der Einrichtung der verschlüsselten und integritäts-sicheren Kommunikation zwischen Client und Server festgelegt, können aber Anwendungsdaten-Fragmentierung und Komprimierung beinhalten, die in Kombination mit Authentifikation von Client und Server sowie Integrität, Authentizität und Vertraulichkeit der Transportdaten angewendet werden. TLS/SSL-Schicht ist in zwei Teil-Schichten angeordnet. Den Kern des TLS/SSL-Protokolls bildet eine TLS-Datensatz-Protokollsschicht, die einen sicheren Kanal zwischen Client und einem Server implementiert.

### Schichteneinordnung

Die TLS/SSL-Schicht befindet sich zwischen der Transport- und Anwendungsschicht. Sie übernimmt zusätzlich die Aufgaben der Sitzungs- und Präsentationsschicht

(Schichten 5 und 6) des ISO/OSI-Modells. Ein wesentlicher Vorteil der Sitzungsschicht gegenüber der Transportschicht besteht darin, dass Zustandsinformationen über einen längeren Zeitraum und über verschiedene Einzelverbindungen hinweg gespeichert und für die Verwaltung genutzt werden können.

Für das zustandslose HTTP-Protokoll, das für jeden Zugriff auf eine Webseite eine neue TCP-Verbindung aufbauen kann, bedeutet das, dass mehrere solcher Verbindungen zu einer TLS/SSL-Sitzung gebündelt und damit effizienter als die jeweiligen Einzelverbindungen verwaltet werden können.

Die TLS/SSL-Protokolle sind erweiterbar und flexibel, um Zukunftssicherheit vor allem bei den Verschlüsselungsalgorithmen zu gewährleisten.

TLS/SSL arbeitet transparent, sodass es leicht eingesetzt werden kann, um Anwendungsprotokollen/-diensten, ohne eigene Cyber-Sicherheitsmechanismen, vertrauenswürdige Verbindungen zur Verfügung zu stellen.

### Funktionsweise der TLS/SSL-Schicht

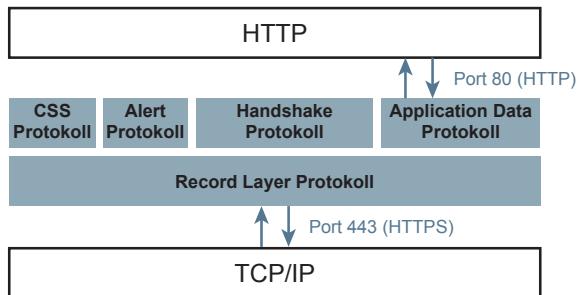
Die Umsetzung der TLS/SSL-Schicht funktioniert so, dass für die Anwendungsprotokolle eine weitere Port-Nummer als Transportadresse definiert wurde, die genutzt wird, wenn die Kommunikation zu diesen Anwendungen TLS/SSL-gesichert umgesetzt werden soll. Eine Kommunikationsanwendung hat dann zusätzlich eine Port-Nummer für die Nutzung der TLS/SSL-Sicherheitsdienste. Im Folgenden sind beispielhaft Kommunikationsanwendung, Port-Nummer und die passende Port-Nummer für die entsprechende TLS/SSL-gesicherte Kommunikation aufgezeigt, siehe Tab. 11.1.

Anhand der Portnummer lässt sich erkennen, um welches ursprüngliche Kommunikationsanwendungsprotokoll es sich bei den übertragenen Daten handelt. Beispielsweise ist Port 443 HTTPS, also wird auf der Kommunikationsanwendung das HTTP-Protokoll zwischen dem entsprechenden Client und Server genutzt.

**Tab. 11.1** Port-Nummer Kommunikationsanwendungen und entsprechende TLS/SSL-Zugänge

Kommunikationsanwendung	Port-Nummer	TLS/SSL Port-Nummer
Hypertext Transfer Protocol – HTTP	80	443
Simple Mail Transfer Protocol – SMTP	25	465
Internet Message Access Protocol – IMAP	143	993
Session Initiation Protocol – SIP	5060	5061
File Transfer Protocol – FTP	20, 21	989, 990
Teletype Network – TELNET	23	992
...	...	..

**Abb. 11.2** Zwei Schichten von TLS/SSL mit den entsprechenden HTTP-Ports



In Abb. 11.2 ist am Beispiel der Kommunikationsanwendung HTTP die Integration der TLS/SSL-Schicht mit den Protokollen und den verschiedenen Port-Nummer dargestellt.

Der Client kann durch die Wahl des Ports entscheiden, ob die Kommunikation TLS/SSL-gesichert sein soll oder im Klartext:

- Port 80: http-Kommunikation im Klartext
- Port 443: http-Kommunikation TLS/SSL-gesichert

### Aufbau der TLS/SSL-Schicht

Die TLS/SSL-Schicht besteht aus zwei Teil-Schichten:

- höhere Schicht mit den TLS/SSL-Teil-Protokollen (CCS, Alert, Handshake, Application)
- Record-Schicht mit dem Record Layer-Protokoll

Besondere Bedeutung haben dabei die Nachrichten-Typen des Handshake-Protokolls, die zum Verbindungsauftbau dienen. Im selben IT-System können Prozesse auch an TLS/SSL vorbei direkt auf TCP zugreifen oder den definierten Port für die Kommunikationsanwendung nutzen, siehe Abb. 11.2. – direkte Ansprache Port 80.

### Praktische Relevanz von TLS/SSL

Da TLS/SSL in allen wichtigen Technologien wie Browern, Web-Servern, E-Mail-Servern usw. eingebunden ist, wird TLS/SSL faktisch als Standard für die Transportverschlüsselung verwendet.

---

## 11.3 Protokolle der TLS/SSL-Schicht

Im Folgenden werden die einzelnen Protokolle der TLS/SSL-Schicht beschrieben.

### 1. TLS/SSL – Record Layer-Protokoll

Das Record Layer Protokoll leitet die Klartext-Anwendungsdaten aus der Anwendungsschicht verschlüsselt an die Transportschicht weiter.

Das Record Layer-Protokoll bietet zwei verschiedene Cyber-Sicherheitsdienste, die zusammen oder einzeln genutzt werden können:

- Client-to-Server-Verschlüsselung zwischen den beiden Transport-Endpunkten
- Sicherung der Nachrichten-Integrität und -Authentizität

Zu den Aufgaben des Record-Protokolls gehören

- die Fragmentierung der Klartext-Anwendungsdaten der Anwendungsschicht,
- Kompression der resultierenden Fragmente,
- Berechnung von HMACs über die (komprimierten) Fragmente und
- Verschlüsselung der TLS/SSL-Records (komprimierte Fragment mit HMAC).

### A) Aufbau des Record-Protokoll-Headers

0	1	2	3	5
Type	Version Major	Version Minor	Length	Weitere Daten

Gesamtgröße des Record-Protokoll-Headers: 5 Byte

**Type** (1 Byte) Nummer der „höheren“ TLS/SSL-Teil-Protokolle

- Change Cipher Spec 20
- Alert 21
- Handshake 22
- Application Data 23

**Version Major** (1 Byte) Hauptnummer der Version

**Version Minor** (1 Byte) Unterversionsnummer

**Length** (2 Byte) Länge der Nutzdaten in Byte.

Maximalwert darf nicht größer sein als  $2^{14} + 2.048$  (16.384 + 2048 Byte).

### B) Ablauf in der Record-Schicht

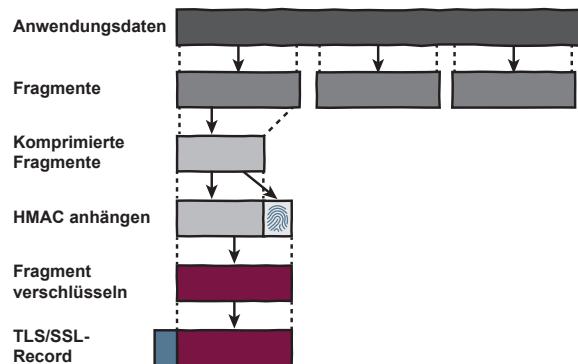
Die Record-Schicht hat die Aufgabe, Anwendungsdaten in TLS/SSL-Records mit einer maximalen Größe von  $2^{14}$  Byte zu fragmentieren. Optional werden die Fragmente dann komprimiert. Das Komprimierungsverfahren wird beim Handshake ausgehandelt. Diese (komprimierten) Fragmente + Sequenznummer werden dann mit einer HMAC-Funktion gehasht.

### Berechnung des HMACs für die Integritätssicherheit der Anwendungsfragmente:

HMAC = KH (HMAC-Key,

SeqNum || Compressed.type || Compressed.version ||  
Compressed.length || Compressed.fragment)

**Abb. 11.3** Ablauf in der Record-Schicht



**KH** „Keyed-Hashing for Message Authentication“-Verfahren; HMAC-Verfahren

Die (komprimierten) Fragmente sowie der HMAC werden dann verschlüsselt und als TLS/SSL-Records an die Transportschicht übergeben, siehe Abb. 11.3.

Hinweis:

Die Kompression muss verlustfrei sein und darf die Länge des Fragments nicht mehr als 1024 Byte vergrößern. Bei kleinen Blöcken kann es vorkommen, dass durch die Kompression der Block vergrößert anstatt verkleinert wird.

### C) Verschlüsselte Daten

Die eigentlichen Nutzdaten der Anwendungsprotokolle werden bei TLS/SSL bei der Version 1.2 verschlüsselt und HMAC-gesichert übertragen. Der komplette Record-Layer-Header ist ungeschützt und somit lesbar. Zudem kann beim Handshake-Protokoll die Art der Handshake-Nachricht ausgelesen werden, siehe Abb. 11.4.

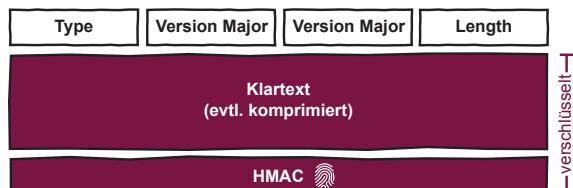
## 2. TLS/SSL – Application Data Protokoll

Anders als die anderen Protokolle oberhalb des Record Protokolls reicht das Application Data Protokoll die Anwendungsdaten transparent durch.

Die Daten werden entsprechend der ausgehandelten Sicherheitsparameter aus dem Handshake Protokoll in dem Record Layer fragmentiert, komprimiert, gegen Verfälschung geschützt und verschlüsselt.

Gesamtgröße: variabel

**Abb. 11.4** Record-Layer-Header



### 3. TLS/SSL – ChangeCipherSpec (CCS) Protokoll

Das ChangeCipherSpec (CCS) Protokoll wird bei Änderung des kryptografischen Algorithmus beziehungsweise der Parameter genutzt. Es enthält nur eine Meldung bestehend aus einem Byte mit dem Wert 1. CCS bewirkt, dass der Empfänger die während des Handshakes ausgehandelten Parameter für die aktive Sitzung übernimmt. Wird eine vorhandene Sitzung reaktiviert, erfolgt die Meldung ChangeCipherSpec nach der Meldung ServerHelloDone.

### 4. TLS/SSL – Alert Protokoll

Das Alert Protokoll dient der Signalisierung von besonderen Zuständen beziehungsweise Problemen wie Fehler oder Verbindungsabbruch.

Die Protokollnachricht enthält zwei Felder: Sicherheitslevel und Fehlercode.

0	1	3
Type	Error	Weitere Daten

Gesamtgröße des Alert Protokoll Headers: 2 Byte

Das erste Byte kann den Wert warning 1) oder fatal 2) haben und gibt den Grad der Fehlermeldung an. Wird der Wert „fatal“ übertragen, beendet TLS/SSL sofort die Verbindung. Andere Verbindungen aus der Session bleiben bestehen, aber es kann keine neue Verbindung erzeugt werden.

Das zweite Byte beschreibt den Fehler genauer. Fatale Alert-Meldungen stehen in der Tab. 11.2 und Warnungs Alert-Meldungen stehen in der Tab. 11.3.

**Tab. 11.2** Fatale Alert-Meldungen

Name	Inhalt
Bad_record_mac(20)	Falscher HMAC für Record
Record_overflow(22)	Record Länge ist größer als $2^{14} + 2048$ Byte
Decompression_failure(30)	Dekomprimierungsfunktion erhält falschen Input
Handshake_failure(40)	Sender akzeptiert die Sicherheitsparameter nicht
Illegal_parameter(47)	Feld im Handshake war inkonsistent
Unknown_ca(48)	Root-Zertifikat konnte nicht gefunden werden oder ist nicht unter den vertrauenswürdigen Zertifizierungsinstanzen
Access_denied(49)	Zertifikat gültig, aber die Zugangskontrolle hat entschieden, keinen Zugriff zu gewähren
Decode_error(50)	Länge der Nachricht falsch oder Nachricht konnte nicht decodiert werden, da ein Feld nicht korrekt ist
Decrypt_error(51)	Beim Handshake ist die kryptografische Operation fehlgeschlagen; Sender war nicht fähig, die Signatur oder das Ende der Nachricht zu verifizieren
Protocol_version(70)	Protokollversion wird nicht unterstützt
Insufficient_security(71)	Server erwartet höhere Cipher Suite als der Client unterstützt
Internal_error(80)	Interner Fehler unabhängig von Nutzern

**Tab. 11.3** Warnungs-Alert-Meldungen

Name	Inhalt
Decryption_failed_RESERVED(21)	Nicht mehr verwendet
No_certificate_RESERVED(41)	Nicht mehr verwendet
Export_restriction_RESERVED(60)	Nicht mehr verwendet
Bad_certificate(42)	Zertifikat konnte nicht erfolgreich verifiziert werden
Unsupported_certificate(43)	Zertifikat eines nicht unterstützten Types
Certificate_revoked(44)	Zertifikat wurde vom „Signer“ gesperrt
Certificate_expired(45)	Zertifikat ist abgelaufen
Certificate_unknown(46)	Sonstige Zertifikatsprobleme
User_canceled(90)	Handshake von Nutzer abgebrochen
No_renegotiation(100)	Wenn nach dem ClientHello oder Hello die Parameter neu ausgehandelt werden sollen
Unsupported_extension(110)	Versendet von Clients, die vom Server eine Erweiterung bekommen, die sie nicht verlangt haben

## 5. TLS/SSL – Handshake Protokoll

Die Handshake-Nachrichten ermöglichen den Aufbau einer TLS/SSL-Verbindung. Das Handshake Protokoll dient zur Identifikation und Authentifizierung der Kommunikationspartner sowie zum Aushandeln kryptografischer Algorithmen, Schlüssel und Parameter, die im TLS/SSL Record Layer Protokoll verwendet werden und zum Austausch benötigter vertrauenswürdiger Informationen.

### A) Aufbau

0	1	2	5
Type	Length	Content	Weitere Daten

Gesamtgröße des Handshake Protokoll Headers: 5 Byte

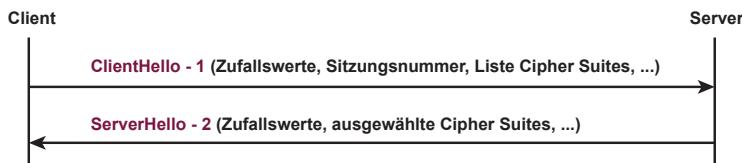
**Type** (1 Byte) Zeigt eine von zehn möglichen Nachrichten an (siehe Abb. 11.5)

**Length** (3 Byte) Länge der Nachricht in Bytes

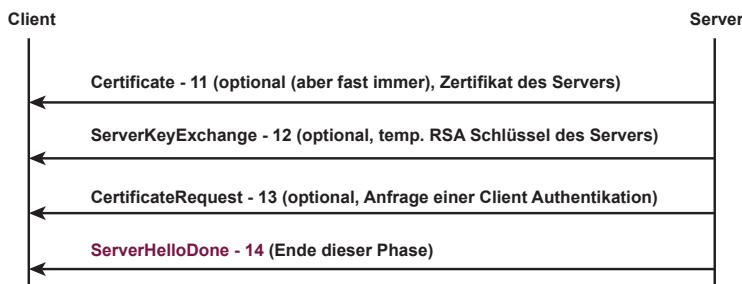
**Content** (1 Byte) Parameter, die mit dieser Nachricht assoziiert sind

**B) In Abb. 11.5 sind die Nachrichten-Typen des Handshake Protokolls dargestellt.**

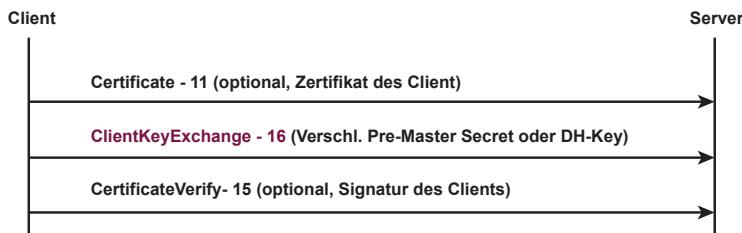
### Phase 1 (Aushandlung der Sicherheitsparameter)



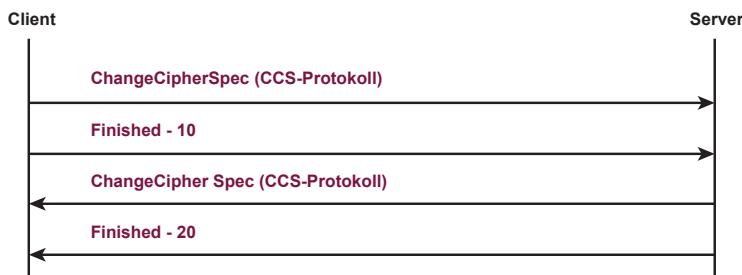
### Phase 2 (Serverauthentifizierung und Schlüsselaustausch)



### Phase 3 (Clientauthentifizierung und Schlüsselaustausch)



### Phase 4 (Cipher Suite wird aktiviert und der Handshake beendet)



**Abb. 11.5** Übersicht der Nachrichten-Typen des Handshake Protokolls mit den verschiedenen Phasen

### Handshake Protokollablauf

TLS/SSL ist ein zustandsbehaftetes Cyber-Sicherheitsprotokoll, mit dem Sitzungen zwischen Kommunikationspartnern etabliert werden können. Ein Client kann zu einem Zeitpunkt mehrere solche Sitzungen zum gleichen oder zu verschiedenen Servern unterhalten. TLS/SSL benutzt eine Session, um Zustandsinformationen über einen längeren Zeitraum zu speichern und nutzen zu können. Wie bei IPSec nutzt TLS/SSL für die bidirektionale Verbindung zwischen Client/Server zwei unterschiedliche Sitzungsschlüssel. Kryptografische Verfahren und Hashfunktion werden pro Sitzung ausgehandelt.

TLS/SSL versucht, möglichst wenig geheime Informationen über das nicht vertrauenswürdige Transportsystem Internet zu übertragen. Daher werden lediglich Basisinformationen ausgetauscht, womit die beteiligten Kommunikationspartner (Client und Server) dezentral ihre Geheimnisse, wie die gemeinsamen Session Keys und HMAC-Schlüssel, berechnen. Eine TLS/SSL-Session ist eine „Security-Assoziation“ zwischen einem Client und einem Server. Sessions werden über das Handshake-Protokoll aufgebaut. Eine Session definiert eine Menge von kryptografischen Sicherheitsparametern, die gemeinsam über mehrere Verbindungen genutzt werden können.

Der Sinn der Session besteht darin, nicht jedes Mal eine neue zeitaufwendige Verhandlung der Sicherheitsparameter auszuführen.

### Ein Session-Zustand ist definiert über folgende Parameter

<b>Session-Identifier</b>	Zufällige Bytesequenz, die vom Server erzeugt wird, um eine aktive oder wiederherstellbare Session zu identifizieren.
<b>Peer-Certificate</b>	X509.v3 Zertifikat des Clients (falls vorhanden).
<b>Compression-Method</b>	Kompressionsalgorithmus.
<b>Cipher-Spec</b>	Definiert den Verschlüsselungsalgorithmus sowie die One-Way-Hash- funktion für den HMAC. Es werden noch weitere Attribute, wie die HMAC- Länge, festgelegt.
<b>Master-Secret</b>	48-Byte, die vom Client und Server benutzt werden, um die geheimen Schlüssel daraus abzuleiten.
<b>Is-Resumable</b>	Mit diesem Flag wird angezeigt, ob diese Session für neue Verbindungen genutzt werden kann

### TLS/SSL-Connection

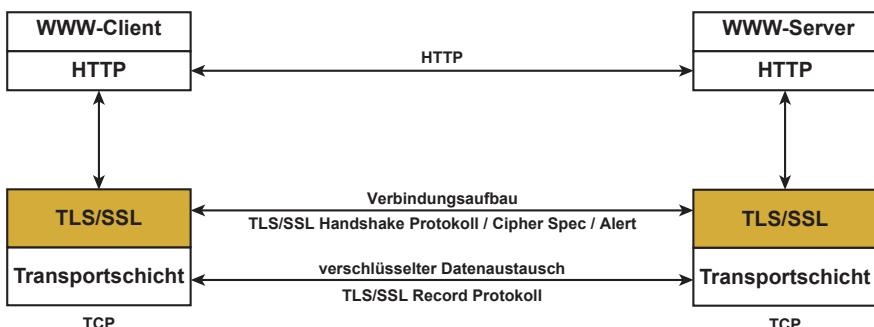
Die TLS/SSL-Connection ist ein logischer Transportkanal zwischen Client und Server. Es handelt sich bei TLS/SSL um eine Peer-to-Peer-Verbindung, die nur temporär genutzt wird. Die TLS/SSL-Connection ist immer mit einer Session assoziiert. Damit können aus einer Session mehrere TLS/SSL-Connections aufgebaut und parallel betrieben werden.

### Zustände einer TLS/SSL-Connection (Verbindung)

<b>Server-And-Client-Random</b>	Zufallszahlen, die von Server und Client für jede Verbindung neu erzeugt werden.
<b>Server-Write-MAC-Secret</b>	Geheimer Schlüssel für die HMAC-Operationen von Daten, die zum Server übertragen werden.
<b>Client-Write-MAC-Secret</b>	Geheimer Schlüssel für die HMAC-Operationen von Daten, die zum Client übertragen werden.
<b>Server-Write-Key</b>	Symmetrischer Schlüssel für die Verschlüsselung vom Server und für die Entschlüsselung vom Client.
<b>Client-Write-Key</b>	Symmetrischer Schlüssel für die Verschlüsselung vom Client und für die Entschlüsselung vom Server.
<b>Initialization-Vectors</b>	Wird genutzt, wenn ein entsprechender Mode of Operation mit Initialization Vector (IV) verwendet wird.
<b>Sequence-Numbers</b>	Sowohl Client als auch Server nutzen Sequenznummern für die gesendeten und empfangenen Daten jeder Verbindung. Falls der Client oder der Server ein Change Cipher Spec verschickt oder erhält, wird die Sequenznummer wieder auf Zero gesetzt. Sequenznummern können nicht größer als $2^{64} - 1$ werden.

### TLS/SSL: Session/Connection $\Leftrightarrow$ Verfahren/Schlüssel

An den Zuständen der Verbindungen wird deutlich, dass die verwendeten Schlüssel jeweils nur für eine Verbindung gelten. Für alle Verbindungen einer Sitzung werden die gleichen Verfahren genutzt, das heißt, bei der erneuten Verwendung einer bereits bestehenden Verbindung kann auf das Aushandeln der Verfahren im Handshake verzichtet werden, siehe Abb. 11.6.



**Abb. 11.6** Übersicht des Protokollablaufs bei TLS/SSL am Beispiel von HTTP

## Übersicht des Protokollablaufs bei TLS/SSL

### Schichten und Phasen

Der Protokollablauf bei TLS/SSL erfolgt in zwei Schritten.

#### 1. Schritt

Verbindungsauftbau, unterteilt in vier Phasen:

1. Phase Aushandlung der Sicherheitsparameter
2. Phase Serverauthentifizierung (optional) und Schlüsselaustausch
3. Phase Clientauthentifizierung (optional) und Schlüsselaustausch
4. Phase Beendigung des Handshakes

#### 2. Schritt

verschlüsselte und integritätsgesicherte Datenübertragung (Transfer-Mode)

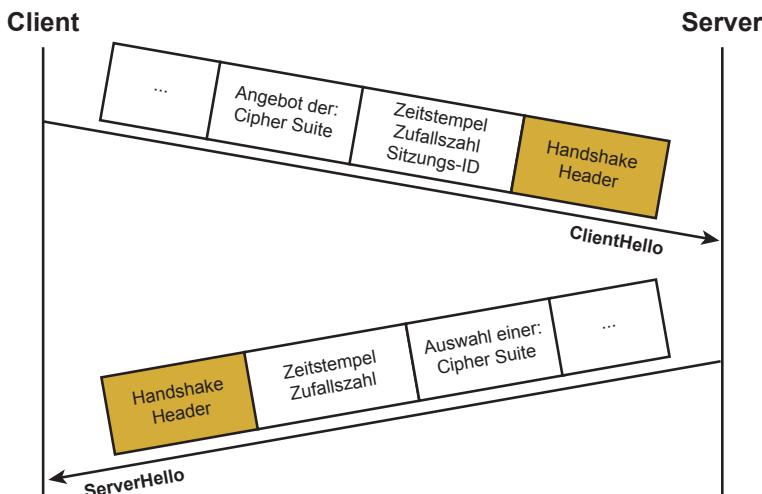
### TLS/SSL – Verbindungsauftbau (Schritt 1)

#### Phase 0: HelloRequest

Der Server kann ein „HelloRequest (0)“ immer zum Client senden. Diese Nachricht hat keine Parameter. Sie wird vom Server geschickt, um den Client zu einem „ClientHello“ zu veranlassen.

Der Client antwortet nur, wenn er sich nicht in einem Handshake befindet. Dieser Nachrichten-Typ soll nicht zum Aufbau einer Verbindung genutzt werden, dies ist die Aufgabe des Clients mit ClientHello. Erhält der Server auf ein HelloRequest keine Antwort, kann die Verbindung geschlossen werden.

**Phase 1: Aushandlung der Sicherheitsparameter (Übersicht), siehe Abb. 11.7.**



**Abb. 11.7** Aushandlung der Sicherheitsparameter

### Phase 1: ClientHello

In der ersten Phase werden die Sicherheitsparameter festgelegt.

Mit dem Nachrichten-Typ „ClientHello (1)“ startet der Client den Aufbau der TLS/SSL-Verbindung.

In einer bereits aktiven TLS/SSL-Verbindung führt diese Nachricht zu einer Neuverhandlung der Sicherheitsparameter.

In dieser Klartextnachricht sind bereits wichtige Informationen zur Erzeugung des gemeinsamen geheimen Schlüssels enthalten:

- Random Client – RC (4 Byte Zeitstempel + 28 Byte Zufallszahl)
- Sitzungs-ID,
- Prioritätenliste der Cipher Suites (Kryptografie- und Kompressionsverfahren), die der Client unterstützt.

Der Client sollte nur kryptografische Verfahren und Funktionen sowie Schlüssellängen für die Chiper Suite anbieten, die sein gewünschtes Cyber-Sicherheitsniveau erfüllen.

### Phase 1: ServerHello

Mit dem Nachrichten-Typ „ServerHello (2)“ antwortet der Server auf das „ClientHello“ des Clients.

Die Nachricht enthält die gleichen Parameter wie der Nachrichten-Typ „ClientHello“, teilweise allerdings mit leicht abgewandelter Bedeutung.

- Random Server – RS (4 Byte Zeitstempel + 28 Byte Zufallszahl)

Zudem enthält dieser Nachrichten-Typ die ausgewählte Cipher Suite vom Server, die Client und Server nachfolgend nutzen. Hat der Client eine Sitzungs-ID vorgeschlagen, überprüft der Server diese Sitzungs-ID und übernimmt sie, sofern diese Sitzung noch nicht zu lange zurückliegt.

Gibt der Server keine Sitzungs-ID an, so bedeutet dies, dass die gegenwärtige Sitzung später nicht erneut aufgenommen wird.

Der Server sollte nur kryptografische Verfahren und Funktionen sowie Schlüssellängen auswählen, die sein gewünschtes Cyber-Sicherheitsniveau erfüllen.

### Cipher Suites

Beim Nachrichten-Typ „Server/Client Hello“ werden die sogenannten Cipher Suites ausgewählt.

Dabei handelt es sich um eine Kombination aus Schlüsselaustauschverfahren, Verschlüsselungsverfahren mit Schlüssellänge und eine One-Way-Hashfunktion zum Integritätscheck.

In Abb. 11.8 ist ein Beispiel des Aufbaues einer Cipher Suite zu sehen.



**Abb. 11.8** Aufbau einer TLS/SSL Cipher Suite

Jede Cipher Suite definiert mögliche Kombinationen aus Schlüsselaustauschverfahren (DHE\_RSA), Verschlüsselungsalgorithmus (AES)/Schlüssellänge (256)/Mode of Operation (GCM) und die One-Way-Hashfunktion (SHA384) für den HMAC.

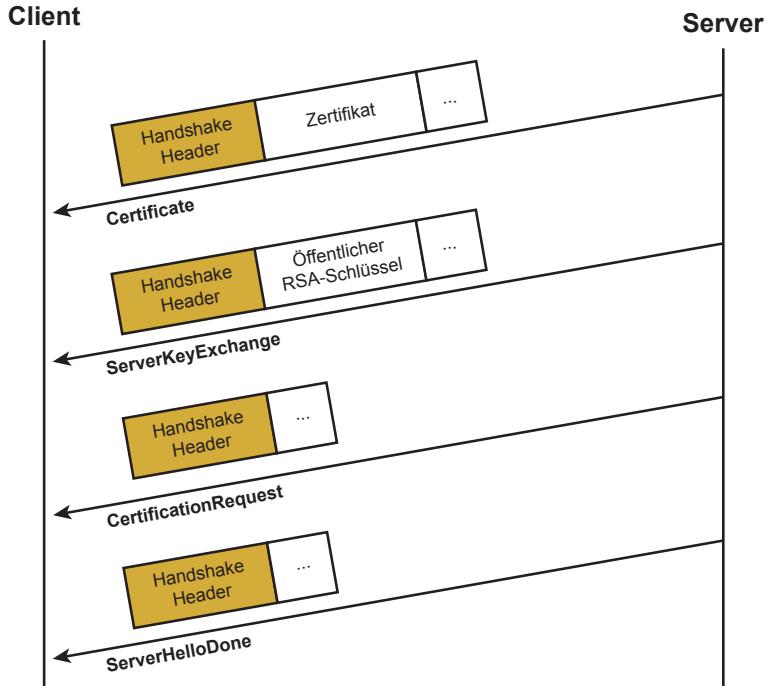
### Phase 2: Serverauthentifizierung und Schlüsselaustausch, siehe Abb. 11.9.

#### Phase 2: Certificate

In der zweiten Phase finden die implizierte Serverauthentifizierung und der Schlüsselaustausch statt.

Soll der Server authentifiziert werden, so muss er dem Client im Nachrichtentyp „Certificate (11)“ sein Zertifikat zukommen lassen.

Beim Server handelt es sich im Normalfall um ein X.509v3-Zertifikat, das für eine Domäne einer Organisation (zum Beispiel `internet-sicherheit.de`) von einer Zertifizierungsinstanz ausgegeben wurde. Dabei muss das Certificate zu



**Abb. 11.9** Serverauthentifizierung und Schlüsselaustausch

der Cipher Suite passen! Wird RSA verwendet, muss das Zertifikat einen RSA-Schlüssel enthalten etc.

### Phase 2: ServerKeyExchange

Diese Meldung wird nicht gesendet, wenn der Server ein Zertifikat mit festen Diffie-Hellman Parametern oder mit einem RSA-Schlüssel besitzt. Versendet der Server kein Zertifikat, so lässt er dem Client im Nachrichten-Typ „ServerKeyExchange“ (12) einen temporären öffentlichen RSA-Schlüssel zukommen.

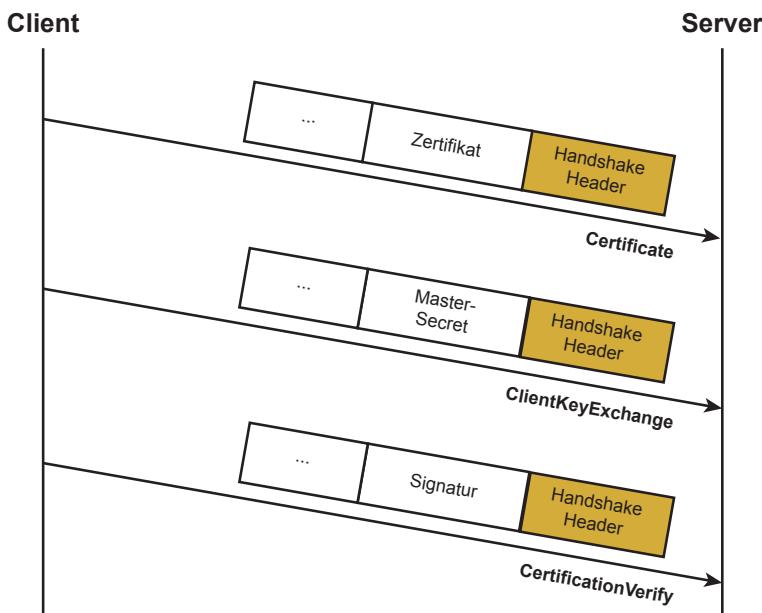
### Phase 2: CertificationRequest

Falls der Server auch eine Authentifikation des Client fordert, sendet er den Nachrichten-Typ „CertificationRequest“ (13).

### Phase 2: ServerHelloDone

Der Server beendet seine Übertragung dieser Phase mit dem Nachrichten-Typ „ServerHelloDone“ (14). Dieser Nachrichten-Typ ist notwendig, da die Nachrichten-Typen „Certificate“, „ServerKeyExchange“ und „CertificateRequest“ nicht notwendigerweise geschickt werden. So erkennt der Client das Ende der Phase 2.

### Phase 3: Clientauthentifizierung und Schlüsselaustausch, siehe Abb. 11.10.



**Abb. 11.10** Clientauthentifizierung und Schlüsselaustausch

### Phase 3: Certificate

In der Phase 3 kann der Client vom Server authentisiert werden und der Schlüsselaustausch wird fortgeführt. Soll der Client authentifiziert werden, so muss er dem Server sein Zertifikat im Nachrichten-Typ „Certificate (11)“ zukommen lassen.

### Phase 3: ClientKeyExchange

Der Client prüft zunächst die Gültigkeit des Server-Zertifikats. Anschließend übermittelt er dem Server mit dem Nachrichten-Typ „ClientKeyExchange (16)“ seine geheime Basisinformation mithilfe des Kryptoverfahrens aus der ausgewählten Cipher Suite, das 48 Byte Pre-Master-Secret (Pre).

Haben sich Client/Server auf das RSA-Verfahren geeinigt, so verschlüsselt der Client das Pre-Master-Secret mit dem öffentlichen Schlüssel des Servers aus dem „Certificate“ (Server-Zertifikat) oder aus dem „ClientKeyExchange“.

Beim Diffie-Hellman-Schlüsselaustauschverfahren sendet der Client nur seinen öffentlichen Schlüssel an den Server zurück. Das Diffie-Hellman-Verfahren wird hier nicht zur Berechnung des geheimen Schlüssels genutzt, sondern zur dezentralen Berechnung des Pre-Master-Secrets (Pre).

### Phase 3: CertificateVerify

Mit dem Nachrichten-Typ „CertificateVerify (15)“ signiert der Client Informationen, sofern er sie in dieser Phase gesendet hat.

Client „beweist“ dem Server, dass er im Besitz des geheimen Schlüssels für das Zertifikat ist.

Ablauf:

- Client berechnet einen Hashwert über die Bytes aller bisher ausgetauschten Handshake-Nachrichten, von ClientHello bis ClientKeyExchange.
- Client signiert diesen Hashwert mit seinem geheimen Schlüssel.
- Der Server berechnet einen Hashwert über die gleichen Handshake-Nachrichten und verifiziert die Signatur mit dem öffentlichen Schlüssel aus dem Zertifikat.

#### A) Master-Secret-Berechnung

Das Pre-Master-Secret und die ausgetauschten Zufallszahlen werden nun von Client und Server genutzt, um das 48 Byte Master-Secret zu berechnen, aus dem die benötigten geheimen Schlüssel (Session Keys, Key zur HMAC-Berechnung, ...) abgeleitet werden.

#### Berechnung des Master-Secrets:

Master-Secret = KH (Pre-Master-Secret, ClientHello.random || ServerHello.random)

KH „Keyed-Hashing for Message Authentication-Verfahren; HMAC-Verfahren

## B) Schlüsselerzeugung

Alle Schlüssel (Session Keys, Key zur HMAC-Berechnung, ...) werden nach dem einen gleichartigen Schema sowohl vom Client als auch vom Server aus dem Master-Secret abgeleitet.

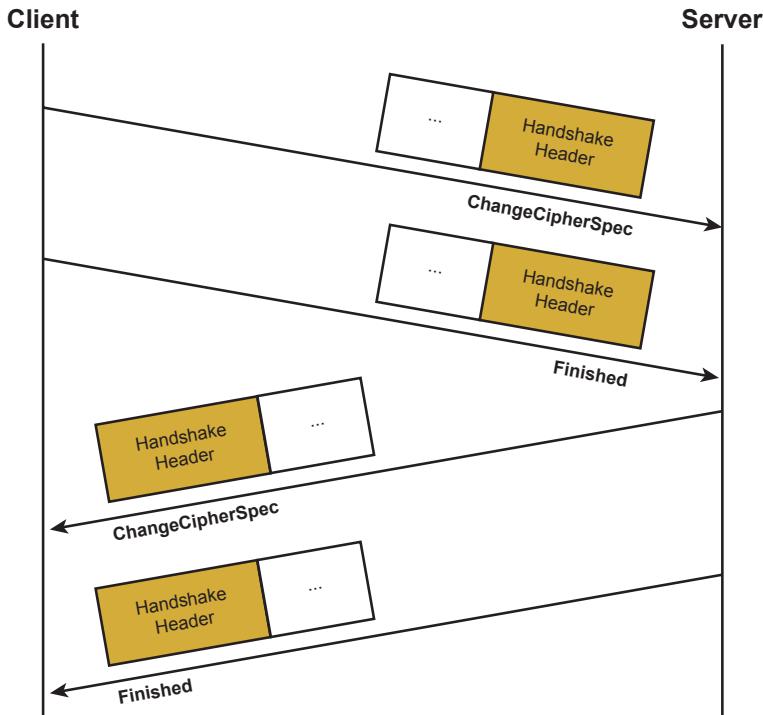
Dazu generiert das Protokoll so lange eine Folge von Schlüsselblöcken „Key-Block“, bis alle Schlüssel damit konstruiert sind.

### Berechnung des Key-Blocks (Schlüsselblock)

Key-Block = KH (Master-Secret, ServerHello.random || ClientHello.random)

KH „Keyed-Hashing for Message Authentication“-Verfahren; HMAC-Verfahren

**Phase 4: Cipher Suite wird aktiviert und der Handshake beendet**, siehe Abb. 11.11.



**Abb. 11.11** Aktivierung der Cipher Suite und Beendigung des Handshakes

#### Phase 4: ChangeCipherSpec + Finished

Die Phase 4 beendet den Handshake.

Mit der „ChangeCipherSpec“-Nachricht (CCS-Protokoll) zeigen Client und Server, dass sie ab jetzt die ausgehandelten Verfahren/Parameter nutzen.

Mit der „Finished (20)“-Nachricht symbolisieren beide, dass ihr Teil des Verbindungs aufbaus abgeschlossen ist.

Diese Meldung ist die erste Nachricht, die bereits mit den neuen Sicherheitsparametern für das Record Protokoll behandelt wird.

---

### 11.4 TLS/SSL-Zertifikate

TLS/SSL-Zertifikate helfen, Attribute von Domänen zu überprüfen.

Wesentliche Inhalte eines Domänen-Zertifikates sind die folgenden Attribute:

- Name der Organisation, deren Authentizität durch dieses Domänen-Zertifikat bestätigt wird
- Public-Key der Organisation (Domäne)
- Name der ausstellenden Zertifizierungsstelle
- Gültigkeitsdauer des Zertifikats

Aufgabe eines Domänen-Zertifikats:

- eindeutige Zuordnung eines Public-Keys zu einer Organisation (zur Domäne)
- Für die Korrektheit dieser Zuordnung und dass die Organisation, die den passenden geheimen Schlüssel besitzt, auch existiert, verbürgt sich die ausstellende Zertifizierungsstelle.
- Diese signiert das Domänen-Zertifikat, wodurch es für Dritte ohne die Kenntnis des geheimen Schlüssels der Zertifizierungsstelle unmöglich wird, das Domänen-Zertifikat zu verändern.

Der Aufbau von Zertifikaten ist standardisiert (X.509v3):

Wichtige Aspekte bei TLS/SSL-Zertifikaten:

Eine Domäne muss schon registriert sein, bevor ein TLS/SSL-Zertifikat beantragt wird, weil Zertifizierungsstellen, die ein Zertifikat ausstellen, die Domain-Inhaberschaft überprüfen müssen.

Bezüglich der Überprüfung der Domain-Inhaberschaft gibt es verschiedene Vertrauensstufen:

- Domain Validated (DV)
- Organisation Validated (OV)
- Extended Validation (EV)

Domain Validated (DV)-Zertificate:

DV-Zertifikate sind die einfachste Art von TLS/SSL-Zertifikaten. DV steht für Domain Validation, das bedeutet, eine Validierung/Überprüfung der Domain. Eine Zertifizierungsstelle bestätigt damit, dass zum Beispiel der Website-Inhaber die

administrative Kontrolle über die Domain nachweisen kann. Sie enthalten wenige Identitätsinformationen im Zertifikat, zum Beispiel enthalten sie keinerlei Unternehmensinformationen. Die DV-Zertifikate können auch für andere Anwendungen wie SMTP verwendet werden.

#### Organization Validated (OV)-Zertificate:

OV-Zertifikate enthalten eine Unternehmensverifizierung. Das heißt, es sind Informationen zum jeweiligen Unternehmen enthalten. Im Gegensatz zu EV-Zertifikaten werden diese Informationen allerdings nicht so prominent angezeigt. Um die Identitätsdaten eines Unternehmens zu erkennen, müssen sich die Besucher der Webseite die Zertifikatdetails ansehen.

#### Extended Validation (EV)-Zertificate:

EV-Zertifikate enthalten die meisten Unternehmensdaten, und Firmen müssen bei dieser Variante die strengsten Anforderungen erfüllen, bevor sie ein solches TLS/SSL-Zertifikat erhalten. Hier steht die verifizierte Identität eines Unternehmens im Mittelpunkt und verleiht so der Webseite das höchste Maß an Glaubwürdigkeit: der Name des betreffenden Unternehmens wird deutlich in der grünen Adresszeile eines Browsers angezeigt.

### Root-Zertifikat (Wurzelzertifikate)

Das Root-Zertifikat ist ein selbstsigniertes Zertifikat der oberen Zertifizierungsinstanz. Sinn und Zweck eines Root-Zertifikates ist es, die Gültigkeit aller untergeordneten Zertifikate validieren zu können. Ein Wurzelzertifikat ist ein wichtiges Element einer Public-Key-Infrastruktur, siehe auch Kap. 4 „Digitale Signatur, elektronische Zertifikate sowie Public Key Infrastruktur (PKI) und PKI-enabled Application (PKA)“. Inhalte eines Zertifikats sind im Allgemeinen der Name des Inhabers, der öffentlichen Schlüssel des Inhabers, die Gültigkeitsdauer des Zertifikates und der Name der Zertifizierungsinstanz, die das Zertifikat ausgestellt hat. Die Zertifizierungsinstanz signiert das Zertifikat mit ihrem geheimen Schlüssel und bestätigt dadurch die Korrektheit der in dem Zertifikat enthaltenen Angaben. Das Zertifikat kann mit dem zugehörigen öffentlichen Schlüssel der Zertifizierungsinstanz überprüft werden.

Dies setzt wiederum voraus, dass die Authentizität und die Integrität dieses öffentlichen Schlüssels der Zertifizierungsinstanz überprüfbar sind. Dazu hat eine Zertifizierungsinstanz auch ein Zertifikat für den eigenen öffentlichen Schlüssel. Dieses Zertifikat wird in der Regel von einer übergeordneten Zertifizierungsinstanz zur Verfügung gestellt, die selber auch ein Zertifikat von einer übergeordneten Zertifizierungsinstanz braucht usw.

Durch die Vorgehensweise wird eine Hierarchie von Zertifikaten generiert, die alle verifiziert werden müssen, um am Ende die Gültigkeit eines eigentlichen Zertifikats überprüfen zu können. Diese Zertifikatshierarchie endet immer an einer Stelle, an der das Wurzelzertifikat steht. Wurzelzertifikate werden von keiner anderen Zertifizierungsinstanz ausgestellt und enthalten keinen nachprüfbares Verweis auf ein anderes Zertifikat. Die oberste Zertifizierungsinstanz signiert ihr eigenes Zertifikat selbst. Das Wurzelzertifikat bildet damit den Vertrauensanker aller ihm untergeordneten Zertifikate. Aus diesem Grund müssen die Wurzelzertifikate auch besonders vertrauenswürdig sein.

Um Zertifikate überprüfen können, muss das entsprechende übergeordnete Wurzelzertifikat für Anwendungen zur Verfügung stehen. Viele Softwareanwendungen enthalten bereits Listen vorinstallierter Wurzelzertifikate verschiedener Zertifizierungsinstanzen. Als wichtiges Beispiel sind in allen Webbrowsern die Wurzelzertifikate für TLS/SSL gespeichert. Die Entscheidung, ob diesen Wurzelzertifikaten vertraut werden kann, liegt letztendlich beim Nutzer. Der Nutzer verlässt sich in der Regel darauf, dass der Herausgeber des Browser nur „echte“ Wurzelzertifikate in seine Liste aufnimmt. Dazu haben die Browser-Hersteller Vertrauensprozesse aufgebaut, damit das Vertrauen gerechtfertigt ist. Die gängigsten Browser haben die wichtigsten Root-Zertifikate der größten Zertifizierungsinstanzen validiert und entsprechend vorinstalliert.

## 11.5 Authentifikationsmethoden

TLS/SSL benutzt elektronische Zertifikate für die Authentifizierung von Server und Client.

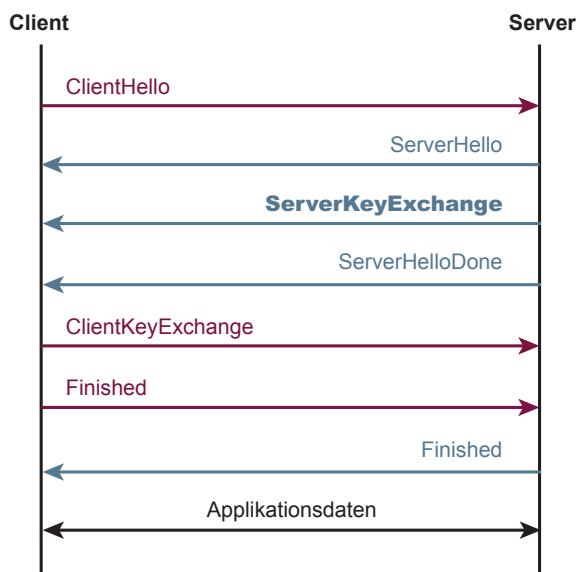
Es werden drei Verbindungsarten bezüglich der Authentifizierung unterschieden:

- Server und Client ohne Authentifizierung
- Server authentifiziert, Client anonym (gängigste Art)
- Server und Client authentifiziert

### Server und Client ohne Authentifizierung

Bei dieser Verbindungsart verlangt weder der Server noch der Client eine Authentifizierung seines Kommunikationspartners durch ein Zertifikat, siehe Abb. 11.12.

**Abb. 11.12** Server und Client authentifiziert



Nach Beendigung des Verbindungsaufbaus können Applikationsdaten ausgetauscht werden.

Die beiderseits anonyme Verbindung ist nicht sicher gegenüber aktiven Man-In-The-Middle-Angriffen.

Diese Verbindungsart sollte daher vermieden werden!

### Server authentifiziert, Client anonym

In diesem Fall sendet der Server Zertifikate mit dem Nachrichten-Typ „Server Zertifikat“. Kann der Client das Zertifikat verifizieren, so kann sich dieser sicher sein, dass nach einem erfolgreichen Verbindungsaufbau eine TLS/SSL-Verbindung zu genau jenem Server zustande gekommen ist, dessen Zertifikat empfangen wurde, siehe Abb. 11.13.

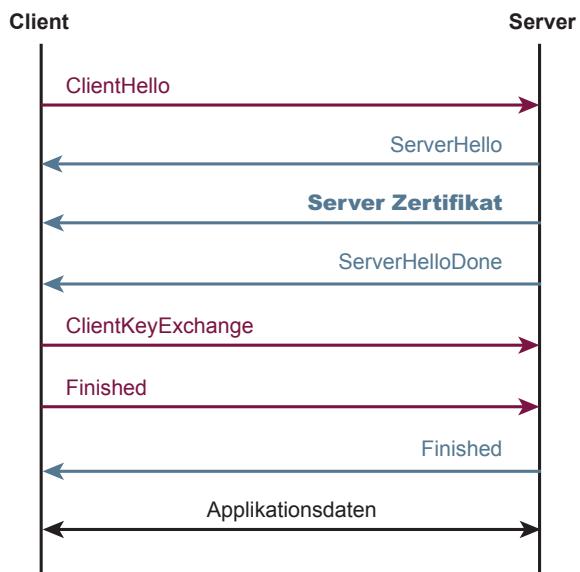
Hier kann sich ein Man-In-The-Middle in Richtung des Clients nun nicht mehr als falscher Server ausgeben, womit durch die Server-Authentifizierung aktive Angriffe verhindert werden.

### Server und Client authentifiziert

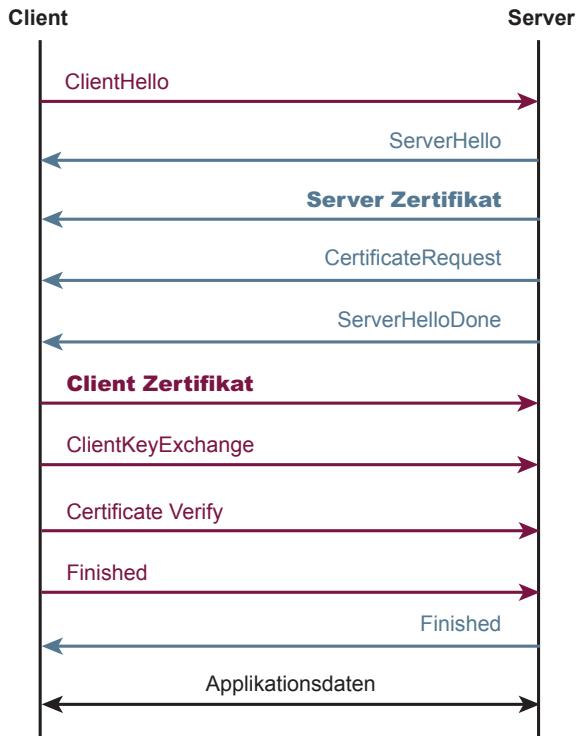
Der Server kann mit dem Nachrichten-Typ „CertificateRequest“ auch eine Client-Authentifikation über ein Zertifikat des Clients beantragen.

Dieser stellt das Zertifikat mit dem Nachrichten-Typ „ClientCertificate“ zu und beweist mit dem Nachrichten-Typ „CertificateVerify“, dass er auch tatsächlich jener ist, dessen Name im Zertifikat erscheint.

**Abb. 11.13** Server authentifiziert, Client anonym



**Abb. 11.14** Server und Client authentifiziert



Falls der Client kein Zertifikat besitzt, das in der vom Server bekannt gegebenen Liste auftaucht, wird der Verbindungsauflauf abgebrochen, siehe Abb. 11.14.

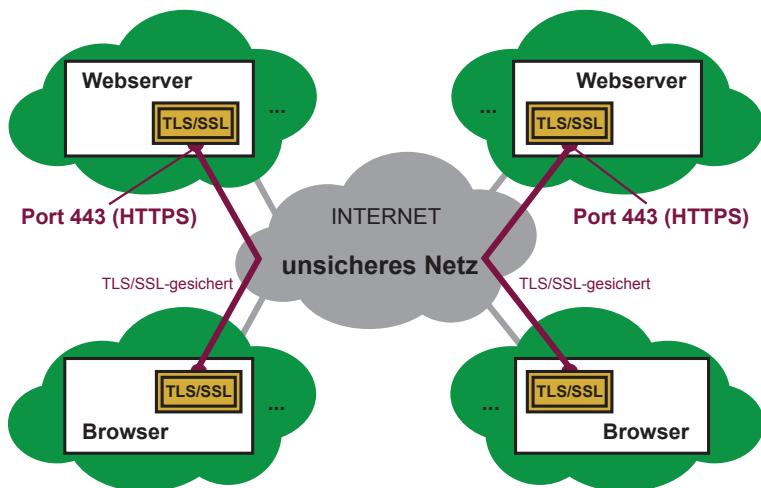
## 11.6 Anwendungsformen von TLS/SSL-Lösungen

In diesem Abschnitt werden einige Anwendungsformen von TLS/SSL-Lösungen exemplarisch beschrieben.

### Verschlüsselte und integritätsgesicherte Web-Kommunikation

Insbesondere bei der Web-Kommunikation werden oft sicherheitsrelevante Informationen wie Name, Passwörter, Bankdaten usw. über das Internet für die Eingabe von Web-Formularen übertragen. Bei dieser Anwendungsform nutzen die Web-Server und Browser die TLS/SSL-Sicherheitsfunktionen, um einen gesicherten Kanal einzurichten, siehe Abb. 11.15.

In der Regel wird der Server authentifiziert. Die Anwendung der TLS/SSL-Sicherheitsfunktionen wird durch das geschlossene Schloss in der Adresszeile des Browsers für den Nutzer angezeigt. Bei Extended Validation wird der Name des entsprechenden Unternehmens noch zusätzlich deutlich in der grünen Adresszeile angezeigt.



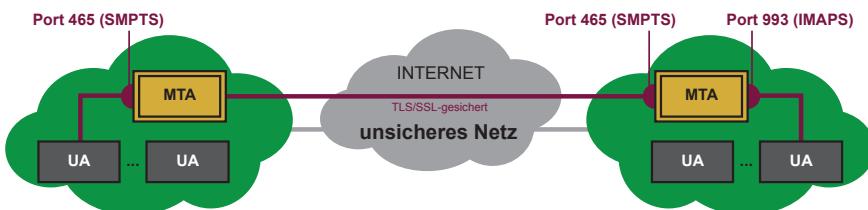
**Abb. 11.15** Verschlüsselte und integritätsgesicherte Web-Kommunikation

Durch die Verschlüsselung der Web-Kommunikation wird auch verhindert, dass ein Mitlesen der Kommunikationsdaten nicht dazu genutzt werden kann, was der Nutzer genau auf einer Webseite tut, beispielsweise welche Teile einer Parteien-Webseite sich ein Nutzer besonders genau ansieht.

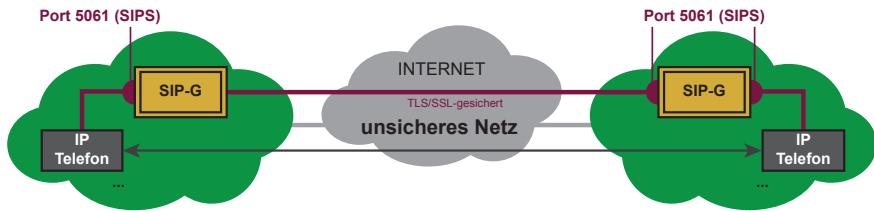
Webserver sind eShops, Social Media, Banken, Google usw. Browser sind auf PCs, Notebooks, Smartphone usw.

### Verschlüsselte und integritätsgesicherte Mail-Kommunikation

Bei dieser Anwendungsform werden die TLS/SSL-Sicherheitsfunktionen für die verschlüsselte und integritätsgesicherte Mail-Kommunikation verwendet. Wenn die Nutzer ihrer E-Mail an den Mail-Server (Message Transfer Agent – MTA) senden oder die Mail-Server miteinander die E-Mail austauschen, wird vorher eine TLS/SSL-Verbindung auf Port 465 für SMTP aufgebaut und die E-Mail geschützt übertragen. Das Abholen der E-Mail wird dann mit dem Mail-Client (User Agent – UA) über Port 993 für IMAP für eine gesicherte Kommunikation umgesetzt, siehe Abb. 11.16.



**Abb. 11.16** Verschlüsselte und integritätsgesicherte E-Mail-Kommunikation



**Abb. 11.17** Verschlüsselte und integritätsgesicherte SIP-Kommunikation

Wichtig bei einer Einschätzung des Risikos ist, dass die E-Mails auf dem MTAs im Klartext liegen.

### Verschlüsselte und integritätsgesicherte SIP-Kommunikation

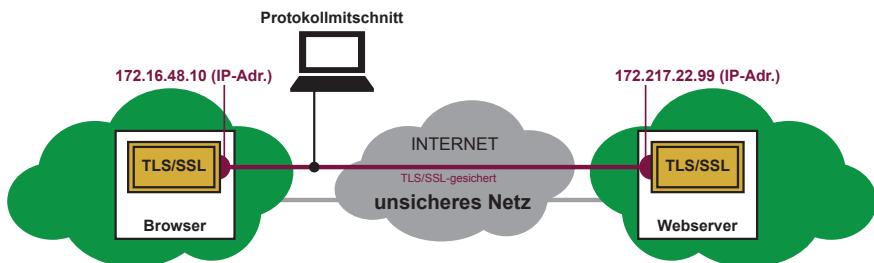
Bei der SIP Anwendungsform werden die TLS/SSL-Sicherheitsfunktionen für die verschlüsselte und integritätsgesicherte SIP-Kommunikation verwendet. Wenn die Nutzer mit ihrem Smart Telefon (IP-Telefon) die IP-Telefonie initialisieren oder die SIP-Gateways (Session Initiation Protocol Gateway – SIP-G) miteinander die SIP-Nachrichten austauschen, wird vorher eine TLS/SSL-Verbindung auf Port 5061 für SIP aufgebaut und die SIP-Nachrichten geschützt übertragen, siehe Abb. 11.17.

---

## 11.7 Protokollmitschnitt

In diesem Abschnitt wird ein Protokollmitschnitt beschrieben, der aufzeigen soll, wie das TLS/SSL-Protokoll real umgesetzt sein kann.

In Abb. 11.18 greift ein IT-System mit der IP-Adresse 172.16.48.10 mit einem Browser auf einen Webserver mit der IP-Adresse 172.217.22.99 zu.



**Abb. 11.18** Verschlüsselte und integritätsgesicherte TLS/SSL-Kommunikation

## Protokollmitschnitt

### TCP-Verbindungsauflaufbau

```
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0  C >>> S
Internet Protocol Version 4, Src: 172.16.48.10 (172.16.48.10), Dst: 172.217.22.99 (172.217.22.99)
Transmission Control Protocol, Src Port: 36102 (36102), Dst Port: https (443), Seq: 0, Len: 0
Flags: 0x002 (SYN)

Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0  C <<< S
Internet Protocol Version 4, Src: 172.217.22.99 (172.217.22.99), Dst: 172.16.48.10 (172.16.48.10)
Transmission Control Protocol, Src Port: https (443), Dst Port: 36102 (36102), Seq: 0, Ack: 1, Len: 0
Flags: 0x012 (SYN, ACK)

Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0  C >>> S
Internet Protocol Version 4, Src: 172.16.48.10 (172.16.48.10), Dst: 172.217.22.99 (172.217.22.99)
Transmission Control Protocol, Src Port: 36102 (36102), Dst Port: https (443), Seq: 1, Ack: 1, Len: 0
Flags: 0x010 (ACK)
```

### Aushandlung der Sicherheitsparameter, Serverauthentifizierung und Schlüsselaustausch

```
Frame 4: 236 bytes on wire (1888 bits), 236 bytes captured (1888 bits) on interface 0  C >>> S
Internet Protocol Version 4, Src: 172.16.48.10 (172.16.48.10), Dst: 172.217.22.99 (172.217.22.99)
Transmission Control Protocol, Src Port: 36102 (36102), Dst Port: https (443), Seq: 1, Ack: 1, Len: 170
Flags: 0x018 (PSH, ACK)
```

### Secure Sockets Layer

TLSSv1.2 Record Layer: Handshake Protocol: Client Hello

**Handshake Protocol: Client Hello**

Random

gmt\_unix\_time: Jan 23, 2025 15:01:26.000000000 CET

random\_bytes: 3f823c9ec03c535a245b6a5e78212356556bcf188d4b3a9f...

Session ID Length: 0

**Cipher Suites (11 suites)**

Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02b)

```

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)

Compression Methods Length: 1
Compression Methods (1 method)
  Compression Method: null (0)
  ...

```

### **TCP- Bestätigung für Frame 4**

```

Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528
bits) on interface 0  C <<< S
Internet Protocol Version 4, Src: 172.217.22.99 (172.217.22.99),
Dst: 172.16.48.10 (172.16.48.10)
Transmission Control Protocol, Src Port: https (443), Dst Port:
36102 (36102), Seq: 1, Ack: 171, Len: 0
  Flags: 0x010 (ACK)

```

```

Frame 6: 2780 bytes on wire (22240 bits), 2780 bytes captured (22240
bits) on interface 0  C <<< S
Internet Protocol Version 4, Src: 172.217.22.99 (172.217.22.99), Dst:
172.16.48.10 (172.16.48.10)
Transmission Control Protocol, Src Port: https (443), Dst Port: 36102
(36102), Seq: 1, Ack: 171, Len: 2714
  Flags: 0x018 (PSH, ACK)

```

### **Secure Sockets Layer**

```

TLSv1.2 Record Layer: Handshake Protocol: Server Hello
  Handshake Protocol: Server Hello
    Random
      gmt_unix_time: Aug 28, 2018 11:12:01.000000000 CEST
      random_bytes: 32b5bbb6291f31b56d071ceaeel4e1e7be0863ac6c7c3a06...
    Session ID Length: 0
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
    Compression Method: null (0)
    Extensions Length: 24
    Extension: renegotiation_info
      Type: renegotiation_info (0xff01)
      Length: 1
      Renegotiation Info extension
        Renegotiation info extension length: 0
        ...

```

```
TLSSv1.2 Record Layer: Handshake Protocol: Certificate
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 2289
Handshake Protocol: Certificate
Certificates Length: 2282
Certificates (2282 bytes)
    Certificate Length: 1156
    Certificate (id-at-commonName=www.google.de,id-at-organizationName=Google LLC,id-at-localityName=Mountain View,id-at-stateOrProvinceName=California,id-at-countryName=US)
        signedCertificate
version: v3 (2)
serialNumber: 25340433
signature (sha256WithRSAEncryption)
    Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
issuer: rdnSequence (0)
    rdnSequence: 3 items (id-at-commonName=Google Internet Authority G3,id-at-organizationName=Google Trust Services,id-at-countryName=US)
...
TLSSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 333
Handshake Protocol: Server Key Exchange
    Handshake Type: Server Key Exchange (12)
    Length: 329
    EC Diffie-Hellman Server Params
        curve_type: named_curve (0x03)
        named_curve: secp256r1 (0x0017)
        Pubkey Length: 65
        pubkey: 04fa540dea1e37e332080d8d9ecafec2764a50ecb689b78d...
        Signature Hash Algorithm: 0x0401
            Signature Hash Algorithm Hash: SHA256 (4)
            Signature Hash Algorithm Signature: RSA (1)
            Signature Length: 256
            signature: 14ed6843402163b44f1d5699c329732ad3856c43b4792361...
TLSSv1.2 Record Layer: Handshake Protocol: Server Hello Done
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 4
Handshake Protocol: Server Hello Done
    Handshake Type: Server Hello Done (14)
    Length: 0
```

### **TCP- Bestätigung für Frame 6**

```
Frame 7: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0  C >>> S
Internet Protocol Version 4, Src: 172.16.48.10 (172.16.48.10), Dst: 172.217.22.99 (172.217.22.99)
Transmission Control Protocol, Src Port: 36102 (36102), Dst Port: https (443), Seq: 171, Ack: 2715, Len0
Flags: 0x010 (ACK)
```

### **Schlüsselaustausch, CCS, ...**

```
Frame 8: 192 bytes on wire (1536 bits), 192 bytes captured (1536 bits) on interface 0  C >>> S
Internet Protocol Version 4, Src: 172.16.48.10 (172.16.48.10), Dst: 172.217.22.99 (172.217.22.99)
Transmission Control Protocol, Src Port: 36102 (36102), Dst Port: https (443), Seq: 171, Ack: 2715, Len: 126
Flags: 0x018 (PSH, ACK)
```

### **Secure Sockets Layer**

```
TLStv1.2 Record Layer: Handshake Protocol: Client Key Exchange
Handshake Protocol: Client Key Exchange
    Handshake Type: Client Key Exchange (16)
    Length: 66
    EC Diffie-Hellman Client Params
        Pubkey Length: 65
        pubkey: 0418395fd6c8855b0e43de39ad413466f3a4c513e8e58c2e...
TLStv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    Content Type: Change Cipher Spec (20)
    Version: TLS 1.2 (0x0303)
    Length: 1
    Change Cipher Spec Message
TLStv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 40
    Handshake Protocol: Hello Request
        Handshake Type: Hello Request (0)
        Length: 0
    Handshake Protocol: Hello Request
        Handshake Type: Hello Request (0)
        Length: 0
```

**CCS, ...**

**Frame 9:** 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits) on interface 0 C <<< S  
Internet Protocol Version 4, Src: 172.217.22.99 (172.217.22.99), Dst: 172.16.48.10 (172.16.48.10)  
Transmission Control Protocol, Src Port: https (443), Dst Port: 36102 (36102), Seq: 2715, Ack: 297, Len: 279  
Flags: 0x018 (PSH, ACK)

**Secure Sockets Layer**

**TLSv1.2 Record Layer: Handshake Protocol: New Session Ticket**  
**Handshake Protocol: New Session Ticket**  
Handshake Type: New Session Ticket (4)  
Length: 219  
TLS Session Ticket  
Session Ticket Lifetime Hint: 100800  
Session Ticket Length: 213  
**Session Ticket:** 00f7fe033d2ec55ea45919d7b87195bf3247ae08e9462ea...  
**TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec**  
Content Type: Change Cipher Spec (20)  
Version: TLS 1.2 (0x0303)  
Length: 1  
Change Cipher Spec Message  
**TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages**  
Content Type: Handshake (22)  
Version: TLS 1.2 (0x0303)  
Length: 40  
Handshake Protocol: Hello Request  
Handshake Type: Hello Request (0)  
Length: 0  
Handshake Protocol: Hello Request  
Handshake Type: Hello Request (0)  
Length: 0

**Verschlüsselte und integritätsgesicherte Datenübertragung**

**Frame 10:** 229 bytes on wire (1832 bits), 229 bytes captured (1832 bits) on interface 0 C >>> S  
Internet Protocol Version 4, Src: 172.16.48.10 (172.16.48.10), Dst: 172.217.22.99 (172.217.22.99)  
Transmission Control Protocol, Src Port: 36102 (36102), Dst Port: https (443), Seq: 297, Ack: 2994, Len: 163

**Secure Sockets Layer**

**TLSv1.2 Record Layer: Application Data Protocol: http**  
Content Type: Application Data (23)  
Version: TLS 1.2 (0x0303)

Length: 158  
**Encrypted Application Data:** 00000000000000019758b52e6af38f29-2ada9eafc118770...

**Frame 11:** 454 bytes on wire (3632 bits), 454 bytes captured (3632 bits) on interface 0   **C >> S**  
Internet Protocol Version 4, Src: 172.16.48.10 (172.16.48.10), Dst: 172.217.22.99 (172.217.22.99)  
Transmission Control Protocol, Src Port: 36102 (36102), Dst Port: https (443), Seq: 460, Ack: 2994, Len: 388

### Secure Sockets Layer

**TLSv1.2 Record Layer: Application Data Protocol: http**  
Content Type: Application Data (23)  
Version: TLS 1.2 (0x0303)  
Length: 383  
**Encrypted Application Data:** 00000000000000025d9a6a016536db15-bbcfa2b4e37eb1a3...

**Frame 12:** 135 bytes on wire (1080 bits), 135 bytes captured (1080 bits) on interface 0   **C << S**  
Internet Protocol Version 4, Src: 172.217.22.99 (172.217.22.99), Dst: 172.16.48.10 (172.16.48.10)  
Transmission Control Protocol, Src Port: https (443), Dst Port: 36102 (36102), Seq: 2994, Ack: 460, Len: 69

### Secure Sockets Layer

**TLSv1.2 Record Layer: Application Data Protocol: http**  
Content Type: Application Data (23)  
Version: TLS 1.2 (0x0303)  
Length: 64  
**Encrypted Application Data:** 000000000000000131f990c1519fe80b83a-b43a6ec15eb65...

**Frame 13:** 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface 0   **C << S**  
Internet Protocol Version 4, Src: 172.217.22.99 (172.217.22.99), Dst: 172.16.48.10 (172.16.48.10)  
Transmission Control Protocol, Src Port: https (443), Dst Port: 36102 (36102), Seq: 3063, Ack: 460, Len: 38

### Secure Sockets Layer

**TLSv1.2 Record Layer: Application Data Protocol: http**  
Content Type: Application Data (23)  
Version: TLS 1.2 (0x0303)  
Length: 33  
**Encrypted Application Data:** 000000000000000211199f018207c91-8fd98d8e0a3e7a5ca...

## 11.8 Zusammenfassung

TLS (Transport Layer Security)/SSL (Secure Socket Layer) ist ein anwendungsunabhängiges Cyber-Sicherheitsprotokoll, das logisch auf einem Transportprotokoll aufsetzt. Mithilfe von weiteren definierten Port-Nummern werden die Anwendungsprotokolle für die TLS/SSL-gesicherte Kommunikation adressiert.

Es werden die Cyber-Sicherheitsdienste: Authentifizierung, Verschlüsselung und Integritätsüberprüfung angeboten.

---

## 11.9 Übungsaufgaben

### Übungsaufgabe 1

Bitte kreuzen Sie Ihre Antworten an!

	Cyber-Sicherheitsmechanismen
	TLS/SSL
Gewährleistung von Cyber-Sicherheitsbedürfnissen	Vertraulichkeit
	Authentifikation
	Authentizität
	Integrität
	Verbindlichkeit
	Verfügbarkeit
	Anonymisierung/ Pseudonymisierung
Cyber-Sicherheitsstrategien	Vermeiden von Angriffen
	Entgegenwirken von Angriffen
	Erkennen von Angriffen

### Übungsaufgabe 2

Erläutern Sie die Aufgaben der TLS/SSL-Protokolle „Record Layer“, „Application Data“, „ChangeCipherSpec“, „Alert“ und „Handshake“.

### Übungsaufgabe 3

Beschreiben Sie kurz die vier Phasen des Verbindungsaufbaues bei TLS/SSL.

### Übungsaufgabe 4

Welche Vorteile ergeben sich aus Sicht eines Anwendungsentwicklers durch die Lage von TLS/SSL im ISO/OSI-Referenzmodell?

### Übungsaufgabe 5

Welche Voraussetzungen muss ein Webbrower zum erfolgreichen Aufbau einer TLS/SSL-Verschlüsselung erfüllen, in Bezug auf...

1. das Zertifikat des Servers,
2. die Art der Verschlüsselung (CipherSuite),
3. den internen persistenten Schlüsselspeicher.

### Übungsaufgabe 6

Bewerten Sie folgende Aussage: Wenn die Voraussetzungen an einen Webbrower für den erfolgreichen Aufbau einer TLS/SSL-Verschlüsselung erfüllt sind, dann sind ebenfalls die durch TLS/SSL ermöglichten Cyber-Sicherheitsbedürfnisse gewährleistet.

### Übungsaufgabe 7

1. Nennen Sie drei Arten von Zertifikaten in Bezug auf die Validierung!
2. Worauf beruht architekturbedingt das gesamte Vertrauen bei TLS/SSL-Verbindungen?
3. Wer initiiert klassischerweise eine TLS/SSL-Verbindung?

### Übungsaufgabe 8

Sie können auswählen, welche der beiden folgenden Typen Sie bei Ihrer Chiper Suite im Browser anbieten sollen:

- Typ 1: TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- Typ 2: TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

Welchen Typ würden Sie wählen und warum?

Ergebnisse siehe: <https://norbert-pohlmann.com/cyber-sicherheit/uebungen/>.

---

## Literatur

1. Campo Ma, Pohlmann N (2003) Virtual Private Network (VPN). MITP-Verlag, Bonn



# Cyber-Sicherheitsmaßnahmen gegen DDoS-Angriffe

12

Die Gewährleistung der Verfügbarkeit von IT-Systemen ist ein wichtiges Cyber-Sicherheitsbedürfnis, um Informationen und Dienste immer nutzen zu können.

In diesem Kapitel werden DDoS-Angriffe, Ziele von DDoS-Angriffsmethoden und hilfreiche Cyber-Sicherheitsmaßnahmen gegen DDoS-Angriffe beschrieben.

---

## 12.1 Einleitung

Die Abkürzung DDoS steht für Distributed Denial of Service. Das sind in der Regel Angriffe von Internet-Aktivisten und/oder kompromittierten IT-Systemen, die von Angreifern dazu genutzt werden, ausgesuchte Ziel-IT-Systeme koordiniert mit einer großen Last spezieller Anfragen durch Erschöpfung der verfügbaren Ressourcen (CPU, RAM, Bandbreite, ...) lahmzulegen. Es gibt Botnetze mit sehr vielen Bots (kompromittierten IT-Systemen mit Malware): 1000, 10.000, 100.000 oder sogar 1.000.000. Wenn ein Angreifer 100.000 Bots nutzen kann, jeder Bot 100 KBit/s upstream hätte (also nur ein Bruchteil der verfügbaren Bandbreite), dann könnte der Angreifer mit 10 G Bit einen DDoS Angriff durchführen. Bei 500.000 Bots und 200 KBit/s Bandbreite hätte der Angreifer 100 GBit/s zur Verfügung [1]. Botnetze sind schon länger als Bedrohung auch auf die Verfügbarkeit von Diensten im Internet bekannt. IoT-Botnetze stellen eine neue Stufe der Gefahr für die Infrastruktur des Internets dar [2]. Im Unterschied zu konventionellen Botnetzen bestehen IoT-Botnetze hauptsächlich aus kompromittierten IoT-Geräten. Die IoT-Geräte haben die Eigenschaft, dauerhaft und mit guter Bandbreite und nicht unter der direkten Kontrolle des Nutzers online verfügbar zu sein. Dadurch stehen die IoT-Geräte, einmal unter der Kontrolle eines Angreifers, immer für einen Angriff mit einer hohen verfügbaren Bandbreite bereit.

Welches Gefahrenpotenzial die Masse an ungesicherten IoT-Geräten mit sich bringt, zeigten die massiven DDoS-Angriffe des Mirai Botnetzes. Das Botnetz Mirai bestand aus mehr als einer Million kompromittierter IoT-Geräte. Die Intensität der DDoS-Angriffe erreichte eine bis dahin nicht dagewesene Dimension, mit einem durch die Anfragen erzeugten Traffic von 665 Gigabit bis zu 1,5 Terabit pro Sekunde. Die Menge der kompromittierten IoT-Geräte bestand hauptsächlich aus ungesicherten, mit dem Internet verbundenen Sicherheitskameras, digitalen Videorekordern und Haushaltsgeräten. Die Analyse des Quellcodes zeigte deutlich, mit welch simpler, auf menschlicher Schwäche basierender Strategie die Malware agierte. Sie durchsuchte das Internet nach IoT-Geräten, testete, ob diese noch auf das Default-Passwort des Herstellers konfiguriert waren, und brachte sie dann unter ihre Kontrolle. Gegenüber den üblichen Methoden wie „Social Engineering“ oder „E-Mail-Poisoning“ ermöglichte diese Herangehensweise eine enorme Senkung des Aufwands. Stattdessen können die meist schlecht gesicherten IoT-Geräte über die Ports 22 (SSH) oder 23 (Telnet) direkt angegriffen werden. Die ständige Verfügbarkeit der IoT-Geräte macht sie zu sehr attraktiven Bots. Basierend auf dem offenen Quellcode von Mirai entstanden viele Ableger des Botnetzes.

Solche Überlastungen sind schwierig zu kontrollieren und eine kontinuierlich wachsende Herausforderung. Heutzutage sollte sich jeder Verantwortliche einer IT-Infrastruktur mit den möglichen Cyber-Sicherheitsmaßnahmen auseinandersetzen, um im Angriffsfall vorbereitet zu sein, um so die verursachten Schäden im Rahmen halten zu können.

Durch die Nickerreichbarkeit der Internet-Dienste entstehen Umsatzeinbußen, SLA-Verletzung, Kundenabwanderung oder mögliche Reputationsschäden sowie oft hohe Schadsummen auf Seiten der Angegriffenen. Nicht nur „Big Player“ werden heutzutage regelmäßig Ziel solcher DDoS-Angriffe auf die Verfügbarkeit ihrer Internet-Dienste. Die finanziellen Schäden ziehen sich neben der IT- und Sicherheitsabteilung oft auch durch die Marketing-Abteilung, den Kundenservice und das Risiko-Management. Das macht DDoS-Angriffe natürlich insgeheim auch für Mitbewerber interessant. In erster Linie sind sie allerdings ein seit Jahren eingesetztes Mittel von Cyberkriminellen und Aktivisten. DDoS-Angriffe werden illegal und kriminell eingesetzt, um Firmen und Organisationen zu erpressen, gezielt hohen Geschäftsschaden zu verursachen oder um auf politische Ziele aufmerksam zu machen. Zu beliebten Zielen gehören ebenfalls Onlinespiele-Server, Onlinebanking-Portale, politische und ideologische Webseiten, Nachrichtenportale, VoIP-Dienstleister und viele mehr. Technisch wenig bewanderte Kriminelle können solche Angriffe für ihre Zwecke bei „Stresstest“-Dienstleistern und in einschlägigen Portalen einkaufen. Über die vergangenen Jahre haben sich DDoS-Angriffsmethoden zudem weiterentwickelt. Angriffe haben heutzutage ein deutlich höheres Datenvolumen oder zielen sogar auf bestimmte Schwachstellen

in Anwendungen. Um eine adäquate Abwehrstrategie aufstellen zu können, sind verschiedene Cyber-Sicherheitsmaßnahmen zu beachten.

Solche oder ähnliche Angriffe finden in Deutschland jährlich mehrere 1.000 Mal statt. Viele zahlen das Geld, um die Verfügbarkeit sicherzustellen, andere tragen den Schaden der Nicht-Verfügbarkeit. Allen gemeinsam: Sie erleiden einen Schaden!

Relativ einfach und preiswert durchzuführende DDoS-Angriffe zielen vermehrt auf die Verfügbarkeit von Internet-Diensten. Das Risiko, Ziel eines Angriffs zu werden, wird häufig unterschätzt. Jedermann kann – je nach Intensität und Dauer – so einen Angriff ab etwa 50 € von cyberkriminellen Dienstleistern im Internet buchen. Die auf der anderen Seite entstehenden Schäden wiederum gehen schnell in die Millionen. Firewalls und IPS-Systeme liefern entgegen weitläufiger Meinung keinen ausreichenden Schutz gegen professionelle DDoS-Angriffe.

## 12.2 Gezielte Überlastung

Durch eine Kombination unterschiedlicher DDoS-Angriffsmethoden kann ein Angreifer unterschiedliche Teile eines Internet-Dienstes speziell überlasten sowie flexibel auf unzureichende Abwehrmaßnahmen und deren Schwachstellen reagieren, siehe Abb. 12.1.

Folgende Teile der Dienst-Architektur können Ziel von DDoS-Angriffsmethoden werden:

Die Kommunikationsanbindung – durch Überlastung der **verfügbaren Bandbreite**. Der Angreifer produziert so viele unsinnige Datenpakete, dass die Bandbreite nicht mehr ausreicht, um die gewünschten Datenpakete zum Server zu transportieren. Bei hoher Last wird die Quality of Service schlecht und bei extremer Last muss der Router die meisten Datenpakete verwerfen, weil die Warteschlangen voll sind. Dadurch sind die eigentliche Anwendung oder der Dienst nicht mehr nutzbar.

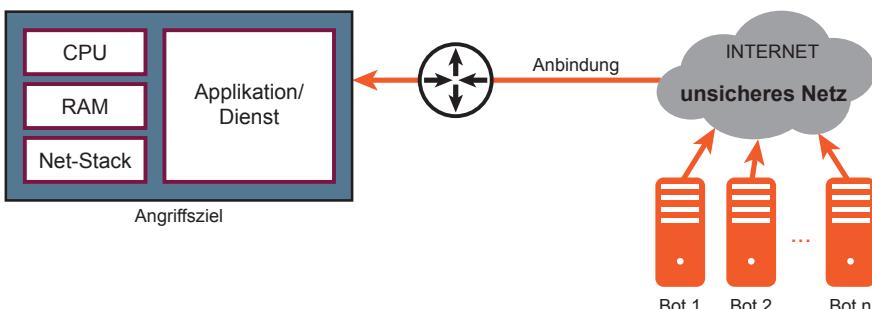


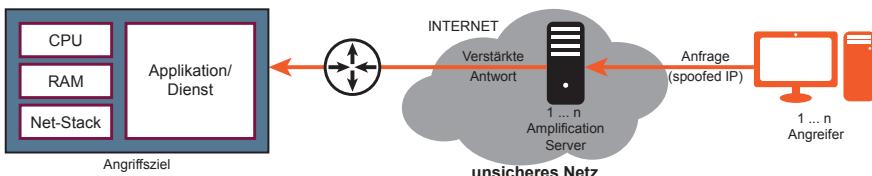
Abb. 12.1 Gezielte Überlastung

**Der Netzwerk-Stack:** Hier kann ein Crash oder ein Überlastungszustand durch Angreifer aufgrund von Fehlern in der Implementierung oder Eigenarten verschiedener Protokollfamilien, insbesondere auch bei eingesetzten Verschlüsselungsverfahren, hervorgerufen werden. Ebenfalls kann eine Auslastung des **RAM** durch sehr viele unvollständige Verbindungsanfragen eines Angreifers hervorgerufen werden, was die Verfügbarkeit eines Dienstes schnell stark einschränkt.

**Die Applikation:** Anwendungsspezifisch erzeugte Anfragen durch Angreifer, die auf Fehler oder wenig performant implementierte Teile einer **Anwendung** ziehen. Dazu gehören auch harmlos anmutende Funktionen wie Hashing und datenbankintensive Suchanfragen, die zum Beispiel die **CPU-Ressourcen** für reale, gewünschte Anfragen nicht mehr verfügbar machen. Diese Angriffe werden auch „Low and Slow“ genannt, wenn sich die für einen solchen Angriff benötigten Netzwerkpakete hinsichtlich Frequenz und Payload kaum oder gar nicht vom gewöhnlichen Datenverkehr unterscheiden lassen.

## 12.3 Reflection und Amplification

Ein DDoS-Trend der vergangenen Jahre sind Reflection- beziehungsweise Amplification-Angriffe, auch Distributed-Reflected-Denial-of-Service (DRDoS) genannt. Diese Angriffe machen sich in erster Linie fremde Server mit UDP-Netzwerkprotokollen zunutze, die ein relativ kleines Anfragepaket mit sehr großen Paketen beantworten. Die Reflection-Eigenschaft beruht auf IP-Spoofing, womit die Antwort an eine beliebige anzugreifende Ziel-IP gelenkt wird. Der Angreifer muss für so einen Angriff keine Kontrolle über den fremden Server gewinnen. Prominentester Vertreter solcher Angriffe ist der eigentlich veraltete NTP Monlist-Befehl. Dieser sendet als Antwort die Adressen der letzten 600 IT-Geräte, die sich mit dem NTP-Server verbunden haben. Daraus ergibt sich ein Verstärkungsfaktor von über 200, der das Protokoll damit sehr attraktiv für Angreifer macht. Das bedeutet, wenn der Angreifer 1 Byte zu einem Amplification Server sendet, schickt dieser 200 Byte an das Angriffsziel, siehe Abb. 12.2.



**Abb. 12.2** Prinzip eines Amplification-Angriffs

Viele weitere Protokolle sind anfällig für derartigen Missbrauch, darunter DNS, SNMP und sogar P2P-Protokolle verschiedener Botnetze. Ein anderes Beispiel für das Ausnutzen von Software für Amplification ist die Pingback-Funktion der bekannten CMS- beziehungsweise Blogging-Software Wordpress. Diese Funktion erlaubt es, Anfragen von einer Wordpress-Instanz zu anderen Webseiten zu schicken, um Querverweise zwischen Blogs zu generieren. Diese Funktion lässt sich einfach für Verfügbarkeitsangriffe missbrauchen, kann aber inzwischen mit Hilfe eines Plug-ins [3], das gezielt entsprechende Pingback-Funktionen im XML-RPC-Modul von Wordpress deaktiviert, verhindert werden. Ein Angreifer schickt hierbei Pingback-Requests mit der anzugreifenden Webseite als Ziel an beliebig viele Wordpress-Seiten. Diese kontaktieren daraufhin alle das anzugreifende IT-System. Als Nebeneffekt stehen dem Angreifer mit dieser Methode nahezu beliebig viele verschiedene Source-IP-Adressen für einen DRDoS-Angriff zur Verfügung, der in erster Linie auf eine Überlastung der verfügbaren Anbindung seitens des angegriffenen Dienstbetreibers zielt. Besonders kritisch wird ein derartiger Angriff, wenn ein Botnetz-Betreiber mehrere Amplification-Server von verschiedenen Teilen seines Botnetzes aus parallel ansteuert. Laut Akamai PLXsert Q4 2014 State of the Internet – Security Report liegt der Anteil von Reflection-Angriffen im Vergleich zu allen DDoS-Angriffen inzwischen bei etwa 40 %.

---

## 12.4 Abwehrstrategien gegen Angriffe auf die Verfügbarkeit

Auf einen DDoS-Angriff sollte jedes Unternehmen vorbereitet sein, dessen Geschäft von der Verfügbarkeit seiner Internet-Dienste abhängig ist. Aber auch alltäglicher Geschäftsbetrieb kann durch einen DDoS-Angriff stark beeinträchtigt werden, beispielsweise wenn ein VPN-Gateway beziehungsweise dessen Anbindung überlastet wird oder Mailserver nicht mehr erreichbar sind. Eine Abwehrstrategie eines Unternehmens gegen DDoS-Angriffe kann dabei aus drei grundlegenden Kategorien bestehen:

- Cyber-Sicherheitsrichtlinien zum Schutz vor Verfügbarkeitsangriffen
- On-Site-Robustheitsmaßnahmen
- Off-Site-Robustheitsmaßnahmen/Nutzung von Dienstleistern

### 12.4.1 Cyber-Sicherheitsrichtlinien zum Schutz vor Verfügbarkeitsangriffen

Als Teil der eigenen DDoS-Abwehrstrategie sollte zuallererst eine Risikoanalyse bezüglich der notwendigen Verfügbarkeit der eigenen Internet-Dienste durchgeführt werden. Durch eine Kalkulation von Risiko und Folgeschäden muss das vorhandene Budget für die Robustheitsmaßnahmen bestimmt werden. Dabei sollte die Eintrittswahrscheinlichkeit eines DDoS-Angriffes nicht, wie leider häufig der Fall, unterschätzt werden. Es folgt die eigentliche Strategie: Ein Ablaufplan

mit Richtlinien für die Vorgehensweise in einem akuten Angriffsfall muss aufgestellt werden. Spezielle Handlungsrollen für das IT-Personal, andere Geschäftsabteilungen und eingebundene Dienstleister müssen darin festgelegt sein. Im Anschluss an die Konzeptionierung sollte die Wirkung der Strategie mithilfe simulierter Angriffsszenarien getestet werden. Regelmäßiges Überprüfen und Testen der Abwehrstrategie ist ebenso wichtig. Es dient der Verifikation, ob die etablierten Robustheitsmaßnahmen zeitgemäßen Angriffen noch standhalten und sorgt dafür, dass das Personal im Falle eines Angriffs noch planmäßig handelt.

### **12.4.2 On-Site-Robustheitsmaßnahmen**

DDoS-Angriffen lässt sich kaum komplett entgegenwirken. Umso wichtiger ist es, ihnen möglichst mit unterschiedlichen Cyber-Sicherheitsmaßnahmen zu begegnen. Das fängt bereits beim Basisschutz der eigenen Infrastruktur an.

#### **Aufrüsten der Ressourcen**

Zunächst mag es sinnvoll erscheinen, diejenigen Ressourcen aufzustocken, die durch einen DDoS-Angriff überlastet werden könnten. Dafür kommen mehr Anbindungsbandbreite und leistungsstärkere Server (CPU, RAM, ...) infrage. Die Kapazitäten eines gezielten Angriffs übersteigen jedoch mit Leichtigkeit den Schutz durch jede sinnvolle Ressourcenaufrüstung innerhalb von kurzer Zeit. Derartige Cyber-Sicherheitsmaßnahmen haben einen schlechten Kosten-Nutzen-Effekt, da die erhebliche Mehrkapazität nur im Angriffsfall wirklich benötigt wird und dann selten ausreicht. Ein wirksamer Schutz muss bereits vor der Infrastruktur ansetzen.

#### **Sofortmaßnahmen bei einem aktiven Angriff**

Findet bereits ein DDoS-Angriff statt, so können dessen Auswirkungen unter bestimmten Umständen eingedämmt werden. Da DDoS-Angriffe meist von vielen verschiedenen IPs ausgehen, kommt ein Whitelisting für besonders wichtige, zugriffsberechtigte Nutzer oder Kunden infrage. Bei umsatzkritischen Webdiensten hingegen, auf die viele Nutzer Zugriff haben, können eine Login-Wall, Captchas oder eine Überprüfung der Browser-Echtheit den Dienst auf Anwendungsebene schützen. Ist die Angriffsmethode von einfacher Natur und nicht besonders volumenintensiv, so kann eventuell das vorhandene Sicherheits-equipment passend konfiguriert werden, um entsprechenden Traffic zu blockieren. Wenn hingegen die globale Verfügbarkeit des jeweiligen Internet-Dienstes nicht essentiell ist, so besteht die Möglichkeit, kurzerhand bestimmte IP-Adressbereiche (Geolocation) zu blockieren, um die Traffic-Flut einzuschränken. Eine solche Sofortmaßnahme ist oft nicht ausreichend, da der Effekt sehr unterschiedlich wirken kann. Angreifer können heute sehr schnell ihre Taktik ändern, sowie die Angriffsressourcen problemlos schnell aufrüsten.

Ebenso wichtig wie das Einleiten technischer Gegenmaßnahmen ist der richtige Umgang mit der Öffentlichkeit. Schnell kommt es durch nicht verfügbare Internet-Dienste zu frustrierten Nutzern. Es empfiehlt sich, den Angriff und Erpressungsversuch öffentlich mitzuteilen, die Hintergründe zu erklären und das weitere Vorgehen im Sinne der Nutzer ausreichend transparent zu kommunizieren. Mit einer Erläuterung, dass der Ausfall durch kriminelle Akteure zustande kommt, und dass intensiv an einer schnellen Problemlösung gearbeitet wird, kann der Frust über den Ausfall auf den Angreifer gelenkt und somit ein Imageschaden abgeschwächt werden. Zwar erwarten die Kunden von wichtigen Internet-Diensten zunehmend eine Robustheit gegen solche Angriffe, als Hauptursache für den Ausfall wird in diesem Moment dennoch ein Angriff deutlich kommuniziert – und nicht die Inkompetenz der zuständigen IT-Abteilung.

### Anti-DDoS Appliance – Möglichkeiten und Grenzen

Ein schnell installierter Basisschutz gegen Verfügbarkeitsangriffe auf die eigenen Dienste sind DDoS-Appliances. Auch viele Next-Generation-Firewalls bieten inzwischen DDoS-Schutzfunktionen, siehe Abb. 12.3.

Eine mögliche Cyber-Sicherheitsmaßnahme ist die Nutzung einer Anti-DDoS-Appliance, mit deren Hilfe der eingehende Datenverkehr gefiltert wird. Mit einer Anti-DDoS-Appliance kann einigen Angriffsmustern im Rahmen der verfügbaren Anbindungsbandbreite entgegengewirkt werden. Solche Anti-DDoS-Appliances bieten, je nach Ausführung, neben Filterung von altbekannten DoS-Mustern inzwischen auch selbstlernende Filter gegen unbekannte Angriffe auf Applikations-Ebene, „Low and Slow“-Angriffe und Multivektor-Angriffe. Sie integrieren sich einfach in die bestehende Infrastruktur und helfen dabei, DDoS-Angriffe frühestmöglich zu erkennen und die Robustheit gegen DDoS-Angriffe zu erhöhen.

Übersteigt das Angriffsvolumen allerdings die verfügbare Bandbreite – und das ist bei der Nutzung von Amplification bei den meisten Angriffen der Fall, so kann die Anti-DDoS-Appliance kaum helfen. Die Leitung wird dann bereits am Router zur Infrastruktur „verstopft“. Zudem sind auch die implementierten Filtertechnologien oft nicht gegen alle Angriffe wirksam, insbesondere bei eingesetzter Verschlüsselung und Application-Angriffen. Eine schnelle Rundum-sorglos-Lösung sind diese Anti-DDoS-Appliances daher nicht. Zur Abwehr von Angriffen mit großem Datenvolumen sollte unbedingt die Zusammenarbeit mit einem externen Dienstleister für DDoS-Abwehr und Monitoring mit eingebunden werden. Dabei gibt es unterschiedliche Schutzmodelle für verschiedene Anwendungsfälle.

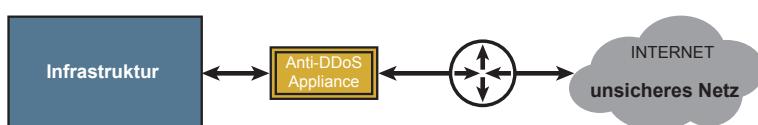
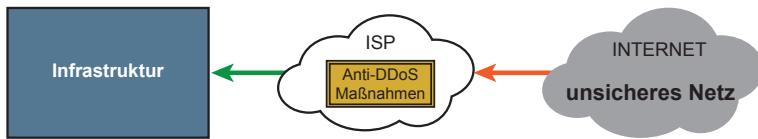


Abb. 12.3 Anti-DDoS-Appliance



**Abb. 12.4** Der ISP übernimmt DDoS-Filterung

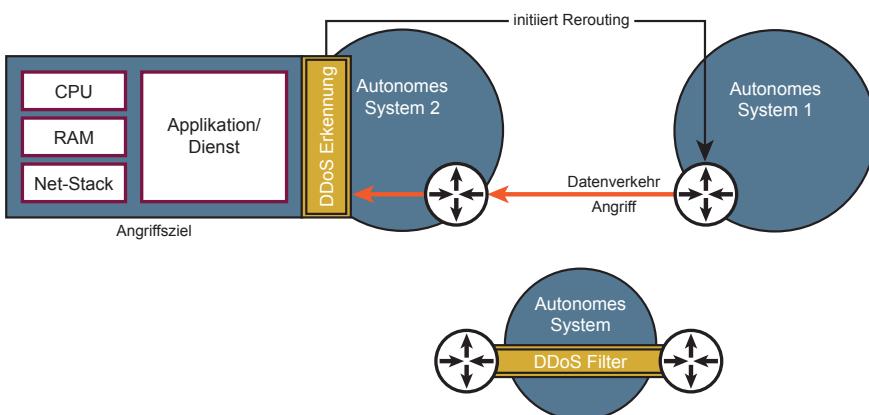
### 12.4.3 Off-Site-Dienstleistungsmodelle

Zuallererst sollte geklärt werden, ob der eigene Internet-Provider im Notfall bei einem Angriff unterstützend aktiv werden kann, beispielsweise durch eigene Filter beziehungsweise temporäre Blockade bestimmter Adressbereiche. Durch seine Ressourcen kann der Internet-Provider eventuell den nicht gewollten Angriffsdatenverkehr abfangen, bevor er das eigene Netz erreicht, siehe Abb. 12.4.

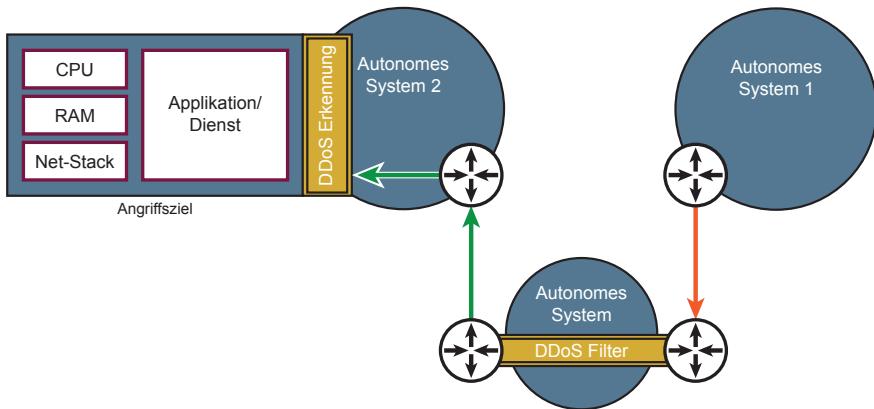
Aber nicht jeder Provider sieht sich in der Lage oder Verantwortung, bei einem DDoS-Angriff Maßnahmen zu ergreifen. In den meisten Fällen ist es deutlich wirkungsvoller, auf DDoS-Abwehr spezialisierte Dienstleister mit eigenen Filternetzwerken in Anspruch zu nehmen. Diese bieten eine Reihe von Schutzkonzepten mit verschiedenen Vor- und Nachteilen und Wirkungsgraden an.

#### Traffic-Scrubbing-Netze (Verkehrssäuberungs-Netze)

Robustheitsanbieter betreiben spezielle autonome Systeme, die sehr gut dabei helfen, DDoS-Traffic zu filtern. Bei dieser Methode ist die Infrastruktur speziell für die Filterung von DDoS-Angriffen konzipiert. Mithilfe dieser Abwehr-Technologie kann eine gesamte Infrastruktur mittels eines BGP-Rerouting-Mechanismus vor DDoS-Angriffen geschützt werden. Source- und Destination-IP der Kommunikation bleiben dabei unverändert, die Umleitung durch das Filternetz verursacht nur minimale Verzögerung. Alternativ steht meist eine DNS-Umleitung speziell für Webserver zur Verfügung. Der Schutzmechanismus: Die Filtertechnik steht bei einem DDoS-Angriff im Hot-Standby, siehe Abb. 12.5. Das bedeutet, dass nur in



**Abb. 12.5** Ein DDoS-Angriff wird im Hot-Standby durch das Modul „DDoS Erkennung“ identifiziert



**Abb. 12.6** Datenverkehr wird über ein spezielles AS umgeleitet, um nicht gewünschten Inhalt zu filtern

dem Fall, dass der DDoS-Erkennungsfilter einen Angriff feststellt, der Datenverkehr per Netz-Announcement über das Filternetz geroutet wird, siehe Abb. 12.6.

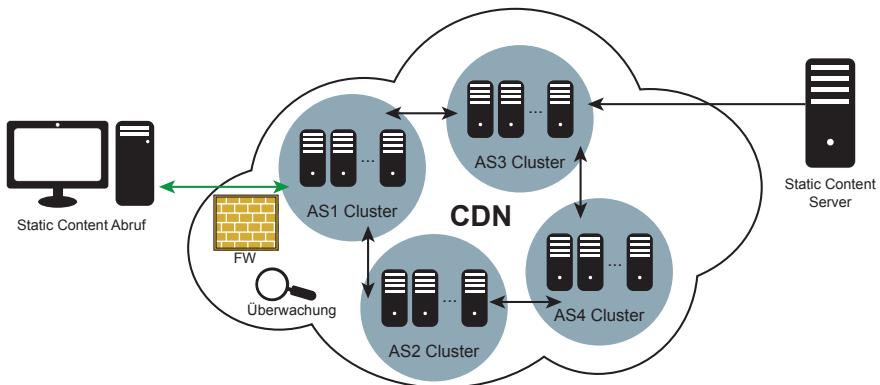
Für diese Cyber-Schutzmaßnahme ist mindestens ein eigenes/24 Subnetz erforderlich. Dienstleister verfügen über Rechenzentren mit 500-Gbps-Anbindung an verschiedene Carrier und setzen auf eine eigene intelligente DDoS-Filter-Technologie, die Angriffe erkennt und ausfiltert. Kriterium für die Filterung von DDoS-Verkehr ist neben bekannten Mustern ein Scoring-Modell. Wie in der Abb. 12.6 zu sehen ist, wird, wenn entsprechender Netzwerkverkehr zu stark von dem normalen Netzwerkverkehr abweicht, ein DDoS-Angriff erkannt und der Traffic geht über ein anders autonomes System und die DDoS-Pakete werden durch den DDoS-Filter aussortiert und nur die gewollten IP-Pakete gehen über das gewünschte autonome System 2 zur Anwendung. Durch die Nutzung eines weiteren autonomen Systems und sehr gute DDoS-Filter können auch sehr starke DDoS-Angriffe unwirksam gemacht werden.

### Content-Delivery-Network (CDN)

Ein CDN verteilt statische Inhalte redundant via Caching oder Replikation auf Servern, die an vielen verschiedenen Standorten in verschiedene autonome Systeme eingebunden sind, siehe Abb. 12.7.

Ein CDN bietet durch kombinierte Bandbreiten der autonomen Systeme große Robustheit bezüglich der Anbindung. Diese Inhalte können dann vom jeweils physikalisch nächstgelegenen oder am besten verfügbaren Servercluster mit einer guten Antwortzeit ausgeliefert werden.

Der Cyber-Schutzmechanismus: Befindet sich ein Server unter einem DDoS-Angriff, so kann ein anderer Server oder Cluster für die Auslieferung der

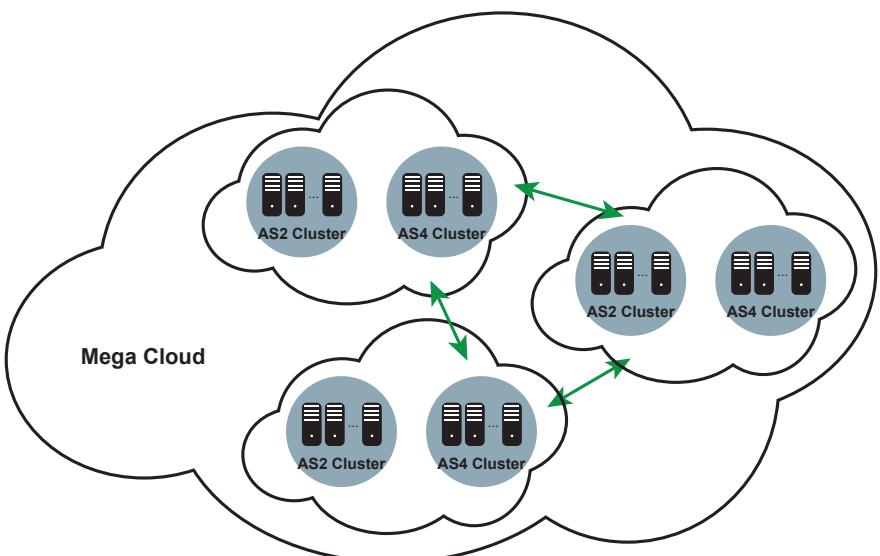


**Abb. 12.7** Content-Abruf in einem CDN mit Clustern in verschiedenen autonomen Systemen

Inhalte einspringen. Ein Angreifer müsste also seinen Angriff in mehrere autonome Systeme lenken. Dynamische Inhalte sind nicht cachebar. Daher kommt ein CDN als Cyber-Schutzmaßnahme hier weniger in Frage. Auch sonst bietet es keine gesonderte Cyber-Schutzfunktion gegen DDoS-Angriffe. Sinnvoller für Angreifer ist es, die Server der dynamischen Inhalte anzugreifen, welche die statischen Inhalte ausliefern.

### Mega-Cloud

Eine weitere Lösung ist eine Mega-Cloud, siehe Abb. 12.8. Hier können Anwendungen, Datenbanken, Webseiten und Inhalte direkt in einer gesicherten Cloud abgelegt werden.



**Abb. 12.8** Mega-Cloud mit hoher Redundanz an Ressourcen an vielen verteilten Standorten

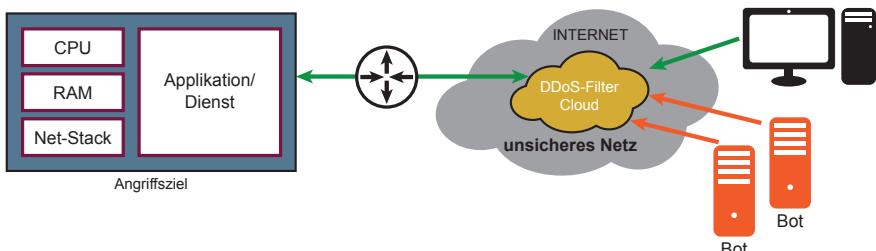
Der Cyber-Schutzmechanismus: Die Cloud-Umgebung bietet viele redundante Ressourcen in einer weltweit verteilten Umgebung. Durch hohe Anbindungs-Bandbreiten kombiniert mit Skalierbarkeit und Replikation können hier Webservices mit umfangreichen Cyber-Sicherheitsfeatures geschützt zur Verfügung gestellt werden. Nachteil: Ein Umzug in die Cloud kann viel Aufwand bedeuten und nicht für alle Teile der eigenen Infrastruktur in Frage kommen, insbesondere in Bezug auf hochsensible Daten.

### Cloud-Filter – redundante Kapazitäten mit Filtertechnologie

Dienstleister von Cloud-Filternetzen vereinen alle bisher vorgestellten Konzepte in einer Lösung. Sie bieten unterschiedliche Schutzstufen für Webserver und Infrastrukturen. Die Anbieter agieren hier als Reverse-Proxy über einem weltweiten Content Delivery Network (CDN) mit DNS-Servern, Caching, Blocklisten, BGP Origin Protection, Web-Application-Firewall (WAF), Malware-Scanner, Spam-Schutz und in Bezug auf Schutz vor DDoS-Angriffen verschiedenen modernen Cyber-Schutzmechanismen. Durch die Redundanz in verschiedenen Autonomen Systemen, stetige Weiterentwicklung der Cyber-Schutztechnologien und rundum großzügig dimensionierte Kapazitäten erreichen diese Cloud-Filternetze einen starken Schutz mit vielen einfach nutzbaren Zusatzleistungen zum Schutz von Webanwendungen, siehe Abb. 12.9.

Die Preise liegen je nach Schutzbedarf, SLA und Support zwischen einem kostenlosen Basis-Schutz und über 5.000 US-Dollar monatlich. Die eigenen Server werden hierbei von der Cloud-Infrastruktur vor Angriffen abgeschirmt. Dafür muss der Dienstleister lediglich als verantwortlicher Nameserver der eigenen Domain(s) eingetragen werden. Die übrige Konfiguration findet dann über die Webseite des Anbieters statt. Einfachheit und Flexibilität bei der Auswahl der verschiedenen Angebote macht diese Lösung für kleine und größere Unternehmen besonders attraktiv. Webseiten können mit wenig Aufwand und geringem Budget effektiv geschützt werden.

Trotz aller Cyber-Sicherheitsmaßnahmen gibt es heutzutage bereits einzelne Angriffsswellen, bei denen sogar die Bandbreiten-Kapazitäten solcher Anbieter überschritten werden und die somit zur Beeinträchtigung des Betriebs führen. Beispiele von DDoS-Angriffen mit mehr als 1,5 Terabit pro Sekunde verdeutlichen



**Abb. 12.9** Schutz durch die Cloud

diese Situation. Bei gezielten Multivektor-Angriffen („hybriden“ Angriffen) ist es einem eigenständigen Filtersystem zudem meist nicht möglich, alle Arten von „Low and Slow“-Angriffen zu erkennen und zu unterbinden.

---

## 12.5 Präventiv gegen Beteiligung – Sichere Konfiguration von Diensten

Schlecht konfigurierte IT-Endgeräte und Server sind ein großes Problem bei DDoS-Angriffen, da diese Botnetze und Amplification-Angriffe ermöglichen. Admins sollten verhindern, dass das eigene Netzwerk an DDoS-Angriffen teilnimmt. Die eigenen öffentlich erreichbaren Server müssen auf Missbrauchspotential für Amplification-Angriffe geprüft werden. Eine wichtige Cyber-Sicherheitsmaßnahme ist beispielsweise das Abschalten von offener Rekursion auf DNS-Servern. Es sollten nur rekursive DNS-Anfragen aus vertrauenswürdigen Quellen zugelassen werden. NTP-Server laufen häufig auf älteren Servern, denen oft keine große Beachtung mehr geschenkt wird. Dabei sollten gerade diese unbedingt auf den aktuellen Stand gebracht werden. Grundlegende Cyber-Sicherheitsmaßnahmen wie Awareness-Kampagnen und Endpoint-Protection dämmen das Infektionsrisiko für Botnetz-Malware weiter ein. Zusätzlich sollte IP-Spoofing mittels Egress-Filtering (Ausgangsfilterung) unterbunden werden.

---

## 12.6 Zusammenfassung

Mit dem Internet-of-Everything kommt – mit Zombie-Armeen aus vielen schlecht gesicherten Embedded-Devices – ein zusätzlicher Schwung von erfolgreichen DDoS-Angriffen. Die Angriffe kommen schnell und meist unvorhergesehen. Verantwortliche in Firmen und Organisationen, deren Umsatz und Geschäftsbetrieb von Internet-Diensten abhängig ist, sollten sich um Robustheitsmaßnahmen mit passender Abwehrstrategie bei DDoS-Angriffen kümmern.

Unzureichende Wirkung	Beschreibung
	Hundertprozentigen Schutz vor DDoS-Angriffen gibt es ebenso wenig wie absolute Cyber-Sicherheit. Ziel von Cyber-Sicherheitsmaßnahmen gegen DDoS-Angriffe ist immer, das Schutzniveau und somit die Hürden für Angreifer möglichst hoch zu setzen

## 12.7 Übungsaufgaben

### Übungsaufgabe 1

Was ist das Problem bei der Erhöhung der Ressourcen von IT-Systemen und deren Internet-Anbindung gegen Angriffe auf die Verfügbarkeit?

### Übungsaufgabe 2

Nennen Sie den prinzipiellen Unterschied der Möglichkeiten von On-Site- und Off-Site-Robustheitsmaßnahmen?

### Übungsaufgabe 3

Sie wurden von Ihrem Unternehmen damit beauftragt, die Resistenz der Netzwerkinfrastruktur vor Cyber-Angriffen aus dem Internet zu überprüfen. Nennen und beschreiben Sie bereits dokumentierte Vorgehensweisen von Cyber-Kriminellen für die Durchführung von DDoS-Angriffen im Internet!

### Übungsaufgabe 4

Welche Eigenschaften der Netzwerkinfrastruktur (Hard- und Software) sollten bei der Überprüfung berücksichtigt werden, um Rückschlüsse auf mögliche Schwachstellen für zukünftige DDoS-Angriffe zu ziehen?

### Übungsaufgabe 5

Nennen und beschreiben Sie mögliche Probleme bei der Erkennung von DDoS-Angriffen auf Schicht 7 des ISO/OSI-Referenzmodells!

Ergebnisse siehe: <https://norbert-pohlmann.com/cyber-sicherheit/uebungen/>.

---

## Literatur

1. Fritzen R, Pohlmann N (2015) Von überall her – Internetdienste vor DDoS-Angriffen schützen, iX Mag Prof Informationstech 2015(9):87–91
2. Hoang J, Jötten O, Pohlmann N, Wojzechowski C (2017) Internet of Things (IoT) – Herausforderung für die IT-Sicherheit. IT-Sicherh Fachmag Informationssicherh Compliance 2017(3):44–49
3. Aguilera S. <https://wordpress.org/plugins/disable-xml-rpc-pingback/>. Stand: 22.11.2018



Die E-Mail-Anwendung ist eine der wichtigsten Kommunikationsmöglichkeiten, insbesondere im Business-Bereich. Aus diesem Grund wird in diesem Kapitel das Thema E-Mail-Sicherheit behandelt und es werden die verschiedenen Cyber-Sicherheitskonzepte und Möglichkeiten diskutiert.

---

## 13.1 Einleitung

Der E-Mail-Dienst ist eine elastische Anwendung, in der diskrete Medien, die zeitunabhängig sind, wie Text und Grafik, ausgetauscht werden. Der E-Mail-Dienst ist einer der am weitest verbreiteten und meist genutzten Dienste des Internets. Obwohl die E-Mail-Anwendung nicht als verlässlicher Dienst konzipiert wurde, wird sie als Mittel zur einfachen und professionellen nachrichtenbasierten Kommunikation im Internet eingesetzt [1].

Die Vorteile der E-Mail-Anwendung sind sehr klar zu erkennen: Jeder kann damit umgehen, weil die Handhabung sehr einfach ist. Die E-Mails werden innerhalb weniger Sekunden weltweit übertragen und jeder kann jederzeit mithilfe von Mail-Boxen erreicht werden. Die Inhalte und Anhänge der E-Mails können sofort weiter verwendet werden, es tritt kein Medienbruch auf. Die E-Mail Anwendung ist sehr kostengünstig, da in der Regel keine extra Gebühren für den Austausch der E-Mail bezahlt werden müssen. Der E-Mail-Dienst ist für die vernetzte Informations- und Wissensgesellschaft inzwischen eine nicht mehr wegzudenkende Anwendung.

## 13.2 Generelle Cyber-Sicherheitsprobleme des E-Mail-Dienstes

Der Basis-E-Mail-Dienst hat einige generelle Cyber-Sicherheitsprobleme, die bei der Nutzung grundsätzlich betrachtet werden müssen.

### **Weltweit kann jeder E-Mails versenden!**

Für die E-Mails, die gewünscht sind, ist das eine sehr gute Eigenschaft! Für die E-Mails, die nicht gewollt sind (E-Mails mit Werbung, politischen Inhalten, kriminellen Absichten, ...) hat sich das Wort „Spam“ etabliert. Es gibt aber auch E-Mails, die uns einen direkten Schaden zufügen sollen. Das sind E-Mails mit Malware (Viren, Würmen, Trojanern ...) oder auch Phishing-E-Mails, mit denen Zugangsdaten „gefischt“ werden sollen. Mit Phishing-E-Mails werden Nutzer motiviert, auf gefälschten Webseiten ihre persönlichen Daten einzugeben.

Alle E-Mails, die nicht gewünscht sind, stellen ein großes Problem für die E-Mail-Anwendung dar, insbesondere weil die eigene E-Mail-Infrastruktur das Senden nicht verhindert und der Sender nicht eindeutig verifiziert werden kann.

Laut einer Studie der ENISA ist der Spam-Anteil größer als 95 % in der E-Mail-Infrastruktur. Bei den Nutzern kommen zwar durch intelligente Spam-Filtermechanismen nicht mehr so viele Spam-E-Mails in den E-Mail-Postfächern an, aber das Aufkommen ist immer noch hoch und produziert einen sehr großen Schaden, weil 95 % der E-Mail-Infrastruktur für nicht gewollte E-Mails vorgehalten werden muss.

E-Mail-Anhänge können und werden dazu missbraucht, beim Empfänger Schadcode (Malware) auf das IT-System zu schleusen. Dies kann in Form einer Datei im E-Mail-Anhang geschehen, die der Nutzer erst selbst ausführen muss, damit der Schadcode ausgeführt wird. Oder der Dateianhang nutzt direkt eine Sicherheitslücke in dem verwendeten E-Mail-Programm, das die erhaltene E-Mail in einem bestimmten Format darstellt. Eine weitere Möglichkeit, Schadcode über E-Mails einzuschleusen, ist das Verlinken aus der E-Mail heraus auf eine kompromittierte Webseite. Solche E-Mails sind oftmals personalisiert und werden deshalb vom Nutzer als vertrauenswürdig eingestuft. Aber durch das Anklicken eines Links auf eine kompromittierte Webseite gelangt das Schadprogramm auf das eigene IT-System und wird infiziert. Aus diesem Grund müssen geeignete Anti-Malware-Systeme in die E-Mail-Infrastruktur eingebunden werden.

### **Eine E-Mail ist wie eine Postkarte!**

Es wird vom E-Mail-Dienst keine Vertraulichkeit garantiert! Passwörter, Kreditkartennummern und weitere Bankdaten sowie vertrauliche Unternehmensinformationen, wie Kundendaten, Entwicklungsdaten, Kalkulationen usw., werden im Klartext übertragen und stellen so ein großes Risiko dar! Die Möglichkeiten, eine E-Mail im Internet oder in Bürogebäuden abzugreifen sind sehr hoch. In einigen

Ländern werden alle E-Mails analysiert, um zum Beispiel an das Know-how von Firmen andere Länder zu kommen. Untersuchungen und Befragungen zeigen auf, dass weniger als 4 % aller E-Mails verschlüsselt werden. Es wird aber auch aufgezeigt, dass über 40 % der E-Mails in Business-Prozessen verwendet werden. Aus diesem Grund sollten den Mitarbeitern im Unternehmen E-Mail-Verschlüsselungs-technologien zur Verfügung gestellt werden, damit die E-Mails gegen unberechtigte Einsichtnahme geschützt werden. Die Mitarbeiter müssen aber wissen, wie und – ganz wichtig – wann diese Verschlüsselungs-technologien für vertrauliche E-Mails verwendet werden sollen.

### **Fehlende Nachweisbarkeit**

Der Absender einer E-Mail und die Echtheit des Inhaltes einer E-Mail können nicht verifiziert werden, das heißt, es kann nicht eindeutig festgestellt werden, ob die E-Mail während der Übertragung manipuliert wurde. Außerdem können Sender und Empfänger nicht sicher sein, mit wem sie E-Mails austauschen.

Die Gewissheit, dass eine E-Mail angekommen ist (Bestellungen usw.) hängt von der Qualität von E-Mail-Servern anderer ab, auf die der Sender keinen Einfluss hat (vertraglich, rechtlich, ...). Die Verbindlichkeit einer Bestellung durch eine E-Mail (Zimmer, Tagungsräume usw.) ist nicht zweifelsfrei möglich, da der Sender jede E-Mail-Adresse annehmen kann.

Mithilfe einer digitalen Signatur auf der Basis von Public-Key-Verfahren kann eine E-Mail signiert werden und damit ist eine gesetzliche Verbindlichkeit von E-Mails realisierbar. Außerdem werden auf der Geschäftsebene Sicherheits-funktionen gebraucht, die zum Beispiel durch die Bestätigung des Empfangs auf der Anwendungsebene oder auf der Infrastrukturebene Verbindlichkeit herstellen, siehe auch Abschn. 4.1 „Digitale Signatur“.

Es muss aber zurzeit festgestellt werden, dass Spam, Malware, Phishing-Mails und andere Schwachstellen, wie schlecht konfigurierte und betriebene E-Mail-Server, unzureichende Nutzung von Verschlüsselung und digitaler Signatur sowie nicht-aufgeklärte Mitarbeiter ein ernsthaftes Problem mit hohem Schadens-potenzial und ein sehr hohes Cyber-Sicherheitsrisiko für jeden Einzelnen, die Unternehmen und für die Gesellschaft darstellen!

---

## **13.3 E-Mail-Verschlüsselung**

Bis auf einige isolierte PGP- und S/MIME-Inseln gibt es in der Praxis kaum fundierte Cyber-Sicherheitskonzepte für unternehmensweite und übergreifende E-Mail-Verschlüsselungslösungen. Die Ursachen für die geringe Nutzung sind neben dem Unwissen über die Risiken, die hohen Kosten für die E-Mail-Ver-schlüsselungsinfrastruktur durch Clientsoftware, Token, Lesegeräte, Rollout, Helpdesk, Zertifikatsmanagement usw.

### **End-to-End-Verschlüsselungslösungen**

End-to-End-Verschlüsselungslösungen für E-Mails haben sich in der Praxis kaum durchgesetzt. Neben den hohen Kosten und aufwendiger Administration kranken die End-to-End-Lösungen an den folgenden Problemfeldern:

- Interoperabilitätsprobleme, insbesondere bei unternehmensübergreifender und produktübergreifender Verschlüsselung
- Message-Recovery-Problematik
- Vertreter-Regeln
- Malware-Problematik in E-Mail-Anhängen

End-to-End-Konzepte sind individuelle Konzepte, das heißt, sie benötigen so viele Schlüssel wie Mitarbeiter im Unternehmen sind. Scheidet ein Mitarbeiter aus dem Unternehmen aus, muss gewährleistet sein, dass berechtigte Personen die an diesen Mitarbeiter gerichteten oder von ihm bereits erhaltenen E-Mails lesen und beantworten können. Die Schlüssel der Mitarbeiter müssen bei diesen Konzepten entweder an zentraler Stelle hinterlegt werden, oder jede E-Mail muss zusätzlich mit einem „Hauptschlüssel“ – also doppelt – verschlüsselt werden. Die gleiche Problematik gilt für die Vertretung bei Abwesenheit des Mitarbeiters.

Bei der Prüfung verschlüsselter Mail-Anhänge auf Malwarebefall wären aufwendige Umverschlüsselungen erforderlich, da Anti-Malware-Programme nur im Klartext die Anhänge analysieren können.

Hier müssen dann auf den IT-Systemen besondere Anti-Malware-Maßnahmen getroffen werden, um nach der Entschlüsselung die Anhänge auf Malwarebefall zu untersuchen.

### **Ablauf der E-Mail-Verschlüsselung**

Wie der Ablauf der E-Mail-Verschlüsselung prinzipiell bei S/MIME funktioniert, kann dem Abschn. [4.6.1 „E-Mail-Sicherheit“](#) entnommen werden.

#### **13.3.1 PGP und S/MIME sowie deren Unterschiede**

PGP (GNUPGP) und S/MIME sind E-Mail-Sicherheitslösungen, die sich weitestgehend auf dem Markt als Standards für die Sicherheit von E-Mails etabliert haben. Beide E-Mail-Sicherheitslösungen sind zueinander nicht kompatibel. Das heißt, Nutzer können keine verschlüsselten oder signierten E-Mails untereinander austauschen, obwohl beide Verfahren nach einem ähnlichen Prinzip arbeiten und sogar dieselben kryptografischen Algorithmen verwenden. Dieser Umstand ist auf die unterschiedliche konzeptionelle Struktur der beiden Sicherheitsverfahren zurückzuführen. Im Wesentlichen unterscheiden sich die Konzepte beider

Standards beim verwendeten Nachrichtenformat, Vertrauensmodell, Schlüsselformat und der Schlüsselverwaltung.

## 1. Nachrichtenformat

Das Nachrichtenformat von S/MIME baut auf dem Multipurpose Internet Mail Extension (MIME)-Datenformat auf, das auch von regulären E-Mails als Datenformat genutzt wird. S/MIME nutzt lediglich eine Erweiterung des MIME-Datenformats, das um zusätzliche kryptografische Elemente erweitert wurde. Durch diese gemeinsame Grundlage ist die Nutzung von S/MIME auf vielen E-Mail-Programmen ohne die Notwendigkeit von zusätzlichen Erweiterungen oder Software bereits möglich.

PGP benötigt hingegen zusätzliche Erweiterungen und Software, um seine kryptografischen Funktionen erfüllen zu können. Die Gründe dafür sind historisch bedingt. Während PGP aus einem anfangs privaten Projekt entstanden ist, wurde S/MIME von einem Konsortium von Herstellern entwickelt. Dadurch war die Integrierbarkeit von S/MIME in E-Mail-Programmen begünstigt.

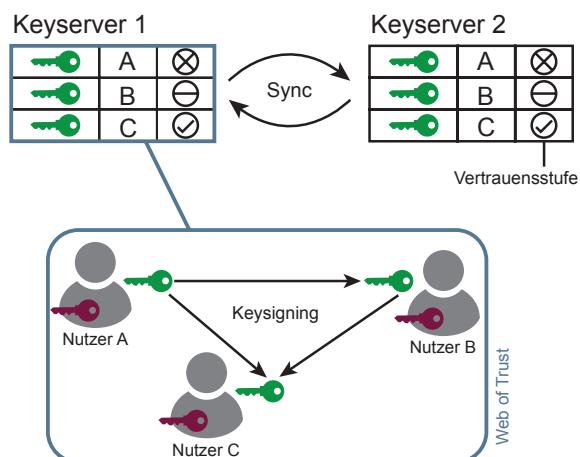
## 2. Vertrauensmodelle der E-Mail-Sicherheitslösungen PGP und S/MIME

Bei jeden Public Key-Verfahren stellt das Cyber-Sicherheitsbedürfnis „Gewährleistung der Authentizität“ für den öffentlichen Schlüssel eine besondere Aufgabe dar. Die Vertrauensstruktur ist bei beiden E-Mail-Sicherheitslösungen PGP und S/MIME sehr unterschiedlich. Um die Authentizität eines öffentlichen Schlüssels der Nutzer zu gewährleisten, gibt es verschiedene Vertrauensmodelle für unterschiedlichen Public-Key-Lösungen.

### Prinzipielles Vertrauensmodell von PGP

PGP setzt auf eine dezentrale Vertrauensstruktur, das sogenannte „Web of Trust“, ein Netzwerk des Vertrauens, das die Zugehörigkeit eines öffentlichen Schlüssels zu einem Nutzer bestätigen soll, siehe Abb. 13.1. Es gibt keine zentrale

**Abb. 13.1** Web of Trust



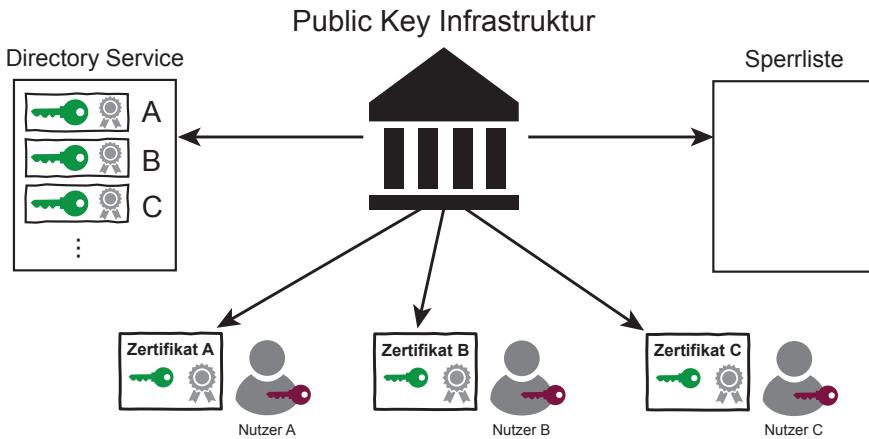
administrative Instanz, die einem öffentlichen Schlüssel der Nutzer das Vertrauen ausspricht. Jeder Nutzer kann einen öffentlichen Schlüssel, einschließlich seiner eigenen Schlüssel, signieren und somit zur Vertrauenswürdigkeit der Authentizität der öffentlichen Schlüssel beitragen. Je mehr Schlüsselhaber die Authentizität eines öffentlichen Schlüssels eines anderen Nutzers bestätigen, desto mehr Vertrauen wird gegenüber diesem öffentlichen Schlüssel im Web of Trust generiert.

Eine Veranstaltung, auf der sich Nutzer von PGP treffen, um ihre öffentlichen Schlüssel gegenseitig digital zu unterschreiben, wird Keysigning-Party genannt.

Jeder Nutzer kann seinen öffentlichen Schlüssel auf einem Schlüsselserver hinterlegen, der den öffentlichen Schlüssel auf andere verbundene Schlüsselserver synchronisiert. So kann ein Nutzer an vertrauenswürdige öffentliche Schlüssel von anderen Nutzern gelangen.

### Prinzipielles Vertrauensmodell von S/MIME

Bei S/MIME wird für das Cyber-Sicherheitsbedürfnis „Gewährleistung der Authentizität des öffentlichen Schlüssels“ elektronische Zertifikate verwendet, die von Zertifizierungsinstanzen erstellt werden, siehe auch Abschn. 4.2 „Elektronische Zertifikate/Digitale Zertifikate“. Damit baut das S/MIME-Konzept auf ein stark hierarchisches und zentralisiertes Vertrauensmodell auf, diese Abb. 13.2. Die Gewährleistung der Authentizität der Zertifikate beruht auf der digitalen Signatur einer zentralen vertrauenswürdigen Zertifizierungsinstanzen (Certification Authority), die die Authentizität für ein gültiges Zertifikat bestätigt. Auf diese Weise kann die Authentizität der Zertifikate gegenüber Dritten verifiziert werden. Ferner



**Abb. 13.2** Zertifizierungsinstanz

gibt es bei S/MIME unterschiedliche Stufen von Zertifikaten, die sich in ihrer Vertrauensstufe unterscheiden, jedoch nicht in ihrer kryptografischen Sicherheit. Es gibt drei unterschiedliche Klassen von Zertifikaten.

- Bei Klasse-1-Zertifikaten wird die Echtheit der E-Mail-Adresse verifiziert und in die Signatur aufgenommen.
- Klasse-2-Zertifikate beinhalten neben der E-Mail-Adresse auch den Namen, die Firma oder Organisation des Antragstellers, die mit dem Personalausweis und dem Handelsregister abgeglichen werden müssen.
- Bei Klasse-3-Zertifikaten muss sich der Antragsteller persönlich bei einer Zertifizierungsstelle verifizieren lassen. Die Klassen unterscheiden sich nur in der Stärke der Authentizität.

### **3. Schlüsselerstellung und Schlüsselformat**

Prinzipiell kann bei beiden Verfahren jeder ein Schlüsselpaar beziehungsweise ein Zertifikat erstellen. Bei PGP kann jeder ein gültiges Schlüsselpaar erstellen und auch für Verschlüsselung und Signierung von E-Mails nutzen. Das Schlüsselformat erlaubt es für den Schlüsselhaber, einen primären öffentlichen Schlüssel und mehrere sekundäre öffentliche Schlüssel auf derselben Identität zu verwalten, ähnlich wie bei einem Schlüsselbund. Der primäre öffentliche Schlüssel kann mehr als eine Nutzer-ID mit jeweils mehreren Signaturen beinhalten. Jeder einzelne dieser öffentlichen Schlüssel kann auch bei Bedarf widerrufen werden.

Bei S/MIME ist im Prinzip ebenfalls jeder in der Lage, ein Zertifikat zu erstellen, jedoch ist dies kein gültiges Zertifikat. Gültige Zertifikate können nur durch eine zentrale Zertifizierungsinstanz erstellt werden. In der Regel ist das ein kostenpflichtiger Vertrauensdienstanbieter. Das Schlüsselformat von S/MIME kann nur einen einzigen öffentlichen Schlüssel, eine Benutzer-ID und eine Signatur verwalten. Dieser kann auch nur durch eine offizielle Zertifizierungsstelle signiert werden.

### **4. Widerrufen eines Schlüssels**

Im Umgang mit dem Widerrufen eines Schlüssels gehen PGP und S/MIME unterschiedliche Wege. Bei PGP wird der widerrufene Schlüssel ebenfalls auf den Schlüsselservern, auf dem auch die aktiven Schlüssel liegen, gespeichert. Bei einem Widerruf wird der Schlüssel um eine spezielle Signatur erweitert, an der der Widerruf des Schlüssels erkannt werden kann. Wird ein Schlüssel auf Gültigkeit überprüft, kann festgestellt werden, ob dieser widerrufen wurde oder noch gültig ist. Für eine Überprüfung wird eine Internet-Verbindung benötigt. Da es bei PGP keine höhere zentrale Instanz wie bei S/MIME gibt, kann nur der Schlüsselhaber einen Widerruf für einen seiner öffentlichen Schlüssel durchführen.

S/MIME pflegt stattdessen spezielle Certificate Revocation Lists (CRLs). Das sind Sperrlisten, die alle gesperrten Schlüssel beinhalten. Die CRLs werden von

den entsprechenden Zertifizierungsstellen (CA) aktualisiert und verwaltet. Die Nutzer müssen sich regelmäßig aktualisierte Sperrlisten herunterladen oder über einen Service prüfen. Im Gegensatz zu PGP ist bei S/MIME eine Überprüfung auf einen gesperrten öffentlichen Schlüssel auch ohne Internet möglich, da die Listen lokal gespeichert werden können. Wird ein Zertifikat beziehungsweise ein Schlüssel widerrufen, kann der Schlüsselinhaber nur einen Antrag stellen, dieser muss dann durch die CA erst bestätigt werden.

### Fazit

PGP und S/MIME sind E-Mail-Sicherheitslösungen, die beide auf unterschiedlichen konzeptionellen Strukturen beruhen und dadurch beide ihre Vor- und Nachteile besitzen. S/MIME besitzt den Vorteil, dass das Austauschformat auf dem MIME-Datenformat basiert und dadurch auf vielen E-Mail-Programmen bereits integriert ist und oft ohne zusätzliche Plug-ins oder Erweiterungen auskommt. Ferner verwalten zentrale Zertifizierungsinstanzen die Erstellung und Verwaltung von gültigen Zertifikaten.

PGP hingegen nutzt das „Web of Trust“ als dezentrales Vertrauensmodell. Jeder Schlüsselinhaber kann Schlüssel signieren und so dazu beitragen, die Authentizität eines Schlüssels zu gewährleisten. Das Vertrauensmodell kommt auch bei der Schlüsselerstellung und -verwaltung ohne die Abhängigkeit gegenüber einer zentralen Verwaltungsinstanz aus und ist dadurch flexibler als bei S/MIME.

Die beiden Standards haben nahezu den gleichen Funktionsumfang, aber unterscheiden sich dann doch im Detail. Welche Lösung sich am besten zur E-Mail-Sicherheit eignet, kommt letztendlich immer auf den individuellen Anwendungsfall und die Anforderungen des Nutzers oder Organisation an.

In der Praxis nutzen Privatpersonen und kleine KMUs mehr PGP und große Unternehmen mehr S/MIME.

### 13.3.2 Weitere Alternativen für E-Mail-Sicherheit

In diesem Abschnitt werden weitere alternative E-Mail-Sicherheitslösungen beschrieben und diskutiert.

#### Gateway E-Mail-Sicherheitslösungen

Bei dem Gateway-Ansatz befindet sich ein E-Mail-Gateway mit Cyber-Sicherheitsfunktionen an zentraler Stelle im Netzwerk. Diese E-Mail-Sicherheits-Gateways entschlüsseln und verifizieren eingehende E-Mails und sind in der Lage, hinausgehenden E-Mail-Verkehr zu verschlüsseln und zu signieren. Die E-Mail-Sicherheits-Gateways können das in der Regel auch für die beiden Standards PGP und S/MIME.

Auf diese Weise wird ein hoher Nutzerkomfort geschaffen, da der Nutzer sich nicht aktiv an dem Prozess beteiligen muss. Ferner bieten E-Mail-Gateways

eine hohe Kompatibilität zwischen unterschiedlichen Gerätetypen und Betriebssystemen. Durch die zentrale Positionierung bietet das E-Mail-Sicherheits-Gateway Vertraulichkeit (Verschlüsselung), Integrität und Verbindlichkeit (Signatur), jedoch keine Ende-zu-Ende-Verschlüsselung. Die Einhaltung und Anwendung von Pollicys bezüglich der E-Mail-Sicherheit wird durch die zentrale Umsetzung deutlich begünstigt.

Auf der Gegenseite kann ebenfalls ein E-Mail-Sicherheits-Gateway stehen oder eine entsprechende Client-Software, um die Cyber-Sicherheitsfunktionen zu realisieren. Steht keine dieser Komponenten auf der Gegenseite zur Verfügung, können solche E-Mail-Sicherheits-Gateways verschlüsselte, selbstextrahierende Dateien zuschicken, die mittels Passphrase wieder entschlüsselt werden können. Da bei dem Gateway-Ansatz die Entschlüsselung zentral im E-Mail-Sicherheits-Gateway durchgeführt wird, können eine Vertreter-Regelung sowie die zentrale Überprüfung der E-Mail-Anhänge sehr einfach realisiert werden.

### „E-Mail made in Germany“

„E-Mail made in Germany“ ist eine Initiative, die von GMX, Telekom und [Web.de](#) ins Leben gerufen wurde und für die Verschlüsselung der E-Mail Kommunikationen zwischen dem IT-Endgerät und E-Mail-Servern (MTAs) sorgt [2]. Egal ob der E-Mail-Dienst per Browser oder App auf dem Smartphone, Tablet, Notebook oder PC genutzt wird, die E-Mail-Daten werden immer TLS/SSL-verschlüsselt übermittelt und so vor unberechtigtem Lesen geschützt. Wichtig ist natürlich, dass die E-Mail-Programme TLS/SSL aktiviert haben. Damit eine sichere Übertragung auf allen Übertragungswegen gewährleistet werden kann, werden zwischen den E-Mail-Servern von freenet, GMX, Telekom und [WEB.DE](#) alle Daten ausschließlich TLS/SSL-verschlüsselt und -integritätsgesichert übertragen. Damit bietet „E-Mail made in Germany“ einen guten Basis-Schutz für die E-Mail Kommunikationen. Die E-Mails sind aber bei dieser Lösung auf den E-Mail-Servern (MTA) selber im Klartext, siehe Abb. 13.3.



**Abb. 13.3** Verschlüsselte und integritätsgesicherte E-Mail-Kommunikation

## De-Mail

De-Mail ist eine kostenpflichtige Alternative, um vertrauliche E-Mails sicher und verbindlich elektronisch zu versenden und zu empfangen. Wie bei „E-Mail made in Germany“ werden die E-Mail-Daten immer zwischen dem IT-System und E-Mail-Server und zwischen den E-Mail-Servern TLS/SSL-verschlüsselt und -integritätsgesichert übermittelt. Optional kann eine Ende-zu-Ende Verschlüsselung genutzt werden. Ursprünglich wurde die De-Mail als sicheres und verbindliches elektronisches Pendant zum regulären Briefverkehr entwickelt.

Die De-Mail-Dienste stützen sich auf eine gesetzliche Grundlage von eIDAS. Die gesetzliche Verbindlichkeit und Gewährleistung des Erhalts der E-Mail steht bei der Nutzung von De-Mail im Vordergrund, da diese eine Rechtsgültigkeit eines regulären Briefes widerspiegeln soll [3].

Anbieter von De-Mail müssen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) in regelmäßigen Abständen akkreditiert werden. Um die Verbindlichkeit zu gewährleisten, muss bei der Registrierung ein Identitätsnachweis durchgeführt werden, um die Authentizität des Antragsstellers zu verifizieren.

Ein besonderer De-Mail-Dienst ist das De-Mail-Einschreiben.

Der Absender erhält zusätzlich qualifizierte Bestätigungen, wann er die E-Mail verschickt hat und wann sie an das Postfach des Empfängers ausgeliefert wurde.

Außerdem kann ein Absender auch folgende Optionen vor dem Versand einer De-Mail wählen:

- Persönlich

Das erforderliche Authentisierungsniveau von Absender und Empfänger muss mindestens hoch sein, um die E-Mail lesen zu können, beispielsweise wegen der besonderen Vertraulichkeit der Nachricht.

- Absender-Bestätigt

Das erforderliche Authentisierungsniveau des Absenders muss wegen der besonderen Verbindlichkeit der E-Mail mindestens hoch sein. Der De-Mail-Provider des Absenders bestätigt nach Entgegennahme der E-Mail mittels qualifizierter Signatur, dass er den angegebenen Nachrichteninhalt von dem Absender entgegengenommen hat und dieser sich mindestens mit hoch authentisiert hat. Der Empfänger erhält dadurch einen glaubwürdigen („starken“) Nachweis der Authentizität des Absenders und der Integrität der Nachricht.

- Versandbestätigung

Der De-Mail-Anbieter des Absenders erstellt eine qualifizierte signierte Bestätigung, dass er eine referenzierte E-Mail zu einem bestimmten Zeitpunkt für den Versand an einen bestimmten Empfänger entgegengenommen hat.

- Zugangsbestätigung

Der De-Mail-Anbieter des Empfängers erstellt nach Ablage der E-Mail in das Postfach des Empfängers eine qualifiziert signierte Bestätigung, dass er eine referenzierte E-Mail zu einem bestimmten Zeitpunkt in das Postfach des Empfängers eingestellt hat.

- Abholbestätigung

Der De-Mail-Anbieter des Empfängers erstellt nach einer sicheren Anmeldung des Nutzers und bei Vorhandensein einer E-Mail mit Abholbestätigungs-Anforderung im Postfach des Empfängers eine qualifiziert signierte Bestätigung, dass der Nutzer eine E-Mail einsehen konnte.

Dadurch kann die E-Mail-Dienst auch für besonders wichtige Prozesse genutzt werden.

### Manuelle Dateiverschlüsselung

Eine pragmatische Alternative, um vertrauliche Dateien mithilfe von E-Mails zu versenden, ist eine manuelle Dateiverschlüsselung. Falls keine sichere Infrastruktur für einen verschlüsselten E-Mail-Versand vorhanden ist, kann auf diese Methode zurückgegriffen werden, um dennoch Vertraulichkeit zwischen den Kommunikationspartnern herzustellen. Verschlüsselte Dateien werden bei diesem Verfahren als Anhang an die E-Mail angehängt. Die E-Mail dient lediglich zum Transport der Datei. Eine Einsicht durch Dritte ist aufgrund der Verschlüsselung der Datei auf dem Transportweg nicht möglich. Der sichere Austausch der Passphrase zwischen den beteiligten Kommunikationspartnern zur Entschlüsselung der Dateien stellt jedoch eine weitere Herausforderung dar. Außerdem kann die Authentizität der Nachricht nicht verifiziert werden, da keine Vertrauensstruktur wie bei PGP und S/MIME vorhanden ist.

Ein Anwendungsbeispiel könnte der Versand einer vertraulichen PDF sein. Der Sender versieht die PDF mit einer Passphrase und verschlüsselt die Datei. Die verschlüsselte Datei wird als Anhang einer E-Mail zum Empfänger versendet. Anschließend wird die Passphrase über einen zweiten Kanal übertragen, beispielsweise über SMS oder telefonisch. Die größte Sicherheit bietet ein persönlicher Austausch der Passphrase, jedoch ist das in der Praxis nicht immer realisierbar. Der Anhang wird lokal beim Empfänger runtergeladen und mithilfe der Passphrase entschlüsselt und wird dadurch für den Empfänger einsehbar. Ob die PDF wirklich vom erwarteten Sender stammt, kann nicht verifiziert werden. In der Tab. 13.1 werden die Vor- und Nachteile sowie die Skalierbarkeit der verschiedenen E-Mail-Sicherheitslösungen dargestellt [4].

**Tab. 13.1** E-Mail-Sicherheit: Vor- und Nachteile sowie Skalierbarkeit

Lösung	Vorteile	Nachteile	Skalierbarkeit
PGP	<ul style="list-style-type: none"> <li>• Open Source</li> <li>• Kostenfrei</li> <li>• Ende-zu-Ende-Verschlüsselung</li> </ul>	<ul style="list-style-type: none"> <li>• Komplexes Verfahren</li> <li>• Veränderte User Experience</li> <li>• Web of Trust als Sicherheitsanker</li> <li>• Verschlüsselt gespeicherte E-Mails sind nicht mehr durchsuchbar</li> <li>• Verlust des privaten Schlüssels oder Passworts führt zum Verlust der verschlüsselten E-Mails</li> </ul>	<ul style="list-style-type: none"> <li>• Gute Skalierbarkeit</li> <li>• Einsatz möglich in allen Unternehmensgrößen</li> </ul>
S/MIME	<ul style="list-style-type: none"> <li>• Ende-zu-Ende-Verschlüsselung</li> <li>• Einfache Verwendung</li> <li>• Kein Schlüsselmanagement durch den Nutzer</li> </ul>	<ul style="list-style-type: none"> <li>• Identitätsüberprüfung zur Steigerung des Vertrauens</li> <li>• Achtsamkeit nötig</li> <li>• Veränderte User Experience</li> <li>• Verlust des privaten Schlüssels oder Passworts führt zum Verlust der verschlüsselten E-Mails</li> </ul>	<ul style="list-style-type: none"> <li>• Gute Skalierbarkeit</li> <li>• Einsatz möglich in allen Unternehmensgrößen</li> </ul>
E-Mail-Gateway		<ul style="list-style-type: none"> <li>• Hoher Nutzerkomfort</li> <li>• Policykonforme Verschlüsselung</li> <li>• Kein geändertes Bedienverhalten</li> <li>• Unterstützung verschiedener Standards</li> <li>• Zentrale Schlüsselverwaltung</li> <li>• Malware-Prüfung vor Zustellung der Mails</li> <li>• Revisionssicher</li> <li>• Data-Loss-Prevention</li> </ul>	<ul style="list-style-type: none"> <li>• Sehr gute Skalierbarkeit</li> <li>• Einsatz geeignet für mittlere und große Unternehmen</li> </ul>

(Fortsetzung)

**Tab. 13.1** (Fortsetzung)

Lösung	Vorteile	Nachteile	Skalierbarkeit
„E-Mail made in Germany“	<ul style="list-style-type: none"> <li>• Hoher Nutzerkomfort</li> <li>• Transportverschlüsselung</li> <li>• Zusätzlich kann auch unabhängig von der „E-Mail made in Germany“ PGP und S/MIME verwendet werden</li> </ul>	<ul style="list-style-type: none"> <li>• Keine standardmäßige Ende-zu-Ende Verschlüsselung</li> </ul>	<ul style="list-style-type: none"> <li>• Einsatz für jede Unternehmensgröße geeignet</li> </ul>
De-Mail	<ul style="list-style-type: none"> <li>• Hoher Nutzerkomfort</li> <li>• Transportverschlüsselung</li> <li>• Optionale Ende-zu-Ende-Verschlüsselung</li> <li>• Verbindlichkeit der E-Mail ist gesetzlich gewährleistet</li> <li>• Nutzerregistrierung erfordert eine Identitätsprüfung</li> <li>• Mehrere Anbieter vorhanden</li> </ul>	<ul style="list-style-type: none"> <li>• Kostenpflichtig</li> <li>• Postfach muss regelmäßig eingesehen werden</li> <li>• Lange Anmeldezeiten zur Prüfung der Identität des Antragstellers</li> <li>• Empfänger muss ebenfalls bei De-Mail registriert sein</li> <li>• Geringe Verbreitung, inkompatibel mit anderen E-Mail-Diensten</li> </ul>	<ul style="list-style-type: none"> <li>• Einsatz für jede Unternehmensgröße geeignet</li> </ul>
Manuelle Datei-verschlüsselung	<ul style="list-style-type: none"> <li>• Datei bleibt nach dem Herunterladen geschützt, E-Mail dient nur als Transport</li> <li>• Keine Infrastrukturweiterung notwendig</li> </ul>	<ul style="list-style-type: none"> <li>• Inhalt der Mail bleibt unverschlüsselt</li> <li>• Sicherheit ist abhängig vom Format und der Software</li> <li>• Passwortstärke legt Sicherheitsniveau fest</li> <li>• Händische Ver- und Entschlüsselung der Dokumente</li> <li>• Benötigt verschlüsselten Kommunikationskanal für den Schlüsselaustausch</li> </ul>	<ul style="list-style-type: none"> <li>• Skalierung schlecht bei vielen Dokumenten</li> </ul>

## 13.4 Zusammenfassung

Die E-Mail-Anwendung wird in vielen Bereichen verwendet, in denen Vertrauenswürdigkeit und Vertrauen eine besondere Rolle spielen. Aus diesem Grund ist es wichtig, dass die richtigen Cyber-Sicherheitsmechanismen genutzt werden, damit das Risiko eines Schadens bei der Nutzung von E-Mail minimiert werden kann.

---

## 13.5 Übungsaufgaben

### Übungsaufgabe 1

Sie wollen einem Freund eine vertrauliche E-Mail senden. Also verschicken Sie Ihrem Freund eine reguläre E-Mail über eine webbasierte Anwendung. Können Sie sich sicher sein, dass nur Sie und der Empfänger den Inhalt der E-Mail lesen können?

### Übungsaufgabe 2

Was bedeutet eine Ende-zu-Ende-Verschlüsselung für die E-Mail-Sicherheit?

### Übungsaufgabe 3

Welche Methoden oder Sicherheitslösungen gibt es für E-Mail-Sicherheit?

### Übungsaufgabe 4

Wie unterscheiden sich die Sicherheitslösungen PGP und S/MIME voneinander? Welche Vertrauensmodelle nutzen die Verfahren? Wie unterscheiden sich die Schlüsselgenerierung beziehungsweise die Zertifikatserstellung bei den beiden Verfahren?

### Übungsaufgabe 5

Welche Herausforderungen in der Praxis können Ende-zu-Ende-Sicherheitslösungen mit sich bringen? Welche Faktoren oder Szenarien spielen dabei für Unternehmen eine wichtige Rolle?

### Übungsaufgabe 6

Was sind die generellen Cyber-Sicherheitsprobleme bei der E-Mail-Anwendung?

Ergebnisse siehe: <https://norbert-pohlmann.com/cyber-sicherheit/uebungen/>.

---

## Literatur

1. Pohlmann N (2010) Bedrohungen und Herausforderungen des E-Mail-Dienstes – Die Sicherheitsrisiken des E-Mail-Dienstes im Internet. DuD Datenschutz und Datensicherheit 2010(9):667–673
2. E-Mail made in Germany. <https://www.e-mail-made-in-germany.de/Verschlüsselung.html>. Stand 20.11.18
3. De-Mail. <https://de.wikipedia.org/wiki/De-Mail>. Stand 20.11.18
4. Kompass IT-Verschlüsselung – Orientierungs- und Entscheidungshilfen für KMU zum Einsatz von Verschlüsselungslösungen. [https://norbert-pohlmann.com/app/uploads/2018/02/BMWI\\_Kompass\\_IT-Verschlüsselung\\_web\\_Prof.\\_Norbert\\_Pohlmann.pdf](https://norbert-pohlmann.com/app/uploads/2018/02/BMWI_Kompass_IT-Verschlüsselung_web_Prof._Norbert_Pohlmann.pdf). Stand 20.11.18



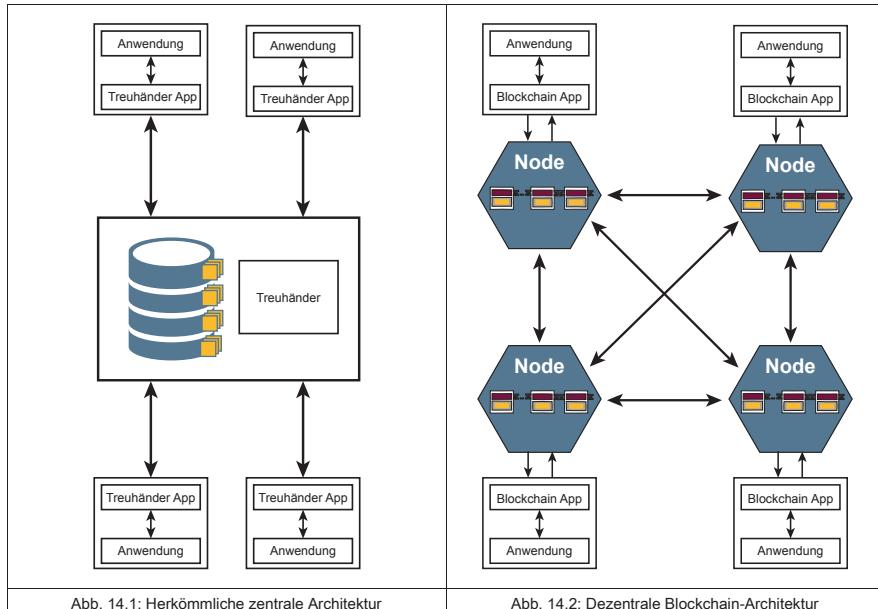
In diesem Kapitel werden die Grundzüge der Blockchain-Technologie, das Cyber-Sicherheitskonzept, die notwendigen Netzwerk-, Cyber-Sicherheits- und Vertrauenswürdigkeitsmechanismen sowie Beispielanwendungen der Blockchain-Technologie erläutert.

## 14.1 Einleitung

Die Blockchain-Technologie ist eine spannende und faszinierende IT-Technologie, die das Potenzial hat, Politik, Verwaltung und Wirtschaftszweige zu revolutionieren. Sie ist eine Querschnittstechnologie mit hohem disruptiven Potenzial für viele Wirtschaftsbereiche und bietet kooperative Vertrauensdienste. Die blockchainbasierten Systeme könnten in vielen Bereichen zentrale Instanzen, wie Treuhänder, Banken oder Notare, ablösen. Das ist möglich, weil die verteilten Konsensfindungs- und Validierungsverfahren der Blockchain-Technologie ganz ohne Intermediäre die Vertrauenswürdigkeit der aufgezeichneten Transaktionsdaten garantieren. Sogenannte Smart Contracts machen eine vorprogrammierte, selbstausführende Vertragsabwicklung möglich. Mithilfe der Blockchain-Technologie wird eine Zusammenarbeit auf verschiedenen Ebenen effektiver und sicherer umgesetzt.

### Blockchain-Technologie auf den Punkt gebracht

In Abb. 14.1 und 14.2 werden eine herkömmliche zentrale Architektur und die dezentrale Blockchain-Architektur von Transaktionsspeichern aufgezeigt, um den Unterschied grob darzustellen.



Bei einem zentralen herkömmlichen Transaktionsspeicher werden die Zusammenarbeit oder das Eigentum von digitalen Werten durch eine zentrale Instanz oder einen Treuhänder verwaltet und verifiziert. Beispiel einer zentralen Instanz ist eine Public-Key-Infrastruktur (PKI) und ein Treuhänder, ein Notar, der die Abwicklung eines Vertrages kontrolliert und verwaltet, siehe Abb. 14.1.

In einem dezentralen Blockchain-Transaktionsspeicher werden die Zusammenarbeit oder das Eigentum von digitalen Werten durch die Nodes eines Peer-to-Peer Netzwerkes mithilfe von smarten Cyber-Sicherheits- und Vertrauenswürdigkeitsmechanismen verwaltet und verifiziert. Daher ist keine kostenaufwendige zentrale Instanz notwendig, siehe Abb. 14.2.

### Unterschiedliche Sichtweisen auf die Blockchain-Technologie

Die verschiedenen Disziplinen können die Blockchain-Technologie aus sehr unterschiedlichen Blickwinkeln betrachten und bewerten.

Für einen **Informatiker** produziert die Blockchain-Technologie eine einfache Datenstruktur, die Blockchain, die Daten als Transaktionen in einzelnen Blöcken verkettet und in einem verteilten Peer-to-Peer-Netz redundant verwaltet. Die Alternative wäre eine konventionelle Datenbank, die kontinuierlich von allen Teilnehmern repliziert wird.

Für die **Cyber-Sicherheitsexperten** hat die Blockchain-Technologie den Vorteil, dass die Daten als Transaktionen in den einzelnen Blöcken manipulations-sicher gespeichert werden können, das heißt, die Teilnehmer der Blockchain sind in der Lage, die Echtheit, den Ursprung und die Unversehrtheit der gespeicherten Daten (Transaktionen) zu überprüfen. Die Alternative wäre hier zum Beispiel ein PKI-System als zentraler Vertrauensdienstanbieter.

Für den **Anwendungsdesigner** bedeutet die Nutzung der Blockchain-Technologie eine vertrauenswürdige Zusammenarbeit zwischen verschiedenen Organisationen, ohne die Einbindung einer zentralen Instanz, eines PKI-Systems, Notars usw. Die Alternative könnte hier ein kostenintensiver Treuhänder sein, der die Zusammenarbeit und Eigentumsübertragung zwischen den verschiedenen Organisationen verwaltet und verifiziert. Da die Blockchain-Technologie dies automatisiert macht, werden durch die vertrauenswürdige Zusammenarbeit die Prozesse auch sehr viel schneller und effektiver.

### Die Blockchain-Technologie als Kollaborations-Tool

Grundsätzlich wird mit der Blockchain-Technologie eine Blockchain erzeugt, in der fälschungssichere, verteilte Datenstrukturen und in denen Transaktionen in der Zeitfolge protokolliert nachvollziehbar, unveränderlich und ohne zentrale Instanz abgebildet sind.

Die Cyber-Sicherheitseigenschaften einer Blockchain-Technologie werden prinzipiell mit den folgenden Cyber-Sicherheitsmechanismen umgesetzt:

- „**fälschungssicher/unveränderlich**“ mithilfe von *One-Way-Hashfunktionen und digitalen Signaturen von Public-Key-Verfahren*
- „**verteilte/redundante Datenstrukturen (Fähigkeit der Verfügbarkeit der Daten)**“, viele Nodes des Peer-to-Peer-Netzwerkes haben die Daten/Transaktionen in der Blockchain verteilt und redundant gespeichert
- „**Transaktionen in der Zeitfolge protokolliert nachvollziehbar, unveränderlich**“, wird durch die Art der Verkettung mithilfe der Hashwerte „*HashPrev*“ und „*Merkle Hash*“ über die Daten in den Transaktionen sichergestellt
- „**ohne zentrale Instanz abgebildet sind**“, wird durch geeignete verteilte Vertrauenswürdigkeitsverfahren wie verteilte Konsensfindungsverfahren und verteilte Validierungsprozesse erzielt.

### Internet der Werte

Mit der Blockchain-Technologie werden neben der vertrauenswürdigen Zusammenarbeit auch Eigentumsverhältnisse (Digital Assets) direkter und effizienter als bislang gesichert und geregelt, da eine lückenlose und unveränderliche Datenaufzeichnung hierfür die Grundlage schafft. Alle Beglaubigungsprozesse werden schneller, sicherer und billiger. Aus diesem Grund wird die Blockchain auch als „**Internet der Werte**“ bezeichnet.

Die Blockchain-Technologie stellt mit den unterschiedlichen Cyber-Sicherheitsmechanismen ein „programmiertes Vertrauen“ zur Verfügung, weil alle Cyber-Sicherheitseigenschaften als *Security-by-Design* inhärent in der Blockchain-Technologie eingebunden sind.

**Wichtig** Bei der Nutzung der Blockchain-Technologie werden die Daten redundant, dezentral und manipulationssicher gespeichert, das heißt, die Teilnehmer an der Blockchain sind in der Lage, die Echtheit, den Ursprung und die Unversehrtheit der gespeicherten Daten jederzeit zu überprüfen.

**„Geschichte“ der Blockchain-Technologie** Als „Satoshi Nakamoto“ an der Bitcoin-Kryptowährung arbeitete, benötigte er eine dezentrale, öffentliche und vor Manipulationen geschützte Datenstruktur, auf welcher die einzelnen Transaktionen gespeichert werden konnten und dabei noch öffentlich einsehbar waren, sozusagen ein öffentliches Transaktionsbuch (Distributed Ledger). Da dies mit traditionellen relationalen Datenbanken nicht möglich war, entwickelte er die Blockchain-Technologie [1].

Bei „Satoshi Nakamoto“ handelt es sich um ein Pseudonym, und es ist bis heute nicht klar, welche Person oder Personengruppe sich dahinter verbirgt.

## 14.2 Aufbau der Blockchain-Technologie

In diesem Abschnitt werden die Elemente, Prinzipien, Strukturen und Architektur der Blockchain-Technologie als Grundlagen beschrieben.

### 14.2.1 Element: Daten

Mit der Blockchain-Technologie wird eine gemeinsame Blockchain erzeugt, die eine einfache Datenstruktur darstellt. Die Daten werden in der Blockchain in einzelnen, chronologisch miteinander verketteten Blöcken als Transaktionen verwaltet. Die Daten werden in Transaktionen manipulationsgesichert in Blöcken der Blockchain gespeichert, siehe auch Abschnitt Transaktionen. Jede Node hat eine eigene Blockchain-Version, daher sind die Daten verteilt und redundant vorhanden, das heißt, es besteht eine sehr hohe Verfügbarkeit der Daten.

Eine Blockchain kann sehr groß werden, wie beispielsweise die Bitcoin-Blockchain etwa 189 G Byte groß ist (Stand: November 2018).

Die grauen rechteckigen Kästchen in Abb. 14.3 sind Transaktionen, die gelben Quadrate sind die Daten in der Transaktion, der grüne Schlüssel ist der öffentliche Schlüssel des Blockchain-Teilnehmers, der die Transaktion erstellt und signiert hat. Das rote „Sign“-Symbol ist die Signatur unter der Transaktion. Der rote „HashPrev“ ist der Hashwert über den Vorgänger-Block-Header, mit dem die Verkettung umgesetzt wird. Alle Blöcke zusammen bilden die Blockchain (Block (1) bis Block (n)).

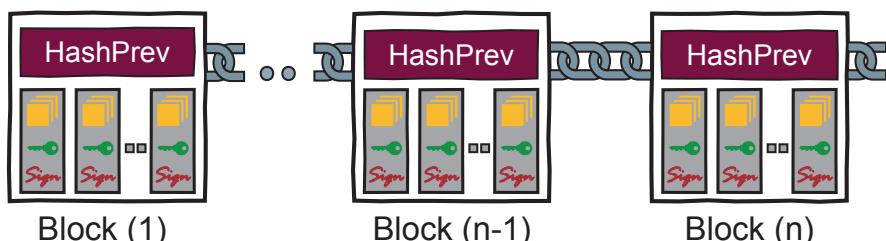


Abb. 14.3 Architektur einer Blockchain

### 14.2.2 Element: Block

Ein Block in einer Blockchain ist ein strukturierter Datensatz, der im Prinzip beliebige Transaktionen mit Daten enthalten kann und vor Manipulationen gesichert ist.

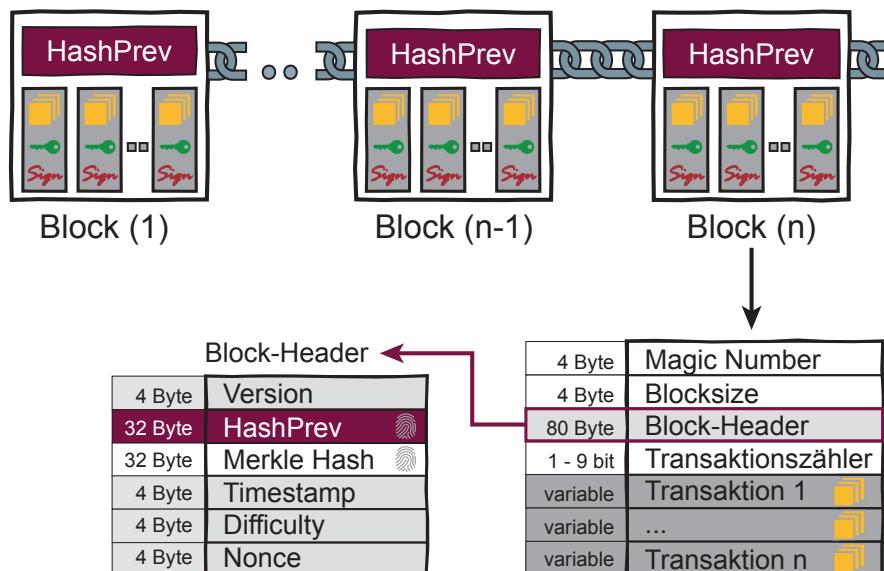
#### Erstellung eines neuen Blockes

In definierten Zeitintervallen wird ein neuer Block von der Node erstellt, die im Konsensfindungsverfahren ausgewählt wurde. Diese wählt aus, welche Transaktionen in welcher Reihenfolge in diesem Block enthalten sind (zumindest bei den gängigsten Konsensverfahren für öffentliche Blockchains). Nachdem dieser neue Block von der Node versandt wurde, verteilt er sich anschließend über das Peer-To-Peer-Netzwerk weiter.

Alle anderen Nodes validieren auch den empfangenen neuen Block. Die verteilte Validierung aller Blöcke in den verschiedenen Nodes ist wichtig, um Vertrauen aufzubauen. Zum Beispiel wird bei der Bitcoin-Blockchain alle zehn Minuten ein neuer Block erstellt.

Was die Blockchain interessant macht, ist der sogenannte Block-Header. In der Abb. 14.4 ist ein Bitcoin-Blockchain-Block dargestellt.

Im Block-Header ist die „Version“ und ein „Zeitstempel“ sowie ein „Difficulty“ und „Nonce“ enthalten. „Difficulty“ und „Nonce“ sind für das Konsensfindungsverfahren wichtig, siehe Abschnitt Konsensfindungsverfahren. Der Hashwert „HashPrev“ realisiert die Blockverkettung und der „Merkle Hash“ sorgt für die Integrität der Transaktionsdaten in einem Block.



**Abb. 14.4** Inhalt eines Blocks

**Wichtig** Durch die clevere Nutzung von Hashfunktionen können interessante Cyber-Sicherheitseigenschaften umgesetzt werden.

### 14.2.3 Element: HashPrev

Im Element „HashPrev“ wird der jeweilige aktuelle Hashwert des Block-Headers vom Vorgänger Block (Block-Header<sub>n-1</sub>) gespeichert. Dieser Hashwert, HashPrev<sub>n</sub>, wird dabei über den gesamten letzten Block-Header – inklusive des Hashwertes des Vorgänger Blockes (HashPrev<sub>n-1</sub>) – generiert, wodurch die Verkettung der Blöcke manipulationssicher umgesetzt werden kann.

$$\text{HashPrev}_{n+1} = \text{Aktueller-Hashwert}_n$$

$$= H(\text{Block-Header}_n(\dots || \text{HashPrev}_n || \text{Merkle-Hash}_n || \dots))$$

$$\text{HashPrev}_n = H(\text{Block-Header}_{n-1}(\dots || \text{HashPrev}_{n-1} || \text{Merkle-Hash}_{n-1} || \dots))$$

$$\text{HashPrev}_{n-1} = H(\text{Block-Header}_{n-2}(\dots || \text{HashPrev}_{n-2} || \text{Merkle-Hash}_{n-2} || \dots))$$

...

$$\text{HashPrev}_2 = H(\text{Block-Header}_1(\dots || \text{HashPrev}_1 || \text{Merkle-Hash}_1 || \dots))$$

$$\text{Aktueller-Hashwert}_n = \text{HashPrev}_{n+1}$$

H One-Way-Hashfunktion

Jeder Block in der Blockchain kann im Prinzip gelesen und überprüft werden. In den Blöcken finden sich die verschiedenen Daten in Transaktionen, die in der Blockchain gespeichert werden. Blöcke können auf ihre Integrität geprüft werden, indem getestet wird, ob der aktuelle Hashwert eines Blockes (Aktueller-Hashwert<sub>n</sub>) mit dem gespeicherten Hashwert im Folgeblock (HashPrev<sub>n+1</sub>) übereinstimmt. Der erste HashPrev<sub>1</sub> wird mit einem definierten Wert vorgegeben.

$$\text{Aktueller-Hashwert}_n = \text{HashPrev}_{n+1}$$

$$\text{Aktueller-Hashwert}_n = H(\text{Block-Header}_n(\dots || \text{HashPrev}_n || \text{Merkle-Hash}_n || \dots))$$

H One-Way-Hashfunktion

Dies ist für jede Node ohne weiteres möglich, da jede Node im Normalfall alle Informationen innerhalb eines Blockes lesen kann. Soll ein neuer Block hinzugefügt werden, so kann dieser nicht einfach an die Blockchain angehängt werden. Für jeden neuen Block muss die Richtigkeit des Blockes geprüft und validiert und mithilfe eines Konsensfindungsverfahrens bestimmt werden, welche Node des P2P-Blockchain-Netzwerkes einen Block mit ausgewählten Transaktionen hinzufügen darf, damit es nicht möglich ist, die Blockchain zu manipulieren (siehe Abschn. 14.2.10).

Die Blockverkettung mithilfe HashPrev-Hashwerte sorgt für die Cyber-Sicherheitseigenschaft, dass in einer Blockchain keine Daten gelöscht werden

können. Diese Cyber-Sicherheitseigenschaft kann in einer rechtlichen Situation problematisch sein, wie zum Beispiel bei der EU-Datenschutzgrundverordnung, bei der ein Recht auf Löschen besteht, aber auch, wenn nicht gewollte Daten, wie zum Beispiel Kinderpornografie, in der Blockchain gespeichert sind.

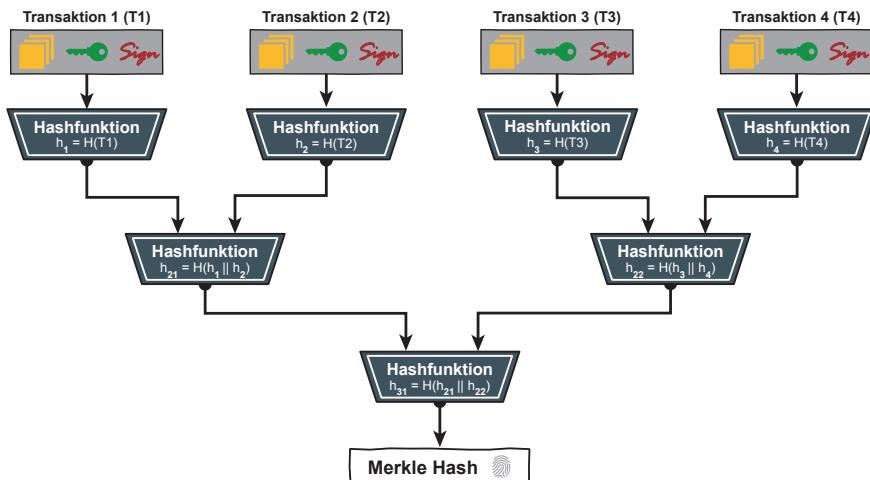
**Wichtig** Durch die Blockverkettung können die Daten in einer Blockchain nicht gelöscht werden.

#### 14.2.4 Element: Merkle Hash

Der „Merkle Hash“ wird verwendet, um aus den vielen Transaktionen ( $T$ ) in einem Block einen zusammenfassenden Hashwert zu bilden (Merkle Hash).

Die Blätter des Merkle-Baums sind die Hashwerte der Transaktionen  $h_i = H(T_i)$ . Jeder Knoten im Merkle-Baum wird als Hashwert  $H(h_1 \parallel h_2)$  seiner Kinder  $h_1$  und  $h_2$  gebildet. Dabei ist  $h_1$  der Hashwert der Transaktion 1 und  $h_2$  der Hashwert der Transaktion 2 und „ $\parallel$ “ die Verkettung, Konkatenation der Hashwerte und so weiter, siehe Abb. 14.5.

Der „Merkle Hash“ steht im Block-Header und kann daher für die Überprüfung der Integrität der Daten und Transaktionen in einem Block verwendet werden. Damit kann die Cyber-Sicherheitseigenschaft „Transaktionen in der Zeitfolge protokolliert nachvollziehbar, unveränderlich“ realisiert werden.



**Abb. 14.5** Berechnung: Merkle Hash

**Abb. 14.6** Aufbau einer Transaktion



### 14.2.5 Element: Transaktionen

Alle Daten innerhalb der Blöcke werden als Transaktionen gespeichert. Transaktionen enthalten Daten, die in der Zeitfolge protokolliert (chronologisch), nachvollziehbar, unveränderlich und ohne zentrale Instanz in der Blockchain abgebildet sind. Transaktionen werden vom Blockchain-Teilnehmer erstellt und signiert.

Die Daten in den Transaktionen können Kontostände, Werte, Attribute, Zertifikate, Sensor-Daten, Industrie-Daten, Quelltexte, Merkmale usw. oder allgemein digitale Werte sein. Eine Transaktion enthält auch immer den Public-Key der entsprechenden Blockchain-Adresse sowie die Signatur des Blockchain-Teilnehmers, der die Transaktion erstellt und signiert hat, siehe Abb. 14.6.

#### Beispiele von Daten einer **Bitcoin-Transaktion**:

Die Transaktionen enthalten bei Bitcoin im Wesentlichen folgende Inhalte:

- die ID der Transaktion (Hashwert)
- Meta-Data
- Inputs
- Outputs

Die Meta-Daten beinhalten die Versionsnummer, die Anzahl der eingehenden Beträge, die Anzahl der ausgehenden Beträge sowie die Transaktionsgröße in Bytes.

Bei den Inputs handelt es sich um die eingehenden Beträge, das sind die Anzahl der zu verschickenden Bitcoins und die Blockchain-Adresse (Kontonummer), von der diese verschickt werden. Außerdem steht hier die vom Blockchain-Teilnehmer erstellte Signatur.

Die einzelnen Outputs enthalten jeweils die Beträge, die verschickt werden und die jeweiligen Empfänger-Adressen.

#### Beispiel von Daten einer **Ethereum-Transaktion**:

Die Inhalte sind ähnlich der Bitcoin-Transaktion, nur dass hier zusätzlich Smart-Contracts enthalten sein können.

```
pragma solidity 0.4.23;
// Proof of Existence contract
contract ProofOfExistence3 {
    mapping (bytes32 => bool) private proofs;
    // store a proof of existence in the contract state
    function storeProof(bytes32 proof) public {
        proofs[proof] = true;
    }
}
```

```

// calculate and store the proof for a document
function notarize(string document) public {
    bytes32 proof=proofFor(document);
    storeProof(proof);
}
// helper function to get a document's sha256
function proofFor(string document) public pure returns
(bytes32) {
    return sha256(document);
}
// check if a document has been notarized
function checkDocument(string document) public view returns
(bool) {
    bytes32 proof=proofFor(document);
    return hasProof(proof);
}
// returns true if proof is stored
function hasProof(bytes32 proof) public view returns(bool) {
    return proofs[proof];
}
}

```

### Signatur unter einer Transaktion

Jede Transaktion, die einer Blockchain hinzugefügt werden soll, muss zunächst mit dem Private-Key für die entsprechende Blockchain-Adresse m aus der eigenen Wallet ( $GSA_m$ ) des Blockchain-Teilnehmers signiert und an alle Nodes über das P2P-Blockchain-Netzwerk gesendet werden, siehe Abb. 14.7. Alle Nodes sammeln die Transaktionsdaten, damit sie in der Lage sind, einen Block daraus erstellen zu können.

$$s_x = S(H(Daten_1 || \dots || Daten_n), GSA_m))$$

$$\text{Transaktion}_x = \text{Daten}_1 || \dots || \text{Daten}_n || \ddot{\text{OSA}}_m || s_x$$

$s_x$  Signatur der Transaktion<sub>x</sub>

S Signaturfunktion

H One-Way-Hashfunktion

Daten Daten, die zu einer Transaktion gehören (Coins, Programme, Werte, ...)

$GSA_m$  Geheimer Schlüssel aus der Wallet, der die Adresse „m“ zugeordnet ist

$\ddot{\text{OSA}}_m$  Öffentlicher Schlüssel aus der Wallet, der die Adresse „m“ zugeordnet ist

Jede Node im P2P-Blockchain-Netzwerk kann die Identität der Blockchain-Adresse, welche die Transaktion erstellt und abgesendet hat, und den Inhalt der Transaktion verifizieren.

$\ddot{\text{OSA}}_m$  steht in der Transaktion (Öffentlicher Schlüssel der Blockchain-Adresse „m“)

$$\text{Blockchain-Adresse } ,m = f_a(\ddot{\text{OSA}}_m)$$

$f_a$  Funktion zur Berechnung der Blockchain-Adresse

Verifikation, dass die Transaktion des Eigentümers der Blockchain-Adresse „m“, Blockchain-Teilnehmer, signiert worden ist:

$$V(\text{Transaktion}_x, s_x, \text{ÖSA}_m) = \text{true} ?$$

$V$  Verifikationsfunktion

$\text{ÖSA}_m$  Öffentlicher Schlüssel aus der Wallet/Transaktion, ist Blockchain-Adresse „m“ zugeordnet

In Abb. 14.7 wird eine neue und signierte Transaktion  $T_x$  vom entsprechenden Blockchain-Teilnehmer über die Node  $N_4$  über das P2P-Blockchain-Netzwerk an alle Nodes verteilt, die zu dieser Blockchain gehören. Die Nodes, die nicht direkt mit der  $N_4$  verbunden sind, bekommen die Transaktion von einer direkt verbundenen Node weitergeleitet. Alle Nodes speichern diese Transaktion in ihrem Transaktionsspeicher, bis das Konsensfindungsverfahren eine Node bestimmt, die einen neuen Block erstellen soll, siehe Abb. 14.16. Durch diese Verfahren sind im Prinzip alle Nodes in der Lage, einen neuen Block zu verifizieren, zu erstellen und zu verteilen.

Jede Node, die dann den Block anhängen darf, bestimmt, welche Transaktionen in einen neuen Block aus dem Transaktionsspeicher mit aufgenommen werden. Kriterien sind: maximale Größe der Blocks, Transaktionsgebühren usw.

In dieser Zeit gilt die Transaktion noch als pending, das heißt, auch noch nicht als unumkehrbar in der Blockchain verstetigt. In dieser Wartezeit im Transaktionspeicher können die Transaktionen durch eine sogenannte Double-Spend-Transaktion durch den jeweiligen Blockchain-Teilnehmer rückgängig gemacht werden. Double-Spend bedeutet, dass eine Transaktion doppelt gesendet wird und dadurch ungültig wird. Das heißt, um eine Transaktion rückgängig zu machen, kann der Initiator der Transaktion zum Beispiel eine zweite Transaktion mit den gleichen Inputs, die er sich selbst überweist, umsetzen. Wichtig ist, dass diese zweite Transaktion höhere Gebühren haben muss, um sicherzustellen, dass diese Transaktion vor der ursprünglichen ausgeführt wird und somit die ursprüngliche ungültig wird.

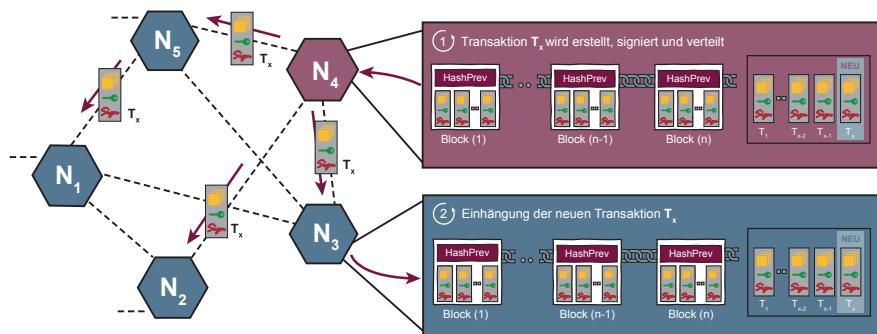


Abb. 14.7 Verteilung der Transaktion P2P-Blockchain-Netzwerk

Statistische Werte von der Bitcoin-Blockchain (April 2018) – <https://blockchain.info/de/charts>.

- ca. 300.000 Transaktionen am Tag
- ca. 3.009.000 Transaktionen, die noch nicht in Blöcken verarbeitet sind (Transaktionsspeicher)
- ca. 1,03 Megabytes Blockgröße
- mehr als 10.000 Nodes im P2P-Bitcoin-Netzwerk
- mehr als 29 Mio. Bitcoin-Konten (Blockchain-Adressen)

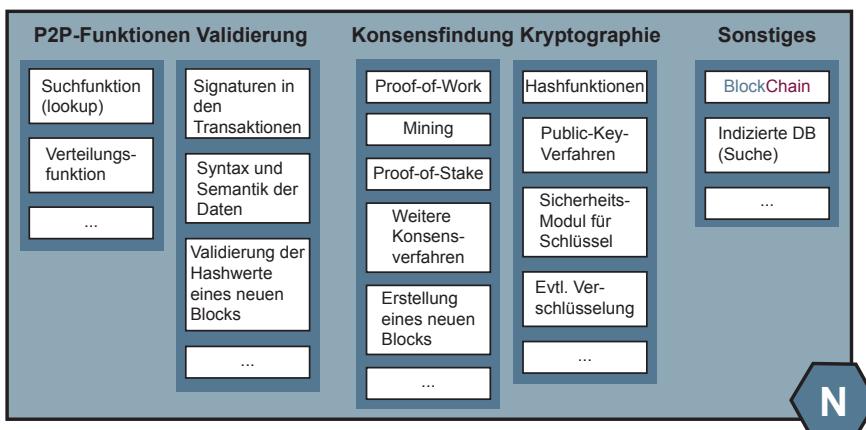
### 14.2.6 Element: Node

Jede Blockchain hat Nodes mit der entsprechenden Blockchain-Technologie, die als Peer-to-Peer-Blockchain-Netzwerk die vielfältigen Mechanismen der Blockchain-Technologie umsetzen. Jede Node hat eine aktuelle Blockchain-Version mit allen Blöcken gespeichert, die fortlaufend erweitert wird. Jede Node, die zu einer bestimmten Blockchain gehört, hat im Prinzip die gleichen Rechte, die Blockchain und neue Transaktionen zu speichern und neue Blöcke hinzuzufügen (validieren). Jede Node kann signierte Transaktionen mit Daten im Peer-to-Peer-Blockchain-Netzwerk verteilen. Die Transaktionen werden mit dem geheimen Schlüssel aus der Wallet von dem entsprechenden Blockchain-Teilnehmer signiert. Die Wallet kann in der Node gespeichert sein, aber auch außerhalb (siehe Abschnitt: [Unterschiedliche Arten von Nodes/Wallets/Entitäten](#)).

Eine Node ist ein Teilnehmer im Peer-to-Peer-Network und Blockchain-Teilnehmer, wenn sie auch Zugriff auf die Wallet hat (Full Node).

#### Architektur und Kommunikations-, Sicherheits- und Vertrauensmechanismen einer Node

In der Node sind sehr unterschiedliche Funktionen vorhanden, die für eine reibungslose, robuste, sichere und vertrauenswürdige Nutzung der Blockchain-Technologie verantwortlich sind, siehe Abb. 14.8.



**Abb. 14.8** Architektur und Kommunikations-, Sicherheits- und Vertrauensmechanismen einer Node

## P2P-Funktionen

Hier sind die Standard-Funktionen vereint, die für den robusten Betrieb eines Peer-to-Peer-Netzwerks notwendig sind. Beispiele sind: Suchfunktion (lookup), Verteilungsfunktion usw.

## Verteilte Validierung

In diesem Funktionsblock sind Validierungsfunktionen vorhanden, die helfen, verteilt eine vertrauenswürde Version der Blockchain auf jeder Node verwalten und verifizieren zu können. Funktionen sind zum Beispiel Überprüfung der Signaturen in den Transaktionen sowie die Syntax und Semantik der Daten und die Validierung der Hashwerte eines neuen Blocks.

## Konsensfindung

Die Konsensfindung stellt Funktionen zur Verfügung, die eine Node auswählt, die für die Erstellung eines nächsten Blocks verantwortlich ist. Funktionen sind Proof-of-Work (Mining), Proof-of-Stake und weitere Konsensverfahren sowie die Erstellung eines neuen Blocks.

## Kryptografie

Mithilfe der Kryptografie-Funktionen werden die Transaktionen gesichert. Funktionen und Mechanismen sind: One-Way-Hashfunktionen, Publik-Key-Verfahren, Hardware-Sicherheitsmodule für die sichere Speicherung von Schlüssel und eventuell Verschlüsselungsverfahren für die Verschlüsselung von Daten.

## Sonstige

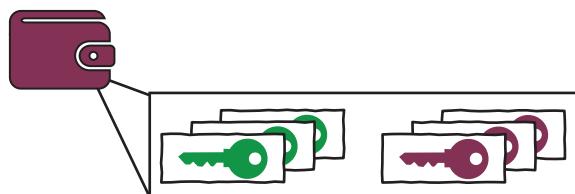
Hier sind weitere Funktionen vereint, die zum Beispiel für die Verwaltung der Blockchain notwendig sind, indizierte Datenbanken und die eigentliche Blockchain.

**Element: Blockchain-Teilnehmer** Der Blockchain-Teilnehmer ist die Instanz, die Transaktionen mithilfe der Schlüssel aus der Wallet signieren kann, weil er die Wallet besitzt oder den Zugriff darauf hat. Der Blockchain-Teilnehmer kann eine Person, aber auch ein IT-System oder ein Prozess in einem IT-System, wie Auto, Payment-System, Produktionssystem usw., sein.

### 14.2.7 Element: Wallet

Eine Wallet ist eine Datenstruktur, in der die geheimen und öffentlichen Schlüssel eines Public-Key-Verfahrens eines Blockchain-Teilnehmers gespeichert sind, siehe Abb. 14.9.

**Abb. 14.9** Inhalte einer Wallet



Aus dem öffentlichen Schlüssel wird mithilfe einer Funktion

$$\text{Blockchain-Adresse} = f_a(\text{öffentlicher Schlüssel})$$

die eindeutige Kennung, die Blockchain-Adresse, berechnet. Mit dem geheimen Schlüssel aus der Wallet wird eine Transaktion von dem entsprechenden Blockchain-Teilnehmer signiert. Der geheime und öffentliche Schlüssel ist der Blockchain-Adresse zugeordnet. Eine Wallet wird von dem Blockchain-Teilnehmer verwendet.

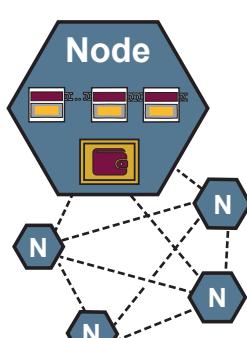
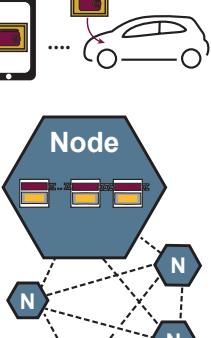
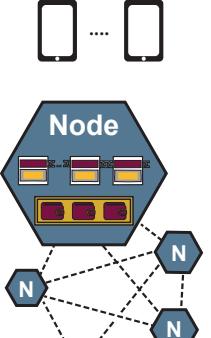
Mithilfe des öffentlichen Schlüssels ist es möglich zu verifizieren, ob Transaktionen von einer bestimmten Blockchain-Adresse („Wallet“) erstellt wurden.

Die grünen Schlüssel-Symbole stellen den öffentlichen Schlüssel und die roten Schlüssel-Symbole den geheimen Schlüssel eines Public-Key-Verfahrens einer bestimmten Blockchain-Adresse dar.

Angriffe auf eine Blockchain passieren sehr häufig auf die Wallet, da mit den geheimen Schlüsseln einfach manipuliert werden kann. Wer den geheimen Schlüssel einer Wallet besitzt, ist in der Lage, gültige Transaktionen zu erstellen und damit zu manipulieren.

Wallets können in verschiedenen Formen existieren beziehungsweise gespeichert werden. Dazu zählt zum Beispiel eine einfache Datei. Es ist aber auch möglich, eine Wallet auf einem Hardware-Sicherheitsmodul, wie zum Beispiel USB-Stick, für Personen oder High-Level-Sicherheitsmodule für Server zu realisieren. Eine weitere Möglichkeit ist es, die Wallet auf einem Papierzettel in Form eines QR-Codes zu halten.

**Struktur: Unterschiedliche Arten von Nodes aus der Sicht der Wallets, Blockchain und Teilnehmer** In der Praxis gibt es unterschiedliche Ausprägungen von Nodes, Wallets und Blockchain-Teilnehmern. Nodes, die die gesamte Blockchain und eine Wallet speichern, werden als „Full Nodes“ bezeichnet, siehe Abb. 14.10.

Verschiedene Arten von Nodes		
		
Abb. 14.10 Full Node	Abb. 14.11 Light Node	Abb. 14.12 Service Node

Für ein portables IT-System, wie zum Beispiel ein Smartphone oder IoT-Geräte wie Autos, ist es allerdings nicht umsetzbar, eine eventuell mehrere Gigabyte große Blockchain zu speichern. Solche Nodes werden auch als „**Light Node**“ bezeichnet, siehe Abb. 14.11.

Sie speichern nur die aktuellen beziehungsweise für sie „relevantesten“ Blöcke, das sind die Blöcke, an denen die Node selber beteiligt ist. Die Wallet ist sicher im IT-System gespeichert, zum Beispiel in einem Hardware-Sicherheitsmodul (HSM).

Zudem gibt es auch noch sogenannte „**Service Nodes**“, welche keine direkten Teilhaber sind. Endgeräte, wie Smartphones, nutzen einen Dienst, der virtuelle Wallets anbietet. Die Aktivierung der Dienste muss bei den Service Nodes sicher umgesetzt werden, um Missbrauch zu vermeiden, siehe Abb. 14.12.

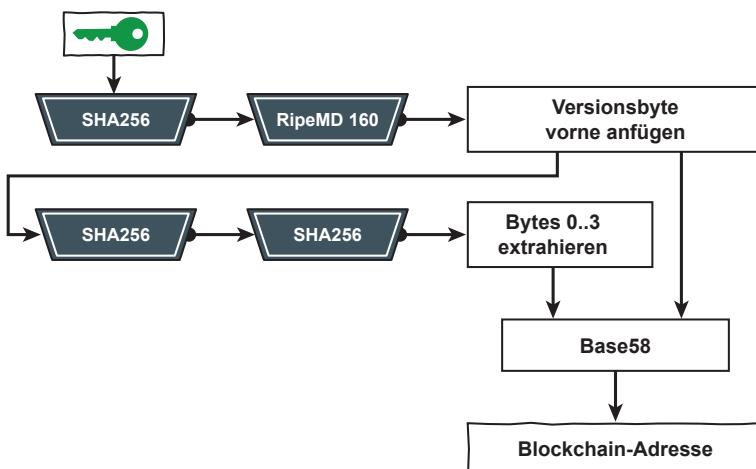
#### 14.2.8 Element: Blockchain-Adresse

Die Blockchain-Adresse wird über den verwendeten öffentlichen Schlüssel, der in der Wallet und in jeder Transaktion steht, repräsentiert. Aus dem öffentlichen Schlüssel wird mithilfe einer Blockchain-Adress-Funktion – Blockchain-Adresse =  $f_a$  (öffentlicher Schlüssel) – die eindeutige Kennung, Blockchain-Adresse, berechnet. Die Blockchain-Adresse wird auch Decentralized Identifier (DID) genannt.

##### Berechnung der Blockchain-Adresse

Die Blockchain-Adresse bei Bitcoin wird wie folgt berechnet, siehe Abb. 14.13.

$$\text{Blockchain-Adresse} = f_a \text{ (öffentlicher Schlüssel)}$$



**Abb. 14.13** Berechnungsfunktion einer Bitcoin Blockchain-Adresse mit dem öffentlichen Schlüssel

Durch die Art und Weise, wie die Blockchain-Adressen berechnet werden, sind sie im Prinzip pseudonym. Solange die Blockchain-Adresse und der öffentlicher Schlüssel nicht einem Blockchain-Teilnehmer zugeordnet werden können, ist es nicht möglich, diesen zu identifizieren.

Die Pseudonymität wird dann aufgehoben, wenn eine Transaktion einem Blockchain-Teilnehmer zugeordnet werden kann. Ein Beispiel ist die Schnittstelle zu Zahlungssystemen. Immer wenn Geld von einem Bitcoin-Konto auf ein Giro-Konto oder umgekehrt transferiert wird, wird deutlich, wem ein Bitcoin-Konto (Blockchain-Adresse) gehört.

Aber auch die Darstellung eines Bitcoin-Kontos auf einer Webseite stellt einen Zusammenhang zum Eigentümer her.

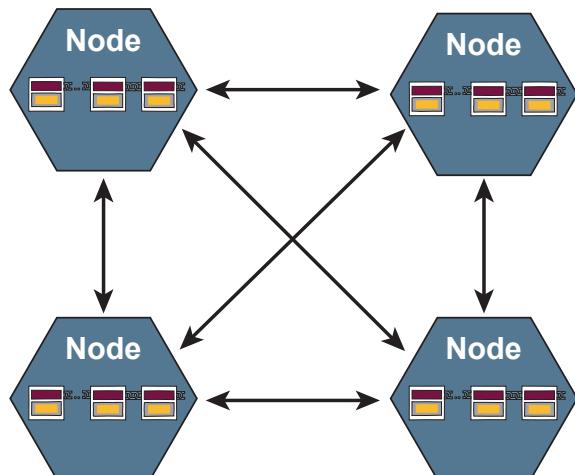
### Beispiel einer Kontonummer/Bitcoin-Adresse des Instituts für Internet-Sicherheit

„1Fm3bsHACJJ7DtC3qE7D9u2EcWV7JVeJdt“

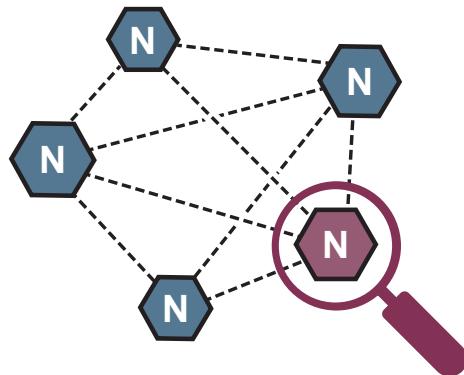
#### 14.2.9 Prinzip: Keine „zentrale Instanz“

Bei der Nutzung einer Blockchain-Technologie gibt es keine „zentrale Instanz“, sondern es sind verschiedene Cyber-Sicherheits- und Vertrauenswürdigkeitsmechanismen auf all ihren Nodes in einem Peer-to-Peer-Blockchain-Netzwerk verteilt. Jeder kommuniziert über das Internet direkt miteinander. Damit gibt es keinen „Single Point of Failure“ mehr und Logs beziehungsweise Back-ups müssen nicht besonders berücksichtigt werden, da die Datenstruktur sich selbst regeneriert. Durch das Peer-to-Peer-Blockchain-Netzwerk und die verteilten Nodes mit der Blockchain ist eine hohe Robustheit sowie die Redundanz der Daten vorhanden, weil jede Node eine Blockchain-Version gespeichert hat, siehe Abb. 14.14.

**Abb. 14.14** Blockchain Peer-to-Peer-Netzwerk



**Abb. 14.15** Auswahl einer Node mithilfe eines Konsensfindungsverfahrens



#### 14.2.10 Konsensfindungsverfahren

Damit ein neuer Block in die Blockchain aufgenommen werden kann, muss dieser zuerst validiert werden. Es muss sichergestellt werden, dass sämtliche darin enthaltenen Transaktionen echt und nicht manipuliert worden sind.

Da beim Blockchain-Konzept keine zentrale Instanz existiert, die einen neuen Block validieren kann, werden verteilte Konsensfindungs- und Validierungsverfahren benötigt, die helfen, diese Aufgabe sicher und vertrauenswürdig umsetzen zu können.

Das Konsensfindungsverfahren ist dazu da, dass ein Konsens gefunden wird und sich untereinander auf einen „korrekten“ Zustand geeinigt wird.

Das Konsensfindungsverfahren hat dabei die Aufgabe, aus dem Peer-to-Peer-Blockchain-Netzwerk eine Node auszuwählen, die als nächstes aus den gesammelten Transaktionen diejenigen heraussuchen darf, aus denen ein neuer Block zusammengestellt, validiert und der Blockchain hinzufügt werden soll, siehe Abb. 14.15.

Jede Transaktion wird vom Blockchain-Teilnehmer signiert, der für die Daten verantwortlich ist und über die Nodes per Peer-to-Peer-Blockchain-Netzwerk verteilt. Das heißt, im Prinzip hat jede Node alle Transaktionen und kann einen neuen Block erstellen.

Ein Konsensfindungsverfahren bestimmt, welche Node konkret als nächstes einen neuen Block erstellen, validieren und verteilen darf. Dabei entscheidet dann die ausgewählte Node anhand von Kriterien, wie Länge, Transaktionsgebühren usw., welche Transaktionen aus dem Transaktionsspeicher in einem neuen Block aufgenommen werden.

#### Verteilte Validierung und Hinzufügen eines neuen Blocks

Die ausgewählte Node nimmt nur die Transaktionen in einen neuen Block auf, die von Semantik und Syntax her richtig sind und die digitalen Signaturen der Blockchain-Teilnehmer der Transaktionen, die mit der Blockchain-Adresse übereinstimmen, siehe Abb. 14.16.

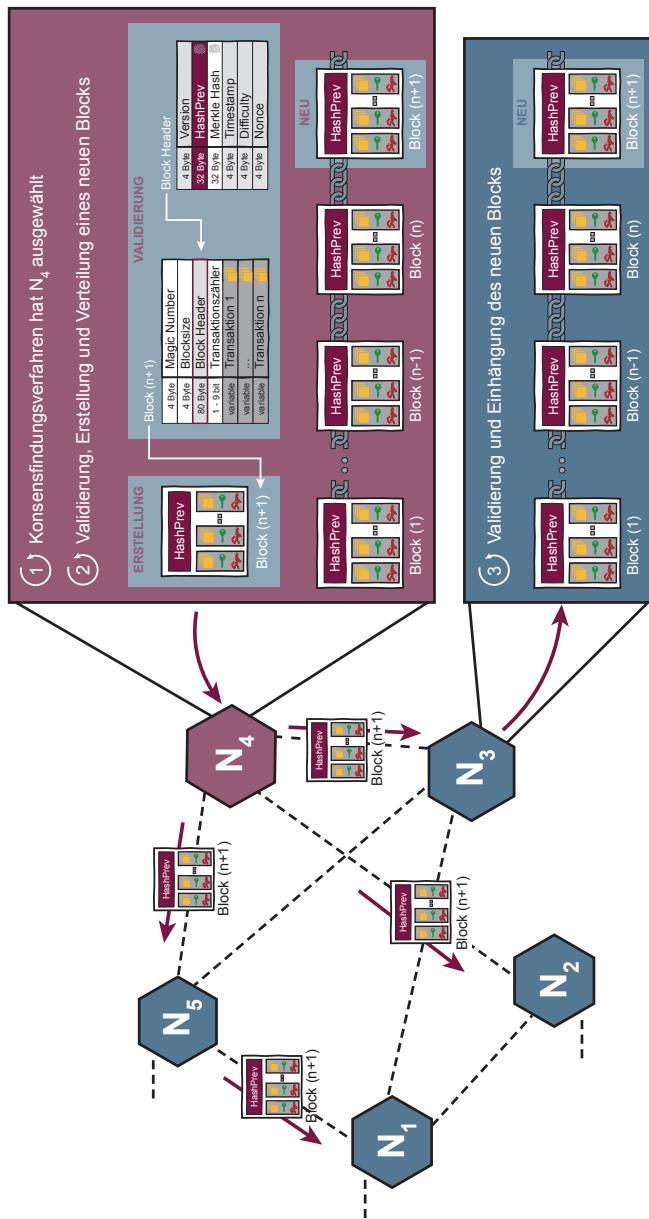


Abb. 14.16 Erstellung und Validierung eines neuen Blocks

Wenn alle Transaktionen in Ordnung sind, wird mit diesen ein neuer Block mit HashPrev, Merkle Hash usw. generiert und an alle anderen Nodes des entsprechenden Peer-to-Peer-Blockchain-Netzwerkes verteilt. Jede Node hat dadurch jederzeit eine vollständige Version der aktuell gültigen Blockchain.

Alle Nodes des Peer-to-Peer-Blockchain-Netzwerkes überprüfen die empfangenen neuen Blöcke der ausgewählten Nodes, ehe sie diese der eigenen Blockchain-Version hinzufügen. Dafür kontrollieren sie sämtliche im Block enthaltenen Transaktionen. Außerdem kontrollieren sie den Block selbst darauf, ob zum Beispiel der Proof-of-Work erbracht ist und ob die Hashwerte korrekt sind. Sobald ein Block oder auch nur eine einzige in dem Block enthaltene Transaktion eine der Regeln verletzt, wird der Block abgelehnt und nicht in die Blockchain der eigenen Version aufgenommen. Das geschieht selbst dann, wenn jede andere Node der Blockchain den Block für zulässig hält. Es ist essentiell für die Sicherheit und Vertrauenswürdigkeit der Blockchain, dass sich alle Nodes ihr Urteil selbst bilden.

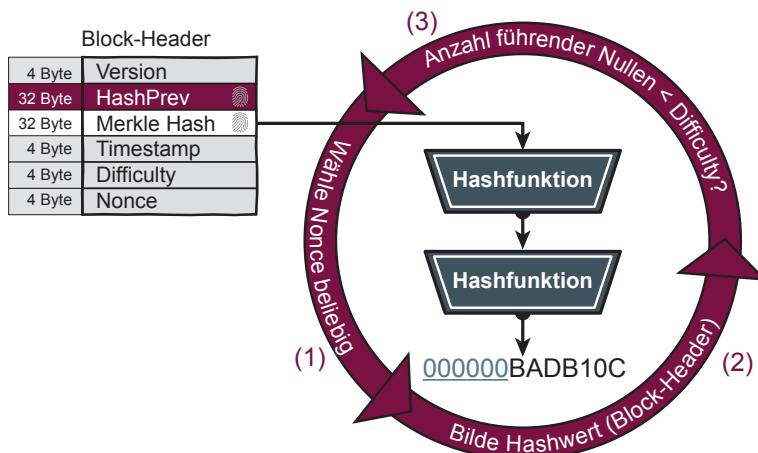
Dieses Prinzip des Distributed Consensus macht die Konsistenzprüfung der Transaktionen vollkommen unabhängig von einer einzelnen vertrauenswürdigen Instanz. Für die Herstellung des Konsenses gibt es verschiedene Verfahren zwischen den Nodes, die festlegen, wer für den Abschluss neuer Transaktionen und das Hinzufügen eines bestimmten Blocks an die Blockchain verantwortlich ist.

### **1. Proof-of-Work-Konsensfindungsverfahren**

Proof-of-Work (PoW) war die erste und ist die aktuell gebräuchlichste Methode zur Konsensfindung und wird zum Beispiel aktuell von der Bitcoin-Blockchain genutzt.

Hier konkurrieren die einzelnen Nodes als sogenannte „Miner“ untereinander, indem sie jeweils ein mathematisches Problem – dessen Schwierigkeit sich dynamisch ändert – lösen müssen. Jeder Miner einer Node muss einen Hashwert für einen Block finden, der einem bestimmten vorgegebenen Muster entspricht. Dieses Muster wird vom Blockchain-Netzwerk eigenständig festgelegt, wobei sich die Schwierigkeit mit der Anzahl der vorgegebenen Stellen des Musters erhöht. Zum Beispiel soll ein Hashwert fünf führende Nullen als Muster besitzen, siehe Difficulty-Feld im Block-Header in Abb. 14.17.

Die einzige Möglichkeit für die Nodes, diesen speziellen Hashwert zu erzeugen, ist die Veränderung des NONCE-Wertes im Block-Header. Somit wird die Konsensfindung eines Blockes zu einem Glücksspiel für die Miner in einer Node, da diese nun einen NONCE-Wert für diesen Block-Header finden müssen, der die Eigenschaften des zu suchenden Hashwertes ergibt. Der Miner, der dieses Problem als erstes gelöst hat, darf den nächsten Block an die Blockchain anhängen. Die Komplexität des Problems wird in der Praxis bei der Bitcoin-Blockchain so gewählt, dass die Aufgabe im Schnitt 10 min dauern soll. Das bedeutet, dass die Transaktionen nur alle 10 min in einem Block der Blockchain hinzugefügt werden und gültig sind.



**Abb. 14.17** Mining (Proof-of-Work)

### Ablauf des Minings

1. Alle Miner generieren eine Nonce (Zufallszahl).
2. Diese Zufallszahl mit allen weiteren Daten im Block-Header wird als Input von Hashfunktionen berechnet.
3. Es wird dann überprüft, ob der berechnete Hashwert den Kriterien vom Feld Difficult (bestimmte Anzahl von führenden Nullen) im Block-Header entspricht.  
Wenn ja, hat der entsprechende Miner gewonnen.  
Wenn nein, wird eine neue Zufallszahl generiert und ein neuer Versuch gestartet.

Es kann passieren, dass zwei Miner zur gleichen Zeit den notwendigen Hashwert berechnen!

Wenn die Nonce 32 Bit lang ist, gibt es  $2^{32}$  verschiedene Kombinationen (42.949.667.296).

Die Berechnung des mathematischen Problems beim Proof-of-Work-Konsensfindungsverfahren kostet sehr viel Energie. Bei Bitcoin werden pro Tag Stromkosten von 2,8 Mio. US\$ verbraucht, 1,3 GW, das sind ca. 10 US\$ pro Transaktion (Anfang 2018).

### Randbedingungen beim Mining

Solange eine Node nicht die Mehrheit an Miner-Kapazitäten besitzt (mehr als 50 %), ist das Mining-Prinzip robust und praktisch nicht zu kompromittieren.

Es ist jedoch anzumerken, dass eine sogenannte Double-Spending-Attacke auch mit weniger Mining-Kapazität probiert werden kann, die Wahrscheinlichkeit eines Erfolges ist bei einer Kapazität von weniger als 50 % jedoch sehr

unwahrscheinlich. Gleichermassen ist der Besitz der Mehrheit der Mining-Kapazität jedoch auch kein Garant dafür, dass ein solcher Angriff sicher funktioniert.

### Double-Spending-Attacke

Bei der Blockchain-Technologie gibt es die Longest Chain Rule. Es ist möglich, dass zwei Miner zeitgleich eine Lösung für die Proof-of-Work Herausforderung finden und daher jeweils ihren Block an die Blockchain anhängen. In diesem Fall entsteht eine Fork. Bei einer Fork teilt sich die Blockchain in zwei Teile (Pfade). Eine Strategie damit umzugehen ist die, dass Nodes die längste Blockchain auswählen, sodass keine Probleme entstehen und nicht weiter verfolgte Forks (Pfade) einfach vernachlässigt werden, siehe Abb. 14.18.

### Longest Chain Rule

Die „weißen“ Blöcke stellen den aktuellen Stand der Blockchain dar. Die „lila“ Blöcke sind vernachlässigte Blöcke, die nicht weiter verfolgt wurden, weil es eine längere Blockchain (Pfad) gab, die stattdessen fortgeführt wurde.

Ein Angreifer mit mehr als 50 % Mining-Kapazität würde statistisch gesehen in einer Mehrheit der Fälle das Recht erlangen, einen neuen Block zur Blockchain hinzuzufügen. Auf diese Weise kann er kontrollieren, welche Transaktionen er zulässt oder nicht. Dies ermöglicht ihm, eine Double-Spending-Attacke durchzuführen.

Der Angreifer (A) könnte zum Beispiel eine legitime Bezahlung für ein Produkt an die Bitcoin-Blockchain-Adresse (B) senden. Sobald diese bestätigt ist und in die Blockchain aufgenommen wurde, erhält er das Produkt. Nebenbei hat der Angreifer einen weiteren Block „gemined“, der seine Bezahlung an B nicht enthält, siehe roter Kasten in Abb. 14.19.

Diesen hält er zurück und „mined“ schon weitere Blöcke, bis er das Produkt erhalten hat. Er kreiert quasi eine private Fork (rote Kästchen). Sobald er hat, was er wollte, wird er diese Fork an das gesamte Netzwerk broadcasten. Hat er genug Blöcke „gemined“, wird seine Blockchain zur longest chain. In dieser gab es nie eine Bezahlung an den Verkäufer und der Angreifer hat sowohl sein Produkt als auch seine Coins noch und eine erfolgreiche Double-Spending-Attacke durchgeführt, siehe Abb. 14.20.

Eine Partei mit mehr als 50 % Mining-Kapazität wäre auch in der Lage, eine Transaktion daran zu hindern, bestätigt zu werden, wenn diese einfach nicht in die Blöcke aufgenommen wird.

### Zeitraum der Validierung

Ein weiteres Problem ist, dass der Zeitraum der Validierung sehr hoch ist. Wenn der Bitcoin-Blockchain-Teilnehmer gerade eine Transaktion signiert hat und über seine Node sendet, wenn ein neuer Block angehängt wurde, dann muss die Transaktion 10 min warten, bis der nächste Block angehängt wird.

Um nicht Opfer einer Double-Spending-Attacke zu werden, wird empfohlen, sechs Blöcke abzuwarten. Dies würde bei einer Bezahlung in einem Geschäft nicht funktionieren, weil Kunden nicht 60 min warten wollen, bis der Verkäufer

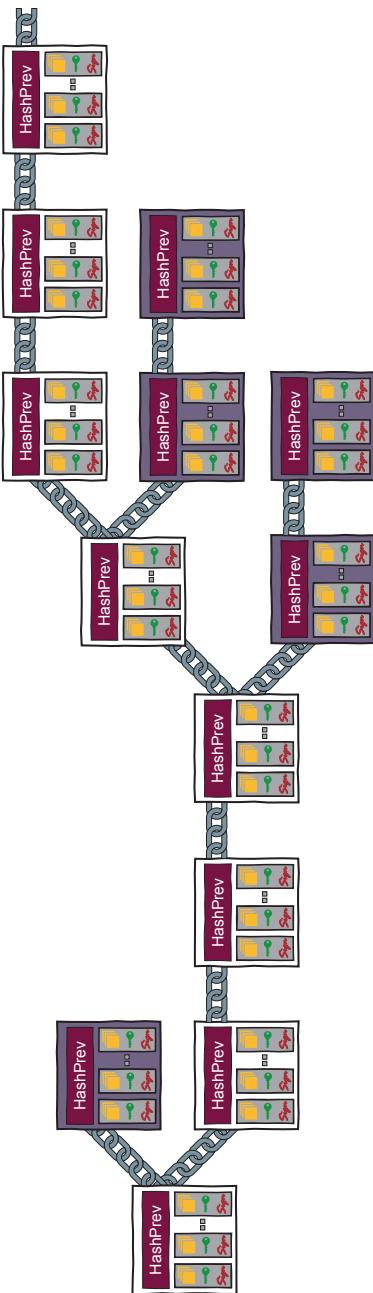
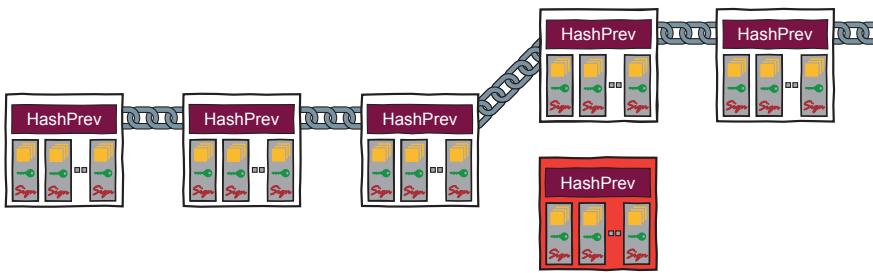


Abb. 14.18 Fork und Longest Chain Rule



**Abb. 14.19** Double-Spending-Attacke

sicher ist, dass die Transaktion, und damit sein Geld, bei ihm nicht mehr veränderbar angekommen ist. Auch wenn das Risiko einer Double-Spending-Attacke eingegangen wird, kann die Ausnahme einer Transaktion in einem neuen Block 10 min dauern.

Dieses Problem existiert bei der Bitcoin-Blockchain-Technologie. Die Ethereum-Blockchain-Technologie nutzt auch ein Proof-of-Work-Konsensfindungsverfahren, aber hier wird alle 15 s ein neuer Block erzeugt. Bei der Ethereum-Blockchain-Technologie wird empfohlen, 12 Confirmations abzuwarten, was auf eine Wartezeit von ca. 3 min hinausläuft. Die Transaktionszeit ist auch hier nicht ideal, allerdings geht es auch mit PoW deutlich schneller als bei der Bitcoin-Blockchain-Technologie.

### Bewertung

Das Proof-of-Work-Konsensfindungsverfahren ist ein bewährtes Verfahren, robust und sicher. Es skaliert aber schlecht und mit dem Erfolg einher geht ein stetig steigender Rechenaufwand und Energieverbrauch.

**2. Proof-of-Stake-Konsensfindungsverfahren** Bei dieser Methode der Konsensfindung wird die Node gewählt, die die meisten Anteile an Blöcken einer Blockchain hinzugefügt hat. Dieses Verfahren beseitigt einige Sicherheitslücken, die bei Proof-of-Work-Problemen vorhanden sind. Es ist zum Beispiel für einen Angreifer nicht mehr möglich, eine beliebige Anzahl an „Pseudo Miners“, die falsche Blöcke als richtig validieren, dem Netzwerk ungesehen hinzuzufügen. Zudem hätte die Node mit den meisten Coins, oder generell mit den höchsten Werten, das größte Interesse an einer stabilen und sicheren Blockchain. Zudem müsste ein Angreifer erst einmal so viele Coins besitzen, dass er Blöcke erstellen darf. Mit einer Attacke würde er sich also im Grunde selbst angreifen. Da der Konsensmechanismus sehr auf „Vertrauen“ basiert, wird dieses Verfahren eher bei privaten Blockchains genutzt (siehe Abschn. 14.2.11).

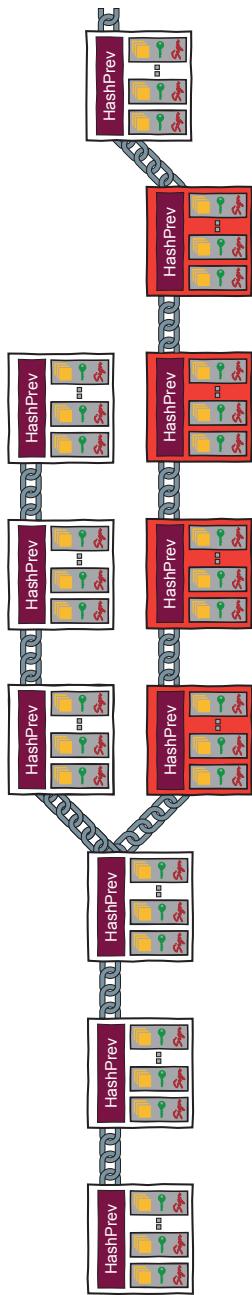


Abb. 14.20 Erfolgreiche Double-Spending-Attacke

## Bewertung

Proof-of-Stake ist die zurzeit vielversprechendste Alternative für Blockchains. Es gibt keine Probleme bei der Skalierbarkeit und das Verfahren hat einen geringen Energieverbrauch.

Proof-of-Stake ist allerdings noch nicht so lange erprobt.

**3. Alternative Konsensfindungsverfahren** Neben den beiden Grundmethoden gibt es noch weitere, sich aktuell in der Probephase befindliche Methoden zur Konsensfindung. Ein Verfahren ist das sogenannte „Byzantine Fault Tolerance“-Verfahren, das eigentlich zur Ermittlung von defekten Sensoren genutzt wird. Damit soll ermittelt werden, welche Node in einer Blockchain versucht, kompromittierte Blöcke an die Blockchain anzuhängen.

Practical Byzantine Fault Tolerance (PBFT) ist ein Verfahren zur Lösung dieses Problems; ein Konsensfindungsverfahren, das beispielsweise in der Hyperledger Fabric Blockchain Anwendung findet.

Hier gibt es eine ausgewählte Gruppe an „Validating Peers“, die alle Transaktionen erhalten. Sie wählen anschließend untereinander einen „Leader“ aus, dieser gibt eine genaue Reihenfolge der Transaktionen vor, in der diese in den Block eingefügt werden. Diese wird von ihm wiederum an alle „Validating Peers“ broadcasted. Anschließend führt jeder „Validating Peer“ sämtliche Transaktionen in dem Block in der vorgegebenen Reihenfolge aus und berechnet anschließend den Hashwert. Dieses Ergebnis wird wiederum an die anderen „Validating Peers“ broadcasted und mit deren Ergebnissen verglichen. Wenn mehr als 2/3 der anderen Peers dasselbe Ergebnis haben, wird der Block endgültig zur lokalen Kopie der Blockchain verstetigt.

### 14.2.11 Struktur: Berechtigungsarchitektur

Eine Blockchain kann sowohl für jeden zugänglich, als auch nur für bestimmte Blockchain-Teilnehmer über Nodes der entsprechenden Blockchain einsehbar und nutzbar sein. Es wird zwischen den Zugriffsberechtigungen der Nutzung einer Blockchain und der Validierungsberechtigung von Nodes, Blöcke hinzuzufügen, unterschieden, siehe Abb. 14.21.

		Validierung	
		Permissionless	Permissioned
Zugriff	Public	Jeder darf <b>lesen</b> und <b>validieren</b> .	Jeder darf <b>lesen</b> , nur Berechtigte <b>validieren</b> .
	Private	Nur Berechtigte dürfen <b>lesen</b> , jeder darf <b>validieren</b> .	Nur Berechtigte dürfen <b>lesen</b> und <b>validieren</b> .

Abb. 14.21 Berechtigungsarchitektur

Bei den Zugriffbeschränkungen wird festgesetzt, wer überhaupt auf eine Blockchain zugreifen darf. Bei einer „Public-Blockchain“ darf jeder Blockchain-Teilnehmer uneingeschränkt die Blockchain der entsprechenden Nodes nutzen. Bei einer „Private-Blockchain“ dürfen nur klar definierte Blockchain-Teilnehmer auf die entsprechenden Blockchains einer Node zugreifen.

Die Validierungsberechtigungen sagen dagegen aus, welche Nodes Blöcke einer Blockchain hinzufügen dürfen. Auf „Permissioned-Blockchains“ dürfen nur bestimmte Nodes einfügen, wohingegen auf „Permissionless-Blockchains“ alle Nodes Blöcke einfügen dürfen, wenn sie ausgewählt wurden.

**Public permissionless** Diese Struktur ist die zurzeit am besten erprobte Blockchain-Struktur. Eine solche Blockchain kann jeder Blockchain-Teilnehmer einsehen und auch jede Node im Prinzip Blöcke hinzufügen. Dabei ist die Identität des Blockchain-Teilnehmers, welche die Blockchain einsieht und/oder Identität der Nodes die Blöcke dieser Blockchain hinzugefügt hat, nicht mehr nachzuweisen. Dieses Modell wird unter anderem für die Blockchain der Kryptowährung Bitcoin verwendet. Hier kann jeder von der Blockchain lesen und jede Node als Miner Blöcke der Blockchain hinzufügen, wenn sie die Challenge gewinnt.

**Private permissionless** Diese Art der Blockchain verpflichtet die Blockchain-Teilnehmer einer Node, sich zunächst zu registrieren, um Zugriff auf die eigentliche Blockchain zu erlangen. Es kann jedoch jede registrierte Node Blöcke zu der Blockchain hinzufügen. Diese Art der Blockchain ist die am wenigsten genutzte Art.

**Private permissioned** Die restriktivste Blockchain-Variante ist eine private permissioned Blockchain, die nicht öffentlich lesbar und auch nicht für alle Nodes beschreibbar ist. Die einzelnen Blöcke dürfen nur die Blockchain-Teilnehmer einsehen, die dazu berechtigte sind. Ansonsten ist es unmöglich für außenstehende Blockchain-Teilnehmer, die Blockchain auf den entsprechenden Nodes einzusehen. Dieses mehr lokalisierte Modell eignet sich vor allem für Unternehmen, die die Vorteile der Blockchain nutzen wollen, jedoch keine öffentliche Einsicht in ihre Transaktionen beziehungsweise Daten geben möchten.

Zum Beispiel möchte eine Bank nicht unbedingt, dass die gesamten Transaktionsdaten ihrer Kunden für jeden (auch für Nicht-Kunden der Bank) öffentlich einsehbar sind. Zudem besitzt eine Bank immer noch eine „zentrale Instanz“ und überlässt das Verifizieren und Hinzufügen von Blöcken lieber den eigenen Nodes, denen sie mehr vertrauen kann, als anderen Nodes, welche zu den Kunden gehören.

Ein weiteres Beispiel für eine private permissioned Blockchain ist „sovrin“.

**Public permissioned** Bei einer solchen Blockchain sind die Blöcke zwar für jeden einsehbar, allerdings haben nur durch Nodes ausgewählte Organisationen das

Recht, Blöcke der Blockchain hinzuzufügen. Dabei wird die Wahl zur vertrauenswürdigen Node nicht dauerhaft festgelegt, allerdings muss deutlich klar sein, warum gerade diese Node zur vertrauenswürdigen Node gewählt wurde. Da in der Regel den Nodes vertraut wird, werden zur Konsensfindung Verfahren wie zum Beispiel das „Practical Byzantine Fault Tolerance (PBFT)“-Verfahren genutzt. Mit PBFT können mehrere tausend Transaktionen in der Sekunde verarbeitet werden. Allerdings ist eine permissioned Blockchain erforderlich, darüber hinaus steigt der Overhead sehr stark mit zunehmender Anzahl an „Validating Peers“.

Wird eine Node als kompromittiert angemahnt, so gibt es eine Gruppe an Entscheidern, die die Node überprüfen und darüber entscheiden, ob der Block, den diese Node einfügen möchte, kompromittiert ist oder nicht. Diese „Entscheider“ werden „Konsortium“ („Consortium“) genannt, weswegen eine solche Blockchain auch als „Consortium Chain“ bezeichnet wird.

**Wichtig** Die Berechtigungsarchitektur entscheidet darüber, wer lesen und validieren darf.

---

### 14.3 Hard und Soft Forks von Blockchains

Bei der Blockchain-Technologie erweist sich das Aktualisieren als deutlich komplizierter als bei herkömmlichen Softwaresystemen. Bei herkömmlichen Softwaresystemen wird ein Update von einer zentralen Stelle eingespielt. Bei der verteilten Blockchain-Technologie müssen sich die einzelnen Nodes einig werden.

Im Prinzip gibt es zwei Möglichkeiten, bei der Blockchain-Technologie mit einem Update umzugehen. Dabei kommt es darauf an, welche Änderungen in dem jeweiligen Update vorgenommen werden und wie umfangreich diese sind. Der Vorgang wird bei der Blockchain-Technologie „Fork“ (Teilung, Gabelung oder Verzweigung) genannt.

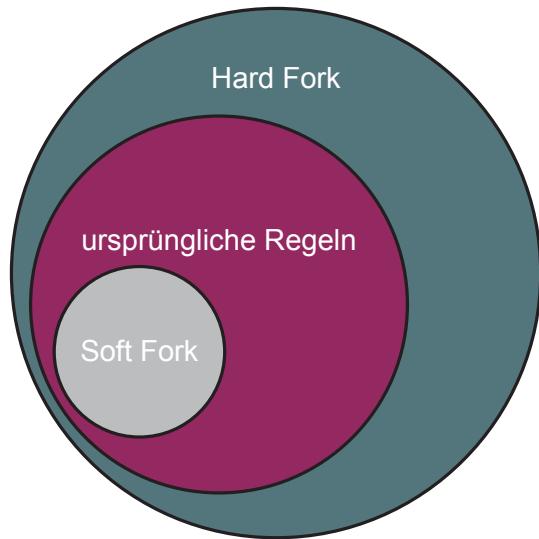
Eine sogenannte Fork kann geschehen, sobald irgendjemand eine neue Version der Blockchain-Technologie präsentiert. Entscheidet sich nun ein Großteil der Nodes einer bestimmten Blockchain-Technologie dafür, auf diese neue Version upzudaten, so tritt eine Fork ein und die Blockchain spaltet sich.

Ob diese Fork mit der ursprünglichen Blockchain-Technologie vorwärts-kompatibel ist oder nicht, ist maßgebend dafür, ob es sich um eine „Soft Fork“ oder eine „Hard Fork“ handelt, siehe Abb. 14.22.

#### Soft Fork

Bei einer Soft Fork handelt es sich um eine vorwärtskompatible Veränderung. Die Regeln der Blockchain-Technologie werden verschärft [2]. Bei einer „Soft Fork“ werden keine neuen Regeln aufgestellt, die dazu führen, dass Blöcke, die bisher

**Abb. 14.22** Darstellung der Regeländerung einer Soft und einer Hard Fork



nicht akzeptiert wurden, jetzt akzeptiert werden. Stattdessen werden Regeln nur dahin gehend geändert, dass Blöcke, die bisher vielleicht noch akzeptiert wurden, nun nicht mehr gültig sind.

Es kommt bei einer „Soft Fork“ also zu keinen Kompatibilitätsproblemen. Nodes, die noch die alte Version verwenden, werden trotzdem sämtliche Transaktionen der neuen Nodes akzeptieren. Dies ist der Fall, weil keine Regeln aufgestellt werden, die mit den alten in Konflikt stehen. Anders herum werden die Nodes, die die neue Version betreiben, allerdings nicht alle Transaktionen von alten Nodes akzeptieren. Lediglich die Transaktionen, die mit den neueren, strengereren Regeln konform sind, werden hier akzeptiert. Eine Koexistenz von Nodes, die alte und neue Regeln betreiben, ist folglich möglich, ohne dass ein Teil der Nodes vollkommen zurückbleibt.

**Wichtig** Bei einer Soft Fork werden die ursprünglichen Regeln eingeschränkt. Alte Versionen von Nodes werden weiterhin sämtliche Transaktionen der neuen Nodes akzeptieren.

### Beispiel: Soft Fork

Auch Nodes, die noch kein Update hatten, können die neue Blockchain nutzen. Die neuen Regeln werden also auch von alten Nodes akzeptiert. Wird ein Block erstellt, der die alten Regeln befolgt, die neuen jedoch verletzt, so wird dieser Ableger aussterben, da er von den neuen Nodes nicht akzeptiert wird, siehe Abb. 14.23.

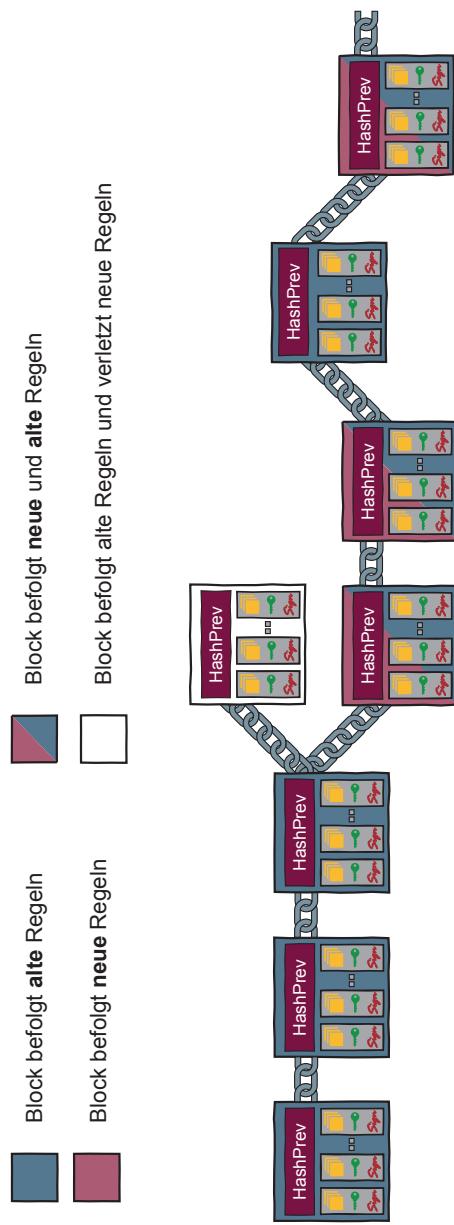


Abb. 14.23 Soft Fork

### Beispiel: Soft Fork BIP66 (2015)

Bei dieser Soft Fork handelte es sich um ein Update, das die Regeln, die die Transaktionssignaturen betreffen, verschärft hat. Danach wurden ausschließlich Signaturen akzeptiert, die DER codiert sind.

Alte Nodes akzeptieren die DER codierten Signaturen selbstverständlich, da diese Nodes Transaktionen, mit allen vorher gültigen Signaturen akzeptieren (DER eingeschlossen).

Nodes, die jedoch schon das Update installiert haben, akzeptieren ausschließlich DER codierte Transaktionen, anders signierte Transaktionen (welche vorher noch gültig waren) werden von neuen Nodes nun abgelehnt.

## 1. Hard Forks

Hard Forks hingegen sind nicht vorwärtskompatibel. Bei einer Hard Fork werden die bisherigen Regeln ausgeweitet [3]. Neue Regeln werden den alten hinzugefügt. Das hat zur Folge, dass Nodes, welche die alte Version verwenden, Transaktionen von einer neuen Node nicht länger akzeptieren werden. Bei einer Hard Fork ist es daher notwendig, dass sämtliche Nodes die bestimmte Blockchain auf die neue Version der Blockchain-Technologie updaten. Andernfalls würde es zu einem Split kommen oder eine der beiden Blockchains wird irrelevant [6].

Eine Koexistenz von Nodes, die die alten und neuen Regeln betreiben, ist hierbei nicht möglich.

Abb. 14.22 verdeutlicht die Veränderung der Regeln bei einer Soft beziehungsweise einer Hard Fork im Vergleich zu den ursprünglichen Regeln.

**Wichtig** Bei einer Hard Fork werden die ursprünglichen Regeln erweitert. Alle Nodes müssen ein Update bekommen oder es kommt zu einem Split.

### Hard Fork (alte Blockchain stirbt aus)

In Abb. 14.24 wird aufgezeigt, wie die alte Blockchain stirbt und eine neue Blockchain entsteht.

Nach und nach bekommen alle Nodes ein Update. Somit werden nur noch Blocks für die neue Blockchain erstellt. Die alte Blockchain wird folglich aussterben. Dazu müssen die Blockchain-Teilnehmer für die neue Blockchain neue Wallets erstellen.

**Organisation des Übergangs zu einer neuen Blockchain**, siehe Abb. 14.25.

1. In einem ersten Schritt werden für alle Blockchain-Adressen ein Snapshot der jeweiligen Guthaben oder entsprechend anderen Assets erstellt.
2. Die Blockchain-Teilnehmer müssen für die neue Blockchain eine neue Wallet mit neuen Public-Key-Schlüsseln und entsprechend neuen Blockchain-Adresse generieren.

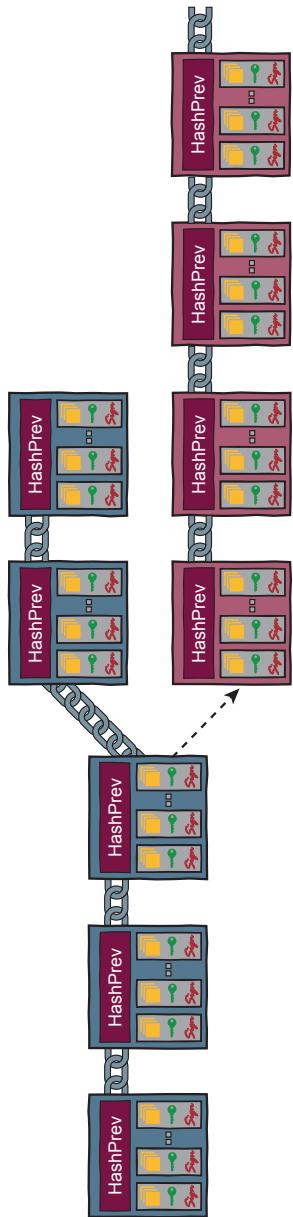


Abb. 14.24 Hard Fork (alte Blockchain stirbt aus)

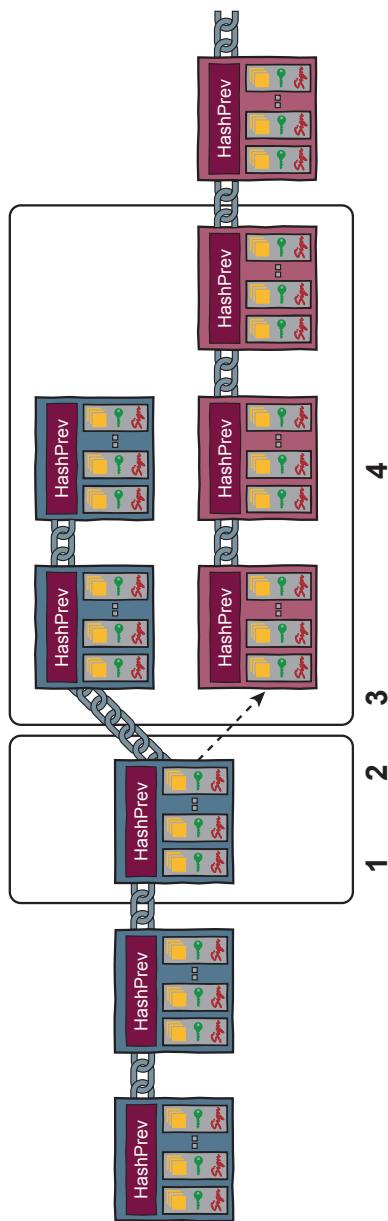


Abb. 14.25 Übergang zu einer neuen Blockchain

3. Die Blockchain-Teilnehmer transferieren die im Snapshot der alten Blockchain festgehaltenen Assets auf die neue Blockchain, in dem dazu eine Transaktion für die neue Blockchain erstellt und mit dem neuen und passenden geheimen Schlüssel für die Blockchain-Adresse signiert wird. Dieser Vorgang kann mit Hilfe eines Smart Contracts unterstützt werden.
4. Die alte Blockchain stirbt aus und die alte Wallet wird unbrauchbar.

Beispiel:

Mit dieser Art des Hard Fork könnte das Prinzip der Europäischen Datenschutzgrundverordnung „Right to be forgotten“ umgesetzt werden. Da nach der Umsetzung der Hard Fork die alte Blockchain nicht mehr gültig ist, kann sie entsprechend auf allen Nodes gelöscht werden.

## 2. Hard Fork (Split)

In Abb. 14.26 wird aufgezeigt, wie ein Split entsteht.

Es wird ein Update von nur einem Teil der Nodes umgesetzt. Die nicht upgedateten Nodes behalten die alten Regeln bei. Dadurch entsteht ein Split und fortan laufen zwei Blockchains parallel zueinander.

**Organisation des Übergangs zu einem Split**, siehe Abb. 14.27.

1. In einem ersten Schritt werden für alle Blockchain-Adressen ein Snapshot der jeweiligen Guthaben oder entsprechend anderen Assets erstellt.
2. Die Blockchain-Teilnehmer müssen für die neue Blockchain eine neue Wallet mit neuen Public-Key-Schlüsseln und entsprechend neuen Blockchain-Adresse generieren.
3. Die Blockchain-Teilnehmer transferieren die im Snapshot der alten Blockchain festgehaltenen Assets auf die neue Blockchain, in dem dazu eine Transaktion für die neue Blockchain erstellt und mit dem neuen und passenden geheimen Schlüssel für die Blockchain-Adresse signiert wird. Dieser Vorgang kann mit Hilfe eines Smart Contracts unterstützt werden.
4. Die alte Blockchain existiert parallel und die Blockchain-Teilnehmer können Transaktionen für beide Blockchains erstellen.

Beispiel:

Bitcoin Cash hat sich im August 2017 von der Bitcoin-Blockchain „abgesplittet“. Bitcoin Cash hat die Blockgröße auf 8 MB erhöht.

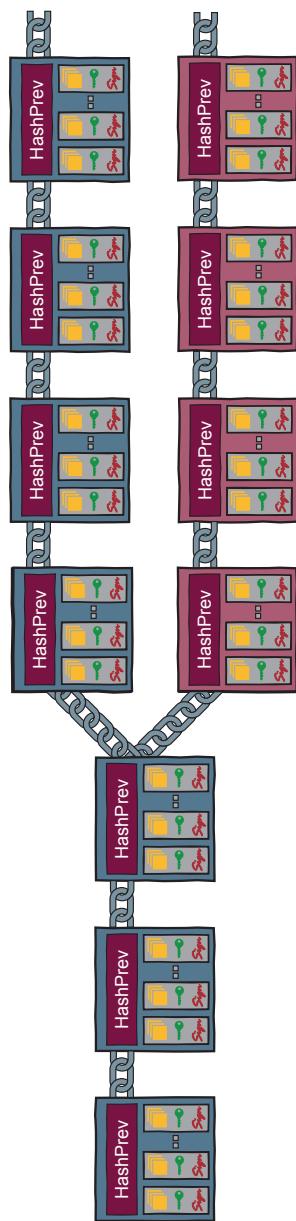


Abb. 14.26 Hard Fork (Split)

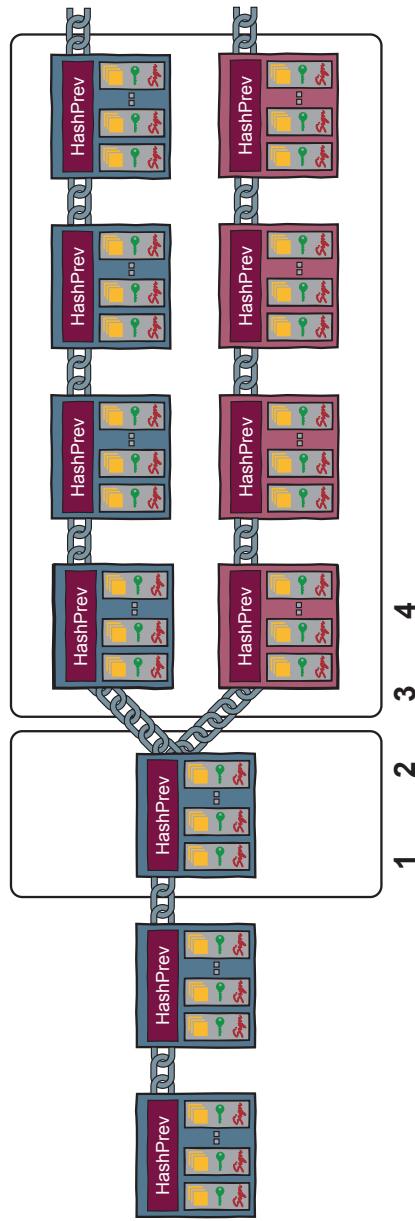


Abb. 14.27 Übergang zu einem Split

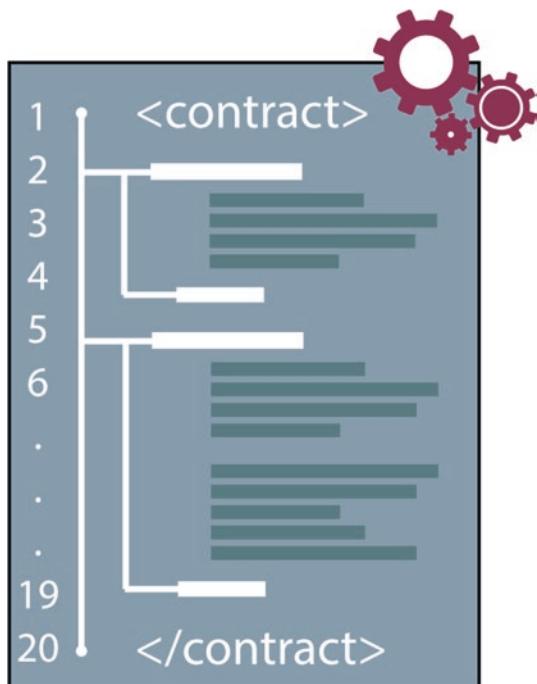
## 14.4 Anwendungsformen und Anwendungen der Blockchain

Mithilfe der Blockchain-Technologien können verschiedene Anwendungsformen und Anwendungen realisiert werden. Im Folgenden werden einige Anwendungsformen exemplarisch dargestellt, um den Nutzen von Blockchain-Technologien zu veranschaulichen [4].

**Anwendungsform „Smart Contracts“** In den Blöcken einer Blockchain lassen sich beliebige Elemente in den Transaktionen speichern. So ist es möglich, Quelltext, ausführbaren Programmcode, abzulegen, der bei einem bestimmten definierten Ereignis ausgeführt wird. Der in einem Block abgelegte Quelltext ist dabei blockchain-charakteristisch unveränderlich. Diese Idee wird auch als „Smart Contracts“ bezeichnet, siehe Abb. 14.28.

Smart Contracts sind Verträge zur automatisierten Umsetzung von Vertragsbedingungen über Programmcode. Damit werden zentrale Instanzen für die Überwachung von Konditionen einer Zusammenarbeit überflüssig. Ein Treuhänder hat bisher die Aufgabe, bei einem Vertrag die Bedingungen, die dieser Vertrag stellt, nachzuprüfen. Soll beispielsweise für den Kauf eines Autos ein Betrag von einem auf das andere Konto fließen, so muss dies ein Treuhänder nachvollziehen, bevor der Schlüssel übergeben werden kann. Durch einen Smart Contract ist es möglich, die

Abb. 14.28 Smart Contracts



Vertragsbedingungen in „Wenn-Dann-Funktionen“ einzuteilen. Wenn zum Beispiel ein Blockchain-Teilnehmer einen bestimmten Betrag auf das Konto eines anderen Blockchain-Teilnehmers überweist, erkennt dies der entsprechende Smart Contract und schaltet beispielsweise den elektronischen Autoschlüssel des Verkäufers für den entsprechenden Käufer frei. Falls es sich bei dem Kauf um ein älteres Auto handelt, wird der Verkäufer per E-Mail darüber informiert, dass sein Auto verkauft wurde. So kann der Verkäufer dem Käufer den Schlüssel des Autos übergeben.

Smart Contracts stellen eine Kontroll- oder Geschäftsregel innerhalb eines technischen Protokolls dar und helfen, die Zusammenarbeit zwischen verschiedenen Organisationen vertrauenswürdig und vor allem automatisiert umzusetzen.

Die Blockchain-Technologie wird in der Integration mit verschiedenen Blockchain-Teilnehmern genutzt, um Prozesse zu automatisieren.

**Kryptowährung „Bitcoin“** Angefangen hatte alles mit der Realisierung der Bitcoin-Kryptowährung, die Banken als dritte Instanz, also als Vermittler zwischen zwei Parteien, überflüssig macht.

### Idee und Verfahren von Bitcoin

Bitcoin ist eine digitale Währung oder Internetwährung, die verteilt, dezentral und unabhängig von einer Zentralbank ein globales Zahlungsnetzwerk zur Verfügung stellt. Die Funktionsweise des Bitcoin-Systems stellt sicher, dass es in ein paar Jahrzehnten maximal 21.000.000 Bitcoins weltweit geben wird. Die Node, die beim Mining gewonnen hat, bekommt 12,5 Bitcoins als Belohnung (Stand 2018). Jede Person (Blockchain-Teilnehmer) hat eine Wallet und der öffentliche Schlüssel entspricht über eine Funktion der Blockchain-Adresse – Blockchain-Adresse =  $f_a$  (öffentliche Schlüssel). Mit dem geheimen Schlüssel aus der Wallet werden Transaktionen signiert, um Guthaben auf diesem Bitcoin-Konto (Blockchain-Adresse) an ein anderes Bitcoin-Konto zu überweisen (public permissionless Blockchain).

Der schwankende Kurs ist ein Grund, warum sich Bitcoin nicht als globales Zahlungssystem im Alltag durchgesetzt hat. Bitcoin ist aber dennoch eine sehr relevante Währung, vergleichbar mit zum Beispiel Gold. Am 07.12.17 um 21:45 Uhr waren ca. 16,65 Mio. Bitcoins vergeben und ein Bitcoin hatte einen Wert von 12.559,45 EUR. Damit sind alle Bitcoin zusammen, das heißt, die Bitcoin-Blockchain, über 209 Mrd. EUR wert.

### Bewertung

Ein besonderer Aspekt bei Bitcoin ist, dass die Coins (Daten) nicht von außen in die Blockchain eingebracht werden, sondern durch das Mining bis zur maximalen Grenze erzeugt werden. Im Prinzip werden die Coins nur zwischen den Kontonummern (Blockchain-Adressen) vertrauenswürdig verschoben. Der Grund für die Verschiebung der Coins zwischen den Blockchain-Teilnehmern liegt außerhalb der Bitcoin-Blockchain: kaufen, spekulieren, verschenken usw.

**Digitale Währung „Utility Settlement Coin“** Die Banken gingen nach dem ersten Schock selbst in die Offensive und stellten Forscherteams zusammen, mit dem Ziel, die Blockchain-Technik für sich selber nutzbar zu machen.

Die Schweizer Bank UBS hat zusammen mit der Deutschen Bank, Santander, BNY Mellon, Icap beispielsweise eine digitale Währung entwickelt, den sogenannten „Utility Settlement Coin“, kurz USC. Zum Einsatz kommt die Währung beim Handel an der Börse mit dem Ziel, Clearinggesellschaften zu ersetzen, die sich bisher um die Geld- und Wertpapiertransfers gekümmert haben. So lassen sich Tage beim Transfer einsparen, da sich Geld und Wertpapiere sofort durch einen neu hinzugefügten Block austauschen lassen. Smart Contracts regeln dabei die automatische Überweisung der USC des Käufers an den Verkäufer. Eine private permissioned Blockchain wird für Wertpapiere und den Transfer von USC eingesetzt. Full Nodes befinden sich bei den Banken, die mit den Wertpapieren handeln. Für Kunden würden Light Nodes infrage kommen, die nur die für den Kunden wichtigen Blöcke mit den entsprechenden Wertpapieren abspeichern.

**Kryptowährung „RSCoin“** Der RSCoin wurde von Forschern für die britische Zentralbank entworfen und ist eine Kryptowährung, die zentral verwaltet werden soll. Die Blockchain ist immer noch dezentral, jedoch weist die Zentralbank das Recht auf Einträge in diese zu – mithilfe von kryptografischen Schlüsseln, anderen Parteien, wie zum Beispiel Geschäftsbanken. Begrenzte Geldmengen, sieben Transaktionen pro Sekunde und das Proof-of-Work-Problem, wie es bei Bitcoin zum Einsatz kommt, fallen weg. Zweitausend Transaktionen pro Sekunde sollen verarbeitet werden. Was bleibt ist die Pseudoanonymität der Teilnehmer. Werden keine zusätzlichen Maßnahmen für den Schutz der Privatsphäre getroffen, entsteht ein transparenter Teilnehmer, dessen Transaktionen immer und überall nachverfolgt werden können. Zudem ist, wie bei der Schweizer Bank UBS, eine private permissioned Blockchain vorstellbar, damit nicht in bestehende Transaktionen eingesehen werden kann. Andere Parteien, die die Blockchain verändern wollen, können Light Nodes oder Service Nodes einrichten. Im Bereich rund um die Bezahlung von Dienstleistungen, Inhalten und Rohstoffen werden ebenfalls Überlegungen und Lösungen präsentiert.

**Kryptowährung: Weitere Ideen** Das Start-up-Unternehmen Pey möchte Firmen auf einfacherem Wege ermöglichen, ihren Mitarbeitern Teile des Gehalts in Bitcoin auszuzahlen. Pey arbeitet mit dem Dienst „PayrollAPI“ von Bitpay, der den Umtausch von Euro in Bitcoin und die Auszahlung an die Arbeitnehmer übernimmt. Das Geschäftsmodell sieht vor, die Nutzung zunächst kostenlos anzubieten und später eine Gebühr von einem Euro pro Mitarbeiter pro Monat einzuführen. Die Mitarbeiter müssen sich zunächst auf der Pey-Plattform anmelden und den Wert, den sie von ihrem Gehalt umwandeln wollen, eintragen.

Ein Ärgernis für Inhalte-Anbieter sind Ad-Blocker. Viele finanzieren sich durch die auf ihrer Seite gezeigte Werbung. Für Ad-Block-Nutzer, aber auch um mit den bereitgestellten Informationen Geld zu verdienen, gibt es Paywalls. Gegen Bezahlung wird ein Inhalt für den Leser freigegeben. Das deutsche

Bitcoin-Startup „Satoshipay“ möchte die Zahlung für Paywalls leichter machen. An den Browser wird ein Online-Wallet angedockt, worüber die Inhalte mit einem Klick bezahlt werden. Den Dienst von Satoshipay zahlt der Inhalte-Anbieter mit 10 % seines Verdienstes. Gefördert wird das Start-up von Axel Springer und Visa. Das Wallet soll zukünftig auch mit der Visa-Karte aufgeladen werden können. Zudem sind Bezahlungen in die andere Richtung geplant, das heißt, der Anbieter zahlt seinen Nutzern für die Teilnahme an Umfragen oder Tests Geld.

Große Energiekonzerne wie RWE wollen gleich mehrere Probleme mit der Blockchain-Technologie lösen. Hier gibt es zum einen noch kein einheitliches Bezahlungssystem für das Aufladen von E-Autos, und zum anderen ist die Reichweite dieser im Vergleich zu Autos mit Verbrennungsmotoren geringer.

Ladesäulen werden von verschiedenen Energiekonzernen angeboten. Jedes Unternehmen hat eine andere Art der Bezahlung. Bei längeren Fahrten, bei denen öfter an einer Ladestation Halt gemacht werden muss, ist es also schwierig, eine Säule passend zum eigenen Bezahlungssystem zu finden. RWE arbeitet an einer auf einer Blockchain basierten Lösung mittels Smart Contracts. Ladesäulen sollen nur noch mit dem Auto kommunizieren und die Bezahlung automatisch abwickeln. Diese Entwicklung würde RWE auch bei einem anderen Projekt helfen. Micropayments sind Bezahlungen zum Beispiel im Cent-Bereich und sind in großen Massen sehr aufwendig und teuer. Durch Smart Contracts wäre dies wiederum einfach und schnell. Micropayment kann genutzt werden, um Ladungen an Ampeln für E-Autos zu ermöglichen, wie RWE es für die Zukunft plant. Dadurch würde auch die Reichweite von E-Autos verbessert, da die Aufladung automatisch und problemlos während der Rotphase an einer Ampel geschieht und so weite Strecken zurückgelegt werden können.

Da es unsinnig ist, eine komplette Blockchain in einem Auto zu speichern, sind treffende E-Autos Light Nodes.

**Manipulationssicherheit von Zuständen** Eine weitere Anwendung ist, das Manipulieren von Tachometern bei Autos zu erkennen und damit einen Betrug zu verhindern. Das Verfahren könnte dabei wie folgt funktionieren: Wird ein Auto gestartet, so wird eine Transaktion mit dem Kilometerstand gesendet.

So kann über die Zeit die Transaktion auf Plausibilität überprüft werden und dies ermöglicht, eine Manipulation des Tachometers zu erkennen. Aber auch Versicherungen können so einfach die gefahrenen Kilometer berechnen und den Vertrag entsprechend anpassen, siehe Abb. 14.29.

**Abb. 14.29** Manipulieren von Tachometern bei Autos



**Elektronische Auktion** In der Ukraine wurde im Februar 2016 die erste elektronische Auktion mit einer Blockchain durchgeführt. Dies geschah testweise und soll die Welt der Auktionen einfacher und vor allem sicherer machen. Ein Block der Kette fungiert hierbei als eine private Handelsplattform, die eine Schnittstelle für Interessenten und Auktionshäuser bereitstellt. Hier kann nun für das Objekt der Wahl geboten werden. Es können auch feste Anfangsgebote gesetzt werden. Durch das Zahlen einer Teilnahmegebühr ist ein Teilnehmer mit seinem Bankkonto oder einem Konto für Kryptowährungen mit einer API des Systems verbunden und kann bei einem Kauf sofort das erstegebotene Objekt bezahlen.

Der Code, um nach diesem Prinzip elektronische Auktionen zu starten, ist frei erhältlich. Denkbar ist für Auktionshäuser, dass eine private permissionless Blockchain erstellt wird, damit jeder, der registriert ist, unkompliziert mitbieten kann.

Alle können immer den Verlauf der Auktion in der Blockchain beobachten. Nach der Auktion wird die Blockchain geschlossen.

**Supply Chain** Die Idee bei diesem Beispiel ist, eine automatische 3D-Druck-Produktions-, Bezahl- und Lieferkette umzusetzen. Der Kunde bestellt ein bestimmtes Design einer Tasse und möchte ein Exemplar geliefert bekommen. Außerdem bestätigt der Kunde über ein Smart Contract in der Transaktion verbindlich, dass er die Ware bezahlt, wenn sie innerhalb der nächsten drei Tage bei ihm eintrifft. Danach wird das gewünschte Design von der 3D-Design-Firma automatisch über eine Transaktion an die Blockchain gesendet (one time use only). Die 3D-Druck-Firma druckt dann automatisch das gewünschte Teil (pay per use) und die Fertigstellung wird durch eine Transaktion in der Blockchain dokumentiert. Daraufhin wird automatisch der Zulieferer aktiv und liefert die Tasse an den Kunden. Der Kunde bestätigt den Empfang, und eine entsprechende Transaktion sorgt dafür, dass die 3D-Design- und 3D-Druck-Firma sowie der Zulieferer die entsprechenden Beträge für die erbrachte Leistungen erhält. Das Besondere an dieser Umsetzung ist, dass dieser Ablauf automatisiert und vertrauenswürdig mithilfe der Blockchain-Technologie umgesetzt wird, siehe Abb. 14.30.

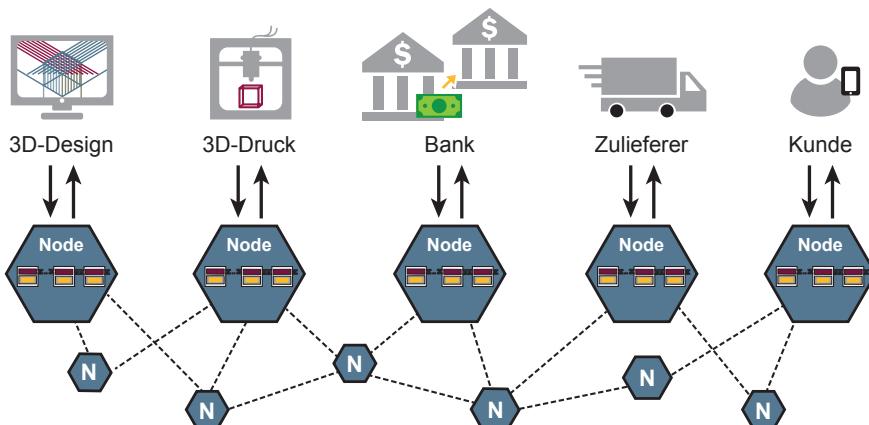


Abb. 14.30 Supply Chain

**Identity Management** Große Vorteile können auch für das Identity-Management gefunden werden. Jeder Mensch trägt seinen Personalausweis oder andere Ausweisdokumente bei sich. Die persönlichen Informationen liegen schriftlich wie digital vor. Im Grunde genommen gibt es keine Kontrolle darüber, wer was sehen darf. Kauft ein Jugendlicher ein Spiel, das erst ab 16 oder 18 freigegeben ist, muss er seinen Personalausweis vorzeigen, um zu bestätigen, dass er das betreffende Alter erreicht hat. Einzusehen sind aber auch andere Daten, wie der vollständige Name und die Adresse. Das Unternehmen ShoHei bietet ein Konzept zu einer blockchainbasierten Lösung an. Alle persönlichen Daten werden in einem Block gespeichert. ShoHei nutzt dazu den BlockCypher Blockchain Service. Es soll unter anderem möglich sein, sich mit dem Handy auszuweisen. Der Identifikationsnachweis geschieht dabei biometrisch. Nach der Identifikation kann festgelegt werden, welche Daten gezeigt werden sollen. Da die Blockchain nicht manipuliert werden kann, ist diese Technologie zum Identifizieren von Personen in vielen Lebensbereichen hilfreich, nicht zuletzt für die EU und die Anforderung nach mehr Sicherheit beim Überprüfen von Geflüchteten.

Da vertrauliche Daten verwaltet werden, sollten Full Nodes nur in den entsprechenden Ämtern stehen und die genutzten Smartphones als Light Nodes dienen, die nur die eigenen Daten Blockdaten speichern, siehe auch im Abschn. 5.2.7 „Identifikation und Authentifikation“ Self-Sovereign Identity.

**Diamantenhandel** Im Diamantenhandel werden alle Edelsteine zertifiziert. In der Blockchain wird vermerkt, wem diese gehören und was für eine Qualität vorliegt. Wichtige Informationen werden oft nur auf Zettel geschrieben, was Kriminellen in die Hände spielt und es Behörden nicht leicht macht, Fälschungen oder Betrüger schnellstmöglich in Kontrollen zu entlarven. Selbst Datenbanken wurden gehackt und Tausende von Informationen verändert. Bei der Diamantenhandel-Blockchain werden alle Diamanten aufgenommen mit Informationen über den Besitzer, die Qualität und mehr mit als 40 Merkmalen, die diesen Diamanten auszeichnen, siehe Abb. 14.31.

Wird der Diamant X von Person A an Person B verkauft, wird an die Blockchain einfach ein neuer Block gehängt mit den Informationen von Diamant X, nur dass als Besitzer Person B eingetragen ist. Mehr als 800.000 Diamanten wurden

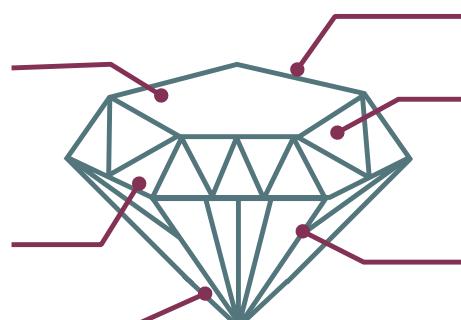


Abb. 14.31 Diamantenhandel

bereits eingetragen. Minengesellschaften, Händler und Versicherer unterstützen diese Art der Verwaltung.

---

## 14.5 Blockchain-as-a-Service

Da die Blockchain-Technologie nicht nur in der IT-Branche große Fortschritte bringen soll, sondern in möglichst vielen Arbeitsbereichen, in denen jedoch das nötige Wissen für den Umgang mit einer solchen IT-Technik nicht vorhanden ist, wird die Blockchain-Technologie auch als „Blockchain-as-a-Service“ angeboten.

Hierbei handelt es sich um vorgefertigte Blockchain-Lösungen, die bei Unternehmen eingepflegt werden. Zwei große Anbieter sind IBM und Microsoft.

Microsoft widmet sich unter dem Projektnamen „Bletchley“ der Verkettung und bietet in seinem Clouddienst „Azure“ den Aufbau einer eigenen Blockchain und deren Verwaltung an. Nodes können einfach festgelegt und entweder mit einem Passwort oder einem SSH Key gesichert werden. Zusätzlich können bestimmte Pakete eingebunden werden, wie zum Beispiel das „Ethereum Studio“ für 0,001 US\$ je Stunde zuzüglich der Kosten für die Azure-Infrastruktur. Hiermit können Smart Contracts erstellt und getestet werden. Die Einbindung ins Netzwerk geschieht nach Abschluss aller Tests einfach mit einem Klick. Microsoft möchte mit seinem Angebot besonders Entwicklern entgegenkommen. Für Visual Studio gibt es Erweiterungen, die es erlauben, Smart Contracts zu erstellen, wodurch später der Umstieg auf Ethereum vereinfacht werden soll.

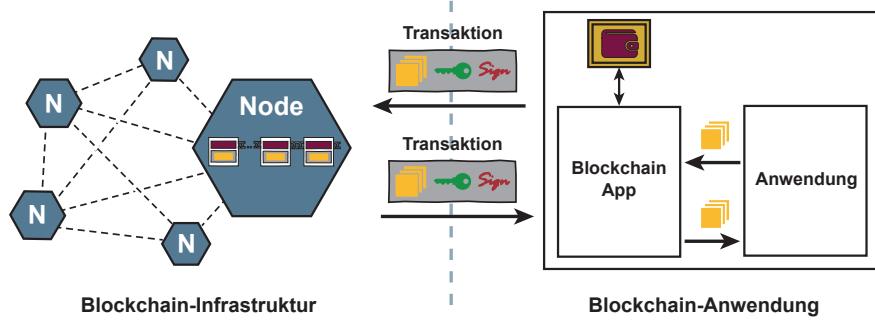
IBM bietet seine Blockchain-Lösung ebenfalls im eigenen Clouddienst „Bluemix“ an. Mit mehr Sicherheit und einer schnelleren Verwaltung richtet sich das Angebot gezielt an Unternehmen. Die Blockchain-Technologie kann zunächst mittels vier bereitgestellter Nodes und einer Zertifizierungsstelle in einer virtuellen Umgebung getestet werden. Zudem werden Beispiel-Code und Beispiel-Apps zur Verfügung gestellt. Entscheidet sich ein Unternehmen, den Dienst in Anspruch zu nehmen, wird eine einzelne isolierte Umgebung aufgebaut, deren Miete 10.000 US\$ im Monat kostet. Smart Contracts stehen hier ebenso im Fokus wie bei Microsoft. Informationen von IoT-fähigen Geräten sollen integriert werden, um als Auslöser der Verträge zu dienen. Als zusätzliche Hilfe sollen in Großstädten wie New York, London und Tokyo Anlaufstellen entstehen, in denen Unternehmen und Entwickler Hilfestellungen zu verschiedenen Problemstellungen bekommen.

IBM ist Teil des von der Linux Foundation ins Leben gerufene „Hyperledger“-Projekts. Das Projekt kümmert sich um die Festlegung von Standards im Umgang mit der Blockchain-Technologie.

---

## 14.6 Sicherheit und Vertrauenswürdigkeit der Blockchain-Technologie

Damit eine Blockchain-Technologie sicher und vertrauenswürdig langfristig genutzt werden kann, müssen Kommunikations-, Sicherheits- und Vertrauenswürdigkeitsaspekte berücksichtigt werden.



**Abb. 14.32** Sicherheit und Vertrauenswürdigkeit von der Blockchain-Technologie

Um die Sicherheitsaspekte besser diskutieren zu können, wird die Blockchain-Technologie in die Blockchain-Infrastruktur und die Blockchain-Anwendung unterteilt, siehe Abb. 14.32.

Auf der linken Seite sind die Blockchain-Infrastruktur mit dem Peer-to-Peer-Netzwerk, die Nodes mit allen Kommunikations- und Sicherheitsfunktionen und die Blockchain als Datenstruktur.

Auf der rechten Seite sind die Blockchain-Anwendung, eine mögliche Blockchain-App, eine Wallet mit dem Schlüssel und die eigentliche Anwendung.

Die Transaktionen werden als Schnittstelle zwischen der Blockchain-Infrastruktur und der Blockchain-Anwendung betrachtet.

#### 14.6.1 Sicherheit der Blockchain-Infrastruktur

Im Folgenden werden die Cyber-Sicherheitseigenschaften und die dazu notwendigen Cyber-Sicherheitsmechanismen diskutiert, die für die Wirksamkeit und Robustheit der Blockchain-Infrastruktur eine wichtige Rolle spielen.

##### 1. Cyber-Sichersicherheitseigenschaft: Verfügbarkeit der Daten

(*Cyber-Sicherheitsattribute: „verteilt“ und „redundant“*)

Mithilfe des Peer-to-Peer-Netzwerks der Blockchain-Infrastruktur werden die Daten in der Blockchain auf den Nodes verteilt, redundant gespeichert und dadurch eine hohe Verfügbarkeit der Daten erzielt. Das Peer-to-Peer-Netzwerk muss dafür robust sein, um zuverlässig die Verfügbarkeit der Daten und die Vertrauensdienste erbringen zu können. Auch DDoS-Angriffe auf eine Blockchain sollten keinen nachhaltigen Einfluss auf die Funktionalität der Blockchain-Technologie haben.

Aspekte, die bei der Robustheit eine Rolle spielen sind: Die Anzahl der Nodes, die Bandbreite zwischen den Nodes, die Speicherplatz- und Rechnerkapazität auf der Node. Eine Bitcoin-Blockchain ist zum Beispiel größer als 160 G Byte. Außerdem muss die Verteilfunktion von neuen Transaktionen und Blöcken robust sein, damit alle Elemente immer vollständig auf allen Nodes verteilt werden.

**Wichtig** Robustheit des Peer-to-Peer-Netzwerks ist eine Grundvoraussetzung für den Betrieb einer Blockchain-Infrastruktur.

## 2. Sicherheitseigenschaften: Integrität und Authentizität der Daten in den Transaktionen

(*Cyber-Sicherheitsattribute: „fälschungssicher/unveränderlich“*)

Die Integrität und Authentizität der Daten in den Transaktionen ist eine wichtige Cyber-Sicherheitseigenschaft, um die Cyber-Sicherheitsattribute fälschungssicher und unveränderlich umsetzen zu können. Dazu spielt die Kryptografie-Agilität der Blockchain-Technologie eine besondere Rolle.

### *Kryptografie-Agilität der Blockchain-Infrastruktur*

Eine Blockchain-Technologie nutzt ein Public-Key-Verfahren für die Signierung und Verifikationen von Transaktionen, um die Echtheit, den Ursprung und die Unversehrtheit der Daten überprüfen zu können.

Hashfunktionen dienen der Blockchain-Adresserzeugung, der notwendigen Verkettung der Blöcke (HashPrev) und der Berechnung des Merkle-Hash-Wertes zur Integritätsüberprüfung aller Transaktionen in einem Block.

Für eine sichere und vertrauenswürdige Nutzung einer Blockchain-Technologie müssen das verwendete Public-Key-Verfahren und die Hashfunktionen dem Stand der Technik genügen. Außerdem müssen die passenden Schlüssellängen verwendet werden. Der Stand der Technik kann aus der Technischen Richtlinie des BSI: „Kryptografische Verfahren: Empfehlungen und Schlüssellängen“ entnommen werden.

In der BSI – Technische Richtlinie „Kryptografische Verfahren: Empfehlungen und Schlüssellängen“ steht beschrieben, welche kryptografischen Verfahren und Schlüssellängen genutzt werden sollten, damit sie für die nächsten zehn Jahre als sicher gelten: Hashfunktionen müssen ein Mindesthashwertlänge von 256 Bit haben, das RSA eine Schlüssellänge von mindestens 3000 Bit und für elliptische Kurven gilt eine Mindestschlüssellänge von 256 Bit (Stand 2018). Siehe: [https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index\\_htm.html](https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html).

Außerdem müssen langfristig Post-Quantum-Kryptoverfahren berücksichtigt und genutzt werden.

Daher muss die Lebensdauer einer Blockchain-Technologie von Anfang an berücksichtigt werden, damit die Werte in einer Blockchain auch langfristig geschützt werden können (zum Beispiel wenn die Lebensdauer länger als zehn Jahre ist).

Bei den Kryptografie-Verfahren spielt aber auch die Schüssel- und Zufallszahlengenerierung eine sicherheitsrelevante Bedeutung. Bei der Erzeugung der Schlüssel besteht das Risiko, dass der Anwender einen zu einfachen Schlüssel wählt. Wird zum Beispiel der eigene Vorname als Schlüssel verwendet, können selbst ungeübte Angreifer das leicht erraten. Aus diesem Grund sollten die Schlüssel immer mithilfe von echten Zufallszahlengeneratoren berechnet und der vollständige Schlüsselraum ausgenutzt werden. Darüber hinaus sind Aspekte wie Streuung, Periodizität und Gleichverteilung zu beachten.

**Wichtig** Die Lebensdauer einer Blockchain-Technologie muss von Anfang an berücksichtigt werden, damit die Werte in einer Blockchain auch langfristig geschützt werden können.

Wenn es notwendig wird, ein Update mit neuen kryptografischen Verfahren umzusetzen, wird eine Hard Fork notwendig. Die Blockchain-Teilnehmer müssen dann neue Blockchain-Adressen generieren und ihre „Werte“ dahin transferieren.

### 3. Cyber-Sicherheitseigenschaften: Integrität der Blockchain

(*Cyber-Sicherheitsattribut: „in der Zeitfolge protokolliert nachvollziehbar“*)

Die Cyber-Sicherheitseigenschaft Integrität der Blockchain ist wichtig, um die Abläufe der Transaktionen in der Zeitfolge nachvollziehen zu können. Für diese Cyber-Sicherheitseigenschaft wird zusätzlich noch eine geschickte Verwendung der Hash-Funktionen (Transaktionen, Blockverkettung) genutzt.

In der Abb. 14.4 sind die Elemente eines Blocks exemplarisch für die Bitcoin-Blockchain zu sehen. Der Block-Header beinhaltet den Merkle-Hash, einen Hash-Wert der alle Transaktionen in einem Block einschließt und damit den Inhalt eines Blocks überprüfbar macht, siehe Abb. 14.5.

Mithilfe des Hashwertes „HashPrev“ im Block Header wird die Blockverkettung der Blockchain sichergestellt. „HashPrev“ ist das Ergebnis der Hash-Funktion (H), die als Input den letzten Block Header nutzt.

$$\text{HashPrev}_n = H(\text{Block} - \text{Header}_{n-1})$$

Die Blockverkettung ist ein wichtiger Aspekt für die Überprüfbarkeit der Reihenfolge der Blöcke, aber sie macht es unmöglich, die Daten in der Blockchain zu löschen. Dies kann wiederum zu Datenschutzproblemen oder Problemen mit unerwünschten Inhalten führen.

#### 4. Cyber-Sicherheitseigenschaften: „ohne zentrale Instanz“

(*Cyber-Sicherheitsattribut: Vertrauen durch „Security-by-Design“*)

Die Blockchain-Technologie bietet „programmiertes Vertrauen“ mithilfe verschiedener Cyber-Sicherheits- und Vertrauensmechanismen. Alle Cyber-Sicherheits- und Vertrauensfunktionen sind inhärent als „Security-by-Design“ in die Blockchain-Technologie integriert.

#### Vertrauenswürdigkeitsmechanismen der Blockchain-Infrastruktur

Für die Blockchain-Anwendung muss ein passendes Konsensfindungsverfahren, auch in Abhängigkeit der ausgewählten Berechtigungsarchitektur, ausgewählt und genutzt werden, um sicher und vertrauenswürdig arbeiten zu können.

Ein Validierungsalgorithmus überprüft die Hashwerte und Signaturen der Transaktionen und auch neue Blöcke, die von der ausgewählten Node erstellt und verteilt worden sind. Zusätzlich werden aber auch die Syntax und Semantik der Elemente überprüft: Stimmt die Blockchain-Adresse? Sind genug Coins vorhanden? usw.

Ein Risiko ist die Fremdnutzung von Elementen, wie sie bei Bitcoin festgestellt worden ist.

Es wurde wissenschaftlich aufgezeigt, dass in Blockchain-Technologien wie Bitcoin auch Daten in eine Transaktion eingebracht werden können, die mit der Bitcoin-Blockchain nichts zu tun haben. Diese Fremdnutzung ist nicht neu und schon seit 2013 bekannt. Das können zum Beispiel 80 Byte in einem fehlerhaften Output-Daten-String (OP\_RETURN) sein. In einem solchen Feld können URLs abgelegt werden, die auf Inhalte anderer Server verweisen. Bilder können in diesem Feld nicht gespeichert werden. Bei dieser Fremdnutzung bleibt die eigentliche Transaktion gültig und wird richtig umgesetzt.

Es könnte aber auch zum Beispiel das Feld für die Bitcoin-Adresse des Empfängers oder ein Hashwert sein. Dann liegt die Größenordnung bis zu 92 K Byte. Wenn in diesen Feldern andere Daten gespeichert werden, gehen die angegebenen Bitcoins im Input verloren.

In 92 K Bytes können Bilder untergebracht werden. Diese sind zwar nicht hochauflösend, aber die Inhalte sind gut erkennbar.

Bei 0,0007 % wurde eine Fremdnutzung der Transaktionsdaten identifiziert. Das ist wie Steganografie: Daten werden in der Masse von Informationen versteckt. Ein normaler Blockchain-Teilnehmer wird diese Daten nicht sehen, weil er nicht auf Transaktionen zugreift, mit denen er nichts zu tun hat. Diese Daten zu finden bedeutet, dass entsprechende Tools programmiert werden müssen, um die Inhalte für die Fremdnutzung zu finden.

Aus diesem Grund sollte als Schutz für die Fremdnutzung die Validierung der Syntax und Semantik so genau wie möglich umgesetzt werden, um die Fremdnutzung zu verhindern.

## Sicherheit und Zuverlässigkeit der Software

Da die Blockchain-Technologie einen Vertrauensdienst anbietet, spielt die Sicherheit und Zuverlässigkeit der Software eine entscheidende Rolle. Es muss sichergestellt werden, dass die Peer-to-Peer-Mechanismen, die Vertrauenswürdigkeitsmechanismen, die verwendete Kryptografie, die Smart-Contract-Umsetzung usw. keine Schwachstellen enthalten und nur das tun, was erwartet wird.

### 14.6.2 Sicherheit der Blockchain-Anwendung

Die Blockchain-Anwendung kann aus einer Blockchain-App bestehen, die Daten von der Anwendung in Transaktionen vom Blockchain-Teilnehmer mit seiner Wallet signiert und in der Blockchain verfestigt.

Außerdem werden Transaktionen in der Blockchain-App verifiziert und die Daten von der Anwendung „verarbeitet“. Die Blockchain-App nutzt die Wallet des Blockchain-Teilnehmers, die als Hardware-Sicherheitsmodule (USB-, NFC-Token, ...) realisiert ist und in der die Schlüssel gespeichert sind.

Die eigentliche Anwendung nutzt die Blockchain-Technologie, siehe Abb. [14.32](#).

#### 1. Geheimhaltung des gemeinen Schlüssels des Public-Key-Verfahrens

Die Sicherheit der Blockchain-Technologie hängt auch von der Geheimhaltung der geheimen Schlüssel der Public-Key-Verfahren in der Wallet ab. Der geheime Schlüssel muss immer geheim bleiben. Wer den geheimen Schlüssel einer Wallet besitzt, ist in der Lage, über die gesamten Transaktionen der Wallet zu verfügen. Ein Verlust des geheimen Schlüssels bedeutet, dass sämtliche in der Blockchain-Adresse gespeicherten Transaktionen für immer „verloren“ sind.

Gefahren bei nicht ausreichendem Schutz des geheimen Schlüssels sind zum Beispiel:

- Das private IT-System des Blockchain-Teilnehmers wird mithilfe von Malware ausgespäht.
- Bei einem IoT-Device, zum Beispiel Auto (Light Node) wird der geheime Schlüssel ausgelesen.
- Die Website der Online-Wallet (Service Node) wird gehackt.
- Ein nicht ausreichend gesichertes Smartphone wird gestohlen (Light Node) und genutzt.

Der Schutz des geheimen Schlüssels in der Wallet sollte mithilfe von Hardware-Security-Modulen realisiert werden (SmartCards, Sec-Token, High-Level-Sicherheitsmodule). Außerdem muss eine unberechtigte Nutzung aktiv verhindert werden.

Indirekter Angriff	Beschreibung
	Auch wenn der Angreifer die Schlüssel nicht auslesen kann, könnte er den Angriff so organisieren, dass er die angebotenen Sicherheitsfunktionen des Hardware-Sicherheitsmoduls unberechtigt nutzt. Dies kann der Angreifer mithilfe einer Malware umsetzen, die bei der Verwendung einer Smartcard oder eines USB-Sicherheitstokens nach der Aktivierung deren Sicherheitsdienste unberechtigt für Angriffe nutzt. Oder der Angreifer schafft sich Zugang zu einer Node, um dort eine Wallet unberechtigt zu nutzen. Diese unberechtigte Nutzung muss aktiv verhindert werden

### Angreifer erstellt unberechtigt echte Transaktionen

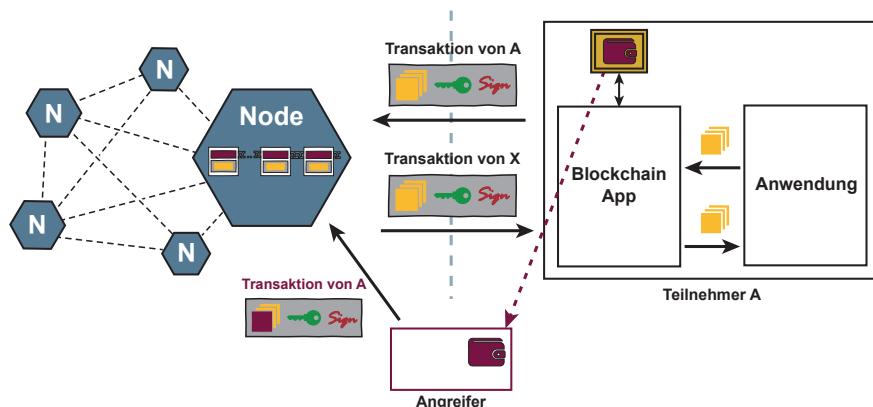
In Abb. 14.33 wird dargestellt, wie der Angreifer mit dem Besitz der Wallet oder dem unerlaubten Zugriff auf die Wallet des Teilnehmers A echte Transaktionen erstellen und damit manipulieren kann.

Der Angreifer ist in der Lage, valide Transaktionen für den entsprechenden Teilnehmer A zu erstellen und dadurch die Blockchain und die Blockchain-Anwendung zu manipulieren. Daher ist es besonders sicherheitsrelevant, dass die Wallet nicht gestohlen oder unberechtigt genutzt werden kann.

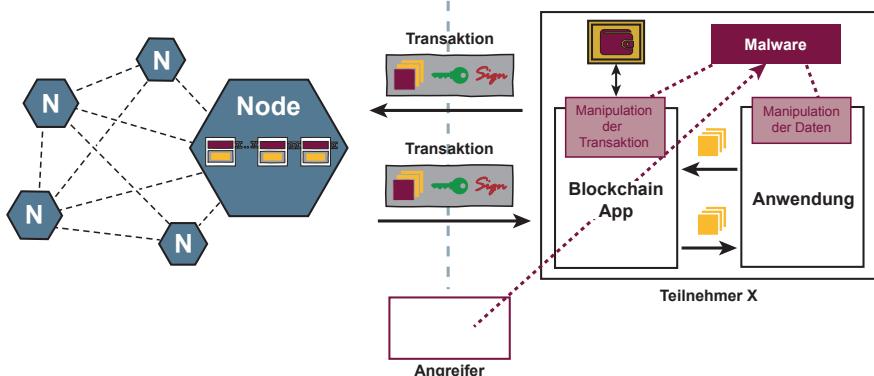
### 2. Schutz der Blockchain-Anwendung

Wenn die Blockchain-Technologie auf der Node an sich eine hohe Sicherheit bietet, werden die Angreifer über die eigentliche Anwendung, die die Blockchain nutzt, angreifen. Daher muss auch die Blockchain-Anwendung manipulations-sicher sein, damit keine erfolgreichen Angriffe umgesetzt werden können.

Abb. 14.34 zeigt, wie ein Angreifer auf dem IT-System des Blockchain-Teilnehmers eine Malware positioniert hat und damit die Blockchain und die Anwendung manipulieren kann. Sowohl ausgehende Transaktionen des entsprechenden Teilnehmers können vor der Sendung an die Blockchain-Infrastruktur



**Abb. 14.33** Unberechtigte Erstellung von Transaktionen



**Abb. 14.34** Manipulation der Blockchain-Anwendung

manipuliert werden, als auch „eigene“ Transaktionen und von anderen Teilnehmern, die aus der Blockchain ausgelesen werden und vor der Weiterleitung manipuliert werden.

Der Angreifer ist in der Lage, dem Teilnehmer eine falsche Realität der Blockchain vorzutäuschen und so zu manipulieren. Dieser Art des Angriffes kann mit Hilfe einer vertrauenswürdigen Laufzeitumgebung entgegengewirkt werden.

#### Sicherheitsmechanismus: Vertrauenswürdige Laufzeitumgebung

Um Malware-Angriff auf Blockchain-Anwendungen zu verhindern, müssen diese in einer vertrauenswürdigen Laufzeitumgebung betrieben werden.

Vertrauenswürdige Laufzeitumgebungen können auf den Technologiefeldern „Trusted Computing“, „Trusted Execution Environment“ und „Sandboxing“ umgesetzt werden.

---

## 14.7 Gegenüberstellung PKI- und Blockchain-Technologien

Die PKI- und die Blockchain-Technologie bieten Vertrauensdienste an. Beide Konzepte nutzen für die Erbringung der Vertrauensdienste One-Way-Hashfunktionen und digitale Signaturen mit Public-Key-Verfahren.

Die PKI nutzt für die Erbringung der Vertrauensdienste zentrale Komponenten, wie die Zertifizierungsstelle für die Erstellung von Zertifikaten, einen Directory Service für die zentrale Zurverfügungstellung von Zertifikaten und die Sperrliste für Zertifikate (Certificate Revocation List), außerdem auch einen zentralen Zeitstempeldienst, siehe auch Kap. 4 „Digitale Signatur, elektronische Zertifikate sowie Public Key Infrastruktur (PKI) und PKI-enabled Application (PKA)“.

**Tab. 14.1** Kriterien für den Vergleich von PKI- und Blockchain-Technologien

Kriterium	Bedeutung/Verständnis
Organisation	Organisatorische Strukturen, die das Konstrukt betreiben
Steuerung	Steuerungsmechanismen, die das Konstrukt steuern und Entscheidungen treffen
Technik	Technische Systeme und Infrastrukturkomponenten, die den Betrieb des Konstrukt s sicherstellen
Vertrauensbildung	Mechanismen der Vertrauensbildung innerhalb des Konstrukt s
Effizienz	Wirtschaftliche und energetische Effizienz des Konstrukt s
Angriffsvektoren	Mögliche Angriffsvektoren gegen das Konstrukt
Regulatorik	Verfügbare verlässliche rechtliche Bedingungen, die das Konstrukt betreffen
Transparenz	Nachvollziehbarkeit der durch das Konstrukt unterstützten Transaktionen und Entscheidungen
Reifegrad	Organisatorischer und technischer Reifegrad des Konstrukt s
Verbreitung	Verbreitungsgrad des Konstrukt s in der praktischen Anwendung
Zukunftssicherheit	Erwartung zur Zukunftssicherheit des Konstrukt s
Interoperabilität	Interaktionsmöglichkeit zwischen verschiedenen Instanziierungen des Konstrukt s
Skalierbarkeit	Skalierbarkeit des Konstrukt s, um sehr hohe Anwenderzahlen zu ermöglichen
Integrationsaufwand	Integrationsaufwand für die Nutzbarmachung des Konstrukt s allgemein und in Fachanwendungen
Endanwenderkreis	Mögliche Zielgruppe für die praktische Anwendung des Konstrukt s

Eine Blockchain-Technologie nutzt für die Erbringung der Vertrauensdienste verteilte Cyber-Sicherheits- und Vertrauenswürdigkeitsmechanismen.

Bei beiden Konzepten ist es für viele Anwendungen notwendig, dass die Angaben in einem Zertifikat der PKI und in der Blockchain der Blockchain-Technologie richtig sind!

In Tab. 14.1 und 14.2 werden Kriterien für den Vergleich von PKI- und Blockchain-Technologien dargestellt. [5].

In einigen Bereichen kann die Blockchain-Technologie die PKI-Technologie ergänzen, wie zum Beispiel bei der Speicherung von Zertifikaten und bei der Sperrliste für Zertifikate.

**Tab. 14.2** Gegenüberstellung PKI und Blockchain

Kriterium	PKI	Blockchain Public Permissionless	Blockchain Public Permissioned
Organisation	Zentralistisch (Unternehmern)	Dezentral („freiwillige“ Betreiber)	Dezentral (selektierte Betreiber)
Steuerung	Betreiberorganisation	„Community“	Konsortium
Technik	Hierarchische Server	Verteilte Nodes	Verteilte Nodes
Vertrauensbildung	Vertrauen in eine zentrale Instanz	Konsensmechanismus	Vertrauen in Konsortium, Konsens
Effizienz	Hoch, da singulärer Aufbau	Gering, da paralleler Wettlauf (PoW) Konsens	Hoch, da „alternativer“
Angriffsvektoren	CA Kompromittieren (zum Beispiel Digi-Notar)	51 %-Attacke	Kompromittierung
Regulatorik	Vorhanden (eIDAS)	Nicht oder nur gering vorhanden	Nicht oder nur gering vorhanden
Transparenz	Eingeschränkt, da kaum überwachbar	Nachvollziehbarkeit durch Verkettung	Nachvollziehbarkeit mit Protokollierung
Reifegrad	Ausgereift und aktiv im Einsatz	Erprobungsstadium	Erprobungsstadium
Verbreitung	Hauptsächlich große Organisationen	Relativ weit bei Kryptowährungen	Prototypischer Einsatz
Zukunftssicherheit	Ja, im geschlossenen Kontext	Ja, mit Einschränkungen	Ja
Interoperabilität	Verbund möglich, zum Beispiel EBCA	Standard in Arbeit (ISO, W3C DID Spec)	Standard in Arbeit (ISO, W3C DID Spec)
Skalierbarkeit	Mit hohem Aufwand	Mit hohem Aufwand	Möglich und vorgesehen
Integrationsaufwand	Hoch (insb. bei „Nachrüstung“)	Hoch (insb. bei „Nachrüstung“)	Hoch (insb. bei „Nachrüstung“)
Endanwenderkreis	Hauptsächlich professionelles Umfeld	Jedermann und „Things“ (IoT)	Jedermann und „Things“ (IoT)

## 14.8 Zusammenfassung

Die Blockchain-Technologie schafft eine Basis für eine verteilte und vertrauenswürdige Zusammenarbeit und stellt damit ein hohes Potenzial für neue Geschäftsmodelle und Ökosysteme dar. Die Elemente, Prinzipien und Architektur der Blockchain zeigen den technischen Hintergrund und interessante Möglichkeiten auf, Sicherheit und Vertrauen zu erzielen.

Alle Cyber-Sicherheits- und Vertrauensfunktionen sind inhärent als „Security-by-Design“ in die Blockchain-Technologie integriert. Die Blockchain-Infrastruktur hat komplexe Kommunikations-, Sicherheits- und Vertrauenswürdigkeitsfunktionen, die im Einklang zueinander die notwendigen Sicherheits- und Vertrauenseigenschaften erbringen.

Die Blockchain-Anwendung ist dem „realen Leben“ ausgesetzt und muss für die sicher Speicherung, Generierung und Nutzung der Schlüssel sowie für eine manipulationsfreie Laufzeitumgebung sorgen.

Für viele Unternehmen ist Blockchain eine ideale Technologie für eine vertrauenswürdige verteilte Zusammenarbeit. Vertrauensdienste wie die Blockchain-Technologie spielen in der Zukunft eine immer wichtigere Rolle.

---

## **14.9 Übungsaufgaben**

### **Übungsaufgabe 1**

Was ist der prinzipielle Unterschied einer zentralen Architektur und einer dezentralen Blockchain-Architektur von Transaktionsspeichern?

### **Übungsaufgabe 2**

Wie wird das Cyber-Sicherheitsattribute „in der Zeitfolge protokolliert nachvollziehbar“ umgesetzt?

### **Übungsaufgabe 3**

Welche Cyber-Sicherheitseigenschaften hat eine Blockchain-Technologie und mit welchen Cyber-Sicherheitsmechanismen werden sie umgesetzt?

### **Übungsaufgabe 4**

Erläuterten Sie den Unterschied zwischen einer Soft und Hard Fork!

### **Übungsaufgabe 5**

Nennen und beschreiben Sie mögliche Angriffspotenziale auf die Blockchain-Infrastruktur!

### **Übungsaufgabe 6**

Nennen und beschreiben Sie mögliche Angriffspotenziale auf die Blockchain-Anwendung!

### **Übungsaufgabe 7**

Nennen und beschreiben Sie mögliche Konsensfindungsverfahren! Welches Verfahren hat sich für die Bitcoin-Blockchain durchgesetzt und warum?

### Übungsaufgabe 8

Wie werden Transaktionen in der Bitcoin-Blockchain autorisiert? Nennen und beschreiben Sie die grundlegende Technologie dahinter! Gehen Sie bei der Beschreibung sowohl auf die Sichtweise des Senders, als auch die des Empfängers ein. Was müssen die Besitzer von digitalen Währungen im Kontext der verwendeten Technologie besonders beachten?

### Übungsaufgabe 9

Sie wurden damit beauftragt, für eine unternehmensübergreifende Datenspeicherung einen Blockchain-Ansatz zu erarbeiten. Welche Anforderungen ergeben sich aus dieser Aufgabenstellung im Gegensatz zu den Anforderungen an die Bitcoin-Blockchain?

### Übungsaufgabe 10

Welche konzeptionellen Probleme müssen bei der Planung des Blockchain-Ansatzes berücksichtigt werden, wenn die langfristige Archivierung von Daten über mehrere Jahrzehnte im Vordergrund steht?

### Übungsaufgabe 11

Bitte kreuzen Sie Ihre Antworten an!

	Cyber-Sicherheitsmechanismen	Blockchain-Technologie
Gewährleistung von Cyber-Sicherheitsbedürfnissen	Vertraulichkeit	
	Authentifikation	
	Authentizität	
	Integrität	
	Verbindlichkeit	
	Verfügbarkeit	
	Anonymisierung/Pseudonymisierung	
Cyber-Sicherheitsstrategien	Vermeiden von Angriffen	
	Entgegenwirken von Angriffen	
	Erkennen von Angriffen	

Ergebnisse siehe: <https://norbert-pohlmann.com/cyber-sicherheit/uebungen/>.

## Literatur

1. Kammler C, Pohlmann N (2013) Kryptografie wird Währung – Bitcoin: Geldverkehr ohne Banken. *IT-Sicherheit – Management und Praxis* 2013(6):60–63
2. Pohlmann N (2018) Eine vertrauenswürdige Zusammenarbeit mithilfe der Blockchain-Technologie. In: Bartsch M, Frey S (Hrsg) *Cybersecurity Best Practices – Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden*. Springer Vieweg, Wiesbaden
3. Investopedia: “Soft Fork”. <https://www.investopedia.com/terms/s/soft-fork.asp>. Stand 08.01.2018
4. Palkovits R, Pohlmann N, Schwedt I (2017) Blockchain-Technologie revolutioniert das digitale Business: Vertrauenswürdige Zusammenarbeit ohne zentrale Instanz. *IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance* 2017(2):54–60
5. TeleTrusT. <https://www.teletrust.de/arbeitsgremien/blockchain/>. Stand 19.11.2018
6. Investopedia: “Hard Fork”. <https://www.investopedia.com/terms/h/hard-fork.asp>. Stand 08.01.2018



# Künstliche Intelligenz und Cyber-Sicherheit

15

In diesem Kapitel wird behandelt, wie die Algorithmen aus dem Maschinellen Lernen und Künstlicher Intelligenz genutzt werden können, um die Cyber-Sicherheit zu verbessern.

## 15.1 Einleitung

Cyber-Sicherheitssysteme, die Künstliche Intelligenz (KI) berücksichtigen, werden in der Zukunft helfen, deutlich besser die intelligenten Hacker und deren Angriffe zu entdecken, Schäden zu vermeiden und Risiken im gewünschten Digitalisierungsprozess zu minimieren. Mithilfe von Künstlicher Intelligenz kann die Erkennungsrate von Angriffen im Netzwerk und in ubiquitären IT-Endgeräten (Smartphone, Notebook, Server, IoT etc.) deutlich erhöht werden. Anders gesagt, können die Erkennungsraten von IT-Systemen, die keine Form der Künstlichen Intelligenz verwenden, nicht dauerhaft auf dem gleichen Sicherheits- und Schutzniveau gehalten werden, wenn auch Angreifer Methoden der KI einsetzen, um IT-Systeme anzugreifen.

Somit hat Künstliche Intelligenz vermehrt Auswirkungen auf die Cyber-Sicherheitslage, die durch aktuelle Lagebilder aufzeigbar gemacht werden muss.

Eine große Herausforderung für die Verteidiger ist, für welche der sehr vielen erkannten sicherheitsrelevanten Ereignisse zusätzliche noch menschliche Analysten notwendig sind. Nicht alle Ereignisse können durch Spezialisten verarbeitet werden, da die Anzahl der Ereignisse die Verarbeitungsfähigkeit und Verarbeitungskapazitäten menschlicher Analysten an ihre Grenzen bringen. Diesen Umstand können Angreifer ausnutzen und die Verteidiger gezielt ablenken, um unbemerkt in das IT-System einzudringen. Künstliche Intelligenz kann dabei helfen, die Ereignisse in Echtzeit zu analysieren und situationsgerecht zu entscheiden, ob ein menschliches Eingreifen überhaupt noch notwendig ist. In anderen Einsatzszenarien, bei denen eine Teilautonomie technisch nicht möglich ist

und der Mensch zwingend eingebunden werden muss, kann der Einsatz von KI die Aufgaben und Tätigkeiten des Menschen wesentlich unterstützen. Damit werden die vorhandenen Ressourcen gezielter eingesetzt und das Cyber-Sicherheitsniveau insgesamt erhöht. Situationsgerecht bedeutet dabei, dass klassische Verfahren auf Basis von Signaturen nur noch unterstützend eingesetzt werden und neuartige, verhaltensbasierte Verfahren, wie fortgeschrittene Anomalie-Erkennung oder Predictive Analysis, Einzug halten. Durch den Einsatz von KI können solche Verfahren möglich werden und einen deutlichen Fortschritt für die Cyber-Sicherheit bringen.

Weiterhin profitieren Identitäts- und Zugangsmanagementsysteme von der automatischen Auswertung der Bewegungsdaten von Nutzern, um nur berechtigten Nutzern den Zugriff zu IT-Systemen und Anwendungen zu geben. Die Sammlung, Verarbeitung und Speicherung von personenbezogenen Daten müssen jedoch im Einklang mit den datenschutzrechtlichen Bestimmungen (zum Beispiel DSGVO) stehen. Hierbei ist zu beachten, dass die Datenschutzkonformität eine Asymmetrie bei Angriffsszenarien zwischen Verteidiger und Angreifer darstellen kann.

Neuartige, passive Identifikations- und Authentifizierungsverfahren können einen Beitrag leisten und zu einer erhöhten Resilienz und Robustheit von IT-Systemen führen. Durch die fehlende aktive Nutzerinteraktion bei dieser Form der Identifizierung und Authentifizierung, beispielsweise durch die Auswertung von Sensordaten im Smartphone, können IT-Systeme sehr einfach sicherer gemacht werden. Aber auch im Bereich der risikobasierten und adaptiven Authentifizierung wird die KI helfen, angemessene Cyber-Sicherheit situationsbedingt umzusetzen und so die Schäden deutlich zu minimieren.

---

## 15.2 Einordnung der Künstlichen Intelligenz

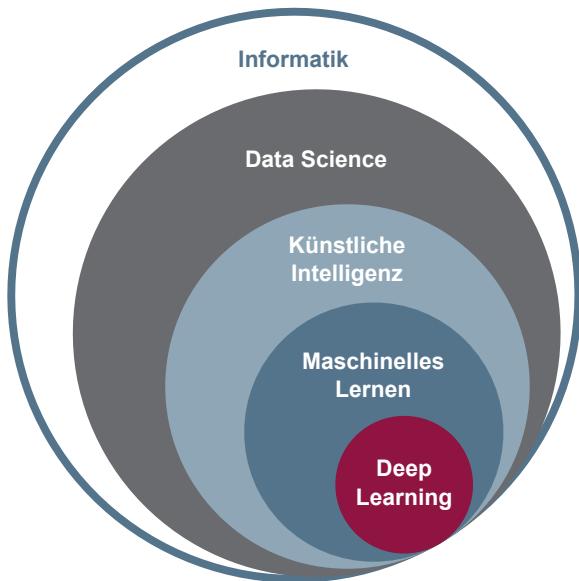
Die Wissenschaft „Data Science“, ein Fachgebiet der Informatik, beschäftigt sich mit der Extraktion von Wissen aus den Informationen in Daten. Da es immer mehr Daten mit Informationen gibt, kann auch immer mehr Wissen aus den Informationen der Daten abgeleitet werden, insbesondere auch im Bereich der Cyber-Sicherheit, siehe Abb. 15.1.

Dabei setzt „Künstliche Intelligenz“ intelligentes Verhalten in Algorithmen um, mit der Zielsetzung, automatisiert „menschähnliche Intelligenz“ so gut wie möglich nachzubilden.

Bei Künstlichen Intelligenzen kann zwischen schwacher und starker KI unterschieden werden. Eine starke KI soll eine Intelligenz schaffen, die dem Menschen gleicht kommt oder sogar übertrifft, während die schwache KI sich in der Regel mit konkreten Anwendungsproblemen des menschlichen Denkens beschäftigt.

Maschinelles Lernen (Machine Learning/ML) ist ein Begriff im Bereich der Künstlichen Intelligenz für die „künstliche“ Generierung von Wissen aus den Informationen in Daten mit der Hilfe von IT-Systemen. Mithilfe der Algorithmen des Maschinellen Lernens werden mit vorhandenen Datenbeständen Muster und Gesetzmäßigkeiten erkannt und verallgemeinert, um damit neue Problemlösungen

**Abb. 15.1** Einordnung der Künstlichen Intelligenz



umzusetzen. In Lernphasen lernen entsprechende ML-Algorithmen, aus vielen diversen Beispielen simple Muster und Strukturen, hin zu komplexen Merkmalen und Gesetzmäßigkeiten zu erkennen. Daraus entstehende Regeln können auf neue Daten und ähnliche Situationen angewendet werden, in denen die KI beispielsweise entscheiden muss, ob es sich um einen Angriff oder eine legitime Nutzeraktion handelt.

Maschinelles Lernen wird noch effektiver durch Deep Learning. Deep Learning ist eine Spezialisierung des maschinellen Lernens und nutzt vorwiegend Künstliche Neuronale Netze (KNN).

## 15.3 Erfolgsfaktoren der Künstlichen Intelligenz

Die Erfolgsfaktoren der Künstlichen Intelligenz sind vielfältig. Die Entwicklung sowie die Zeit werden diesen Trend weiter fördern. Folgende Aspekte spielen eine Rolle:

### 1. Leistungsfähigkeit der IT-Systeme

Es stehen enorme Fortschritte der Leistungsfähigkeit von IT-Systemen (CPU, RAM, ...) zur Verfügung, die eine (zentrale) Speicherung und Verarbeitung von immer größeren Massen von Eingangsdaten möglich macht.

Standard-Hardware: 20 CPU Kerne, 2,2 GHz Taktfrequenz, 14 M Cache, 64 GB Arbeitsspeicher, 1 TB SSD usw.

Spezial-Hardware: GPUs und Field Programmable Gate Array (FPGA) sowie TensorFlow Processing Unit (TPU) von Google und Lake Crest von Intel.

Zentrale Speicherung und Verarbeitung von massenhaften Input-Daten ist heute sehr einfach möglich. Viele umfangreiche Prozesse von Maschinellem Lernen sind heute in akzeptabler Zeit durchführbar. Parallelisierung steigert diese Leistung nochmals deutlich. Hohe Geschwindigkeiten in der Datenübertragung erlauben ein Auslagern verschiedener Prozesse und Aufgaben auf weitere Server. Spezielle Software-Frameworks helfen, die Umsetzung zu optimieren.

Es gibt aber zunehmend auch sehr leistungsfähige Cloud-Lösungen, wie Amazon Web Services, Microsoft Azure, Google Cloud Platform und die IBM Cloud.

## **2. Immer mehr vorhandene Daten**

Neben der Entwicklung der technischen Leistungsfähigkeit sind die mit der fortschreitenden Digitalisierung stetig zunehmenden Daten ein relevanter Faktor für den Erfolg von KI. Auf der einen Seite ist die Quantität der vorhandenen Daten durch sehr viele Sensoren (in IT-Systemen, in Diensten, am Körper, im Auto, ...) rasant gestiegen. Auch der Austausch von Daten hat zugenommen.

Auf der anderen Seite ist die Qualität der Daten durch weitere Individualisierung der (persönlichen) Daten von IT-Systemen (PC, Notebook, Smartphone, Smartwatch, Automobile, ...) gestiegen. Außerdem werden zunehmend gezielt sicherheitsrelevante Informationen in Daten durch spezielle Sensoren im Cyber-Sicherheitsbereich zur Verfügung gestellt.

## **3. Immer bessere Algorithmen**

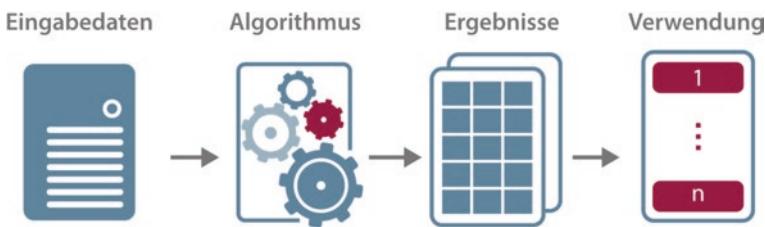
Hinzu kommt die Verfügbarkeit effizienterer Algorithmen, die optimiertes Maschine-Learning ermöglichen. Der Gesamtlauf wird optimiert, wie zum Beispiel eine Reduktion der Komplexität durch intelligent gewählte Eingangsdaten. Es findet ein iterativer Lernprozess der Algorithmen statt. Algorithmen des maschinen Lernens werden durch diese stetigen Verbesserungen praktisch umsetzbar gemacht und auch für komplexere Daten effizient. In der weiteren Entwicklung wird Maschinelles Lernen durch Deep Learning noch effektiver. Deep Learning ist eine Spezialisierung des Maschinellen Lernens und nutzt vorwiegend komplexe Künstliche Neuronale Netze. Dabei werden zusammenhängende Schichten aus künstlichen Neuronen zur Datenverarbeitung genutzt. Das Potenzial von Deep Learning besteht darin, dass im Vergleich zu traditioneller KI nicht nur effektiver analysiert wird, sondern durch den effektiveren Lernprozess der KI auch mit unvollständigen Daten eine Analyse erfolgreich umgesetzt werden kann. So kann durch den ständigen Lernprozess des Deep Learnings eine KI in bis dahin unbekannten Situationen angewandt werden.

## **4. Immer mehr Erfahrungen mit dem Umgang**

Durch die immer häufigere Nutzung von KI werden die Erfahrungen mit dem Umgang der Daten und Algorithmen immer größer.

## **5. Immer einfacherer Zugang**

Algorithmen werden immer zugänglicher und nutzbarer durch bessere Frameworks, Dokumentationen, Bibliotheken.



**Abb. 15.2** Workflow des Maschinellen Lernens

## 15.4 Das Prinzip des Maschinellen Lernens

Die Algorithmen des Maschinellen Lernens haben als Input **Eingangsdaten** mit Informationen, berechnen mit einem **Algorithmus** nach einem vorgegebenen Verfahren und liefern als Output die **Ergebnisse**. Die Anwendung entscheidet, wie die Verwendung der Ergebnisse stattfinden soll, siehe Abb. 15.2.

### Eingangsdaten

Die Eingangsdaten können sehr vielfältig sein. Beispiele aus dem Cyber-Sicherheitsbereich:

- Smartphone: Lage- und Beschleunigungssensoren, GPS-Daten, Nutzereingaben, ...
- Notebook, PC: Nutzereingaben, Log-Daten, ...
- Netzwerke: Bandbreite, Verzögerung, ..., Header- und Kommunikationsdaten, ...
- IoT: Sensorik- und Aktorik-Daten
- allgemein IT-Systeme: CPU-Aktivitäten, RAM-Verbrauch, SW-Aufrufe, Kommunikation, ...

### Algorithmen

- Support-Vector-Machine (SVM)
- k-Nearest-Neighbor (kNN)
- k-Means-Algorithmus
- hierarchische Clustering-Verfahren
- Convolutional Neural Network
- ...

### Ergebnisse

Ergebnisse aus der Verarbeitung der Eingangsdaten mit den Algorithmen können sein:

- Klassifizierung der Eingangsdaten, wie Erkennung von Angriffen
- numerische Werte, wie Hinweise zur Verbesserung eines Produkts
- binäre Werte, wie eine erfolgreiche biometrischer Authentifizierung

### Verwendung

Die Anwendung entscheidet, wie die Ergebnisse verwendet werden.

## 15.5 Kategorien und Algorithmen des Maschinellen Lernens

In diesem Abschnitt werden die Kategorien und beispielhaften Algorithmen des Maschinellen Lernens beschrieben und anhand von Beispielen im Bereich der Cyber-Sicherheit erläutert.

### 1. Überwachtes Lernen

Beim überwachten Lernen wird ein Algorithmus mithilfe von Eingabedaten und Ergebnissen trainiert. Dadurch kann der Algorithmus lernen, ob das Ergebnis mit den Eingabedaten den Erwartungen entspricht. Zum Aufgabenfeld des überwachten Lernens gehört das Regressions- und Klassifizierungsproblem. Mit der Regressionsanalyse ist es möglich, Werte von abhängigen Variablen zu prognostizieren. Aufgaben der Klassifikation befassen sich damit, Daten in verschiedene Klassen mit ähnlichen Ausprägungen einzuteilen [1].

Ziele des überwachten Lernens sind:

- Regression: Vorhersagen von numerischen Werten
- Klassifizierung: Einteilung von Eingabedaten in Klassen

Beispiele im Bereich der Cyber-Sicherheit sind:

- Erkennung von Spammails
- Erkennen von Angriffen in Intrusion Detection Systems (IDS)

**ML-Algorithmen aus dem Bereich des überwachten Lernens sind zum Beispiel:**

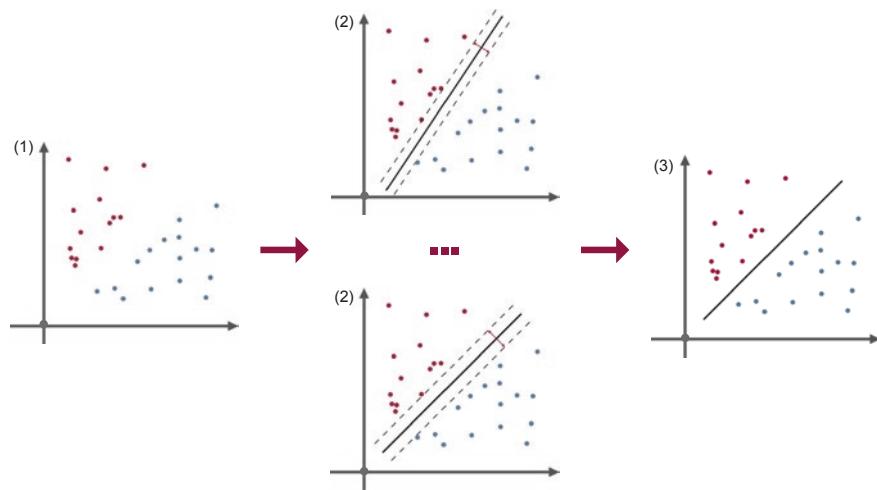
- Support-Vector-Machine (SVM)
- k-Nearest-Neighbor (kNN)

### 15.5.1 ML-Algorithmus: Support-Vector-Machine (SVM)

Eine Support-Vector-Machine ist ein mathematisches Verfahren zur Klassifizierung von Eingabedaten (Objekte). Eine SVM arbeitet mit Trainingsdaten, für die bereits definiert ist, welcher Klasse sie zugehören. Jedes Eingabedatum wird dabei durch einen Vektor in einem  $n$ -dimensionalen Vektorraum repräsentiert. Für diesen Vektorraum versucht die SVM, eine optimale Hyperebenen zu berechnen, um damit die Daten in zwei Klassen zu unterteilen. In Abb. 15.3 ist exemplarisch dargestellt, wie in einem zweidimensionalen Raum nach einer optimalen Hyperebene zu den gegebenen Eingabedaten gesucht wird. In einem  $n$ -dimensionalen Raum hat die Hyperebene die Dimension  $n - 1$ . Aus diesem Grund ist jede der betrachteten Hyperebenen in dem dargestellten Beispiel eine Linie.

Eine Hyperebene ist optimal, wenn der Abstand zu den sogenannten „Support-Vectors“ am höchsten ist. Ein „Support-Vector“ ist der nächste Vektor einer Klasse zu der betrachteten Hyperebene. In dem dargestellten Beispiel sind es jeweils die nächsten Punkte einer Klasse (rot oder blau) zu der betrachteten Linie.

### Trainieren einer Support-Vector-Machine



**Abb. 15.3** Support-Vector-Machine (SVM) – Training

#### Eingabedaten: (1) in Abb. 15.3

- Klassifizierte Objekte (Trainingsdaten, für die bereits definiert ist, welcher Klasse sie zugehören)
- Abstandsmaß der Objekte untereinander (durch Beschreibung als Vektor)

#### ML-Algorithmus: (2) in Abb. 15.3

- Ermitteln von Geraden zur Trennung der klassifizierten Objekte
- Bewertung durch Abstand zu den Punkten
- Wahl der Geraden mit maximalem Abstand zu beiden Klassen

#### Ergebnis: (3) in Abb. 15.3

- Gerade als Modell zur Klassifizierung

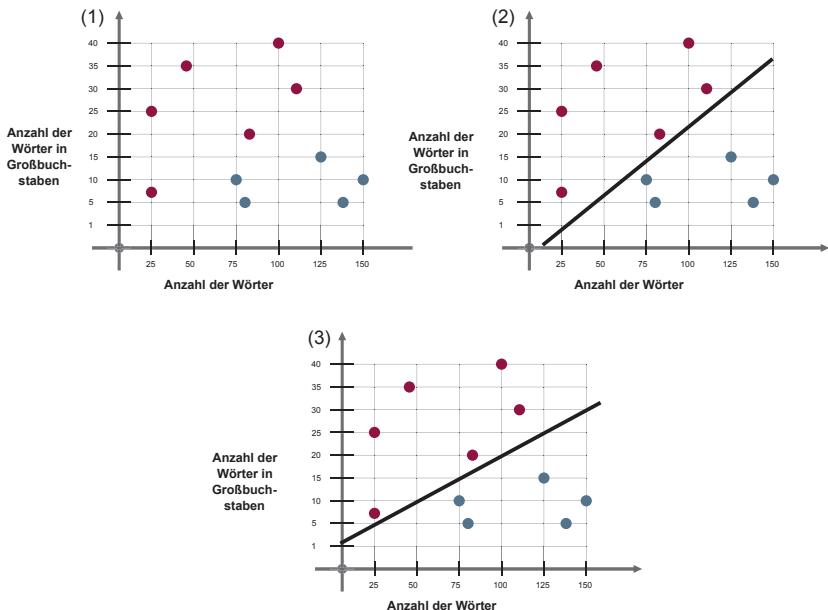
Danach klassifiziert das Modell mithilfe der Lage der Punkte der Eingabewerte in eine Klasse.

#### Beispiel: Training für das Erkennen von Spam-E-Mails

In diesem Beispiel werden E-Mails in Vektordarstellung als Trainingsdaten verwendet. Jede Spalte repräsentiert eine E-Mail, die aus der Gesamtanzahl der Wörter, die Anzahl der Wörter in Großbuchstaben und die jeweilige Klassifizierung besteht. Der Algorithmus (SVM) berechnet anhand der Trainingsdaten die optimale Hyperebene (Geraden), die den Datensatz in zwei Klassen unterteilt.

**Tab. 15.1** Trainingsdaten für das Erkennen von Spam-E-Mails

Anzahl Wörter	25	25	47	75	79	82	100	110	125	140	150
Anzahl Wörter in Großbuchstaben	7	25	35	10	5	20	40	30	15	5	10
Spam-E-Mail	Ja	Ja	Ja	Nein	Nein	Ja	Ja	Ja	Nein	Nein	Nein

**Abb. 15.4** Training für das Erkennen von Spam-E-Mails

Anmerkung:

Um die Verständlichkeit der Beispiele zu erhöhen, wurde bewusst die Komplexität der jeweiligen Anwendungsbeispiele reduziert. Diese entsprechen ggf. nicht der Realität (Tab. 15.1; Abb. 15.4).

**Eingabedaten:** (1) in Abb. 15.3

- E-Mails als Vektor mit entsprechender Klassifikation (zum Beispiel 25/7 ja, 75/10 nein)

**ML-Algorithmus:** (2) in Abb. 15.3

- Ermittlung der Geraden, die die Objekte trennen
- Bestimmung der besten Geraden

**Ergebnis:** (3) in Abb. 15.3

- Gerade als Modell zur Klassifizierung von E-Mails als Spam/kein Spam

### Beispiel einer Spam-E-Mail-Erkennung

Als Eingabedaten wird ein Modell zur Klassifizierung sowie eine zu klassifizierende E-Mail übergeben. Die zu prüfende E-Mail hat in diesem Beispiel insgesamt 63 Wörter, wovon 25 in Großbuchstaben geschrieben sind. Der ML-Algorithmus bestimmt das Verhältnis zwischen der Gesamtanzahl der Wörter und die Anzahl der Wörter in Großbuchstaben. Mithilfe des Modells wird geprüft, wo die Position der zu prüfende E-Mail zur Hyperebene liegt. Anhand der Position zur Hyperebene kann die neue E-Mail klassifiziert werden. In diesem Beispiel liegt die E-Mail über der Hyperebene und wird als Spam markiert.

#### Eingabedaten:

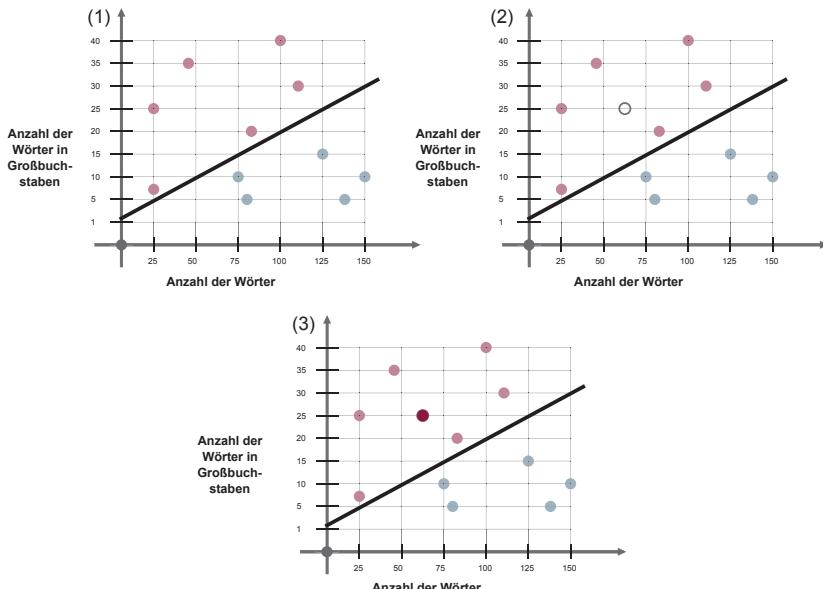
- Modell zur Erkennung von möglichen Spammails – (1) in der Abb. 15.5
- zu beurteilende E-Mail, mit den Eingabedaten (Vektor): (2) in der Abb. 15.5
  - Anzahl der Wörter = 63 und
  - Anzahl Wörter in Großbuchstaben = 25

#### ML-Algorithmus:

- Berechnung der Lage der zu untersuchenden E-Mail

#### Ergebnis:

- Lage der Punkte zum Modell klassifiziert die E-Mail als **Spammail**, siehe (3) in der Abb. 15.5.



**Abb. 15.5** Spam-E-Mail-Erkennung

### 15.5.2 ML-Algorithmus: k-Nearest-Neighbor (kNN)

Der k-Nearest-Neighbor-Algorithmus ist ein Klassifikationsverfahren, bei dem eine Klassenzuordnung auf Basis seiner  $k$  nächsten Nachbarn durchgeführt wird. Auch bei diesem Klassifikationsverfahren müssen bereits klassifizierte Objekte vorhanden sein. Die Klassifikation eines neuen Objektes erfolgt im einfachsten Fall durch Mehrheitsentscheidung. Für die Mehrheitsentscheidung werden die  $k$  nächsten bereits klassifizierten Objekte herangezogen. Als Maß für den Abstand der Objekte zueinander kann zum Beispiel die euklidische Distanz verwendet werden. Die euklidische Distanz beschreibt eine räumliche Distanz zwischen zwei Objekten und ist nachfolgend definiert:

$$\text{dist}(v, w) = \sqrt{\sum (v_i - w_i)^2}, \text{ wobei } v, w \in \mathbb{R}$$

**Eingabedaten:** (1) in Abb. 15.6

- bereits klassifizierte Objekte
- Anzahl der zu betrachtenden Nachbarobjekte  $k$
- unklassifiziertes Objekt, das klassifiziert werden soll

**ML-Algorithmus:** (2) in Abb. 15.6

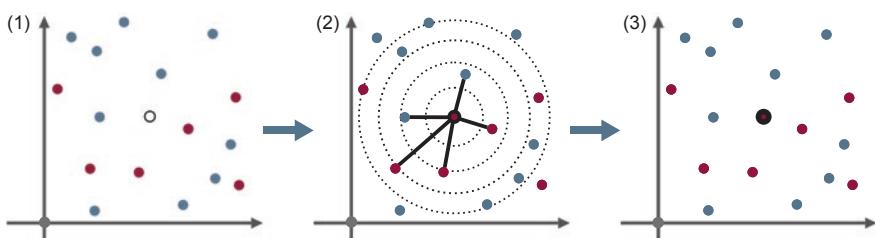
- Berechnung der Distanz zu allen anderen Objekten
- Betrachtung der  $k$  nächsten Nachbarobjekte
- Zuordnung zur am häufigsten vorkommenden Klasse

**Ergebnis:** (3) in Abb. 15.6

- Klassifizierung des neuen Objekts durch Mehrheitsentscheidung

#### kNN – am Beispiel eines IDS

In diesem Beispiel werden die Systemaufrufe und deren Anzahl betrachtet. Die unterschiedlichen Systemaufrufe werden durch kleine Buchstaben repräsentiert, hier „a“ bis „z“. Ein Prozess besteht aus einer beliebigen, festen Sequenz von Aufrufen. Die Reihenfolge der Aufrufe wird in diesem Beispiel nicht berücksichtigt.



**Abb. 15.6** k-Nearest-Neighbor (kNN)

Systemaufruf Prozess	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
$P_1("waafwz")$	2	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	1
$P_2("asdf")$	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
$P_3("axzb")$	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1
$P_4("bbffe")$	0	2	0	0	1	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

**Abb. 15.7** Gemessene Prozesse und Systemaufrufe

Die Häufigkeit jedes Aufrufs wird für jeden normalen Prozess gespeichert. Die Prozesse werden als  $P_1$  bis  $P_4$  dargestellt. Die Sequenz der Vorkommen der Systemaufrufe steht hinter den jeweiligen Prozessen in Klammern. So besitzt beispielsweise der Prozess  $P_1$  den Systemaufruf „w“, zweimal „a“, ein „f“, ein weiteres Mal ein „w“, gefolgt von einem „z“, siehe Abb. 15.7.

Dann wird das Gleichheitsmaß und der Schwellenwert bestimmt, um zu definieren, was „normal“ ist beziehungsweise „nicht normal“. Die Funktion  $\text{sim}(X, P_i)$  beschreibt das Ähnlichkeitsmaß des unbekannten Prozesses  $X$  zu dem jeweiligen bekannten Prozessen  $P_i$ . Häufig verwendete Ähnlichkeitsmaße sind die Euklidische Distanzfunktion oder die Kosinus-Ähnlichkeit.

Die Auswahl oder Erstellung einer geeigneten Funktion für das Maß der Ähnlichkeit muss unter Berücksichtigung der zugrunde liegend Problemstellung erfolgen. Nicht jede Distanzfunktion ist per se für die Erfüllung einer speziellen Problemstellung geeignet. Im weiteren Verlauf dieses Beispiels wird die Kosinus-Ähnlichkeit verwendet, da sie für die gegebene Problemstellung akzeptable Ergebnisse produziert. Würde beispielsweise für die gleiche Problemstellung die Euklidische Distanzfunktion verwendet, würden die Prozessaufrufe überwiegend falsch klassifiziert werden. Für zwei Vektoren  $X, P$  wird die Kosinus-Ähnlichkeit folgendermaßen berechnet:

$$\text{sim}(X, P) = \frac{\sum_{i=1}^n x_i p_i}{\sqrt{\sum_{i=1}^n x_i^2} \sqrt{\sum_{i=1}^n p_i^2}}, \text{ mit } x_i, p_i \text{ Komponenten von } X, P, \quad 1 \leq i \leq n$$

Die Vektoren  $X, P$  und deren Komponenten  $x_i, p_i$  ergeben sich in diesem Beispiel direkt aus den Systemaufrufen und deren Anzahl. Jede Zeile in Abb. 15.7 wird somit als Eingabevektor betrachtet.

**Beispiele der Klassifizierung eines Prozesses in „normal“ und „nicht normal“**  
Für einen neuen Prozess  $X_A$  („wasd“), der analysiert werden soll, wird zuerst die Ähnlichkeit zu allen bereits gelernten Prozessen berechnet. In diesem Beispiel sind die Eingabewerte für die Kosinus-Ähnlichkeit ausschließlich positiv. Aus diesem Grund produziert die Funktion  $\text{sim}(X, P)$  Ausgabewerte im Bereich von 0

System-aufruf Prozess	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	$sim(X_A, P_i)$
$P_1("waafwz")$	2	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	1	0,63
$P_2("asd")$	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0,75
$P_3("axzb")$	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0,25
$P_4("bbfe")$	0	2	0	0	1	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00
$X_A("wasd")$	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	

**Abb. 15.8** Beispiele der Klassifizierung eines Prozesses  $X_A$  in „normal“ und „nicht normal“

bis 1 (einschließlich). Ein Ausgabewert von 0 bedeutet, dass keine Ähnlichkeit zu einem gelernten Prozess vorliegt. Ein Ausgabewert von 1 signalisiert, dass es sich um die gleichen Prozesse handelt. Je näher der Ausgabewert an 1 liegt, desto ähnlicher sind sich die beiden betrachteten Prozesse.

Für die Klassifizierung werden die  $k$  nächsten Nachbarn mit der geringsten Distanz zu dem neuen Prozess betrachtet. In unserem Beispiel sei der Einfachheit halber  $k = 2$ , siehe Abb. 15.8.

Das Ähnlichkeitsmaß der beiden nächsten Prozesse wird in diesem Beispiel gemittelt und mit einem vorher definierten Schwellenwert verglichen. Wird der Schwellenwert erreicht oder überschritten, wird der betrachtete Prozess als „normal“ eingestuft. Die Festlegung des Schwellenwertes kann auf vorher durchgeführten Untersuchungen (zum Beispiel mittels Trainings- und Testdaten) oder auf Erfahrungswerten basieren. In diesem Beispiel wurde der Schwellenwert auf 0,65 festgelegt.

$$\bar{x} = \frac{(0,63 + 0,75)}{2} = 0,69 \geq 0,65$$

Der gemittelte Wert beträgt 0,69, welcher die Bedingung für einen bekannten „normalen“ Prozess erfüllt. Dementsprechend wird der Prozess  $X_A$  als „normal“ eingestuft.

Für einen weiteren unbekannten Prozess  $X_B$  („cytq“) ergeben sich mit der gleichen Vorgehensweise die in Abb. 15.9 berechneten Ähnlichkeiten.

Die Berechnung der Kosinus-Ähnlichkeit hat ergeben, dass der Prozess  $X_B$  keinem der bekannten Datensätze ähnelt. Folglich beträgt das arithmetische Mittel in jeder Kombination von zwei Nachbarn 0 und  $X_B$  wird als „nicht normal“ klassifiziert.

System-aufruf Prozess	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	$sim(X_B, P_i)$
$P_1("waafwz")$	2	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	1	0,00
$P_2("asd")$	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0,00
$P_3("axzb")$	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0,00
$P_4("bbfe")$	0	2	0	0	1	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00
$X_B("cytq")$	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	

**Abb. 15.9** Beispiele der Klassifizierung eines Prozesses  $X_B$  in „normal“ und „nicht normal“

## 2. Unüberwachtes Lernen

Beim unüberwachten Lernen werden Muster und Gesetzmäßigkeiten in unklassifizierten Objekten gesucht.

Die Stärke im unüberwachten Ansatz liegt darin, nach Mustern auch in unklassifizierten Daten zu suchen, um sie nach vorheriger Aufbereitung besser beschreiben zu können. Mittels Clustering werden ähnliche Datengruppen miteinander in Verbindung gesetzt. Die Erwartungshaltung an diesen Ansatz liegt unter anderem darin, Dinge zu erkennen, die vorher anderweitig nicht sichtbar waren und ist im Weiteren auch gut geeignet, um unüberschaubare Datensets auf die wichtigsten Eigenschaften sowie Kriterien zu reduzieren. Da der Algorithmus selbstständig lernt, werden klassische Fehler in diesem Sinne nicht produziert. Dies kann jedoch zu einem anderen Problem führen: Lernt der Algorithmus auch in die gewünschte Richtung? Zur Überprüfung des unüberwachten Lernens müssen folglich alle relevanten Gegebenheiten miteinander abgeglichen werden, um so Korrelationen zu finden.

Clustering setzt ähnliche Datengruppen miteinander in Verbindung.

**ML-Algorithmen aus dem Bereich des unüberwachten Lernens sind zum Beispiel:**

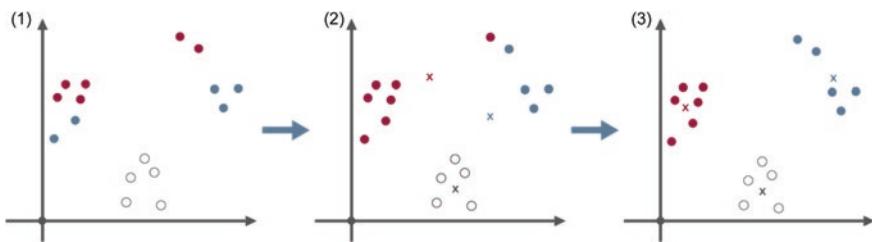
- k-Means-Algorithmus
- hierarchische Clustering-Verfahren

### 15.5.3 ML-Algorithmus: k-Means-Algorithmus

Der k-Means-Algorithmus ist ein Verfahren zur Clusteranalyse. Mit vorhandenen Eingangsdaten werden zufällig aus den gebildeten Mittelwerten für jeden Cluster ein Zentrum (Zentroid) ausgewählt. Die Elemente werden initial (zum Beispiel zufällig) zu den Clustern zugeordnet. Im nächsten Schritt werden die Abstände der einzelnen Punkte zum Beispiel mithilfe der euklidischen Distanz zu den Zentroiden neu berechnet. Dann werden die Elemente zu den am nächsten befindlichen Zentroid und seinem Cluster zugeordnet. Im nächsten Schritt werden die Zentroide erneut berechnet und die Elemente dementsprechend zugeordnet. Diese Schritte wiederholen sich iterativ so lange, bis kein Punkt mehr zu einem anderen Cluster zugeordnet werden kann. Der k-Means-Algorithmus ist einfach umzusetzen, er besteht im Prinzip nur aus Abstandsberechnungen und Neuzuordnungen und kommt iterativ zu einem stabilen und effektiven Cluster. Die Anzahl der gewünschten Cluster müssen als Eingabewert ( $k$ ) bestimmt werden.

**Eingabedaten (1)** in Abb. 15.10:

- beliebige Objekte
- Abstandsmaß
- Anzahl  $k$  Cluster
- initiale Zuordnung der Elemente zu Clustern (zum Beispiel zufällig)



**Abb. 15.10** k-Means-Algorithmus

#### ML-Algorithmus (2) in Abb. 15.10:

- Berechnung der **Schwerpunkte** (Zentroide)
- Zuordnung der Elemente zu Cluster mit dem nächsten Zentroid
- Neuberechnung der Zentroide und erneute Zuordnung

#### Ergebnis (3) in Abb. 15.10:

- Einteilung der Objekte in k Cluster

#### k-Means-Algorithmus – Beispiel

Die Daten von Malware (Palevo, Virut, Mariposa), ein Abstandsmaß, die Anzahl der Cluster  $k=3$  werden als Eingabedaten übergeben. Die Objekte erhalten eine initiale Zuordnung zu den drei Clustern. Dabei repräsentiert jede Farbe eine Malware-Familie, Rot für Virut, Weiß für Palevo und Blau für Mariposa. Im nächsten Schritt werden die Abstände der Objekte zu den Zentroiden berechnet und gegebenenfalls zu einem näher liegenden Zentroid neu zugeordnet. Anschließend werden die Zentroide, durch die neuen Zuordnungen, ebenfalls neu berechnet und angepasst. Der Prozess wiederholt sich so lange, bis keine Verbesserungen mehr möglich sind.

#### Eingabedaten (1) in Abb. 15.11:

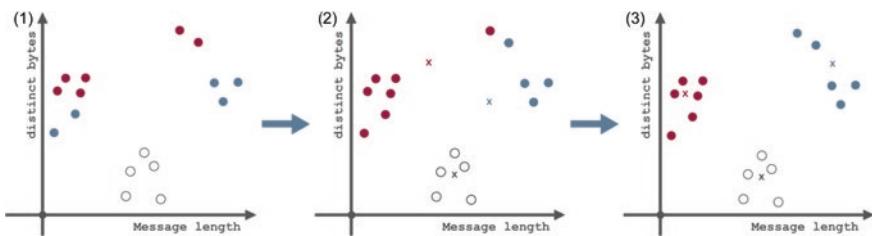
- Daten von Malware (Palevo, Virut, Mariposa)
- Abstandsmaß
- $k=3$
- initiale Zuordnung nach Message length, distinct bytes

#### ML-Algorithmus (2) in Abb. 15.11:

- Berechnung der Durchschnitte
- Zuordnung der Elemente zur Art der Malware mit dem nächsten Zentroid
- Neuberechnung der Zentroide und erneute Zuordnung

#### Ergebnis (3) in Abb. 15.11:

- Einteilung der Malware in die drei Malwarearten
  - Rot = Virut
  - Weiß = Palevo
  - Blau = Mariposa



**Abb. 15.11** Einteilung der Malware in verschiedene Malwarearten

#### 15.5.4 ML-Algoritmus: Hierarchische Clustering-Verfahren

Bei hierarchischen Cluster-Verfahren entstehen geschachtelte Cluster, die wiederum aus Clustern entstehen. Hierbei werden zu Anfang viele kleine Cluster gebildet, die im weiteren Verlauf zur größeren Clustern zusammengeführt werden. Das Ergebnis wird in einem Dendrogramm dargestellt.

Jedes Objekt der Eingabedaten ist zu Beginn ein eigenes Cluster. Durch das gewählte Ähnlichkeitsmaß werden ähnliche Cluster zu einem größeren Cluster zusammengeführt. Die zusammengeführten Cluster werden wiederum als Eingabedaten verwendet und weiter zusammengeführt. So entsteht nach jeder Iteration eine hierarchische Struktur.

**Eingabedaten (1)** in Abb. 15.12:

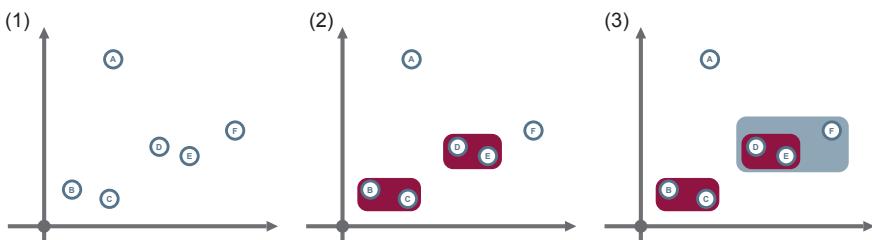
- beliebige Daten
- Ähnlichkeitsmaß

**ML-Algoritmus (1) bis (5)** in den Abb. 15.12 und 15.13:

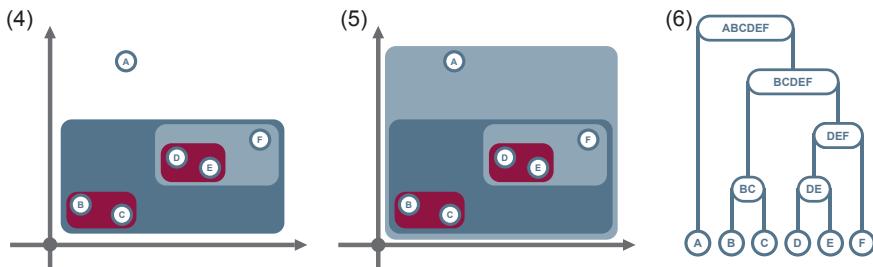
- jeder Datenpunkt ist ein eigenes Cluster
- ähnliche Cluster werden zuerst zusammengeführt
- entstandene Cluster werden erneut als Eingabedaten verwendet
- iteratives Zusammenführen der Cluster induziert eine hierarchische Struktur

**Ergebnis (6)** in Abb. 15.13:

- hierarchische Beziehungen zueinander in Form eines Binärbaums (Dendrogramm)

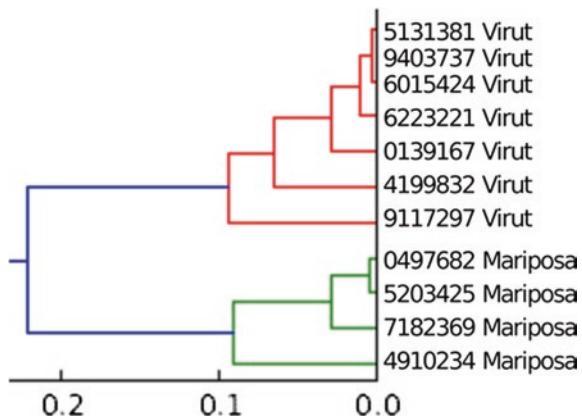


**Abb. 15.12** Hierarchische Clustering-Verfahren – Teil 1



**Abb. 15.13** Hierarchische Clustering-Verfahren – Teil 2

**Abb. 15.14** Hierarchisches Clustering für die Malware-Familien



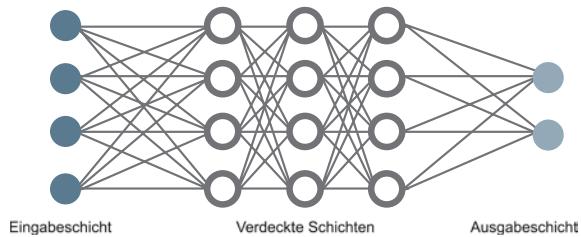
### Hierarchische Clustering-Verfahren – Beispiel

Die Daten aus der Botnet-Analyse werden einem hierarchischen Clustering unterzogen. Dazu wird eine komplexe Distanzfunktion benutzt, welche das Ähnlichkeitsmaß zwischen den Objekten beziehungsweise den Clustern berechnet. Der Wertebereich liegt zwischen 0 und 1. Bei einer hohen Ähnlichkeit der Cluster werden diese zu einem neuen Cluster zusammengefasst. Die Malware-Daten werden schrittweise zusammengeführt. Im vorliegenden Beispiel werden durch das hierarchische Clustering zwei Cluster für die Malware-Familien Virut und Mariposa gebildet, siehe Abb. 15.14.

### 15.5.5 Künstliche Neuronale Netze (KNN)

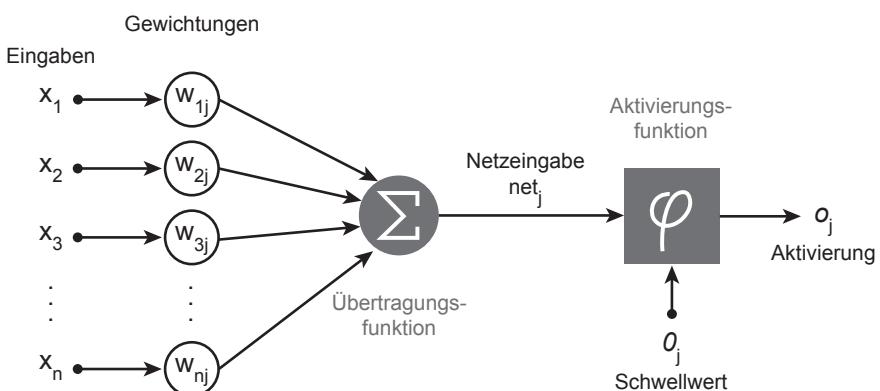
Die Vorlage von Künstlichen Neuronalen Netzen (KNN) ist die biologische Struktur des Gehirns und seiner Neuronen, siehe Abb. 15.15. Dabei werden Gewichtete, mathematische Funktionen und miteinander verbundene Schichten aus künstlichen Neuronen für die Informationsverarbeitung genutzt. Die Struktur eines Künstlichen Neuronalen Netzes besteht aus einer Eingabeschicht, verdeckten Schichten und einer Ausgabeschicht. Die Schichten selbst bestehen wiederum aus einer Vielzahl an künstlichen Neuronen.

**Abb. 15.15** Künstliche Neuronale Netze (KNN)

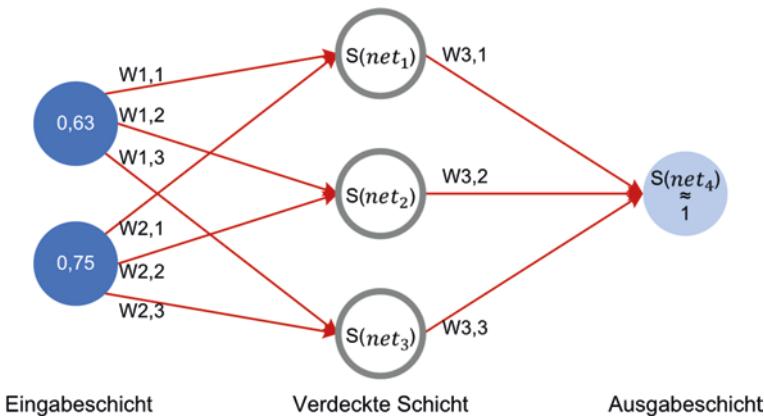


Die Eingabeschicht dient der Informationsaufnahme. Die Eingabedaten werden in verwendbare Repräsentationen transformiert. Je nach Komplexität und Problematik der Aufgabe kann ein KNN bis zu einer beträchtlichen Anzahl miteinander verknüpfter verdeckter Schichten besitzen, welche mit jeder weiteren Schicht immer komplexere Merkmale und Strukturen herausfiltern soll. Am Ende gibt die Ausgabeschicht die Ergebnisse in sämtlichen möglichen Repräsentationen aus.

Bei einem künstlichen Neuron (siehe Abb. 15.16) berechnet die Übertragungsfunktion anhand der Summe der Gewichtungen der Eingaben die Netzeingabe. Jedes Neuron hat einen individuellen Schwellenwert, der durch eine Schwellenfunktion berechnet wurde. Im Lernvorgang wird der Schwellenwert anhand der Eingaben stetig optimiert. Übersteigt die Netzeingabe den Schwellenwert, wird das Neuron aktiviert. Biologisch stellt der Schwellenwert die Reizschwelle dar, ab der das Neuron aktiviert wird. Als Aktivierungsfunktion kann zum Beispiel die Sigmoidfunktion verwendet werden, die die Summe der Eingabe für die Ausgabe auf einen Wertebereich zwischen 0 und 1 abbildet. Im Gegensatz zum Schwellenwert, der bei jedem Neuron individuell sein kann, gilt die Aktivierungsfunktion für jedes Neuron.



**Abb. 15.16** Künstliches Neuron



**Abb. 15.17** KNN-Beispielkonzept

### KNN-Beispiel

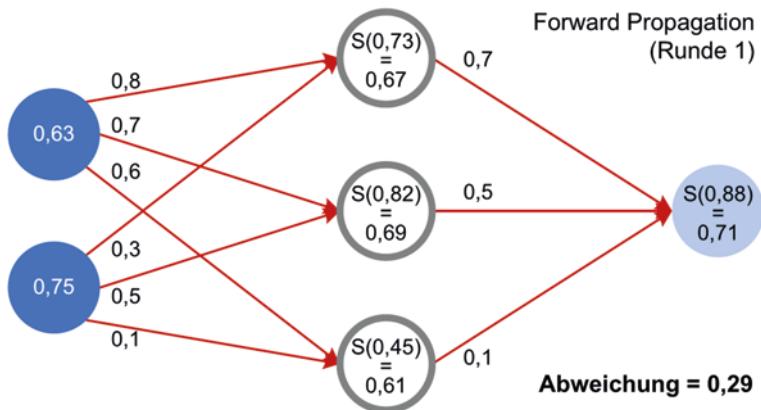
Eine wesentliche Stärke von KNNs liegt darin, dass die verdeckten Schichten autark ein Modell zu den gelieferten Ein- und Ausgabedaten approximieren können. Der Entwickler eines KNN muss dafür die Ein- und Ausgabedaten in eine verwendbare Repräsentation transformieren und einige Stellschrauben betätigen, wie zum Beispiel die Anzahl der verdeckten Schichten und die Anzahl der Neuronen.

Nachfolgend wird anhand eines Rechenbeispiels dargestellt, wie ein KNN zu den bereitgestellten Ein- und Ausgabedaten ein Modell in mehreren Evaluationsrunden erstellt. Als Eingabe werden die zwei höchsten Ähnlichkeitsmaße der verschiedenen Prozessauftrufe aus dem Beispiel in Abschn. 15.5.2 verwendet. Basierend auf den Ähnlichkeitsmaßen soll das erzeugte KNN berechnen, ob ein Prozess „normal“ ist, also im Sinne der Cyber-Sicherheit ungefährlich ist.

In diesem Beispiel wird der Einfachheit halber nur ein Ausgabewert betrachtet. Wenn das KNN eine 1 ausgibt, dann wird ein Prozess als „normal“ betrachtet. Die zugehörige Struktur des konzipierten KNNs ist in Abb. 15.17 dargestellt.

Die Berechnungen innerhalb des KNN lassen sich grundsätzlich in zwei Phasen unterteilen. In der ersten Phase werden die Berechnungen von der Eingabeschicht in Richtung der Ausgabeschicht durchgeführt (Forward Propagation). Abweichungen im daraus resultierenden Ergebnis werden anschließend durch eine rückwärts gerechnete Anpassung der Kantengewichte minimiert (Back Propagation). Nachdem die Kantengewichte angepasst wurden, werden die beiden Phasen erneut durchlaufen. Diese Vorgehensweise wird so lange wiederholt, bis das Ergebnis in der Ausgabeschicht möglichst genau approximiert wurde. Abhängig von der konkreten Problemstellung können mehrere tausend Runden nötig sein. In diesem einfachen Rechenbeispiel werden nur zwei vorwärts gerichtete Runden und eine rückwärtsgerichtete Runde betrachtet.

In Abb. 15.18 ist die erste vorwärts gerichtete Runde mit zufällig gewählten Kantengewichten dargestellt.



**Abb. 15.18** KNN Forward Propagation Runde 1

Als Aktivierungsfunktion wird in diesem Beispiel die Sigmoidfunktion verwendet. Die Sigmoidfunktion ist folgendermaßen definiert:

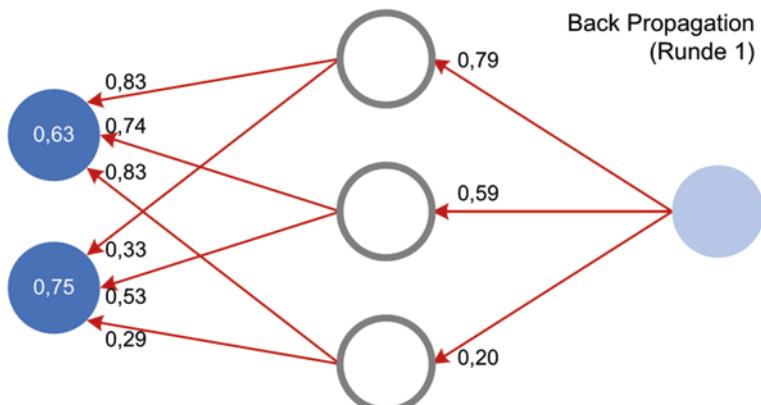
$$S(t) = \frac{1}{1 + e^{-t}}$$

Bei der Forward Propagation werden die Netzeingaben für jedes Neuron auf Basis der Eingabewerte und der entsprechenden Kantengewichte folgendermaßen berechnet:

$$\text{net}_j = 0,63 * W1,j + 0,75 * W2,j, \quad 1 \leq j \leq 3$$

$$\text{net}_4 = S(\text{net}_1) * W3,1 + S(\text{net}_2) * W3,2 + S(\text{net}_3) * W3,3$$

Der Abb. 15.19 kann entnommen werden, dass in der ersten Forward Propagation eine Abweichung von 0,29 erzielt wurde. Diese Abweichung berechnet sich aus der Differenz von dem gewollten Ausgabewert (in diesem Beispiel der Wert 1 für einen „normalen“ Prozess) und dem aktivierte Ausgabewert des KNNS.



**Abb. 15.19** KNN Back Propagation Runde 1

$$\text{Abweichung} = 1 - S(\text{net}_4)$$

Diese Abweichung wird nun zurück gerechnet, damit die Kantengewichte entsprechend angepasst werden können. In diesem Beispiel wird die folgende Ableitung der Sigmoidfunktion für die benötigte Änderungsrate der Kantengewichte verwendet:

$$S'(t) = S(t) * (1 - S(t))$$

Die konkrete Änderungsrate wird dann wie folgt berechnet:

$$\Delta = S'(\text{net}_4) * \text{Abweichung}$$

Die neuen Kantengewichte zwischen der verdeckten Schicht und der Ausgabeschicht werden mit der folgenden Formel berechnet:

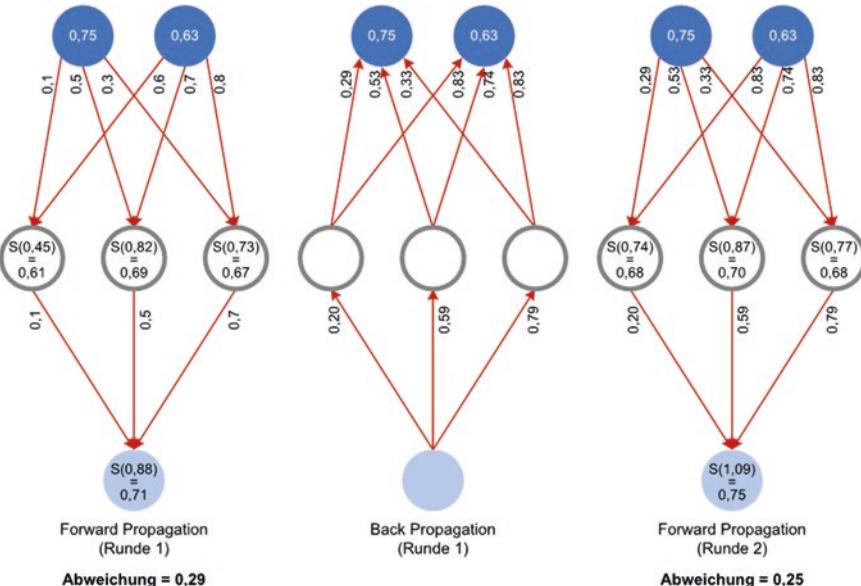
$$W_{3,j\text{new}} = W_{3,j} + \frac{\Delta}{S(\text{net}_j)} \quad 1 \leq j \leq 3$$

Alle neuen Kantengewichte zwischen der Eingabeschicht und der verdeckten Schicht lassen sich nun folgendermaßen berechnen:

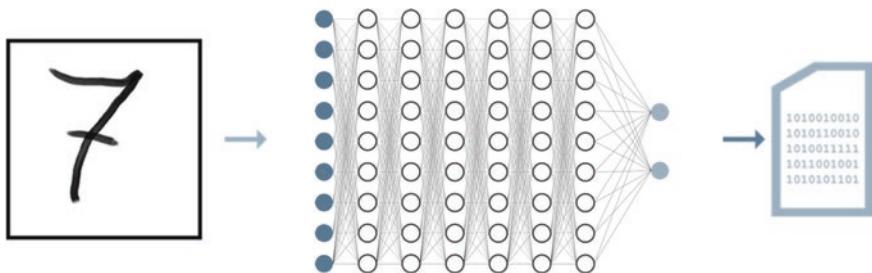
$$W_{i,j\text{new}} = \frac{\Delta}{W_{3,j}} * S'(\text{net}_j), \quad 1 \leq i \leq 2, 1 \leq j \leq 3$$

Das Ergebnis der neu berechneten Kantengewichte ist in Abb. 15.19 dargestellt.

Mit den neu berechneten Kantengewichten kann nun eine erneute Forward Propagation durchgeführt werden. In der zweiten Runde kann festgestellt werden, dass die Abweichung auf 0,25 reduziert werden konnte. Das Gesamtergebnis aller Berechnungen innerhalb der einzelnen Runden ist in Abb. 15.20 zusammengefasst.



**Abb. 15.20** KNN Gesamtergebnis



**Abb. 15.21** Beispiel Handschriftenerkennung

### 15.5.6 Deep Learning

Die KI-Forschung hat in den vergangenen Jahren und Jahrzehnten verschiedene Architekturen hervorgebracht, die bestimmte Aufgabentypen besonders gut lösen. Die komplexen Schichtenarchitekturen, wie Convolutional Neural Nets (CNN) oder Long Short-Term Memory Networks (LSTM), profitieren von enormen Datenmengen und haben daher bessere Ergebnisse im Big-Data-Bereich. Bei Deep Learning ist kein händisches Feature Engineering mehr notwendig, daher ist weniger Domänenwissen erforderlich.

#### Deep Learning Handschriftenerkennung Beispiel

Die Eingabe besteht aus einem Bild mit einer handschriftlichen Ziffer, siehe Abb. 15.21. Je nach der Größe des Bildes könnte ein Eingabeneuron genau ein Bildpixel repräsentieren. Bei diesem Vorgang werden die Helligkeitswerte der Pixel an die Eingabeneuronen übergeben. Die Helligkeitswerte aus der Eingabeschicht werden in den Neuronen der verdeckten Schichten weiterverarbeitet. Die Ausgabeschicht besteht aus zehn Neuronen, wobei ein Neuron jeweils eine Ziffer von 0–9 repräsentiert. Die Ausgabe liefert als Ergebnis eine Tabelle mit den Ziffern und deren Wahrscheinlichkeit einer Übereinstimmung. Folglich ist aus der Tabelle zu entnehmen, dass es sich zu 85 % um eine Sieben handeln könnte.

#### Eingangsdaten:

- Bilddatei mit einer Zahl, die klassifiziert werden soll

#### ML-Algorithmus (Deep Learning):

- Eingabedaten werden in den künstlichen Neuronen in den Schichten verarbeitet

#### Ergebnis:

- Tabelle mit einer Verteilung der Wahrscheinlichkeiten für eine Übereinstimmung mit einer Ziffer, siehe Abb. 15.22

Ziffer	0	1	2	3	4	5	6	7	8	9
Übereinstimmung	0 %	7 %	1%	0 %	4 %	0 %	0 %	85 %	0 %	3 %

**Abb. 15.22** Wahrscheinlichkeiten für eine Übereinstimmung mit einer Ziffer

## 15.6 Anwendungsszenarien von KI und Cyber-Sicherheit

Im Folgenden werden einige ausgewählte Anwendungsszenarien von KI und Cyber-Sicherheit aufgezeigt, um die Anwendungsvielfalt zu demonstrieren.

### Betrugsschutz im Online-Banking

Im Bereich des Online-Bankings kann zum Beispiel mithilfe von KI ermittelt werden, ob eine erhöhte Bedrohungslage herrscht. Dazu werden verschiedene Datenquellen herangezogen und beispielsweise ermittelt, wie viele Banking-Trojaner aktuell aktiv sind, ob es aktuell bekannte Software-Schwachstellen im Umfeld von Online-Banking gibt, die für einen Angriff auf Bankkunden verwendet werden könnten oder ob derzeit vermehrt versucht wird, mit Phishing-Mails Zugangsdaten zu Online-Konten abzugreifen. Diese und andere Indikatoren, wie identifizierte Betrugs- oder Betrugsvorfallsfälle der Bank, können dann verwendet werden, um mit verschiedenen Algorithmen aus dem Bereich des Maschinellen Lernens ein Bedrohungslagebild zu erstellen und den Bankkunden bei hoher Bedrohung zu warnen und entsprechend aufzuklären, um die Schäden zu verhindern.

### Erkennen von Angriffen über das Internet und Kommunikationslagebild

Durch die Analyse der Kommunikationsdaten kann mithilfe von KI Angriffe über das Internet erkannt werden. Dadurch können die Kommunikationsmöglichkeiten entsprechend reduziert werden, um den Angriff abzuwehren. Die Reduzierung kann sich zum Beispiel auf einen bestimmten Port oder die ganze Internet-Kommunikation beziehen. Ob ein IT-Sicherheitsexperte bei der Entscheidung eingebunden wird oder das Cyber-Sicherheitssystem dies automatisiert durchführt, ist ein wichtiger Aspekt für die Effektivität und Kosten des Systems. Die Ergebnisse können dann in ein Security Information and Event Management (SIEM)-System einfließen und zum besseren Management von Vorfällen führen. Zusätzlich kann auch ein Kommunikationslagebild erstellt werden, um Angriffe, Bedrohungen und Schwachstellen eines Netzwerks auszuwerten und Handlungsempfehlungen zu geben.

### Authentifikationsverfahren

Passive, kontinuierliche Authentifizierung ist besonders bei der zunehmenden Verbreitung mobiler Endgeräte ein Zukunftsfeld für KI-Algorithmen. Sensordaten aus Beschleunigungsmessgeräten oder Gyroskopen können während der Nutzung des Gerätes erhoben und ausgewertet werden. Die KI kann folglich unberechtigte Nutzer von der Gerätenutzung ausschließen. Solche Authentifizierungsverfahren sind ein weiterer Schritt zur Usability von robusten und sicheren Cyber-Sicherheitsmechanismen. Diese sind außerdem inklusiv, da sie keine zusätzliche Nutzerinteraktion erfordern und auch von Nutzern mit (beispielsweise kognitiven) Einschränkungen genutzt werden können. Neben der Analyse von Sensordaten ist auch eine verbesserte Authentifizierung anhand von Bild- oder Spracherkennung

möglich, da die Hardware zum Aufnehmen in den Endgeräten vorhanden und die Algorithmen zur Auswertung besser geworden sind.

### Malware-Erkennung

Die konventionelle Malware-Erkennung basiert zumeist auf signaturorientierten Detektoren, die bei einer Überprüfung die Signaturen von Dateien und Programmen mit bekannten Signaturen von Malware vergleicht. Wird Malware jedoch nur minimal verändert, kann die Signatur nicht mehr zur Erkennung genutzt werden. Heutige Malware verändert sich daher dynamisch. Dies hat zur Folge, dass immer neuere Varianten erscheinen und die Analyse und Aktualisierungen der Signatur-Datenbanken kaum noch effizient zu bewältigen ist. KI-basierte Detektoren können genutzt werden, um in Echtzeit verdächtige Aktivitäten zu erkennen. Anomalie-Erkennung oder Predictive Malware Analysis sind Verfahren, die durch den Einsatz von KI deutlich verbessert werden können.

### Threat Intelligence

Threat Intelligence ist aktuell meist auch signaturbasiert, mit denselben Nachteilen wie bei der signaturbasierten Malware-Erkennung. Threat Intelligence hat mit der starken Heterogenität von Unternehmensnetzwerken bei der Auswertung und Erkennung von Bedrohungen zu kämpfen. Hier könnten Deep Learning-Ansätze, die auch mit heterogenen Datensätzen arbeiten können, unter anderem bei der Analyse von Verhaltensmustern und Verhaltensprofilen den gewünschten Erfolg bringen und normale Prozesse von bösartigen unterscheiden (beispielsweise Latent Movement oder Exfiltration von Daten).

### Identifizierung von Spammails

Die klassischen Filtermethoden zur Identifizierung und Klassifizierung von Spammails anhand statistischer Modelle, Blacklists oder Datenbank-Lösungen stoßen schon heute an ihre Grenzen. Diese können zum Teil einen hohen Pflegeaufwand erzeugen, da diese regelmäßige und manuelle Überprüfungen oder Aktualisierungen erfordern. Absender von Spammails sind zunehmend in der Lage, ihre Mails als legitimate Mails zu obfuscieren und somit Filter zu überwinden. KI-Lösungen können dazu beitragen, komplexe Muster und Strukturen von Spammails zu identifizieren und zu erlernen, damit Spammails effektiv klassifiziert werden können. Durch jede neue richtig erkannte Spammail lernt die KI weitere Merkmale für die Erkennung. Das Automatisierungspotenzial ist bei einem Einsatz von KI hoch und hilft, IT-Spezialisten zu entlasten.

### IT-Forensik

Im Bereich der IT-Forensik werden KI-Systeme ebenfalls ein relevanter Faktor. Durch die vermehrte Verlagerung von Lebensbereichen in die digitale Welt werden auch zunehmend Straftaten im digitalen Raum begangen, deren Spuren in den gewaltigen Datenmengen der alltäglichen Nutzung gefunden werden müssen. Dabei stoßen klassische Analysewerkzeuge immer schneller an ihre Grenzen,

da IT-Systeme prinzipiell heterogener Natur sind. Verschiedene IT-Geräte mit unterschiedlichen Betriebssystemen, Installationen und Konfigurationen können unzählige Fragmente aufweisen, die im Kontext von Ermittlungen vielfältige Relevanz besitzen. KI-Anwendungen können hier beispielsweise dabei helfen zu entscheiden, ob bestimmte „Adressen“ von einer verdächtigten Person kontaktiert wurden, oder ob es sich um Fragmente handelt, die von Software-Entwicklern standardmäßig in ihr Programm eingebunden wurden – wie es unter anderem bei Support-Adressen häufig der Fall ist.

### **Advanced Persistent Threats & Cyber-Crime**

Analog zur Sammlung von Informationen zu Akteuren in klassischen Sicherheitsbereichen, um beispielsweise terroristische Aktivitäten bestimmten Gruppierungen zuordnen zu können, wird auch im digitalen Raum für Verteidiger immer wichtiger, Informationen über verschiedene Akteure zu sammeln und zu verarbeiten. So konnten in der Vergangenheit wiederholt Schadprogramme und Angriffe auf IT-Systeme, Einzelpersonen oder auch Gruppierungen zugeordnet und laufende Kampagnen identifiziert werden. Diese Informationen sind zum einen unerlässlich, wenn es um die Strafverfolgung, die Gewinnung weiterer Ermittlungsansätze und letztendlich gerichtsverwertbarer Beweise geht. Zum anderen können sie aber auch in Bedrohungslagebilder eingebettet werden und die Effektivität von Warnmeldungen erhöhen oder auch ganze Strategieentwicklungen im geschäftlichen wie (sicherheits-politischen) Sinne beeinflussen. Die korrekte Identifizierung von Akteuren und den von ihnen ausgehenden Bedrohungen hat demnach eine steigende Bedeutung, unterliegt dabei aber den gleichen Problemen wie in der analogen Welt. Indikatoren können manipuliert, Spuren verschleiert und sogar falsche Spuren gelegt werden. Zugehörigkeiten, Organisationsstrukturen und Geldflüsse werden verschleiert und Handlungsweisen verändern sich mit der Zeit. Des Weiteren steigt die Anzahl der potenziellen Opfer von Cyber-Kriminalität durch den digitalen Wandel kontinuierlich und erfolgreich angegriffene Systeme versprechen steigende Profite. Hier kann Künstliche Intelligenz unterstützen, indem bisher unerkannte Muster in Datenströmen und -mengen aufgedeckt und Manipulationsversuche enttarnt werden.

Zur Identifizierung von Akteuren auf der Angreiferseite kann eine Klassifizierung der Akteure vorgenommen werden, um Angriffsziele, Motivation, Risiken beziehungsweise Kritikalität und mögliche Gegenmaßnahmen einzustufen und zu bewerten. Eine Klassifizierung von Akteuren kann dabei anhand von Kategorien und Einordnungen erfolgen, beispielsweise interne versus externe Angreifer, Einzeltäter versus organisierte Gruppen, White Hats versus Black Hats, kriminell motivierte Angreifer versus Scriptkiddies, terroristisch motivierte Angreifer sowie staatliche Angreifer.

### **Weitere Anwendungsszenarien**

Weitere Anwendungsszenarien sind sichere Softwareentwicklung, Erkennen von Fake-News, Bilderkennung von Ausweisen, VideoIdent, biometrische Verfahren wie Tippverhalten, Gestik-Erkennung, Seitenkanalanalyse, Kryptoanalyse usw.

## 15.7 Manipulationen von Künstlicher Intelligenz

In diesem Abschnitt wird diskutiert, wie und an welchen Stellen die Künstliche Intelligenz mit ihren Algorithmen manipuliert werden kann [2].

**Eingabedaten** Die Qualität der Eingabedaten bestimmt auch die Güte der Ergebnisse. Hierbei gilt es, einige Faktoren zu beachten. So ist es beispielsweise bei Verwendung der persönlichen Daten eines Nutzers wichtig, dass diese auch Eigenschaften und Interessen der jeweiligen Person beschreiben. Wenn beispielsweise diese Daten aus dem Surfverhalten eines Browsers auf einem Smartphone resultieren, werden die Ergebnisse nicht optimal sein können, da sich nicht garantieren lässt, dass die Recherche des Nutzers ausschließlich seinem Informationsbedarf entspricht und nicht zufällig auch dem von Freunden oder Kollegen. Über eine Parametrisierung des Algorithmus ist der Betreiber zudem in der Lage, durch die Festlegung etwa von Schwellenwerten oder Grenzwerten die Ergebnisse zu beeinflussen. Die Eingabedaten, die Wissen und Erfahrungen in einem bestimmten Bereich dokumentieren, haben ebenso Einfluss auf die Ergebnisse. Daher ist die Kenntnis darüber, was davon genutzt wird, für die Bewertung sehr relevant. Denn wenn in den Eingabedaten Vorurteile und diskriminierende Ansichten enthalten sind, werden die modernen neuronalen Netze auch entsprechende Ergebnisse erzeugen. Heute ist es schwierig, die Eingabedaten darauf hin zu überprüfen, weil dafür ein gewünschtes Abbild bezüglich definierter Werte einer Gesellschaft vorhanden sein müsste, das jedoch (noch) nicht existiert.

**Manipulieren von Trainingsdaten** Die Eingangsdaten werden so manipuliert, dass Angriffe nicht mehr oder nicht mehr so gut erkannt werden. Zum Beispiel werden bei der Support-Vector-Machine die klassifizierten Eingangsdaten so modifiziert, dass die Hyperebene zur Trennung der klassifizierten Objekte so verändert wird, dass dadurch gezielt unerkannte Angriffe möglich sind.

**Algorithmus** Der Umgang mit Maschinellem Lernen ist oftmals geprägt durch Ausprobieren und benötigt viel Erfahrung. Es lässt sich vorab nicht eindeutig bestimmen, welcher Ansatz der bestmögliche für eine bestimmte Aufgabenstellung ist. Gerade im unüberwachten Ansatz besteht die reale Möglichkeit, dass Korrelationen in den Input-Daten gefunden werden, die in die Irre führen können. Die Herausforderungen in diesem Bereich liegen darin, eine geeignete Skalierbarkeit der Dateninfrastruktur und eine passende Architektur sowie Algorithmen der automatisierten Entscheidungsfindung abzuleiten. Die Architekten (Zielsetzungsgeber) und Programmierer (Umsetzer) können somit im Prinzip die Ergebnisse durch die konkreten Methoden und deren Umsetzung beeinflussen. Aus diesem Grund wird es zunehmend essenzieller, dass die Richtigkeit der Nutzung von Algorithmen validiert werden kann.

**Ergebnisse** Die Ergebnisse sind erst einmal (theoretisch) neutral, weil diese durch den Algorithmus berechnet worden sind. Abhängig von der konkreten Problemstellung, können die gelernten Ergebnisse in der Praxis als schützenswerte Ressource betrachtet werden, da sie beispielsweise Rückschlüsse auf sensible Eingabe- oder Ausgabedaten aus der Lernphase ermöglichen können (Model Inversion Attack).

Im Kontext eines Cyber-Sicherheitsmechanismus auf Basis einer Künstlichen Intelligenz könnten Cyber-Kriminelle die gelernten Ergebnisse verwenden, um beispielsweise den Erfolg von Angriffen im Vorfeld zu simulieren. Darauf aufbauend könnten von den Cyberkriminellen ggf. weitere Schutzvorkehrungen gegen eine Erkennung im Produktivumfeld implementiert werden.

Für derartige Angriffsszenarios könnten die Cyber-Kriminellen entweder direkt auf die gespeicherten Datenstrukturen einer Künstlichen Intelligenz zugreifen oder bereitgestellte Funktionen in der Anwendung einer Künstlichen Intelligenz verwenden (zum Beispiel API-Aufrufe), um anschließend die Ergebnisse zu rekonstruieren (Model Extraction Attack).

**Verwendung** Bei Verwendung der Ergebnisse sind die Einflussmöglichkeiten dann am größten. So kommen etwa bei der Google-Suchmaschine basierend auf dem Algorithmus die relevantesten Einträge in einer entsprechenden Reihenfolge heraus. Bei der Auflistung von Suchergebnissen jeglicher Art setzt Google jedoch an die erste Stelle Werbung, was eine Manipulation der Resultate darstellt, wie beispielsweise über den Hinweis „Anzeige“ dokumentiert wird. Aufgrund dessen ist es leicht vorstellbar, dass jegliche Ergebnisse mithilfe eines weiteren Algorithmus gemäß der Zielsetzung von Google manipuliert werden können, und damit nicht mehr die „relevantesten Einträge“ des eigentlichen Algorithmus sind, sondern die von Google präferierten. Diese Art der Manipulation lässt sich bei jedem automatisierten Entscheidungssystemen anwenden – nachlesbar auch in [3].

---

## 15.8 Beispiele von KI und Cyber-Sicherheit

In diesem Abschnitt werden Beispiele dargestellt, bei denen KI für Cyber-Sicherheitssysteme verwendet wird.

### 15.8.1 Alert-System auf der Basis eines kontinuierlichen Lagebilds über die aktuelle Gefahrenlage im Online-Banking

Für die Berechnung der aktuellen Gefahrenlage im Online-Banking wurden für die Evaluierung eines Alert-System unterschiedliche Off-the-shelf-Algorithmen des Maschinellen Lernens verwendet und miteinander verglichen. Die Effektivität des Alert-Systems wurde anhand von echten Betrugsfällen evaluiert, die bei einer Bankengruppe in Deutschland aufgetreten waren [4].

## Eingangsdaten

Phishing ist im Online-Banking eine weit verbreitete Strategie, um beispielsweise Passwörter, Kreditkartendaten oder TAN-Nummern zu stehlen. Phishing bezeichnet dabei die Technik, den Nutzer z. B. durch gefälschte E-Mails und Internetseiten dazu zu bewegen, dem Angreifer seine geheimen Informationen preiszugeben. Daher ist es für das hier beschriebene Alert-System wichtig, Informationen zum aktuellen Aufkommen von Phishing (Spam) zu erhalten. Aus den verwendeten Quellen wurden nur Informationen extrahiert, die im direkten Zusammenhang mit Online-Banking stehen. Innerhalb des entwickelten Alert-Systems wurden drei Quellen genutzt, die für Phishing-Angriffe relevant sind:

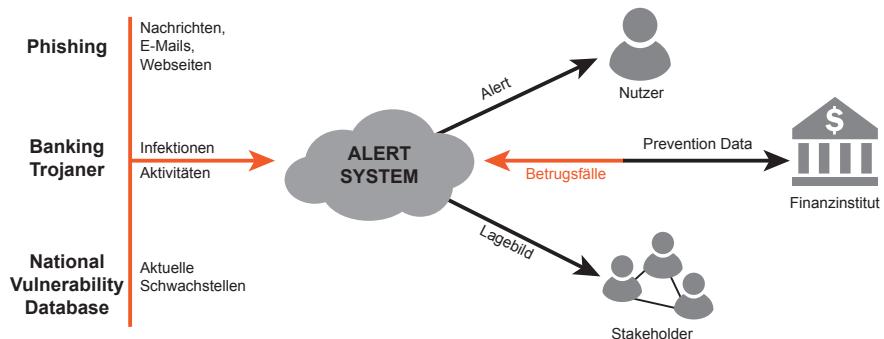
**E-Mail** Klassischerweise werden Phishing-Angriffe über E-Mails durchgeführt. Die Angreifer versenden eine E-Mail, die einer echten Nachricht der Bank gleicht, um den Kunden zu täuschen. In diesem Projekt wurden Spam-Nachrichten verwendet, die im „Spam Archive“ (<http://untroubled.org/spam/>) zur Verfügung gestellt werden. Im Beobachtungszeitraum (456 Tage) wurden insgesamt 670.622 Spammails im Archiv veröffentlicht. Anhand einer Stichwortsuche konnten 5589 relevante Mails für die Evaluierung identifiziert werden.

**Foren/Soziale Netzwerke** Phishing-Angriffe werden auch auf anderen Plattformen, z. B. in sozialen Netzwerken, Foren, oder Ähnlichem durchgeführt. Hier wird das Phishing z. B. über private Nachrichten oder öffentliche Posts durchgeführt. In dieser Evaluierung wurden Spam-Nachrichten genutzt, die auf den Webseiten des Stackoverflow-Netzwerkes erkannt werden (<https://metasmoke.erwaysoftware.com/search.json?body=financial>). Basierend auf einer Schlagwort-Suche wurden 1904 Nachrichten identifiziert.

**Webseiten** Zusätzlich wurde auf Information zu aktuellen Phishing-Webseiten zurückgegriffen. Als Quelle für Phishing-Seiten wurden alle Seiten verwendet, die von der Organisation PhishTank (<https://www.phishtank.com/>) veröffentlicht wurden. Insgesamt wurden anhand einer Klassifizierung von PhishTank und einer Schlagwortsuche 2776 Phishing-Seiten für den Testzeitraum gefunden.

Die Kennzahlen mit Bezug zum Phishing wurden zusammengefasst, um die Dimension der entwickelten Ansätze möglichst klein zu halten.

Wichtig für die Einschätzung der aktuellen Gefahrenlage beim Online-Banking ist auch die Aktivität von Banking-Trojanern. Da keine globale Sicht zu den zugehörigen Botnetzen verfügbar ist, müssten andere Indizien genutzt werden, um die Gefahr, die von einem Botnetz ausgeht, beurteilen zu können. Die Anzahl der Endgeräte, die mit einem Banking-Trojaner infiziert wurden, ist ein starker Indikator dafür, dass sich ein Nutzer mit einem Banking-Trojaner infizieren könnte (zum Beispiel wenn der Angreifer eine ‚Kampagne‘ zum Verteilen des Trojaners durchführt). In dieser Evaluierung wurden die erkannten Infektionen (insgesamt 23.184 im Testzeitraum) von Banking-Trojanern durch einen großen Hersteller von Antivirus-Produkten genutzt.



**Abb. 15.23** Konzept des Alert-Systems für Online-Banking

Die Gefahr, dass sich Nutzer mit Schadsoftware infizieren, kann aber auch anhand aktueller Software-Schwachstellen gemessen werden. Die Kennzahlen zu bekannten Schwachstellen wurden aus der National Vulnerability Database – NVD (<https://nvd.nist.gov/>) extrahiert. Die NVD beinhaltet Informationen zu Software-Schwachstellen, Fehlkonfigurationen und Metriken zu deren Einfluss. Von dem entwickelten Alert-System wurden nur Schwachstellen beachtet, die remote ausgenutzt werden können, gängige Browser und Betriebssysteme betreffen und die es erlauben, beliebigen Code auszuführen. In dem Testzeitraum traten 875 solcher Schwachstellen auf.

Für die Kontrolle des Alert-Systems wurden Betrugsfälle, die bei einer deutschen Bankgruppe aufgetreten sind, genutzt. Anhand dieser Betrugsfälle konnte die Effizienz der entwickelten Verfahren gemessen werden. In dem Testzeitraum lagen 459 Betrugsfälle vor. Abb. 15.23 zeigt die genutzten Quellen und deren Verwendung in dem Aufbau des Alert-Systems.

Die Effektivität des Alert-Systems  $S$  wurde in erster Linie anhand der Anzahl der korrekt identifizierten Betrugsfälle gemessen. Dieser Wert wurde in Relation zur Anzahl aller vorhandenen Betrugsfälle gesetzt. Für die Zielsetzung des Alert-Systems wurde zusätzlich eine Zeitkomponente zur Bestimmung der Effektivität hinzugefügt, damit die Menge der aktiven Alerts reguliert werden konnte. Ohne die Zeitkomponente könnte beispielsweise die Menge der aktiven Alerts zu groß und somit der angestrebte Mehrwert durch eine punktuelle Warnung verringert werden. Es musste also eine Metrik gewählt werden, die alle Alerts  $A$  und die daraus resultierende „Alert-Zeit“  $T$  in Betracht zieht.

Insgesamt ergibt sich aus diesen Überlegungen die Berechnungsvorschrift für die Ermittlung der Effektivität  $\text{eff}(S)$ .

$$\text{eff}(S) := \frac{\omega / \Omega}{T_{\text{Alert}} / T} = \frac{\omega * T}{\Omega * T_{\text{Alert}}}$$

$\Omega$  ist die Anzahl aller Betrugsfälle, die im gesamten Testzeitraum  $T$  aufgetreten sind. Des Weiteren ist  $T_{\text{Alert}}$  der Zeitraum, zu dem Alerts aktiv sind ( $n$  Tage nach

einem Alert) und  $\omega$  die Anzahl der Betrugsfälle, die in  $T_{\text{Alert}}$  liegen. Die Effektivität des Alert-Systems steigt demnach, wenn  $\omega$  steigt oder  $T_{\text{Alert}}$  fällt (oder beides).

Für die Bestimmung der Alert-Zeitpunkte wurden die gesammelten Kennzahlen aller Kategorien zuerst nach Tagen sortiert. Anschließend wurde mithilfe der betrachteten Off-the-shelf-Algorithmen für jeden Tag ein Maß bestimmt, das die aktuelle Gefahrenlage beschreibt.

### Trainings- und Testset

Alle gesammelten Daten wurden in ein Trainingsset (das erste Drittel der Daten – 152 Tage) und ein Testset (die restlichen zwei Drittel der Daten – 304 Tage) aufgeteilt, um die Vorhersagekraft der einzelnen Ansätze zu ermitteln und zu vergleichen.

Zum Trainieren der unterschiedlichen Ansätze wurden die gesammelten Daten in Bezug zu den Betrugsfällen, die in den zehn Tagen nach dem Auftreten der Kennzahl aufgetreten sind, gesetzt. Bei der Vorhersage handelt es sich also um ein Regressionsproblem. Anhand der vorliegenden Kennzahlen (Phishing, Malware und Schwachstellen) zum Zeitpunkt  $t$  wurde versucht vorherzusagen, wie viele Betrugsfälle in den folgenden  $n$  Tagen auftreten werden.

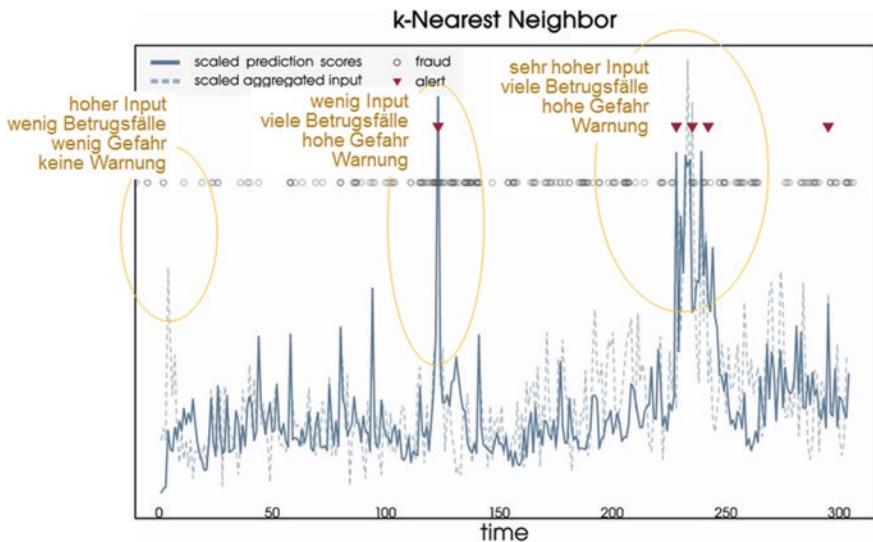
Als Grenzwerte für das Ausgeben eines Alerts wurden die Top 5 % (insgesamt ca. 16 Alerts je Ansatz) der bestimmten Gefahrenwerte (Anzahl der vorhergesagten Betrugsfälle) innerhalb des Trainingszeitraums genutzt. Der bestimmte Gefahrenwert der verschiedenen Ansätze kann ebenfalls für *Fraud-Prevention-Systeme* genutzt werden, um Transaktionen zu bewerten.

Als Vergleichswert für die Verfahren wurde ein allgemeines lineares Modell der Form  $\vec{y} := \mathbf{X} \vec{\beta} + \vec{\epsilon}$  mit  $X$  den unabhängigen Variablen (hier den Kennzahlen),  $\vec{\beta}$  den Regressionskoeffizienten, die anhand des Traingsets bestimmt wurden und  $\vec{\epsilon}$  dem Störfaktor genutzt. Zur Optimierung des Modells wurde die Methode *iteratively reweighted least squares* (IRLS) verwendet. IRLS bestimmt die Maximum-Likelihood in einem allgemeinen linearen Modell.

### k-Nearest Neighbor

Als erstes Verfahren wurde der *k-Nearest Neighbor* (k-NN)-Algorithmus zur Bestimmung der Alert-Zeitpunkte verwendet. Bei einer gegebenen Datenreihe (die aufaddierten Kennzahlen) kann der *k-NN*-Wert für einen Datenpunkt als lokale Dichte der Datenreihe gesehen werden. Je größer der *k-NN*-Wert ist, desto geringer ist die lokale Dichte und umso wahrscheinlicher ist es, dass es sich bei dem Punkt um einen Ausreißer handelt. Dieser „*local outlier factor*“ ist verhältnismäßig simpel. Die Ergebnisse sind allerdings mit moderneren Verfahren vergleichbar [4]. Der Vorteil des *k-NN*-Verfahrens ist, dass für jeden Datenpunkt ein Wert vorliegt, der angibt, wie stark sich dieser von den Nachbarn unterscheidet.

Bei der Bestimmung der Ausreißer werden nur die  $k$  Datenwerte der Reihe verwendet, die vor dem zu untersuchendem Punkt liegen. Bei einem realistischen Einsatz des Alert-Systems liegen nur Messwerte aus der Vergangenheit vor, die zur Bewertung der Situation genutzt werden können. Zur Bestimmung von  $k$  wurden die Trainingsdaten verwendet. Dazu wurde  $k$  anhand der Funktion  $\text{eff}(S)$  optimiert:  $\max \text{eff}_k(S); \quad k \in [1; 20]$ . Die Optimierung hat  $k = 8$  als optimales  $k$  bestimmt.



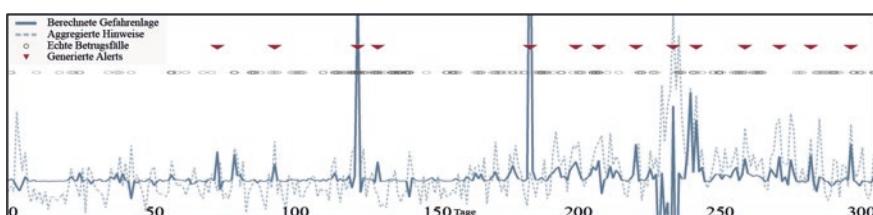
**Abb. 15.24** Berechnete Gefahrenlage mittels Support-State-Vector-Machine

In Abb. 15.24 – linke Seite – ist zu sehen, dass die aggregierten Hinweise (hoher Input) hoch waren, aber der Algorithmus trotzdem keine Warnung ausgegeben hat, was auch eine richtige Einschätzung war, da nur sehr wenige Betrugsfälle.

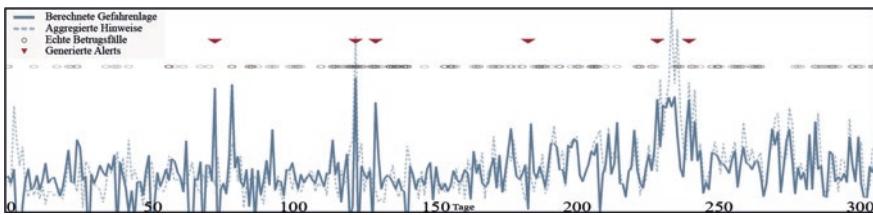
In Abb. 15.24 – in der Mitte – hat der Algorithmus eine hohe Gefahr berechnet und eine Warnung herausgegeben, was den realen Betrugsfällen auch entspricht.

### Support-State-Vector-Machine

Als weitere Technik wurde eine *Support-State-Vector-Machine* (SVM) oder passender *Support-Vector-Regression* (SVR) [4] verwendet, um das geschilderte Regressionsproblem zu lösen. Die verwendete SVM nutzt eine *polynomische* Kernel-Funktion ( $\phi$ ) dritten Grades und führt eine  $\epsilon$ -Regression durch. Zur Bestimmung des Models („model selection“) wurden die Hyperparameter der SVM (*cost* und *gama*) mittels „grid search“ optimiert. Die Alerts, die von der SVM berechnet werden, sind in Abb. 15.25 dargestellt.



**Abb. 15.25** Berechnete Gefahrenlage mittels Support-State-Vector-Machine



**Abb. 15.26** Berechnete Gefahrenlage mittels Künstlicher Neuronaler Netze

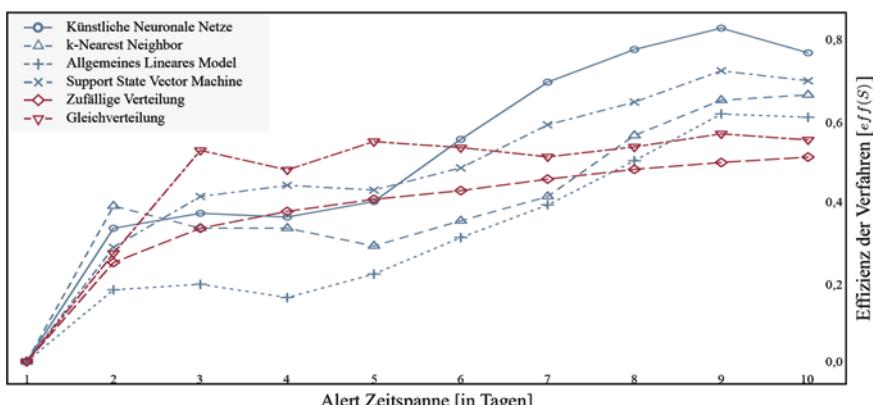
### Künstliche Neuronale Netze

Als letzter Ansatz wurde ein *Künstliches Neuronales Netz* (KNN) eingesetzt. Das Netz wurde als (3,3,1) Feed-Forward-Netz implementiert. Das heißt, dass jede Schicht nur mit der nächst höheren Schicht verbunden ist. 3 steht für die Anzahl der Input-Knoten, 3 für die Anzahl der Hidden-Knoten und 1 für die Anzahl der Output-Knoten. Das Netzwerk wurde mittels des RPROP-Verfahrens aufgebaut. Das Ergebnis des KNN-Ansatzes wird in Abb. 15.26 dargestellt.

### Vergleich der Verfahren

Zur besseren Einschätzung der Qualität der entwickelten Verfahren wurden diese mit zwei Basiswerten verglichen. Für den ersten Basiswert wurden Alerts zufällig platziert und deren Effektivität ( $eff(S)$ ) gemessen. Diese Effektivität wurde über 100 Durchläufe gemessen und anschließend gemittelt. Als weiterer Vergleichswert wurden 16 Alerts gleichmäßig auf den gesamten Testzeitraum aufgeteilt. Die Effektivität wird dann anhand dieser 16 Alerts gemessen.

Alle entwickelten Verfahren zeigen eine höhere Effektivität für  $n = 10$  als die verwendeten Basiswerte, wobei das *Neuronale Netz* die besten Ergebnisse liefert, siehe Abb. 15.27. Ebenfalls wird deutlich, dass ein Alarmierungszeitraum von mehr als sieben Tagen zu einem deutlichen Anstieg der Effizienz des Systems führt. Dies liegt auch daran, dass die Verfahren mit einem Wert von  $n = 10$  trainiert wurden.



**Abb. 15.27** Vergleich der Effizienz aller Verfahren

## Diskussion

Das erzeugte *Neuronale Netz* hat im durchgeführten Vergleich die besten Ergebnisse geliefert, allerdings ist die Zeit für das Trainieren des Systems deutlich höher (ca. dreifach so hoch) als bei den anderen betrachteten Verfahren.

Zur weiteren Optimierung der Bestimmung der Gefahrenwerte können weitere Kennzahlen in Betracht gezogen werden (z. B. die Aktivitäten von Banking-Malware innerhalb von Botnetzen oder auf mobilen Endgeräten). Ebenfalls können die Schadensfälle selbst als Hinweise genutzt werden und nicht wie in dieser Arbeit nur als Kontrollwerte.

Die von uns genutzten Hinweise bezüglich Phishing können weitaus umfangreicher gesammelt werden. Es können beispielsweise weitere soziale Netzwerke oder weitere Spam Honeypots als Hinweise genutzt werden. Bei einer größeren Menge an Hinweisen sollten jedoch modernere Ansätze der künstlichen Intelligenz („deep learning“) evaluiert werden. In dieser Arbeit wurden diese, aufgrund der limitierten Menge an Trainingsdaten, nicht betrachtet.

Die vom Alert-System bestimmte Gefahrenlage kann von einem Fraud-Prevention-System genutzt werden, um die Erkennung von bösartigen Transaktionen zu unterstützen. Infolgedessen könnte bei einem hohen Gefahrenwert und bei einer verdächtigen Transaktion das Autorisierungsverfahren dynamisch (zum Beispiel mehr Sicherheit auf Kosten von weniger Benutzerfreundlichkeit oder umgekehrt) festgelegt werden. Somit kann das Alert-System gleichermaßen zum bankenseitigen und nutzerseitigen Schutz genutzt werden.

### 15.8.2 Identifikation/Authentifikation eines Nutzers mittels Smartphone- Sensoren

In diesem Projekt wurde die Identifikation/Authentifikation eines Nutzers mittels Smartphone-Sensoren auf Basis von Maschinellem Lernen umgesetzt. Hierbei wurde nach einer Lösung für das Smartphone gesucht, die auf dem Produkt XignQR aufbaut, bei dem ein QR-Code eingescannt werden muss. Ziel des Projekts war es, die App so zu erweitern, dass als zweiter Faktor ein biometrischer Wert verwendet werden konnte, der ohne weitere Aktivität des Nutzers genutzt werden kann. Als Lösung wurde die Interaktion des Nutzers mit der XignQR-App ausgewählt. Die Bewegungsdaten des Nutzers mit dem Smartphone können als biometrisches Merkmal angesehen werden. Um diese Interaktion zu messen, wurden Sensoren des Smartphones verwendet. Die Erweiterung zur XingQR App sollte hierfür den Nutzer eines Smartphones anhand gesammelter Sensordaten identifizieren und ihm so den Zugang zu bestimmten Anwendungen oder Geschäftsprozessen durch eine positive Identifikation erlauben. Die Identifikation des Nutzers sollte über verschiedene Bewegungssensoren geschehen.

Als Sensoren wurden die folgenden ausgewählt:

**Accelerometer** Der Accelerometer oder Beschleunigungssensor misst die Beschleunigung des Smartphones und rechnet diese für jede der drei Achsen um.

**Gyroskop** Bestimmt die aktuelle Ausrichtung und Lage des Smartphones. Das Gyroskop misst im Gegensatz zum Accelerometer keine Beschleunigung, sondern eine rotatorische Geschwindigkeit. Auch beim Gyroskop ist das Koordinatensystem dreidimensional und relativ zum Gerät.

Die Nutzung der Sensordaten basiert auf der Idee, dass sich die Handbewegung sowie die Haltung des Smartphones bei jedem Nutzer beim Abscannen des QR-Codes voneinander unterscheidet und dadurch unterschiedliche Sensordaten initiieren. Die unterschiedlichen Sensordaten werden als nutzerbezogen betrachtet. Diese Betrachtung basiert auf der Annahme, dass der Nutzer sich die Handbewegung und die Haltung durch die jahrelange Smartphone-Nutzung antrainiert hat und diese für ihn typische Bewegung beim Abscannen des QR-Codes gewohnheitsgemäß verwendet. Ein Nutzer verursacht in der aktuellen Realisierung im Durchschnitt 230 Datensätze beim Abscannen des QR-Codes.

Die Sensordaten wurden mithilfe des Support-Vector-Machine-Algorithmus (SVM) und k-Nearest Neighbor Algorithmus (k-NN) untersucht. Das Verfahren liefert adäquate Ergebnisse, die die beschriebene Annahme bestätigen. Mit dem Verfahren ist das System momentan in der Lage, die Handbewegung des jeweiligen Nutzers sicher zu identifizieren. In einem Testlauf wurden 30 Nutzer mit 40 Authentifizierungen pro Nutzer umgesetzt. Die Ergebnisse sind:

### **k-NN: 46 Features**

FAR: 10 %, FRR: 0 %

- + einfach
- + gut geeignet für wenig Daten
- Rechendauer steigt proportional zur Anzahl der Daten
- Feature Extraction notwendig
- keine Klassifizierung mit einer Klasse

### **SVM: 6 Features**

FAR: 30 %, FRR: 5 %

- + schneller als k-NN
- + Klassifizierung mit einer Klasse möglich
- neigt zum over-fitting
- stark abhängig von den Parametern des SVM

### **Bewertung der Ergebnisse**

Beim k-NN Algorithmus sind die Ergebnisse schon sehr gut. Die Falschrückweisungsrate ist Null, was einen hohen Komfort des biometrischen Verfahrens mittels der Smartphone Sensoren darstellt. Die Falschakzeptanzrate ist mit 10 % gar nicht so schlecht. Einem von 10 Angreifern wird fälschlich Zugang gewährt. Das bedeutet in der Praxis, dass dieses Verfahren für den Nutzer einen Aufwand bedeutet und für die Anwendung ein weiteres Indiz dafür ist, dass der Nutzer echt ist. Bei wirklich wichtigen Anwendungen kann dieser Faktor nicht alleine verwendet werden.

### 15.8.3 Erkennung von netzwerkbasierten Angriffen mittels Künstlicher Intelligenz

In den vergangenen Jahren wurde in erster Linie mit signaturbasierten Systemen versucht, unerwünschten und bösartigen Netzwerkverkehr zu erkennen. Dies hat in der Vergangenheit für bekannte Angriffe dann funktioniert, wenn die dafür benötigten Signaturen, die mit erheblichem Aufwand kontinuierlich gepflegt werden müssen, verfügbar waren.

Um auch unbekannte Angriffe ohne Signaturen zu detektieren, wurden in den vergangenen Jahren vor allem mittels Machine Learnings (ML) große Erfolge erzielt. Hierbei werden typischerweise anhand des bekannten Netzwerkverkehrs Modelle (das Gedächtnis) trainiert, die den gewünschten Normalzustand des Netzwerks beinhalten und den Live-Verkehr damit abgleichen. Die Qualität der Ergebnisse von Machine Learning hängt vor allem von zwei Hauptfaktoren ab: den zur Verfügung stehenden Daten und den eingesetzten Algorithmen.

Für alle modernen Machine Learning-Algorithmen werden in der Regel sehr viele Trainingsdaten benötigt. Diese müssen einen sehr hohen Detailgrad von sicherheitsrelevanten Informationen aufweisen und sich gleichzeitig für eine Bearbeitung eignen. Den kompletten Netzwerkverkehr als „Big Data“ permanent speichern und diesen mittels ML trainieren zu wollen, ist technisch nicht machbar. Daher ist eine wichtige Strategie bei der Analyse von Netzwerkverkehr, alle wichtigen und sicherheitsrelevanten Informationen aus dem Netzwerkverkehr zu extrahieren und reduziert abzuspeichern, damit sie für das Trainieren von Algorithmen verwendet werden können.

Im Netzwerkbereich ist Netflow/IPFIX ein gängiges Format, das für eine Netzwerkverbindung (Flow) einige Merkmale (IP-Adressen, Ports, übertragene Bytes, etc.) extrahiert. Durch diesen Ansatz können eine grobe Netzwerkverkehrsvisualisierung dargestellt sowie einfache Angriffserkennungen realisiert werden. Für komplexe Detektionen werden allerdings noch mehr Details über die Netzwerkverbindung sowie deren Inhaltsdaten benötigt.

#### Technologischer Lösungsansatz

Diese Herausforderung kann mit einem innovativen Flow-Format (fs-Flow) für Netzwerksensoren umgesetzt werden, das den Datenverkehr viel detaillierter auf sicherheitsrelevanten Informationen analysiert und für die jeweiligen Flows bis zu vier Millionen Merkmale aus unterschiedlichen Netzwerkprotokollen unterscheiden und speichern kann (Smart Data). Diese beinhalten unter anderem Informationen über verwendete Browser und Betriebssysteme, Daten zur verwendeten Verschlüsselung, Inhaltsdaten von Web-Verkehr, aufgelöste Domains usw. Durch die Extraktion der Merkmale werden die ursprünglich enthaltenen wichtigsten sicherheitsrelevanten Informationen beibehalten und es wird darüber hinaus ermöglicht, diese sehr leicht mittels ML-Verfahren und Deep Learning zu trainieren (was auf Basis von reinem und rohen Netzwerkverkehr so nicht funktioniert). Dabei wird darauf geachtet, dass auch versteckte, aber gleichwohl sicherheitsrelevante Informationen weiterhin enthalten sind. Durch jahrelange

Erfahrung auf dem Gebiet und den Eigenentwicklungen können sehr schnell anhand gesammelter neuer Erkenntnisse das Flow-Format und die Sensoren angepasst und optimiert werden, um kontinuierlich noch bessere Ergebnisse zu erzielen.

Der komplette Netzwerkverkehr wird somit sehr detailliert auf die wichtigsten Merkmale reduziert sowie um sicherheitsrelevante Informationen angereichert, um diese Daten zum einen als Smart Data sehr lange vorhalten und zum anderen für die Machine Learning Algorithmen die Basis bieten zu können. Die anfallenden Daten können direkt in den Unternehmen unter Berücksichtigung der jeweiligen datenschutzrechtlichen Anforderungen analysiert werden, allerdings auch datenschutzkonform an eine zentralisierte Stelle übermittelt werden, um aus sehr vielen verschiedenen Unternehmen und Bereichen Daten für die Algorithmen zu erhalten, um diese damit stetig zu verbessern und kontinuierlich zu optimieren. Diese Smart Data-Ansammlungen sind zudem der Kern, um aus unstrukturierten Daten verwendbare Informationen zu generieren (Data Science). fs-Flow ist damit ideal für moderne und innovative Erkennungen sowie Vorhersagen und Prognosen geeignet.

Bei der Entwicklung von fs-Flow wurden die Expertise und die Erfahrungen im Umgang mit Algorithmen von Machine Learning und Data Science auf extrahierten Smart Data-Netzwerksdaten von 13 Jahren genutzt. Hierbei kommen sehr viele Algorithmen für unterschiedliche Problemlösungen zum Einsatz. Diese umfassen unter anderem sowohl Supervised Learning wie Naive Bayes und k-Nearest-Neighbor sowie Seasonal Average, Verhaltensanalysen und Decision Trees als auch Unsupervised Learning wie Apriori und das Hidden Markov-Modell.

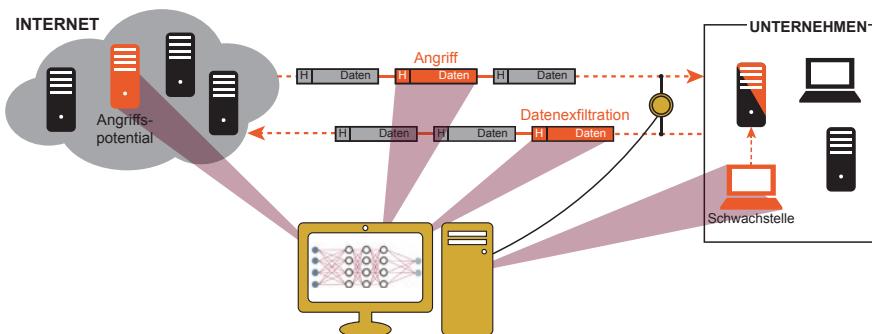
Schon vor über zehn Jahren wurden in diesem Kontext auch Neuronale Netze (NN) aus probabilistischen Ansätzen heraus verwendet. Diese waren damals allerdings aufgrund mehrerer Faktoren (Hardwareunterstützung, eingeschränkte Varianten von Neuronalen Netzen) nicht so geeignet. Dies hat sich in den jüngsten Jahren radikal geändert, sodass Neuronale Netze mittels Deep Learning nun mit den Smart Data-Ansammlungen mittels fs-Flow angewendet werden können. Dabei kann sowohl der Normalverkehr im Unternehmen als auch der bekannte Schadverkehr trainiert werden, um diesen noch zielgerichteter im Live-Betrieb detektieren zu können.

### Innovative Erkennungen

In vielen anderen Bereichen konnten durch den Einsatz von KI-Technologien bereits deutliche Verbesserungen erreicht werden. Daher bietet der Einsatz von KI auch im Kontext der Netzwerkerkennung sehr viele Chancen und Potenzial. Die fs-Flow-Daten eignen sich ideal, um innovative Erkennungen mittels KI und Verhaltensanalysen von Systemen durchzuführen. Es werden Verbindungen identifiziert, für die im Vorfeld sowohl „gutartige“ (normale Anwendungen wie E-Mail-Versand, TeamViewer, Cloud-Nutzung oder unternehmenseigene Protokolle) als auch „bössartige“ Netzwerkverbindungen (schadhafter Verkehr wie Trojaner, Ransomware etc.) trainiert wurden. Auf der Basis sowie aus detaillierten fs-Flow-Merkmalen wird ein Verhaltensmodell über die Kommunikationsbeziehungen für die jeweiligen Systeme

erstellt, das im Live-Betrieb kontinuierlich abgeglichen wird. Darüber hinaus werden die Systeme automatisch zu einer Gruppe klassifiziert, und Klassenänderungen beispielsweise durch eine Malware-Infektion gemeldet. So lassen sich neben klassischen Angriffen wie Distributed Denial of Service (DDoS), Brute-Force etc. auch moderne Schadsoftware mit Nutzung von Zero-Day-Exploits, Trojaner, Remote Administration Tools (RAT), Ransomware etc. sowie versteckte Kanäle für Command & Control (C&C), Lateral Movement und Exfiltration erkennen, die mit bisher gebräuchlichen Datenformaten nicht detektiert werden konnten. Weitere Beispiele sind ein infizierter Client-PC, der plötzlich nachts ungewöhnlich viel kommuniziert, eine unbekannte Malware-Kommunikation, die ähnlich bekannter/erlerner schadhafter Netzwerkverbindung ist oder eine Malware, die mittels Steganografie in Bildern periodisch auf sogenannte Image-Server zugreift. So konnten mit den neuen Ansätzen laterale Ausbreitungen in Unternehmen, Schadsoftware auf Steuerungssystemen (Industrial Control System – ICS) im Produktionsumfeld (Operational Technology – OT) sowie versteckte Kanäle, wie sie bei der Malware UDPoS und bekannten Advanced Persistent Threat-Gruppen (APT) zum Einsatz kamen, erkannt werden, siehe Abb. 15.28.

fs-Flow kann mit seinem universellen Ansatz alle netzwerkbasierten Bereiche eines Unternehmens wie Office, IT, ICS/OT und dem (Industrial) Internet of Things ((I)IoT) abdecken und deren spezifische Protokolle analysieren. In Verbindung mit dem verwendeten Machine Learning auf Smart Data und angepassten Modellen kommt der technologische Lösungsansatz so auch in der klassischen IT, als auch im ICS-Bereich sowie IoT-Diensten zum Einsatz. Beispiele sind hier ein bisher passiver ICS-Monitor, der plötzlich einigen ICS-Geräten fragwürdige Befehle gibt oder ein IoT-Gerät (wie Kühlschrank oder Webcam), das plötzlich mit einer Bürofernwartung gesteuert wird. Darüber hinaus kann kontinuierlich ein Lagebild über die IT-Sicherheit eines Unternehmens generiert und eine vollständige Netzwerktransparenz geschaffen werden.



**Abb. 15.28** Innovative Erkennung von schadhaftem Netzwerkverkehr

### Erkennen von Angriffen über das Internet

Durch die Analyse der Kommunikationsdaten in einem Unternehmensnetzwerk können mithilfe von KI Angriffe über das Internet auf das Netzwerk erkannt werden. Dadurch können die Kommunikationsmöglichkeiten des Netzwerkes sowohl intern als auch extern sowie zwischen Intranet, Extranet als auch Internet entsprechend kontrolliert und eingeschränkt werden, um den Angriff abzuwehren. Die Reduzierung kann sich zum Beispiel auf einen bestimmten Port oder die ganze Internet-Kommunikation beziehen. Ob in diesen Prozess auch ein Cyber-Sicherheitsexperte in die Entscheidung eingebunden wird oder das Cyber-Sicherheitssystem dies automatisiert durchführt, ist ein wichtiger Aspekt für die Effektivität und Kosten des Systems. Die Ergebnisse der Netzwerkanalyse können dann in ein Security Information and Event Management (SIEM)-System einfließen und zum besseren Management von Vorfällen beitragen. Darüber hinaus kann auch ein Kommunikationslagerbild des Firmennetzwerkes beziehungsweise Unternehmens erstellt werden, um Angriffe, Bedrohungen und Schwachstellen eines Netzwerks auszuwerten und konkrete Handlungsempfehlungen daraus abzuleiten.

### Gemeinsamer Austausch und Erstellung eines globalen Lagebildes

Ein wichtiger Aspekt für die Unternehmen ist, dass sie in Zukunft mehr Informationen über die allgemeine Angriffs- und Bedrohungslage in Netzwerken als Grundlage zur Einschätzung der Sicherheitslage haben, als die aktuellen Monitoring-Systeme in den eigenen Netzen zur Verfügung stellen. Derzeit beziehen Unternehmen relevante Sicherheitsinformationen üblicherweise über extern verfügbare Sharing-Plattformen und Feeds anderer Institutionen. Auf der operativen Ebene kommen vor allem bekannte Indicator of Compromise (IoC), wie IP-Adressen, Domains und URLs von bösartigen Systemen, Hashes von Malware-Samples etc. zum Einsatz. Dieser Austausch ist wichtig, um die bekannte Infrastruktur von Angreifern im eigenen Netzwerk leichter erkennen und aufspüren zu können.

Darüber hinaus werden allerdings noch Einblicke in die allgemeine Angriffs- und Bedrohungslage zur Vergleichbarkeit mit anderen Unternehmen benötigt, damit die noch nicht bekannten TI-Informationen zugeordnet werden können. Die fs-Flow-Daten bilden die Grundlage, um eine detaillierte und übergreifende Sichtbarkeit zu gewährleisten. Diese können unter Einbehaltung vieler qualifizierter Merkmale aggregiert und datenschutzkonform mit anderen Unternehmen ausgetauscht werden, um eine Vergleichbarkeit herzustellen.

---

## 15.9 Zusammenfassung

Die Cyber-Sicherheit im Internet kann auf vielfältige Weise von den bereits existierenden Verfahren aus dem Bereich der Künstlichen Intelligenz und den zugehörigen Teildisziplinen profitieren. Als konkrete Beispiele hierfür wurde die Erstellung von Lagebildern im Online-Banking, die Identifikation und Authentifizierung mithilfe von Sensordaten und die Erkennung von netzwerkbasierten

Angriffen vorgestellt. Diese äußerst unterschiedlichen Beispiele sollen verdeutlichen, dass bei der Entwicklung eines KI-gesteuerten Cyber-Sicherheitsmechanismus grundsätzlich die Prinzipien des Maschinellen Lernens in den Kontext der zugrunde liegend Problemstellung gebracht werden müssen. Aus Sicht eines Entwicklers können die einzelnen Bestandteile eines KI-Verfahrens als „Black-box“ betrachtet werden. Die Güte der Ergebnisse hängt überwiegend von der Güte der Modellierung der Problemstellung ab und wie die einzelnen Verfahren dort integriert werden.

Da ein Cyber-Sicherheitsmechanismus auf Basis von KI grundsätzlich ein IT-System im klassischen Sinne darstellt, müssen sowohl die klassischen Angriffsvektoren, als auch neue spezielle Angriffe auf die KI verhindert werden.

Künstliche Intelligenz im Bereich Cyber-Sicherheit wird helfen, Angriffe besser zu identifizieren, die wenigen Cyber-Sicherheitsexperten zu unterstützen und die Wirkung von Cyber-Sicherheitslösungen zu erhöhen.

Außerdem wird Cyber-Sicherheit benötigt, um den Schutz von Künstlicher Intelligenz und deren Ergebnissen zu gewährleisten.

---

## 15.10 Übungsaufgaben

### Übungsaufgabe 1

Beschreiben Sie die zentralen Unterschiede des überwachten und des unüberwachten Lernens!

### Übungsaufgabe 2

Nennen und beschreiben Sie die grundlegenden Prinzipien des Maschinellen Lernens. Gehen Sie dabei insbesondere auf mögliche konzeptionelle Probleme und Gefahren innerhalb der einzelnen Prinzipien ein!

### Übungsaufgabe 3

Was ist die zentrale Idee eines Künstlichen neuronalen Netzes?

### Übungsaufgabe 4

Beschreiben Sie die Phasen eines Künstlichen neuronalen Netzes für die Erstellung eines Modells zu den gegebenen Ein- und Ausgabedaten!

Ergebnisse siehe: <https://norbert-pohlmann.com/cyber-sicherheit/uebungen/>.

---

## Literatur

1. Pohlmann N (2015) Kann Big Data Security unsere IT-Sicherheitssituation verbessern? KES Z Informations-Sicherh 2015(März)
2. Coester U, Pohlmann N (2018) Diskriminierung und weniger Selbstbestimmung? Die Schattenseiten der Algorithmen. tec4u, 12/17

3. Google: Konzern kassiert Milliardenstrafe für Manipulation von Suchergebnissen. <http://www.buffed.de/Google-Firma-97880/News/milliardenstrafe-manipulation-von-suchergebnissen-1231694/>
4. Paulisch C, Pohlmann N, Riedel R, Urban T (2018) Sei gewarnt! Vorhersage von Angriffen im Online-Banking. In: Proceedings der DACH Security 2018 Konferenz, syssec Verlag



Soziale Netzwerke als Mitmach-Web, wie Facebook, Partnerbörsen, YouTube, Instagram, XING, LinkedIn, Twitter und Co. bringen Nutzer aus verschiedenen Gesellschaftsgruppen zusammen und ermöglichen ihnen, sich darzustellen, Informationen und Meinungen auszutauschen sowie sich einfacher und zielgerichteter real zu begegnen. Soziale Netzwerke schaffen auch neue Wege, Demokratie und Bürgerbeteiligungen zu gestalten [1].

Aber der Erfolg der sozialen Netzwerke hat auch bekannte Nachteile und Herausforderungen im Bereich der Cyber-Sicherheit. Social Bots, Fake-News und Psychometrie können auch im Rahmen von Social Engineering-Angriffen verwendet werden.

Das typisch zugrundeliegende Geschäftsmodell bei sozialen Netzwerken, „Bezahlen mit persönlichen Daten“, ist für die informationelle Selbstbestimmung und den Datenschutz ein sehr großes Problem. Auch die Risiken des Verlustes der Privatheit und der Reputation der Nutzer werden immer größer mit der Bedeutung der sozialen Netze.

Die große Menge des „User generated Contents“ der vielen Nutzer bei Mitmach-Web ist enorm, wird immer größer und macht zunehmend Probleme. „User generated Content“ ist der Inhalt, den die Nutzer selber einstellen. Die Inhalte, die dabei Probleme machen, sind zum Beispiel rechtlich verboten, wie Kinderpornografie, Hate Speech, aber auch Fake-News. Es geht aber auch um mit Rechten behaftete Objekte, wie Bilder, Musik, Filme usw.

Social Bots sind Meinungsroboter, die Stimmungsbilder und Reputationsverlust zum Beispiel von Politikern und Unternehmen zielgerichtet beeinflussen. Beispiele der Beeinflussung sind: Ukraine-Konflikt, BREXIT, US-Präsidentschaftswahlkampf, Islamfeindlichkeit, Fremdenhass schüren, Unternehmen diskriminieren und damit Kurse beeinflussen usw. In diesem Kapitel werden die Herausforderungen analysiert und potenzielle Auswege diskutiert.

Das Risiko persönlich beleidigt oder diskreditiert zu werden oder Information, die falsch sind, nicht erkennen zu können, wird größer. Aus diesem Grund spielt die Cyber-Sicherheit im Bereich des Social Webs eine immer wichtigere Rolle.

## 16.1 Soziale Netzwerke

Inhalte, die Nutzer in soziale Netzwerke einstellen, User generated Content genannt, sind in der Regel Texte, Bilder, Grafiken, Videos, Filme, Kommentare, Musik, Audiodateien, Quellcode usw., siehe Abb. 16.1.

Der Sinn und Zweck von sozialen Netzwerken ist in der Regel die Darstellung des Nutzers zur Generierung seines Images und der Austausch von Meinungen, Informationen und Erfahrungen. Die interaktive Zusammenarbeit vieler Nutzer und der Austausch von Informationen und Meinungen helfen, auf dem neuesten Stand zu bleiben, insbesondere in den Gruppen, für die sich die Nutzer am meisten interessieren, wie zum Beispiel Freunde, Kollegen, Hobbys und politische Themen. Bei sozialen Netzwerken sind die Nutzer gleichzeitig Anbieter und Konsumenten von Inhalten. Der Betreiber der Plattform stellt lediglich eine soziale Netzwerkanwendung zur Verfügung, und die Nutzer sorgen selber für die Inhalte.

Die bekanntesten sozialen Netzwerke mit ihren spezifischen Kennzahlen sind:

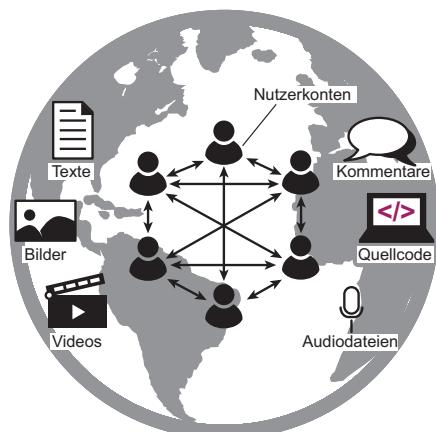
### Facebook

- hat über 2 Mrd. Nutzer und
- es werden jeden Tag durch die Nutzer ca. 4 Mrd. Texte, 60 Mio. Bilder und 100 Mio. h Videos eingestellt.

### Instagram

- hat ca. 800 Mio. Nutzer,
- es werden jeden Tag 95 Mio. Bilder eingestellt und
- 4,2 Mrd. Likes am Tag durchgeführt.

**Abb. 16.1** Web  
2.0-Anwendung – Soziales  
Netzwerk



### Bei Twitter

- sind ungefähr 330 Mio. Nutzer registriert und
- es werden 500 Mio. Tweets am Tag versendet.

### YouTube

- hat mehr als 1 Mrd. Nutzer,
- es werden jeden Tag mehr als 100 Mio. h Videos angesehen und
- ca. 450 Mio. h Videos eingestellt.

### Was ist das eigentliche Problem beim Mitmach-Web?

Beim Mitmach-Web stellt der Nutzer die Inhalte selber ein und ist dafür auch verantwortlich. Da viele Nutzer nicht ihre wahre Identität angeben, kann die Verantwortung nur sehr unzureichend vollstreckt werden. Die Betreiber von sozialen Netzwerken verstehen sich nur als Plattform und wollen keine Verantwortung für die Inhalte, die die Nutzer einstellen, übernehmen. Es gibt also keine zentrale Instanz, die für die Inhalte verantwortlich ist und dafür sorgt, dass keine rechtlich verbotenen Inhalte sowie mit Rechten behaftete Objekte eingestellt werden.

### Unterschied zu klassischen Medien wie Presse, Hörfunk und Fernsehen

Bei klassischen Medien übernehmen Redakteure die Aufgabe, aus der Fülle an Informationen, die in die Redaktion gelangen, interessante und bedeutsame Beiträge herauszufiltern und für das entsprechende Medium aufzubereiten. Hierbei steht vor allem die Zielgruppe des entsprechenden Mediums im Vordergrund und welche Berichte oder Nachrichten für diese von Interesse sind. Ein Redakteur recherchiert auch selbst und schreibt eigene Artikel. Nicht selbst geschriebene Texte werden vom Redakteur redigiert. Redigieren ist die Tätigkeit eines Redakteures, die darauf abzielt, aus dem eingegangenen Material eine inhaltliche und formale Einheit zu gestalten. Redigieren steht für Auswählen, Bearbeiten und Präsentieren des Stoffes in der dem Medium entsprechenden Form. Durch Redigieren wird auf das Wesentliche reduziert, Texte werden verständlich gemacht und auf die Zielgruppe zugeschnitten. Neben der Überprüfung des formalen Aufbaus, Rechtschreibung, Grammatik, Zeichensetzung, Rechte von genutzten Bildern sowie der sprachlich-stilistischen Überprüfung, wie Wortwahl und Verständlichkeit, ist es die Aufgabe des Redakteurs, die Richtigkeit der Fakten zu überprüfen. Die Überprüfung der Fakten ist ein wesentlicher Unterschied zu den Nachrichten, die in sozialen Netzwerken verteilt werden. Redakteure haben in der Überprüfung von Fakten sehr viele Erfahrungen und tun dies für alle, die auf entsprechende Medien zugreifen.

Aus diesem Grund treten Fake-News bei den klassischen Medien relativ selten auf. Wird eine Nachricht im Nachhinein als Fake-News erkannt, wird die Fake-News entfernt und dies in einer Klarstellung dokumentiert.

### Unterschied Meinungsfreiheit und Fake-News

Im Artikel 5 des Grundgesetzes steht: „Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film werden gewährleistet.“

Eine Zensur findet nicht statt.“ Die „Meinung“ ist der Ausdruck einer persönlichen Auffassung, die jemand von einer Sache hat. Dies kann uns gefallen oder nicht. Die Toleranz unterschiedlicher Meinungen ist ein wichtiger Garant für eine funktionierende Demokratie.

Fake-News sind Falschmeldungen, die auf falschen Tatsachen beruhen, und damit unabhängig von einer bestimmten Meinung falsch sind.

## 16.2 Fake-News

In diesem Abschnitt wird das Thema Fake-News diskutiert.

### 16.2.1 Was sind Fake-News?

Fake-News sind Falschmeldungen, die sich insbesondere in sozialen Netzwerken und anderen sozialen Medien verbreiten. Fake-News sind frei erfunden und sollen die Konsumenten bewusst täuschen. Im weiteren Sinne werden oft auch solche Nachrichten zu den Fake-News gezählt, die zwar einen wahren Kern besitzen, deren Aussagen aber verfälscht oder dekontextualisiert wurden (zum Beispiel durch irreführende Überschriften). Aber auch satirische Nachrichten können im weiteren Sinne ebenfalls als eine Art Fake-News bezeichnet werden, falls diese von den Lesern nicht als Satire erkannt werden.



Abb. 16.2: Frei erfundene Nachricht



Abb. 16.3: Aussage verfälscht



Abb. 16.4: Satire

#### Frei erfundene Nachricht: Renate Künast, siehe Abb. 16.2.

*Renate Künast „Der traumatisierte junge Flüchtling hat zwar getötet, man muss ihm aber jetzt trotzdem helfen.“*

Inhaltlich bezog sich diese Fake-News auf die Ermordung einer Studentin. Die junge Frau wurde Opfer eines Gewaltverbrechens. Täter war ein 17-jähriger Schüler aus Afghanistan, der 2015 nach Deutschland einreiste.

Mit dieser Fake-News sollte die Politikerin Renate Künast diskreditiert werden.

**Aussage verfälscht: Flüchtling**, siehe Abb. 16.3.

„Flüchtling aus dem Jemen findet 1.360 Euro und tut, was man erwartet.“

Durch diese irreführende Überschrift soll der Leser glauben, dass der Flüchtling aus dem Jemen das Geld eingesteckt hat und dass wir uns auf die Flüchtlinge nicht verlassen können. Real hat der Mann das Geld zurückgegeben und alles ist, wie wir es erwarten.

**Satire: Stiftung Warentest testet Atombombe**, siehe Abb. 16.4.

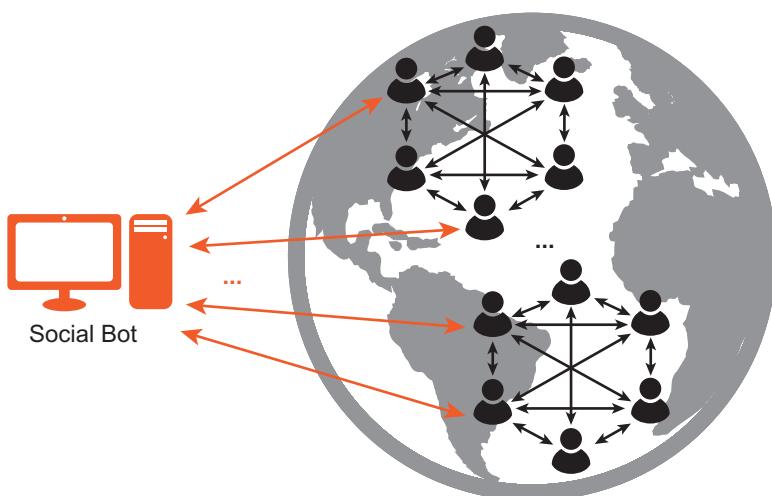
„Nur zwei schnitten „gut“ ab: Stiftung Warentest testet Atombomben.“

Diese Nachricht ist eine Satire, aber für die Leser, die das nicht sofort erkennen, bleibt nur der Gedanke zurück, dass wir uns nicht auf die Atombomben verlassen können.

## 16.2.2 Social Bot (die digitale Propaganda-Maschine)

Damit Fake-News eine sehr große Verbreitung und damit eine starke Wirkung haben, werden sogenannte Social Bots genutzt. Social Bots sind die digitalen Propaganda-Maschinen.

Ein Bot ist ein Roboter, ein autonom agierendes Programm im Internet. Eine Social Bot ist ein Meinungsroboter, der in den sozialen Netzwerken aktiv ist. Social Bots erstellen sehr viele Fake-Accounts, die vorgeben, von echten Nutzern eines sozialen Netzwerks zu sein und simulieren menschliches Verhalten. Sie werden programmiert und eingesetzt, um gezielt Meinungen im Internet massenhaft automatisiert zu verbreiten. Das Ziel von Social Bots ist es, durch ein verzerrtes Stimmungsbild eine größere Gruppe oder Gesellschaft in eine bestimmte Richtung zu beeinflussen, siehe Abb. 16.5.



**Abb. 16.5** Social Bot

Beispiele, bei denen Social Bots erfolgreich genutzt worden sind: Ukraine-Konflikt, Brexit-Wahl in Großbritannien, der US-Wahlkampf, ... Islamfeindlichkeit, Fremdenhass schüren, ...

Die Herstellung von Social Bots ist anspruchsvoll, es finden sich aber viele Ideen und Anleitungen im Internet. Social Bot-Technologien können auch gekauft oder gemietet werden. Betreiber von Social Bots sind Geheimdienste, die politisch in ihrem Sinne manipulieren wollen, Terrorgruppen, Wahlkämpfer, Unternehmen, die die Konkurrenz schädigen oder Börsenkurse beeinflussen wollen usw.

### **Social Bots einrichten**

Damit Social Bots ihre Aufgabenstellung gut erfüllen können, brauchen sie sehr viele simulierte Nutzer, die sich wie echte Nutzer verhalten. Dazu müssen die Social Bots als erstes Fake-Accounts/Fake-Profile in den verschiedenen sozialen Netzwerken erstellen. Meist werden Bilder schöner, junger Menschen verwendet, um die falschen Nutzer interessant wirken zu lassen. Dann werden, in Abhängigkeit davon, welche Art von Fake-News verbreitet werden soll, entsprechende Beiträge erstellt, um auch inhaltlich interessant für die Zielgruppe zu werden. Anschließend werden aktiv Verbindungsanfragen gestellt und Anfragen von anderen bestätigt. Alle Aktionen der Social Bots werden zufällig, aber zu typischen Tageszeiten menschlicher Interaktion umgesetzt, um das Erkennen zu erschweren. Dabei wird die Erfahrung berücksichtigt, dass, je homogener der Kreis der Nutzer ist, die eine Nachricht teilen, umso größer die Wahrscheinlichkeit ist, dass die Nachricht immer weiter geteilt wird und somit ein großes Publikum erreicht wird.

### **Social Bot – Nutzen**

Wenn ein Social Bot mit sehr vielen Fake-Accounts, mit sehr guter Vernetzung (Freunden oder Followern) und passenden Inhalten eingerichtet ist, können darüber gezielt Fake-News verteilt werden, um das gesetzte Ziel erfolgreich umzusetzen.

### **Bewertung von Social Bots**

Zwischen 9 und 15 % der Twitter-Konten sind nach Schätzungen von US-Forschern nicht menschlich, sondern botgesteuert [2]. Aber auch bei Facebook werden sehr viele Accounts von Social Bots betrieben. In der Summe gibt es bei Facebook 6 % Fake-Accounts. Aber nicht alle Fake-Accounts werden von Social Bots verwendet.

Das Beeinflussungspotenzial von Social Bots ist sehr groß. Insbesondere wenn bei Entscheidungen nur eine knappe Mehrheit erwartet wird, haben Social Bots einen besonderen Einfluss, wie zum Beispiel bei der BREXIT-Entscheidung oder dem US-Präsidentenwahlkampf.

Aber auch die Diskreditierung von Mitarbeitern oder der Unternehmensführung ist eine Möglichkeit, Konkurrenten zu schädigen und damit besser dazustehen oder Börsenwerte zu beeinflussen.

Die Vorteile von sozialen Netzwerken bezüglich der neuen Wege, Demokratie und Bürgerbeteiligungen zu gestalten, werden durch Fake-News beschädigt. Langfristig stellen Social Bots eine große Gefahr für das Vertrauen und das Überleben von sozialen Netzwerken dar.

**Tab. 16.1** Facebook-Empfehlungen mit dem Umgang von Fake-News**Lies Überschriften kritisch!**

→ Wenn Behauptungen **unglaublich klingen**, sind sie es vermutlich auch

**Sieh dir die URL genau an!**

→ Unechte oder nachahmende URL → Falschmeldung

**Überprüfe die Quelle!**

→ Für ihre Glaubwürdigkeit bekannt?

**Achte auf ungewöhnliche Formatierungen!**

→ Tippfehler, seltsame Layouts → Falschmeldung

**Sieh dir Fotos genau an!**

→ Manipulierte Bilder, Videos → Falschmeldung

**Überprüfe die Datumsangabe!**

→ Geänderte Datumsangabe, chronologisch unlogisch → Falschmeldung

**Überprüfe die Beweise!**

→ Mangelnde Beweise, Verweis auf ungenannte Experten → Falschmeldung

**Sieh dir andere Berichte an!**

→ Keine anderen Nachrichtenquellen mit derselben Meldung

→ Falschmeldung

**Ist die Meldung ein Scherz?**

→ Wenn Scherz (Humor, Satire, Parodie, ...) → *keine* Falschmeldung

**Einige Meldungen sind bewusst falsch**

→ Nur teilen, wenn glaubwürdig

**Wie können Fake-News erkannt werden?**

Die Problematik von Fake-News bei sozialen Netzwerken ist relativ neu, daher ist die Forschung in diesem Bereich noch sehr jung. Hier werden ein paar Ideen und Verfahren aufgezeigt, die ein Weg zur Lösung sind oder sein könnten.

**Der Nutzer findet selber heraus, ob es sich um Fake-News handelt**

In Tab. 16.1 sind die Empfehlungen dargestellt, die Facebook seinen Nutzern vorschlägt.

Die Empfehlungen sind sicherlich gut, werden aber in einer Welt, in der die Nutzer gelernt haben, Informationen schnell aufzunehmen, keinen großen Effekt verursachen und auf keinen Fall das Problem Fake-News lösen. Bei den klassischen Medien sind wir gewohnt, dass die Redakteure dies für uns tun.

**Automatische Erkennung**

Grundsätzlich könnten die beschriebenen Aspekte, die Facebook vorschlägt, auch durch passende Programme automatisch analysiert werden. Die Ergebnisse werden auf jeden Fall schneller, und es können sehr viele Nachrichten parallel überprüft werden.

**Erkennen von Fake-News mithilfe von KI-Algorithmen**

In den vergangenen Jahren sind insbesondere im Bereich der neuronalen Netze (deep neural networks – DNN) enorme Fortschritte erzielt worden, die prinzipiell in der Lage sind, eine solche Aufgabenstellung zu lösen. Ein neuronales Netz ist

ein komplexes mathematisches System, das Aufgaben erlernt, indem es gewaltige Datenmengen analysiert. In diesem Bereich werden die größten Erfolge in der Zukunft erwartet, siehe auch Kap. 15 „Künstliche Intelligenz und Cyber-Sicherheit“.

### **Journalisten werde mit der Prüfung beauftragt**

Wie beschrieben, ist das Redigieren eine Aufgabenstellung, die Journalisten lernen und für die klassischen Medien erfolgreich umsetzen. Das Problem dabei ist, dass eine sehr große Anzahl von Journalisten notwendig ist, um diese Aufgabenstellung zum Beispiel für Facebook erfüllen zu können. Wahrscheinlich müssten es mindestens 10.000 Journalisten sein.

### **Was ist zu tun, wenn ich weiß, dass es sich um eine Fake-News handelt?**

Wenn ein Betreiber eines sozialen Netzes weiß, dass eine Nachricht eine Fake-News ist, kann er diese mit einem Warnhinweis versehen oder er kann sie löschen.

### **Warnhinweis**

Da es immer eine Wahrscheinlichkeit gibt, dass eine erkannte Fake-News doch wahr ist, wäre die Kennzeichnung daher im Sinne der Meinungsfreiheit eine gute Kompromisslösung. Der große Nachteil ist, dass Nutzer, die aufgrund ihres Weltbildes oder Voreinstellung diese Falschinformation eher glauben, sich mit einer hoher Wahrscheinlichkeit nach einiger Zeit noch an die inhaltlichen Informationen erinnern werden, nicht aber an den Fake-News-Warnhinweis (Sleeper Effect).

### **Löschen von Fake-News**

Im von der Bundesregierung eingebrachten Netzwerkdurchsetzungsgesetz ist das zügige Löschen von Fake-News durch die Betreiber von sozialen Netzwerkwerken-Plattformen vorgesehen [3]. Eine der größten Nachteile dieser Methode ist, dass die Betreiber von sozialen Netzwerkwerken-Plattformen Inhalte vorsorglich löschen, wenn nur ein Verdacht besteht, es könne sich um strafrechtlich relevante Unwahrheiten handeln. Die Androhung von Strafzahlungen ist so hoch, dass dieses Verhalten sehr wahrscheinlich eintreten wird. Das bedeutet aber, dass viele Nachrichten gelöscht werden, die keine Fake-News sind. Das wiederum berührt das Recht auf Meinungsfreiheit.

### **Wann soll eine Nachricht überprüft werden?**

Hier wird diskutiert, wann der beste Zeitpunkt ist, eine Nachricht auf Fake-News zu überprüfen.

### **Immer dann, wenn ein Inhalt eingestellt wird**

Das ist sicherlich die beste Möglichkeit. Das Problem ist nur, dass bei Facebook am Tag 4 Mrd. Texte, 60 Mio. Bilder und sehr viel Videos überprüft werden müssen, bevor sie freigeschaltet werden können. Bei Twitter müssten am Tag 500 Mio. Tweets überprüft werden, bevor sie versendet werden können.

Wenn 10.000 Journalisten bei Facebook die 4 Mrd. Texte überprüfen müssten, bevor sie freigegeben würden, wären das 400.000 Texte am Tag pro Journalist. Oder wenn ein Journalist 20 Texte am Tag auf Echtheit überprüfen könnte, wären 200.000.000 Journalisten notwendig. Hier wird sehr schnell deutlich, dass diese Vorgehensweise nicht mit echten Personen umgesetzt werden kann.

Diese Aufgabe könnte nur mit einem sehr guten Algorithmus ausgeführt werden, und nur in schwierigen Fällen würde ein Journalist eingebunden.

### **Immer dann, wenn ein Nutzer eine Fake-News meldet**

Alle Nutzer, die sich nicht sicher sind, dass eine Nachricht echt ist, melden diese an eine Stelle, die dann die Entscheidung mit Algorithmen und/oder Journalisten trifft.

Das können wir heute schon bei den meisten sozialen Netzwerken tun. Leider ist die Anzahl der Meldungen sehr gering.

### **Zusammenfassung Fake-News**

Fake-News gibt es schon sehr lange. Die klassischen Medien haben Redaktionen, die für uns Konsumenten eine Prüfung auf Echtheit durchführen, die in der Regel ganz gut funktioniert.

Mit dem Erfolg der sozialen Netzwerke ist das Problem, dass es dort keine Redaktionen mehr gibt und der Nutzer gleichzeitig Anbieter und Konsumenten von Inhalten ist, eine neue problematische Erscheinung, die schnell und zufriedstellend gelöst werden muss.

Das Problem von Fake-News ist sehr groß geworden, Stimmungsbilder werden beeinflusst mit dem Effekt, dass Wahlen manipuliert, Aktienkurse beeinflusst werden usw.

Wenn das Problem nicht gelöst wird, werden die sozialen Netzwerke an Bedeutung verlieren und die Vorteile für eine moderne und globale Gesellschaft werden nicht mehr zur Verfügung stehen.

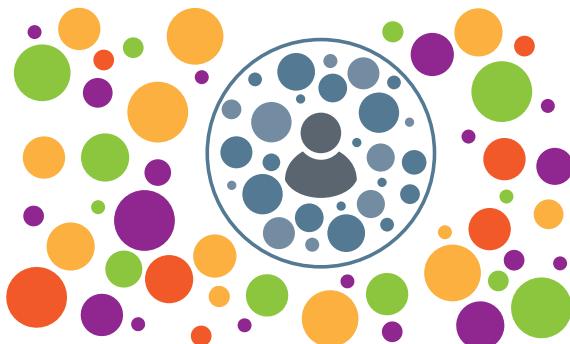
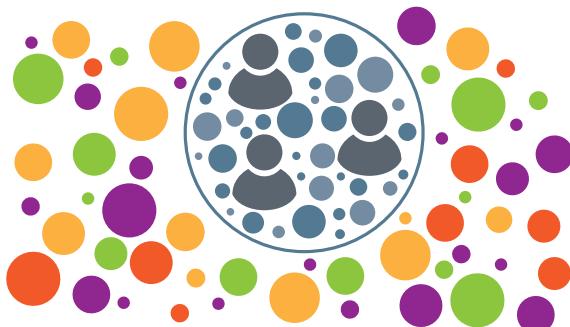
---

## **16.3 Filterblasen und Echokammern**

Soziale Netzwerke arbeiten auch mit Filterblasen und deren Eigenschaft, dass einem Nutzer tendenziell nur Nachrichten angezeigt werden, die mit seinen bisherigen Ansichten übereinstimmen. Diese Informationen werden zum Beispiel durch das Like- und Klick-Verhalten des Nutzers bestimmt, siehe Abb. 16.6.

Das Problem dabei ist, dass der Nutzer keine Nachrichten bekommt, die seinem Standpunkt widersprechen und damit eine objektive Selbstbestimmung nicht mehr möglich ist.

Eine Echokammer beschreibt darüber hinaus das Phänomen, dass viele Menschen in den sozialen Netzwerken dazu neigen, sich mit Gleichgesinnten zu umgeben und sich dabei gegenseitig in der eigenen Position verstärken. Echokammern sind Filterblasen, in denen mehrere Nutzer sind, siehe Abb. 16.7.

**Abb. 16.6** Filterblasen**Abb. 16.7** Echokammern

Auf diesem Wege erwächst der Eindruck, keine Minderheitsmeinung zu vertreten, sondern eine gesellschaftlich relevante Mehrheit zu sein. Soziale Netze wie etwa Facebook unterstützen und verstärken diesen Effekt dadurch, dass die Algorithmen dafür sorgen, dass überwiegend nur Inhalte angezeigt werden, die von Gleichgesinnten stammen oder von ihnen „gelikt“ wurden.

Filterblasen und Echokammern sorgen dafür, dass die Bürger keine Diversität mehr haben, was für eine aktive Demokratie schädlich ist.

---

#### 16.4 Psychometrie bei sozialen Netzwerken

Die Psychometrie ist das Gebiet der Psychologie, das sich allgemein mit Theorie und Methode des psychologischen Messens befasst.

Psychometrie kann genutzt werden, um Personen mit bestimmten Eigenschaften zu identifizieren.

Ein Beispiel einer solchen Messung ist eine Analyse auf Facebook, die von Cambridge Analytics durchgeführt worden ist.

### Generelle Idee dieser speziellen Analyse

**Input:** Was haben Nutzer gelikt, geteilt oder gepostet

**Output:** Geschlecht, Alter, Wohnort, Hautfarbe, sexuelle und politische Ausrichtung, ...

Mit der Analyse, was die Nutzer gelikt, geteilt oder gepostet haben, konnte Cambridge Analytics die folgenden Zusammenhänge herausbekommen.

Mit durchschnittlich 68 Facebook-Likes kann vorhergesagt werden,

- welche Hautfarbe der Nutzer hat (95-prozentige Treffsicherheit),
- welche sexuelle Ausrichtung er hat (88-prozentige Wahrscheinlichkeit),
- ob es sich um einen Demokraten oder Republikaner handelt (85 %).

Aber auch Intelligenz, Religionszugehörigkeit, Alkohol-, Zigaretten- und Drogenkonsum lassen sich berechnen.

Die Information, ob ein Nutzer Demokrat oder Republikaner ist, war bei der Verteilung von individuellen Fake-News während der US-Wahlen eine wichtige Information, um gezielt vorgehen zu können [4].

Den Nutzern von sozialen Netzwerken muss bewusst sein, dass die Informationen, die sie gelikt, geteilt oder gepostet haben, sehr viel über sie preisgeben. Diese persönlichen Informationen können sowohl positiv wie auch negativ für die einzelnen Nutzer, aber auch für die Gesellschaft verwendet werden.

---

## 16.5 Zusammenfassung

Social Web-Anwendungen bringen Gesellschaftsgruppen zusammen, schaffen Bürgerbeteiligungen und fördern auch Demokratie.

Auf der anderen Seite wird es immer wichtiger, dass Lösungen umgesetzt werden, die das Einstellen von rechtlich verbotenen Inhalten und mit Rechten behaftete Objekte verhindern, ohne zu zensieren.

Negative Aspekte wie Filterblasen und Echokammern müssen erkannt und deren Auswirkungen verhindert werden. Aber auch das Thema Psychometrie stellt Risiken für den einzelnen Nutzer und für die Gesellschaft dar.

Wichtig für die Cyber-Sicherheit wird sein, dass die negativen Potenziale von sozialen Netzwerken nicht das Risiko von IT-Schäden erhöht.

---

## 16.6 Übungsaufgaben

### Übungsaufgabe 1

Wer stellt überwiegend die Inhalte bei sozialen Netzwerken ein?

### Übungsaufgabe 2

Warum fallen Fake-News nicht unter die Meinungsfreiheit?

**Übungsaufgabe 3**

Mithilfe von welchen Informationen entscheiden soziale Netzwerke bei der Umsetzung von Filterblasen und Echokammern, welche Nachrichten einem Nutzer angezeigt werden?

**Übungsaufgabe 4**

Welche Informationen können mithilfe der Psychometrie gewonnen werden?

Ergebnisse siehe: <https://norbert-pohlmann.com/cyber-sicherheit/uebungen/>.

---

**Literatur**

1. Pohlmann N (2017) Fake-News in Sozialen Netzwerken – Das „Mitmach-Web“ hat seine Unschuld (endgültig) verloren. IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance 2017(5):52–57
2. [www.arxiv.org/pdf/1703.03107.pdf](http://www.arxiv.org/pdf/1703.03107.pdf)
3. [de.wikipedia.org/wiki/Netzwerkdurchsetzungsgesetz](http://de.wikipedia.org/wiki/Netzwerkdurchsetzungsgesetz)
4. [https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/](http://https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/)



# Wirtschaftlichkeit von Cyber-Sicherheitsmaßnahmen

17

Cyber-Sicherheitsmaßnahmen sind kein Selbstzweck. Mithilfe von Cyber-Sicherheitsmaßnahmen kann das Risiko bei der Nutzung von IT-Systemen erheblich reduziert und damit ein Schaden verhindert werden. In diesem Kapitel sollen die Kosten und der Nutzen der Cyber-Sicherheitsmaßnahmen diskutiert werden. Da eine Cyber-Sicherheitsmaßnahme eine Investition für eine erfolgreiche Zukunft darstellt, sollten die Kosten-Nutzen-Aspekte schon bei der Planung von Cyber-Sicherheitsmaßnahmen besonders berücksichtigt werden [1].

## 17.1 Einführung

Die Aufgabe von IT-Systemen ist es, die Geschäftsprozesse in Unternehmen zu optimieren und dadurch Kosten zu reduzieren oder den Umsatz zu steigern, um letztlich mehr Profit zur erzielen. Die IT und die IT-Dienstleistungen dienen dem Zweck der Bestandssicherung und Gewinnmaximierung.

Dies kann zum Beispiel dadurch erreicht werden, dass die Aufgaben vereinfacht oder beschleunigt werden, zum Beispiel durch die Nutzung der neuen Anwendungen wie sprachgesteuerte, intelligente persönliche Assistenten. Abläufe können mithilfe von IT-Systemen störungsfreier oder flexibler gestaltet werden. Die Digitalisierung stellt eine Vielzahl an innovativen Lösungen zur Verfügung.

Mitarbeiter können von Routineaufgaben entlastet und bei komplexen Aufgaben unterstützt werden.

Was für sämtliche Geschäftsbereiche eines Unternehmens gilt, gilt auch für den Einsatz von IT-Systemen: Sie müssen wirtschaftlich sein. Diese Wirtschaftlichkeit kann durch unterschiedliche Wirtschaftlichkeitsprinzipien erreicht werden:

Das **Minimierungsprinzip** hat den Schwerpunkt, bei einem gesetzten Ziel minimalen Aufwand zu betreiben. Wenn das Ziel ein bestimmter Gewinn ist, müssen bei gleichem Umsatz die Kosten gesenkt werden. Somit soll das Ziel Gewinn (Profit) durch den minimalen Mittelverbrauch (Kosten/Input) erreicht werden.

Das **Maximierungsprinzip** bedeutet, dass mit gegebenen Mitteln ein maximales Ziel erreicht werden soll. Der Gewinn ist dabei eine individuell wählbare Zielvorstellung und soll mit den gegebenen Mitteln maximiert werden. Die Mittel (Kosten/Input) sind also vorgegeben, der Umsatz (Output) ist jedoch ein Ziel, das bezüglich des Profits optimiert werden soll.

Das **generelle Extremumprinzip** ist so zu verstehen, dass Mitteleinsatz und Ergebnis so aufeinander abgestimmt sind, dass der durch sie definierte Prozess, gemessen an problemindividuellen Kriterien, optimal wird. Hierbei strebt keine Größe nach einem bestimmten Ergebnis oder Ziel, sondern Kosten und Umsatz stehen in einer variablen Wechselwirkung zueinander. Um den Prozess des Wirtschaftens zu optimieren, müssen Arbeitsschritte einer ständigen Qualitätskontrolle unterliegen.

Diese unterschiedlichen Wirtschaftlichkeitsprinzipien haben nichts mit Cyber-Sicherheit zu tun, sie stellen wirtschaftliche Ziele einer unternehmerischen Tätigkeit da. Dabei kann die Bewertung der Wirtschaftlichkeit nach den folgenden Aspekten durchgeführt werden:

#### **Nach Kostenaspekten:** Total Cost of Ownership

Total Cost of Ownership sind die Kosten für Anschaffung, Schulung, Installation, Betrieb, Wartung und Ersatz von IT-Systemen und Cyber-Sicherheitsmaßnahmen. Die Berechnung erfolgt durch die Kapitalwert-Methode, das heißt, was kostet ein Investment in der Summe aller Aspekte, die berücksichtigt werden müssen? Dieser Wert kann mit den Kosten verglichen werden, die zum Beispiel durch einen erfolgten oder geschätzten Schaden und dessen sofortige, mittelfristige und langfristige finanziellen Auswirkungen entstehen.

#### **Nach Nutzenaspekten:** ROI = Return on Investments

Hier wird der Nutzen den Kosten gegenübergestellt. Was nützt ein Investment bezüglich Kostenminimierung und/oder Umsatzsteigerung? Wann hat sich eine Investition amortisiert, das heißt, die Anschaffungskosten für eine Investition durch den mit der Investition erwirtschafteten Ertrag gedeckt? Je schneller eine Deckung erzielt wird, umso schneller kann ein Gewinn, zum Beispiel durch das Investment von Cyber-Sicherheitsmaßnahmen, generiert werden.

---

## **17.2 Cyber-Sicherheit**

Im Folgenden werden einige Begriffe definiert, die helfen, unterschiedliche Sichtweisen auf die Cyber-Sicherheit bezüglich der Wirtschaftlichkeit besser zu verstehen.

### **17.2.1 Schutzbedarf von IT-Systemen**

Der Schutzbedarf wird in IT-Werten bemessen. Die Höhe des IT-Wertes zeigt dessen Bedeutung für den Eigentümer und hilft, Cyber-Sicherheitsmaßnahmen

ökonomisch und zielgerichtet einzusetzen. Zu den IT-Werten gehören unter anderem die Daten (Entwicklungsdaten, Vertriebsdaten, Logistikdaten usw.), IT-Systeme (Hardware) und IT-Anwendungen (Software). Um den Schutzbedarf von IT-Werten einheitlich festzustellen, wird ein festgelegter Maßstab benötigt, der bezüglich der Cyber-Sicherheitsbedürfnisse, wie Vertraulichkeit, Authentifikation, Authentizität, Integrität, Verbindlichkeit und Verfügbarkeit, festlegt, wann der Schutzbedarf als „niedrig bis mittel“, „hoch“ oder „sehr hoch“ anzusehen ist. Wenn dann der Schutzbedarf der IT-Applikationen und Daten gemäß des Schutzbedarfsmaßstabes festgestellt ist, lässt sich der Schutzbedarf für die IT-Systeme einfach ableiten, siehe auch Abschn. 7.2 „Das richtige Firewall-Konzept für jeden Anwendungsfall“.

### 17.2.2 Wie sicher ist „sicher“?

Bei so vielen Risiken und Angriffspotenzialen in der IT-Welt stellt sich unweigerlich die Frage, wie wirksam Cyber-Sicherheitsmaßnahmen überhaupt sein können. Ein grundsätzlich wichtiges Kriterium für die Beurteilung von Cyber-Sicherheitsmaßnahmen ist die Frage danach, ob die Cyber-Sicherheitsmaßnahmen auch tatsächlich in der Lage sind, den realen Angriffen entgegenzuwirken. Dabei kann die Stärke der eingesetzten Cyber-Sicherheitsmaßnahmen unterschiedlich bewertet werden. Meist werden hier für die Bewertungen der Wirksamkeit „hoch“, „mittel“ und „niedrig“ verwendet. Wichtige Kriterien für die Bewertung der Stärke der Wirksamkeit sind dabei Fachkenntnisse, Ressourcen und Gelegenheit der potentiellen Angreifer. Unter Fachkenntnisse werden alle Kriterien zusammengefasst, die das Anwendungs-Know-how des Angreifers beschreiben. Handelt es sich um einen Laien, einen versierten Nutzer (eine kenntnisreiche Person) oder gar einen Experten? Ressourcen sind die für einen erfolgreichen Angriff erforderlichen Mittel. Dabei werden die Komponenten Zeit und Ausstattung unterschieden – die Zeit, die zur Durchführung des Angriffs benötigt wird und die erforderliche Ausstattung in Form von Hardware, Werkzeugen und Software. So entstehen Bewertungsbandbreiten von „Sonderausstattung – innerhalb von Monaten“ bis hin zu „Ohne Ausstattung – innerhalb von Minuten“. Das Bewertungskriterium „Gelegenheit“ beschreibt im Gegensatz zu den anderen Punkten die eher schwer kontrollierbaren Gegebenheiten wie Zufall, geheime Absprachen und Entdeckung. Darunter fällt die eher zufällige Zusammenarbeit mit einem Anwender genauso wie Absprachen mit dem eigentlich als vertrauenswürdig eingestuften Systemverwalter. Daraus ergeben sich Sicherheitsbewertungen, die der jeweiligen Situation entsprechend greifen können. So kann eine Cyber-Sicherheitsmaßnahme, die innerhalb von Minuten von einem Laien alleine überwunden werden kann, wohl nicht einmal mehr als „niedrig“ bezüglich der Wirksamkeit eingestuft werden. Jedoch könnte eine Cyber-Sicherheitsmaßnahme bezüglich der Wirksamkeit als „hoch“ eingestuft werden, die nur mittels Sonderausstattung und in monatelanger Expertenarbeit in die Knie gezwungen werden kann. Ein weiteres Kriterium zur Beurteilung einer Cyber-Sicherheitsmaßnahme ist die Korrektheit. Mit dem Faktor Korrektheit soll überprüft und beurteilt werden, ob die Cyber-Sicherheitsmaßnahmen korrekt

implementiert sind und wie groß das Vertrauen in die Implementierung der Lösungen ist. Grundsätzlich kann also gesagt werden, dass Cyber-Sicherheitsmaßnahmen nur als wirklich sicher eingestuft werden können, wenn Wirksamkeit, Stärke und Korrektheit zu gleichen Teilen in angemessener Qualität vorherrschen, siehe auch Abschn. 1.6 „Konzept der Wirksamkeit von Cyber-Sicherheitssystemen“.

### 17.2.3 Verwundbarkeit

Die Angriffspotenziale sind für alle Organisationen und Unternehmen gleich. Der Unterschied liegt in der Verwundbarkeit, wenn ein Schaden auftritt. Durch die oft geringen finanziellen Reserven und Möglichkeiten, Geld zu beschaffen, ist die Verwundbarkeit bei klein- und mittelständischen Unternehmen (KMUs) oft ungleich höher als bei sehr großen Unternehmen. Die größte Gefahr für den Mittelstand ist das fehlende Bewusstsein für die Notwendigkeit der Cyber-Sicherheit. Aber gerade die vielen geschäftsführenden Gesellschafter, deren Existenz unmittelbar mit dem Geschäftserfolg verknüpft ist, sollten hier wachsam sein.

## 17.3 Return on Security Investment RoSI – Nutzenaspekt

Im Folgenden soll eine „Return on Security Investment (RoSI)“ Berechnung dargestellt werden, mit der ein Nutzenaspekt von Cyber-Sicherheitsmaßnahmen aufgezeigt werden kann, siehe Abb. 17.1.

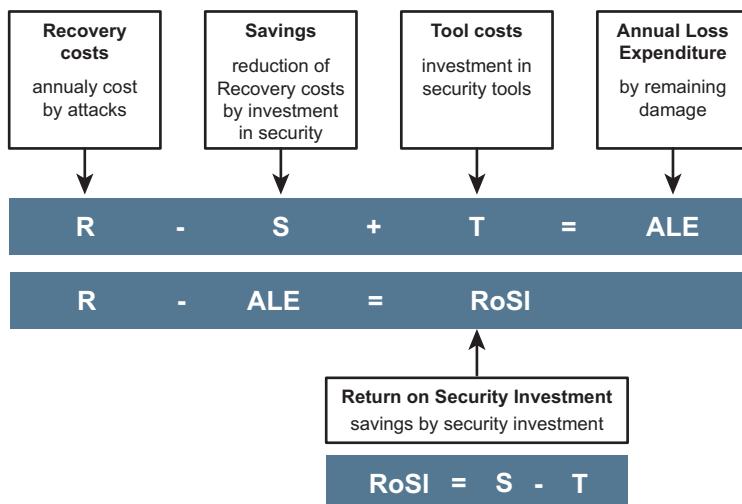


Abb. 17.1 Return on Security Investment

RoSI bedeutet, dass bei der Betrachtung aller Kosten (auch die, die durch Schäden eines Angriffes verursacht werden) aufgezeigt werden kann, ob und wann ein Investment in Cyber-Sicherheitsmaßnahmen zur einem Return on Investment führt oder nicht.

Beschreibung der Abkürzungen:

#### **Recovery Costs – R (Kosten der wahrscheinlichen Schäden)**

Diese Kosten beschreiben alle Aufwendungen, die notwendig sind, um nach einem aufgetretenen Schaden den ursprünglichen Zustand wiederherzustellen. Sie werden in die Gesamtkosten der geschäftlichen Tätigkeiten mit einbezogen. Die Recovery Costs hängen von dem tatsächlichen Eintritt von Schäden ab, müssen aber aus Erfahrungswerten für die Zukunft abgeschätzt werden.

Hinweis:

In den Recovery Costs können aber auch Aspekte wie die Erhöhung der Fremdkapitalkosten durch zum Beispiel Basel II mit einfließen. Falls keine geeigneten Cyber-Sicherheitsmaßnahmen eingeführt sind, müssen die Unternehmen für zum Beispiel Investitionskredite mehr Zinsen zahlen. Dieses Mehr an Zinsen ist ein Schaden, der auftritt, weil keine angemessene Cyber-Sicherheit im Unternehmen vorhanden ist. Durch geeignete Investitionen in Tools kann der Schaden verhindert werden. Ein weiterer Aspekt ist die Reduzierung des Prämienaufwands für die Cyber-Versicherung, falls Cyber-Sicherheitsmaßnahmen eingesetzt werden.

#### **Savings – S (Reduzierung der Kosten der wahrscheinlichen Schäden)**

Hierbei handelt es sich um die Kosten, die durch die Einführung von Cyber-Sicherheitsmechanismen (Tools) gespart werden, weil sie mit einer sehr hohen Wahrscheinlichkeit einen Angriff erfolgreich verhindern. Auch diese Kosten müssen abgeschätzt werden.

#### **Tool Costs – T (Kosten für Cyber-Sicherheitsmaßnahmen)**

Dies sind die vollständigen Kosten (Total Cost of Ownership – TCO) für die Cyber-Sicherheitsmaßnahmen, die potenzielle Angriffe mit einer hohen Wahrscheinlichkeit verhindern sollen.

#### **Annual Loss Expenditure – ALE (verbleibende Kosten)**

Das sind die verbleibenden Kosten (Schaden) nach einem Investment in Cyber-Sicherheitsmaßnahmen.

#### **Return on Security Investment – RoSI (gesparte Kosten, erzielter Profit)**

Einsparungen der Recovery Cost (Schäden), die durch das Investment in Cyber-Sicherheitsmaßnahmen erzielt wurden.

Hinweis:

Solange T (Tools), die TCO der Cyber-Sicherheitsmaßnahmen, kleiner sind als S (Savings), die Reduzierung der Kosten, ist RoSI positiv.

$$\text{Formel: } \mathbf{R - (R - S + T)} = \mathbf{RoSI = S - T}$$

## 17.4 Beispielberechnung RoSI: Notebookverluste

In diesem Beispiel soll anhand der Verluste von Notebooks und die Investition in eine passende Cyber-Sicherheitsmaßnahme, die die Daten auf den Notebooks schützt, exemplarisch eine Berechnung des Return on Security Investment (RoSI) durchgeführt werden.

Als erstes wird diskutiert, wie wahrscheinlich der Verlust oder der Diebstahl eines Notebooks ist, und welcher Schaden dabei auftreten kann.

### Wie hoch ist die Wahrscheinlichkeit des Verlustes eines Notebooks?

Jeder, der die Verantwortung für Notebooks im Unternehmen hat, weiß wie viele Notebooks jährlich aus nachvollziehbaren und nicht nachvollziehbaren Gründen verschwinden. Dennoch ist die offene Kommunikation darüber in den Unternehmen unüblich. Die meisten bekommen ein neues Notebook ohne lange Analysen darüber durchzuführen, warum und wie das alte Notebook abhandengekommen ist. Da die meisten sowieso alle zwei bis drei Jahre ein neues Notebook bekommen, geht die Verlustrate gerade in großen Unternehmen und Organisationen oft in der Masse der neuen Notebooks unter.

Wenn aber die unterschiedlichen vorliegenden Studien über verlorene oder gestohlene Notebooks analysiert werden, so zeigt sich, dass im Schnitt **6 % der Notebooks** jährlich gestohlen werden oder verlorengehen (Eintrittswahrscheinlichkeit).

### Wie hoch ist der Schaden, wenn die Daten, die auf einem Notebook gespeichert sind, von Dritten missbräuchlich verwendet werden?

Auch den Schaden, der auftritt, wenn ein Notebook zum Beispiel durch die Konkurrenz gestohlen wird, kann der Nutzer des Notebooks am besten bemessen. Die Schwierigkeit, die hier auftritt, ist, dass der Schaden oft nicht genau analysiert werden kann, sondern durch Reduktion des Umsatzes und des Gewinns nur schwer zu beziffern ist. Wenn betrachtet wird, dass die meisten Notebooks eines Unternehmens von der Unternehmensleitung, den Vertriebsleuten und den wichtigsten Entwicklern verwendet werden, diese mit ihrem Notebook auf Reisen gehen oder von zu Hause aus arbeiten, wo die Eintrittswahrscheinlichkeit höher ist und hier oft alle wichtigen Unternehmensinformationen wie zum Beispiel Preis-kalkulationen, Entwicklungsdaten, Finanzanalysen, Lieferanten Einkaufspreise, Kundendaten, usw. gespeichert sind, fällt es nicht schwer zu erkennen, dass der mögliche Schaden sehr groß sein kann.

Wenn die unterschiedlichen Studien (Computer Security Institut – Crime&Security Survey, Security Issues and Trends, ...) über die Schäden von verlorenen Notebooks analysiert werden, kommt als Ergebnis raus, dass im Schnitt der **Schaden pro gestohlenem Notebook über EUR 10.000 liegt**. Dies ist nur der Schaden, der durch missbräuchliche Verwendung der Daten entsteht, der Verlust der Hardware, Software und Wiederherstellung eines Ersatzgerätes muss noch zusätzlich betrachtet werden (EUR 2000 bis 3000).

### Cyber-Sicherheitsmaßnahme zum Schutz der Informationen, die auf einem Notebook gespeichert sind

Um die Kosten abzuschätzen, die notwendig sind, um ein Notebook angemessen zu schützen, wird angenommen, dass ein Festplattenverschlüsselungsprodukt verwendet wird. Das Festplattenverschlüsselungsprodukt arbeitet mit einer Boot-Authentifikation, das heißt, der Nutzer muss sich beim Hochfahren des Notebooks erst über die Eingabe eines Passwortes authentisieren. Alle Daten auf dem Notebook sind auf der Festplatte nur in verschlüsselter Form vorhanden. Nachdem sich der Nutzer authentisiert hat, werden durch diese Cyber-Sicherheitsmaßnahme die Daten, die verwendet werden, jeweils für die Verarbeitung entschlüsselt und in verschlüsselter Form wieder auf der Festplatte gespeichert. Wenn ein Dieb dieses Notebook stiehlt, kann er zum Beispiel durch den Ausbau der Festplatte an die Daten gelangen. Da diese aber verschlüsselt sind, kann der Dieb sie nicht für sich verwenden, und daher mit den Informationen auf dem Notebook keinen Schaden für den Besitzer, das Unternehmen, anrichten.

Der Schaden für den Nutzer, für das Unternehmen, bleibt bei dem Verlust des Notebooks einschließlich der installierten Software (2000 bis 3000 EUR) und der Wiederbeschaffung und Fertigstellung eines neuen Notebooks begrenzt.

Die Anschaffung einer solchen Cyber-Sicherheitsmaßnahme kostet ca. 110 EUR, das heißt, im Schnitt ca. 4 % des Anschaffungspreises eines Notebooks.

### Berechnung der Return on Security Investment (RoSI)

Als Beispiel wird ein Unternehmen angenommen, bei dem 500 Mitarbeiter ein Notebook besitzen, auf dem sich für die Arbeit schützenswerte, wertvolle Daten befinden.

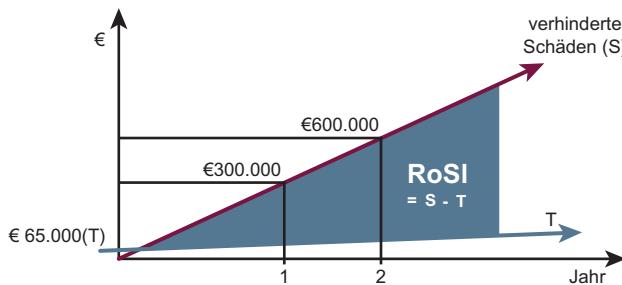
Annahmen:

- Schaden durch den Verlust der gespeicherten Daten pro gestohlenem Notebook = EUR 10.000
- Die Anzahl der Notebooks, die jedes Jahr gestohlen werden, wird mit 6 % = 30 Notebooks angenommen (Eintrittswahrscheinlichkeit). Tool Costs – T (Kosten für das Festplattenverschlüsselungsprodukt).
- Einmalige Lizenzkosten:  $500 * \text{EUR } 110 = \text{EUR } 55.000$
- Für die weiteren Kosten von Installation, Rollout und Verwaltung wird im ersten Jahr EUR 10.000 und in den folgenden Jahren EUR 5000 angenommen. Savings – S (vermiedener Schaden).
- $30 \text{ Notebooks} * \text{EUR } 10.000 = \text{EUR } 300.000$
- Hier wird nur der Schaden durch die missbräuchliche Verwendung der gespeicherten Daten betrachtet.

In Tab. 17.1 sind die Kosten für die Cyber-Sicherheitsmaßnahmen und der potenzielle Verlust auf vier Jahre eingetragen.

**Tab. 17.1** Return on Security Investment RoSI – Berechnung: 1. Beispiel

Calculation					In total
Time span	1st year	2nd year	3rd year	4th year	4 years
Initial costs	EUR 55.000	–	–	–	EUR 55.000
Implementation/ Rollout, Admin	EUR 10.000	EUR 5000	EUR 5000	EUR 5000	EUR 25.000
Reduced costs??	–	–	–	–	–
Value of no losses from sec breaches	EUR 300.000	EUR 300.000	EUR 300.000	EUR 300.000	EUR 1.200.000
ROI 1st year	EUR 235.000				
ROI 2nd year		EUR 530.000			
ROI 3rd year			EUR 825.000		
ROI 4th year				EUR 1.120.000	EUR 1.120.000

**Abb. 17.2** Return on Security Investment

Hier zeigt sich, dass schon im ersten Jahr ein ROI von EUR 235.000 erzielt werden kann. Nach vier Jahren liegt der ROI bei EUR 1.120.000.

Abb. 17.2 zeigt deutlich, dass das Investment  $T$  in Festplattenverschlüsselung kleiner ist als der verhinderte Schaden  $S$ , der durch die missbräuchliche Verwendung der gespeicherten Daten auftreten würde.

### Beispiel mit anderen Annahmen

In diesem Beispiel werden die Annahmen für den Schaden und die Eintrittswahrscheinlichkeit anders angenommen, siehe Tab. 17.2.

Annahmen:

- Schaden durch den Verlust der gespeicherten Daten pro gestohlenem Notebook = EUR 5000

**Tab. 17.2** Return on Security Investment RoSI – Berechnung: 2. Beispiel

Calculation					In total
Time span	1st year	2nd year	3rd year	4th year	4 years
Initial costs	EUR 55.000	–	–	–	EUR 55.000
Implementation/Rollout, Admin	EUR 10.000	EUR 5000	EUR 5000	EUR 5000	EUR 25.000
Reduced costs??	–	–	–	–	–
Value of no losses from sec breaches	EUR 75.000	EUR 75.000	EUR 75.000	EUR 75.000	EUR 300.000
ROI 1st year	EUR 10.000				
ROI 2nd year		EUR 80.000			
ROI 3rd year			EUR 150.000		
ROI 4th year				EUR 220.000	EUR 220.000

- Die Anzahl der Notebooks, die jedes Jahr gestohlen werden, wird mit  $3\% = 15$  Notebooks angenommen (Eintrittswahrscheinlichkeit) Tool Costs – T (Kosten für das Festplattenverschlüsselungsprodukt).
- Einmalige Lizenzkosten:  $500 * \text{EUR } 110 = \text{EUR } 55.000$
- Für die weiteren Kosten von Installation, Rollout und Verwaltung wird im ersten Jahr EUR 10.000 und in den folgenden Jahren EUR 5000 angenommen. Savings – S (vermiedener Schaden).
- $15 \text{ Notebooks} * \text{EUR } 5000 = \text{EUR } 75.000$

Auch bei diesem Beispiel kann aufgezeigt werden, dass schon im ersten Jahr ein ROI von EUR 10.000 erzielt werden kann. Nach vier Jahren liegt der ROI bei EUR 220.000.

Weitere Beispiele, bei denen eine RoSI-Berechnung in der Regel einfach durchgeführt werden kann, sind:

#### *Anti-Malware-Lösungen:*

Hier haben die meisten Unternehmen in den vergangenen Jahren selber Zahlen über die Kosten, die durch Schäden bei Malware aufgetreten sind, zur Verfügung.

#### *ID-Management, SingleSignOn (SSO) oder Authentifikation mit biometrischen Verfahren:*

Hier kann der Einspareffekt durch Helpdesk-Kosten sehr gut nachgewiesen werden (100 bis 200 EUR/Jahr pro Nutzer).

#### **Herausforderungen bei der RoSI-Berechnung**

Die RoSi-Berechnung kann, anders als im Notebook-Beispiel, ein sehr komplexer Prozess sein. Die Komplexität bei vielen Berechnungen kommt durch die Abschätzung des direkten und indirekten Schadens eines möglichen erfolgreichen

Angriffes und die Beurteilung der Reduzierung des Schadens durch eine spezielle Cyber-Sicherheitsmaßnahme, die dagegen wirkt, zustande. Weitere, schwer kalkulierbare Aspekte sind zum einen die Beurteilung des direkten Zusammenhangs zwischen einem konkreten Angriff und einem speziellen Schaden und zum anderen die Abschätzung zwischen einem Angriff und der unmittelbaren Wirkung einer Cyber-Sicherheitsmaßnahme. Hier müssen in der Praxis die Kosten für die Cyber-Sicherheitmaßnahmen oft auf verschiedene Schadensfälle, die möglicherweise durch unterschiedliche Angriffe verursacht wurden, anteilig berechnet werden.

---

## 17.5 Zusammenfassung

Die Wirtschaftlichkeit von Cyber-Sicherheitsmaßnahmen ist ein zunehmend wichtiger und sehr komplexer Punkt, mit dem sich die Verantwortlichen in Unternehmen, Behörden, aber auch die Regierungen, in einer gesellschaftlichen Verantwortung auseinandersetzen müssen.

Dennoch gibt es Cyber-Sicherheitsmaßnahmen, die rein wirtschaftlich betrachtet nicht sinnvoll sind und dennoch durchgeführt werden, wie zum Beispiel als gesetzliche Notwendigkeit, wenn es um die Sicherheit von Menschen geht, Militär, Angst oder übertriebenes Sicherheitsgefühl.

Wenn die Schäden nicht nur zu qualifizieren, sondern auch zu quantifizieren sind, dann kann, wie aufgezeigt wurde, ein Return of Security Investment (RoSI) berechnet und oft auch in der Praxis erzielt werden. Der Einsatz von Cyber-Sicherheitsmaßnahmen kann also weit mehr von Nutzen sein und sollte nicht nur als kostspieliger Nebeneffekt betrachtet werden oder aus Angst vor Haftung oder zur Einhaltung von Gesetzen in Betracht gezogen werden.

Um diesen Aspekt erfüllen zu können, müssen die Angriffe und die resultierenden Schäden so gut wie möglich dokumentiert werden, damit die tatsächlichen Kosten der Schäden benannt werden können. Dazu werden geeignete Hilfsmittel notwendig, die die Kosten von erfolgreichen Angriffen festhalten.

---

## 17.6 Übungsaufgaben

### Übungsaufgabe 1 (Wirtschaftlichkeitsprinzipien)

Sie sollen einen Profit von 1 Mio. EUR bei einem Umsatz von 12 Mio. EUR erzielen. Mit welchen Wirtschaftlichkeitsprinzipien kann dieses Ziel erreicht werden?

### Übungsaufgabe 2 (ROSI)

Berechnen Sie nach RoSI den ROI nach zwei Jahren. Sie sollten dabei die folgenden Annahmen treffen:

- Das Unternehmen hat 300 Notebooks.
- Schaden durch den Verlust der gespeicherten Daten pro gestohlenem Notebook = EUR 6000
- Die Anzahl der Notebooks, die jedes Jahr gestohlen werden, wird mit 2 % angenommen.
- Einmalige Lizenzkosten: EUR 110
- Für die weiteren Kosten von Installation, Rollout und Verwaltung wird im ersten Jahr EUR 6000 und in den folgenden Jahren EUR 3000 angenommen.

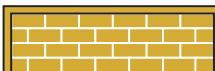
Ergebnisse siehe: <https://norbert-pohlmann.com/cyber-sicherheit/uebungen/>.

---

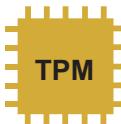
## Literatur

1. Pohlmann N (2006) Wie wirtschaftlich sind IT-Sicherheitsmaßnahmen? In Mörike M, Teufel S (Hrsg) Kosten & Nutzen von IT-Sicherheit. HMD – Prax Wirtschaftsinf 43(248):26–34

# Anhang

	Symbol für die Cyber-Sicherheitsmechanismen: Verschlüsselung, Entschlüsselung, Public-Key-Verfahren, Signatur, ...
	
	Symbol für die Cyber-Sicherheitsmechanismen: IPSec-Gateway, TLS/SSL, Anti-DDoS, Löschschaltung, Zähler, Zufallszahlengenerator, ...
	Symbol für den Cyber-Sicherheitsmechanismus: Firewall-Systeme
	Symbol für den Cyber-Sicherheitsmechanismus: One-Way-Hashfunktion
	Symbol für eine Modulo-2-Operation: XOR-Verknüpfung
	Symbol für allgemeine Funktionen: PC, Server, ...

	<p>Symbol für einen Input/Output/Wert (<b>Bits und Bytes</b>): Klartext, Schlüsseltext, Hashwert, ...</p> <p>Attribute für Bits und Bytes</p>
	 <p>Symbol für einen Hashwert: Output einer One-Way-Hashfunktion</p>
	 <p>Symbol für ein elektronisches Zertifikat: Ergebnis einer Signaturfunktion über den Inhalt eines Zertifikats</p>
	 <p>Symbol für eine digitale Signatur: Ergebnis einer Signaturfunktion</p>
	<p>Symbol für einen geheimen Schlüssel: Asymmetrische Verfahren</p>
	<p>Symbol für einen geheimen Schlüssel: Symmetrische Verfahren</p>
	<p>Symbol für einen öffentlichen Schlüssel: Asymmetrische Verfahren</p>
	<p>Symbol für einen allgemeinen Schlüssel</p>
	<p>Symbol für geschützte Informationen: Verschlüsselte Informationen</p>
	<p>Symbol für offene Informationen: Klartext-Informationen</p>
	<p>Symbol für Werte: Bit und Bytes (Entwicklungsdaten, Kundendaten, ...) Verfügbarkeit eines IT-Systems oder IT-Dienstes</p>
	<p>Symbol und Farbe für einen Angreifer</p>

	Symbol für einen normalen Nutzer
	Symbol für ein Hardware-Sicherheitsmodul: Smartcard, USB-Stick mit Hardware-Sicherheitsmodul, ...
	Symbol für Verkettung: Konkatenation
	Symbol für ein Trusted Platform Module (TPM)
	Symbol für einen Router
	Symbol für einen WLAN-Router
	Symbol für ein zu schützendes Netz: Internes Unternehmensnetz, ...
	Symbol für ein unsicheres Netz: Internet, ...
	Symbol für einen Sensor: NetFlow-Sensor, Netzwerk-Sensor, SNMP-Sensor, ...
	Symbol für eine Blockchain-Node

	Symbol für eine Blockchain-Wallet
	Symbol für ein Smartphone
	Symbol für ein Tablet
	Symbol für ein Notebook
	Symbol für einen PC/Server
	Symbol für einen Drucker
	Symbol für eine erfolgreiche Abwehr eines Angriffes: Die Wirkung eines Cyber-Sicherheitsmechanismus ist ausreichend
	Symbol für einen erfolgreichen Angriff: Die Wirkung eines Cyber-Sicherheitsmechanismus ist unzureichend
	Symbol für einen indirekten Angriff: Die Wirkung eines Cyber-Sicherheitsmechanismus ist zwar ausreichend, kann aber umgangen werden

---

# Stichwortverzeichnis

## A

Access Requestor, 273  
Advanced Encryption Standard, 62  
Advanced Evasion Techniques, 302  
Advanced Persistent Threat (APT), 5, 287  
Adware, 286  
Alert Protokoll, 413  
Amplification-Angriff, 442  
Analysekonzept, 292, 311  
Angreifer, 30  
Angriff, 281  
    1:1-Angriff, 286  
    1:N-Angriff, 284  
    aktiver, 327  
    Entgegenwirken, 28  
    Erkennen, 29  
    indirekter, 23  
    M:N-Angriff, 283  
    passiver, 326  
    Vermeiden, 26  
Angriffspotenziale, 281  
Annual Loss Expenditure, 577  
Anti-Replay Service, 378  
Anwendungsebene, 335  
Application  
    Data Protokoll, 412  
    Gateway, 349  
Attestation, 259  
    Identity Key, 253  
Attribute-Based Access Control, 229  
Authenticated Boot, 256  
Authentication Header, 375  
Authentifikation, 152  
Authentifizierung  
    adaptive, 189  
    Sichtweise IT-System, 153  
Authentifizierungsverfahren, 166  
    Klassen, 227  
Authentisierung, Sichtweise Nutzer, 153

Autorisierung, 153  
Management, 227

## B

Basic Quick Mode, 391  
Bedrohung, asymmetrische, 289  
Berechtigungsarchitektur, 490  
Betriebssystem, Kernelarchitekturen, 247  
Beweissicherung, 294  
Binding, 257  
Binding Key, 254  
Biometrie, 181  
Bitcoin, 502  
    Transaktion, 474  
Blockchain  
    Adresse, 480  
    as a Service, 507  
    Sicherheit der Anwendung, 512  
    Sicherheit der Infrastruktur, 508  
    Technologie, 467  
    Grundlagen, 470  
Blockverschlüsselung, 68  
Bridge CA, 133  
Brute-Force-Angriff, 49, 170

## C

CBC-Mode, 69  
Certificate Revocation List, 125  
Certification Authority, 124  
CFB-Mode, 70  
Chain of Trust for Measurement, 250  
Challenge-Response-Verfahren, 179  
ChangeCipherSpec, 413  
Chipkarte, intelligente, 102  
Chosen-ciphertext attack, 48  
Chosen-plaintext attack, 48  
Ciphertext-only attack, 48

- Click Fraud, 283  
 Cluster-Verfahren, hierarchisches, 535  
 Common Point of Trust, 357  
 Content-Delivery-Network (CDN), 447  
 Convolutional Neural Nets (CNN), 541  
 Core Root of Trust for Measurement, 250  
 Cross-Zertifizierung  
     1:n, 133  
     n:n, 133  
 CTR-Mode, 72  
 Cyber Security s. Cyber-Sicherheit  
 Cyber-Sicherheit, 2  
     Frühwarn- und Lagebildsystem, 281  
     proaktives System, 242  
     Probleme, 14  
     reaktives System, 242  
     Strategie, 26  
 Cyber-Sicherheitslage, 281  
 Cyberwar, 17
- D**
- Data Encryption Standard, 61  
 Data Science, 522  
 Dateiverschlüsselung, manuelle, 463  
 Daten, persönliche, 15  
 DDoS-Angriff, 439  
     Methode, 441  
 Decentralized Identifier, 480  
 Deep Learning, 523, 541  
 De-Mail, 462  
 Diffie-Hellman-Verfahren, 82  
 Directory Service, 125  
 Distinguishing Identifier, 152  
 Distributed Denial of Service, 283, 439  
 Distributed-Reflected-Denial-of-Service  
     (DDoS), 442  
 Dokument  
     Signatur, 139  
     Verschlüsselung, 141  
 Domain Validated (DV)-Zertifikat, 424  
 Domänen-Zertifikat, 424  
 Double-Spending-Attacke, 486
- E**
- ECB-Mode, 68  
 Echokammer, 569  
 eIDAS, 134  
 eid-Verfahren, 159  
 Einmal-Passwort, 178  
 Einmal-Schlüssel-Verfahren, 60  
 Einschreiben, elektronisches, 137  
 Einwegfunktion, 78
- F**
- Facebook Connect, 205  
 Fake News, 13, 564  
 Falschakzeptanzrate, 183  
 Falschrückweisungsrate, 184  
 False Acceptance Rate, 183  
 False Rejection Rate, 184  
 Fast Identity Online Alliance (FIDO), 197  
 Fernidentifizierung, 155  
 Fernsignatur, elektronische, 136  
 Filterblase, 569  
 Firewall  
     Element, 340  
     Konzept, 355  
     Modell, 333  
     System, 325  
 Föderation, 232  
 Frühwarnsystem, 289  
 Frühwarn- und Lagebildsystem, 281  
 Full Node, 479
- G**
- Gateway E-Mail-Sicherheitslösung, 460  
 GCM-Mode, 73  
 Gefahren, 231  
     des Internets, 10  
     durch Nutzung mobiler Geräte, 7  
     Online-Banking, 546  
 Gegenüberstellung PKI und Blockchain, 515

- H**
- Handshake Protokoll, 414
  - Hard Fork, 495
  - Hardware-Sicherheitsmodule (HSM), 101
  - HashPrev, 472
  - High-Level Security
    - Firewall-System, 355
    - Module (HLSM), 106
  - Honeypot, 306
- I**
- Identifikation, 151
  - Identität
    - abgeleitete, 165
    - digitale, 214
  - Identity Provider, 201
  - Information, sicherheitsrelevante, 101
  - Integrity Measurement
    - Collector, 273
    - Verifier, 274
  - Internet
    - der Werte, 469
    - Sicherheit, 4
  - Internet-Key-Exchange-Protokoll (IKE), 384
    - Aggressive Mode, 390
    - Main Mode, 386
  - IPSec
    - Client, 382
    - Gateway, 381
    - Security-Assoziation, 391
    - Verschlüsselung, 373
  - ISAKMP Security Association, 386
  - IT-Sicherheit, 2, 103, 104, 110, 313
- K**
- Kernel, monolithischer, 248
  - Kernelarchitekturen von Betriebssystemen, 247
  - Keyed-Hashing for Message Authentication (HMAC), 89
  - Keylogger, 6, 176, 286
  - Key Management, 66
  - Key-Recovery, 130
  - Klassen von Authentifizierungsverfahren, 227
  - k-Means-Algorithmus, 533
  - k-Nearest-Neighbor-Algorithmus, 530
  - Know-plaintext attack, 48
  - Kollisionsresistenz, 88
  - Kommunikationslagebild, 315
  - Kommunikationsmodell, 333
  - Komplexitätsklasse, 51
- L**
- Konsensfindungsverfahren, 482
  - Konzepte
    - der PKI- und Blockchain-Technologie, 514
    - der risikobasierten und adaptiven Authentifizierung, 189
    - der Wirksamkeit von Cyber-Sicherheitssystemen, 22
  - Kryptoanalyse, 47
  - Kryptografie, 43, 47
    - Grundlagen, 43
  - Kryptologie, 47
  - Kryptosystem, 47
  - Kryptowährung, 502
  - Künstliche Intelligenz (KI), 522
    - Manipulationen, 545
    - schwache, 522
    - starke, 522
    - und Cyber-Sicherheit, 542
  - Künstliche Neuronale Netze (KNN), 536
  - Kurve, elliptische, 83
- M**
- Lawineneffekt, 65
  - Lernen
    - maschinelles, 522
    - Prinzip, 525
    - überwachtes, 526
    - unüberwachtes, 533
  - Lite Node, 480
  - Logdaten, 308
  - Longest Chain Rule, 486
  - Long Short-Term Memory Networks (LSTM), 541
- N**
- Machine Learning (ML) s. Lernen, maschinelles
  - Malware, 4, 286
  - Manual Keying, 384
  - Match-on-Card-Verfahren, 103
  - Maximierungsprinzip, 574
  - Meinungsroboter, 565
  - Merkle Hash, 473
  - Merkmale, biometrische, 182
  - Message Authentication Code, 88
  - Messung
    - aktive, 296
    - passive, 296
  - Migratable Key, 252
  - Mikrokernel, 248
  - Minimierungsprinzip, 573

- 
- Mitmach-Web (Problem), 563  
 Modes of Operation, 68  
 Multifaktor-Authentifizierung (MFA), 188
- N**  
 NetFlow, 297  
 Network Access Authority, 275  
 Netzwerk, soziales, 562  
 Netzwerkschicht, 334  
 Netzwerk-Sensor, 299  
 Netzzugangsschicht, 334  
 Neuron, künstliches, 537  
 Next-Generation-Firewall, 353  
 Non-Migratable Key, 252  
 No Security by Obscurity, 46  
 Nutzung von Hintertüren, 302
- O**  
 OAuth 2.0, 204  
 OFB-Mode, 71  
 One-Time-Pad, 59  
 One-Time Password (OTP), 178  
 One-way-Hashfunktionen, 86  
 One-way trap door functions, 79  
 OpenID, 201  
     Connect, 208  
 Organization Validated (OV)-Zertifikat, 425
- P**  
 Packet Filter, 345  
     zustandsorientierter, 347  
 Paradigmenwechsel, 18  
 Pareto-Prinzip, 33  
 Passwort  
     Hash-Verfahren, 173  
     Recovery, 178  
     Regel, 171  
     Verfahren, 167  
 Pepper, 175  
 Perfect Forward Secrecy, 392, 394  
 Personalausweis, elektronischer (ePA), 159  
 Personal Security Environment, 125  
 PGP, 456  
     Vertrauensmodell, 457  
 Phishing  
     Angriff, 176  
     E-Mail, 454  
 Ping Scan, 284  
 PKI-enabled Application (PKA), 126  
 Platform Configuration Register, 104, 257
- Plattform-Zertifikat, 252  
 Policy Decision Point, 274  
 Policy Enforcement Point, 275  
 Port Scan, 284  
 PostIdent-Verfahren, 161  
 Post-Quanten-Kryptografie, 85  
 Pre-Shared Seced, 384  
 Prinzip des Maschinellen Lernens, 525  
 Private  
     permissioned, 491  
     permissionless, 491  
 Privatsphäre, 14  
 Produktverschlüsselung, 61  
 Proof-of-Stake, 488  
 Proof-of-Work, 484  
 Psychometrie, 570  
 Public  
     Key-Infrastrukturen (PKI), 122  
     permissioned, 491  
     permissionless, 491
- Q**  
 Quantencomputer, 84
- R**  
 Rainbow-Table, 174  
 Ransom-Ware, 286  
 Record Layer-Protokoll, 410  
 Recovery Costs, 577  
 Registration Authority, 123  
 Return  
     on Investments (ROI), 574  
     on Security Investment (RoSI), 576  
 Rijndael-Algorithmus, 62  
 Role-Based Access Control, 228  
 Root CA, 132  
 Root-Zertifikat, 425  
 RSA-Verfahren, 79  
 RSCoin, 503
- S**  
 S/MIME, 456  
     Vertrauensmodell, 458  
 Salt, 174  
 Savings, 577  
 Schlüsselverteilung, 67  
 Schlüsselwechsel, 67  
 Schutzbedarf, 574  
 Schwachstellen in der Software, 3  
 Sealing, 257

- Secure Socket Layer (SSL), 407  
Security  
    Association, 379  
        Database (SAD), 385  
        Policy Database, 385  
    Self-Sovereign Identity, 164  
    Sensor, 291  
        Grundprinzip, 294  
    Service Node, 480  
    SHA-3, 88  
    Shared Secret, 82  
    Short-Cut-Methode, 49  
    Sicherheit  
        absolute, 50  
        der Blockchain-Anwendung, 512  
        der Blockchain-Infrastruktur, 508  
        praktische, 50  
    Sicherheitsanker, 249  
    Sicherheitsplattform, 260  
    Signatur  
        digitale, 115  
        eines Dokuments, 139  
    Signing Key, 254  
    Single Sign-On, 228  
    Smartcard, 102  
    Smart Contracts, 501  
    SNMP-Sensor, 303  
    Social Bots, 565  
    Social Engineering, 177, 287  
    Social-Ident-Verfahren, 164  
    Soft Fork, 492  
    Spam, 454  
        Spam-E-Mail, 283  
    Spear-Phishing, 177  
    Speicherung, sichere, 67  
    Stateful Inspection-Firewall, 348  
    Steganografie, 47, 76  
    Storage Key, 253  
    Storage Root Key, 253  
    Stuxnet, 17  
    Substitution  
        homofone, 55  
        monoalphabetische, 54  
        polyalphabetische, 57  
    Suche, vollständige, 49  
    Support-Vector-Machine, 526
- TLS/SSL  
    Schicht, 409  
    Zertifikat, 424  
Tool Costs, 577  
Total Cost of Ownership, 574  
Transport Layer Security (TLS), 407  
Transportmodus, 380  
Transportschicht, 334  
Transportverschlüsselung, 407  
Transpositionsverfahren, 58  
Trial-and-Error-Methode, 49  
Trojanisches Pferd, 286  
Trusted Computing, 241  
    Base (TCB), 244  
    Group (TCG), 241  
    Grundlagen, 247  
Trusted Network Connect (TNC), 268  
Trusted Platform, 247  
    Module (TPM), 104  
    Schlüsselhierarchie, 254  
Trusted Viewer, 263  
Tunnelmodus, 380
- U**  
Unterschiede, kulturelle, 15  
User-generated Content, 562  
Utility Settlement Coin, 503
- V**  
Verfahren  
    biometrisches, 181  
    kryptografisches, 46  
    Verfügbarkeitssensor, 310  
    Verifikation von Signaturen, 143  
    Vermeiden von Angriffen, 26  
    Verschlüsselung, 44  
        eines Dokuments, 141  
    Verschlüsselungsverfahren  
        asymmetrisches, 77  
        elementares, 53  
        hybrides, 84  
        symmetrisches, 60  
    Vertrauen, transitives, 251  
    Vertrauensmodell, 131  
        von PGP, 457  
        von S/MIME, 458  
    Videoidentifikation, 156  
    VideoIdent-Verfahren, 156  
    Vier-Augen-Prinzip, 111  
    Vulnerability Scan, 285

- W**  
Währung, digitale, 503  
Wallet, 478  
Web of Trust, 457  
Whaling, 177  
Wireshark als Sensor, 305  
Wirksamkeit, 22  
Wirtschaftsspionage, 17  
Wissensdatenbank, 293  
Wörterbuchangriff, 169  
Wurzel-CA, 132  
Wurzelzertifikat, 425
- X**  
XignQR, 191
- Z**  
Zertifikat  
    digitales, 119  
    elektronisches, 119  
Zertifizierungshierarchie, 131  
Zertifizierungsinstanz, 119  
Zufallszahlengenerierung, 67  
Zweifaktor-Authentifizierung (2FA), 188