

Lernskript

# IT-SICHERHEIT UND DATENSCHUTZ

DLMCSITSDS01



# **IT-SICHERHEIT UND DATENSCHUTZ**

## **IMPRESSIONUM**

Herausgeber:  
IU Internationale Hochschule GmbH  
IU International University of Applied Sciences  
Juri-Gagarin-Ring 152  
D-99084 Erfurt

Postanschrift:  
Albert-Proeller-Straße 15-19  
D-86675 Buchdorf  
[media@iu.org](mailto:media@iu.org)  
[www.iu.de](http://www.iu.de)

DLMCSITSDS01  
Versionsnr.: 001-2024-0320

N.N.

© 2024 IU Internationale Hochschule GmbH  
Dieses Lernskript ist urheberrechtlich geschützt. Alle Rechte vorbehalten.  
Dieses Lernskript darf in jeglicher Form ohne vorherige schriftliche Genehmigung der  
IU Internationale Hochschule GmbH (im Folgenden „IU“) nicht reproduziert und/oder  
unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet wer-  
den.  
Die Autor:innen/Herausgeber:innen haben sich nach bestem Wissen und Gewissen  
bemüht, die Urheber:innen und Quellen der verwendeten Abbildungen zu bestimmen.  
Sollte es dennoch zu irrtümlichen Angaben gekommen sein, bitten wir um eine dement-  
sprechende Nachricht.

# INHALTSVERZEICHNIS

## IT-SICHERHEIT UND DATENSCHUTZ

### Einleitung

Wegweiser durch das Studienskript .....	6
Literaturempfehlungen .....	7
Pflichtliteratur .....	9
Übergeordnete Lernziele .....	11

### Lektion 1

Grundlagen von Datenschutz und IT-Sicherheit .....	13
1.1 Terminologie und Risikomanagement .....	14
1.2 Kernkonzepte der IT-Sicherheit .....	16
1.3 Kernkonzepte von Datenschutz und Privatsphäre .....	22
1.4 Kernkonzepte der Kryptografie .....	23
1.5 Rechtliche Aspekte .....	24

### Lektion 2

Datenschutz .....	29
2.1 Grundbegriffe des Datenschutzes (ISO/IEC 29100, Privacy by Design) .....	30
2.2 Datenschutz in Europa: die DSGVO .....	36
2.3 Datenschutz in den USA .....	41
2.4 Datenschutz in Asien .....	45

### Lektion 3

Anwendung des Datenschutzes .....	49
3.1 Anonymität und Pseudonyme .....	50
3.2 Datenschutz in der Datenwissenschaft und Big Data .....	54
3.3 Benutzer-Tracking im Onlinemarketing .....	56
3.4 Cloud-Computing .....	58

### Lektion 4

Bestandteile der IT-Sicherheit .....	63
4.1 Authentifizierung, Zugriffsverwaltung und -kontrolle .....	64
4.2 Endgerätesicherheit .....	70
4.3 IT-Sicherheit in Netzwerken .....	71
4.4 Entwicklung sicherer IT-Systeme .....	74

<b>Lektion 5</b>	
IT-Sicherheitsmanagement	81
5.1 Sicherheitsrichtlinie .....	82
5.2 Sicherheits- und Risikoanalyse .....	84
5.3 Die ISO-27000-Reihe .....	91
5.4 IT-Sicherheit und IT-Governance .....	94
5.5 Beispiel: IT-Sicherheit für Kreditkarten (PCI DSS) .....	97
<b>Lektion 6</b>	
Kryptografie	99
6.1 Grundbegriffe der Kryptografie .....	100
6.2 Symmetrische Kryptografie .....	103
6.3 Asymmetrische Kryptografie .....	107
6.4 Kryptografie mit elliptischer Kurve .....	109
6.5 Hash-Funktion .....	110
6.6 Sicherer Schlüsselaustausch .....	113
<b>Lektion 7</b>	
Kryptografische Anwendung	117
7.1 Digitale Unterschriften .....	118
7.2 Sichere Internet-Protokolle .....	122
7.3 Blockchain .....	126
7.4 Elektronisches Geld .....	128
<b>Verzeichnisse</b>	
Literaturverzeichnis .....	134
Abbildungsverzeichnis .....	141

# EINLEITUNG

# **HERZLICH WILLKOMMEN**

## **WEGWEISER DURCH DAS STUDIENSKRIPT**

Dieses Studienskript bildet die Grundlage Ihres Kurses. Ergänzend zum Studienskript stehen Ihnen weitere Medien aus unserer Online-Bibliothek sowie Videos zur Verfügung, mit deren Hilfe Sie sich Ihren individuellen Lern-Mix zusammenstellen können. Auf diese Weise können Sie sich den Stoff in Ihrem eigenen Tempo aneignen und dabei auf lerntypspezifische Anforderungen Rücksicht nehmen.

Die Inhalte sind nach didaktischen Kriterien in Lektionen aufgeteilt, wobei jede Lektion aus mehreren Lernzyklen besteht. Jeder Lernzyklus enthält jeweils nur einen neuen inhaltlichen Schwerpunkt. So können Sie neuen Lernstoff schnell und effektiv zu Ihrem bereits vorhandenen Wissen hinzufügen.

In der IU Learn App befinden sich am Ende eines jeden Lernzyklus die Interactive Quizzes. Mithilfe dieser Fragen können Sie eigenständig und ohne jeden Druck überprüfen, ob Sie die neuen Inhalte schon verinnerlicht haben.

Sobald Sie eine Lektion komplett bearbeitet haben, können Sie Ihr Wissen auf der Lernplattform unter Beweis stellen. Über automatisch auswertbare Fragen erhalten Sie ein direktes Feedback zu Ihren Lernfortschritten. Die Wissenskontrolle gilt als bestanden, wenn Sie mindestens 80 % der Fragen richtig beantwortet haben. Sollte das einmal nicht auf Anhieb klappen, können Sie die Tests beliebig oft wiederholen.

Wenn Sie die Wissenskontrolle für sämtliche Lektionen gemeistert haben, führen Sie bitte die abschließende Evaluierung des Kurses durch.

Die IU Internationale Hochschule ist bestrebt, in ihren Skripten eine gendersensible und inklusive Sprache zu verwenden. Wir möchten jedoch hervorheben, dass auch in den Skripten, in denen das generische Maskulinum verwendet wird, immer Frauen und Männer, Inter- und Trans-Personen gemeint sind sowie auch jene, die sich keinem Geschlecht zuordnen wollen oder können.

# LITERATUREMPFEHLUNGEN

## ALLGEMEIN

Amoroso, E./Amoroso, M. (2017): *From CIA to APT: An introduction to cyber security*. Selbstverlag, o. O.

National Institute of Standards and Technology (2018): *Framework for improving critical infrastructure cybersecurity*. Gaithersburg (MD). (Im Internet verfügbar).

Paar, C./Pelzl, J. (2011): *Understanding cryptography: A textbook for students and practitioners*. Springer, Berlin/Heidelberg.

Walker, B. (2019): *Cyber security comprehensive beginners guide to learn the basics and effective methods of cyber security*. Selbstverlag, o. O.

## LEKTION 1

Eckert, C. (2018): *IT-Sicherheit: Konzepte – Verfahren – Protokolle*. De Gruyter Oldenbourg, Berlin, S. 1–41.

Hintzbergen, J. et al. (2015): *Foundations of Information Security Based on ISO27001 and ISO27002*. 3. Auflage, Van Haren, Zaltbommel.

## LEKTION 2

ISO/IEC 29100:2011: *Information technology — Security techniques — Privacy framework*. (Im Internet verfügbar).

## LEKTION 3

Cloud Security Alliance (2017): *Security guidance for critical areas of focus in cloud computing 4.0*. (Im Internet verfügbar).

Information Commissioner's Office (2017): *Big data, artificial intelligence, machine learning and data protection*. (Im Internet verfügbar).

## LEKTION 4

Bartsch, M./Frey, S. H. (2018): *Cybersecurity best practices*. Springer Vieweg, Wiesbaden.

Eckert, C. (2018): *IT-Sicherheit: Konzepte – Verfahren – Protokolle*. De Gruyter Oldenbourg, Berlin, S. 239–277.

National Institute of Standards and Technology (2018): *Framework for improving critical infrastructure cybersecurity*. (Im Internet verfügbar).

Nieles, M./Dempsey, K./Pilliteri, V. (2017): *An introduction to information security*. NIST Special Publication 800.12. Revision 1. (Im Internet verfügbar).

### **LEKTION 5**

Bundesamt für Sicherheit in der Informationstechnik (o. J.): *BSI-Standard 200-1. Managementsysteme für Informationssicherheit (ISMS)*. (Im Internet verfügbar).

Bundesamt für Sicherheit in der Informationstechnik (o. J.): *BSI-Standard 200-2. IT-Grundsatz-Methodik*. (Im Internet verfügbar).

Cole, E./Krutz, R./Conley, J. (2005): *Network security bible*. Wiley, Indianapolis.

Payment Card Industry Security Standards Council (2019): *Secure software lifecycle (secure SLC) requirements and assessment procedures, version 1.0*. (Im Internet verfügbar).

### **LEKTION 6**

Boneh, D./Shoup, V. (2015): *A graduate course in applied cryptography*. Stanford University. (Im Internet verfügbar).

Ertel, W. (2012): *Angewandte Kryptographie*. Hanser, München, S. 21–96.

### **LEKTION 7**

Ertel, W. (2012): *Angewandte Kryptographie*. Hanser, München, S. 97–116 u. 123–143.

Schneider, B. (1995): *Applied cryptography: Protocols, algorithms and source code in C*. Wiley, Indianapolis.

# PFLICHTLITERATUR

## LEKTION 1

Open Web Application Security Project (2017): *OWASP Top 10 – 2017. The The Most Critical Web Application Security Risks.* (Im Internet verfügbar).

## LEKTION 2

California Legislative Information (2018): *SB-456 California consumer privacy act of 2018.* (Im Internet verfügbar).

Europäische Union (2016): *Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR).* In: Amtsblatt der Europäischen Union, 59. Jg., S. 1–88. (Im Internet verfügbar).

## LEKTION 3

Bowman, C. et al. (2015): *The architecture of privacy: On engineering technologies that can deliver trustworthy safeguards.* O'Reilly, Sebastopol (CA), S. 129–144.

## LEKTION 4

Meucci, M./Muller, A. (2019): *OWASP testing guide V4.0, OWASP project.* Open Web Application Security Project. (Im Internet verfügbar).

National Institute of Standards and Technology (o. J.): *An introduction to computer security: The NIST handbook, special publication 800-12.* Gaithersburg (MD). (Im Internet verfügbar).

## LEKTION 5

Microsoft (2009): *The STRIDE Thread Model.* (Im Internet verfügbar).

## LEKTION 6

PGP (2002): *An Introduction to Cryptography.* (Im Internet verfügbar).

## **LEKTION 7**

Kessler, G. C. (2020): *An Overview of Cryptography*. Kapitel 1–3 und 5.1–5.3. (Im Internet verfügbar).

Menezes, J. A./Van Oorschot, P. C./Vanstone, S. A. (1996): *Handbook of applied cryptography*. CRC Press, Boca Raton (FL).

# ÜBERGEORDNETE LERNZIELE

Für Unternehmen, die im Bereich der Informations- und Kommunikationstechnologien (IKT) tätig sind, ist der Schutz von Daten und Informationen eine Herausforderung höchsten Ranges. Im Kurs **IT-Sicherheit und Datenschutz** erklären wir Ihnen, wie Sie die wichtigsten Informationswerte in einer Organisation schützen können, und Sie erfahren, welche Methodik, Ressourcen und Werkzeuge Sie dafür benötigen.

Sie lernen die Bedürfnisse von Organisationen kennen und erfahren, wie man einen soliden Rahmen für die IT-Sicherheit entwickelt, der digitale Informationen, Daten und andere Geräte (ICT-Assets) im Cyberspace schützt. Darüber hinaus erhalten Sie einen Einblick in verschiedene IT-Sicherheitsmodelle und lernen, wie Sie feststellen können, welches für die jeweilige Situation am besten geeignet ist.

Heutzutage ist die angewandte Kryptografie ein sehr wichtiger Bestandteil jedes IT-Systems, da sie zu den wichtigsten Bausteinen im Bereich der IT-Sicherheit gehört. Der Grund dafür ist einfach: Das Wichtigste in jedem Unternehmen ist heute der Schutz von Daten, Informationen und Wissen. Sie sollten während ihrer gesamten Erstellung, Nutzung, Übertragung und Speicherung geschützt werden, was ohne die angewandte Kryptografie weit aus schwieriger wäre.



# LEKTION 1

## GRUNDLAGEN VON DATENSCHUTZ UND IT-SICHERHEIT

### LERNZIELE

Nach der Bearbeitung dieser Lektion werden Sie wissen, ...

- welches die Grundbegriffe von Sicherheit und Risikomanagement sind.
- was die Grundbegriffe und Konzepte von Datenschutz und Privatsphäre ausmachen.
- wo rechtliche Aspekte der IT-Sicherheit zum Tragen kommen können.

# 1. GRUNDLAGEN VON DATENSCHUTZ UND IT-SICHERHEIT

## Einführung

Praktisch jede Organisation ist heutzutage auf Daten und Informationen angewiesen. Diese ermöglichen es ihnen, im Geschäftsleben zu überleben. Ein Verlust dieser Informationen hat enorme Konsequenzen und kann schlimmstenfalls dazu führen, dass ein Unternehmen gezwungen ist, den Markt zu verlassen. Die Gefährdung der Sicherheit persönlicher Daten betrifft in der Folge nicht nur das Unternehmen selbst, sondern auch die Person, zu der diese Daten gehören. Deshalb ist der Schutz von Informationen immer essenzieller geworden.

In der vorliegenden Lektion werden einige grundlegende Konzepte vorgestellt, die Ihnen helfen werden, Sicherheit und Datenschutz zur Gänze zu verstehen. Die rechtlichen Erläuterungen werden nicht nur den Datenschutz und die Privatsphäre zum Thema haben, sondern auch andere rechtliche Aspekte, die bei der IT-Sicherheit eine Rolle spielen. Schließlich und endlich handelt es sich hierbei auch um einen Bereich, der immer stärkerer Steuerung unterliegt und gerade in den letzten Jahren Gegenstand immer intensiverer gesetzlicher Regulierung und Diskussion geworden ist.

### 1.1 Terminologie und Risikomanagement

In diesem Kurs wird häufig der Terminus „IT-Sicherheit“ verwendet. Wenngleich dieser und der Begriff „Informationssicherheit“ häufig synonym verwendet werden, bedeuten sie nicht immer dasselbe. Einige Regulierungsbehörden verlangen von Unternehmen im Finanzsektor, dass sie getrennte Funktionen für Informations- und IT-Sicherheit haben. Wo die Informationssicherheit versucht, Informationen in ihrer analogen Form zu sichern, versucht die IT-Sicherheit, Informationen zu schützen, die durch den Einsatz von Informations- und Kommunikationstechnologie gefährdet sind. In diesem Studienskript soll der Begriff „IT-Sicherheit“ auch die Sicherheit analoger Informationen bezeichnen; insbesondere aber, wenn es um Normen und Gesetze geht, wird der Begriff „Informationssicherheit“ verwendet, wie er in Rechtsdokumenten üblich ist.

#### CIA-Triade

Dieses Modell beeinflusst die Politik der Informationssicherheit in Organisationen.

Die **CIA-Triade** (mitunter auch „CAI“ genannt) der Informationssicherheit definiert die IT-Sicherheit. Diese dient dem Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen.

Abbildung 1: CIA-Triade der IT-Sicherheit



Quelle: Martin Macke, 2020.

Das „C“ in „CIA“ steht für Vertraulichkeit („confidentiality“). Das bedeutet, dass Informationen nur denjenigen zur Verfügung gestellt werden, die zum Zugriff berechtigt sind. Ein Angriff auf die Vertraulichkeit könnte zur unbeabsichtigten Offenlegung einer Kundendatenbank führen, die auf einem Cloud-Speicherplatz gespeichert ist.

Das „I“ steht für Integrität, also die Aufrechterhaltung und Sicherstellung der Richtigkeit und Vollständigkeit von Informationen über ihren gesamten Lebenszyklus hinweg. Ein Hacker, der z. B. die Noten in einem Universitäts-Informationssystem verändert, um die Bewertungen eines Studenten zu verbessern, würde die Integrität beeinträchtigen.

Schließlich steht das „A“ für Verfügbarkeit („availability“); Informationen müssen dann verfügbar sein, wenn sie benötigt werden. Die Verfügbarkeit kann beeinträchtigt werden, wenn ein System angegriffen wird, beispielsweise durch einen DDoS-Angriff („Distributed Denial of Service“), in dessen Folge nicht mehr auf das System zugegriffen werden kann.

Neben der CIA existieren jedoch auch noch andere Sicherheitsziele. Zum Teil können wir sie Teilen oder Kombinationen der CIA-Triade zuordnen, oft stehen sie jedoch auch für sich allein:

1. **Resilienz** stellt sicher, dass Systeme so gebaut werden, dass sie einem Angriff oder Ausfall standhalten können.
2. **Authentizität** stellt sicher, dass das Personal und die Benutzer die sind, für die sie sich ausgeben.
3. **Nachweisbarkeit** bedeutet, dass eine Person eine durchgeführte Aktivität nicht im Nachhinein leugnen kann.

Informationen werden durch Risikominimierung geschützt, daher wird IT-Sicherheit oft als Teil des Risikomanagements gesehen. Dies wird durch einen strukturierten Risikomanagementprozess erreicht, bestehend aus ...

- ... Identifizierung des Risikos,
- Risikoanalyse,
- Steuerung des Risikos sowie
- Berichterstattung über Risiken.

## 1.2 Kernkonzepte der IT-Sicherheit

IT-Sicherheit besteht aus vielen Disziplinen und ist häufig in unterschiedliche Bereiche unterteilt. Verschiedene Organisationen haben Rahmenwerke entwickelt, die speziell auf ihre individuellen Bedürfnisse zugeschnitten sind. Das International Information System Security Certification Consortium (IISSCC) unterteilt die IT-Sicherheit in acht verschiedene Bereiche (o. J.):

- “security and risk management,
- asset security,
- security architecture and engineering,
- communication and network security,
- identity and access management (IAM),
- security assessment and testing,
- security operations, and
- software development security”.

Das National Institute of Standards and Technology (NIST) der USA betrachtet die folgenden Aspekte als Teil der IT-Sicherheit in seiner Standardfamilie SP-800:

1. “Information security governance
2. System development life cycle
3. Awareness and training
4. Capital planning and investment control
5. Interconnecting systems
6. Performance measures
7. Security planning
8. Information technology contingency planning
9. Risk management
10. Certification, accreditation, and security assessments
11. Security services and product acquisition
12. Incidence response
13. Configuration management” (Bowen 2008).

Diese Listen zeigen, dass ein ganzheitliches IT-Sicherheitsprogramm einen breiten Anwendungsbereich hat, der viele Aspekte und Bereiche abdeckt; im Folgenden wird eine Kombination beider Ansätze verwendet, um einige der Kernbegriffe der Sicherheit vorzustellen.

Das Verteidigungskonzept beruht auf der Annahme, dass eine oder mehrere Kontrollen bereits gebrochen ist/sind, sodass andere Verteidigungsschichten in der Lage sein müssen, die Informationsswerte zu schützen. Wir können nicht davon ausgehen, dass einzelne Perimeter, etwa das interne Netzwerk, undurchdringlich wären oder Ressourcen innerhalb dieses Perimeters nicht geschützt werden müssten. Stattdessen setzen wir voraus, dass auch im Inneren ein Schutz erforderlich ist. Aufgrund des neuen Trends von Ressourcen außerhalb des internen Netzwerks (Cloud Computing, SaaS usw.) ist es entscheidend, bei der Umsetzung von Abwehrmaßnahmen alle Teile der Organisation zu berücksichtigen.

## **Unternehmensführung und Risikomanagement**

Die IT-Sicherheits-Governance wird implementiert, um die IT-Sicherheit proaktiv zu managen sowie die notwendigen Kontrollen zu implementieren und zu überwachen; jedoch muss sie auch in Bezug auf die Ziele des IT-Sicherheits-Programms mit dem Unternehmen abgestimmt sein. Nachdem die Bedürfnisse des Unternehmens berücksichtigt wurden, entwickelt eine Organisation ihre IT-Sicherheits-Strategie und es werden Planungs- und Governance-Strukturen eingerichtet. Governance Boards oder Risikoausschüsse zur IT-Sicherheit spielen eine entscheidende Rolle bei der Entscheidung über das weitere Vorgehen, welches wiederum davon abhängt, ob Unternehmen, IT und IT-Sicherheit in dieser Hinsicht dieselben Prioritäten setzen. Es werden eine Sicherheitsrichtlinie sowie ein Plan zur kontinuierlichen Verbesserung und Überprüfung der IT-Sicherheit entwickelt; anschließend überwacht der Governance-Aspekt der IT-Sicherheit deren Umsetzung.

Das Risikomanagement trägt dazu bei, IT-Sicherheitsrisiken zu identifizieren, zu bewerten und zu steuern sowie angemessene Kontrollen zu implementieren, um so die Risiken auf ein tolerierbares Niveau zu bringen.

## **Sicherheitsbewusstsein**

Der Mensch spielt beim Schutz der Organisation die Hauptrolle. Social Engineering ist ein Angriffsvektor, der Menschen dahingehend manipuliert, dass sie Handlungen ausführen, welche einer Organisation schaden könnten. Beispiele dafür sind Phishing-E-Mails, unerbetene Telefonanrufe oder Identitätswechsel-Angriffe. Sicherheitsbewusstsein trägt dazu bei, diese Angriffe einzudämmen, indem es jedem in der Organisation seine Pflichten und Verantwortlichkeiten in Bezug auf die IT-Sicherheit bewusst macht.

Ein Awareness-Programm muss für das Publikum relevant sein, indem beispielsweise ein Benutzer eine andere Schulung erhält als ein Sicherheitsfachmann. Awareness, Schulung und Zertifizierung sind die Komponenten, aus denen sich das Programm zur Förderung des Sicherheitsbewusstseins zusammensetzt. Zu guter Letzt sollte der Erfolg des Programms überwacht werden. Eine Organisation kann kontrollieren, wer die Schulung abgeschlossen hat, oder das Bewusstsein der Benutzer testen, indem sie Test-Phishing-E-Mails versendet.

## **Identitäts- und Zugriffsverwaltung**

Das Identitäts- und Zugriffsmanagement stellt sicher, dass Benutzer in einer Organisation identifiziert werden, und verwaltet ihren Zugriff auf Ressourcen. Ein zentrales Konzept, das dabei zum Einsatz kommt, ist die Access Control List (ACL). Eine solche enthält die Zugriffsrechte für jede Ressource. In den Unix-Betriebssystemen wie Linux und BSD Unix werden alle Benutzer oder Gruppen auf der Grundlage ihrer Berechtigung zum Lesen, Schreiben oder Ausführen von Rechten an einer bestimmten Ressource eingestuft. Diese Kategorien werden als das „rwx-Tripel“ bezeichnet.

Das Konzept der Identifizierung und Authentifizierung, Autorisierung und Rechenschaftspflicht ist auch als „IAAA“ bekannt und beinhaltet die folgenden Schritte:

1. „Identifikation“ bedeutet, dass ein Benutzer angibt, wer er ist. Dies kann durch die Eingabe eines Benutzernamens oder durch die Angabe des Namens an einem Eingangstor erreicht werden.
2. „Authentifizierung“ ist der Prozess, bei dem ein Benutzer in Schritt eins zeigt, dass er die Person ist, für die er sich ausgibt. Dies sollte durch die Darstellung mehrerer Faktoren geschehen, da ein einzelner Faktor leicht beeinträchtigt werden könnte. Es gibt fünf verschiedene Faktoren:
  - a) was man kennt: Typ-1-Authentifizierung (Passwörter, Passphrase, PIN usw.);
  - b) was man hat: Typ-2-Authentifizierung (Ausweis, Reisepass, Chipkarte, Token, Cookie auf dem PC usw.);
  - c) was man ist: Typ-3-Authentifizierung (biometrische Daten wie Fingerabdruck, Iris-Scan, Gesichtsgeometrie usw.);
  - d) wo man ist: Typ-4-Authentifizierung (IP/MAC-Adresse);
  - e) was man tut: Typ-5-Authentifizierung (Unterschrift, Musterfreigabe).
3. Die „Autorisierung“ prüft, auf welche Ressourcen ein Benutzer Zugriff hat. Dies geschieht über RBAC, DAC oder MAC und ACLs.
4. Die Rechenschaftspflicht bedeutet, dass ein Audit-Trail, wie z. B. ein Protokoll, existiert. Es verfolgt die Handlungen der Benutzer und zeichnet auf, was sie getan haben, um Nachweisbarkeit zu gewährleisten.

## **Netzwerksicherheit**

Netzwerksicherheit umfasst alle Mittel, die zum Schutz der Netzwerk-CIA der Organisation eingesetzt werden. Es bestehen zahlreiche Möglichkeiten, ein Netzwerk zu schützen, einige davon werden im Folgenden vorgestellt.

Die Verschlüsselung des Netzwerkverkehrs ist ein grundlegendes Konzept um sicherzustellen, dass ein möglicher Angreifer, wenn er Zugang zu einem Netzwerk hat, innerhalb von diesem keine Informationen sehen kann. Heutzutage sollten Organisationen so viel Netzwerkverkehr wie möglich verschlüsseln, um die Angriffsvektoren möglichst weitgehend zu reduzieren. Nicht-verschlüsselte Protokolle wie Telnet oder ftp müssen vermieden und durch ihre verschlüsselten Alternativen ersetzt werden. Bei der Verwendung von drahtlosen Netzwerken (WiFi) ist die Verschlüsselung i. d. R. in die Protokolle eingebaut, z. B. WiFi Protected Access 2 (WPA2).

Eine Firewall überwacht und kontrolliert den ein- und ausgehenden Datenverkehr auf der Grundlage vordefinierter Regeln. Ursprünglich wurden Firewalls an den Außengrenzen eines Netzwerks platziert, heutzutage finden wir sie jedoch auch innerhalb von Organisationen, wo sie das Netzwerk segmentieren und eine umfassende Sicherheit gewährleisten. Komplexe Firewall-Strukturen sind die neue Norm. So haben sich Firewalls im Laufe der Zeit wie folgt entwickelt:

1. Firewalls der ersten Generation, oder Paketfilter-Firewalls, inspizieren jedes Paket und filtern es nach bestimmten Regeln, i. d. R. nach IP-Adresse und Ports.
2. Filter der zweiten Generation, oder Stateful-Filter, nutzen auch Informationen, die auf der Verbindung (Session) zwischen zwei Hosts basieren.
3. Firewalls der dritten Generation, oder Anwendungs-Firewalls, verstehen bestimmte Anwendungen und ihre Schwachstellen, sodass sie diese schützen können.
4. Next Generation Firewalls (NGFW) können Verbindungen auf einer tieferen Ebene inspizieren. Intrusion Prevention Systems (IPS) lernen aus dem Verhalten von Hosts und Netzwerkverbindungen, um so Angriffe verhindern zu können.

## Sicherheit bei der Software-Entwicklung

Der System Development Life Cycle (SDLC) umfasst die Entwicklung, Wartung und schließlich Außerbetriebnahme von Informationssystemen. Sicherheit muss für alle Phasen des SDLC gewährleistet werden. Das Open Web Application Security Project (OWASP) ist eine gemeinnützige Organisation, die typische Schwachstellen von Webanwendungen veröffentlicht, aber auch Standards zum Thema der sicheren Implementierung von Software entwickelt.

Die OWASP-Top-10-Liste, zuletzt aktualisiert in 2021, besteht aus den folgenden zehn Schwachstellen, die häufig in Webanwendungen zu finden sind (OWASP 2021):

- A1:2021 – Broken Access Control (gebrochene Zugangskontrolle): Beschränkungen dessen, was authentifizierte Benutzer tun dürfen, werden oft nicht richtig durchgesetzt. Angreifer können diese Mängel ausnutzen und so über nichtautorisierte Funktionen und/oder Daten verfügen, etwa Zugriff auf die Konten anderer Benutzer und Einsicht in sensible Dateien sowie die Möglichkeit, die Daten anderer Benutzer oder die Zugriffsrechte auf diese zu ändern.
- A2:2021 – Cryptographic Failures (kryptographische Gefährdung sensibler Daten): Viele Webanwendungen und APIs schützen sensible Daten, wie z. B. Finanzdaten, Daten aus dem Gesundheitswesen und personenbezogene Daten, nicht richtig, da sie kryptographische Methoden fehlerhaft oder überhaupt nicht anwenden. Beispielsweise werden schwache oder für die Aufgabe ungeeignete Algorithmen und Protokolle verwendet, oder auch schwache Schlüssel. Angreifer können derlei schlecht geschützte Daten stehlen oder verändern, um Kreditkartenbetrug, Identitätsdiebstahl oder andere Straftaten zu begehen. Sensible Daten sind ohne zusätzlichen Schutz, wie z. B. Verschlüsselung im Ruhezustand oder bei der Übertragung, gefährdet und bedürfen daher beim Austausch mit dem Browser besonderer Vorsichtsmaßnahmen.
- A3:2021 – Injection (Injektionsfehler): Injektionsfehler wie die SQL-, NoSQL-, OS- und LDAP-Injektion können auftreten, wenn nicht vertrauenswürdige Daten als Teil eines Befehls oder einer Abfrage an einen Interpreter gesendet werden, meist weil sie unge-

prüft aus einem Eingabefeld übernommen werden. Die feindlichen Daten des Angreifers können den Interpreter austricksen, sodass er unbeabsichtigte Befehle ausführt oder ohne entsprechende Autorisierung auf Daten zugreift.

- A4:2021 – Insecure Design (unsicherer Entwurf): Selbst bei perfekter Implementierung ist eine Webanwendung unsicher, wenn der Entwurf der Anwendung unsicher und beispielsweise wichtige Kontrollen nicht einbezieht. Um einen sicheren Entwurf zu erreichen, werden meist Werkzeuge wie die Modellierung von Bedrohungen, sichere Entwurfsmuster und -prinzipien, oder Referenzarchitekturen verwendet.
- A5:2021 – Security Misconfiguration (sicherheitstechnische Fehlkonfiguration): Dies ist häufig eine Folge unsicherer Standardkonfigurationen, nicht benötigten offenen Ports oder Diensten, falsch konfigurierter HTTP-Header, oder unangemessen ausführlicher Fehlermeldungen, die sensible Informationen enthalten. Alle Betriebssysteme, Frameworks, Bibliotheken und Anwendungen müssen sicher konfiguriert sowie zeitnah gepatcht und aktualisiert werden.
- A6:2021 – Vulnerable and Outdated Components (Verwendung verwundbarer und veralteter Komponenten): Bibliotheken, Frameworks und andere Softwaremodule laufen mit den gleichen Privilegien wie die Anwendung selbst. Wenn nun eine solche verwundbare oder veraltete Komponente für einen Angriff ausgenutzt wird, kann dies einem schwerwiegenden Datenverlust oder einer Serverübernahme Tür und Tor öffnen. Anwendungen und APIs, die verwundbare oder veraltete Komponenten verwenden, können den Schutz von Anwendungen untergraben und verschiedene Angriffe ermöglichen.
- A7:2021 – Identification and Authentication Failures (fehlerhafte Identifikation und Authentifizierung): Anwendungsfunktionen im Zusammenhang mit Authentifizierung und Sitzungsverwaltung sind oft fehlerhaft implementiert, so dass Angreifer Passwörter, Schlüssel oder Sitzungs-Tokens compromittieren oder andere Implementierungsfehler ausnutzen können, um vorübergehend oder dauerhaft die Identität anderer Benutzer anzunehmen. Dazu gehören beispielsweise das Erlauben schwacher Passwörter, die Möglichkeit zu Brute-Force-Angriffen, oder schwache Prozesse, um mit vergessenen Passwörtern umzugehen.
- A8:2021 – Software and Data Integrity Failures (Integritätsfehler bei Software und Daten): Wenn Software oder Daten zwischen Umgebungen transferiert wird, muss ihre Integrität sichergestellt werden. Das betrifft beispielsweise den Transfer von Code entlang einer CI/CD-Pipeline, das Herunterladen von Programmaktualisierungen, oder unsichere **Deserialisierung**.

### **Serialisierung und Deserialisierung**

Serialisierung beschreibt die Konvertierung von Objekten in ein lineares (serielles) Format, beispielsweise eine Zeichenkette (String). Deserialisierung beschreibt umgekehrt die Konvertierung eines solchen linearen Formats zurück in das zugehörige Objekt.

- A9:2021 – Security Logging and Monitoring Failures (fehlerhafte Protokollierung und Überwachung): Gekoppelt mit fehlender oder ineffektiver Integration mit der Reaktion auf Vorfälle, ermöglicht eine unzureichende Protokollierung und Überwachung den Angreifern, Systeme weiter zu attackieren, zu weiteren Systemen überzugehen, und dabei Daten zu manipulieren, zu extrahieren oder zu zerstören. Die meisten Studien zu Sicherheitsverletzungen zeigen, dass bis zur Entdeckung eines Angriffs über 200 Tage vergehen können, und sie werden erfahrungsgemäß eher von externen Parteien als von internen Prozessen oder der Überwachung entdeckt.
- A10:2021 – Server-Side Request Forgery (SSRF): Bei einem SSRF-Angriff wird ein unsicherer Server dazu verwendet, HTTP-Anfragen an ein System zu senden, das der Angreifer nicht direkt angreifen kann. So kann der Server beispielsweise dazu gebracht werden, sich mit einem externen System zu verbinden und vertrauliche Daten wie Login-Daten an den Angreifer offenzulegen. Ein SSRF-Angriff ist meist möglich, weil ein Server von einem Dritten als vertrauenswürdig eingestuft wird und diesem Anfragen sendet,

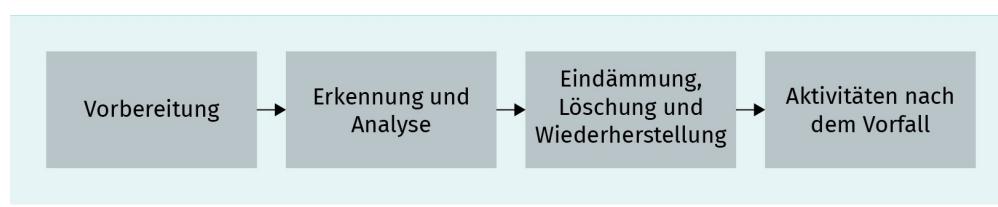
die eine URL enthält. In diesem Fall kann ein Angreifer versuchen, die URL oder andere Teile der Anfrage zu modifizieren und damit den Empfänger (möglicherweise der gleiche unsichere Server) dazu zu bringen interne Ressourcen offenzulegen oder zu verändern.

OWASP schlägt das Software Assurance Maturity Model (SAMM) als erstes Reifegradmodell für Software Assurance vor. Es bietet einen effektiven und messbaren Weg für alle Arten von Organisationen, die Sicherheitslage ihrer Software zu analysieren und zu verbessern. OWASP SAMM unterstützt, beginnend bei Entwicklung und Erwerb, den gesamten Software-Lebenszyklus und ist technologie- sowie prozessunabhängig. Es ist absichtlich so aufgebaut, dass es evolutionär und risikogetrieben ist. Die jüngste entwickelte Version von OWASP SAMM ist die Version 2.0.

## Management von Sicherheitsvorfällen

Jede Organisation und jedes Sicherheitsmanagement wird sich dafür einsetzen, die Auswirkungen kritischer Zwischenfälle auf ein akzeptables Maß zu reduzieren. Ein Plan zur Bewältigung von Sicherheitsvorfällen beinhaltet daher die notwendigen Schritte, um deren Auswirkungen zu beschränken. Dieser Plan sollte mindestens einmal pro Jahr getestet werden. Die folgende Abbildung zeigt den typischen Lebenszyklus eines Vorfalls.

Abbildung 2: Lebenszyklus eines Sicherheitsvorfalls



Quelle: Martin Macke, 2020.

Zur Vorbereitung wird eine Richtlinie für die Reaktion auf Vorfälle ausgearbeitet und der Reaktions- und Meldeplan entwickelt. In Standardarbeitsanweisungen (Standard Operational Procedures – SOPs) werden die zu verwendenden spezifischen technischen Prozesse, Techniken und Checklisten definiert. Struktur und personelle Besetzung des Teams zur Reaktion auf Vorfälle werden festgelegt, das Team wird geschult und es werden Präventionsmaßnahmen ergriffen.

Das Erkennen und Analysieren eines Vorfalls ist oft die schwierigste Phase des Reaktionsprozesses. Um zu verstehen, ob und wann ein Vorfall eintritt, kann ein System für das Management von Sicherheitsvorfällen und Ereignissen (Security Incident and Event Management – SIEM) verwendet werden, da es jede Sekunde zu Millionen verschiedener Ereignisse kommt und die Teams sich auf die relevanten Vorfälle konzentrieren müssen, um eine Ermüdung durch das Beachten zu vieler Ereignisse (Event Fatigue) zu vermeiden.

Ist der Vorfall identifiziert, müssen Maßnahmen zur Eindämmung ergriffen werden, damit er sich nicht in der gesamten Organisation oder auf andere Systeme ausbreitet. Nach der Durchführung dieser Maßnahmen kann eine Löschung erforderlich sein, um alle Überreste

des Vorfalls zu beseitigen, z. B. das Löschen eines Virus. Die Wiederherstellung kann sich auf Daten aus Backups, das Installieren von Patches oder das Ändern von Passwörtern beziehen.

Zu den Überprüfungen und Aktivitäten nach einem Zwischenfall gehören die Erörterung daraus zu ziehender Lehren und die Durchführung weiterer Sicherheitskontrollen, um ähnliche Vorfälle in Zukunft zu vermeiden.

## 1.3 Kernkonzepte von Datenschutz und Privatsphäre

Datenschutz verweist auf den immerwährenden Konflikt zwischen dem Schutz der Privatsphäre und der Verarbeitung von Personendaten. IT-Sicherheit wird zum Schutz personenbezogener Daten (Personal Identifiable Information – PII) verwendet, die Sicherheitskontrollen werden als technische und administrative (oder organisatorische) Maßnahmen bezeichnet.

Weltweit gelten unterschiedliche Gesetze für den Datenschutz, und viele Gesetze befinden sich derzeit (Stand: Anfang 2020) noch im Gesetzgebungsverfahren. Jüngste Ergänzungen zum Zeitpunkt der Verfassung dieses Artikels sind die Datenschutz-Grundverordnung (DSGVO) in der Europäischen Union und der Californian Consumer Privacy Act (CCPA), der, wenngleich auf einen einzelnen Bundesstaat beschränkt, eine neue Ära der Datenschutzgesetze in den USA einläutet. Insbesondere die DSGVO hat viele Länder dazu veranlasst, ihre Datenschutzgesetze zu überdenken, und einige davon, darunter Indien, Brasilien und Nigeria, haben bereits neue Datenschutzgesetze erlassen oder durchlaufen gerade den Gesetzgebungsprozess.

Die Grundprinzipien des Datenschutzes nach ISO/IEC 29100 lauten wie folgt:

1. „Consent and choice“
2. „Purpose legitimacy and specification“
3. „Collection limitation“
4. „Data minimization“
5. „Use, retention, and disclosure limitation“
6. „Accuracy and quality“
7. „Openness, transparency, and notice“
8. „Individual participation and access“
9. „Accountability“
10. „Information security“
11. „Privacy compliance“

## 1.4 Kernkonzepte der Kryptografie

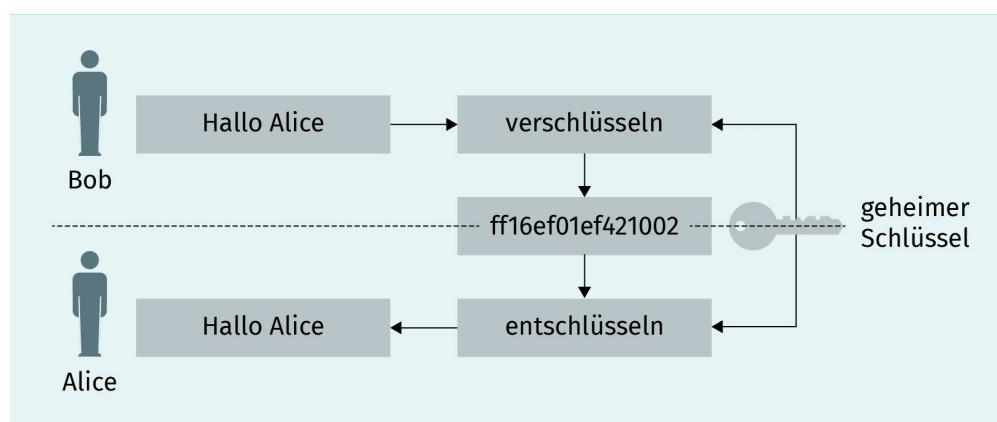
Kryptografie ist die Lehre von der sicheren Kommunikation. Die Kryptoanalyse versucht, Schwachstellen in kryptografischen Algorithmen zu finden, welche die Entschlüsselung von verschlüsselten Nachrichten ermöglichen.

Zunächst müssen wir die Terminologie der Kryptografie definieren.

1. **Klartext** ist der Name, der für die Nachricht verwendet wird, bevor eine Verschlüsselung angewendet wird, wenn sie also noch für Computer oder Menschen lesbar ist.
2. **Verschlüsselung** ist der Prozess, bei dem eine Nachricht so verschlüsselt wird, dass niemand ohne die entsprechende Berechtigung auf sie zugreifen kann.
3. **Chiffretext** ist die Bezeichnung für die verschlüsselte Nachricht.
4. **Chiffre** ist der Algorithmus, der den Klartext ver- und entschlüsselt.
5. **Die Entschlüsselung** ist das Verfahren, mit dem die Chiffre auf den Chiffretext angewendet wird, wodurch der Klartext entsteht.
6. **Der Schlüssel** ist nur autorisierten Personen oder Systemen bekannt und erlaubt zusammen mit der Chiffre die Ver- und Entschlüsselung von Klar- und Chiffretext.

Das Kerckhoffs-Prinzip besagt, dass ein kryptografisches System auch dann sicher sein muss, wenn außer dem Schlüssel alles bekannt ist (Kerckhoffs 1883). Sicherheit wird nicht erreicht, indem man den Verschlüsselungsalgorithmus, sondern indem man den Schlüssel sicher aufbewahrt. Verstöße gegen diesen Grundsatz werden als Sicherheit durch Unklarheit (Security by Obscurity) bezeichnet und haben sich auf lange Sicht als unsicher erwiesen. Der Grund dafür ist, dass bekannte Algorithmen durch kryptografische Forschungen überprüft, bewiesen und verbessert werden können und geheime Algorithmen viel eher eine Schwäche haben.

Abbildung 3: Symmetrische Kryptografie



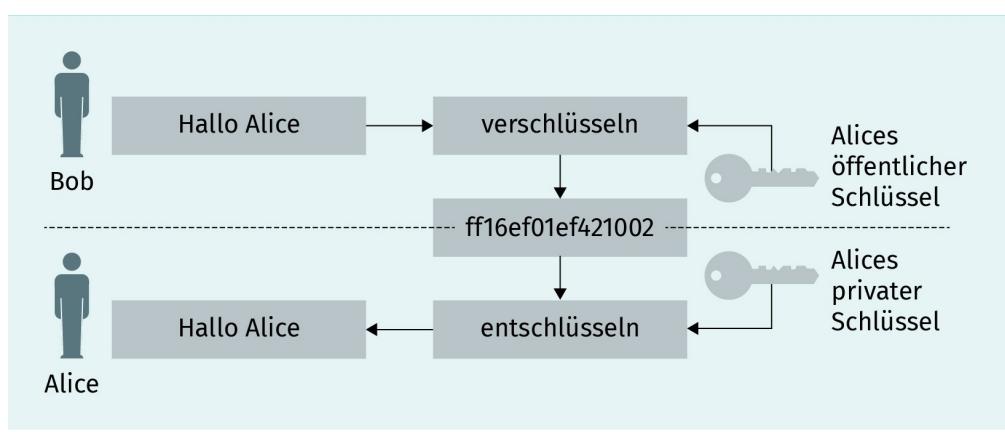
Quelle: Martin Macke, 2020.

Um Akteure zu repräsentieren, die eine Botschaft austauschen wollen, ist es üblich, die Namen Bob und Alice zu verwenden. In der obigen Abbildung kennen sie beide einen geheimen Schlüssel, den sie zur Verschlüsselung des Klartextes „Hallo Alice“ verwenden.

Sie tauschen einen Chiffriertext aus und Alice verwendet den geheimen Schlüssel, um den Chiffriertext in den ursprünglichen Klartext zu entschlüsseln. Da ein gemeinsamer Schlüssel verwendet wird, nennt man dies symmetrische Kryptografie.

Bei der symmetrischen Kryptografie besteht die Herausforderung, den geheimen Schlüssel auf sichere Weise auszutauschen. In modernen Szenarien, in denen wir jede Nachricht in einem weltweiten Computernetzwerk verschlüsseln wollen, wäre ein Schlüsselaustausch unmöglich. Die asymmetrische Kryptografie löst dieses Problem, indem sie jedem Akteur zwei Schlüssel gibt: einen öffentlichen Schlüssel, der allen bekannt ist, und einen privaten, der geheim ist. Der öffentliche Schlüssel kann verwendet werden, um eine Nachricht an eine Person zu verschlüsseln, und der private Schlüssel kann verwendet werden, um sie zu entschlüsseln.

**Abbildung 4: Asymmetrische Kryptografie**



Quelle: Martin Macke, 2020.

Asymmetrische Kryptografie kann auch verwendet werden, um digitale Signaturen anzubringen und Nachweisbarkeit zu gewährleisten.

Im Allgemeinen ist die asymmetrische Kryptografie viel langsamer als die symmetrische. Moderne kryptografische Systeme verwenden daher oft asymmetrische Kryptografie, um einen geheimen symmetrischen Schlüssel auszutauschen, und anschließend für den Nachrichtenaustausch weiterhin symmetrische Kryptografie.

Allgemein bekannte Algorithmen für symmetrische Kryptografie sind AES oder 3DES, für asymmetrische Kryptografie RSA oder ECC.

## 1.5 Rechtliche Aspekte

Wenngleich bereits Gesetze zum Schutz von Daten und Privatsphäre wirksam umgesetzt werden, beeinflussen doch auch noch andere rechtliche Aspekte die IT-Sicherheit.

## **Gesetze zur IT-Sicherheit in den USA**

Die wichtigste US-amerikanische Regelung im Bereich der IT-Sicherheit ist der Federal Information Security Management Act von 2002, welcher durch den Federal Information Security Modernization Act von 2014 noch einmal modifiziert wurde (beide auch bekannt als FISMA). Das Gesetz erkennt die Bedeutung der IT-Sicherheit in Bezug auf die wirtschaftliche und nationale Sicherheit der Vereinigten Staaten an und verpflichtet jede Bundesbehörde, ein behördeneites Programm zur Gewährleistung der Sicherheit jener Informationen und Systeme zu entwickeln, zu dokumentieren und umzusetzen, welche ihre Operationen und Informationswerte unterstützen, einschließlich derer, die von einer anderen Behörde, einem Auftragnehmer oder einer anderen Quelle bereitgestellt oder verwaltet werden.

Der FISMA verlangt von den Bundesbehörden ein risikobasiertes Sicherheitsmanagement und ein Sicherheitsprogramm, das die folgenden Aufgaben erfüllt (Hansche 2005):

1. Planung der Sicherheit,
2. Gewährleistung, dass die Verantwortung bezüglich der Sicherheit an die zuständigen Beamten übertragen wird,
3. regelmäßige Überprüfung der Sicherheitskontrollen in ihren Systemen sowie
4. Genehmigung zur Verarbeitung vor und, in regelmäßigen Abständen, nach dem Betrieb.

Das National Institute of Standards and Technology (NIST) stellt Dokumente dazu zur Verfügung, wie eine Bundesbehörde dem FISMA nachkommen kann, und gibt Hinweise zum Vorgehen (NIST o. J.).

## **Gesetze zur IT-Sicherheit in Europa**

Die wichtigsten Vorschriften in Europa sind die Verordnungen über die Agentur der Europäischen Union für Computer- und Netzsicherheit (European Network and Information Security Agency – ENISA) und die Richtlinie über die Sicherheit von Netz- und Informati-onssystemen (NIS).

ENISA (o. J.) leistet einen aktiven Beitrag zur europäischen IT-Sicherheits-Richtlinie, indem sie Mitgliedstaaten und Interessenvertreter der Europäischen Union bei der Reaktion auf groß angelegte Cyberzwischenfälle unterstützt, wenn zwei oder mehr EU-Mitgliedstaaten betroffen sind. Diese Arbeit trägt auch zum ordnungsgemäßen Funktionieren des digitalen Binnenmarkts bei.

Der Ansatz von ENISA (ebd.) besteht aus Aktivitäten in den folgenden Bereichen:

- Empfehlungen und unabhängige Beratung zur IT-Sicherheit,
- Aktivitäten zur Unterstützung der Richtliniengestaltung und -umsetzung,
- praktische Arbeit, bei der die ENISA direkt mit operativen Teams in der gesamten EU zusammenarbeitet,

- Zusammenarbeit der EU-Gemeinschaften und Koordination der Reaktion auf groß angelegte grenzüberschreitende Zwischenfälle im Bereich der Computer- und Netz sicherheit sowie
- Ausarbeitung von Zertifizierungssystemen für die IT-Sicherheit.

Die ENISA arbeitet mit den nationalen Computer Security Incident Response Teams (CSIRTs) zusammen.

Die NIS trägt dazu bei, das Niveau der IT-Sicherheit innerhalb der EU zu erhöhen. Sowohl Anbieter digitaler Dienste (Data Processing Services – DPS) als auch Betreiber wesentlicher Dienste (Operators of Essential Services – OES) fallen in den Geltungsbereich der Richtlinie. OES bieten Dienstleistungen wie Energie- und Lebensmittelversorgung sowie Finanzdienstleistungen an, die einen großen Einfluss auf gesellschaftliche und wirtschaftliche Aktivitäten haben.

DPS wie OES müssen größere Sicherheitsvorfälle an ihre CSIRTs melden.

Die NIS verfolgt einen risikobasierten Ansatz, der sowohl von den DPS als auch von den OES Folgendes verlangt (Europäische Kommission 2016):

- Risiken vorbeugen: technische und organisatorische Maßnahmen, die dem Risiko angemessen und verhältnismäßig sind.
- Gewährleistung der Sicherheit von Netz- und Informationssystemen: Die Maßnahmen sollten ein risikoadäquates Sicherheitsniveau rund um das Netzwerk und die Informationssysteme gewährleisten.



## ZUSAMMENFASSUNG

IT-Sicherheit und Datenschutz spielen in der heutigen Welt eine entscheidende Rolle. Unter „IT-Sicherheit“ versteht man dabei den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen durch einen risikobasierten Ansatz. Viele Aspekte oder Bereiche machen ein ganzheitliches IT-Sicherheitsprogramm aus, darunter Zugangskontrolle, Netzwerksicherheit oder die sichere Entwicklung von Software.

Die Kryptografie hilft bei der geheimen Übertragung von Nachrichten, wobei zwischen symmetrischer und asymmetrischer Kryptografie unterschieden wird. Die Kryptoanalyse versucht, Schwachstellen in kryptografischen Systemen zu finden.

Datenschutz und Datensicherheit schützen die Interessen des Einzelnen, wenn seine persönlichen Daten verarbeitet werden.

Viele zusätzliche gesetzliche Regelungen betreffen die IT-Sicherheit, darunter der FISMA aus den Vereinigten Staaten oder die NIS-Verordnungen und -Gesetze, die in der Europäischen Union umgesetzt werden.



# **LEKTION 2**

## **DATENSCHUTZ**

### **LERNZIELE**

Nach der Bearbeitung dieser Lektion werden Sie wissen, ...

- welche grundlegenden Prinzipien der Privatsphäre und des Datenschutzes in allen Datenschutzbestimmungen anwendbar sind.
- wie die ISO 29100 die Grundlagen des Datenschutzes beschreibt.
- was die Besonderheiten der Datenschutzbestimmungen in Europa (DSGVO) sind.
- wie der Datenschutz in den USA im Allgemeinen und in Kalifornien im Besonderen gehandhabt wird.
- welche Bestimmungen es zum Datenschutz in Asien gibt.

## 2. DATENSCHUTZ

### Einführung

Datenschutz und Datensicherheit spielen eine immer wichtigere Rolle in unserem Privatleben wie auch bei der Datenverarbeitung in aller Art von Organisationen. Im Jahr 2019 machte der japanische Premierminister Shinzo Abe den Datenschutz zu einer der Prioritäten für den von seinem Land ausgerichteten G20-Gipfel. Viele Industrie- und Entwicklungsländer haben bereits neue Datenschutzregularien erlassen oder führen derzeit Gesetzgebungsverfahren zu deren Einführung durch. Dies zeigt, dass Vorschriften ein wichtiger Faktor sind, den es im 21.Jahrhundert zu berücksichtigen gilt.

Der Schutz der Privatsphäre jedes Einzelnen ist ein wichtiges ethisches Erfordernis, weshalb Zivilgesellschaften auf der ganzen Welt weiteren Schutz fordern. Globale und ganzheitliche Konzepte definieren den Datenschutz und legen Prinzipien fest, die in jeder nationalen und internationalen Regelung enthalten sind.

### 2.1 Grundbegriffe des Datenschutzes (ISO/IEC 29100, Privacy by Design)

#### Datenschutz versus Privatsphäre

Datenschutz und Privatsphäre stehen zwar miteinander in engem Zusammenhang, werden aber weltweit als zwei getrennte Rechte anerkannt. In vielen Ländern gelten sie als wesentliche Bestandteile einer nachhaltigen Demokratie.

In Artikel 1 der Allgemeinen Erklärung der Menschenrechte (UN 1948) wird die Menschenwürde als ein absolutes Grundrecht anerkannt. Diese Vorstellung von Würde, Privatsphäre oder dem Recht auf ein Privatleben, auf Autonomie oder darauf, in Ruhe gelassen zu werden, spielt eine zentrale Rolle. Die Privatsphäre ist nicht nur ein individuelles Recht, sondern auch ein gesellschaftlicher Wert.

Historisch gesehen wurde die Privatsphäre in bestimmten Teilen der Welt, etwa den USA, häufig als ein Element der Freiheit betrachtet, beispielsweise als das Recht, frei von staatlichen Eingriffen zu sein.

#### Privatsphäre – ein Grundrecht

Fast jedes Land der Welt erkennt die Privatsphäre auf irgendeine Weise an, sei es in seiner Verfassung oder anderen Bestimmungen. Darüber hinaus wird die Privatsphäre als ein universelles Menschenrecht anerkannt, der Datenschutz hingegen nicht – zumindest noch nicht.

Das Recht auf Privatsphäre oder ein Privatleben ist in der Allgemeinen Erklärung der Menschenrechte (Artikel 12) (UN 1948), in der Europäischen Menschenrechtskonvention (Artikel 8) (EGMR 2013) und in der Europäischen Charta der Grundrechte (Artikel 7) verankert (EU 2000, S. C 364/10).

### **Was ist Datenschutz?**

Der Datenschutz bezieht sich auf alle Informationen, die auf eine identifizierte oder identifizierbare natürliche (lebende) Person verweisen, einschließlich Namen, Geburtsdaten, Fotos, Videomaterial, E-Mail-Adressen, Telefonnummern und mehr.

Verschiedene Regelungen haben unterschiedliche Bezeichnungen für diese Personen, z. B. „Betroffene“ in der EU, „PII-Principals“ in internationalen Normen wie ISO 27701 und ISO 29100 oder Verbraucher („consumers“) in Kalifornien. In diesem Studienskript wird der Begriff „Betroffene“ verwendet, um die Konsistenz und Neutralität bestimmter spezifischer Regelungen zu gewährleisten.

Der Begriff, der für die Daten über einen Betroffenen verwendet wird, lautet für den Rest dieser Lektion Personal Identifiable Information (PII – personenbezogene Daten), auch dies ein Begriff, der in vielen Vorschriften und in den einschlägigen ISO-Normen verwendet wird.

Der Begriff des Datenschutzes hat seinen Ursprung im Recht auf Privatsphäre – beide dienen nicht nur der Wahrung und Förderung grundlegender Werte und Rechte, sondern auch der Ausübung anderer Rechte und Freiheiten wie der Meinungs- oder Versammlungsfreiheit.

Der Datenschutz umfasst die Rechte des Betroffenen, die in einer fairen Verarbeitung, in Transparenz und bestimmten Rechten auf Zugang oder Änderung von PII bestehen. Er verfolgt präzise Ziele, um eine faire Verarbeitung (Erhebung, Nutzung und Speicherung) von personenbezogenen Daten sowohl im öffentlichen als auch im privaten Sektor zu gewährleisten.

### **Grundsätze des Datenschutzes**

Die folgenden Prinzipien leiten alle globalen Datenschutzbestimmungen. Sie finden sich in internationalen Normen, insbesondere ISO/IEC 29100 („Information technology – Security techniques – Privacy framework“; 2011), ISO/IEC 27701 („Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines“; 2019).

### **Verantwortliche und Auftragsverarbeiter**

Die für die Verarbeitung von PII Verantwortlichen bestimmen die Mittel und Zwecke der Verarbeitung von PII. Sie müssen sicherstellen, dass die geltenden Gesetze eingehalten werden und sind verpflichtet, dies auch nachzuweisen. Ein Auftragsverarbeiter verarbeitet

PII, indem er die Anweisungen eines für die PII-Verarbeitung Verantwortlichen befolgt. In vielen Vorschriften wird für die Beziehung zwischen den beiden ein schriftlicher Vertrag verlangt.

### **Zustimmung und Wahl**

Betroffene sollten die Wahl haben, ob ihre Daten verarbeitet werden oder nicht. Diese Wahl sollte im Voraus bestehen und die Konsequenzen eines Opt-in oder Opt-out sollten korrekt dargestellt werden. „Opt-in“ bedeutet dabei, dass ein Betroffener aktiv seine Zustimmung erteilen muss, während „Opt-out“ heißt, dass eine voreingestellte Zustimmung aktiv abgelehnt werden muss.

Die von den Betroffenen erteilte Zustimmung kann zu einem späteren Zeitpunkt zurückgezogen werden. Dieser Grundsatz steht nicht im Widerspruch zu der Tatsache, dass die Verarbeitung in vielen Fällen auf der Grundlage bestehender Verträge, rechtlicher Anforderungen oder anderer rechtlicher Regeln erfolgt. Dies gilt für Fälle, in denen die Zustimmung die rechtliche Grundlage für die Verarbeitung von PII ist.



#### **BEISPIEL**

Bevor Cookies verwendet werden, um das Verhalten eines Benutzers auf einer Website zu verfolgen, sollte die Zustimmung eingeholt werden, dass Cookies auf dem Gerät des Benutzers gespeichert werden können.

### **Legitimierung und Zweckbindung**

Jede Verarbeitung von PII muss in Übereinstimmung mit den geltenden Gesetzen erfolgen. Der Zweck der Datenverarbeitung muss den Betroffenen im Voraus mitgeteilt werden; wenn sich aber der Zweck im Laufe der Zeit ändert, sollte dies Gegenstand einer neuerlichen Mitteilung sein.



#### **BEISPIEL**

Wenn Daten von einem Webshop zum Zweck der Lieferung der bestellten Produkte an den Betroffenen gesammelt wurden, sollte der Zweck nicht geändert werden (etwa dahingehend, dass diese Daten nun Teil einer großen Datenanalyse sind), ohne weitere Zustimmung einzuholen und den Betroffenen zu informieren.

### **Angemessenheit**

Die Sammlung von PII sollte sich auf das beschränken, was für den definierten Zweck und innerhalb der Grenzen der anwendbaren Gesetze unbedingt erforderlich ist.



### BEISPIEL

Ein Arbeitgeber könnte möglicherweise die E-Mail-Postfächer seiner Mitarbeiter überwachen, um festzustellen, wie oft sie vertriebliche E-Mails schreiben. Da auf diese Weise jedoch sehr stark in die Persönlichkeitsrechte eingegriffen würde, wäre dieses Vorgehen nicht angemessen.

## Datensparsamkeit

Die Datensparsamkeit steht im Zusammenhang mit der Beschränkung des Sammelns, geht aber noch weiter, wenn man auch die Verarbeitung nach der ursprünglichen Sammlung von PII betrachtet. Die Prozesse und Systeme, die PII verarbeiten, müssen also die Anzahl der Beteiligten begrenzen, die Zugang zu Daten haben oder diese verarbeiten; sie müssen sicherstellen, dass auf die PII nur auf einer Need-to-know-Basis zugegriffen werden kann, und Optionen anbieten, welche ohne die Verwendung von PII auskommen. Darüber hinaus müssen PII gelöscht werden, wenn sie nicht mehr benötigt werden und es keine gesetzlichen Bestimmungen gibt, die ihre Speicherung vorschreiben.



### BEISPIEL

In einem Krankenhaus könnte es für das gesamte Verwaltungs- und medizinische Personal praktisch sein, Zugang zu den Patienten-PII zu haben. Allerdings sollten Ärzte und Krankenschwestern auf einer Need-to-know-Basis nur Zugang zu den Daten ihrer eigenen Patienten haben; das Verwaltungspersonal wiederum benötigt nur Daten, die für die Bewältigung von Versicherungs- und Rechnungsfragen relevant sind.

## Einschränkung der Verwendung, Aufbewahrung und Offenlegung

Daten dürfen nicht für immer aufbewahrt werden. Bei diesem Prinzip geht es darum, die Aufbewahrung an einen definierten Zweck zu koppeln und nur so lange andauern zu lassen, wie es von der Organisation und vom Gesetz verlangt wird. Nach Ablauf dieser Frist sollten PII vernichtet werden. Ein Beispiel dafür ist die Sperrung von Aufzeichnungen, wenn die Verarbeitung von Daten nicht mehr erforderlich ist, geltende Gesetze jedoch die Aufbewahrung zu Archivzwecken verlangen. In diesem Fall muss die Aufzeichnung gesperrt werden, was bedeutet, dass sie außerhalb des gesetzlich vorgeschriebenen Zugriffs auf sie nicht mehr verwendet werden kann.



### BEISPIEL

Der Zweck der Aufbewahrung von Lohn- und Gehaltsabrechnungsdaten ist auf die Zeit beschränkt, die eine Person bei einer Organisation beschäftigt ist. Geltende (z. B. Sozialversicherungs- oder Arbeits-)Gesetze oder Steuervorschriften können es allerdings erforderlich machen, die Daten für mehrere Jahre zu archivieren. Die Aufzeichnungen müssen nach dem Ausscheiden der Person aus dem Unternehmen gesperrt und später vernichtet werden, wenn die durch die anderen Gesetze festgelegten Aufbewahrungsfristen überschritten sind, z. B. nach sechs oder zehn Jahren.

## Sachliche Richtigkeit

Der verarbeitende Prozess muss genau und soweit abgeschlossen sein, dass er für den definierten Zweck angemessen genutzt werden kann. Wenn PII von einer anderen Quelle als dem Betroffenen selbst erhoben werden, muss die Zuverlässigkeit der Daten gewährleistet sein. Richtigkeit und Qualität der Daten sollten regelmäßig überprüft werden.



### BEISPIEL

Ein Kreditwürdigkeitsprüfungssystem stützt sich auf genaue Daten aus der Kredithistorie einer Person. Wenn diese nicht korrekt ist, also beispielsweise ein zurückgezahlter Kredit als ausgefallen erfasst wird, kann der Person ein Kredit verweigert werden, auf den sie eigentlich Anspruch gehabt hätte. Sowohl die Einzelperson als auch das Kreditinstitut würden durch diese Ungenauigkeit der Daten geschädigt.

## Transparenz der Datenverarbeitung

Dieses Prinzip bedeutet, dass Informationen über die Verarbeitung von PII, die Zwecke und die dafür verwendeten Mittel den Betroffenen zur Verfügung gestellt werden sollten. Im Sinne der Transparenz sollte dieser Hinweis leicht lesbar sein, insbesondere wenn eine Verarbeitungstätigkeit die Entscheidungsfindung auf Grundlage der verarbeiteten PII beinhaltet.



### BEISPIEL

Wenn eine Person eine Internet-Suchmaschine benutzt, werden die Daten der Person verarbeitet. Der Anbieter der Suchmaschine veröffentlicht einen Datenschutzhinweis, der erklärt, welche Daten verarbeitet werden und wie. Dieser Hinweis enthält Informationen, die die Suchergebnisse beeinflussen, sowie Anzeigen, die für die Person veröffentlicht werden.

## Betroffenenrechte

Der Betroffene hat u. a. das Recht, auf seine Daten zuzugreifen, sie zu ändern, wenn sie ungenau sind, sie unter bestimmten Bedingungen löschen oder sperren zu lassen und diese Rechte auf einfache Weise geltend zu machen. In einigen Gesetzgebungen (z. B. DSGVO und CCPA) haben Betroffene zudem das Recht auf Portabilität, nach dem ihnen die Daten in einer elektronischen, standardisierten Form zur Verfügung gestellt werden. Häufig werden dazu CSV-, JSON- oder XML-Formate verwendet.



### BEISPIEL

Einzelnen können einen Online-Shop bitten, ihnen ihre Daten zur Verfügung zu stellen. Wenn sie sich entscheiden, nicht mehr von Newslettern angeprochen zu werden, können sie ihren Datensatz sperren lassen. Eine Löschung kann erfolgen, sobald andere Gesetze eine Archivierung der Datensätze nicht mehr verlangen.

## Rechenschaftspflicht

Es besteht eine Sorgfaltspflicht, die besagt, dass eine Organisation Maßnahmen zum Schutz von PII ergriffen muss. Rechenschaftspflicht bedeutet, dass eine Organisation in der Lage sein muss, die Einhaltung der Regeln nachzuweisen. Dazu müssen Datenschutzrichtlinien und -prozesse dokumentiert werden. Vertragliche Vereinbarungen bieten Schutzmaßnahmen bei der Übertragung von Daten an Dritte. Wenn ein Verstoß auftritt, müssen die Personen darüber informiert werden. Wenn Datenschutzbehörden existieren, haben sie bestimmte Prüfungsrechte sowie das Recht, über die Verarbeitung von PII informiert zu werden.



### BEISPIEL

In Israel schreibt das Gesetz zum Schutz der Privatsphäre vor, dass eine Organisation jede Datenbank, in der sie Daten von mehr als 10.000 Personen verarbeitet, bei einer entsprechenden Behörde registrieren lassen muss. Diese Registrie-

nung umfasst eine Dokumentation über die Art der Datenbank, die Verarbeitung der Daten und die zum Schutz der Datenbank getroffenen Sicherheitsmaßnahmen.

## Informationssicherheit

PII müssen geschützt und ihre CIA (Vertraulichkeit, Integrität und Verfügbarkeit) muss vom Verantwortlichen sichergestellt werden. Die getroffenen Vorkehrungen basieren i. d. R. auf einer Risikobeurteilung sowie einem Katalog, in dem die dazu notwendigen Schritte detailliert aufgeführt sind. Dazu gehören Zugangskontrollen nach dem Grundsatz „Need to know“, die Verschlüsselung von Daten, relevante physische und Netzwerk- sowie andere Sicherheitsmaßnahmen.



### BEISPIEL

Eine Datenbank, die PII enthält, sollte verschlüsselt werden, die Passwörter der Benutzerkonten sollten zum Schutz von Vertraulichkeit und Integrität **gehasht und salted** werden.

#### Hashing und Salting

Das Hashing transformiert einen Input in einen Output und ist nicht umkehrbar. Salting fügt einen weiteren Wert hinzu, bevor gehasht wird, damit Tabellen mit gehaschten Passwörtern nicht mehr anwendbar sind.

## Einhaltung des Datenschutzes

Eine Organisation muss in der Lage sein, die Einhaltung der Vorschriften nachzuweisen, indem sie ihre internen Kontrollen unabhängig überprüfen lässt. Ein angemessenes und dokumentiertes Risikomanagementsystem ist eine Möglichkeit, die Einhaltung des Datenschutzes nachzuweisen.



### BEISPIEL

Interne und externe Auditprogramme, einschließlich der Zertifizierung durch akkreditierte Zertifizierungsstellen, sind Möglichkeiten, die Konformität nachzuweisen.

## 2.2 Datenschutz in Europa: die DSGVO

Die wichtigste internationale Organisation innerhalb Europas ist die Europäische Union (EU). Die Allgemeine Datenschutz-Grundverordnung 616/679 (DSGVO) gilt unmittelbar in allen EU-Mitgliedsstaaten und den Staaten des Europäischen Wirtschaftsraums. Sie wird begleitet von der Datenschutzrichtlinie für elektronische Kommunikation (ePD) 2002/58/EG, die durch eine aktualisierte Verordnung ersetzt werden soll. (Beachten Sie,

dass der Gesetzgebungsprozess für diese Richtlinie mehrmals verschoben wurde und Vorschläge abgelehnt wurden.) Die DSGVO ersetzt die frühere Datenschutzrichtlinie 95/46/EG. Als Verordnung ist die DSGVO in den Mitgliedsstaaten unmittelbar anwendbar und bedarf zu ihrer Wirksamkeit keiner lokalen Gesetzgebung. Die Mitgliedsstaaten haben allerdings lokale Datenschutzgesetze zur Unterstützung der DSGVO umgesetzt. Darüber hinaus sind verschiedene andere nationale Regelungen anwendbar, darunter Landes-, Kirchen- und Arbeitsgesetze sowie vertragliche Vereinbarungen, z. B. zwischen Gewerkschaften und Arbeitgeberorganisationen.

Die DSGVO ist weltweit als Maßstab für die Regulierung des Datenschutzes anerkannt. Geplante Regelungen in mehreren Ländern, darunter den USA, Indien, Brasilien und Nigeria, basieren auf den gleichen Prinzipien und sind sogar ähnlich strukturiert.

Die DSGVO besteht aus 99 Artikeln in elf Kapiteln. 173 Erwägungsgründe helfen bei der Auslegung des Gesetzes.

## Geltungsbereich der DSGVO

Der sachliche Anwendungsbereich der DSGVO umfasst alle persönlichen und materiellen Eigenschaften einer identifizierten oder identifizierbaren natürlichen Person. PII müssen entweder automatisiert, halbautomatisiert oder als papierbasiertes Archiv verarbeitet werden. Es gibt nur wenige Ausnahmen vom sachlichen Geltungsbereich der DSGVO, darunter private Haushalte, Strafverfolgungsaktivitäten und die Datennutzung für die nationale Sicherheit. Die DSGVO gilt sowohl für die Verarbeitung Verantwortlichen als auch für die Verarbeiter.

Der territoriale Geltungsbereich folgt dem Marktprinzip. Er gilt für alle in der EU niedergelassenen Organisationen, aber auch für solche, die innerhalb der EU Dienstleistungen oder Produkte anbieten oder die EU-Bürger überwachen. Da die EU der größte Binnenmarkt der Welt ist, gilt die DSGVO daher auch für viele Organisationen, die außerhalb der EU tätig sind.

## Besondere Datenkategorien

Artikel 9, Absatz 1 der DSGVO definiert besondere **Datenkategorien**. Die Verarbeitung dieser ist nur zulässig, wenn ein besonderes gesetzliches Erfordernis besteht oder der Betroffene eingewilligt hat. Diese Kategorien sind die folgenden:

- „rassistische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen [...],
- Gewerkschaftszugehörigkeit [...],
- sowie die Verarbeitung von genetischen Daten,
- biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person,
- Gesundheitsdaten oder
- Daten zum Sexualleben oder der sexuellen Orientierung“ (EU 2018).

**Kategorien von Daten**  
Beachten Sie, dass sensible Informationen manchmal indirekt in den Daten enthalten sind, z. B. könnte eine Personalabteilung, die den Namen des Partners einer Person verlangt, deren sexuelle Orientierung offenbaren.

Wenn besondere Datenkategorien verarbeitet werden, muss die Sicherheit der Verarbeitung dem hohen Risiko dieser Daten Rechnung tragen.

### **Rechenschaftspflicht in DSGVO**

Um die Verantwortlichkeit nachzuweisen, verlangt die DSGVO von den Organisationen die Führung eines Verzeichnisses der Verarbeitungsaktivitäten. Artikel 30 der DSGVO (EU 2018) beschreibt, was eine Aufzeichnung von Verarbeitungsaktivitäten enthalten muss. Die Behörden können Einsicht in das Verzeichnis der Verarbeitungstätigkeiten verlangen, wenn sie Organisationen prüfen. Diese müssen ebenfalls Sicherheitsvorkehrungen treffen, welche die CIA-Triade sowie die Belastbarkeit als vierten Sicherheitsfaktor einschließen. Während der Implementierung muss das Sicherheitsrisiko berücksichtigt werden. Artikel 25 der DSGVO besagt, dass die Risikobeurteilung durchzuführen ist unter Berücksichtigung ...

- ... „des Stands der Technik,
- der Implementierungskosten und
- der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie
- der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der [...] Risiken für die Rechte und Freiheiten natürlicher Personen“ (ebd.).

Im Falle einer geplanten Aktivität, die ein hohes Risiko für die Rechte und die Freiheit einer Person darstellt, muss eine Datenschutzfolgenabschätzung durchgeführt werden (ebd.). Nationale Behörden und der Europäische Datenschutzrat (European Data Protection Board – EDPB) stellen klar, dass einige Aktivitäten immer eine Datenschutzfolgenabschätzung erfordern. Beispiele dafür sind die Videoüberwachung oder die Kreditwürdigkeitsprüfung.

Die Prinzipien „Privacy by design“ und „Privacy by default“, die eine Organisation befolgen muss, bedeuten, dass der Datenschutz nicht erst nachträglich implementiert, sondern bereits in der Entwurfsphase von Prozessen und Applikationen umgesetzt werden muss. „Privacy by default“ meint, dass datenschutzfreundliche Einstellungen die Standardoption sein müssen. Ein Beispiel dafür sind die Einstellungen von Cookies, die nur dann voreingestellt sein sollten, wenn sie für das Funktionieren einer Website wesentlich sind, während alle anderen Arten von Cookies standardmäßig abgewählt sein müssen.

### **Rechtmäßigkeit der Verarbeitung**

Gemäß Artikel 6 der DSGVO gibt es genau sechs Gründe, die die Verarbeitung von PII rechtmäßig machen. Sie lauten wie folgt:

- „Die betroffene Person hat ihre Einwilligung [...] gegeben;
- die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
- die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung notwendig, der der Verantwortliche unterliegt;

- die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich [...]“ (EU 2018).

Es ist wichtig, die rechtliche Grundlage der Verarbeitung von PII zu verstehen. Eine Zustimmung wird jedoch oft als eine weitere Rechtsgrundlage missbraucht, obwohl sie freiwillig gegeben werden muss und jederzeit zurückgezogen werden kann. Die Rechtsgrundlage für lebenswichtige Interessen wird so ausgelegt, dass sie für Notfallsituationen gilt. Jedoch fällt nicht jede gesundheitsbezogene Tätigkeit unter diese Rechtsgrundlage.

## **Einhaltung des Datenschutzes**

Die Einhaltung der DSGVO wird sowohl vom Verantwortlichen selbst kontrolliert als auch von Aufsichtsbehörden überwacht. Eine entscheidende Rolle bei der Kontrolle der Einhaltung kommt den Datenschutzbeauftragten (DSB) zu. Sie arbeiten direkt bei den Organisationen in einem externen Auftragsverhältnis und überwachen/prüfen die Einhaltung der DSGVO. Sie beraten bei der Umsetzung und bearbeiten auch die Beschwerden der Betroffenen. Um sicherzustellen, dass sie unabhängig handeln können, darf ein DSB keine direkten Anweisungen erhalten. Er muss allerdings der höchsten Führungsebene in einer Organisation Bericht erstatten.

Die externe Kontrolle wird über die Aufsichtsbehörden sichergestellt. Die einzelnen EU-Mitgliedsstaaten haben diese Behörden entweder auf Landes- oder nationaler Ebene eingerichtet. Sie arbeiten über den Europäischen Datenschutzrat zusammen, der früher als Artikel-29-Gruppe bekannt war. Sie können Informationen einholen, Organisationen prüfen, Beschwerden bearbeiten und das Abstellen von ermittelten Datenschutzverstößen anweisen. Auch können sie Geldstrafen für die Nichteinhaltung von Vorschriften aussprechen. Diese sollten wirksam, verhältnismäßig und abschreckend sein. Die Bußgelder sind auf maximal vier Prozent der weltweiten Einnahmen einer Organisation oder 20 Millionen Euro begrenzt.

Artikel 42 der DSGVO (EU 2018) erleichtert eine Zertifizierung, die eine Einhaltung der Bestimmungen nachweisen könnte. Bei Redaktionsschluss dieses Studienskriptes (2020) lag allerdings noch kein genehmigtes Zertifizierungsprogramm vor. Beachten Sie, dass eine Zertifizierung nach ISO 27001 in Verbindung mit ISO 27701 keine Zertifizierung nach Artikel 42 der DSGVO sein wird.

## **Rechte der Betroffenen**

In Kapitel III DSGVO (EU 2018) werden die Rechte der betroffenen Person festgehalten. Diese sind:

- Transparenz über die Verarbeitung von Daten und die Rechte des Einzelnen,
- Informationspflicht und Recht auf Auskunft zu persönlichen Daten,

- Berichtigung und Löschung (Recht auf Vergessen) sowie
- Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall.

Im Schadensfall können die betroffenen Personen eine Organisation haftbar machen. Die Haftung ist unbeschränkt und richtet sich nach dem verursachten Schaden, z. B. durch eine Datenverletzung.

### **Datenübertragungen – Auftragsdatenverarbeitung**

Datenübertragungen zwischen für die Verarbeitung Verantwortlichen und Auftragsverarbeitern sowie zwischen verschiedenen für die Verarbeitung Verantwortlichen erfordern einen schriftlichen Vertrag, eine Vereinbarung über die Datenverarbeitung (Data Processing Agreement, DPA). Für die Auftragsdatenverarbeitung schreibt Artikel 28 DSGVO vor (EU 2018):

- Der Verarbeiter erklärt sich damit einverstanden, personenbezogene Daten nur dann zu verarbeiten, wenn er schriftliche Anweisungen des für die Verarbeitung Verantwortlichen erhalten hat.
- Jeder, der mit den Daten in Berührung kommt, ist zur Vertraulichkeit verpflichtet.
- Zum Schutz der Datensicherheit werden alle geeigneten technischen und organisatorischen Maßnahmen (TOMs) eingesetzt.
- Der Auftragsverarbeiter wird keinen Unterauftrag an einen anderen Auftragsverarbeiter vergeben, es sei denn, der für die Verarbeitung Verantwortliche weist ihn schriftlich dazu an; in diesem Fall muss eine andere DSV mit dem Unterauftragsverarbeiter unterzeichnet werden (gem. Artikel 28 Absätze 2 und 4).
- Der Auftragsverarbeiter unterstützt den für die Verarbeitung Verantwortlichen bei der Einhaltung seiner Verpflichtungen nach der DSGVO, insbesondere in Bezug auf die Rechte der betroffenen Personen.
- Der Auftragsverarbeiter hilft dem für die Verarbeitung Verantwortlichen, die Einhaltung der DSGVO in Bezug auf Artikel 32 (Sicherheit der Verarbeitung) und Artikel 36 (Beratung mit der Datenschutzbehörde vor der Durchführung einer Verarbeitung mit hohem Risiko) zu gewährleisten.
- Der Auftragsverarbeiter erklärt sich bereit, alle personenbezogenen Daten nach Beendigung der Dienste zu löschen oder die Daten an den für die Verarbeitung Verantwortlichen zurückzugeben.
- Der Auftragsverarbeiter muss dem für die Verarbeitung Verantwortlichen die Durchführung eines Audits gestatten und wird alle Informationen zur Verfügung stellen, die zum Nachweis der Einhaltung der Vorschriften erforderlich sind.

Ein Datentransfer kann auch zu Parteien außerhalb der Europäischen Union stattfinden. In diesem Fall müssen spezifische zusätzliche Schutzvorkehrungen getroffen werden. Die gebräuchlichsten Schutzmaßnahmen sind folgende:

- **Angemessenheitsentscheidungen:** Die EU-Kommission entscheidet, dass das Datenschutzniveau in einem Drittland auf einem für die EU akzeptablen Niveau liegt. Gegenwärtig gehören Argentinien, Japan und Kanada (Privatsektor) zu den großen Volkswirt-

schaften, die eine Angemessenheitsentscheidung erhalten haben. Die USA verfügen hingegen über keinen gültigen Angemessenheitsstatus mehr, seit der EUGH den bisher gültigen EU-US Privacy Shield für ungültig erklärt hat.

- **EU-Standardvertragsklauseln:** Die EU hat Muster- oder Standardvertragsklauseln herausgegeben. Unterzeichnet und befolgt ein Auftragsverarbeiter oder für die Verarbeitung Verantwortlicher außerhalb der EU diese, dürfen die Daten an ihn übermittelt werden. Dies ist die gebräuchlichste Art der Sicherung von Datenübermittlungen in Drittländer.
- **verbindliche interne Datenschutzvorschriften:** Ein Unternehmen kann die verbindlichen Datenschutzvorschriftenhalten der nationalen Behörden des Landes befolgen, in dem sich sein EU-Hauptsitz befindet. Wenn diese genehmigt werden, können Daten innerhalb dieses Unternehmens fließen. Verbindliche Datenschutzvorschriften haben keine Auswirkungen auf Beziehungen außerhalb dieses Unternehmens.

## Datenpannen

Wann immer eine Datenpanne (also eine Verletzung des Schutzes von PII) auftritt, hat die Organisation ab dem Zeitpunkt der Entdeckung 72 Stunden Zeit, um die Datenschutzaufsichtsbehörden darüber zu informieren. Wenn die Risiken für die Rechte und Freiheiten der betroffenen Personen hoch sind, müssen auch diese betroffenen Personen über die Verletzung informiert werden.

## 2.3 Datenschutz in den USA

Zum Zeitpunkt der Verfassung dieses Textes machen die Datenschutzgesetze in den USA einen erheblichen Wandel durch. Mindestens 17 Bundesstaaten führen derzeit Gesetzgebungsverfahren zur Verabschiedung neuer Datenschutzgesetze durch, wobei Kalifornien mit dem Californian Consumer Privacy Act (CCPA) eine Vorreiterrolle einnimmt. Sowohl die Republikanische als auch die Demokratische Partei haben neue Datenschutzgesetze auf Bundesebene vorgeschlagen; beide Vorschläge beziehen sich auf die europäische DSGVO und orientieren sich an ähnlichen Prinzipien. Die derzeitige Gesetzgebung ist größtenteils vom jeweiligen Bundesstaat abhängig und ergibt sich aus den Verbraucherrechten. Auch spielen sektorspezifische Gesetze eine große Rolle, wie der Health Insurance Portability and Accountability Act (HIPAA) für den Gesundheits- oder der Fair Credit Reporting Act (FCRA) für den Bankensektor.

Die Federal Trade Commission (FTC), eine wichtige Bundesbehörde, setzt sich seit den 1970er-Jahren für den Schutz der Privatsphäre von Verbrauchern in den USA ein. Zwar hat sie nicht die gleiche Bedeutung wie die Datenschutzbehörden in anderen Ländern, jedoch versuchen die vorgeschlagenen Gesetze auf Bundesebene, die Aufsichtsfunktion in die FTC zu verlagern, wodurch die Rolle betont wird, die sie in den Vereinigten Staaten bezüglich der Privatsphäre spielt.

In diesem Lernzyklus werden wir uns auf die Rolle der FTC, des CCPA und des HIPAA als Beispiele für US-amerikanische Datenschutzvorschriften konzentrieren. Wenngleich es in Ermangelung eines Bundesgesetzes nicht möglich ist, einen vollständigen und ganzheitlichen Überblick zu geben, ermöglicht es, diese Auswahl doch zu verstehen, was Datenschutz in den Vereinigten Staaten derzeit bedeutet.

## Die Rolle der FTC

Wenn Unternehmen den Verbrauchern mitteilen, dass sie ihre persönlichen Daten schützen werden, kann die FTC Maßnahmen ergreifen um sicherzustellen, dass diese Versprechen auch eingehalten werden. Sie hat rechtliche Schritte gegen Organisationen eingeleitet, die die Persönlichkeitsrechte der Verbraucher verletzt oder sie irregeführt haben, indem sie es versäumten, die Sicherheit sensibler Verbraucherinformationen aufrechtzuhalten, oder den Verbrauchern erheblichen Schaden zugefügt haben. In vielen dieser Fälle hat die FTC die Beklagten beschuldigt, gegen Abschnitt 5 des FTC-Gesetzes (FTC Act) verstoßen zu haben, der unlautere und irreführende Handlungen und Praktiken im oder mit Einfluss auf den Handel verbietet. Neben dem FTC Act setzt die Behörde auch andere Bundesgesetze durch, die sich auf Privatsphäre und Sicherheit der Verbraucher beziehen (FTC o. J.).

Daher spielt die FTC eine Rolle beim Schutz der Privatsphäre der Verbraucher. Ein Beispiel ist die Causa YouTube (FTC Nr. 172 3083) (FTC 2019), in welcher die FTC eine Geldstrafe von 170 Millionen Dollar verhängte, da die Website Informationen von Minderjährigen ohne vorherige Zustimmung der Eltern sammelte.

## Kalifornisches Gesetz zum Schutz der Privatsphäre von Verbrauchern

Am 1. Januar 2020 trat in Kalifornien das Gesetz zum Schutz der Privatsphäre von Verbrauchern (englisch: Californian Consumer Privacy Act; CCPA) in Kraft, mit dem die Modernisierung der Datenschutzgesetze der Vereinigten Staaten eingeleitet wurde. Der Titel des CCPA ist ein wenig irreführend, denn er schützt nicht nur die Verbraucher, sondern alle in Kalifornien ansässigen Personen, ihre Geräte und die kalifornischen Haushalte. Der Staat Kalifornien repräsentiert etwa zwölf Prozent der Bevölkerung der Vereinigten Staaten und wäre als unabhängiger Staat die siebtgrößte Volkswirtschaft der Welt. Daher hat der CCPA nationale und internationale Auswirkungen.

Um in den Geltungsbereich des CCPA zu fallen, muss eine Organisation mindestens eines der folgenden Kriterien erfüllen (Bryan Cave Leighton Paisner 2019):

1. hat einen jährlichen Bruttoumsatz von 25 Millionen Dollar;
2. kauft, erhält, verkauft oder teilt die persönlichen Daten von 50.000 oder mehr Verbrauchern, Haushalten oder Geräten;
3. erzielt mindestens 50 % ihres Jahresumsatzes durch den Verkauf persönlicher Daten von Verbrauchern.

Die Betroffenen gelten gemäß CCPA als Verbraucher und haben die folgenden Rechte (ebd.):

1. Transparenz darüber, welche PII über sie gesammelt werden;
2. Zugriff auf ihre PII in einem leicht nutzbaren Format;
3. Transparenz darüber, ob ihre persönlichen Daten verkauft oder weitergegeben werden, und wenn ja, an wen;
4. Opt-out des Verkaufs ihrer PII (Opt-in, im Falle von Minderjährigen);
5. gleicher Service und Preis unabhängig von der Ausübung individueller Rechte;
6. Recht auf Löschung.

Die von Konsumenten anforderbaren Daten sind auf die letzten zwölf Monate beschränkt. Einzelpersonen können innerhalb eines Zeitraums von zwölf Monaten bis zu zwei Anträge stellen. Eine Organisation muss eine gebührenfreie Telefonnummer und eine E-Mail-Adresse oder ein Webformular einrichten, über welche die Verbraucher beantragen können, eines dieser Rechte in Anspruch zu nehmen.

Das Gesetz verwendet den Begriff „persönliche Informationen“ („personal information“) im weitesten Sinne, sodass darunter sowohl traditionelle Informationen als auch verhaltens- oder präferenzbasierte Informationen fallen. Außerdem definiert der CCPA den Begriff „Verkauf“ („selling“) in einem weiten Sinne und es werden weitere Klarstellungen erwartet: Er schließt Verkauf, Vermietung, Freigabe, Offenlegung, Verbreitung, Verfügbar machen, Übertragung oder die anderweitige Weitergabe von PII an ein anderes Unternehmen oder eine Drittpartei gegen eine finanzielle oder sonstig entgeltliche Gegenleistung mit ein. Verkauft ein Unternehmen Daten, muss es einen Link auf seiner Webseite platzieren, über den sich Einzelpersonen gegen den Verkauf ihrer Daten entscheiden können. Die Standardoption kann für Erwachsene aktiviert werden, für Minderjährige hingegen ist die Standardoption Opt-out.

Der CCPA wendet den Begriff „Dienstleister“ („service providers“) auf für die Verarbeitung Verantwortliche und „Dritte“ („third parties“) auf Verarbeiter an.

Um das Gesetz durchzusetzen, kann der kalifornische Generalstaatsanwalt Geldstrafen von bis zu 7.500 US-Dollar pro Verstoß verhängen. Allerdings ist noch nicht klar, wie die Verstöße gezählt werden. Wenn sie aus einem Versäumnis resultieren, eine angemessene Sicherheit aufrechtzuerhalten, ist das private Klagerecht auf 750 Dollar begrenzt; diese werden normalerweise im Rahmen einer Sammelklage durchgesetzt. Zu bedenken ist, dass der private Schadenersatz pro Datensatz erfolgt. Werden also 100.000 Datensätze verletzt und nehmen alle betroffenen Verbraucher an der Sammelklage teil, könnte die Haftung bis zu 75 Millionen Dollar betragen.

Mehrere Änderungen wurden erlassen, um den Geltungsbereich des CCPA zu klären oder ein Moratorium darauf zu verhängen. Wichtige Änderungen sind die Assembly Bill 25 (AB-25), die Arbeitnehmerdaten für ein Jahr vom Anwendungsbereich ausnimmt, und die AB-1355 für ein Moratorium auf B2B-bezogene PII. Die CCPA verlangt allerdings nicht, dass eine Organisation über einen Datenschutzbeauftragten verfügen müsste.

## **Health Insurance Portability and Accountability Act**

Aufgrund seines sensiblen Charakters wurde 1996 ein Bundesgesetz über den Schutz der Privatsphäre im Gesundheitswesen erlassen. Dabei handelt es sich um den Health Insurance Portability and Accountability Act, kurz HIPAA. Dieser wurde regelmäßig aktualisiert, um mit dem technologischen Fortschritt und Änderungen des Anwendungsbereichs Schritt zu halten.

Die Betroffenen werden im HIPAA als „Patienten“ („patients“) bezeichnet, und das Gesetz schützt ihre Daten in jeder Form, etwa in Gesundheitsplänen, in Clearing-Stellen für das Gesundheitswesen und bei Gesundheitsdienstleistern, einschließlich Ärzten, Krankenschwestern, Krankenhäusern und Therapeuten. Patienteninformationen in mündlicher, schriftlicher oder elektronischer Form sind geschützt. Dazu gehören demografische Informationen, die an die Identität des Patienten gebunden sind. Die Patienten haben das Recht auf Zugang zu ihren Daten und Organisationen können für deren Bereitstellung eine angemessene Gebühr verlangen.

Die Datenschutzbestimmungen des HIPAA stellen sicher, dass die Richtlinien in einer Weise angewendet werden, die einen angemessenen Datenschutz gewährleistet und keinen Raum für Fehler lässt. Sie legen für Organisationen der medizinischen Versorgung klare Regeln dazu fest, wie Patientendaten verarbeitet werden müssen. Für die Weitergabe von Patientendaten ist eine schriftliche Genehmigung erforderlich.

Das HIPAA erfordert administrative, physische sowie technische Kontrollen, Richtlinien und Verfahren, um die CIA von elektronischen persönlichen Gesundheitsinformationen (engl. „electronic personal health information“; ePHI) zu gewährleisten. Beispiele für erforderliche administrative Maßnahmen sind die Implementierung eines Risikomanagements oder eines Datensicherungsplans; Beispiele für erforderliche physische Sicherheitsvorkehrungen sind u. a. Gebäude Sicherheit und die sichere Entsorgung von Medien. Beispiele für technische Sicherheitsvorkehrungen sind Authentifizierungs- oder Notfallzugriffsverfahren.

Bei Nichteinhaltung des HIPAA werden Strafen verhängt. Für den Diebstahl eines Laptops mit unverschlüsselten Patientendaten in einem Hospiz im Norden des Bundesstaates Idaho wurde eine Strafe von 50.000 US-Dollar fällig. Insgesamt summierten sich die Strafen bisher auf mehr als 36 Millionen Dollar. Allerdings sind die Bußgelder auf 1,5 Millionen Dollar pro Jahr und Einrichtung begrenzt. Sie werden vom Büro für Bürgerrechte (Office for Civil Rights – OCR) des Gesundheitsministeriums und den Generalstaatsanwälten durchgesetzt.

Die US-amerikanische Food & Drug Administration (FDA) prüft medizinische Geräte, bevor sie auf den Markt kommen, und auch dabei wird der Datenschutz berücksichtigt (FDA 2018).

## 2.4 Datenschutz in Asien

In Asien gibt es kein führendes Datenschutzgesetz. Jedes Land in Asien hat seine eigenen Datenschutzbestimmungen und die größte Handelsorganisation in Asien, **ASEAN (Association of Southeast Asian Nations)**, verfügt über keine eigenen Datenschutzbestimmungen. In diesem Lernzyklus werden wir die Situation in Indien und Singapur untersuchen und uns somit auf zwei wichtige Volkswirtschaften in der Region konzentrieren.

**ASEAN**  
Diese Organisation umfasst zehn asiatische Länder und fördert viele verschiedene Arten der Integration unter ihren Mitgliedern.

### Datenschutz in Indien

Derzeit kennt Indien ein verfassungsmäßiges Recht auf Privatsphäre, aber kein Datenschutzgesetz. Ein solches existiert nur für die Rechtsprechung und folgt keiner prägnanten Struktur wie in den zuvor beschriebenen Gesetzgebungen. Im Jahr 2018 wurde ein Gesetz zum Schutz personenbezogener Daten vorgeschlagen, das sich weiterhin im Gesetzgebungsverfahren befindet; mehrere Änderungen und Ergänzungen wurden diskutiert. Bis zur Verabschiedung des Gesetzes bleibt die Regulierung des Datenschutzes in Indien ein schwieriges Thema.

Das bestehende Informationstechnologiegesetz („Information Technology Act“; Parliament of India 2000) enthält zwei Abschnitte zum Datenschutz. Abschnitt 43A verlangt von einer Organisation, angemessene Sicherheitspraktiken für sensible persönliche Daten zu implementieren und eine Person zu entschädigen, wenn ein Verstoß erfolgt; als sensible persönliche Daten gelten hierbei Passwörter, Gesundheitsdaten, die sexuelle Orientierung, biometrische Daten und Finanzinformationen. Abschnitt 72A definiert Geldstrafen von umgerechnet bis zu ca. 6.800 US-Dollar und/oder Freiheitsstrafen von bis zu drei Jahren für die Verursacher von Datenverstößen.

Andererseits verleiht dasselbe Gesetz der indischen Regierung viel Macht, um in die Daten ihrer Bürger einzugehen. Es erlaubt das Abfangen, Überwachen und Entschlüsseln von digitaler Kommunikation und gestattet der Regierung, nationale Verschlüsselungsstandards festzulegen. So existieren Regierungsprojekte, die Telefone und das Internet abhören. Das Indian National Intelligence Grid Project (NATGRID) ist ein Beispiel dafür, wie verschiedene Datenbanken mit Bürgerdaten kombiniert und den Geheimdiensten leicht zugänglich gemacht werden.

Die nun vorgeschlagenen Datenschutzgesetze würden die Privatsphäre zu einem grundlegenden Recht machen und die Bürger besser vor staatlicher Überwachung schützen.

### Datenschutz in Singapur

In Singapur wird Datenschutz seit 2012 durch das Personal Data Protection Act (PDPA) geregelt. Im Jahr 2013 wurden mehrere Verordnungen hinzugefügt, um die Durchsetzung des Gesetzes zu regeln, das spezielle Bestimmungen zu Telefongesprächen sowie Ausnahmen enthält, wodurch ein umfassender Rahmen für den Datenschutz in Singapur geschaffen wurde (PDPC o. J.).

Der PDPA legt ein Datenschutzgesetz mit verschiedenen Regeln für die Sammlung, Verwendung, Offenlegung und Pflege von persönlichen Daten fest. Es erkennt sowohl die Rechte von Einzelpersonen zum Schutz ihrer persönlichen Daten, inklusive eines Rechtes auf Zugang und Korrektur, als auch die Bedürfnisse von Organisationen an, persönliche Daten für legitime und angemessene Zwecke zu sammeln, zu verwenden oder offenzulegen.

Der PDPA sieht die Einrichtung eines nationalen DNC-Registers („Do Not Call“) vor. Dieses ermöglicht es Einzelpersonen, ihre Telefonnummern zu registrieren, um Werbeanrufen, -textnachrichten (wie SMS oder MMS) und -faxen von Organisationen im Vorhinein zu widersprechen.

Der Geltungsbereich des PDPA umfasst alle personenbezogenen Daten, mit den folgenden vier Ausnahmen (PDPC o. J.):

1. jeder Person, die auf persönlicher oder häuslicher Basis handelt;
2. jedem Mitarbeiter, der im Rahmen seiner Beschäftigung bei einer Organisation handelt;
3. jeder öffentlichen Einrichtung oder Organisation, die hinsichtlich Sammlung, Verwendung oder Weitergabe der persönlichen Daten im Namen einer öffentlichen Einrichtung handelt;
4. geschäftlichen Kontaktinformationen.

Das Gesetz etabliert die Kommission für den Schutz personenbezogener Daten (Personal Data Protection Commission; PDPC), eine Behörde für den Schutz der Privatsphäre, die für die Verwaltung des Gesetzes zuständig ist. Die Kommission berät nicht nur, sondern setzt das Gesetz auch durch und überwacht seine Einhaltung.

Im Allgemeinen bedarf die Handlung der Zustimmung. Das Gesetz definiert eine lange Liste von Aktivitäten, für die keine Zustimmung erforderlich ist. Diese sind in der zweiten Liste des Gesetzes festgelegt und umfasst Dinge wie das Interesse des Einzelnen, künstlerische Zwecke und mehr.

Das Gesetz gibt Einzelpersonen das Recht auf Zugang und Korrektur ihrer Daten hinsichtlich Genauigkeit, Schutz und angemessener Aufbewahrung. Im Falle von Streitigkeiten hilft die Kommission der Person und dem für die Verarbeitung Verantwortlichen, ein Schlichtungsverfahren zur Lösung des Konflikts durchzuführen.

Mögliche Strafen für die Nichteinhaltung reichen von Geldstrafen bis hin zu drei Jahren Haft. Viele Geldstrafen bewegen sich bisher in der Größenordnung zwischen 5.000 bis 100.000 Singapur-Dollar (umgerechnet ca. 3.000 bzw. 60.000 Euro).

Der PDPA schreibt vor, dass eine Organisation einen Datenschutzbeauftragten (DSB) haben muss. Der DSB hat die folgenden Verpflichtungen (PDPC o. J.):

- Gewährleistung der Einhaltung des PDPA bei der Entwicklung und Umsetzung von Richtlinien und Verfahren zum Umgang mit personenbezogenen Daten,

- Förderung einer Datenschutzkultur unter den Mitarbeitern sowie Vermittlung der Richtlinien zum Schutz personenbezogener Daten an die Interessenvertreter,
- Verwaltung von Fragen und Beschwerden im Zusammenhang mit dem Schutz personenbezogener Daten,
- Alarmierung des Managements über alle Risiken, die hinsichtlich personenbezogener Daten entstehen könnten, und,
- falls erforderlich, Kontaktaufnahme mit der PDPC in Datenschutzfragen.

In Singapur wird derzeit das Datenschutzgesetz geändert. Im März 2019 erklärte die PDPC, dass die Benachrichtigung bei Verstößen obligatorisch werden könnte und Einzelpersonen eine größere Kontrolle über Datenübertragungen an Dritte haben sollten.



### ZUSAMMENFASSUNG

Privatsphäre und Datenschutz sind nicht dasselbe. Entsprechende Regelungen in der ganzen Welt folgen ähnlichen Prinzipien, allerdings existieren auch erhebliche Unterschiede. In Europa gibt die DSGVO klare und strenge Richtlinien vor, während die Regelungen in den USA vielfältiger sind und stark vom Bundesstaat, dem Industriesektor und dem Umfang der Verarbeitung abhängen.

In Asien ist die Situation noch vielfältiger, da jedes Land seine eigenen Datenschutzbestimmungen hat. Einige Länder, wie z. B. Indien, befinden sich noch mitten in einem Gesetzgebungsverfahren, während andere, beispielsweise Singapur, über ausgereiftere Regelungen verfügen.

Aufgrund der empfindlichen Bußgelder und des extraterritorialen Geltungsbereichs setzt die DSGVO den weltweiten Maßstab für Datenschutzbestimmungen und ist auf viele Organisationen anwendbar.

In fast allen Ländern der Welt sind Datenschutzgesetze im Entstehen oder werden derzeit modernisiert, sodass der Datenschutzrechtsbeobachter sorgfältig neue Entwicklungen im Auge behalten muss.



# LEKTION 3

## ANWENDUNG DES DATENSCHUTZES

### LERNZIELE

Nach der Bearbeitung dieser Lektion werden Sie wissen, ...

- wie Datenschutzbestimmungen in mehreren Szenarien praktisch angewendet werden können.
- was Anonymität ist und wie sie erreicht werden kann.
- worin die Herausforderungen bei der Verwendung von PII in Big-Data-Szenarien bestehen.
- wie datenschutzkonformes Online-Marketing funktionieren kann.
- welche Auswirkungen Datenschutz auf das Cloud Computing hat.

## 3. ANWENDUNG DES DATENSCHUTZES

### Einführung

In dieser Lektion werden wir Möglichkeiten zur Umsetzung von Gesetzen und Vorschriften untersuchen, die den Schutz der Privatsphäre und den Datenschutz regeln. Die Praxis zeigt, dass die Umsetzung der gesetzlichen Anforderungen nicht so einfach ist, wie es sich anhört. Jüngste Berichte über den Einfluss personenbezogener Daten auf Wahlen und die Verfügbarkeit von Standortdaten zeigen, dass die Umsetzung angemessener Kontrollen in Bezug auf den Datenschutz in einigen Bereichen versagt. Wir werden verschiedene Wege zur Verwirklichung des Datenschutzes untersuchen und sehen, worin die Herausforderungen bestehen.

### 3.1 Anonymität und Pseudonyme

Anonymität ist eine Situation, in welcher die Identität der handelnden Person unbekannt ist. In der Informationstechnologie bezieht sie sich auf Daten, bei denen es unmöglich ist, die Person zu identifizieren, deren Daten verarbeitet werden. Eine Herausforderung im Umgang mit der Anonymität besteht darin, dass es oft möglich ist, Personen neu zu identifizieren. Einige Beispiele hierfür sind ...

- ... IP-Adressen, die von Internet Service Providern (ISPs) vergeben werden, die Einzelpersonen identifizieren können,
- Standortdaten, die in vielen Fällen eine Person offenbaren können,
- eindeutige Identifikatoren wie Sozialversicherungs-, Kunden- oder Personalnummern, die einer Person zugeordnet werden können, und
- das Filtern statistischer Daten, welches häufig die Identität einer Person aufdecken kann.

Diese Herausforderungen waren Auslöser für die Forschung im Bereich der Anonymität sowie zu der Frage, wie man sie erreichen kann.

#### k-Anonymität

k-Anonymität ist ein Konzept, das zur Bewältigung des Konfliktes beitragen soll, Daten für den benötigten Zweck zu speichern und gleichzeitig die Privatsphäre der Personen zu schützen, deren Daten verarbeitet werden. Dieser Kompromiss wird dadurch erreicht, dass die Daten weniger genau sind.

Das folgende Beispiel zeigt, wie dies funktioniert. Angenommen, wir haben eine Liste von Teilnehmern an einer Umfrage zur Mitarbeiterzufriedenheit. Wir wollen den Führungskräften einerseits genügend Informationen geben, damit sie auf das Feedback reagieren kön-

nen, aber andererseits sicherstellen, dass sie nicht feststellen können, wer genau welches Feedback gegeben hat. Die anfängliche, nicht anonymisierte Feedback-Tabelle sieht dann wie folgt aus:

**Tabelle 1: Nicht anonymisierte Feedback-Tabelle**

Name	Alter	Land	Geschlecht	Rückmeldung
Susan	24	USA	weiblich	schlecht
Martin	27	Deutschland	männlich	gut
Rachel	20	Israel	weiblich	schlecht
Ramu	28	Indien	männlich	mittel
Ralf	32	USA	männlich	gut
Natalie	33	Israel	weiblich	mittel
Miriam	33	Deutschland	weiblich	gut
Sven	34	Deutschland	männlich	mittel
Aurélie	30	Belgien	weiblich	mittel
Eva-Maria	29	USA	weiblich	mittel

Quelle: Martin Macke, 2020.

Die Herausforderung bei dieser Art von Daten besteht darin, dass selbst dann, wenn der Name entfernt wird, Filter in Bezug auf Land oder Alter immer noch anzeigen könnten, wer die Rückmeldung gegeben hat. Sieht man das Alter und das Land der Personen, wäre es einfach, das Feedback von Rachel und Natalie zu identifizieren.

Daher werden zwei Methoden angewandt:

1. Unterdrückung: Attribute werden vollständig entfernt, in diesem Fall der Name und das Land.
2. Verallgemeinerung: Der Prozess des Ersetzens spezifischer Daten durch umfassendere Kategorien. Ein Beispiel dafür wird unten im Bereich Alter gezeigt.

**Tabelle 2: Zwei-Anonymitäts-Feedback-Tabelle**

Name	Alter	Land	Geschlecht	Rückmeldung
*	< 25	*	weiblich	schlecht
*	25-35	*	männlich	gut
*	< 25	*	weiblich	schlecht
*	25-35	*	männlich	mittel

Name	Alter	Land	Geschlecht	Rückmeldung
*	25-35	*	männlich	gut
*	25-35	*	weiblich	mittel
*	25-35	*	weiblich	gut
*	25-35	*	männlich	mittel
*	25-35	*	weiblich	mittel
*	25-35	*	weiblich	mittel

Quelle: Martin Macke, 2020.

Dieser Datensatz erreicht Zwei-Anonymität, da für jede Kombination von Alter und Geschlecht immer mindestens zwei Zeilen mit den gleichen Attributwerten vorhanden sind. Dies ist allerdings noch nicht ideal, denn im Beispiel kann man für die weiblichen Personen in der Altersgruppe <25 erkennen, dass beide eine schlechte Rückmeldung gegeben haben.

### *l*-Diversity

*l*-Diversity (alternative Schreibweise:  $\ell$ -Diversity) ist eine Erweiterung des  $k$ -Anonymitätsmodells und behandelt einige seiner Schwächen. Eine Datenmenge oder Tabelle erreicht *l*-Diversität, wenn sie für einen Wert  $k \geq lk$ -anonym ist und für jede Menge von Datensätzen mit der gleichen Kombination identifizierender Attribute (im Beispiel: Alter und Geschlecht) es mindestens *l* verschiedene Werte im sensiblen Attribut (im Beispiel: Rückmeldung) gibt. Auch hier handelt es sich um einen Kompromiss zwischen der Qualität der Daten, der Privatsphäre und der Möglichkeit, die Daten dennoch nutzen zu können. Eine Drei-Diversitäts-Feedback-Tabelle würde wie die in der folgenden Abbildung gezeigte aussehen.

**Tabelle 3: Drei-Diversitäts-Feedback-Tabelle**

Name	Alter	Land	Geschlecht	Rückmeldung
*	2*	*	weiblich	schlecht
*	2*	*	weiblich	mittel
*	2*	*	weiblich	schlecht
*	2*	*	männlich	gut
*	2*	*	männlich	mittel
*	2*	*	männlich	gut
*	3*	*	*	mittel
*	3*	*	*	mittel

Name	Alter	Land	Geschlecht	Rückmeldung
*	3*	*	*	gut
*	3*	*	*	mittel

Quelle: Martin Macke, 2020.

### Differenzielle Privatheit – Differential Privacy

Bei differentieller Privatheit werden Daten so geändert, dass sie statistisch weiterhin verwendet werden können, die Privatsphäre des Einzelnen jedoch gewahrt bleibt. Ein gängiges Beispiel ist die Befragung von Einzelpersonen, wenn sie ein bestimmtes Merkmal besitzen. Jeder wirft eine Münze, bevor er antwortet. Wenn der Münzwurf Kopf zeigt, antwortet die Person mit der Wahrheit. Wenn nicht, antwortet die Person mit „Ja“. Auf diese Weise ist die Gesamtstatistik des Datensatzes immer noch nützlich, aber es macht es unmöglich, für eine bestimmte Person zu erkennen, ob "Ja" die wahre oder die wegen des Münzwurfs gewählte Antwort war.

Die Definition der differenziellen Privatheit verwendet den Parameter  $\epsilon$ , um den Datenschutz des eingesetzten Verfahrens zu messen.

Differenzielle Privatheit fügt einem Datensatz zufälliges Rauschen hinzu, um den gewünschten Grad an Privatsphäre zu erreichen. Dabei kann es sich um zufällige Dummy-Datensätze handeln, die hinzugefügt werden, oder um zufällige Änderungen an den Datensätzen selbst.

### Pseudonymisierung

In einigen Anwendungsfällen ist die Anonymisierung von Daten nicht angemessen, da man den Bezug der Daten zu den betroffenen Personen nicht völlig verlieren möchte, auch wenn man ihn nur eingeschränkt benötigt. In einer medizinischen Langzeitstudie beispielsweise muss man die Identität der Patienten, deren Daten verarbeitet werden, nicht kennen, aber man möchte vielleicht in der Lage sein, neue Daten, die ein Jahr später erhoben werden, denselben Patienten zuzuordnen.

Dies kann durch eine Pseudonymisierung der Daten erreicht werden, eine Form der Verarbeitung personenbezogener Daten, die sicherstellt, dass Personen zwar immer noch anhand der Daten identifiziert werden können, dies aber nur mit Hilfe zusätzlicher Informationen möglich ist, die separat und mit eingeschränktem Zugang aufbewahrt werden. So können die Daten beispielsweise eine Zufallszahl (das Pseudonym) anstelle des Namens der Person enthalten, und die Tabelle, die Zahlen und Namen miteinander verbindet, wird vertraulich behandelt.

Aus datenschutzrechtlicher Sicht unterscheiden sich pseudonymisierte Daten stark von anonymen Daten. Die Pseudonymisierung von Daten ist eine Maßnahme, die dazu beitragen kann, personenbezogene Daten angemessen zu schützen, und wird daher in Vorschriften wie der DSGVO oder dem für Kreditkartendaten verwendeten PCI DSS-Standard empfohlen. (In PCI DSS wird dieser Ansatz als Maskierung bezeichnet.) Trotzdem gelten

pseudonymisierte Daten als personenbezogene Daten und müssen daher den relevanten Datenschutzbestimmungen entsprechen. Anonyme Daten hingegen gelten nicht als personenbezogen und die Datenschutzbestimmungen sind daher nicht anwendbar.

## 3.2 Datenschutz in der Datenwissenschaft und Big Data

Die Begriffe „Big Data“, „Datenwissenschaft“ oder „Data Science“ und „Künstliche Intelligenz“ werden oft zusammen verwendet, um ähnliche Dinge zu definieren. Da diese Begriffe ähnliche Herausforderungen in Bezug auf den Datenschutz haben, werden wir die folgenden Definitionen verwenden:

Big Data sind Informationsressourcen mit hohem Volumen, hoher Geschwindigkeit und großer Vielfalt, die kosteneffiziente, innovative Formen der Informationsverarbeitung für einen besseren Einblick und eine bessere Entscheidungsfindung erfordern (Gartner Glossary o. J.). Dies ist auch als 3V (volume, variety und velocity) bekannt.

Künstliche Intelligenz (KI) ist ein Teilgebiet der Informatik, das sich mit der Erforschung der Mechanismen von intelligentem menschlichen Verhalten befasst und versucht, bei Menschen als "intelligent" bezeichnetes Verhalten in IT-Systemen zu implementieren. Dabei basiert sie häufig auf der Analyse von Daten, die verwendet werden, um einen bestimmten Aspekt der Welt zu modellieren. Die Schlussfolgerungen aus diesen Modellen werden dann verwendet, um mögliche zukünftige Ereignisse vorherzusagen und zu antizipieren.

In dieser gesamten Lektion werden wir den Begriff „Big Data“ verwenden, was aber auch künstliche Intelligenz und datenwissenschaftliche Anwendungen einschließen soll.

Die folgenden Aspekte machen diese Art der Verarbeitung besonders:

- Verwendung von Algorithmen,
- die Undurchdringbarkeit der Verarbeitung (Black Box),
- die Tendenz, alle Daten zu sammeln,
- die Neuverwendung von Daten und
- die Verwendung neuer Datentypen.

Aus Sicht des Datenschutzes werden daher mehrere Prinzipien verletzt, die es zu beachten gilt, um die Einhaltung der Datenschutzbestimmungen zu gewährleisten. Wenn beispielsweise für operative Zwecke erhobene personenbezogene Daten anschließend für Big Data (in dieser weiten Interpretation) verwendet werden, handelt es sich dabei um eine Zweckänderung, die ggf. im Konflikt zum Prinzip der Zweckbestimmung steht.

Aus diesen neuen Formen der Verarbeitung ergeben sich aber auch Vorteile, etwa die gezieltere Ausrichtung auf Kunden, die Gewährleistung, dass angemessenere personalisierte Ressourcen für die Ausbildung produziert werden, oder die effizientere Gestaltung von Transportwegen.

Auch bestehen viele Risiken, dass diese Instrumente zu unbeabsichtigten Ergebnissen führen können. Ein Beispiel sind Algorithmen, die bei Bewerbungsverfahren nach Geschlecht oder bei der Festlegung von Haftstrafen nach Rasse diskriminieren.

Das ICO (Information Commissioner's Office), die Datenschutzbehörde im Vereinigten Königreich, verlangt von Organisationen, bei der Verwendung großer Datenmengen die folgenden Aspekte zu berücksichtigen:

#### 1. Fairness

- a) Einige Arten von großen Datenanalysen, wie z. B. Profiling, können **Auswirkungen haben, die nicht im Interesse der Betroffenen sind.**
- b) Organisationen müssen sich überlegen, ob die Verwendung persönlicher Daten in großen Datenanwendungen innerhalb der vernünftigen Erwartungshaltung der Betroffenen liegt (ICO 2017, S. 19).

#### Auswirkungen, die nicht im Interesse der Betroffenen sind

Dabei kann es sich um Kreditbewertungen oder Entscheidungen über Bewerbungen handeln.

#### 2. Bedingungen für die Verarbeitung personenbezogener Daten

- a) In einem Kontext großer Datenmengen ist es oft schwierig, eine aussagekräftige Zustimmung zu erhalten, aber neue und innovative Ansätze können dabei helfen.
- b) Sich auf die rechtliche Grundlage des legitimen Interesses zu berufen, ist keine Option. Big-Data-Organisationen müssen immer ihre eigenen Interessen gegen jene der betroffenen Personen abwägen (ebd., S. 29).

#### 3. Zweckbindung

Das Prinzip der Zweckbindung stellt nicht notwendigerweise eine Barriere für große Datenanalysen dar, aber es bedeutet, dass eine Bewertung der Kompatibilität der Verarbeitungszwecke abgeschlossen sein muss (ebd., S. 37).

#### 4. Datensparsamkeit und -speicherung

Große Datenanalysen können dazu führen, dass persönliche Daten gesammelt werden, die über das hinausgehen, was für den Verarbeitungszweck erforderlich ist. Die Aufbewahrungsfristen dürfen nicht verlängert werden, um sicherzustellen, dass große Datenanalysen durchgeführt werden können (ebd., S. 40).

#### 5. Korrektheit

- a) Die Korrektheit personenbezogener Daten ist in allen Phasen eines Big-Data-Projektes (Sammlung, Analyse und Anwendung) von Bedeutung.
- b) Versteckte Verzerrungen in Datensätzen können zu ungenauen Vorhersagen über Personen führen (ebd., S. 43).

#### 6. Betroffenenrechte

Die riesigen Datenmengen, die in großen Analysen verwendet werden, können es den Organisationen schwieriger machen, das Recht auf Zugang zu persönlichen Daten einzuhalten (ebd., S. 46).

#### 7. Befangenheit ausschließen

- a) Algorithmen des maschinellen Lernens haben das Potenzial, Entscheidungen zu treffen, die diskriminierend, fehlerhaft und ungerechtfertigt sind.
- b) Die Datenqualität ist eine Schlüsselfrage für diejenigen, die in einem großen Datenkontext für die Information Governance verantwortlich sind (ebd., S. 51).

8. **für die Datenverarbeitung Verantwortliche und Verarbeiter**  
Organisationen, die Analysen an auf KI und maschinelles Lernen spezialisierte Unternehmen auslagern, müssen sorgfältig abwägen, wer die Kontrolle über die Verarbeitung personenbezogener Daten hat (ebd., S. 56).
9. **Anonymisierung**  
Oftmals wird bei großen Datenanalysen die Verwendung von Daten, die Personen identifizieren, nicht erforderlich sein, sodass die Anonymisierung viele der Risiken mindern kann (ebd., S. 58).
10. **Datenschutz von Beginn an und standardmäßig**  
Die Einbettung von „Privacy by Design“-Lösungen in große Datenanalysen kann durch eine Reihe von technischen und organisatorischen Maßnahmen zum Schutz der Privatsphäre beitragen (ebd., S. 72).
11. **algorithmische Transparenz**
  - a) Mithilfe von Auditing-Techniken lassen sich solche Faktoren identifizieren, die eine algorithmische Entscheidung beeinflussen.
  - b) Zur algorithmischen Transparenz sollte eine Kombination aus technischen und organisatorischen Ansätzen verwendet werden (ebd., S. 86).

Diese Maßnahmen bei der Umsetzung und Gestaltung im Auge zu behalten, hilft einer Organisation, die Regeln des Datenschutzes einzuhalten und PII auf faire und ethische Weise zu verarbeiten.

### 3.3 Benutzer-Tracking im Onlinemarketing

**Tracking**  
Anzeigen im Internet richten sich an einen User aufgrund seines bisherigen Interesses an einem Thema. Dies wird über Tracking und häufig über Cookies erreicht.

**Tracking** im Onlinemarketing bedeutet die Protokollierung von Benutzeraktivitäten im Web. Tracking wird verwendet, um den Erfolg von Marketingkampagnen zu ermitteln, um Klicks mit einem Partner in Verbindung zu bringen, der zur Finanzierung vieler Websites beiträgt, sowie um zu prüfen, ob eine Website genutzt werden kann oder nicht.

Das Tracking liefert üblicherweise die folgenden Informationen:

- von wo aus ein Benutzer auf eine Webseite zugegriffen hat,
- wie oft auf Seiten zugegriffen wird,
- wie lange ein Benutzer auf einer bestimmten Seite bleibt, und
- wohin die Benutzer gehen, wenn sie die Website verlassen.

Das Risiko für die Privatsphäre besteht darin, dass durch die Verfolgung des Verhaltens der Benutzer dieses Verhalten gesteuert werden kann. Cambridge Analytica nutzte das Tracking, um Anzeigen in einer politischen Kampagne zu schalten, die gefälschte Nachrichten enthielten, welche jedoch äußerst schwer zu erkennen waren, da sie nur eine kleine Anzahl von Personen erreichten (Hern 2018). Sensible persönliche Daten können auch durch das Verständnis der Surfgewohnheiten einer Person aufgedeckt werden.

Um das Verhalten der Benutzer zu verfolgen, werden verschiedene Werkzeuge verwendet:

- First-Party-Cookies werden von der Domain (Website) gespeichert, die ein Benutzer direkt besucht. Sie ermöglichen es Websitebetreibern, Analysedaten zu sammeln, Spracheinstellungen zu speichern und andere Funktionen auszuführen.
- Third-Party-Cookies werden von anderen Domains als der erstellt, die eine Person direkt besucht, daher der Name Third-Party. Sie werden für Cross-Site-Tracking, Retargeting und Adserving verwendet. Dabei geht es um Verfahren, die den Verlauf von Besuchern unterschiedlicher Webseiten überwachen, um darauf basierende Werbung auszuspielen.
- Cross-Device-Tracking ist eine Technik zur Verfolgung eines Benutzers über verschiedene Geräte hinweg.
- Fingerprint Tracking verwendet bestimmte Merkmale eines Browsers (Version, installierte Schriftarten, Hardware-Details usw.), um einen Benutzer zu identifizieren. Es muss nichts auf dem Gerät des Benutzers gespeichert werden.
- Gemeinsame IDs, bei denen sich Benutzer anmelden, wie z. B. Google ID oder Apple ID.
- Werbe-IDs ermöglichen das Tracking auf mobilen Geräten.
- Web-Beacons oder Tracking-Pixel können zeigen, dass ein Benutzer auf bestimmte Inhalte zugegriffen hat.

Über die Rechtmäßigkeit des Webtracking in der Europäischen Union unter DSGVO wird derzeit viel diskutiert. Der kalifornische CCPA könnte die Situation in Zukunft ebenfalls ändern. Die Werbeindustrie argumentiert, es sei ihr legitimes, ihrem Geschäftsmodell innewohnendes und auch für die Nutzer vorteilhaftes Interesse, die Tracking-Technologie zu nutzen. Datenschutzbefürworter und Verbraucherverbände hingegen argumentieren, dass dies nicht der Fall sei und ein Nutzer nur dann verfolgt werden dürfe, wenn er eine gültige Einwilligung erteilt habe.

In einem am 1. Oktober 2019 beim Europäischen Gerichtshof verhandelten Fall (Rechtssache C-673/17) wurde eine Vorabentscheidung zwischen Planet49, einer Werbeorganisation, und einer deutschen Verbraucherorganisation getroffen. Der Fall macht deutlich, dass Cookies, die nicht unbedingt notwendig sind, nach dem Prinzip „privacy by default“ (InfoCuria 2019) nicht ohne Einwilligung gesetzt werden dürfen.

Ein typisches Cookie-Banner bietet den Benutzern Auswahlmöglichkeiten für jede Kategorie von Cookies. Schaltflächen können gewählt werden, um alle oder nur bestimmte Kategorien von Cookies zu akzeptieren. Notwendige Cookies sind i. d. R. mit vorausgewählt. Die Benutzer erhalten eine Erklärung über die verschiedenen Kategorien von Cookies. Dies geschieht in einer Sprache, die auch Benutzer ohne technischen Hintergrund verstehen können.

Nur die notwendigen Cookies sollten standardmäßig aktiviert sein. Die meisten Behörden in Europa teilen diese Meinung, wenngleich Werbefirmen sich dagegen wehren. Die erwähnte EU-Richtlinie zum Datenschutz in der elektronischen Kommunikation sollte in Zukunft weitere Orientierungshilfen bieten.

Der CCPA und andere Datenschutzbestimmungen als das DSGVO haben noch keine solche Regelung. Die meisten von ihnen verlangen lediglich die Bereitstellung von Informationen für die Betroffenen.

## 3.4 Cloud-Computing

Cloud Computing ist heute weit verbreitet. ISO/IEC 19941 definiert diesen Begriff als „Paradigma für die Ermöglichung des Netzzugangs zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer physischer oder virtueller Ressourcen mit Selbstbedienungs-Bereitstellung und Verwaltung nach Bedarf“.

Cloud Computing besteht aus den folgenden wesentlichen Merkmalen:

1. Ressourcen-Pooling: Der Cloud-Anbieter extrahiert Ressourcen und sammelt sie in Pools, dann werden die Anteile dieses Pools den Cloud-Kunden zugewiesen.
2. breiter Netzzugang: Alle Ressourcen sind über das Internet verfügbar.
3. schnelle Elastizität: Die Erweiterung und Reduzierung der Nutzung von Cloud-Ressourcen erfolgt nach Bedarf entsprechend den Nachfragemustern.
4. gemessene Leistung: misst, was vom Cloud-Provider zur Verfügung gestellt wird. Die Abrechnung basiert auf dieser Messung.
5. Selbstbedienung auf Abruf: Cloud-Kunden verwalten die Bereitstellung von Ressourcen selbstständig.

Cloud-Modelle gibt es in verschiedenen Servicemodellen, die gängigsten sind unten aufgeführt:

- Software als Dienstleistung (Software as a Service; SaaS): eine vollständige Anwendung, die vom Anbieter verwaltet und gehostet wird.
- Plattform als Dienstleistung (Platform as a Service; PaaS): eine IT-Plattform, die zur Verfügung gestellt wird, beispielsweise eine Datenbankplattform oder mehrere Umgebungen, auf denen ein Kunde seine eigene Anwendung ausführen kann.
- Infrastruktur als Dienstleistung (Infrastructure as a Service; IaaS): ein Pool grundlegender IT-Dienste, wie z. B. Server mit Betriebssystemen, Netzwerk oder Speicher.

Manchmal lassen sich die Grenzen zwischen den verschiedenen Dienstleistungsmodellen nicht genau ziehen.

Schlussendlich gibt es vier verschiedene Einsatzmodelle:

1. Public Cloud: Die Cloud-Infrastruktur wird der Allgemeinheit zur Verfügung gestellt.
2. Private Cloud: Die Cloud-Infrastruktur wird nur für eine Organisation betrieben.
3. Hybrid Cloud: Die Cloud-Infrastruktur ist eine Zusammensetzung aus einer öffentlichen und einer privaten Cloud.
4. Community Cloud: Mehrere Organisationen, oft aus der gleichen Branche oder vom gleichen geografischen Standort, teilen sich Cloud-Ressourcen.

Vom Datenschutzstandpunkt aus liegt die größte Herausforderung in der verteilten Natur von Cloud-Ressourcen. Cloud Computing findet weltweit statt und oft ist nicht geklärt, wo sich die Ressourcen des Cloud-Anbieters wirklich befinden. Infolgedessen kann auch unklar sein, wo sich die Daten einer Organisation derzeit befinden. Andererseits schreiben

mehrere Datenschutzbestimmungen vor, dass PII im selben Rechtsraum gespeichert oder besondere zusätzliche Sicherheitsvorkehrungen getroffen werden müssen, um den Export von PII zu erlauben.

Diese Herausforderungen werden i. d. R. mit den folgenden Mitteln angegangen:

- Der Cloud-Anbieter bietet Optionen zur Einschränkung des Speicherorts der Daten an. Microsoft beispielsweise erlaubt bei der Azure-Cloud, mehrere Regionen und Länder zu definieren; die Preise sind dabei für jede Region unterschiedlich. Auch Amazon bietet solche Speicheroptionen als Teil seiner Amazon Web Service (AWS)-Angebote an.
- Cloud-Provider zeigen die Sicherheit von PII über Zertifizierungen auf. ISO 27017 (Informationstechnologie – Sicherheitstechniken – Verhaltenskodex für Informationssicherheitskontrollen auf der Grundlage von ISO/IEC 27002 für Cloud-Dienste) enthält Sicherheitsrichtlinien, während ISO 27018 (Informationstechnologie – Sicherheitstechniken – Verhaltenskodex für den Schutz personenbezogener Daten (PII) in öffentlichen Clouds, die als Auftragsverarbeiter fungieren) speziell den Datenschutz behandelt. Diese Zertifizierungen können die Notwendigkeit zusätzlicher Schutzvorkehrungen wie Standardvertragsklauseln nicht umgehen, können aber dazu beitragen, die Einhaltung bestimmter Standards zu gewährleisten.
- Es werden Standardvertragsklauseln oder andere vertragliche Vereinbarungen unterzeichnet, um sicherzustellen, dass exportierte PII korrekt verarbeitet werden.

Die verschiedenen rechtlichen Verpflichtungen sind eine Herausforderung. Viele Länder verlangen, dass Organisationen Daten für Regierungsbehörden wie Strafverfolgungsbehörden, nationale Sicherheitsbehörden und andere zur Verfügung stellen. Diese Anforderungen können direkt mit den Datenschutzgesetzen der datenexportierenden Länder kollidieren. Eine Möglichkeit, diese Herausforderung zu entschärfen, besteht darin, zu verstehen und zu definieren, wo Daten gespeichert werden. Informationen können auch dahingehend verschlüsselt werden, dass eine ausländische Regierungsbehörde nicht auf PII zugreifen kann. Bedenken Sie jedoch, dass die Implementierung dieses kryptografischen Schemas sicherstellen muss, Daten im Ruhezustand, bei der Übertragung und bei der Verwendung zu verschlüsseln, um die Informationen vor einem Cloud-Anbieter, der Zugang sucht, angemessen zu schützen.

Die Cloud Security Alliance schlägt 14 Bereiche vor, die untersucht werden sollten, um ein angemessenes Sicherheitsniveau zu erreichen (Cloud Security Alliance 2017). Diese werden im Folgenden zusammengefasst.

### **Bereich 1: Cloud-Computing-Konzepte und -Architekturen**

Konzeptioneller Rahmen für den Rest der Anleitung. Er beschreibt und definiert Cloud Computing, legt unsere Grundterminologie fest und erläutert die allgemeinen logischen und architektonischen Rahmenbedingungen, die im restlichen Dokument verwendet werden.

### **Bereich 2: Governance und Unternehmensrisikomanagement**

Die Fähigkeit einer Organisation, die durch Cloud Computing eingeführten Unternehmensrisiken zu steuern und zu messen.

### **Bereich 3: Rechtsfragen, Verträge und elektronische Entdeckung**

Mögliche rechtliche Probleme beim Einsatz von Cloud Computing. Zu den Themen, die in diesem Abschnitt behandelt werden, gehören Schutzanforderungen für Informationen und Computersysteme, Gesetze zur Offenlegung von Sicherheitsverletzungen, Datenschutz- und behördliche Anforderungen, internationale Gesetze usw.

### **Bereich 4: Compliance und Audit-Management**

Aufrechterhaltung und Nachweis der Compliance beim Einsatz von Cloud Computing.

### **Bereich 5: Informations-Governance**

Verwalten von Daten, die in die Cloud gestellt werden. Hier werden Elemente rund um die Identifizierung und Kontrolle von Daten in der Cloud sowie kompensierende Kontrollen diskutiert, die verwendet werden können, um mit dem Verlust der physischen Kontrolle beim Verschieben von Daten in die Cloud umzugehen.

### **Bereich 6: Verwaltungsebene und Business Continuity**

Sicherung der Verwaltungsebene und der administrativen Schnittstellen, die beim Zugriff auf die Cloud verwendet werden, einschließlich Web-Konsolen und APIs.

### **Bereich 7: Sicherheit der Infrastruktur**

Sicherheit der Kern-Cloud-Infrastruktur einschließlich Netzwerk, Sicherheit der Arbeitslast und Überlegungen zu hybriden Clouds.

### **Bereich 8: Virtualisierung und Container**

Sicherheit für Hypervisor, Container und softwaredefinierte Netzwerke.

### **Bereich 9: Reaktion auf Sicherheitsvorfälle**

Ordnungsgemäße und angemessene Erkennung, Reaktion, Benachrichtigung und Behebung von Vorfällen.

### **Bereich 10: Anwendungssicherheit**

Sicherung von Anwendungssoftware, die auf der Cloud läuft oder in der Cloud entwickelt wird. Dies schließt die Bezugnahme auf die OWASP Top 10 ein.

### **Bereich 11: Datensicherheit und Verschlüsselung**

Implementierung von Datensicherheit und Verschlüsselung und Gewährleistung einer skalierbaren Schlüsselverwaltung.

#### **Bereich 12: Identitäts-, Berechtigungs- und Zugriffsverwaltung**

Verwaltung von Identitäten und Nutzung von Verzeichnisdiensten für die Zugangskontrolle.

#### **Bereich 13: Sicherheit als Dienstleistung**

Bereitstellung von Sicherheitsdiensten, die von Dritten unterstützt werden.

#### **Bereich 14: Verwandte Technologie**

Technologien mit einer Beziehung zum Cloud Computing einschließlich großer Datens Mengen, Internet der Dinge und mobilem Computing.



#### **ZUSAMMENFASSUNG**

Die Umsetzung des Datenschutzes ist möglich, erfordert aber bestimmte Techniken, um erfolgreich zu sein. Verschiedene Varianten des Datenschutzes bieten unterschiedliche Ebenen der Privatsphäre. Grundlegende Techniken wie Verallgemeinerung und Unterdrückung müssen sorgfältig erwogen und eingesetzt werden, da individuelle Daten immer noch preisgegeben werden können. Der differenzierte Datenschutz bietet ein höheres Maß an Datenschutzsicherheit, ist aber immer mit Kosten verbunden, da er die Daten weniger brauchbar macht. An dieser Stelle muss also das richtige Gleichgewicht gefunden werden.

Benutzertracking, Cloud Computing und Big Data bieten einen enormen Wert für eine Organisation, aber jede von ihnen hat aus der Perspektive des Datenschutzes bestimmte Herausforderungen. Wo User Tracking ein Thema von Transparenz und Zustimmung ist, bringt uns die Datenwissenschaft zu einem Bereich, in dem eine Organisation einen Ausgleich zwischen ihren Interessen und denen des Einzelnen finden muss. Zweckbindung und Datensparsamkeit stehen so in direktem Konflikt mit den Bedürfnissen von Big Data.

Cloud Computing bietet zwar Vorteile, aber die Daten verlassen das Unternehmen und werden im Wesentlichen an einem anderen Ort verarbeitet. Mitunter ist es nicht einfach zu bestimmen, wo und wie die PII verarbeitet werden, und die Cloud Security Alliance stellt Richtlinien und Rahmen zur Verfügung, wie das Problem angegangen werden kann. Insbesondere grenzüberschreitende Übertragungen von PII sind so einfach,

dass eine Organisation die Rechtmäßigkeit der PII prüfen und vertragliche Schutzmaßnahmen oder die Datenverarbeitung in einem bestimmten Land oder einer bestimmten Region vereinbaren muss.

# LEKTION 4

## BESTANDTEILE DER IT-SICHERHEIT

### LERNZIELE

Nach der Bearbeitung dieser Lektion werden Sie wissen, ...

- wie grundlegende IT-Sicherheitskonzepte und zentrale IT-Sicherheitsbausteine funktionieren.
- wie man einen soliden Sicherheitsplan schreibt.
- wie man sicheren Code erstellt und Webanwendungen auf Sicherheit testet.
- wie das Konzept der DevSecOps funktioniert.
- wie man ein sicheres IT-System entwickelt.
- wie man am besten einen IT-Sicherheitsrahmen für ein Unternehmen festlegt.

## **4. BESTANDTEILE DER IT-SICHERHEIT**

### **Einführung**

Es ist nicht einfach, die notwendigen Bausteine der IT-Sicherheit zu erklären, ohne einige grundlegende Konzepte zu erläutern. So geht es bei der IT-Sicherheit nicht nur um die Verteidigung digitaler Informationen in der Cyberwelt, sondern auch um die Verteidigung anderer gefährdeter Aspekte der Informations- und Kommunikationstechnologie-Umgebung. Hier gibt es viele Möglichkeiten, die Bausteine der IT-Sicherheit zu definieren, ihre Hauptmerkmale aber sind folgende:

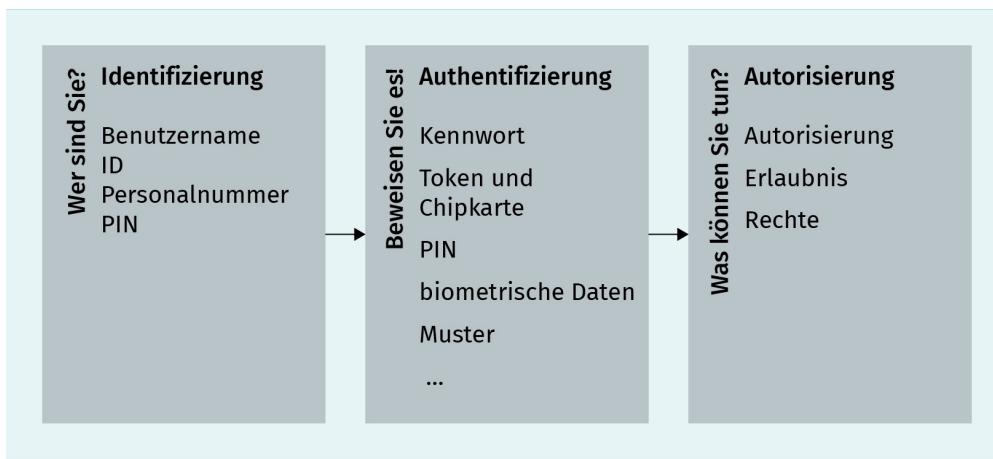
- Identifizierung, Authentifizierung, Autorisierung, Rechenschaft,
- Netzwerksicherheit,
- Endpunktsicherheit,
- Informationsverwaltung,
- Management von Schwachstellen, Bedrohungen und Zwischenfällen sowie
- Sensibilisierung, Schulung und Ausbildung.

### **4.1 Authentifizierung, Zugriffsverwaltung und -kontrolle**

Es gibt vier grundlegende Konzepte, bekannt als IAAA (gesprochen „I triple A“), die für die Zugriffsverwaltung zu einem System benötigt werden. Dies sind:

- Identifikation (wer Sie sind),
- Authentifizierung (Nachweis, wer Sie sind),
- Autorisierung (was Sie tun können), und
- Rechenschaftspflicht (Audit und Audit-Protokolle).

Abbildung 5: Prozess des Zugriffs auf ein System



Quelle: Jasmin Ćosić 2020.

Die obige Abbildung zeigt die Schritte, die unternommen werden sollten, um Zugang zu einem System zu erhalten. Für die Identifikationsphase müssen wir beispielsweise ID, Benutzername, Mitarbeiternummer, PIN o. ä. erhalten haben. Um durch den Authentifizierungsprozess zu gelangen, müssen wir etwas vorweisen können, das wir kennen (PIN, Passwort, Muster usw.), etwas, das wir haben (Token, Smartcard usw.), oder eine biometrische Eigenschaft (Fingerabdruck usw.). Nach erfolgreicher Authentisierung erhalten wir begrenzten Zugang zu den Ressourcen (Erlaubnis und Rechte). Mit der Authentifizierung soll nach Möglichkeit verhindert werden, dass sich ein nicht autorisierter Benutzer Zugang verschafft, indem er sich als ein autorisierter Benutzer ausgibt. Die Sicherheitsrichtlinie der Organisation sollte widerspiegeln, wie schwierig es für einen Benutzer ist, sich als ein anderer auszugeben. Hochsensible oder wertvolle Informationen erfordern stärkere Authentifizierungstechnologien als weniger sensible oder wertvolle Informationen (Chapple/Shinder/Tittel 2002).

Die gebräuchlichste und am wenigsten strenge Form der Authentifizierungstechnologie verlangt lediglich, dass Benutzer einen gültigen Kontonamen und ein Passwort angeben, um Zugang zu einem System oder Netzwerk zu erhalten. In Umgebungen, in denen Passwörter die einzigen Zugangs- und Zugriffsbarrieren darstellen, ist es wichtig zu verstehen, wie man starke Passwörter erstellt und bekannte Konten vor Angriffen schützt. Heute verfügen die meisten IT-Systeme in Unternehmen bereits über einen Mechanismus zur Überprüfung der Komplexität von Passwörtern, der als Komplexitätsregel bekannt ist.

Mindestanforderungen an Passwörter lauten häufig, dass diese mindestens zwölf Zeichen lang sein und eine Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten müssen, beispielsweise „gnlemZUH70\_§“. Das Problem bei dieser Komplexität ist das Erinnern an diese Art von Passwörtern, aber ein Benutzer kann dafür seinen eigenen Algorithmus erstellen oder Software von Drittanbietern für die Passwortverwaltung verwenden. Ein Risiko bei schwachen Passwörtern in computerlesbaren Formaten besteht darin, dass sie bei einem Brute-Force- oder Wörterbuch-Angriff verwendet werden

können. Ein effektives Authentifizierungsmanagement wird in der neuen NIST-Sonderveröffentlichung 800-63A-C, „Digital Identity Guidelines“, beschrieben (Grassi/Garcia/Fenton 2019).

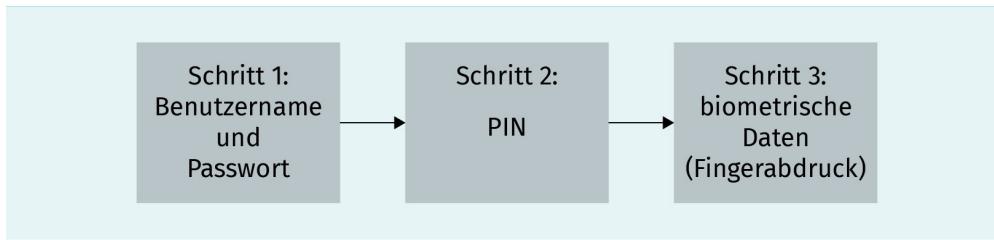
Eine alternative Methode zur Authentifizierung ist die Biometrie. Diese stützt sich auf Metriken im Zusammenhang mit menschlichen Merkmalen. Biometrische Identifikatoren sind messbare, unverwechselbare Merkmale, die zur Kennzeichnung und Beschreibung von Personen verwendet werden. Durch den Einsatz der Biometrie könnte ein Benutzer danach unterschieden werden, wer er ist, anstatt danach, was er besitzt (Karte, Token) oder weiß (Geheimschlüssel, PIN) (Kalyani 2017). Biometrische Systeme „lesen“ einige physische Merkmale des Benutzers wie Fingerabdruck, Gesichtszüge, Netzhautmuster, Stimmabdruck, Handgeometrie oder Unterschrift. Sogar die Art und Weise, wie der Benutzer geht oder auf einer Tastatur tippt, kann als biometrisches Authentifizierungsverfahren verwendet werden. Um die Identität festzustellen, werden diese Messwerte mit einer Datenbank autorisierter Benutzer oder einem Muster verglichen.

Eine Authentifizierung auf Grundlage der Biometrie scheint auf den ersten Blick sehr sicher zu sein, bringt jedoch erfahrungsgemäß auch einige große Nachteile mit sich. Erstens gibt es mehrere Beispiele für die Überwindung eines solchen Systems, z. B. die Verwendung eines Fingerabdruck-Dummys, der auf einem hochauflösenden Foto eines von der betreffenden Person berührten Glases basiert. Zweitens – da verschiedene Messungen biometrischer Eigenschaften ein und derselben Person nie identisch sind – muss man auf ein gewisses Maß an Abweichung zurückgreifen. Wenn die akzeptierte Abweichung zu groß ist, führt dies zu einer hohen Falschakzeptanzrate (false acceptance rate – FAR), bei der auch Personen mit ähnlichen Merkmalen akzeptiert werden. Ist die akzeptierte Abweichung zu gering, führt dies zu einer hohen Falschrückweisungsrate (False rejection rate – FRR), bei der selbst legitime Benutzer nicht akzeptiert werden und bei wiederholtem Auftreten unter Umständen keinen Zugang zum System erhalten. Drittens ist es zwar möglich, ein Passwort oder eine PIN zu ändern, nicht jedoch, seine biometrischen Merkmale zu ändern, selbst wenn sie „gestohlen“ und missbraucht werden.

Die nächste Authentifizierungsmethode sind Sicherheitsvorrichtungen. Diese Systeme erfordern die Verwendung eines speziellen Hardwaregeräts, das wie ein kundenspezifischer Schlüssel funktioniert, um Zugang zum System zu erhalten. Das Gerät kann wie ein Schlüssel in das System eingeführt oder zur Erzeugung eines Codes verwendet werden, der dann ins System eingegeben wird.

Zur Erhöhung der Sicherheit können für die Authentifizierung zwei (Zwei-Faktor-Authentifizierung – 2FA) oder mehr Faktoren (Multi-Faktor-Authentifizierung – MFA) kombiniert werden. Dabei kann es sich um einen Benutzernamen und ein Passwort mit anderen Anmeldedaten handeln, z. B. einen Code vom Smartphone oder der Fingerabdruck des Benutzers, die Antwort auf eine Sicherheitsfrage oder die Gesichtserkennung. Die Abbildung unten zeigt ein spezifisches Beispiel für eine MFA oder eine Drei-Faktor-Kombination der Authentifizierung (Benutzername und Passwort + PIN + Fingerabdruck).

**Abbildung 6: Beispielschritte in der MFA-Methode**

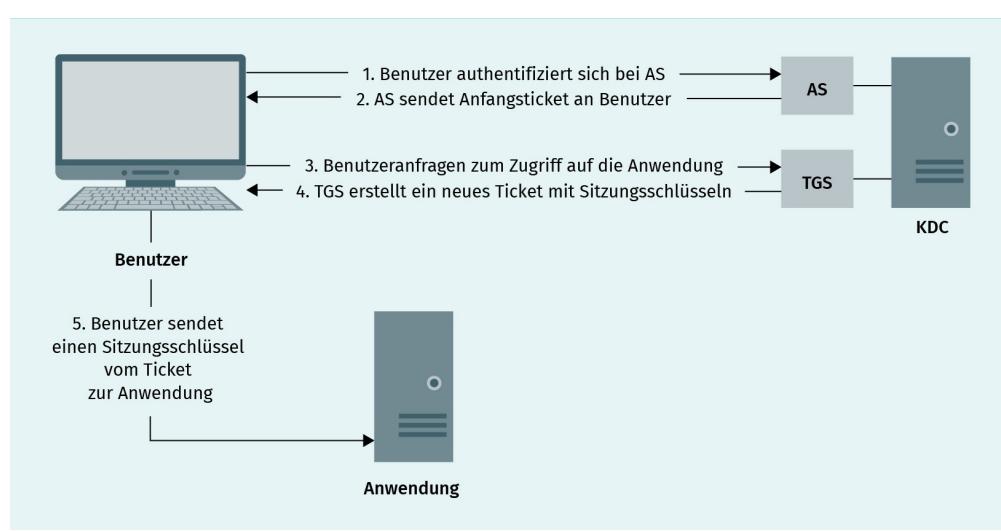


Quelle: Jasmin Ćosić 2020.

Single Sign-on (SSO) ist eine weitere Methode, die von vielen Unternehmen verwendet wird – es ist eine Kombination aus Identitäts- und Zugriffsmanagement (Identity and Access Management – IAM), die es den Benutzern ermöglicht, sich sicher bei mehreren Anwendungen und Websites zu authentifizieren, wobei sie sich nur einmal mit ihren Anmeldeinformationen (z. B. Benutzername und Passwort) anmelden. Dadurch erhält der Benutzer die Möglichkeit, sich mit einer einzigen Authentifizierungsautorität zu authentifizieren und dann auf andere geschützte Ressourcen zuzugreifen, ohne sich erneut authentifizieren zu müssen. Die Open Group definiert SSO als den Mechanismus, durch den eine einzige Aktion der Benuterauthentifizierung und -autorisierung einem Benutzer den Zugang zu allen Computern und Systemen ermöglichen kann, auf die dieser zugriffsberechtigt hat, ohne dass er mehrere Passwörter eingeben muss (De Clercq 2002).

Kerberos ist ein häufig verwendetes Protokoll für SSO in verteilten Umgebungen. Es ist in Open-Source-Produkten, aber auch in Microsoft Active Directory implementiert. Die Hauptkomponente ist ein Key Distribution Center (KDC), dass die geheimen Schlüssel aller Benutzer und Dienste enthält. Es bietet einen Authentifizierungsdienst (authentication service – AS) und eine Schlüsselverteilungsfunktionalität. Das KDC stellt den Auftraggebern Sicherheitsdienste zur Verfügung, bei denen es sich um Benutzer, Anwendungen oder andere Netzwerkdienste handeln kann. Das KDC muss über ein Konto für jeden Auftraggeber verfügen. Ein Ticket wird durch den Ticket-Gewährungsservice (Ticket Granting Service – TGS) auf dem KDC generiert und an einen Auftraggeber ausgegeben. Das Ticket ermöglicht es dem Benutzer, sich bei einem anderen Benutzer zu authentifizieren (Neumann/Hartmann/Raeburn 2005). Nutzer sind hier auch Server, Drucker und andere Einheiten. Der englische Fachbegriff lautet „Principal“.

Abbildung 7: Authentifizierung über das verbreitete SSO-Protokoll Kerberos



Quelle: Jasmin Ćosić 2020.

Zutrittskontrollen sind Maßnahmen, die verhindern, dass unbefugte Personen den physikalischen Zutritt zu Datenverarbeitungsanlagen erhalten. Sie verhindern die Nutzung der Systeme durch Unbefugte und stellen sicher, dass ausschließlich befugte Personen Zugriff auf Informationen erhalten.

Es gibt zwei Methoden des Zugangs: physisch und logisch. Die physische Zugangskontrolle ist eine mechanische Form, z. B. der physische Zugang zu einem Raum (Serverraum) mit Schlüsseln. Der physische Zugang kann mit physischen Schlüsseln erreicht oder durch eine Anwendungs- oder Systemsoftware mit einem Chip auf einer Zugangskarte gesteuert werden.

Werkzeuge für logische Zugangskontrollen, die für Berechtigungsnachweise, Validierung, Autorisierung und Verantwortlichkeit in der Cyberinfrastruktur und den darin befindlichen Systemen verwendet werden, sind oft auf mehreren Ebenen implementiert und setzen Zugangskontrollmaßnahmen für Systeme, Anwendungen, Prozesse und Informationen durch. Diese Art der Zugangskontrolle kann auch in eine Anwendung, ein Betriebssystem, eine Datenbank oder ein Verwaltungssystem eingebettet sein (Vacca 2014).

Heute gibt es zahlreiche Methoden der Zugangskontrolle, die in der realen Welt implementiert sind. Dazu gehören u. a. die folgenden:

- zwingend erforderliche Zugangskontrolle (mandatory access control – MAC),
- benutzerbestimmbare Zugangskontrolle (discretionary access control – DAC),
- regelbasierte Zugangskontrolle und
- rollenbasierte Zugriffskontrolle (role-based access control, RBAC).

In einer Umgebung mit zwingend erforderlicher Zugangskontrolle werden alle Benutzer und Ressourcen klassifiziert und erhalten ein oder mehrere Sicherheitsetiketten (wie „Unclassified“, „Secret“ und „Top Secret“). Eine bekannte Form der MAC ist das Bell-LaPa-

dula-Modell, bei dem ein Benutzer nur dann auf eine Ressource zugreifen kann, wenn sein Sicherheitslabel mindestens so hoch ist wie das der Ressource. Jede von einem Benutzer erstellte oder geschriebene Ressource erhält automatisch das Sicherheitsetikett des Benutzers. Dieser Ansatz eignet sich gut für den Schutz der Vertraulichkeit (kein Read-up, d. h., dass eine Ressource mit einer höheren Vertraulichkeitsstufe nicht gelesen werden kann), aber in seiner reinen Form macht er es einem Benutzer unmöglich, mit anderen Benutzern zu kommunizieren, die ein niedrigeres Sicherheitsetikett haben (keine Herunterstufung). Das Biba-Modell hingegen legt den Schwerpunkt eher auf die Integrität als auf die Vertraulichkeit der Ressourcen und definiert daher, dass ein Benutzer nur dann auf eine Ressource zugreifen kann, wenn die Sicherheitsstufe des Benutzers höchstens so hoch ist wie das der Ressource (kein Read-down, kein Write-up). Da dies zu ähnlichen Problemen wie beim Bell-LaPadula führt, sind beide Modelle als zugrundeliegendes Modell nützlich, werden aber selten in reiner Form, sondern nur in abgeschwächter Form verwendet. Beispielsweise wird beim Biba-Modell dann zusätzlich erlaubt, dass Benutzer auch auf Ressourcen mit niedrigerer Sicherheitsstufe zugreifen können, aber nur, nachdem sie ausdrücklich bestätigt haben, dass sie auf solche weniger vertrauenswürdigen Daten zugreifen wollen.

In einer DAC-Umgebung (Discretionary Access Controlled) kontrollieren Ressourcenbesitzer und -verwalter gemeinsam den Zugang zu Ressourcen. Dieses Modell ermöglicht eine viel größere Flexibilität und reduziert so den Verwaltungsaufwand bei der Umsetzung von Sicherheitsmaßnahmen drastisch. Im Allgemeinen verbinden regelbasierte Zugriffskontrollsysteme explizite Zugriffskontrollen mit bestimmten Systemressourcen, wie z. B. Dateien oder Druckern. In solchen Umgebungen legen Administratoren gewöhnlich Zugriffsregeln auf einer Pro-Ressourcen-Basis fest. Das zugrunde liegende Betriebssystem oder die Verzeichnisdienste verwenden diese Regeln, um Benutzern, die Zugriff auf solche Ressourcen beantragen, diesen zu gewähren oder zu verweigern. Regelbasierte Zugriffskontrollen können ein MAC- oder DAC-Schema verwenden, je nach der Verwaltungsrolle der Ressourcenbesitzer.

Die rollenbasierte Zugriffskontrolle (RBAC) erzwingt Zugriffskontrollen in Abhängigkeit von der/den Rolle(n) eines Benutzers. Rollen stellen spezifische organisatorische Pflichten dar und werden üblicherweise Berufsbezeichnungen wie „Debitorensachbearbeiter“, „Empfangsmitarbeiter“ oder „Geschäftsführer“ zugeordnet. Es liegt auf der Hand, dass diese Rollen sehr unterschiedliche Netzwerkzugriffsprivilegien erfordern (Chapple/Shinder/Tittel 2002).

Bedenkt man, dass die Benutzer Zugang zu einer großen Anzahl von Anwendungen, Web-sites, Webdiensten und dergleichen benötigen, ist es wichtig, eine „einfache“ Methode der Authentifizierung ohne viele komplexe Passwörter oder Karten mit Chips zu haben. Eine Lösung für diese Herausforderung wurde von der FIDO Alliance entwickelt. Die FIDO2-Spezifikationen sind die Web-Authentifizierungsspezifikation (WebAuthn) des World Wide Web Consortiums (W3C) und das entsprechende Client-to-Authenticator Protocol (CTAP) der FIDO Alliance (o. J.). Die Idee, über solide Authentifizierungsmethoden ohne Passwort und/oder komplexe Hardware zu verfügen, wurde durch „passwortlose“ Authentifizierung, Zwei- oder Multi-Faktor-Authentifizierung in Kombination mit Biometrie umgesetzt. All diese Optionen können in einem einfachen Stück Hardware implementiert werden. FIDO2 unterstützt kennwortlose, Zwei- und Multi-Faktor-Authentifizierung mit eingebette-

ten Authentifikatoren wie Biometrie, PINs oder externen (oder Roaming-)Authentifikatoren wie FIDO-Sicherheitsschlüsseln, mobilen Geräten, Wearables usw. Die Protokolle liefern keine Informationen, die von verschiedenen Online-Diensten zur Zusammenarbeit und zur Verfolgung eines Benutzers über die Dienste hinweg verwendet werden können. Wenn biometrische Informationen verwendet werden, verlassen sie niemals das Gerät des Benutzers (Mobiltelefon, USB-Stick, PC usw.) (ebd.).

Protokollierung stellt sicher, dass die Benutzer für ihre Handlungen verantwortlich sind. Sie können verwendet werden, um die Handlungen der Benutzer zu überprüfen und bei Untersuchungen zu helfen. Protokollierungen und Protokolldateien enthalten eine riesige Menge an Informationen und die Herausforderung besteht oft darin, sie auf die relevanten Teile zu reduzieren. Protokolle enthalten Informationen über Betriebssystemaktivitäten, Anwendungs- und Netzwerkereignisse sowie Benutzeraktionen. Protokolle können auch dazu verwendet werden, Systemadministratoren oder Manager über ein bestimmtes Ereignis zu informieren. Später können sie auch für die Forensik während einer strafrechtlichen Untersuchung verwendet werden. Protokolle können manuell oder automatisch überprüft werden, müssen jedoch überprüft und analysiert werden. Ein SIEM-System (Security Information and Event Management) kann bei der Verwaltung von Audit-Trails und Warnmeldungen helfen (Nieles/Dempsey/Pillitteri 2017). Andererseits stellen Protokolle neue Herausforderungen dar, da sie die persönlichen Daten der Benutzer erfassen, sodass für jedes spezifische System ein angemessener Kompromiss gefunden werden muss.

## 4.2 Endgerätesicherheit

Das allgemeine Konzept der Endpunktsicherheit bezieht sich auf die Sicherung von „Endgeräten“ wie Desktops, Laptops und mobilen Geräten. Jedoch können auch Server in Rechenzentren als Endgeräte betrachtet werden. Eine genaue Definition ist schwierig, doch lässt sich im Zusammenhang mit der IT-Sicherheit sagen, dass Endgeräte ganz einfach die Geräte der Benutzer sind, die mit dem Netzwerk verbunden sind.

Endgerätesicherheit umfasst dabei nicht nur den Schutz durch Antiviren-Software. Endgeräte dienen als Zugangspunkte zu einem Unternehmensnetzwerk und schaffen Eintrittspunkte, die von böswilligen Akteuren ausgenutzt werden können. Daher sind verschiedene Arten von Endgeräteschutz erforderlich, darunter Antiviren-Lösungen, Internet of Things (IoT)-Sicherheit, Netzwerkzugriffskontrollen, Erkennung von und Reaktion auf Angriffe, Verschlüsselung und Sandboxing, um nur einige zu nennen. Es gibt zahlreiche Funktionen, die Endgerätesicherheit haben kann, wie z. B. ....

- .... die Verhinderung von Datenverlusten (Data Loss Prevention – DLP),
- Schutz vor Insider-Bedrohung,
- Endgeräterkennung und Reaktion,
- Verschlüsselung (E-Mail, Kommunikation, Festplatte),
- Whitelisting oder Kontrolle der Anwendung,
- Netzzugangskontrolle (Network Access Control – NAC),
- Datenklassifizierung sowie

- Kontrolle privilegierter Benutzer.

Mitunter ist der Schutz von Endpunktgeräten in der Software von Drittanbietern enthalten, er kann aber auch in die Entwicklung der Hardware selbst oder in das Konzept der „Security by Design“ einbezogen werden. Dieser Baustein der IT-Sicherheit muss bei der Entwicklung von IT-Sicherheitsprogrammen oder -strategien ernst genommen werden. Im Folgenden wird die Kombination der vorgestellten Endpunkte erläutert.

Die einfachste Möglichkeit, Endgerätesicherheit in Aktion zu erklären, ist der Schutz von PCs oder Laptops – den in Unternehmen am häufigsten verwendeten Endgeräten. Wenn wir diese Geräte schützen, sichern wir nicht nur die darauf gespeicherten Daten, sondern zugleich auch das gesamte Unternehmensnetzwerk. Dies wiederum bedeutet, dass viele Funktionen implementiert werden müssen, um dieses Sicherheitsniveau zu erreichen.

Bei der Sicherung von Daten und der Verhinderung von Datenverlusten (Data Loss Prevention oder DLP) müssen wir zunächst Informationen priorisieren, kategorisieren (klassifizieren) und kennzeichnen, da nicht alle Informationen den gleichen Grad an Sensibilität aufweisen. Dies geschieht durch ein unternehmensinternes Verfahren, z. B. gemäß ISO 27001, Anhang A.8.2.1 und A.8.2.2. Typische Klassifizierungsstufen im öffentlichen Sektor sind öffentlich, intern, geheim und streng geheim. Im privaten Sektor werden häufig die Stufen öffentlich, intern, vertraulich und privat verwendet. Danach muss das Risiko gesteuert und ein Verfahren zur Überwachung der Datenbewegungen festgelegt werden. Typischerweise gibt es immer eine Art von Überwachung, genannt Logging, wie z. B. ein SIEM. Die Protokollierung des Datenflusses ist in diesem Prozess sehr wichtig, da die einzige Möglichkeit, angemessene Informationen über auftretende oder bereits eingetretene Sicherheitsvorfälle zu erhalten, in der Datenanalyse liegt.

Ebenso wichtig ist der Schutz vor einer externen Bedrohung wie Malware und böswilligen Aktivitäten, der immer Teil der Unternehmenspolitik sein sollte, einschließlich lokaler Virenschutzmaßnahmen, zentralisierter Überwachung und Antiviren-Management. Firewall-Schutz wird sehr oft mit Anti-Malware kombiniert, um den Zugriff auf und von externen Ressourcen zu schützen. Netzwerksicherheit und Datenschutz werden nicht nur durch Firewalls und Regeln implementiert, sondern auch durch Verschlüsselung, Proxy und VPNs. In einer Situation, in der wir unsere Daten und Informationen auf unseren Endgeräten oder den Fluss unserer Daten über das Netzwerk verteidigen und schützen wollen, werden wir Kryptografie- und Verschlüsselungsfunktionen einsetzen. Dabei kann es sich um eine Teilverschlüsselung von „streng geheim“ klassifizierten Daten sowie um eine Verschlüsselung der gesamten Festplatte (eine sehr häufige Situation) oder um eine des Datenflusses über das Netzwerk mit einem VPN handeln.

## 4.3 IT-Sicherheit in Netzwerken

Die Netzwerksicherheit konzentriert sich auf die Sicherheit von Kommunikationsnetzen. Sie besteht aus Richtlinien, Verfahren und Praktiken zur Überwachung, Verhinderung und Abwehr von unbefugtem Zugriff, Missbrauch, Modifikation oder Dienstverweigerung (Denial of Service) und umfasst eine Vielzahl von Computernetzwerken – öffentliche und

private, LAN, WAN und andere, die bei der täglichen Arbeit verwendet werden. Bei den Netzwerken kann es sich um private Firmen- wie auch um öffentlich zugängliche Netzwerke handeln.

IT-Sicherheit in Netzwerken besteht aus Schutz-, Erkennungs- und Reaktionsphasen. Schutz bedeutet, dass Systeme und Netzwerke mit implementierten Sicherheitsmaßnahmen so korrekt wie möglich konfiguriert werden müssen. Die Erkennung stellt fest, ob sich die Konfiguration geändert hat oder ein Teil des Netzwerkverkehrs auf ein Problem hinweist. Die Reaktion bezieht sich auf ein Problem und die schnellstmögliche Rückkehr zu einem sicheren Zustand. Heutzutage empfehlen die meisten IT-Sicherheits-Frameworks wie NIST und CSF, mit diesen Phasen zu arbeiten.

Zu den üblichen Methoden und Techniken gehören u. a. die folgenden:

- Die **Zugangskontrolle** blockiert den Zugriff nicht autorisierter Benutzer und Geräte auf das Netzwerk. Benutzer, denen der Netzwerkzugriff gestattet ist, sollten nur mit den begrenzten Ressourcen arbeiten können, für die sie autorisiert wurden (Prinzip „need to know/need to access“).
- **DLP (Data Loss Prevention)** implementiert Prozesse, die sicherstellen, dass Daten nicht aus dem Netzwerk exfiltriert werden.
- **Firewalls** folgen den Regeln, die definieren, wem der Netzwerkverkehr zwischen dem Netzwerk und dem Internet (militarisierte und demilitarisierte Zone) gestattet oder verweigert wird. Sie errichten eine Barriere zwischen vertrauenswürdigen und nicht vertrauenswürdigen Sites.
- Das **Intrusion Detection and Prevention System (IDS/IPS)** scannt den Netzwerkverkehr, um Angriffe zu identifizieren und zu blockieren, oft durch Korrelation von Signaturen der Netzwerkaktivität mit Datenbanken bekannter Angriffstechniken.
- Software-definierte Segmentierung (**Netzwerksegmentierung**) ordnet den Netzwerkverkehr in verschiedene Klassifizierungen ein und erleichtert die Durchsetzung von Sicherheitsrichtlinien.
- **SIEM-Produkte** zielen darauf ab, Informationen aus einer Vielzahl von Netzwerk-Tools automatisch zusammenzuführen, um die notwendigen Daten zur Erkennung von und Reaktion auf Bedrohungen bereitzustellen.
- **Virtuelle Private Netzwerke (VPN)** sind Systeme (typischerweise basierend auf IPsec oder SSL), die die Kommunikation zwischen einem Gerät und einem sicheren Netzwerk schützen und einen sicheren, verschlüsselten „Tunnel“ über das offene Internet schaffen.
- Die **Web-Sicherheit** kontrolliert die Web-Nutzung durch interne Mitarbeiter, um zu verhindern, dass webbasierte Bedrohungen Browser als Vektor zur Infizierung Ihres Netzwerks verwenden (Fruhlinger 2018).

Das Vorfallmanagement (Incident Management) umfasst proaktive und reaktive Prozesse, damit Vorfälle erkannt und anschließend behandelt werden können. Oft hilft ein SIEM-System, und ein Security Operations Center (SOC) bearbeitet den Vorfall. Das Team, das zur Behandlung eines konkreten Vorfalls aus mehreren (IT-)Experten besteht, ist ein Computer Emergency Response Team (CERT). Es gibt verschiedene Vorfallsmodelle und -prozesse, die typischerweise der nachstehenden Struktur folgen:

- Erkennung:** Eine Organisation muss erkennen, dass sich ein tatsächlicher Vorfall ereignet, z. B. ein Angriff. Sensoren und SIEM-Systeme helfen bei der Erkennung eines Vorfalls.
- Reaktion:** Der nächste Schritt ist die Festlegung der Reaktion. In der Regel werden in dieser Phase mehr Daten gesammelt und analysiert, um angemessen reagieren zu können. Auch empfiehlt es sich nicht, zu diesem Zeitpunkt blind IPS- oder Firewall-Regeln zu ändern, da zunächst verstanden werden muss, was ein Angreifer will, wer er ist und welche Methoden er anwendet.
- Milderung:** Der nächste Schritt besteht darin, den durch den Vorfall verursachten Schaden zu mildern oder einzudämmen. Ziel ist es, weiteren Schaden durch diesen Vorfall zu verhindern oder zu reduzieren. Die Schadensbegrenzung erfolgt nach Priorität, sodass Informationen von hohem Wert (z. B. sensible PII) zuerst zurückgehalten und geschützt werden.
- Berichterstattung:** Die Berichterstattung und Dokumentation von Vorfällen erfolgen während des gesamten Prozesses. Oftmals meldet zunächst jemand anderes ein ungewöhnliches Verhalten eines Systems, daraufhin wird das CERT-Team eingeschaltet. Die Dokumentation des Vorfalls spielt auch eine Rolle bei Rechtsstreitigkeiten oder wenn im Nachhinein eine IT-Sicherheits-Versicherung eingeschaltet werden muss.
- Reaktivierung:** Sobald der Vorfall abgeschwächt ist, müssen alle Systeme und Informationen wieder aktiviert werden. Davor müssen jedoch Beweise für die weitere Forensik gesammelt werden. Diese Phase umfasst die Behebung der durch den Vorfall entstandenen Schäden.
- Lernen:** In der letzten Phase eines Zwischenfalls wird sichergestellt, dass der Angriff kein zweites Mal erfolgreich sein kann. Hier wird entschieden, welche Maßnahmen umgesetzt werden, wie z. B. Firewall-Einstellungen. Zu lernen, was schiefgelaufen ist und besser gemacht werden kann, ist ebenfalls eine wichtige Maßnahme in dieser Phase.

Authentifizierung, Autorisierung und Abrechnung sind wichtige Anforderungen während einer Fernzugriffssitzung (remote access session – RAS).

Ein zentraler Authentifizierungsdienst für Einwahl-Benutzer ist der Standard Remote Authentication and Dial-In User Service (RADIUS). RADIUS umfasst einen Authentifizierungsserver und dynamische Kennwörter. Das RADIUS-Protokoll ist ein offenes, leichtgewichtiges, UDP-basiertes Protokoll und kann so modifiziert werden, dass es mit einer Vielzahl von Sicherheitssystemen zusammenarbeiten kann. Es bietet Authentifizierungs-, Autorisierungs- und Abrechnungsdienste für Router, Modemserver und drahtlose Anwendungen. RADIUS wird in RFC 2865 beschrieben. Das NAS stellt dem RADIUS-Server auch Abrechnungsinformationen für Dokumentationszwecke zur Verfügung (Cole/Krutz/Conley 2005). Eine verbesserte Version des RADIUS-Protokolls wurde als DIAMETER-Protokoll veröffentlicht.

Das Terminal Access Controller Access Control System (TACACS) ist ein Authentifizierungsprotokoll. Es bietet Fernzugriffsauthentifizierung und zugehörige Dienste (Ereignisprotokollierung) an.

Ein weiterer Authentifizierungsmechanismus ist das Password Authentication Protocol (PAP). Dabei stellt ein Benutzer einen unverschlüsselten Benutzernamen und ein Passwort zur Verfügung. Diese werden mit den entsprechenden Informationen verglichen, die in einer Datenbank von autorisierten Benutzern (Muster) gespeichert wurden. Das Challenge Handshake Authentication Protocol (CHAP) ist im RFC-1994-Standard ausführlich beschrieben, bietet aber, kurz gesagt, eine Authentifizierung nach der Herstellung der anfänglichen Kommunikationsverbindung zwischen dem Benutzer und CHAP (ebd.).

Eine weitere Methode der Fernauthentifizierung ist der Rückruf. Beim Callback wählt sich ein Remote-Benutzer in den Authentifizierungsserver ein, gibt eine ID und ein Passwort ein und legt dann auf. Der Authentifizierungsserver sucht die ID des Anrufers in einer Datenbank autorisierter Benutzer und erhält eine Telefonnummer an einem festen Standort. Der Authentifizierungsserver ruft die Telefonnummer an und der Benutzer antwortet, woraufhin er Zugriff auf das System erhält (ebd.).

Das Extensible Authentication Protocol (EAP) ist eine Erweiterung von Punkt zu Punkt und wird in IEEE 802.1x beschrieben. Seine Hauptaufgabe besteht darin, eine Verbindung mit Punkt-zu-Punkt oder den Zugang zum Netzwerk zu sichern, was nur nach Authentifizierung möglich ist.

## 4.4 Entwicklung sicherer IT-Systeme

**IT-Sicherheitsplan**  
Ein IT-Sicherheitsplan muss in die IT-Sicherheits- und Unternehmensstrategien integriert werden.

**Gemeinsame Kriterien**  
Diese können als Leitfäden oder Vorlage für die Entwicklung von IT-Sicherheitssystemen verwendet werden.

Die erste Voraussetzung für ein sicheres IT-System ist ein **IT-Sicherheitsplan**. Dieser ist immer Teil einer IT-Sicherheitsstrategie, welche mit der Unternehmensstrategie kompatibel sein muss. In diesem Abschnitt werden die **Common Criteria (CC)** und die Evaluationsicherheitsstufe beschrieben, die die technische Grundlage für die Evaluierung und Zertifizierung der Produktsicherheit bilden. Am Ende dieses Abschnitts werden zwei Beispiele für gute Praktiken vorgestellt – das Open Web Application Security Project (OWASP) und die Development Security Operation (DevSecOps).

Die Gemeinsamen Kriterien für die Bewertung der Sicherheit von Informationstechnologien (CC) sind die technische Grundlage für ein internationales Abkommen, das Common Criteria Recognition Arrangement (CCRA), das sicherstellt, dass ...

- ... Produkte von kompetenten und unabhängigen lizenzierten Laboratorien evaluiert werden, um die Erfüllung bestimmter Sicherheitseigenschaften bis zu einem gewissen Grad oder eine gewisse Sicherheit festzustellen.
- im Rahmen des Zertifizierungsprozesses nach Common Criteria Begleitdokumente verwendet werden, um festzulegen, wie die Kriterien und Bewertungsmethoden bei der Zertifizierung bestimmter Technologien angewandt werden.
- die Zertifizierung der Sicherheitseigenschaften eines evaluierten Produkts von mehreren Zertifizierungs-Autorisierungsschemata ausgestellt werden kann, wobei diese Zertifizierung auf dem Ergebnis ihrer Evaluation basiert.
- diese Zertifikate von allen Unterzeichnern der CCRA anerkannt werden (Common Criteria 2017).

Die CC können als Leitfaden für die Entwicklung, Evaluierung und/oder Beschaffung von IT-Produkten mit Sicherheitsfunktionalität verwendet werden. CC ist in der ISO-Norm ISO/IEC 15408 beschrieben. Die in der CC-Domäne verwendeten Grundbegriffe sind einerseits der Evaluationsgegenstand mit den Erwartungen an seine Sicherheit, andererseits Anforderungen daran, wie diese Sicherheit erreicht und bewertet wird:

- Evaluationsgegenstand (Target of Evaluation – TOE) – das Produkt oder System, das Gegenstand der Evaluation ist und außerdem die folgenden Sicherheitsmerkmale aufweist:
  - Schutzprofil (Protection Profile – PP) – ein Dokument, das Sicherheitsanforderungen, z. B. für Ausrüstung, beschreibt;
  - Sicherheitsvorgaben (Security Target – ST) – ein Dokument, das die Sicherheitseigenschaften der Evaluationsvorgaben identifiziert;
  - Sicherheitsfunktionsanforderungen (Security Functional Requirement – SFR) – diese spezifizieren einzelne Sicherheitsfunktionen, die von einem Produkt bereitgestellt werden können.

Die Qualität des TOE kann erreicht und bewertet werden durch:

- Security Assurance Requirements (SAR) sind Maßnahmen, die während der Entwicklung und Evaluierung des Produkts ergriffen werden, um die Übereinstimmung mit der beanspruchten Sicherheitsfunktionalität zu gewährleisten.
- Evaluation Assurance Level (EAL) ist die numerische Bewertung, die die Tiefe und Strenge einer Evaluation beschreibt (Common Criteria 2017). Common Criteria listet sieben EAL-Stufen auf, wobei EAL 1 die grundlegendste und EAL 7 die strengste Stufe ist:
  - EAL1 – funktionell getestet;
  - EAL2 – strukturell getestet;
  - EAL3 – methodisch getestet und überprüft;
  - EAL4 – methodisch entworfen, getestet und überprüft;
  - EAL5 – semi-formal entworfen und getestet;
  - EAL6 – semi-formal verifizierter Entwurf, getestet;
  - EAL7 – formal verifizierter Entwurf, getestet.

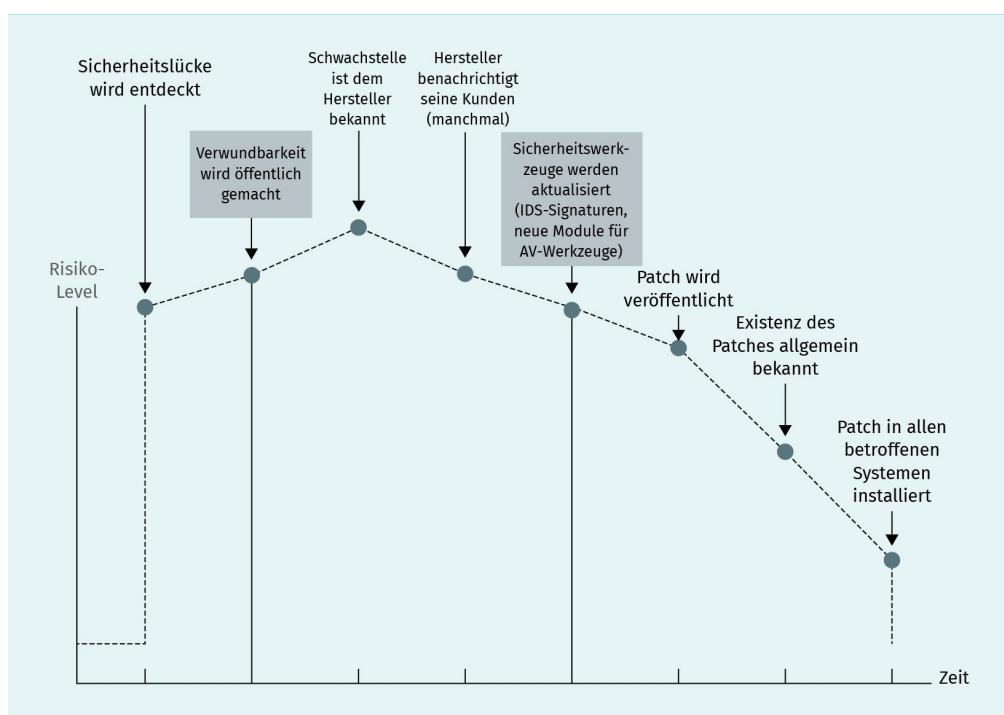
Ein höherer EAL bedeutet nicht unbedingt, dass die Produkte sicherer sind, sondern vielmehr, dass eine gründlichere Verifizierung durchgeführt wurde. Um die CC-Zertifizierung besser zu verstehen, sind im Folgenden Beispiele für einige Schritte aufgeführt, die Unternehmen durchführen müssen, um CC-zertifiziert zu werden:

- Sicherheitsvorgaben (ST) und andere unterstützende Dokumente, wie z. B. ein Überblick über die Produkte mit Schwerpunkt auf Sicherheitsmerkmalen und potenziellen Sicherheitsbedrohungen, müssen vollständig sein.
- Eine Selbsteinschätzung mit Dokumentation über die Art und Weise, wie Produkte mit der Struktur des Schutzprofil- und des Evaluation Assurance Level Tests übereinstimmen, muss abgeschlossen werden.
- Die Bewertung der Produkte muss in einem unabhängigen, lizenzierten Labor durchgeführt werden. Es muss nachgewiesen werden, dass das Sicherheitsniveau der Produkte auf einem „angemessenen Niveau“ liegt.

- Wenn das Produkt die Evaluation besteht und sein Sicherheitsniveau zufriedenstellend ist, wird die Zertifizierung durch ein Certificate Authorizing Scheme (CAS) erteilt.

Eine weitere Möglichkeit, ein sicheres IT-System aufzubauen, ist die Verwendung des OWASP Security Knowledge Framework. Es kann als Leitfaden für Aufbau und Verifikation von sicherer Software verwendet werden. Im Lebenszyklus der Entwicklung sicherer Software ist die Ausbildung der erste Schritt, daher ist dieses Framework nützlich, wenn Entwickler zur Anwendungssicherheit geschult werden.

**Abbildung 8: Konzept der Verwundbarkeit (Höhe des Risikos)**



Quelle: OWASP 2017.

Der Quellcode einer Anwendung muss gut und sicher sein, aber was ist ein guter und sicherer Quellcode? Eine der Organisationen, die gute Kodierungsstandards entwickeln, ist das Software Engineering Institute (SEI) der Carnegie Mellon University. Die zehn sichersten Kodierungspraktiken gemäß dem SEI sind (Seacord 2018):

1. **Eingabe validieren:** Validieren Sie Eingaben aus allen nicht vertrauenswürdigen Datenquellen.
2. **Warnungen des Compilers beachten:** Kompilieren Sie Code mit der höchsten für Ihren Compiler verfügbaren Warnstufe und beseitigen Sie Warnungen durch Modifizieren des Codes.
3. **Architektur und Entwurf der Sicherheitsrichtlinie:** Erstellen Sie eine Software-Architektur und darauf aufbauend Ihre Software zur Implementierung und Durchsetzung von Sicherheitsrichtlinien.

4. **In der Kürze liegt die Würze:** Halten Sie den Entwurf so einfach und kurz wie möglich.
5. **standardmäßig verweigern:** Zugriffsentscheidungen auf Erlaubnis statt auf Ausschluss basieren.
6. **Prinzip des geringsten Privilegs:** Jeder Prozess sollte mit den geringsten Privilegien (Berechtigungen) ausgeführt werden, die zur Ausführung des Auftrags erforderlich sind.
7. **an andere Systeme gesendete Daten prüfen:** Reinigen Sie alle an komplexe Subsysteme übermittelten Daten. Der aufrufende Prozess versteht den Kontext und ist dafür verantwortlich, die Daten vor dem Aufruf des Subsystems zu überprüfen.
8. **Beantwortung von Angriffen eingehend üben:** Managen Sie Risiken mit mehreren Verteidigungsstrategien, sodass, wenn sich eine Verteidigungsebene als unzureichend erweist, eine andere verhindern kann, dass ein Sicherheitsmangel zu einer ausnutzbaren Schwachstelle wird und/oder die Folgen einer erfolgreichen Ausnutzung begrenzt.
9. **wirksame Qualitätssicherungstechniken verwenden:** Gute Qualitätssicherungstechniken können bei der Identifizierung und Beseitigung von Schwachstellen wirksam sein. Fuzzy-Tests, Penetrationstests und Quellcode-Audits sollten alle als Teil eines wirksamen Qualitätssicherungsprogramms einbezogen werden.
10. **sicheren Kodierungsstandard einführen:** Entwickeln und/oder wenden Sie einen sicheren Kodierungsstandard für Ihre Entwicklungszielsprache und -plattform an.

Das SEI veröffentlicht auch sichere Kodierungspraktiken für viele Programmiersprachen, darunter Java, C oder C++.

Ein weiterer guter Ansatz, der dazu beiträgt, „alle für die Sicherheit verantwortlich zu machen“, ist DevSecOps – eine Erweiterung des bekannten Konzepts DevOps. Erfolgreiche Sicherheitsprogramme umfassen drei sich überschneidende Teile: Menschen, Prozesse und Technologien. DevSecOps ist in dieser Hinsicht nicht anders, erkennt aber an, dass in einer Organisation jeder für die Sicherheit verantwortlich ist und eine Rolle in der Sicherheit innehat. Das heißt, dass der Mensch bei der Durchführung von DevSecOps oberste Priorität hat. Die Einstellung von Sicherheitsspezialisten und -experten, die ihnen eine Stimme bei der Projektdurchführung geben und ermöglichen, ihre Prozesse in die agile Entwicklungswelt zu integrieren, wird die erforderlichen Ergebnisse liefern. Agile Entwicklung trägt dazu bei, Produktfreigabetermine zu beschleunigen, wenngleich häufig auf Kosten der Sicherheit. Durch die Ernennung und gute Ausbildung von Sicherheitsverantwortlichen wird zudem gewährleistet, dass die Sicherheit in einer Organisation Priorität hat. Obwohl der Mensch im Mittelpunkt steht, sind auch die Prozesse der Schlüssel zum Erfolg von DevSecOps. Versionskontrolle, Metadaten, Orchestrierung, Integration, Konformität, Sicherheitsarchitektur, Vorfallmanagement und Aufklärung über Bedrohungen sind nur einige der Hauptprozesse bei der Implementierung von DevSecOps. Das Endziel ist es, über Technologien zu verfügen, die es den Menschen ermöglichen, DevSecOps-Prozesse korrekt auszuführen (Raynaud 2017).

Eine weitere wichtige Reihe von Standards zur Informationssicherheit ist die Normenfamilie ISO 27000, insbesondere die ISO 27001. Sie liefert die ISMS-Spezifikation (Information Security Management System) mit Anhang A (eine Checkliste), während der zweite Teil ISO 27002 „Code of Practice“ ist, im Wesentlichen ein Leitfaden, der aus den besten Informatiionssicherheitspraktiken aus der ganzen Welt besteht. ISO 27001 und 27002 sind miteinan-

der verbunden, denn wenn Organisationen Kontrollen nach Anhang A verwenden, bietet ISO 27002 ihnen einen Weg, diese Kontrollen zu implementieren (siehe ISO/IEC 27701:2019).

Die Kontrolle A14.2 in der ISO 27001-Norm über die Sicherheit in Entwicklungs- und Unterstützungsprozessen hat das Ziel, sicherzustellen, dass die Informationssicherheit innerhalb des Entwicklungslebenszyklus von Informationssystemen entworfen und implementiert wird. Die Anforderungen bestehen aus:

- A.14.2.1 Sichere Entwicklungsrichtlinie,
- A.14.2.2 Kontrollverfahren für Systemänderungen,
- A.14.2.3 Technische Überprüfung von Anwendungen nach Änderungen der Betriebsplattform,
- A.14.2.4 Einschränkungen für Änderungen an Softwarepaketen,
- A.14.2.5 Grundsätze der sicheren Systemtechnik,
- A.14.2.6 Sichere Entwicklungsumgebung,
- A.14.2.7 Ausgelagerte Entwicklung,
- A.14.2.8 Prüfung der Systemsicherheit und
- A.14.2.9 Systemakzeptanzprüfung.

Zusätzlich gibt es Anforderungen in der IEC 62443-4-1. Diese Norm beschreibt das Sicherheitsmanagement, den Entwicklungsprozess und alle Sicherheitsanforderungen im Lebenszyklus von IT-Produkten in der Industrie.

Eine Voraussetzung für ein sicheres IT-System ist ein Sicherheitsframework (Rahmenwerk). Im Folgenden soll auf die wichtigsten und am häufigsten verwendeten IT-Sicherheitsrahmenwerke eingegangen werden: NIST CSF, ISO 27k, NIST 800-53 und IEC 62443.

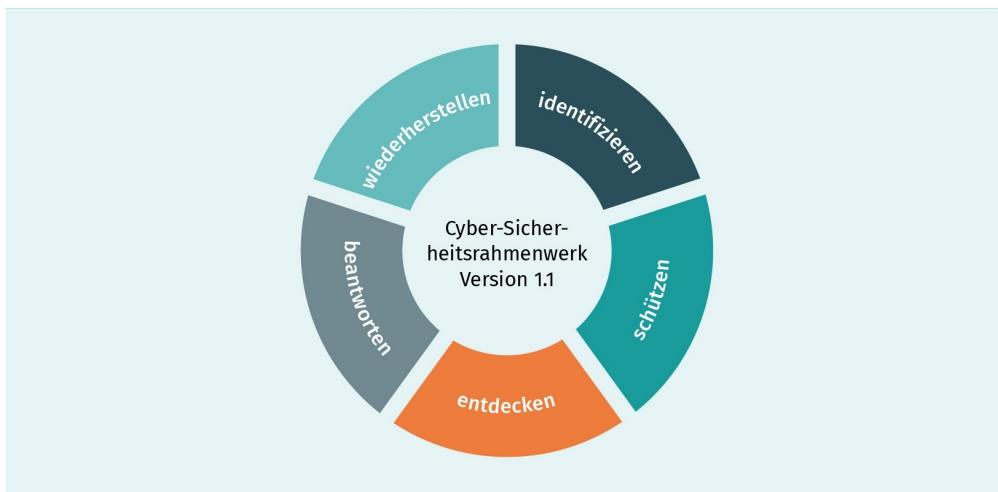
Heutige IT-Sicherheitsmodelle sind von Modellen der Computersicherheit aus einer Zeit abgeleitet, in der die IT in Form von Einzelcomputern existierte, die möglicherweise in einem lokalen Netzwerk verbunden waren, jedoch ohne Internet, Cyberspace und die heutigen Dienste und Technologien. Computersicherheitsmodelle boten ein Schema für die Spezifikation und Umsetzung von Sicherheitsrichtlinien und waren in der Tat formale Beschreibungen von Sicherheitsrichtlinien.

Das Cybersecurity Framework ist ein Produkt des NIST und liegt seit April 2018 in der aktuellen Version 1.1 vor. Es ist ein risikobasierter Ansatz und besteht aus den folgenden drei Komponenten:

- Kernstück ist ein Rahmenwerk, das sich aus einer Reihe von IT-Sicherheitsaktivitäten, gewünschten Ergebnissen und anwendbaren Referenzen zusammensetzt, die für kritische Infrastruktursektoren üblich sind. Die Box selbst besteht aus fünf konkurrierenden und konstanten Funktionen – Identifizieren, Schützen, Aufspüren, Reagieren und Wiederherstellen.
- Die Ebene der Rahmenimplementierung bietet Inhalt und eine Möglichkeit für eine Organisation, sich anzunähern und zu handeln, um das Risiko zu managen.

- Rahmenwerkprofile stellen in der Tat Ergebnisse dar, die auf Geschäftsbedürfnissen basieren und von der Organisation innerhalb des Rahmenwerks selbst ausgewählt werden (NIST 2018).

**Abbildung 9: NIST-Rahmen für IT-Sicherheit**



Quelle: NIST 2018.

Ein praktisch anwendbares Merkmal des Rahmens selbst ist, dass er eine vollständige Liste von Funktionen, Kategorien, Unterkategorien und informativen Verweisen bietet, welche die in allen kritischen Infrastrukturbereichen am häufigsten vorkommenden spezifischen IT-Sicherheitsaktivitäten beschreiben.

Das NIST gab die Publikation 800-53 als Teil einer Sonderreihe von NIST-800-Publikationen heraus, einem Katalog von 20 Sicherheits- und Datenschutzkontrollgruppen. Kontrollgruppen werden als sehr flexibel und anpassungsfähig an Nutzer oder Organisationen unterschiedlicher Profile konzipiert und implementiert. Sie werden meist als Kontrollen für Strategien des Risikomanagements eingesetzt. Die von den Kontrollen abgedeckten Bereiche sind: Zugangskontrolle, Sicherheitsbewusstsein, Risikobewertung, Reaktion auf Vorfälle und Überwachung (NIST 2020).

Critical Security Controls (CIS) ist ein vom SANS-Institut entwickeltes Produkt, das darauf abzielt, eine Reihe von Aktionen/Aktivitäten zur Cyberabwehr zu veröffentlichen. Das Dokument listet 20 Kontrollen auf, priorisiert als Hardware, Software, Konfiguration, Malware-Abwehr, Datenwiederherstellung, Kontenüberwachung, Reaktion auf Vorfälle, Pen-Test und Training für das rote Team (CIS o. J.).

Die Normenreihe IEC 62443 wurde vom ISA99-Komitee (Industrial Standard for Automation) und der IEC (International Electrotechnical Commission) entwickelt, um die Notwendigkeit der Entwicklung eines IT-Sicherheitsrahmens für das Industrial Automation Control System (IACS) hervorzuheben. Ziel der Anwendung dieser Normenreihe ist es, die Sicherheit, Verfügbarkeit, Vertraulichkeit und Integrität der Systemkomponenten sowie des Systems als Ganzes zu verbessern. Die Anforderungen des Standards selbst sollen nicht bloß die elektronische Sicherheit verbessern, sondern auch Schwachstellen identifi-

**ICS, SCADA**  
Industrial Control Systems (ICS) und Supervisory Control and Data Acquisition (SCADA) Systeme steuern und kontrollieren industrielle IT, wie z. B. Fertigungsanlagen oder Kraftwerke.

zieren und aufzeigen, während gleichzeitig das Risiko einer Beeinträchtigung der Information, der Vertraulichkeit sowie von Beeinträchtigung oder Ausfall der kontrollierten Ausrüstung (Hardware oder Software) minimiert wird.

Das Normenwerk wurde für **ICS-, SCADA-** und IACS-Systeme (Industrie) konzipiert und implementiert und besteht aus 13 Normen, die wie folgt in Gruppen unterteilt sind:

- allgemein (62443-1-1, 62443-1-2, 62443-1-3, 62443-1-4),
- Richtlinie und Verfahren (62443-2-1, 62443-2-2, 62443-2-3, 62443-2-4),
- System (62443-3-1, 62443-3-2, 62443-3-3) sowie
- Komponente (62443-4-1, 62443-4-2).

Wie erwähnt gibt es bei der Auswahl von Modellen und Rahmenwerken für die IT-Sicherheit eine Reihe verschiedener Ansätze, jedoch ist die Verallgemeinerung und der einheitliche Ansatz bei der Auswahl des richtigen Modells oder Rahmens fragwürdig. IT-Sicherheit wird von kleinen, mittleren und großen Unternehmen, Organisationen, Verwaltungen, Industrien, der Zivilgesellschaft und Universitäten benötigt – jede dieser Einrichtungen hat seine eigenen Besonderheiten. Sie könnten unterschiedliche Anforderungen an Größe, Domäne und Bereich des Unternehmens, der Aktivität, der angebotenen Dienstleistungen und der hergestellten Produkte stellen. Daraus ergibt sich die Notwendigkeit eines maßgeschneiderten Ansatzes bei der Auswahl eines Rahmens oder eines IT-Sicherheitsmodells (VDE 2019).



### ZUSAMMENFASSUNG

Es ist nicht einfach, über IT-Sicherheitsbausteine zu sprechen, denn es gibt unzählige Konzepte und Ansätze zum Umgang mit IT-Sicherheit. In dieser Lektion wurde erklärt, wie man die wichtigsten Konzepte im Bereich der IT-Sicherheit auswählt und wesentliche Bausteine erkennen kann.

Bei der Wahl eines geeigneten IT-Sicherheitsrahmens ist es sehr wichtig zu wissen, welcher Art von Unternehmen oder Organisation er dienen soll. Manchmal kann nur das ISO-27k-Framework verwendet werden, manchmal ist das IEC-62443-Framework erforderlich. Andere Situationen erfordern es, NIST CSF, IEC 62443 und ISO 27k zu kombinieren.

Für den Aufbau eines IT-Sicherheitssystems ist ein erfahrenes Team von Experten für IT-Sicherheit vonnöten. Diese Gruppe empfiehlt zudem, wenn es an den Aufbau von IT-Sicherheitssystemen geht, die Verwendung der OWASP- und DevSecOps-Konzepte.

# LEKTION 5

## IT-SICHERHEITSMANAGEMENT

### LERNZIELE

Nach der Bearbeitung dieser Lektion werden Sie wissen, ...

- wie man IT-Sicherheit ganzheitlich verwaltet.
- welche Rolle die Sicherheitsrichtlinie spielt.
- wie das Risikomanagement zur Steuerung und Kontrolle der IT-Sicherheit eingesetzt werden kann.
- wie IT-Sicherheit und IT-Governance zusammenwirken.
- was der PCI-DSS-Standard ist und wie er das Sicherheitsmanagement umsetzt.

## 5. IT-SICHERHEITSMANAGEMENT

### Einführung

IT-Sicherheit ist heutzutage nicht nur eine wichtige Praxis innerhalb einer Organisation, sondern spielt auch bei deren Management eine entscheidende Rolle. Da Organisationen vollständig von der Vertraulichkeit, Integrität und Verfügbarkeit der Informationen abhängig werden, mit denen sie umgehen, hat die Dringlichkeit eines Sicherheitsmanagements auch für Branchen, die nicht direkt mit IT zu tun haben, weiter zugenommen. So ist es wichtig, das Unternehmen aus geschäftlicher Sicht zu verstehen, um zu gewährleisten, dass keine Sicherheitsvorfälle die kritischen Systeme eines Unternehmens bedrohen. Die Werkzeuge, Prozesse und Kontrollen, die zum Schutz der Informationswerte eines Unternehmens erforderlich sind, sind ebenso komplex wie die Informationssysteme, die sie schützen sollen.

Geschäftsziele, eine Strategie, Sicherheitsrichtlinien, Prioritäten, Standards, Prozesse, Kontrollen und Metriken beteiligen sich alle zusammen an der Förderung eines ganzheitlichen IT-Sicherheitsverwaltungsprogramms. Dies wird auch als Information Security Management System (ISMS) bezeichnet. Weiteres Risikomanagement trägt dazu bei, potenzielle negative Folgen in Bezug auf die CIA-Triade der IT-Sicherheit zu identifizieren und zu bewerten.

### 5.1 Sicherheitsrichtlinie

Die Entwicklung einer Sicherheitsrichtlinie ist eine grundlegende Komponente in jedem Sicherheitsmanagementsystem. Die Richtlinie definiert die Prinzipien und Maßnahmen, die erforderlich sind, damit die Organisation ihre Informationswerte und ihr Personal schützen kann.

Hauptpublikum einer Sicherheitsrichtlinie ist das Personal einer Organisation. Daher muss sie leicht zugänglich und lesbar sein, um mangelndes Expertenwissen nicht als Entschuldigung für Richtlinienverletzungen gelten zu lassen. Viele Organisationen verlangen, dass ihr Personal die Sicherheitsrichtlinie formell anerkennt, sowohl zu Beginn als auch während eines jährlichen Prozesses. Bestimmte Teile der Richtlinie können sich an unterschiedliche Zielgruppen richten. So können IT-Ingenieure durch technisch spezifischere Erklärungen angesprochen werden als andere einzelne Mitarbeiter in einer Organisation. Um effektiv zu sein, muss die Kommunikation der Richtlinie den organisatorischen Gegebenheiten folgen und kann z. B. durch Videoaufzeichnungen und die Erwähnung der Richtlinie bei regelmäßigen Treffen unterstützt werden. Zudem ist wichtig, dass die Geschäftsleitung mit gutem Beispiel vorangeht und in Übereinstimmung mit der Richtlinie handelt, da diese sonst leicht wirkungslos werden kann.

Die Sicherheitsrichtlinie muss mit den geltenden Gesetzen, Vorschriften, Normen und vertraglichen Verpflichtungen in Einklang gebracht werden. Der Datenschutz ist zu berücksichtigen und muss in die Unternehmenskultur passen.

## Steuerung und Kontrolle

Kontrollen sind formale Beschreibungen, Schutz- oder Gegenmaßnahmen, die dazu dienen, Risiken für die Informationsbestände der Organisation zu erkennen, zu vermeiden, ihnen entgegenzuwirken oder sie zu minimieren. Kontrollen können in drei Gruppen klassifiziert werden.

- **Präventive Kontrollen** verhindern das Auftreten eines unerwünschten Ereignisses. Beispiele hierfür sind Badge-Eingangssysteme oder Meldungen auf dem Anmeldebildschirm, die verhindern, dass unbefugte Personen ein Gebäude betreten oder auf ein IT-System zugreifen.
- **Überwachende Kontrollen** erfassen gute wie schlechte Ereignisse. Videoüberwachung oder Ereignisprotokolle eines Servers sind Beispiele für eine Überwachungskontrolle.
- **Abschreckende Kontrollen** überzeugen jemanden davon, nicht in einer bestimmten Weise zu handeln. Beispiele sind Warnschilder oder Wachhunde. Auch Videoüberwachungssysteme können abschreckend wirken, da es sich bei ihnen um detektivische Kontrollen handelt.

Darüber hinaus existieren drei Arten von Kontrollen:

1. **Physische Kontrollen** gibt es in der physischen Welt, wie z. B. Videoüberwachung, Türschlösser oder Zäune.
2. **Technische Kontrollen** werden in IT-Systemen implementiert, beispielsweise Zugangskontrollisten, Audit-Protokolle oder Verschlüsselungsmechanismen.
3. **Administrative (Management-)Kontrollen** sind Protokolle, Prozesse, Standards und Richtlinien, die eine bestimmte Aktivität verbieten oder erfordern. Beispiele dafür sind Regeln, die nur bestimmte Softwareinstallationen auf einem Gerät erlauben oder den Anschluss privater Geräte an das Netzwerk verbieten.

Die Sicherheitsrichtlinie muss mit den Kontrollen in Einklang stehen. Für jede politische Erklärung muss es eine Kontrolle geben und umgekehrt, jedoch dürfen sie zueinander nicht im Widerspruch stehen.

## Struktur der Sicherheitsrichtlinie

Die Sicherheitsrichtlinie kann auf viele Arten strukturiert werden. Die Entscheidung, ob die Richtlinie aus einem Dokument bestehen soll oder aus mehreren verschiedenen, die aufeinander verweisen, obliegt der Organisation. Im Allgemeinen sollte sie mit der Art und Weise übereinstimmen, wie andere Richtlinien veröffentlicht werden. Die Erklärung zur Sicherheitsrichtlinie sollte allgemein gehalten sein und keine spezifischen Geräte, Technologien oder Konfigurationen zitieren. Sie sollte angeben, was getan werden muss, und nicht, wie es getan werden muss. Auf diese Weise müssen die Erklärungen nicht so oft geändert werden. Es sind verschiedene Themen enthalten, so etwa:

1. akzeptable Nutzung
2. Anti-Virus/-Malware
3. mobile Geräte
4. Kennwort
5. Nutzung persönlicher Geräte (Bring Your Own Device – BYOD)
6. E-Mail und Kommunikation
7. soziale Medien
8. physische Sicherheit
9. Sicherheit in der Cloud
10. Sicherheitsvorfälle
11. Sicherheit von Lieferanten



### BEISPIEL

Ein Beispiel für eine Klausel in einer Sicherheitsrichtlinie im Zusammenhang mit dem Ereignismanagement lautet: „Ereignisprotokolle, die Benutzeraktivitäten, Ausnahmen, Fehler und Informationssicherheitsereignisse aufzeichnen, sollten erstellt, aufbewahrt und regelmäßig überprüft werden“.

## 5.2 Sicherheits- und Risikoanalyse

IT-Sicherheitsrisikomanagement ist die Praxis, ein Gleichgewicht zwischen Geschäftschan- cen und möglichen negativen Auswirkungen auf die IT-Sicherheit herzustellen. Es handelt sich dabei weitgehend um ein qualitatives Unterfangen, da es schwierig ist, Wahrscheinlichkeit und Auswirkungen potenzieller negativer Folgen eines Ereignisses zu quantifizieren. In diesem Lernzyklus werden nichtsdestoweniger mehrere quantitative Metriken vor- gestellt, wie sie zur Messung und zum besseren Verständnis des Umgangs mit Risiken festgelegt wurden.

### Bedrohungen, Schwachstellen und Risiken

Die folgenden Begriffe werden oft missverstanden und müssen klar definiert werden, um Risiken zu verstehen.

- **Wert:** Ein Wert ist das, was geschützt werden muss, z. B. Informationen, Menschen oder Eigentum. Es wird auch als „Asset“ bezeichnet.
- **Schwachstelle:** Eine Schwachstelle ist eine Schwäche oder Lücke im Schutz eines Gutes, die durch Bedrohungen ausgenutzt werden kann, um die CIA-Triade des Gutes zu beeinträchtigen.
- **Bedrohung:** Eine Bedrohung ist alles, was eine Schwachstelle ausnutzen kann. Sie beschädigt, erlangt oder zerstört ein Gut, sei es absichtlich oder unabsichtlich.

- **Risiko:** Ein Risiko ist die Schnittmenge aus einem Wert, einer Bedrohung und einer Verwundbarkeit. Es kann als Risiko = Wert + Bedrohung + Verwundbarkeit beschrieben werden. Eine andere, allgemeinere Definition beschreibt ein Risiko als einen potenziellen Schaden, der eine bestimmte Auswirkung und eine bestimmte Wahrscheinlichkeit des Eintretens hat.

Beispielsweise ist auf einem Windows-Server (dem Wert) nicht der neueste Patch installiert. Dies ist eine Schwachstelle. Ein Hacker (Bedrohungsakteur) kann versuchen, diese Schwachstelle auszunutzen, um Zugang zu der auf diesem Server gespeicherten Kunden-datenbank zu erhalten. Dies ist die Bedrohung. Das Risiko besteht in der Kombination eines nicht gepatchten Servers mit einem fehlenden Patch, das von einem Hacker ausgenutzt werden kann.

Microsoft schlägt das STRIDE-Modell zur Kategorisierung von Bedrohungen vor. Die Abkürzung STRIDE steht für (Microsoft 2009):

- Identitätsfälschung (**Spoofing**),
- Manipulation von Daten (**Tampering**),
- Nichtabstreitbarkeit (**Repudiation**),
- Offenlegung von Informationen (**Information Disclosure**),
- Dienstverweigerung (**Denial of Service**) sowie
- Erhöhung des Privilegs (**Elevation of Privilege**).

Das DREAD-Risikobewertungsmodell hingegen wurde ursprünglich geschaffen, um sowohl Bedrohungen als auch Risiken zu kategorisieren. Der Schöpfer, Microsoft, verwendet es selbst jedoch nicht mehr.

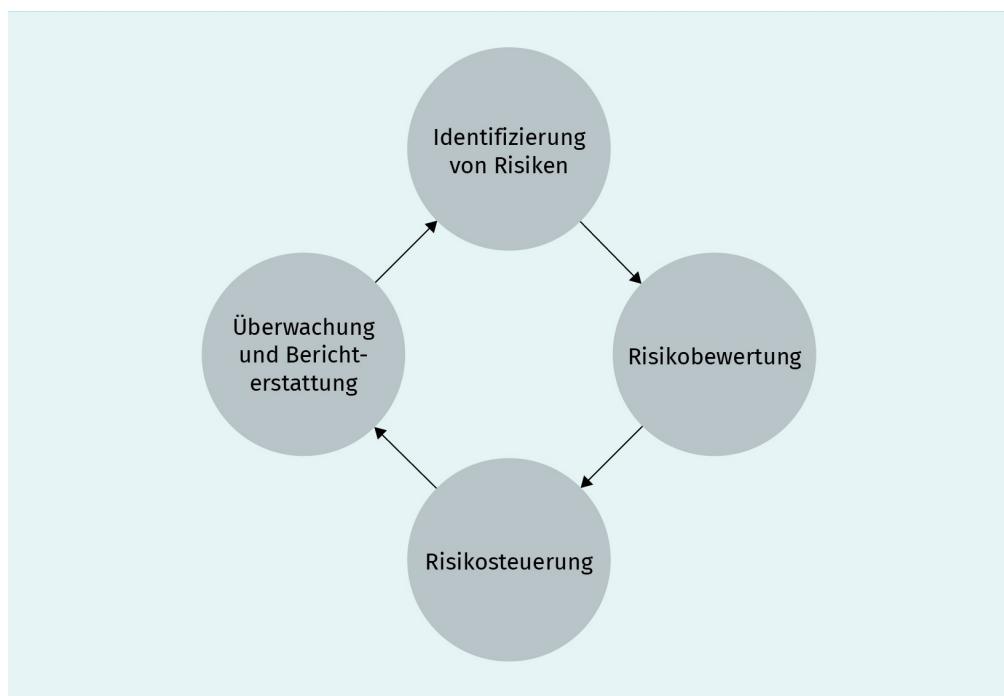
DREAD steht seinerseits für:

- Schaden (**Damage**) – wie schlimm wäre ein Angriff?
- **Reproduzierbarkeit** – wie leicht lässt sich der Angriff reproduzieren?
- Ausnutzbarkeit (**Exploitability**) – wie viel Arbeit ist es, den Angriff zu starten?
- Betroffene Nutzer (**Affected users**) – wie viele Menschen werden betroffen sein?
- Auffindbarkeit (**Discoverability**) – wie einfach ist es, die Bedrohung zu entdecken? (OpenStack o. J.).

Die OWASP-Top-10-Schwachstellen sind ein gutes Beispiel für typische Schwachstellen in Webanwendungen.

## Risiko-Management-Prozess

Abbildung 10: Ein Prozess des Risikomanagements



Quelle: Martin Macke, 2020.

Die obige Abbildung zeigt einen typischen Risikomanagementprozess. Im Risikoprogramm definiert eine Organisation den Umfang der Risikomanagementaktivitäten. Er umfasst i. d. R. die in den Geltungsbereich fallenden Geschäftsbereiche und geografischen Gebiete sowie andere Parameter. Während dieser Phase definiert eine Organisation auch ihren Risikoappetit oder ihre Risikotoleranz. Letztere drückt das Risiko aus, das eine Organisation einzugehen bereit ist. In den meisten Organisationen wird dies in qualitativen Begriffen beschrieben; in der Finanzindustrie (Banken, Versicherungen usw.) finden wir jedoch manchmal quantitative Begriffe. Es ist zu beachten, dass ein völlig risikofreies Geschäft nicht existiert und Risiko, als integraler Bestandteil von Geschäft und Leben, nicht unbedingt per se nur negativ ist.

Die Risikoidentifizierung ist der erste Schritt im iterativen Risikomanagementprozess. Die Organisation identifiziert Risiken, Schwachstellen und Bedrohungen. Der zweite Schritt ist die Risikobewertung, bei der mehrere Merkmale bestimmt werden. Diese sind die Wahrscheinlichkeit, dass das Risiko eintritt, die Auswirkungen, die das Risikoereignis haben würde, alle verfügbaren Risikominderungen sowie eine Empfehlung, wie dem Risiko begegnet werden kann.

Die Risikosteuerung ist i. d. R. der letzte Schritt des Risikomanagementprozesses. Ein Entscheidungsträger oder ein Risikoausschuss entscheidet, wie jedes spezifische Risiko zu behandeln ist. Die Optionen für die Risikobehandlung sind wie folgt:

- Akzeptanz:** Die Organisation beschließt, keine Maßnahmen bezüglich des Risikos zu ergreifen.
- Minderung:** Es werden Maßnahmen ergriffen, um die Auswirkungen, die Wahrscheinlichkeit oder beides auf ein akzeptables Maß zu reduzieren.
- Übertragung:** Ein Risiko wird auf eine dritte Partei übertragen, i. d. R. eine Versicherungsgesellschaft. Es gibt auch andere Formen, so etwa spezifische vertragliche Vereinbarungen mit Dritten, wie z. B. Lieferanten.
- Vermeiden:** Die Organisation entscheidet sich dafür, die mit dem Risiko verbundene Aktivität zu beenden. Dies ist oft die Option, wenn Geschäftsaktivitäten nicht mehr benötigt oder veraltete Systeme abgeschaltet werden.

Beachten Sie, dass Risikoignoranz keine gültige Risikobehandlungsoption ist.

### Qualitatives und quantitatives Risikomanagement

In der qualitativen Risikoanalyse können Wahrscheinlichkeit und Auswirkungen eines Ereignisses auf einer Skala ausgedrückt werden, die mit „hoch“, „mittel“ und „niedrig“ beschriftet ist. Dabei wird nicht versucht, den genauen Wert zu ermitteln, sondern üblicherweise beschrieben, was die verschiedenen Stufen bedeuten. Sie kann verwendet werden, um Risiken schnell in Beziehung zueinander zu verstehen. Die Abbildung unten zeigt eine typische qualitative Risikomatrix.

Abbildung 11: Qualitative Risikomatrix

Wahrscheinlichkeit	<b>hoch</b>	mittleres Risiko	hohes Risiko	hohes Risiko
	<b>mittel</b>	geringes Risiko	mittleres Risiko	hohes Risiko
	<b>niedrig</b>	geringes Risiko	geringes Risiko	mittleres Risiko
	<b>niedrig</b>	<b>mittel</b>	<b>hoch</b>	
	<b>Wirkung</b>			

Quelle: Martin Macke, 2020.

Da die Verwendung einer ungeraden Anzahl von Ebenen die Risiken oft zur Mitte hin tendieren lässt, wird häufig eine gerade Anzahl von Ebenen gewählt.

Auch semi-quantitative Methoden sind nicht unüblich. Diese können erreicht werden, indem den verschiedenen Ebenen Zahlen zugeordnet werden, z. B. 1 zu „niedrig“ und 3 zu „hoch“. Anschließend werden die Zahlen multipliziert, um ein Risikoniveau zu erhalten, wie z. B.: hohe Wahrscheinlichkeit · mittlere Wirkung = 3 · 2 = 6. In diesem Beispiel wäre das Risikoniveau also 6. Hier bestimmen die verschiedenen Werte nur das Risikoniveau im Verhältnis zueinander.

Bei der quantitativen Risikoanalyse werden die tatsächlichen Kosten und die Wahrscheinlichkeit von Ereignissen bestimmt. Es ist schwierig – wenn nicht gar unmöglich –, die erforderliche Genauigkeit zu erreichen, um für jedes Szenario die exakte Ereigniswahrscheinlichkeit zu ermitteln. Auch die genauen Kosten eines Ereignisses sind schwer zu bestimmen, da Vorfälle häufig komplex und die kurz- und langfristigen Ergebnisse nicht leicht vorherzusagen sind. Aufgrund dieser Herausforderungen sollte bei der quantitativen Risikoanalyse eher versucht werden, Schätzungen, wie z. B. Bandbreiten, als genaue Zahlen zu entwickeln.

Mehrere Zahlen können bei der Durchführung einer quantitativen Risikoanalyse hilfreich sein, wie z. B. die folgenden:

1. **Vermögenswert (AV – Asset Value):** Dies ist der Wert einer Anlage, der i. d. R. dem Wiederbeschaffungswert entspricht. Dies ist nicht der abgeschriebene Wert in einem Buchhaltungssystem, wie z. B. beim Ersetzen einer Anlage, insbesondere wenn es sich um immaterielles Vermögen handelt, das nicht durch die Buchhaltung ermittelt werden kann.
2. **Expositionsfaktor (EF):** Dies ist der finanzielle Verlust, der durch die Realisierung einer Bedrohung entsteht. Er wird normalerweise als prozentualer Wert eines Informationswertes ausgedrückt. Eine Bedrohung eliminiert i. d. R. nicht den gesamten Vermögenswert, sondern verringert ihn vielmehr. Verschiedene Bedrohungen haben unterschiedliche Auswirkungen und Expositionsfaktoren.
3. **Einzelverlusterwartung (SLE – Single Loss Expectancy):** Die SLE stellt den finanziellen Verlust bei einmaligem Eintreten eines Bedrohungsszenarios dar. Er ist definiert als  $SLE = AV \cdot EF$ .
4. **annualisierte Häufigkeitsrate (ARO – Annualized rate of occurrence):** Die ARO ist eine Schätzung, wie oft ein Ereignis innerhalb eines Jahres auftritt. Wenn die Wahrscheinlichkeit einer Bedrohung einmal in zehn Jahren liegt, beträgt die ARO 0,1.
5. **annualisierte Verlusterwartung (ALE – Annualized loss expectancy):** Dies ist der erwartete annualisierte Wertverlust des Vermögens aufgrund der Bedrohung. Er ist definiert als  $ALE = SLE - ARO$ .

Es gibt viele Risikorahmenwerke, wie z. B. ISO 27005, NIST SP 800-39 und FAIR OCTAVE. Sie alle verwenden quantitative, qualitative oder eine Kombination beider Ansätze.

### Ziele des Risikomanagements

Eine Vielzahl von Risikomanagement-Zielen wird i. d. R. verwendet, um die Ressourcen zu bestimmen, die zur Fortführung des Geschäftsbetriebs im Falle eines Ereignisses erforderlich sind. Sie stellen hauptsächlich unterschiedliche Zeitintervalle dar, bis Daten oder Systeme und Prozesse betriebsbereit sind. Die Unternehmensleitung ist an der Erstellung dieser Ziele beteiligt, da sich die Zeitintervalle direkt in den Betriebskosten niederschlagen. Daher trägt die Beteiligung der Unternehmensleitung dazu bei, angemessen in die richtigen Ressourcen zu investieren und Prioritäten auf der Grundlage der Geschäftsanforderungen zu setzen. Die typischen Zielparameter sind im Folgenden aufgeführt.

- Wiederherstellungszeit (RTO – Recovery time objective):** RTO ist der Zeitraum vom Beginn eines Ausfalls bis zur Wiederinbetriebnahme des Dienstes. Es ist ein messbares Zeitintervall, in dem die Wiederherstellungsaktivitäten stattfinden. Verschiedene Geschäftsprozesse haben unterschiedliche RTO-Ziele je nach ihrer Priorität für das Geschäft. Eine Business-Impact-Analyse (BIA) kann bei der Festlegung der RTO helfen.
- Wiederherstellungspunkt (RPO – Recovery point objective):** Der RPO ist der Zeitraum eines akzeptablen Datenverlusts aufgrund eines Vorfalls oder einer Katastrophe. Dies ist normalerweise der maximale Zeitraum zwischen Backups oder Replikationen in einem System. Normalerweise werden Stunden oder Minuten gemessen und wie beim RTO sind kürzere Zeiträume mit höheren Kosten verbunden.
- maximal tolerierbare Ausfallzeit (MTD – Maximum tolerable downtime):** Die MTD ist ein Zeitraum, nach dem das Überleben der Organisation gefährdet wäre. Organisationen beginnen häufig damit, diese Maßnahme zu definieren und anschließend RTO und RPO daraus abzuleiten. Die MTD ist nicht als Zielvorgabe zu interpretieren, sondern vielmehr als ein Punkt ohne Wiederkehr, nach dem das Unternehmen schließen müsste.

Abhängig von den Bedürfnissen der Organisation sind ggf. auch andere Zielparameter relevant.

## Das Risikoregister

Risikoregister variieren je nach Organisation. Die nachstehende Tabelle zeigt ein typisches Risikoregister mit einem Beispiel für einen Risikodatensatz.

**Tabelle 4: Risikoregister**

Punkt	Beschreibung	Beispiel
ID	eindeutige Kennung für den Risikodatensatz	15081
Stand	aktueller Status: offen, geschlossen, schwiebig, in Bearbeitung	in Bearbeitung
Erstellungsdatum	Datum, an dem der Risikoeintrag angelegt wurde	2019-10-15
Quelle	Aktivität oder Ereignis, die/das die Quelle der ersten Informationen war, z. B. Risikobewertungen, Schwachstellenmanagement, Sicherheitsvorfall, Bedrohungstelligentenz oder Dritte	Schwachstellen-Management
Titel	kurze Beschreibung des Risikos	„OS-Patch für CRM-System fehlt“

Punkt	Beschreibung	Beispiel
Beschreibung	Beschreibung des Risikos	Aufgrund des fehlenden Patches KB4530691 des Windows-Servers SRWNDUS19007 könnte ein Hacker Zugriff auf die CRM-Datenbank der Organisation erhalten.
Beschreibung der Bedrohung	Beschreibung der potenziellen Bedrohung	Ein externer oder interner Angreifer könnte die Schwachstelle ausnutzen, Root-Zugriff auf den Server erlangen und schließlich die Vertraulichkeit, Integrität oder Verfügbarkeit der auf diesem Server laufenden CRM-Datenbank beeinträchtigen.
Steuerung	beeinflusste Kontrolle	Patch-Verwaltung
unbehandelte Auswirkungen	Ausmaß oder Wert der Auswirkungen, wenn das Risiko nicht behandelt wird	hoch
unbehandelte Wahrscheinlichkeit	Wahrscheinlichkeitsniveau oder -wert, wenn das Risiko nicht behandelt wird	mittel
unbehandeltes Risikoniveau	Risikograd, wenn das Risiko nicht behandelt wird	hohes Risiko
behandelte Auswirkungen	Auswirkungsgrad oder -wert, wenn das Risiko behandelt wird	hoch
behandelte Wahrscheinlichkeit	Wahrscheinlichkeitsniveau oder -wert, wenn das Risiko behandelt wird	niedrig
behandeltes Risikoniveau	Risikoniveau, wenn das Risiko behandelt wird	mittleres Risiko
Risikobehandlung	gewählte Methode der Risikobehandlung: akzeptieren, mindern, übertragen, vermeiden	abschwächen
Details zur Risikobehandlung	Einzelheiten der Risikobehandlung	„Installieren Sie Patch KB4530691 auf diesem Windows-Server und bringen Sie den Server in der Zwischenzeit in eine sichere Zone, die durch ein IPS-System geschützt ist.“
geplante Umsetzungstermine für die Risikobehandlung	geplante Termine, an denen die Aktionen durchgeführt werden	2019-12-15

Quelle: Martin Macke, 2020.

## 5.3 Die ISO-27000-Reihe

Die ISO/IEC-27000-Serie (auch bekannt als ISMS-Normenfamilie oder ISO 27k) umfasst Informationssicherheitsstandards, die gemeinsam von der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) veröffentlicht werden. Die Reihe enthält Empfehlungen zu bewährten Verfahren für das Informationssicherheitsmanagement (das Management von Informationsrisiken durch Informationssicherheitskontrollen) im Rahmen eines umfassenden ISMS. Bis Januar 2020 wurden mehr als 50 Normen innerhalb der Reihe veröffentlicht, mehr als 20 sind in Arbeit. Der Anwendungsbereich der Normen ist sehr breit gefasst, zum Teil aber sehr spezifisch. Es gibt Normen, die sich auf eine bestimmte Gruppe von Technologien oder Industriesektor konzentrieren.

Organisationen können nach der Norm ISO 27001 in Verbindung mit ISO 27002 und ISO 27701 zertifiziert werden. Auch ISO 27017 und ISO 27018 sind zertifizierbar. Die anderen ISO 27k-Normen sind nicht zertifizierbar, bieten jedoch eine Anleitung und bilden einen ganzheitlichen Sicherheitsrahmen.

Die folgenden ISO 27k-Normen sind gut bekannt und spielen in der Praxis eine große Rolle:

**Tabelle 5: ISO-27k-Normen**

ISO-27k-Norm	Beschreibung
ISO/IEC 27000:2018	Übersicht und Einführung in die ISO-27k-Normen sowie Glossar für das Fachvokabular
ISO/IEC 27001:2013	Anforderungsstandard, der ein zertifizierbares ISMS formell spezifiziert
ISO/IEC 27002:2013	Kodex für Informationssicherheitskontrollen
ISO/IEC 27003:2017	Anleitung zur Implementierung von ISO/IEC 27001
ISO/IEC 27004:2016	Messung des Managements der Informationssicherheit
ISO/IEC 27005:2018	Risikomanagement im Bereich Informationssicherheit
ISO/IEC 27018:2019	Betrifft die Sicherheit persönlich identifizierbarer Informationen (PII) in öffentlichen Clouds
ISO/IEC 27701:2019	Anforderungen und Leitfaden zur Erweiterung von ISO/IEC 27001 und 27002 für das Management des Datenschutzes

Quelle: Martin Macke 2020 in Anlehnung an ISO 27000ff.

## **Ein ISMS gemäß ISO 27001**

ISO 27001 definiert ein ISMS. Es ist der meistzitierte Standard in der 27K-Familie und der internationale De-facto-Standard zum Nachweis, dass die IT-Sicherheit in einer Organisation angemessen gehandhabt wird. Der Standard besteht aus zehn Kapiteln und einem Anhang. Die ersten drei behandeln kurz den Anwendungsbereich und verweisen auf ISO 27000, um die Terminologie und die verwendeten Begriffe zu definieren.

In Kapitel vier (Kontext der Organisation) verlangt die Norm von einer Organisation zu verstehen, was die Ziele der Organisation sind, was die Interessengruppen der Organisation erwarten und was ihre Bedürfnisse sind. Außerdem muss der Umfang des ISMS bestimmt werden. Es ist von entscheidender Bedeutung zu verstehen, dass eine Organisation den Geltungsbereich des ISMS i. d. R. auf einen bestimmten geografischen oder organisatorischen Bereich eingrenzt, in dem es Anwendung findet. Der Geltungsbereich kann auch bestimmte Kontrollen in Anhang A ausschließen.

Führung wird in Kapitel fünf behandelt. Es verlangt von einer Organisation, dass sie eine effektive Führung zur Umsetzung und Steuerung des ISMS demonstriert. Es muss eine Richtlinie entworfen werden, die den Bedürfnissen der Organisation entspricht. Außerdem werden Rollen und Verantwortlichkeiten zugewiesen und kommuniziert.

Die Planung des ISMS wird in Kapitel sechs des Standards behandelt. Hauptthema in diesem Kapitel sind Aufbau und Aufrechterhaltung eines Risikomanagementsystems für die IT-Sicherheit. Die Abschwächungen für jedes Risiko müssen so gewählt werden, dass sie mit den Kontrollzielen in Anhang A übereinstimmen. In diesem Kapitel fordert die Norm von einer Organisation die Definition von IT-Sicherheitszielen und Pläne zu deren Erreichung.

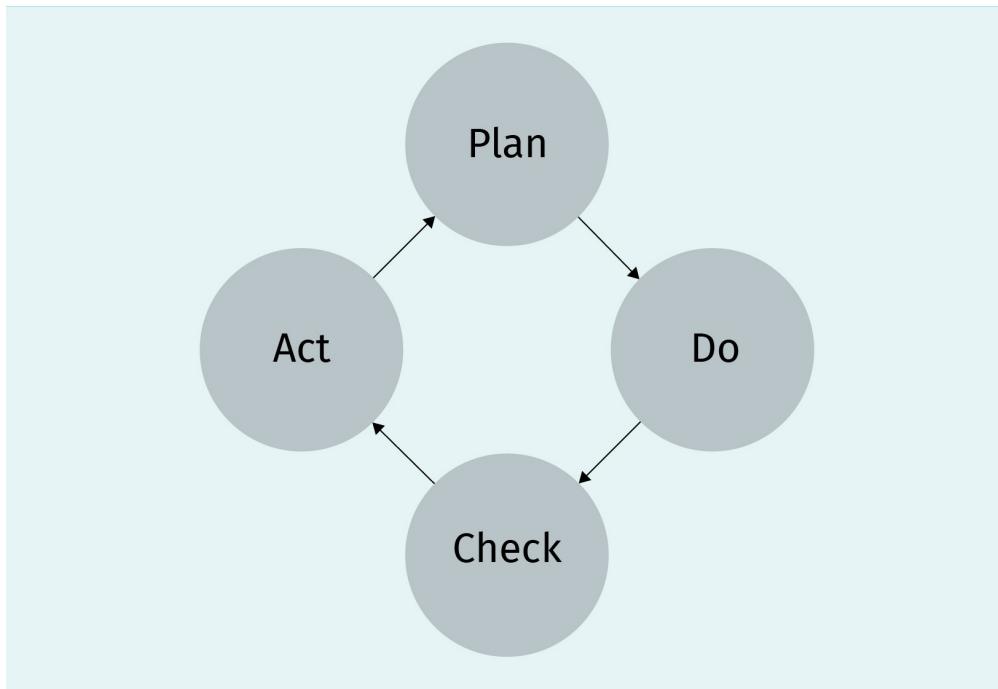
Ein angemessenes Niveau an Ressourcen steht im Mittelpunkt von Kapitel sieben (Unterstützung). Die Ressourcen müssen ausreichen, um ihre Rolle zu erfüllen, und alle Mitwirkenden in der Organisation müssen sich der Richtlinie und ihrer Rolle beim Schutz der Organisation bewusst sein. Die Informationen müssen dokumentiert und einer Dokumentenkontrolle unterzogen werden, die regelmäßige Überprüfungen und Versionskontrolle einschließt.

Kapitel acht befasst sich mit Arbeitsablauf, Risikobewertungen und Risikobehandlung.

In Kapitel neun wird das ISMS evaluiert. Dies geschieht durch Überwachung, interne Audits und Management-Reviews.

Schließlich werden in Kapitel zehn Maßnahmen zur kontinuierlichen Verbesserung des ISMS vorgestellt. Sie sollten dem bekannten PDCA-Zyklus folgen, der in der Abbildung unten dargestellt ist.

Abbildung 12: PDCA-Zyklus



Quelle: Jasmin Ćosić 2020.

Schließlich enthält Anhang A die 144 Kontrollen in 14 verschiedenen Gruppen, beginnend mit **A.5**:

- A.5: Informationssicherheitspolitik (zwei Kontrollen)
- A.6: Organisation der Informationssicherheit (sieben Kontrollen)
- A.7: Personalsicherheit (sechs Kontrollen, die vor, während oder nach der Beschäftigung durchgeführt werden)
- A.8: Asset Management (zehn Kontrollen)
- A.9: Zugriffskontrolle (vierzehn Kontrollen)
- A.10: Kryptografie (zwei Kontrollen)
- A.11: Umgebungs- und physische Sicherheit (fünfzehn Kontrollen)
- A.12: Betriebssicherheit (vierzehn Kontrollen)
- A.13: Kommunikationssicherheit (sieben Kontrollen)
- A.14: Systemerwerb, -entwicklung und -wartung (dreizehn Kontrollen)
- A.15: Lieferantenbeziehungen (fünf Kontrollen)
- A.16: Informationssicherheits-Störfallmanagement (sieben Kontrollen)
- A.17: Informationssicherheitsaspekte des betrieblichen Kontinuitätsmanagements (vier Kontrollen)
- A.18: Compliance/Konformität, wie z. B. Richtlinien, und externe Anforderungen, wie z. B. Gesetze (acht Kontrollen)

**A.5**  
In ISO 27002 werden Kapitel fünf und die folgenden exakt auf die relevanten Anhänge in ISO 27001 abgebildet, sodass Anhang A.5 in ISO 27001 in Kapitel fünf der ISO 27002 abgebildet wird.

ISO 27002 enthält Vorschläge, wie diese Kontrollen umgesetzt werden können. Beachten Sie, dass es nicht zwingend erforderlich ist, diese Vorschläge zu verwenden – andere sind verfügbar, wie z. B. NIST oder der deutsche BSI IT Grundschutz.

## **Ein PIMS gemäß ISO 27701**

ISO 27701 ist eine relativ neue Norm, die 2019 veröffentlicht wurde. Sie ist eine Erweiterung von ISO 27001 und ISO 27002 und beschreibt ein Privacy Information Management System (PIMS), manchmal auch Datenschutzmanagementsystem (DPMS) genannt. Eine Organisation kann nur in Verbindung mit ihrer ISO 27001-Zertifizierung nach ISO 27701 zertifiziert werden. Diese zeigt an, dass ein adäquates Datenschutzmanagementsystem eingerichtet ist, aber es würde nicht die Anforderungen einer Zertifizierung nach Artikel 42 DSGVO erfüllen.

In den Kapiteln eins bis sechs betont die Norm, wie ISO 27001 und ISO 27002 zum Schutz von PII beitragen und wie dieselben Methoden, wie z. B. Richtlinien oder Risikomanagement, in einem PIMS verwendet werden können. In den Kapiteln sieben und acht werden zusätzliche Anleitungen sowohl für die Verarbeiter als auch die für die Verarbeitung Verantwortlichen beschrieben. Der Anhang enthält 49 zusätzliche Kontrollen, die für den Datenschutz relevant sind. Der Standard enthält auch eine Abbildungstabelle, aus der hervorgeht, wie die verschiedenen Kontrollen den rechtlichen Anforderungen des DSGVO entsprechen.

Das Konzept besteht darin, sowohl ISMS als auch PIMS in ein Managementsystem zu integrieren. Nach ISO 9001 entscheiden sich einige Organisationen auch für die Integration mit dem Qualitätsmanagement.

## **5.4 IT-Sicherheit und IT-Governance**

IT-Governance und IT-Sicherheit müssen auf die Geschäftsanforderungen abgestimmt werden. Die Bedeutung dessen darf nicht unterschätzt werden, da viele Organisationen in diesem Bereich unter dem Silodenken leiden, was zu unnötigem Aufwand und Konflikten führt. Ein effektives Programm zur Sicherheits-Governance wird sich mit den folgenden Aktivitäten und Reaktionen befassen:

1. **Risikomanagement:** sicherstellen, dass alle IT-Sicherheitsrisiken angemessen behandelt und gehandhabt werden.
2. **Prozessverbesserungen:** Es werden Änderungen an Geschäftsprozessen vorgenommen, die die Sicherheit verbessern.
3. **Identifizierung des Ereignisses:** Es werden Technologien und Verfahren eingeführt, um Sicherheitsereignisse und Zwischenfälle so schnell wie möglich zu identifizieren.
4. **Reaktion auf Vorfälle:** Es werden Verfahren zur Reaktion auf Zwischenfälle eingeführt, die dazu beitragen, Zwischenfälle zu vermeiden und sie risikogerecht zu handhaben sowie Wahrscheinlichkeit und Auswirkungen eines Zwischenfalls zu verringern.
5. **verbesserte Compliance:** Alle anwendbaren Gesetze, Vorschriften und Normen werden neu identifiziert, um sicherzustellen, dass die Organisation die Einhaltung der Vorschriften einhält.
6. **Geschäftskontinuität und Notfallwiederherstellungsplanung:** Angemessene Geschäftskontinuitäts- und Notfallwiederherstellungspläne werden gepflegt und regelmäßig getestet.

7. **Metrik:** Wichtige Sicherheitsereignisse wie Vorfälle, Änderungen, Richtlinienverletzungen, Schwachstellen, Audits oder Schulungen werden gemessen.
8. **Verwaltung der Ressourcen:** Personelle und finanzielle Ressourcen werden für Sicherheitsmaßnahmen bereitgestellt, um Ziele zu erreichen.
9. **verbesserte IT-Governance:** Eine effektive Sicherheits-Governance hilft, bessere strategische Entscheidungen zu treffen und das Risiko auf einem erträglichen Niveau zu halten.

## Rollen und Verantwortlichkeiten

Organisationen verwenden häufig **RACI-Diagramme**, um Aktivitäten und die beteiligten Rollen zu dokumentieren:

- **Verantwortung (Responsibility):** die Person oder Rolle, die die Arbeit ausführt;
- **rechtliche Verantwortlichkeit (Accountability):** die Person oder Rolle, die letztendlich für die Aktivität verantwortlich ist, oft ein Manager;
- **konsultiert (Consulted):** die hinzuzuziehenden Rollen, beispielsweise bestimmte Experten;
- **informiert (Informed):** die Rollen, die über eine bestimmte Aktivität oder Entscheidung informiert werden müssen.

**RACI-Diagramme**  
Ein RACI-Diagramm wird nicht nur in der IT-Sicherheit, sondern auch in vielen anderen Bereichen der IT und des Geschäftslebens verwendet.

Ein typisches RACI-Diagramm für eine IT-Sicherheits-Benutzerkontoanforderung kann wie folgt aussehen:

Tabelle 6: RACI-Diagramm

Aktivität	Benutzer	Benutzersupport	Leiter	Sicherheitsteam
Benutzerkonto anfordern	R	I	A	I
Benutzerkonto genehmigen	I	C	A	C
Benutzerkonto bereitstellen	I	R	I	I

Quelle: Jasmin Ćosić 2020.

Beim Entwurf von RACI-Matrizen muss eine Aufgabentrennung in Betracht gezogen werden, damit mindestens zwei Rollen oder Personen eine kritische Aufgabe ausführen. Außerdem sind Interessenkonflikte zu vermeiden; so kann ein Genehmigender nicht dieselbe Person sein, welche auch die Aufgabe ausführt oder darum bittet.

Zu den Rollen in einer Sicherheitsorganisation oder im Zusammenhang mit einer solchen gehören gewöhnlich:

1. **leitender Beauftragter für Informationssicherheit (CISO – Chief Information Security Officer):** Dies ist die ranghöchste Rolle in der Sicherheitsorganisation und gehört gewöhnlich dem Vorstand an oder ist ihm zumindest direkt unterstellt. Um Interessenkonflikte zu vermeiden, sollte der CISO nicht dem CIO unterstehen.
2. **leitender Datenschutzbeauftragter (CPO – Chief Privacy Officer):** Organisationen, die eine große Menge an PII verwalten, ernennen meist einen CPO, der die PII der Organisation schützt. Wenn dies gesetzlich vorgeschrieben ist, kann auch der bereits bestimmte Datenschutzbeauftragte CPO sein.
3. **Leiter der Sicherheitsrevision:** Diese Rolle ist für die Audits im Sicherheitsbereich verantwortlich – sie planen und verwalten die Audits.

Es gibt viele andere Rollen, die mit der IT-Sicherheit in IT, Risikomanagement oder anderen Unternehmensbereichen zusammenarbeiten.

## Kontroll-Rahmenwerke

Governance-Rahmenwerke müssen nicht für jede Organisation erfunden werden. Es gibt viele, die dabei helfen, die IT-Ziele einer Organisation zu verwalten. Einige weit verbreitete Beispiele für derlei Rahmenwerke sind unten aufgeführt.

1. „COBIT: Control Objectives for Information and Related Technology“ ist ein von ISACA entwickelter IT-Management- und Steuerungsrahmen. Es konzentriert sich nicht primär auf die IT-Sicherheit, sondern auf die IT-Governance. Es schließt jedoch Sicherheitsprozesse als Teil seines Rahmens ein, und Sicherheit ist ein integraler Bestandteil davon. Die vier COBIT-Bereiche sind:
  - a) ausrichten, planen und organisieren (APO – Align, Plan, Organize);
  - b) bauen, erwerben und implementieren (BAI – Built, Acquire and Implement);
  - c) Serviceerbringung, Service und Unterstützung (DSS – Deliver, Service and Support);
  - d) überwachen, bewerten und beurteilen (MEA – Monitor, Evaluate and Assess)" (ISACA 2019).
2. ISO/IEC 27K: eine Familie von Normen für das IT-Sicherheitsmanagement.
3. ISO/IEC 38500: IT-Governance für die Organisation ist ein internationaler Standard zur Steuerung der IT.
4. ITIL & ISO/IEC 20000: Die IT-Infrastruktur-Bibliothek (ITIL) ist ein Rahmenwerk, das IT-Betriebsprozesse, wie z. B. der Sicherheit, in seinen Rahmen miteinbezieht. ISO/IEC 20000 ist ein zertifizierbarer Standard, der von ITIL übernommen wird. Das Rahmenwerk konzentriert sich auf die Verwaltung von IT-Dienstleistungen.
5. HIPAA: Der Health Insurance Portability and Accountability Act in den USA schreibt den Schutz von Gesundheitsinformationen und die Verwaltung technischer, administrativer und physischer Schutzmaßnahmen vor.
6. NIST SP 800-53: Die Sonderpublikation 800-53 des United States National Institute for Standards and Technology ist eines der bekanntesten Sicherheits-Frameworks und für alle Informationssysteme des öffentlichen Sektors der USA obligatorisch. Viele andere Organisationen haben diese Kontrollen auch außerhalb des öffentlichen Sektors übernommen.

## 5.5 Beispiel: IT-Sicherheit für Kreditkarten (PCI DSS)

Ein Beispiel für ein Sicherheitsrahmenwerk ist PCI DSS (Payment Card Industry Data Security Standard), der Datensicherheitsstandard der Zahlungskartenindustrie. Kreditkartenunternehmen wie VISA und American Express begründeten diesen Standard, um sicherzustellen, dass Kreditkartentransaktionen angemessen gesichert sind und das Risiko im Zahlungskartenprozess reduziert wird.

Dieser Anwendungsbereich bezieht sich auf (PCI Security Standards Council 2018, S. 30) ...

- ... Systeme, die Karteninhaberdaten speichern, verarbeiten oder übertragen,
- Systeme, die Sicherheitsfunktionalitäten bieten oder die Sicherheit von Karteninhaberdaten beeinflussen können, und
- jede andere Komponente oder Vorrichtung, die sich in der Datenumgebung des Karteninhabers (CDE – Cardholder Data Environment) befindet oder mit dieser verbunden ist.

Die Norm gilt für Fälle, in denen die primäre Kontonummer (PAN – Primary Account Number) gespeichert oder verarbeitet wird. Der Standard erlaubt nicht die Speicherung sensibler Authentifizierungsdaten, einschließlich der Daten des Magnetstreifens einer Karte, der Kartenkontrollnummern oder der PIN. Er besteht hauptsächlich aus zwölf groben Anforderungen, in denen der PCI DSS recht detaillierte Kontrollen darüber festlegt, was eine Organisation zu beachten hat, wenn sie Karteninhaberdaten verarbeitet. Die Anforderungen auf hoher Ebene lauten wie folgt (ebd., S. 9):

- Installation und Wartung einer Firewall-Konfiguration zum Schutz der Karteninhaberdaten,
- keine Verwendung der vom Hersteller gelieferten Standardwerte für Systempasswörter und andere Sicherheitsparameter,
- Schutz der gespeicherten Karteninhaberdaten,
- Verschlüsselung der Übertragung von Karteninhaberdaten über offene, öffentliche Netzwerke,
- Schutz aller Systeme gegen Malware und regelmäßige Aktualisierung der Antiviren-Software oder -Programme,
- Entwicklung und Wartung sicherer Systeme und Anwendungen,
- Einschränkung des Zugriffs auf die Karteninhaberdaten je nach geschäftlichem Bedarf,
- Identifizierung und Authentifizierung beim Zugang zu Systemkomponenten,
- Einschränkung des physischen Zugangs zu den Daten des Karteninhabers,
- Verfolgung und Überwachung aller Zugriffe auf Netzwerkressourcen und Karteninhaberdaten,
- regelmäßiges Testen der Sicherheitssysteme und -prozesse sowie
- Aufrechterhaltung einer Richtlinie, die sich mit der Informationssicherheit für das gesamte Personal befasst.

Für jede der Anforderungen werden spezifische Testverfahren festgelegt, mit deren Hilfe nachgewiesen werden kann, dass eine Organisation der Norm entsprechend handelt. Sie werden geprüft, bevor einer Organisation die Verarbeitung von Kreditkartendaten gestattet wird, und diese Prüfungen sind streng.



### ZUSAMMENFASSUNG

IT-Sicherheit muss verwaltet werden. Eine angemessen strukturierte Sicherheitsrichtlinie richtet sich an die gesamte Organisation und stellt sicher, dass jeder seine Pflichten versteht. Sie macht die Sicherheit durchsetzbar und muss überwacht, d. h. auditiert werden. Eine Nicht-einhaltung hat Konsequenzen und ist zu dokumentieren.

Risikomanagement spielt eine integrale Rolle in allen IT-Sicherheitsrahmenwerken wie auch beim Sicherheitsmanagement. Es kann mehrere Formen haben; ein ganzheitlicher Risikomanagementprozess stellt sicher, dass Risiken identifiziert und angemessen priorisiert werden. Die vier Risikobehandlungsstrategien helfen, eine angemessene Behandlung zu finden. Dabei darf nicht vergessen werden, dass Risiken Teil des Geschäfts sind und jedes Unternehmen über eine gewisse Risikotoleranz verfügen muss.

Die ISO-27k-Normenfamilie ist allgemein, spezifisch und wird ständig weiterentwickelt. ISO 27001 ist besonders hilfreich beim Aufbau eines ISMS.

IT-Sicherheits- und IT-Governance arbeiten zusammen, um innerhalb des Unternehmens gute Entscheidungen zu fördern. Rahmenwerke wie COBIT oder NIST SP 800-53 können einer Organisation helfen, geeignete Strukturen und Kontrollen zu finden.

Schließlich ist der PCI DSS ein verbindlicher Standard für Organisationen, die Kreditkartendaten verarbeiten. Er enthält eine Reihe strenger Anforderungen und Kontrollen, die dazu beitragen, Kreditkartendaten zu sichern und somit das Risiko in der Zahlungskartenindustrie sowohl für die Branche als auch für die Karteninhaber zu verringern.

# LEKTION 6

## KRYPTOGRAFIE

### LERNZIELE

Nach der Bearbeitung dieser Lektion werden Sie wissen, ...

- wie das Grundkonzept der Kryptografie aussieht.
- was die Konzepte der symmetrischen und asymmetrischen Verschlüsselung sind.
- wie und warum man Einwegfunktionen und Hashing-Algorithmen verwendet.
- welches die Hauptprobleme im Schlüsselaustauschprozess sind.
- warum Kryptografie für ICT-Prozesse so wichtig ist.

## 6. KRYPTOGRAFIE

### Einführung

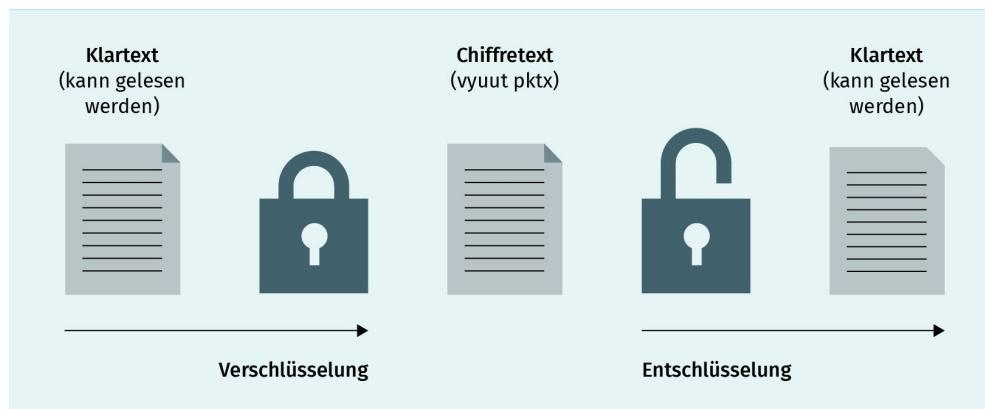
Eine der ersten bekannten Anwendungen von Kryptografie stammt aus der Römerzeit. Als Caesar Nachrichten an seine Armee sandte, ersetzte er jedes „A“ in seinen Nachrichten durch „D“, jedes „B“ durch „E“ usw., weil er den Boten nicht traute. Nur diejenigen, die das Verschlüsselungssystem kannten, konnten die Nachricht lesen (d. h. das „Verschiebe um drei“-System). Würde z. B. „wir werden morgen früh um 3 Uhr angreifen“ mit der Methode Caesars verschlüsselt, so führt das zu einer Nachricht mit dem Wortlaut „zlu zhughq prujhq iuük xp 3 Xku dqjuhlihq“.

### 6.1 Grundbegriffe der Kryptografie

Kryptografie ist in der Sicherheitsdomäne unerlässlich, und in dieser Lektion werden einige der wichtigsten Konzepte erklärt. Bevor wir jedoch in die Welt der Kryptografie einsteigen, müssen die folgenden Begriffe geklärt werden:

- **Klartext** ist eine Information oder ein Text, der direkt von Menschen oder einer Maschine gelesen werden kann.
- Ein **Chiffretext** ist das Ergebnis eines Verschlüsselungsverfahrens – ohne einen speziellen Algorithmus (Chiffre) kann dieser Text nicht gelesen werden. Ohne die Chiffre sieht der Chiffretext wie eine Nachricht ohne Bedeutung aus. Eine Chiffre ist eine mathematische Funktion, die im Ver- und Entschlüsselungsprozess verwendet wird.
- Ein **Schlüssel** ist eine Phrase, eine Zahl, ein Wort oder eine Kombination, die zur Verschlüsselung von Klartext oder zur Entschlüsselung eines Chiffriertextes verwendet wird.
- **Verschlüsselung** ist der Prozess der Übersetzung von Klartext in Chiffretext.
- Die **Entschlüsselung** ist der umgekehrte Prozess – also jener der Umwandlung des Chiffriertextes in seine ursprüngliche Form. Die Abbildung unten zeigt den Prozess der Ver- und Entschlüsselung sowie die Rolle von Klartext und Chiffretext.

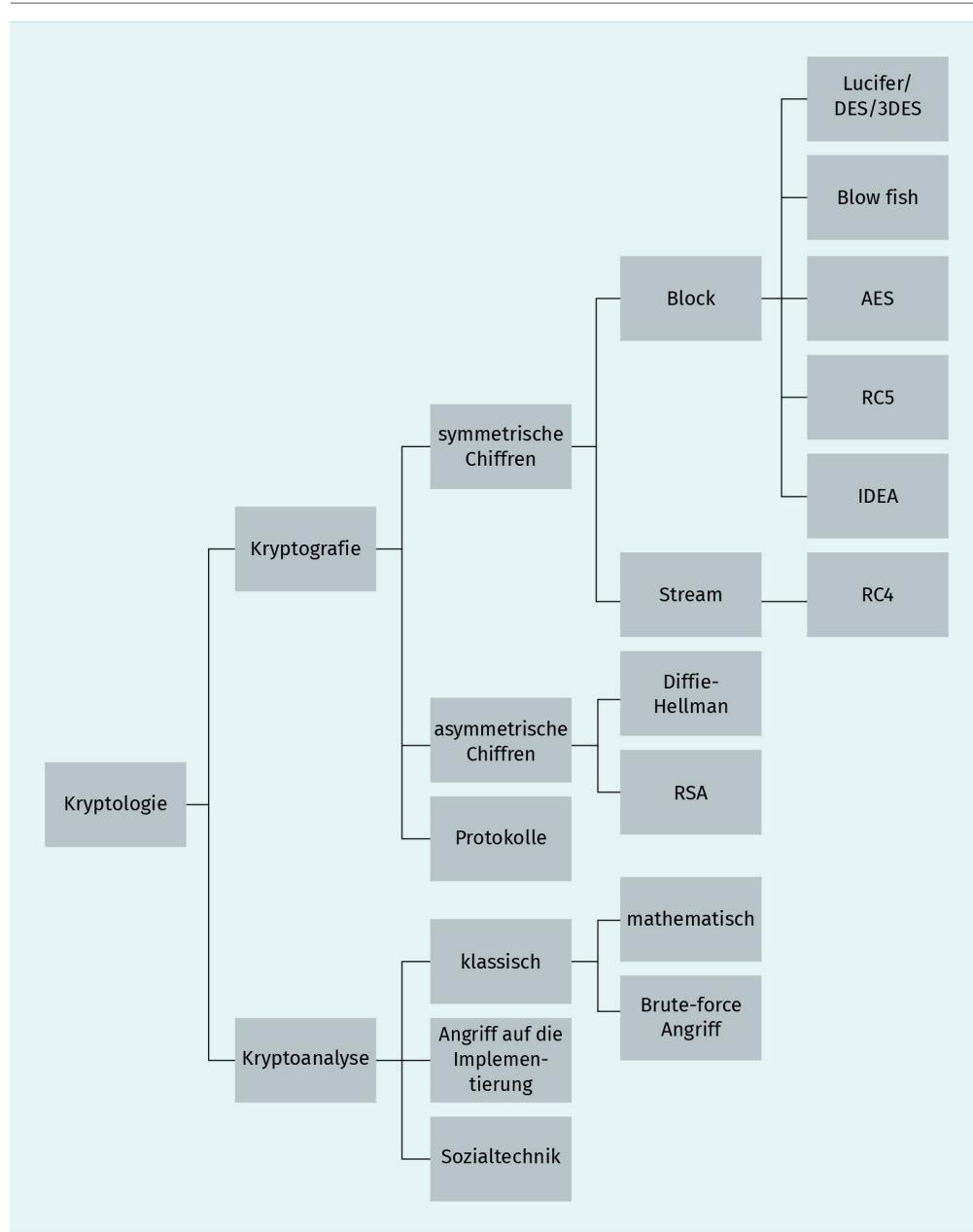
Abbildung 13: Ver- und Entschlüsselungsprozesse



Quelle: Jasmin Ćosić 2020.

- **Kryptografie** ist die Wissenschaft von der Anwendung mathematischer Methoden zur sicheren Verschlüsselung von Daten. Sie ist wichtig in der Informations- und Kommunikationstechnologie (ICT) sowie im Bereich der IT-Sicherheit, weil sie uns hilft, sensible Daten zu speichern und über ein unsicheres Netzwerk (LAN, WAN, Intranet, Internet usw.) zu übertragen.
- Die **Kryptoanalyse** ist die Wissenschaft von Analyse und Aufbrechen dieser verschlüsselten Kommunikation.
- Die **Kryptologie** verbindet beides und ist die Wissenschaft vom Erstellen und Brechen von Chiffren.
- Das **Kryptosystem** ist ein System, das aus einem kryptografischen Algorithmus, allen Schlüsseln, Kombinationen und Protokollen besteht. Ein gutes Beispiel für ein Kryptosystem ist Pretty Good Privacy (PGP).

Abbildung 14: Übersicht Kryptologie



Quelle: Jasmin Ćosić 2020.

Die Klassifikation kryptografischer Algorithmen kann auf verschiedene Weise erfolgen; man unterscheidet zwischen symmetrischen und asymmetrischen Verfahren.

## 6.2 Symmetrische Kryptografie

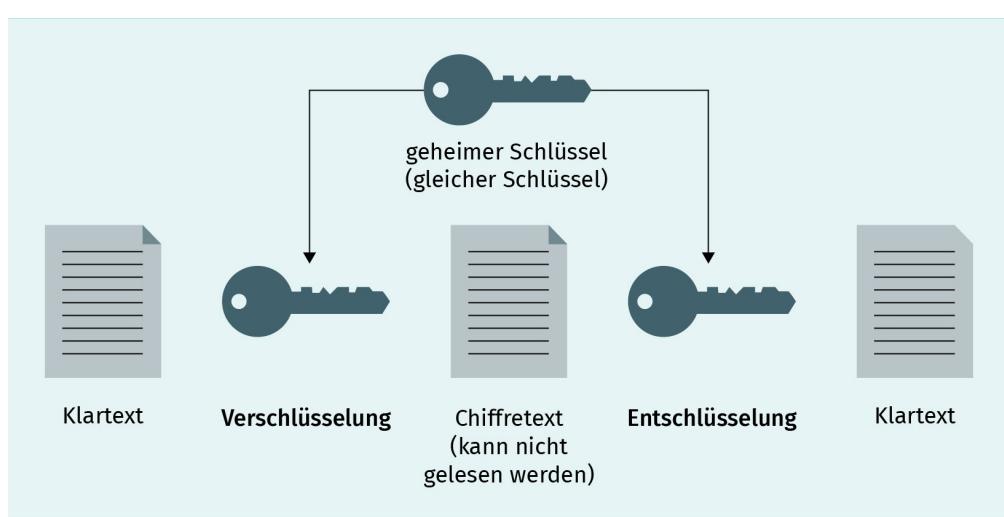
Die erste Art von Algorithmen, die hier behandelt werden sollen, ist die symmetrische Kryptografie oder Secret Key Cryptography (SKC). Dies ist ein Beispiel für symmetrische Verschlüsselung, da ein einziger Schlüssel sowohl zur Ver- als auch zur Entschlüsselung verwendet wird.

Bei der symmetrischen Verschlüsselung verwendet der Sender den „geheimen“ Schlüssel, um den Klartext zu verschlüsseln, und sendet anschließend den Chiffretext an den Empfänger. Dieser muss, wie in der Abbildung unten dargestellt, den gleichen geheimen Schlüssel anwenden, um die Nachricht zu entschlüsseln und den ursprünglichen Klartext wiederherzustellen. Bei dieser Form der Kryptografie muss der Schlüssel sowohl dem Sender als auch dem Empfänger bekannt sein. Die größte Schwierigkeit bei diesem Ansatz ist die Verteilung und Verwaltung der Schlüssel (Kessler 2020). Die Verwendung einer Geheimschlüssel-Chiffre bedeutet, dass mit jedem Kommunikationspartner ein separater Schlüssel ausgetauscht werden muss, selbst für eine kurze Nachricht, was zu einer großen Anzahl von Schlüsseln führt, deren Erläuterung von jedem Benutzer verwaltet werden müssen.

Ein One-Time-Pad ist ein Beispiel für eine solche symmetrische Verschlüsselung und die einzige nachweislich nicht entschlüsselbare Verschlüsselungstechnik, die zur Verfügung steht. Die Schlüssellänge muss dabei mindestens die gleiche Größe wie der Klartext haben. Der Schlüssel muss zufällig sein und darf nur einmal verwendet werden. One-Time-Pads wurden vor der Erfindung des Computers verwendet und kommen auch heute noch zum Einsatz, wenn die Ver- und Entschlüsselung von Hand erfolgt. Sie könnten in der Quantenkryptografie eine Rolle spielen, die jedoch den Rahmen dieser Kurseinheit sprengen würde.

Symmetrische Kryptografieschemata werden im Allgemeinen entweder als Strom- oder als Blockchiffrierung kategorisiert.

Abbildung 15: Symmetrische Verschlüsselung



Quelle: Jasmin Ćosić 2020.

Stream-Chiffrierschemata arbeiten jeweils mit einem einzelnen Bit (oder Byte) und verschlüsseln dieses einzeln. Die meisten Stromchiffrierungen implementieren eine Art Rückkopplungsmechanismus, sodass sich der Schlüssel ständig ändert. Selbstsynchronisierende Stromchiffrierungen berechnen jedes Bit im Schlüsselstrom in Abhängigkeit von den vorherigen  $n$  Bits im Schlüsselstrom. Sie werden als „selbstsynchronisierend“ bezeichnet, weil der Entschlüsselungsprozess mit dem Verschlüsselungsprozess synchronisiert bleiben kann, wenn man nur weiß, wie weit er in den  $n$ -Bit-Schlüsselstrom hineinreicht (Kessler 2020).

Synchrone Stromchiffrierungen erzeugen den Schlüsselstrom, sodass er vom Nachrichtenstrom unabhängig ist, Sender und Empfänger jedoch dieselbe Funktion zur Schlüsselstromerzeugung verwenden. Obwohl Strom-Chiffren Übertragungsfehler nicht propagieren, sind diese von Natur aus periodisch, was bedeutet, dass sich der Schlüsselstrom schließlich wiederholt.

Ein Blockchiffierschema verschlüsselt jeweils einen Datenblock fester Größe. Ein Block ist eine feste Anzahl von Bits. Die meisten Blockchiffrierungen wandeln einen Block Klartext in einen Chiffriertextblock derselben Größe um, indem ein Schlüssel und eine Methode angewendet wird, der/die invertierbar ist.

Bei einer Blockchiffrierung wird der Klartext in eine Folge von Blocks gleicher Länge aufgesplittet (meist 32, 64 oder 128 Bits), die dann jeweils einzeln verschlüsselt werden. Es gibt verschiedene als „Blockchiffriermodi“ (block cipher modes) bezeichnete Verfahren, wie die einzelnen Blocks innerhalb einer Folge von Blocks verschlüsselt werden. Mit Ausnahme des unten beschriebenen ECB-Modus nutzen alle Modi zusätzliche Informationen wie den vorigen Block oder einen Zähler, um sicherzustellen, dass der gleiche Klartext nicht zum gleichen Geheimtext führen, auch wenn sie mit dem gleichen Schlüssel verschlüsselt werden. Die damit entstehenden Blockchiffriermodi unterscheiden sich erheblich in ihren Eigenschaften, insbesondere ihrer Sicherheit, den Auswirkungen einzelner

Bitfehler oder in der Übertragung verlorener Blocks auf die folgenden Blocks, sowie darin, ob Ver- und Entschlüsselung durch parallele Bearbeitung mehrerer Blocks beschleunigt werden können.

Es gibt eine Reihe verbreiteter Blockchiffriermodi (Paar & Pelzl 2010, S. 124-134):

- **ECB: Electronic Codebook** ist der einfachste und offensichtlichste Blockchiffriermodus. Jeder Block wird separat mit Hilfe des geheimen Schlüssels verschlüsselt, und der gleiche Klartextblock führt daher immer zum gleichen Geheimtextblock. Das stellt sicher, dass Bitfehler oder verlorene Blocks keine Auswirkung auf die folgenden Blocks haben, und auch die Ver- und Entschlüsselung verschiedener Blocks ist parallel möglich. Allerdings ist dieser Modus sehr unsicher, denn da der gleiche Klartext beim gleichen Schlüssel immer zum gleichen Geheimtext führt, werden eine Reihe von Angriffen erleichtert, beispielsweise Brute-Force-Angriffe oder die unbemerkte Ersetzung oder Einfügung von Blocks. Selbst ohne den Block entschlüsseln zu können, kann es für einen Angreifer eine wertvolle Information sein, dass der gleiche Block wiederholt gesendet wurde.
- **CBC: Cipher Block Chaining** ist ein weit verbreiteter Blockchiffriermodus bei dem jeder Klartextblock vor der Verschlüsselung mit dem vorherigen Geheimtextblock bitweise addiert (also XOR-verbunden) wird. Für den ersten Klartextblock wird stattdessen ein zufällig erzeugter „Initialisierungsblock“ addiert. Das hat zur Folge, dass jeder Geheimtextblock von allen vorher verarbeiteten Klartextblöcken sowie dem Initialisierungsvektor abhängt.

Die folgenden drei Blockchiffriermodi basieren alle auf der Idee, nicht den Klartext als solches zu verschlüsseln, sondern stattdessen eine Folge von Schlüssel-abhängigen Blocks auf den Klartext (bitweise) zu addieren. Das hat den Vorteil, dass sie auch als Stromchiffren verwendet werden können, da der resultierende Geheimtext bitweise statt blockweise erzeugt werden kann.

- **OFB: Output Feedback** nutzt einen Initialisierungsvektor plus den Schlüssel, um die Folge von Blocks zu erzeugen, die dann bitweise auf den Klartext addiert werden.
- **CFB: Cipher Feedback** funktioniert ähnlich, nutzt aber zusätzlich den Geheimtext des jeweils vorigen Blocks, um die Folge der auf den Klartext zu addierenden Blocks zu erzeugen.
- **CTR: Counter Mode** nutzt einen Zähler sowie einen Initialisierungsvektor, um die Folge der auf den Klartext zu addierenden Blocks zu erzeugen.

Beispiele für beliebte Algorithmen mit symmetrischen Schlüsseln sind Twofish, Serpent, AES (Rijndael), Blowfish, CAST5, Kuznyechik, RC4, DES, 3DES, Skipjack, Safer+// (Bluetooth) und IDEA (Roeder 2020).

**Tabelle 7: Häufigste symmetrische Verschlüsselungsalgorithmen**

Algorithmus	Schlüssellänge (Bits)	Blockgröße (Bits)
DES	56	64
3DES	56,112,168	64

<b>Algorithmus</b>	<b>Schlüssellänge (Bits)</b>	<b>Blockgröße (Bits)</b>
AES	128,192,256	128
IDEA	128	64
RC4	40-256	Stream-Chiffre
RC5	0-2040	32,64,128
Blowfish	32-448	64
Twofish	bis zu 256	128
Safer+/++	128	64/128

Quelle: Jasmin Ćosić 2020.

Die obige Tabelle zeigt uns einige der am häufigsten verwendeten symmetrischen Verschlüsselungsalgorithmen mitsamt ihrer Schlüssellänge und Blockgröße (in Bits).

DES (Data Encryption Standard) war von Mitte der 1970er- bis Mitte der 1990er-Jahre der vorherrschende symmetrische Verschlüsselungsalgorithmus. Er ist ein gutes Beispiel für eine Blockchiffrierung, die in der Hardware sehr effizient implementiert werden kann.

Heute kann jedoch ein Standard-DES mit einer Schlüssellänge von 56 Bit relativ leicht gebrochen werden. Aus diesem Grund wurde Triple-DES (3DES) geschaffen, bei dem dreimal hintereinander mit DES verschlüsselt wird (Paar/Pelzl 2010). Bis vor einigen Jahren galt als sicher, dass es keinen möglichen praktischen Angriff gegen 3DES geben könne.

Der 3DES-Algorithmus wendet seine Schlüssel wie folgt an:

- Verschlüsselung mit dem ersten Schlüssel (k1),
- Entschlüsselung mit dem zweiten Schlüssel (k2) und
- Verschlüsselung mit dem dritten Schlüssel (k3).

Zudem gibt es eine Variante mit zwei Schlüsseln, bei der die Schlüssel k1 und k3 identisch sind.

Im Jahr 2016 fanden Forscher eine neue Methode zur Wiederherstellung und Entschlüsselung von Cookies aus HTTPS-Authentifizierungssitzungen, die mit 3DES verschlüsselt sind. Die Schwäche von Sweet32 wurde öffentlich gemacht und eine bekannte Anfälligkeit für Kollisionsangriffe in 3DES ausgenutzt, die bei längeren Übertragungen, beim Austausch von Inhaltsdateien oder bei Übertragungen möglich werden können, welche durch Textinjektion gefährdet sind (Karthikeyan/Gaëtan 2016). Nachdem diese Schwachstelle aufgedeckt worden war, schlug das NIST im Standard 800-131A vor, 3DES zu verwerfen. Das Dokument „Transitioning the Use of Cryptographic Algorithms and Key Lengths“ (Barker/Roginsky 2019) formalisiert die Ausmusterung von Triple-DES bis Ende 2023. Danach wird es nur noch für die Legacy-Nutzung, also für die Entschlüsselung empfohlen.

Heute ist der am häufigsten verwendete symmetrische (und mittlerweile Standard-)Algorithmus AES (Advanced Encryption Standard) mit seinen Varianten AES-128, AES-192 und AES-256. Der Advanced Encryption Standard (AES) wurde 2001 eingeführt, um 3DES zu ersetzen. AES ermöglicht es, einen 128-, 192- oder (für sehr hohe Sicherheitsanforderungen) 256-Bit-Schlüssel zu wählen, wobei die Sicherheit eines Schlüssels exponentiell mit seiner Größe wächst. AES wird in vielen Anwendungen eingesetzt und ist auch der Algorithmus, dem sowohl die Regierung der USA als auch zahlreiche andere Organisationen als Standard vertrauen. Er ist in Soft- und Hardware effizient. Heute können wir die AES-Implementierung in Messaging-Anwendungen wie WhatsApp und Signal, in Anwendungen wie VeraCrypt und WinZip und auch in einer Reihe von Hardware beobachten.

AES war ursprünglich als „Rijndael“-Blockchiffrierung bekannt, die von den belgischen Kryptografen Joan Daemen und Vincent Rijmen entwickelt wurde, bis es vom NIST als neuer Standardnachfolger von DES ausgewählt und dann in AES umbenannt wurde. Gründe für die Wahl von Rijndael waren seine weitverbreiteten Fähigkeiten, einschließlich seiner Leistung sowohl auf Hardware- als auch auf Softwareebene, sowie die einfache Implementierung und sein Sicherheitsniveau. AES wurde 2002 zum Bundesstandard der USA ernannt und entwickelte sich von da an zum Standard-Verschlüsselungsalgorithmus für die ganze Welt.

## 6.3 Asymmetrische Kryptografie

Die symmetrische Kryptografie ist eine sehr alte Praxis und wird im Prinzip seit Caesars Zeiten verwendet, als es nur einen Schlüssel zur Ver- und Entschlüsselung gab. Die asymmetrische Verschlüsselung oder Public-Key-Kryptografie (Public Key Cryptography) ist jedoch relativ neu – das allgemeine Konzept wurde 1976 erstmals vorgestellt. Bei dieser Art der Verschlüsselung gibt es zwei Schlüssel (ein Paar): einen öffentlichen Schlüssel, der weit verbreitet werden kann, und einen privaten Schlüssel, der nur dem Besitzer bekannt ist. Im PKC-System kann jeder eine Nachricht mit dem öffentlichen Schlüssel des Empfängers verschlüsseln. Verschlüsselte Nachrichten können nur mit dem privaten Schlüssel des Empfängers entschlüsselt werden – dies kann mit einem Briefkasten verglichen werden. Der Briefkasten ist öffentlich, d. h. jeder, der den Standort kennt (öffentlicher Schlüssel), kann zu ihm gehen und einen Brief einwerfen, aber nur der Besitzer des Briefkastens verfügt über einen physischen (privaten) Schlüssel, der es ihm erlaubt, auf die Briefe im Kasten zuzugreifen und sie zu lesen.

Asymmetrische Kryptografie verwendet Falltürfunktionen. Eine solche ist in einer Richtung leicht zu berechnen, aber in der entgegengesetzten oder umgekehrten Richtung schwierig.

Der bekannteste Algorithmus für PKC ist der RSA-Algorithmus (Rivest, Shamir und Adleman). Der RSA-Algorithmus erzeugt ein Paar von öffentlichen und privaten Schlüsseln. Diese sind mathematisch miteinander verknüpft. Öffentliche Schlüssel werden zum Verschlüsseln von Daten verwendet und nur der entsprechende private Schlüssel kann zum Entschlüsseln verwendet werden. Die Kenntnis des öffentlichen Schlüssels ermöglicht es einem Kryptoanalytiker nicht, den privaten Schlüssel zu finden.

Der Algorithmus basiert auf der Eulerschen  $\phi$ -Funktion (gesprochen Phi-Funktion).  $\phi(n)$  ist die Anzahl der ganzen Zahlen  $k$  im Bereich von  $1 \leq k \leq n$  für die der größte gemeinsame Teiler  $\text{ggT}(n,k)$  gleich 1 ist.

#### **Algorithmus**

Das Open-Source-Werkzeug CrypTool kann zum Experimentieren und zur Visualisierung kryptografischer Algorithmen verwendet werden.

Der **Algorithmus** besteht aus den folgenden Schritten:

1. Wählen Sie zwei große Primzahlen  $p$  und  $q$ .
2. Berechnen Sie  $n = pq$ .
3. Wählen Sie eine kleine, ungerade, natürliche Zahl  $e$ , die eine relative Primzahl ist mit  $\phi(n) = (p - 1)(q - 1)$ . Anders ausgedrückt, der größte gemeinsame Teiler ist  $(e, \phi(n)) = 1$ .
4. Berechnen Sie  $d$  als Lösung der Gleichung  $ed \bmod \phi(n) = 1$ . Dazu kann der Euklidische Algorithmus verwendet werden.
5. Das Paar  $P = (e, n)$  ist der öffentliche Schlüssel.
6. Das Paar  $S(d, n)$  ist der private Schlüssel.

Der RSA-Algorithmus wird angewendet von:

1. Verschlüsselung der Nachricht  $M$ :  $E(M) = M^e \bmod n$ .
2. Entschlüsselung des Chiffretextes  $C$ :  $D(C) = C^d \bmod n$ .

Es kann nun mathematisch gezeigt werden, dass  $D(E(M)) = M \bmod n$  und  $E(D(C)) = C \bmod n$ .

**Abbildung 16: Asymmetrische Kryptografie (Kryptografie mit öffentlichem Schlüssel)**



Quelle: Jasmin Ćosić 2020.

Wie wir in der obigen Abbildung sehen können, wollen Sender und Empfänger eine Nachricht (Klartext) über einen ungesicherten Kommunikationskanal, z. B. das Internet, austauschen. Der Sender verwendet den öffentlichen Schlüssel eines Empfängers, um eine Nachricht zu verschlüsseln, und sendet das Resultat an den Empfänger, der dann seinen eigenen privaten Schlüssel verwendet, um die Nachricht zu entschlüsseln. Um einen Text

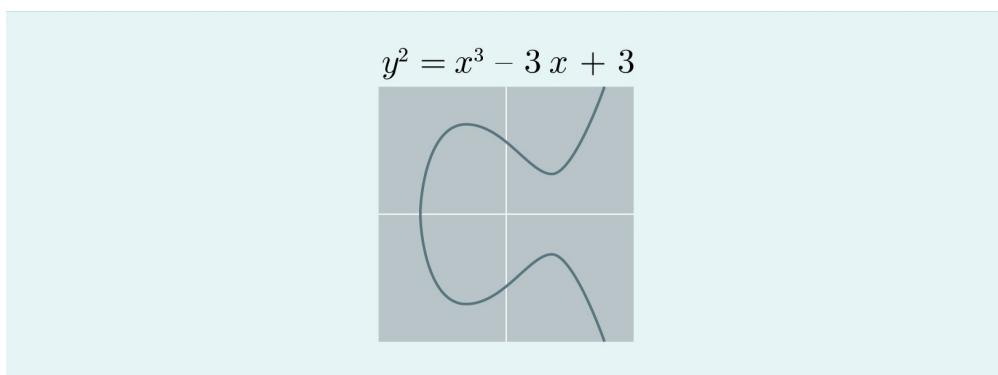
mit dem öffentlichen Schlüssel des Empfängers zu verschlüsseln, muss ein Empfänger dem Sender diesen Schlüssel zur Verfügung stellen, Empfänger verbreiten jedoch niemals ihren eigenen privaten Schlüssel.

Um Vertraulichkeit, Integrität, Authentizität und Nachweisbarkeit zu gewährleisten, müssen Benutzer und Systeme sicher sein, dass ein öffentlicher Schlüssel authentisch ist. Daher muss gewährleistet sein, dass der öffentliche Schlüssel der richtigen Person oder Entität gehört und er nicht manipuliert oder von einem böswilligen Dritten ersetzt wurde. In einer Public-Key-Infrastruktur (PKI) bescheinigen vertrauenswürdige Zertifizierungsstellen (CA – Certificate Authority) den Besitz von Schlüsselpaaren und Zertifikaten, um die digitalen Identitäten der Benutzer zu authentifizieren. Verschlüsselungsprodukte, die auf dem Pretty Good Privacy (PGP)-Modell (d. h. OpenPGP) basieren, beruhen auf einem dezentralisierten Authentifizierungsmodell, das als „Web of Trust“ bezeichnet wird. Dieses „Web of Trust“ ist ein Konzept, das Authentizität gewährleistet, indem es einen öffentlichen Schlüssel an seinen Besitzer bindet. Es stützt sich nicht auf eine zentrale Behörde, sondern auf das Vertrauen zwischen den einzelnen Benutzern des Netzes.

## 6.4 Kryptografie mit elliptischer Kurve

Eine Herausforderung bei RSA besteht darin, dass Algorithmen zur Primfaktorzerlegung immer effizienter werden, je größer die Größe der zu faktorisierenden Zahlen wird. Daher werden die Schlüssellängen, die für RSA verwendet werden müssen, immer größer und größer, sodass dies speziell für kleine Geräte oder Smartcards keine langfristig tragfähige Lösung ist.

Abbildung 17: Beispiel einer elliptischen Kurve



Quelle: Jasmin Ćosić 2020.

Die Kryptografie mit elliptischen Kurven (ECC) ist ein Ansatz zur Public-Key-Kryptografie, der auf der algebraischen Struktur elliptischer Kurven über endlichen Feldern basiert. ECC erfordert im Vergleich zur Nicht-EC-Kryptografie kleinere Schlüssel, um ein gleichwertiges Sicherheitsniveau zu bieten.

Die Mathematik ist nicht so einfach wie bei RSA und wird in diesem Kurs nicht behandelt. In diesem Bereich der Mathematik bilden die Punkte auf der Kurve eine Struktur, die als Gruppe bezeichnet wird. Sie nutzt die horizontale Symmetrie jeder elliptischen Kurve sowie die Tatsache, dass sich beim Zeichnen einer Linie, die zwei Punkte auf der Kurve verbindet, diese an genau einer weiteren Stelle mit der Linie schneidet. Nun verwenden wir die symmetrische Struktur der Kurve, um den Punkt auf der anderen Seite der Symmetriechse der Kurve abzuleiten. Es stellt sich heraus, dass, wenn man zwei Punkte hat, ein Anfangspunkt  $n$ -mal mit sich selbst „gestrichelt“ ist, um zu einem Endpunkt zu gelangen, man  $n$  herausfindet, wenn man nur den Endpunkt kennt und der erste Punkt hart ist. Ist nur der resultierende Punkt dieser Operation bekannt, ist es äußerst schwierig zu verstehen, welche Kombination von anderen Punkten dieses Ergebnis lieferte, daher liegt hier eine Falltürfunktion vor.

## 6.5 Hash-Funktion

In der Mathematik bildet eine Hash-Funktion Daten mit variabler Eingabegröße auf eine Menge von Daten mit fester Größe ab. Sie ist daher normalerweise nicht umkehrbar. Die Zielmenge wird als Hash oder Digest bezeichnet. Eine rein mathematische Hash-Funktion ist nicht resistent gegen kryptografische Angriffe, da sie nicht für die Kryptografie auslegt ist.

### Hash-Funktion

Eine Hash-Funktion ist eine „Einweg“-Funktion, die den „Hash“ einer Datei erzeugt.

Eine kryptografische **Hash-Funktion** ist gegen eine Reihe von kryptografischen Angriffen resistent. Sie verwenden daher Folgendes:

1. Urbildresistenz: Für ein gegebenes  $h$  im Ausgaberaum der Hash-Funktion ist es schwierig, eine Nachricht  $x$  mit  $H(x) = h$  zu finden. Dies ist eine alternative Art und Weise zu sagen, dass  $H$  eine Einwegfunktion sein muss.
2. zweite Urbildresistenz: Für eine bestimmte Botschaft  $x_1$  ist es schwierig, eine zweite Botschaft  $x_2 \neq x_1$  mit  $H(x_1) = H(x_2)$  zu finden. Dies wird auch als schwacher Kollisionswiderstand bezeichnet.
3. Kollisionswiderstand: Es ist schwer, ein Nachrichtenpaar  $x_1 \neq x_2$  mit  $H(x_1) = H(x_2)$  zu finden.

Es ist klar, dass der Kollisionswiderstand nicht erreicht werden kann, wenn die Urbildresistenz nicht erreicht wird.

Kryptografische Hash-Funktionen oder Message Digests (MD), sind Algorithmen, die keine Schlüssel verwenden. Im Idealfall ist es so gut wie unmöglich, den ursprünglichen Inhalt einer gehaschten Datei wiederherzustellen. Dies ist der wichtigste Unterschied zwischen „Hashing“ und „Verschlüsselung“. Hash-Algorithmen werden i. d. R. verwendet, um einen „digitalen Fingerabdruck“ einer Datei zu erstellen, der häufig dazu dient, die Integrität der Datei zu gewährleisten und sicherzustellen, dass die Datei nicht durch einen Virus oder einen Eindringling verändert wurde. Hash-Funktionen werden auch von vielen Betriebssystemen verwendet, um Passwörter sicher zu speichern.

Abbildung 18: Hash-Funktion

Eingabe	Funktion	Digest/Hash
Die Macht	kryptografische Funktion (z. B. MD5)	b25f5b9eb6fd8c673543044beccc10c1
Die Macht ist stark		0bd79bf751c68e50a03555b66f93de97
Die Macht ist stark in meiner Familie		bbd0bec61239553975084aaf93473372

Quelle: Jasmin Ćosić 2020.

Wir können versuchen, mit der Zeichenfolge „IUBH“ zu experimentieren:. Als Ergebnis des Hashings mit der MD5-Funktion erhalten wir die Zeichenfolge „34d4d02d2d2f87b03e94ec3754b64f1392“. Die Zeichenfolge „IUBH is your future“ ergibt die MD5-Zusammenfassung „badae2ff12f456a2da21328d982670a6“. Der Hash hat die gleiche Größe, unterscheidet sich aber völlig vom vorherigen. Häufig verwendete Wörter und ihre Hashes sind in sogenannten „Regenbogentabellen“ (Rainbow tables) enthalten, die zum Hacken von Passworddateien und zur Ableitung der Originalpasswörter verwendet werden.

Es gibt viele verschiedene Hash-Funktionen, die beliebtesten aber sind die der MD4-Familie. MD5, SHA und RIPEMD basieren auf dem MD4-Algorithmus. MD4 war eine innovative Idee von Ronald Rivest, MD5 dann eine ausgebauten Version, die er 1991 vorschlug. MD5 war bald u. a. in Internet-Sicherheitsprotokollen, zur Berechnung von Prüfsummen von Dateien oder zur Speicherung von Passwort-Hashes weit verbreitet. 1993 veröffentlichte das NIST einen neuen MD-Standard namens SHA (Secure Hash Algorithm). Die erste Version war SHA-0, später umbenannt in SHA-1, der ein Ersatz für MD5 ist, da dieser sich als nicht mehr sicher erwies.

2001 schließlich führte das NIST drei weitere Varianten von SHA-1 ein: SHA-256, SHA-384 und SHA-512 mit einer Message-Digest-Länge von 256, 384 bzw. 512 Bit, und im Jahr 2004 wurde SHA-224 als geeignet für die Sicherheitsstufe von 3DES eingesetzt. Diese vier Hash-Funktionen werden oft als SHA-2 bezeichnet.

**Tabelle 8: MD4-Familie von Hash-Funktionen**

<b>Algorithmus</b>		<b>Output [Bit]</b>	<b>Input [Bit]</b>	<b>Rundenanzahl</b>	<b>Kollisionen gefunden</b>
MD5		128	512	64	ja
SHA-1		160	512	80	noch nicht
SHA-2	SHA-224	224	512	64	nein
	SHA-256	256	512	64	nein
	SHA-384	384	1.024	80	nein
	SHA-512	512	1.024	80	nein

Quelle: Paar/Pelzl 2010.

Ähnlich wie bei der Auswahl von Rijndael als symmetrischer Standard-Verschlüsselungsalgorithmus (der damals AES hieß), rief die US-amerikanische Standardisierungsorganisation einen Wettbewerb für einen neuen kryptografischen Hash-Algorithmus ins Leben, der dazu führte, dass der KECCAK-Algorithmus 2012 als neuer SHA-3-Algorithmus ausgewählt wurde. Es wurden vier Hash-Algorithmen mit fester Länge definiert: SHA3-224, SHA3-256, SHA3-384 und SHA3-512 sowie zwei eng verwandte „erweiterbare Ausgabefunktionen“ (XOFs): SHAKE128 und SHAKE256.

Derzeit sind nur die vier SHA-3-Algorithmen mit fester Länge zugelassene Hash-Algorithmen, die Alternativen zur SHA-2-Familie von Hash-Funktionen bieten. Die XOFs können vorbehaltlich zusätzlicher Sicherheitsüberlegungen zu Hash-Funktionen spezialisiert werden. Richtlinien für die Verwendung der XOFs werden in Zukunft zur Verfügung gestellt (NIST 2019).

**Tabelle 9: SHA-3-Familie**

<b>Name</b>	<b>Raute-Länge (Ausgabe)</b>	<b>Blockgröße</b>	<b>Kapazität</b>	<b>Stärken im Sicherheitsbereich (Bits)</b>
SHA3-224	224	1.152	448	224
SHA3-256	256	1.088	512	256
SHA3-384	384	832	768	384
SHA3-512	512	576	1.024	512
SHAKE128	Variable (n)	1.344	256	min (n, 128)
SHAKE256	Variable (n)	1.088	512	min (n, 256)

Quelle: Jasmin Ćosić 2020.

Einige der bisher verwendeten Hash-Funktionen sind nicht kollisionsresistent. Ein Beispiel hierfür ist SHA-1, bei dem gezeigt wurde, dass mehrere Dokumente erstellt werden können, die den gleichen Hash-Wert erzeugen. Er sollte nicht mehr verwendet werden. Derzeit (Stand: Ende 2020) ist SHA3 die zuverlässigste Option.

## 6.6 Sicherer Schlüsselaustausch

Wie bereits erwähnt, besteht eines der Hauptprobleme bei der sicheren Kommunikation darin, wie ein Schlüssel zwischen zwei Parteien ausgetauscht werden kann, die verschlüsselte Informationen austauschen müssen (d. h. Sender und Empfänger). Diese Methode des Austauschs eines Schlüssels wird auch als sicherer Schlüsselaustausch oder Schlüsselaufbau bezeichnet.

In der symmetrischen Kryptografie gibt es nur einen Schlüssel, den geheimen Schlüssel, der ausgetauscht werden muss. Das bedeutet, dass Sender und Empfänger zwecks vertraulicher Kommunikation den geheimen Schlüssel austauschen müssen, bevor sie verschlüsselte Nachrichten austauschen können. In der asymmetrischen Kryptografie hingegen werden der private und der geheime Schlüssel verwendet, und wir müssen den öffentlichen Schlüssel der anderen Person kennen. Der private Schlüssel sollte privat bleiben und wird nicht ausgetauscht. In Situationen, in denen wir mit mehr als einer Person kommunizieren, muss ein System zur Schlüsselverwaltung – das Cryptographic Key Management System (CKMS) – eingerichtet werden. Dieses muss Regeln für diese Informationen festlegen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Authentifizierung der Quellen schützen. CKMS besteht aus Schlüsselaustausch, -speicherung und -nutzung. Schlüsselaustausch ist ein Prozess, bei dem kryptografische Schlüssel zwischen Sender und Empfänger unter Verwendung eines kryptografischen Algorithmus ausgetauscht werden.

Das Diffie-Hellman-Schlüsselaustauschprotokoll wurde 1976 von Whitfield Diffie und Martin Hellman (basierend auf den Konzepten von Ralph Merkle) veröffentlicht. Nach dem Beitrag des Studenten Ralph Merkle im Jahr 2002 schlug Martin Hellman vor, den Algorithmus in „Diffie-Hellman-Merkle“-Schlüsselaustausch umzubennnen.

Der Diffie-Hellman-Schlüsselaustausch ermöglicht es Benutzern (Parteien, die sich vorher noch nicht getroffen haben), sicher Schlüssel auszutauschen, selbst wenn sie eine unsichere Verbindung benutzen (Diffie/Hellman 1976). Wie bei anderen asymmetrischen Kryptosystemen ist die Geheimhaltung dieses Schlüsselaustauschs durch die Verwendung einer Einwegfunktion, in diesem Fall des diskreten Logarithmus, gewährleistet. Dies war das erste veröffentlichte asymmetrische Kryptosystem, nachdem bis dahin nur symmetrische Kryptosysteme bekannt waren.

Der Diffie-Hellman-Schlüsselaustausch ist eine der gebräuchlichsten Methoden, um Schlüssel sicher zu verteilen, und wird deshalb häufig in Sicherheitsprotokollen wie TLS, IPsec, SSH oder PGP implementiert. Dies macht ihn zu einem integralen Bestandteil unserer sicheren Kommunikation. In der Praxis wird der Diffie-Hellman-Schlüsselaustausch selten allein verwendet, da er keine Authentifizierung bietet – ohne diese sind Benutzer

anfällig für Man-in-the-Middle (MitM)-Angriffe. Aus diesem Grund wird Diffie-Hellman oft in Kombination mit RSA oder anderen Algorithmen implementiert, um die Authentifizierung für die Verbindung bereitzustellen (Lake 2019).

Der Diffie-Hellman-Algorithmus wird im Folgenden skizziert.

1. Alice und Bob, die einen Schlüssel austauschen wollen, einigen sich auf eine riesige Primzahl  $n$  und eine riesige Zahl  $g$ . Diese Zahlen können öffentlich sein.
2. Alice wählt eine Zufallszahl  $x$  und sendet  $X = g^x \text{ mod } n$  an Bob.  $(X, g, n)$  ist ihr öffentlicher und  $(x, g, n)$  ihr privater Schlüssel.
3. Bob wählt eine riesige Zufallszahl  $y$  und sendet  $Y = g^y \text{ mod } n$  zu Alice.  $(Y, g, n)$  ist sein öffentlicher Schlüssel und  $(y, g, n)$  ist sein privater Schlüssel.
4. Alice berechnet den geheimen Schlüssel  $k = Y^x \text{ mod } n$ .
5. Bob berechnet den geheimen Schlüssel  $k' = X^y \text{ mod } n$ .

Daher  $k = k'$ , als  $k = Y^x \text{ mod } n = g^{xy} \text{ mod } n = X^y \text{ mod } n = k'$ .

Ein Kryptoanalytiker, der die Verbindung belauscht, kennt  $n$ ,  $g$ ,  $X$  und  $Y$ , aber nicht  $k$ . Er versucht, die Gleichungen  $Y = g^y \text{ mod } n$  und  $X = g^x \text{ mod } n$  zu lösen, um  $x$  und  $y$  zu erhalten. Dies ist zwar möglich, aber sehr schwierig und als Problem der diskreten Logarithmen bekannt.

Perfect Forward Secrecy (PFS) ist ein „Key-Agreement“-Protokoll, das für jede Sitzung zwischen einem Client und einem Server oder z. B. zwischen zwei Benutzern einen eindeutigen öffentlichen Schlüssel verwendet. Der daraus resultierende Schlüssel wird niemals zur Ableitung eines anderen Schlüssels verwendet. So wird sichergestellt, dass eine aktuelle Sitzung nicht durch die Verwendung eines Schlüssels gefährdet werden kann, der von einer früheren Sitzung abgeleitet wurde, und frühere Sitzungen nicht von jemandem entschlüsselt werden können, dem es gelingt, den aktuellen Schlüssel zu erhalten (Villanova University 2019). Dieses Protokoll zur Schlüsselvereinbarung verwendet komplexe mathematische Verfahren und schreckt Brute-Force-Hackingversuche ab. Sollte doch ein Angreifer doch in den Besitz eines Sitzungsschlüssels gelangen, erhält er schlimmstenfalls Zugang zu einer einzigen Sitzung.

## **Steganografie**

Die Steganografie ist eine Methode, um eine Nachricht in einem anderen Medium heimlich zu verstecken. Ihr Hauptziel besteht darin, die Aufdeckung der Nachricht zu vermeiden, aber diese Nachricht könnte mit den gleichen, oben erwähnten Methoden verschlüsselt werden. Eine der einfacheren Methoden ist die vom Least Significant Bit (LSB). Normalerweise bei einem Bild- oder Videostrom verwendet, wird bei dieser Methode das letzte Bit der Farbkodierung geändert. Die Änderung ist für das menschliche Auge nicht sichtbar, daher verdeckt sie die Botschaft. Diese Methode ist jedoch auch leicht zu erkennen, wenn ein Analytiker danach sucht, und es stehen ausgefeilte Methoden zur Verfügung.



## ZUSAMMENFASSUNG

In dieser Einheit wird das Konzept der symmetrischen und asymmetrischen Kryptologie vorgestellt und erklärt, wie sie funktionieren. Es wird das Konzept einer Falltürfunktion als Grundlage für die asymmetrische Kryptografie vorgestellt, die durch Primfaktorzerlegung und durch Kryptografie mit elliptischen Kurven implementiert wird. Hash-Funktionen werden ebenfalls besprochen, wobei zusätzlich das De-Hashing behandelt wird. Schließlich werden der sichere Schlüsselaustausch und Methoden zu dessen Ausführung beschrieben.



# LEKTION 7

## KRYPTOGRAFISCHE ANWENDUNG

### LERNZIELE

Nach der Bearbeitung dieser Lektion werden Sie wissen, ...

- was die grundlegenden Konzepte von angewandter Kryptografie und kryptografischer Anwendung sind.
- was es mit sicheren Internet-Protokollen auf sich hat.
- wie Kryptografie in der Internetsicherheit angewendet werden kann.
- warum angewandte Kryptografie für IT-Prozesse so wichtig ist.

## 7. KRYPTOGRAFISCHE ANWENDUNG

# Einführung

Die Kryptografie war lange Zeit eine esoterische Wissenschaft mit sehr wenigen praktischen Anwendungen. Sie wurde vom Militär und von Regierungen eingesetzt, erreichte aber ohne entsprechende Rechenleistung nie die breite Masse. In der ersten Hälfte des 20.Jahrhunderts wurden elektromechanische Verschlüsselungsmaschinen erfunden, die berühmteste davon war die ENIGMA, die im Zweiten Weltkrieg von den Achsenmächten eingesetzt wurde. Mit der Internet-Revolution ab den 1970er-Jahren wurde deutlich, dass die Kryptografie notwendig ist, um die Privatsphäre der Benutzer zu schützen und moderne Geschäftsmodelle wie den elektronischen Handel zu ermöglichen.

Heutzutage spielt die Kryptografie in unserem täglichen Leben eine entscheidende Rolle. So sind zum Beispiel über 80 % des Internetverkehrs verschlüsselt; Verschlüsselung wird im elektronischen Zahlungsverkehr eingesetzt und auch bei der privaten Kommunikation über E-Mail oder Chat-Dienste wird aus Sicherheitsgründen auf sie zurückgegriffen. Andererseits stellen Strafverfolgungsbehörden den Einsatz von Verschlüsselung infrage und versuchen beim Sammeln von Beweisen, Daten zu entschlüsseln. Zu guter Letzt hat die Kryptografie die Blockchain-Technologie ermöglicht, die in Zukunft die Art und Weise verändern könnte, wie wir Werte abwickeln und speichern.

## 7.1 Digitale Unterschriften

Beim Austausch von Dokumenten liefert eine Signatur den Beweis dafür, dass die Integrität und Authentizität des Dokuments gegeben ist. Siegel, Stempel und das Anbringen von Initialen auf jeder Seite verstärken dies zusätzlich. Eine **digitale Signatur** transportiert diese Methoden unter Verwendung von Kryptografie in die elektronische Welt.

Eine digitale Signatur ist eine kryptografische Operation, bei der ein Absender eine Nachricht oder Datei unter Verwendung seiner Identität versiegelt. Digitale Signaturen werden verwendet, um eine Nachricht zu authentifizieren und ihre Integrität zu gewährleisten, schützen jedoch nicht die Vertraulichkeit einer Nachricht und ersetzen auch nicht die Verschlüsselung. Digitale Signaturen funktionieren, indem sie die Hashes von Nachrichten verschlüsseln. Empfänger überprüfen die Integrität und Authentizität, indem sie die Hashes entschlüsseln und mit der ursprünglichen Nachricht vergleichen.

Eine digitale Signatur bietet auch eine Nachweisbarkeit, d. h. der Absender kann weder die Urheberschaft noch die Gültigkeit des Dokuments bestreiten. Eine digitale Signatur dient dem gleichen Zweck wie eine manuelle Unterschrift, jedoch muss betont werden, dass Letztere viel einfacher zu fälschen ist. Ein weiterer Grund dafür, dass die digitale Signatur überlegen und beinahe fälschungssicher ist, liegt darin, dass eine digitale Signatur sowohl die Integrität der Nachricht als auch die Identität des Unterzeichners bescheinigt (PGP 2002).

## **Digitale Unterschrift**

Mit der digitalen Signatur können wir die Authentizität und Integrität überprüfen und die Unabstreitbarkeit erreichen.

Laut NIST ist eine elektronische Signatur ein kryptografischer Mechanismus, der dazu dient, Herkunft (Authentizität) und Inhalt (Integrität) einer Nachricht zu verifizieren (Gutmann/Roback 1995). Der Unterschied zwischen einer digitalen Signatur und einer elektronischen Unterschrift liegt in der Methode zur Identifizierung von Unternehmen und Unterzeichnern. Digitale Signaturen betonen eine Public-Key-Infrastruktur (PKI) in den Signaturprozess ein, um sowohl die Partei zu identifizieren, die eine Signatur beantragt, als auch jene, die eine Signatur bereitstellt. Elektronische wie digitale Signatur sind gleichermaßen in der Lage, einen Unterzeichner zu identifizieren und beide sind rechtlich gesehen Signaturen, je nach der Gesetzgebung, in deren Anwendungsbereich sie verwendet werden. Ein Beispiel ist die eIDAS-Richtlinie (electronic Identification, Authentication and Trust Services) in der Europäischen Union, die „Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierungs- und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG“ (EU 2014). Andere Länder haben ähnliche Regelungen umgesetzt.

Eine digitale Signatur ist heutzutage eines der wichtigsten und am weitesten verbreiteten kryptografischen Werkzeuge. Zu den Anwendungen, die derzeit eine digitale Signatur verwenden, gehören u. a. E-Commerce, die rechtsgültige Unterzeichnung von Verträgen sowie sichere Software-Updates (Paar/Pelzl 2010).

In der folgenden Liste sind die Sicherheitsziele aufgeführt, die mit elektronischen Signaturen erreicht werden (ebd.):

- **Integrität:** Die Nachrichten wurden während der Übertragung nicht geändert.
- **Authentifizierung der Nachricht:** Der Absender einer Nachricht ist authentisch.
- **Nichtabstreitbarkeit:** Der Absender einer Nachricht kann die Erstellung der Nachricht nicht leugnen.

Zusätzlich zu den vier Hauptsicherheitsdiensten enthält die folgende Liste einige weitere Sicherheitsdienste, die häufig in Kombination mit elektronischen Signaturen erreicht werden (ebd.):

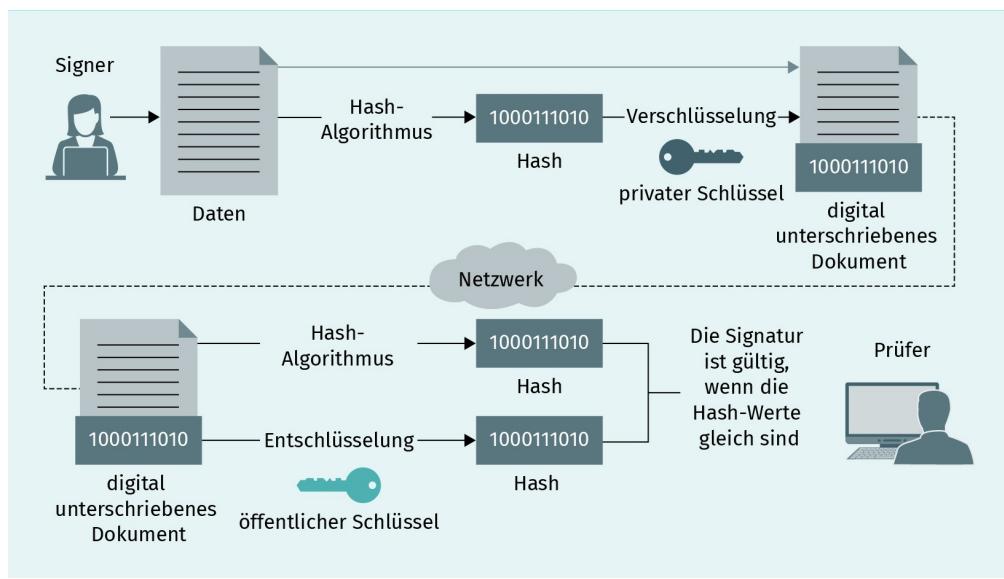
- Die **Vertraulichkeit** wird nicht direkt durch digitale Signaturen unterstützt, sondern ist typischerweise Teil einer Public-Key-Infrastrukturlösung, sodass sie mit demselben Schlüsselpaar implementiert wird.
- **Identifikation:** ermittelt und verifiziert die Identität einer Entität, z. B. einer Person, eines Computers oder einer Kreditkarte.
- **Zugangskontrolle:** schränkt den Zugang zu den Ressourcen für privilegierte Einheiten ein.
- **Verfügbarkeit:** bietet die Sicherheit, dass das elektronische System zuverlässig verfügbar ist.
- **Protokolle:** liefern Nachweise über sicherheitsrelevante Aktivitäten, z. B. durch das Führen von Protokollen über bestimmte Ereignisse.
- **physische Sicherheit:** bietet Schutz gegen physische Manipulation und/oder Reaktionen auf physische Manipulationsversuche.
- **Anonymität:** bietet Schutz vor Entdeckung und Missbrauch der Identität.

#### **Anonymität**

Dieses Konzept bietet Schutz vor Entdeckung und Missbrauch der Identität.

Digitale Signaturen verwenden asymmetrische Kryptografie. Die folgende Abbildung zeigt die Funktionsweise einer digitalen Signatur.

Abbildung 19: Wie digitale Signaturen funktionieren



Quelle: DocuSign o. J.

Der Prozess des digitalen Signierens besteht gewöhnlich aus drei Schritten. Diese sind:

- Schlüsselerzeugung,
- Unterzeichnung, und
- Verifizierung.

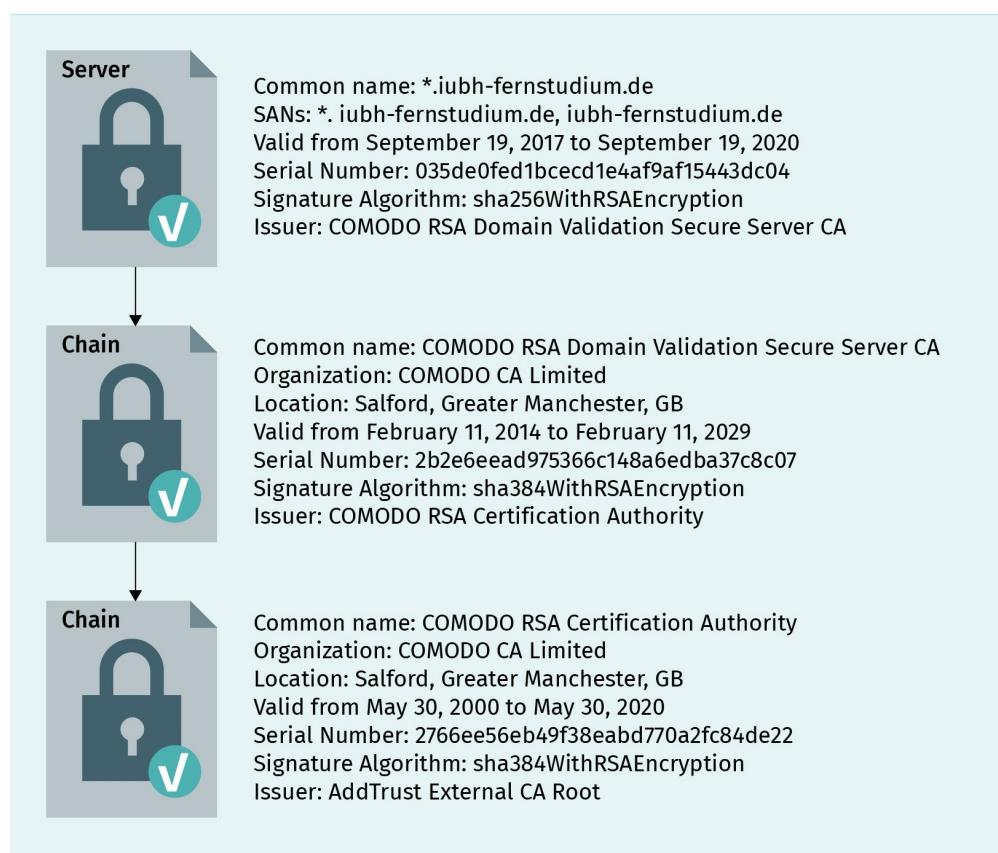
Das Verständnis der Public Key Cryptography (PKC) ist entscheidend für ein besseres Verständnis und eine bessere Nutzung des Konzepts der digitalen Signatur. Public Key Cryptography ist relativ neu – Diffie, Hellman und Merkle stellten sie 1976 vor. Sie bedient sich der asymmetrischen Kryptografie mit einem öffentlichen und einem privaten Schlüsselpaar. Dabei handelt es sich um öffentliche Schlüssel, die weit verbreitet sein können, und private Schlüssel, die nur dem Besitzer bekannt sind. In einem PKC-System kann jede Person eine Nachricht mit dem öffentlichen Schlüssel des Empfängers verschlüsseln. Nachrichten, die auf diese Weise verschlüsselt wurden, können nur mit dem privaten Schlüssel des Empfängers entschlüsselt werden.

Die Public-Key-Infrastruktur (PKI) ist eine zentralisierte Funktion, die zum Speichern und Veröffentlichen öffentlicher Schlüssel sowie anderer Informationen verwendet wird. Sie stellt sich der Herausforderung des Austauschs gültiger öffentlicher Schlüssel. Hier gibt es verschiedene Implementierungen, eine gemeinsame ist z. B. der Active Directory-Dienst von Microsoft. Eine PKI besteht aus zusätzlichen Diensten wie der Zertifizierungsstelle (Certificate Authority; CA), einem digitalen Zertifikat, Software für die Anmeldung von Endbenutzern sowie Tools für die Verwaltung, Erneuerung und Sperrung von Schlüsseln und Zertifikaten (DocuSign o. J.).

Wenn ein Dokument unterzeichnet wird, brauchen wir die Gewissheit, dass die Dokumente und Schlüssel gültig sind und sicher erstellt wurden. Zertifizierungsstellen sind eine Art „Vertrauensdienstleister“, also Drittorganisationen, die die erforderlichen digitalen Zertifikate bereitstellen können und weithin als zuverlässige Quellen zur Gewährleistung der Schlüsselsicherheit akzeptiert wurden. Sowohl die Entität (der Absender des Dokuments) als auch der Empfänger müssen der Verwendung derselben CA zustimmen. Eine CA ist eine Firma oder Organisation, welche die Identitäten von Entitäten validiert. Entitäten können Websites, E-Mail-Adressen, Firmen, einzelne Personen o. ä. sein. Nach der Validierung binden CAs sie an kryptografische Schlüssel, indem sie elektronische Dokumente wie digitale Zertifikate ausstellen (ebd.).

Ein digitales Zertifikat ist ein digitaler Berechtigungsnachweis, der aus einem öffentlichen Schlüssel und einem Informationsblock besteht. Dieser identifiziert den Inhaber des Zertifikats. Die folgende Abbildung zeigt eine Kette von Zertifikaten und ihre Beziehung zu verschiedenen CAs in einer Hierarchie.

**Abbildung 20: Digitale Zertifikatskette**



Quelle: Jasmin Ćosić 2020.

Weitere Dienste in einer PKI sind die Registrierungsstelle (Registration Authority – RA), die neben einer CA arbeitet, um Anträge auf neue Zertifikate anzunehmen. Sie verifiziert die Authentizität eines Antragstellers und stellt, wenn sie mit den bereitgestellten Dokumenten zufrieden ist, ein digitales Zertifikat aus. Eine Zertifikatswiderrufsliste (Certificate

**PGP**  
Es steht für „Pretty Good Privacy“ und braucht keine CAs, sondern stützt sich auf das Netz des Vertrauens.

Revocation List – CRL) ist eine elektronische Liste von digitalen Zertifikaten, die vor ihrem Ablaufdatum widerrufen wurden. Dies kann der Fall sein, wenn ein privater Schlüssel gestohlen wurde, ein Zertifikat irrtümlich oder aus einem anderen Grund ausgestellt wurde.

Ein anderes Konzept, das digitale Signaturen ohne eine PKI implementiert, ist **PGP oder Pretty Good Privacy**, welches ursprünglich 1991 von Phil Zimmerman beschrieben wurde. PGP ist ein Verschlüsselungsprogramm, das verwendet wird, um Vertraulichkeit und Authentifizierung zu erreichen. Seine Funktionen umfassen das Signieren, Verschlüsseln und Entschlüsseln von Text, Dateien, E-Mails usw. Ein PGP-Benutzer verwaltet einen lokalen Schlüsselbund aller seiner bekannten und vertrauenswürdigen öffentlichen Schlüssel (ohne CAs). Der Benutzer trifft sein eigenes Urteil über die Vertrauenswürdigkeit eines Schlüssels mithilfe eines sogenannten „Web of Trust“. Dieser Begriff bezeichnet den Umstand, wenn zwei Personen, die einander vertrauen, sich treffen und ihre öffentlichen Schlüssel miteinander teilen. Sie vertrauen auch den Schlüsseln, denen die andere Person vertraut, sodass ein „Web of Trust“ entsteht (Cole/Krutz/Conley 2005).

PGP kann zum Signieren oder Verschlüsseln von E-Mail-Nachrichten mit einem einfachen Mausklick verwendet werden. Je nach Version von PGP verwendet die Software SHA oder MD5 zur Berechnung des Nachrichtenhashs, CAST, Triple-DES oder IDEA für die Verschlüsselung und RSA oder DSS/Diffie-Hellman für den Schlüsselaustausch und digitale Signaturen (Kessler 2020).

Aufgrund von Bedenken hinsichtlich Lizenzierung und Patenten entstand eine neue, kostenlose Version von PGP, die über die International PGP Page und die OpenPGP Alliance (beschrieben in RFC 4880) erhältlich ist. Das Open-Source-Programmierprojekt hat GnuPG entwickelt. PGP (oder GnuPG) erfordert zum Funktionieren die Kombination von zwei Ver-/Entschlüsselungsschlüsseln – öffentlich und privat. Der öffentliche Schlüssel wird immer mit anderen geteilt und der Absender verwendet ihn, um die Nachricht zu verschlüsseln. Die Nachricht wird gesendet, aber niemand kann sie entschlüsseln, selbst wenn er versucht, die Nachricht zu lesen. Die einzige Person, die die Nachricht entschlüsseln kann, ist der Empfänger, der im Besitz des privaten Schlüssels ist.

## 7.2 Sichere Internet-Protokolle

Das Internet ist kostenlos, einfach zu benutzen und Teil unseres Lebens. Zum Schutz unserer Daten, die über Internetkanäle verschickt werden, sind verschiedene Protokolle erforderlich. Diese können für Dateiübertragung, E-Mail-Kommunikation, finanziellen Transaktionen u. v. m. verwendet werden. Protokolle wie HTTPS, SFTP, SSH, IPSec, SSL und TLS sind Teil vieler Anwendungen, die wir täglich benutzen. Netzwerksicherheitsprotokolle wurden entwickelt, um den unbefugten Zugriff auf alle Daten zu verhindern, die über ein Netzwerk gesendet werden.

**Sichere Internet-Protokolle** implementieren zur Datensicherung Kryptografie- und Verschlüsselungstechniken, was bedeutet, dass verschlüsselte Daten nur mit einem speziellen Algorithmus, einer mathematischen Formel, einem logischen Schlüssel oder einer Kombination von allen entschlüsselt werden können.

Internet Protocol Security (IPSec) ist ein offener Standard zur Gewährleistung privater und sicherer Kommunikation über IP-Netzwerke unter Verwendung kryptografischer Sicherheitsdienste. IPsec-basierte Verschlüsselungsverfahren bieten viele verschiedene Sicherheitsmerkmale, darunter ...

- ... Vertraulichkeit,
- Authentifizierung,
- Datenintegrität und
- Schutz vor Data Replay-Angriffen (Cole/Krutz/Conley 2005).

IPSec arbeitet im Tunnel- oder Transportmodus:

Im Transportmodus bleibt das gesamte IP-Paket (die Kopf- und Datenfelder) ungekapselt, es werden jedoch entsprechende Änderungen an den Protokollfeldern vorgenommen, um es als IPSec-Paket für den Transportmodus darzustellen. Auf den Hosts ist Software direkt installiert, sodass sie IPSec-Pakete des Transportmodus verarbeiten können.

Im Tunnelmodus findet die vollständige Kapselung des IP-Pakets im Datenfeld des IPSec-Paketes statt. Die Router und Gateways sind normalerweise an der Handhabung und Verarbeitung der IPSec-Pakete im Transportmodus beteiligt, doch kann der getunnelte Modus Ziele adressieren, die an der Quelle möglicherweise nicht vorgesehen sind, und bietet zusätzliche Sicherheit, indem er das Quell- und Zielfeld verbirgt.

IPsec besteht aus den zwei Hauptprotokollen ESP (Encapsulating Security Payload) und AH (Authentication Header). Wenn ESP verwendet wird, wird der gesamte eingekapselte Verkehr verschlüsselt. Wenn AH verwendet wird, dann nur das Authentifizierungsmerkmal von IPsec.

IPsec kann anstelle eines Secure Internet Protocol-Netzwerks verwendet werden, um eine sichere verschlüsselte Kommunikation zwischen zwei Hosts bereitzustellen. Es kann auch in virtuellen privaten Netzwerken (VPNs) zur Anwendung kommen.

Zu den kryptografischen Algorithmen, die mit IPsec verwendet werden können, gehören:

- HMAC-SHA1/SHA2 für Integritätsschutz und Authentizität.
- TripleDES-CBC für Vertraulichkeit.
- AES-CBC für Vertraulichkeit.
- AES-GCM sowohl für die Vertraulichkeit als auch für die Authentifizierung.
- ChaCha20 + Poly1305 für Vertraulichkeit wie auch Authentifizierung. IPsec verwendet kryptografische Sicherheitsdienste.

#### **Sichere Internet-Protokolle**

Beinahe der gesamte Verkehr in modernen Netzwerken wird mit sicheren Internet-Protokollen verschlüsselt.

**HTTPS** (Hypertext Transfer Protocol Secure) ist ein Protokoll, das die Integrität und Vertraulichkeit von Daten zwischen dem Computer eines Benutzers und einer Website schützt. Daten, die über HTTPS gesendet werden, werden über eine Verbindung mit dem TLS-Protokoll (**Transport Layer Security**) gesichert.

#### Sicherheit der Transportschicht

TLS arbeitet oben auf der TCP-Schicht im TCP/IP-Protokollstapel.

Das grundlegende Ziel des TLS besteht darin, Authentifizierung und Integritätsverhandlungen zwischen den beteiligten Anwendungen zu ermöglichen. Die Verhandlungen können genutzt werden, um zu entscheiden, welche Verschlüsselungsalgorithmen beim bevorstehenden Datenaustausch zwischen den beiden Parteien verwendet werden sollen. Heute verfügen die meisten Webbrower, wie Chrome und Firefox, über eine eingebaute TLS-Unterstützung, die sie für den Endbenutzer relativ transparent macht (Cole/Krutz/Conley 2005).

#### Secure Sockets Layer

SSL ist eine alte Version von TLS.

**Secure Sockets Layer (SSL)** und sein Nachfolger Transport Layer Security (TLS) sind Verschlüsselungsprotokolle, die verwendet werden, um eine verschlüsselte Verbindung zwischen Knoten herzustellen – typischerweise zwischen einem Webserver (Website) und einem Browser oder einem Mailserver und einem E-Mail-Client.

TLS stützt sich auf Kryptografie mit öffentlichen Schlüsseln zur gegenseitigen Authentifizierung, Vertraulichkeit und Datenintegrität für Web-Browser. Das System bietet High-End-Sicherheit für die Web-Browser zu sehr geringen zusätzlichen Kosten. Die meisten Transaktionen erfordern einen Schutz zwischen den Servern und den Clients. Die Server erfordern die Verifizierung des Benutzers, wenn entfernte Benutzer proprietäre und vertrauliche Informationen vom Server einer Organisation herunterladen. Es gibt drei Versionen des SSL-Protokolls, die erste Version wurde jedoch nie veröffentlicht. Alle diese SSL-Versionen sind inzwischen veraltet und wurden durch TLS ersetzt. Gegenwärtig (Stand: Ende 2020) ist die aktuelle Version TLS 1.3 und nur die TLS Version 1.2 und höher gilt als sicher.

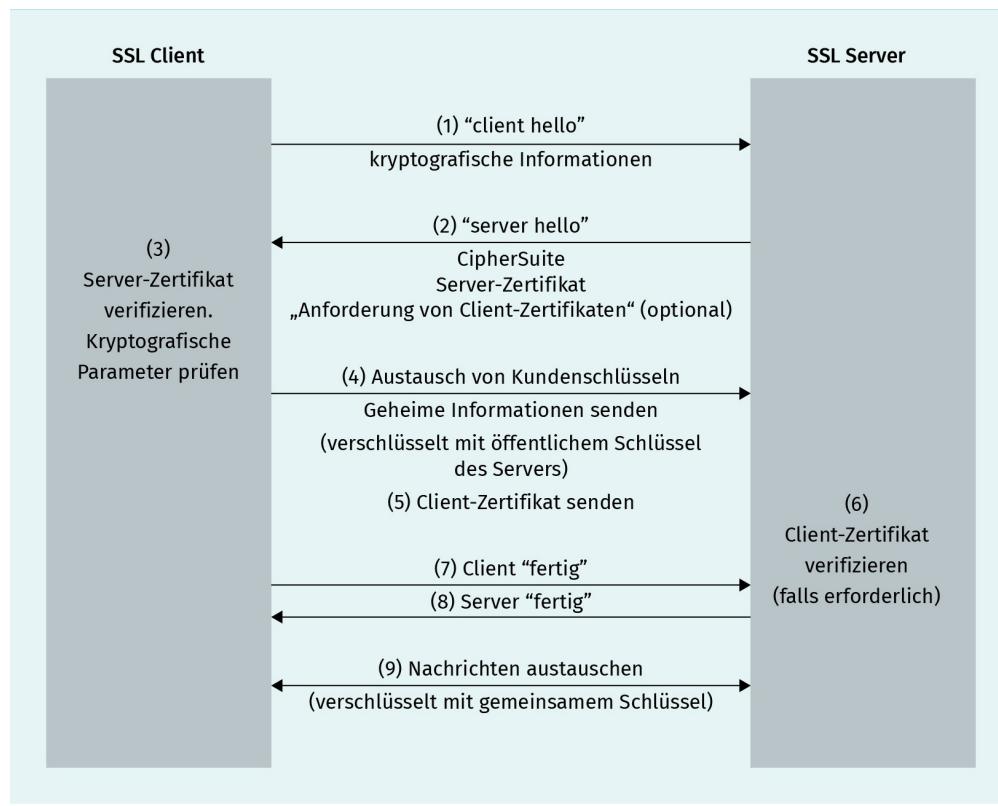
Wenn TLS-Zertifikate (kleine Datendateien, die einen kryptografischen Schlüssel an eine Organisation binden) auf einem (Web-)Server installiert werden, aktivieren sie das „HTTPS“-Protokoll. Dies ermöglicht sichere Verbindungen von einem Webserver zu einem Browser. TLS wird nicht nur zur Sicherung von Kreditkartentransaktionen, Datenübertragungen und Anmeldungen verwendet, sondern ist heute die Norm, wenn es darum geht, das Surfen auf allen möglichen Arten von Websites zu sichern. Dieses Zertifikat muss auf dem Server installiert werden, um eine sichere Sitzung mit dem Webbrower einzuleiten. Nachdem die Verbindung erfolgreich hergestellt wurde, wird der gesamte Webverkehr durch das HTTPS-Protokoll gesichert. Das bedeutet, dass nach der Installation eines Zertifikats auf einem Server HTTP automatisch in HTTPS geändert wird.

Im Folgenden sind die drei Hauptkomponenten des TLS aufgeführt:

- Verschlüsselung (verbirgt die übertragenen Daten vor anderen),
- Authentifizierung (stellt sicher, dass die Seiten, die Informationen austauschen, die sind, für die sie sich ausgeben) sowie
- Integrität (verifiziert, dass die Daten nicht gefälscht oder manipuliert wurden) (Cloudflare o. J.).

Das TLS-Protokoll verschlüsselt Internet-Verkehr aller Art. Der SSL- oder TLS-Handshake ermöglicht es den SSL- oder TLS-Clients und -Servern, die geheimen Schlüssel zu ermitteln, mit denen sie kommunizieren. Der TLS-Handshake ist ein Prozess, der aus mehreren Schritten besteht. Bei einem einfachen TLS-Handshake senden Client und Server „Hallo“-Nachrichten und tauschen Schlüssel, eine Chiffre-Nachricht und eine Fertigmeldung aus. Der mehrstufige Prozess macht TLS so flexibel, dass es in verschiedenen Anwendungen eingesetzt werden kann, da Format und Reihenfolge des Austauschs geändert werden können (Dierks/Rescola 2008).

**Abbildung 21: TLS/SSL Handshake**



Quelle: IBM 2020.

TLS verwendet eine hybride Form der Kryptografie. Die Verbindung wird mittels asymmetrischer Kryptografie hergestellt. Über diese Verbindung wird der Schlüssel ausgetauscht, der anschließend zur symmetrischen Verschlüsselung der Verbindung verwendet wird, da die asymmetrische Kryptografie im Vergleich zur symmetrischen Kryptografie sehr kostspielig und langsam ist.

## 7.3 Blockchain

### Blockchain

Auf der Grundlage von P2P und öffentlichen elektronischen Büchern wird Blockchain verwendet, um den sicheren und manipulationsfreien Datenaustausch zu ermöglichen.

Eine **Blockchain** ist eine wachsende Liste von Datensätzen, die als Blöcke bezeichnet werden. Die Blöcke werden durch Kryptografie miteinander verbunden. Die Blockchain ist normalerweise als Merkle-Trees implementiert. Hashing wird verwendet, um den vorherigen Block zu identifizieren; daher enthält jeder nachfolgende Block den Hash des vorherigen Blocks, einen Zeitstempel und Daten. Eine Blockchain wird als Peer-to-Peer-Netzwerk aufgebaut und ist gegen Manipulationen resistent. Im Gegensatz zu einer klassischen Datenbank ist die Aufzeichnung in einer Blockchain dezentralisiert, sodass es fast unmöglich ist, die Integrität der Aufzeichnungen in der Blockchain zu zerstören.

Knotenpunkte tauschen Daten auf (manipulations-)sichere Weise aus, auch ohne sich gegenseitig vertrauen zu müssen. Blockchain macht dies möglich, weil es Daten mithilfe von Kryptografieregeln speichert, die für Angreifer äußerst schwer zu manipulieren sind (Orcutt 2018). Sie ist jedoch mit Kosten verbunden, denn Blockchain-Datenbanken sind teurer in der Pflege als zentrale Datenbanken wie z. B. relationale Datenbanksysteme.

Die Blockchain-Technologie basiert auf einer Peer-to-Peer-Netzwerktopologie (P2P) und einem „öffentlichen elektronischen Register“. Mit der Blockchain-Technologie können Daten global auf jedem Gerät gespeichert werden. Jeder in diesem Netzwerk kann die Einträge aller anderen in Echtzeit sehen. Diese Funktion der Blockchain ermöglicht es Benutzern, eine „unveränderliche“ Aufzeichnung von Transaktionen zu erstellen. Jede Transaktion wird mit einem Zeitstempel versehen und mit der vorherigen in einer Kette verknüpft. Wird eine neue Gruppe von Transaktionen hinzugefügt, werden die Daten zu einem weiteren Block in der Kette – engl. „Chain“, daher der Name Blockchain. Jede Transaktion auf einer Blockchain wird mit einer digitalen Signatur gesichert, was bedeutet, dass die Authentizität nachgewiesen werden kann. Durch Verschlüsselung und digitale Signaturen bleiben die auf der Blockchain gespeicherten Daten unveränderlich.

Ein Ergebnis der offenen Struktur der Blockchain ist, dass keine Anonymität erreicht werden kann, sondern die Daten nur pseudonymisiert werden. Auch bleiben Daten, die einmal in die Blockchain aufgenommen wurden, dort für immer erhalten. Dies könnte in der Zukunft rechtliche Auswirkungen haben, da auf diese Weise eine Privatsphäre schwierig zu gewährleisten ist. Es könnte zu Situationen kommen, in denen illegale Inhalte auf der Blockchain gespeichert werden, die von niemandem entfernt werden können.

Typische Blockchains verwenden die Elliptische Kurven-Kryptografie (ECC) zum Signieren der Blöcke. Jeder Block in einem Blockchain-Netzwerk speichert einige Informationen innerhalb des Hashs seines vorherigen Blocks. Dieser Hash ist ein eindeutiger Code eines bestimmten Blocks. Wenn wir die Informationen innerhalb des Blocks ändern oder modifizieren, wird auch der Hash des Blocks modifiziert. Einzigartige Hash-Schlüssel, die die Blöcke verbinden, sind der Grund dafür, dass Blockchain sicher ist.

Blockchain kann entweder als öffentlich oder privat klassifiziert werden. In einer öffentlichen Blockchain ist das Register öffentlich und kann von jedem, der Zugang zum Netzwerk in Form einer Internetverbindung hat, eingesehen werden. Private Blockchains werden jedoch nur unter den vertrauenswürdigen Teilnehmern geteilt, z. B. innerhalb einer Firma.

Es gibt vier Hauptmerkmale, die die Blockchain charakterisieren und den zukünftigen Einsatz dieser Technologie bestimmen werden. Diese sind ...

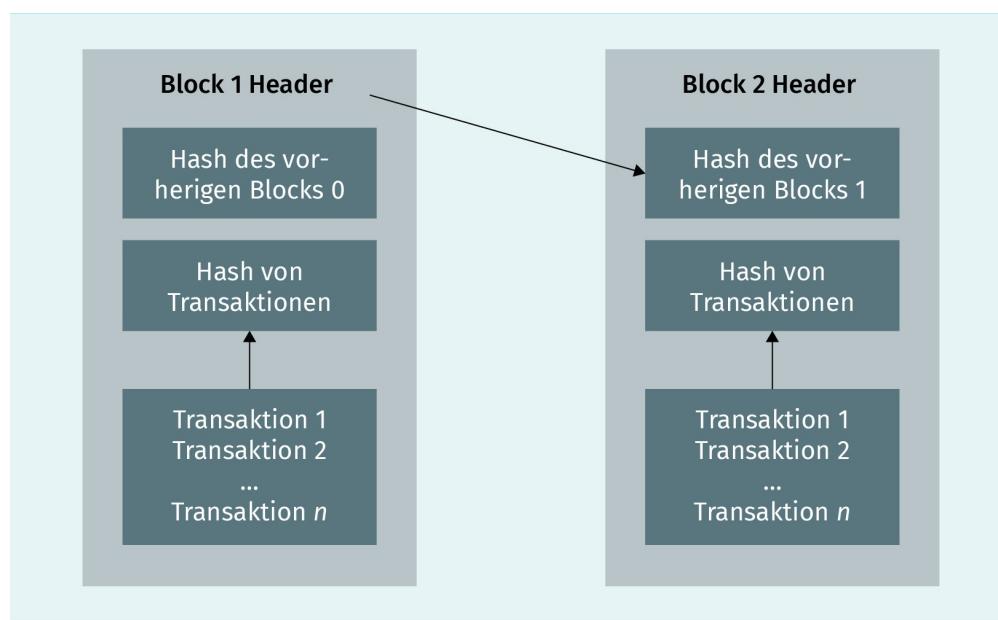
- ... unveränderlich – Die Daten können nicht geändert werden und sind daher integer;
- manipulationssicher – Datenmanipulation wird verhindert oder, wenn sie doch auftritt, sicher erkannt, da Mechanismen zur Bewältigung von Manipulationen vorhanden sind;
- dezentral – Niemand ist Eigentümer des Netzwerks, es gehört allen Einrichtungen, die daran teilnehmen und eine Kopie der aktuellen Blockchain besitzen;
- Peer-to-Peer – Es gibt keinen zentralen Server, was bedeutet, dass alle Peers im Netzwerk einander ebenbürtig sind.

Die Blockchain-Technologie hat viele Anwendungsmöglichkeiten außerhalb der Krypto-Währung. Es gibt zahllose Bereiche, in denen sie derzeit oder in Zukunft eingesetzt wird, darunter die Kommunikation in der Lieferkette, die verteilte Speicherung, digitale Abstimmungen, intelligente Verträge als Rechtsdokumente, der Prozess der Digitalisierung und vieles mehr.

Typische Open-Source-Implementierungen finden Sie beim Hyperledger-Projekt, das von der Linux Foundation (Hyperledger 2018) verwaltet wird. Hyperledger wird oft in privaten Blockchains verwendet, mehrere Cloud-Computing-Anbieter bieten es als Teil ihrer Dienstleistungen an.

Die folgende Abbildung unten stellt eine vereinfachte Blockchain dar.

**Abbildung 22: Blockchain-Schema**



Quelle: Jasmin Ćosić 2020.

## 7.4 Elektronisches Geld

Gängigen Quellen zufolge wird elektronisches Geld („E-Geld“, digitale Währung, digitales Geld oder elektronische Währung) im weitesten Sinne definiert als „elektronische Speicherung eines monetären Wertes auf einem technischen Gerät, das in großem Umfang für Zahlungen an andere Stellen als den E-Geld-Emissenten verwendet werden kann“ (EZB o. J.). E-Geld-Produkte können hardwarebasiert (d. h. Chipkarten) oder softwarebasiert (spezielle Software wie PayPal, die auf Smartphones, Tablets und PCs installiert ist) sein, je nachdem, welche Technologie zur Speicherung des Geldwerts verwendet wird. E-Geld kann entweder zentralisiert mit dem Kontrollpunkt oder dezentralisiert ohne den Kontrollpunkt sein, d. h. es kann aus verschiedenen Quellen oder Quellennetzwerken wie etwa virtuellen Werten oder Bitcoin stammen.

Die beiden wichtigsten Herausforderungen, denen sich E-Geld stellen muss, sind:

1. **Datenschutz:** Im Gegensatz zu physischen Münzen und Geldscheinen existiert elektronisches Geld in einer Datenbank und enthält Informationen darüber, wer Geld an wen überwiesen hat, welchen Betrag und möglicherweise sogar für welche Dienstleistungen die Transaktion ausgeführt wurde.
2. **doppelte Nutzung (Double Spend):** Ein elektronisches System könnte manipuliert werden, sodass eine doppelte Nutzung desselben Geldes durch Betrüger oder auch einfach nur aus Versehen erfolgen könnte. Dies würde zu Inflation und einem Misstrauen gegenüber dem elektronischen Geldsystem führen.

Die Idee des digitalen Bargelds wurde erstmals in der Forschung von David Chaum (1982) vorgestellt. Kurz gesagt ist elektronisches Geld (E-Geld) der Gleichgewichtszustand, der elektronisch auf einer Wertkarte oder von fern auf einem Server gespeichert wird. Die Bank für Internationalen Zahlungsausgleich, eine Zentralbank-Kooperation mit Sitz in Basel, definiert E-Geld als „stored value or prepaid payment mechanisms for executing payments via point-of-sale terminals, direct transfers between two devices, or even open computer networks such as the internet“ (Bank for International Settlements 1997). Manchen Quellen zufolge sind lediglich Bankeinzahlungen, elektronische Geldüberweisungen, Zahlungsprozessoren und digitale Währungen Beispiele für E-Geld. Andersherum lässt sich jedoch auch argumentieren, dass jegliche Transaktionen und Aufbewahrung von Geld, bei der Computersysteme, Datenspeichersysteme und Computernetzwerke beteiligt sind, als E-Geld definiert werden können.

Es gibt verschiedene Arten von E-Geld, die im Einsatz sind oder sich derzeit in der Entwicklung befinden. Die gängigsten Systeme sind die folgenden:

1. Kreditkarten, die sowohl offline als auch im E-Commerce verwendet werden können. Der PCI DSS legt strenge Regeln für diese Zahlungsart fest. Wenn sie online verwendet wird, kommt zur Verschlüsselung der Verbindung normalerweise TLS zum Einsatz. Die Authentifizierungsmethoden variieren, beinhalten aber einen zweiten Faktor wie Verified by Visa oder 3DSecure von MasterCard.
2. Banküberweisungen sind eine weitere Möglichkeit, Geld zu transferieren. Sie können auch so verwendet werden, dass Anbieter direkten Zugang zum Bankkonto eines Benutzers erhalten und die Überweisung so ausführen, dass der Empfänger Vertrauen auf die rechtmäßige Abwicklung der Überweisung hat.
3. Mobile Geldbörsen werden häufig von Personen benutzt, die keinen Zugang zu klassischen Bank- oder Kreditkarten haben. Ein Beispiel dafür ist das M-PESA-System von Safaricom. Seine Sicherheit beruht hauptsächlich auf Schlüsseln und Zertifikaten auf SIM-Karten sowie sicheren SMS.
4. Eine Ebene über Bankkonten oder Kreditkarten sind Online-Zahlungsanbieter wie AliPay oder PayPal. Diese Dienste stützen sich auf diese grundlegende Zahlungsinfrastruktur, fügen aber eine Schicht Komfort hinzu. Diese Anwendungen erfordern nur das Scannen eines QR-Codes oder können Geld auf der Grundlage einer E-Mail-Adresse überweisen. Die Sicherheit stützt sich auf TLS und MFA zur Authentifizierung. Digitale Zertifikate und Signaturen gewährleisten die Nachweisbarkeit.

Die Entwicklung der Kryptowährung ist die jüngste Stufe der Geldentwicklung (Vlasov 2017). Laut Investopedia ist eine Kryptowährung „a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double spend“ (Frankenfield 2020).

Die erste weit verbreitete blockchainbasierte Kryptowährung, die auch als dezentralisiertes E-Geld eingestuft werden kann, ist **Bitcoin**. Sie ist nach wie vor die beliebteste Kryptowährung und weist derzeit die höchste Marktkapitalisierung aller Kryptowährungen auf. Bitcoin ist ein elektronisches Geldsystem, das 2009 eingeführt wurde. Es handelt sich um eine freie und innovative Plattform – es steht jedermann frei, Dienstleistungen auf dem offenen Bitcoin-Standard zu programmieren und auszuführen, da keine Genehmigungen durch zentrale Stellen erforderlich sind.

#### **Bitcoin**

Der Bitcoin und andere Kryptowährungen wurden als Antwort auf die Finanzkrise von 2008 geschaffen.

Bitcoin ist einerseits so beliebt, weil er nicht von Banken oder Regierungen kontrolliert wird, und andererseits, weil er pseudonym ausgeben werden kann. Bitcoins können mit Fiat-Währung gekauft und bezahlt oder mithilfe von Rechenleistung erzeugt (gemined) werden. Nachdem Sie eine Bitcoin-Wallet (zur Speicherung privater Schlüssel von Bitcoins) auf einem elektronischen Gerät installiert haben, wird eine erste Bitcoin-Adresse generiert. Danach können mehr und mehr Bitcoin-Adressen erzeugt werden. Diese können an eine andere Person geschickt werden, um für etwas zu bezahlen, Geld zu senden oder zu empfangen. Bitcoin-Adressen sollten nur einmal verwendet werden.

Jede Bitcoin-Transaktion wird in einer öffentlichen Liste, der Blockchain, aufgezeichnet. Diese ist definiert als eine Organisationsmethode, die zur Sicherstellung der Integrität von Transaktionsdaten verwendet wird, und ist ein wesentlicher Bestandteil vieler Kryptowährungen. Heute verwenden die meisten Kryptowährungen zur Aufzeichnung von Transakti-

onen die Blockchain-Technologie. Obwohl alle Transaktionen aufgezeichnet werden, gibt es keine Kontonummer zur Identifizierung einer Person – die Anonymität wird durch die Blockchain-Technologie weiter gewahrt.

Der dezentralisierte Charakter von Bitcoin kann es teurer und schwieriger machen, neue Dienstleistungen zu vermarkten, da diese wahrscheinlich direkt an die Nutzer und nicht an eine kleine Gruppe von Zwischenhändlern verkauft werden. Innovatoren ohne viel Marketingfahrung sind möglicherweise nicht in der Lage, ihre Innovationen aufrechtzuerhalten (Nian/Chuen 2015).

Transaktionen werden mit asymmetrischer Kryptografie auf der Grundlage elliptischer Kurven (ECC) signiert. Bei der Gewinnung von Bitcoins muss ein SHA-256-Hash für den nächsten Block gefunden werden; dies wird als „proof of work“ bezeichnet. Da dies energieintensiv ist und keinen weiteren Wert liefert, verwenden andere Kryptowährungen einige andere Konzepte, wie z. B. den Einsatz- anstelle des Arbeitsnachweises. Bei einem „proof of stake“-Verfahren erhält der Inhaber der meisten Einheiten einer Kryptowährung die Belohnung für die Genehmigung der nächsten Transaktion anstelle desjenigen, der die meiste Rechenleistung investiert hat.

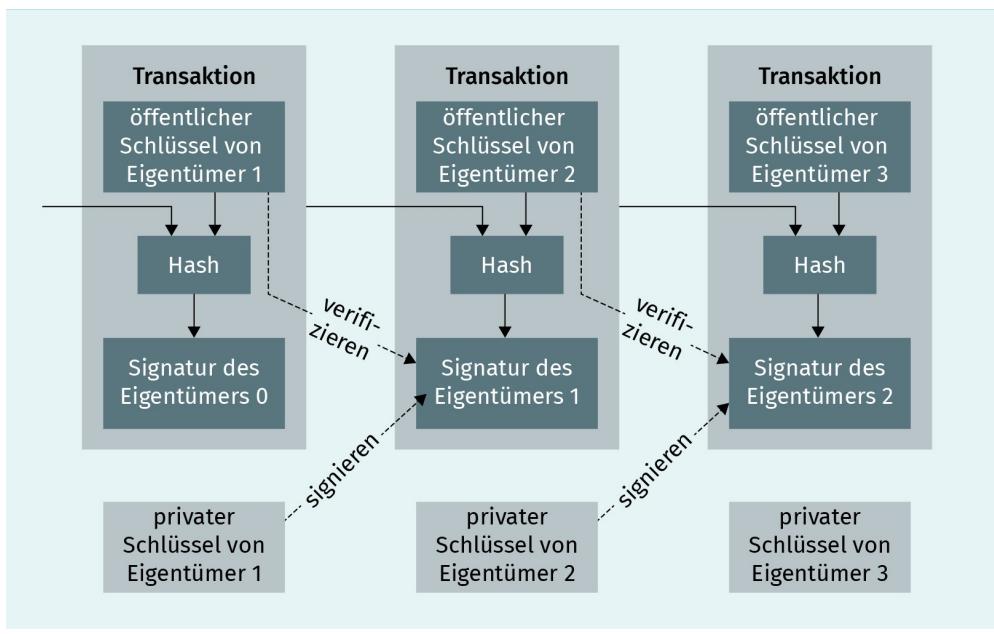
Einige Studien stellen fest, dass die Entwicklung des elektronischen Geldes zu erheblichen Vorteilen der Kryptowährung gegenüber anderen Geldformen geführt hat (Vlasov 2017).

Das Kryptowährungssystem muss jedoch einige Bedingungen erfüllen (Lánský 2018):

- Da das System einen verteilten Konsens hat, besteht keine Notwendigkeit für eine zentrale Behörde.
- Das System behält den Überblick über die Kryptowährungseinheiten und deren Eigentum.
- Das System muss festlegen, ob neue Kryptowährungseinheiten angelegt werden können. Falls ja, legt das System fest, wie das Eigentum an diesen Einheiten und die Umstände ihrer Entstehung zu bestimmen sind.
- Der Besitz von Kryptowährungseinheiten kann nur durch den Einsatz von Kryptografie nachgewiesen werden.
- Das System erlaubt Transaktionen, bei denen das Eigentum an den kryptografischen Einheiten gewechselt wird.
- Wenn zwei verschiedene Anweisungen zur Änderung der Eigentumsverhältnisse an denselben kryptografischen Einheiten gleichzeitig eingegeben werden, führt das System nur eine davon aus.

Die folgende Abbildung zeigt Transaktionen auf der Bitcoin-Blockchain:

Abbildung 23: Transaktionen auf der Bitcoin-Blockchain



Quelle: Nakamoto 2008.



### ZUSAMMENFASSUNG

In dieser Lektion wurden die Konzepte und Möglichkeiten der angewandten Kryptografie erforscht. Die Vorteile von digitalen Signaturen und Public-Key-Kryptografie wurden ausführlich diskutiert, wobei der Schwerpunkt auf den Möglichkeiten lag, wie sie Sicherheit bieten können. Die Blockchain- oder Distributed-Ledger-Technologie und ihre Anwendungen wurden ebenfalls behandelt, wobei der Schwerpunkt auf die Möglichkeiten gelegt wurde, wie Blockchain die Authentizität und Integrität von Daten gewährleisten kann.



# **ANHANG**

# LITERATURVERZEICHNIS

Bank for International Settlements (1997): *Electronic money: Consumer protection, law enforcement, supervisory and cross border issues*. (URL: [https://www.bis.org/publ/gten\\_01.pdf](https://www.bis.org/publ/gten_01.pdf) [letzter Zugriff: 10.11.2020]).

Barker, E./Roginsky, A. (2019): *Transitioning the Use of Cryptographic Algorithms and Key Lengths*. National Institute of Standards and Technology, Gaithersburg (MD). (URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf> [letzter Zugriff: 10.11.2020]).

Bowen, P. (2008): *Special Publication 800-100, Information Security Handbook: A Guide for Managers*. National Institute of Standards and Technology, Gaithersburg (MD). (URL: <https://pdfs.semanticscholar.org/ad03/2e845eeeeed73d1d82bab cbd7d284741e5d88.pdf> [letzter Zugriff: 10.11.2020]).

Bryan Cave Leighton Paisner (2019): *California Consumer Privacy Act – Full Text*. (URL: <https://ccpa-info.com/california-consumer-privacy-act-full-text/> [letzter Zugriff: 11.11.2020]).

Chapple, M./Shinder, D. L./Tittel, E. (2002): *TICSA certification: Information security basic*. Pearson, Hoboken (NJ).

Chaum, D. (1982): *Blind signatures for untraceable payments*. In: Chaum, D./Rivest, R. L./Sherman, A. T. (Hrsg.): *Advances in Cryptology. Proceedings of Crypto 82*. Springer, Boston, S. 199–203.

CIS – Center for Internet Security (o. J.): *Download the CIS controls® V7.1 today*. (URL: <https://learn.cisecurity.org/cis-controls-download> [letzter Zugriff: 02.12.2020]).

Cloud Security Alliance (2017): *Security guidance for critical areas of focus in cloud computing 4.0*. (URL: <https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf> [letzter Zugriff: 02.12.2020]).

Cloudflare (o. J.): *What is transport layer security?* (URL: <https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/> [letzter Zugriff: 02.12.2020]).

Cole, E./Krutz, R./Conley, J. (2005): *Network security bible*. Wiley, Indianapolis.

Common Criteria (2017): *Common criteria for information technology security evaluation – Part 1: Introduction and general model*. (URL: <https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf> [letzter Zugriff: 02.12.2020]).

Crypto-IT (2020): *Block Ciphers Modes of Operation*. (URL: <http://www.crypto-it.net/eng/theory/modes-of-block-ciphers.html> [letzter Zugriff: 02.12.2020]).

De Clercq, J. (2002): *Single sign-on architectures*. In: Davida, G./Frankel, Y./Rees, O. (Hrsg.): Infrastructure Security. Springer, Berlin/Heidelberg, S. 40–58.

Dierks, T./Rescola, E. (2008): *The transport layer security (TLS) protocol: Version 1.2*. (URL: <https://tools.ietf.org/html/rfc5246> [letzter Zugriff: 02.12.2020]).

Diffie, W./Hellman, M. E. (1976): *New Directions in Cryptography*. In: IEEE Transactions on Information Theory, 22. Jg., Heft 6, S. 644–654.

DocuSign (o. J.): *Understanding digital signatures*. (URL: <https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq> [letzter Zugriff: 02.12.2020]).

EGMR – Europäischer Gerichtshof für Menschenrechte (2013): *European convention on Human Rights*. Council of Europe, 02.10.2013. (URL: [https://www.echr.coe.int/Documents/Convention\\_ENG.pdf](https://www.echr.coe.int/Documents/Convention_ENG.pdf) [letzter Zugriff: 02.12.2020]).

ENISA – European Network and Information Security Agency (o. J.): *About ENISA – The European Union Agency for Cybersecurity. Towards a Trusted and Cyber Secure Europe*. (URL: <https://www.enisa.europa.eu/about-enisa> [letzter Zugriff: 02.12.2020]).

Europäische Kommission (2016): *Directive on security of network and information systems*. Brüssel, 06.07.2020. (URL: [https://ec.europa.eu/commission/presscorner/detail/en/MEMO\\_16\\_2422](https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_2422) [letzter Zugriff: 02.12.2020]).

EU – Europäische Union (2000): *Charta der Grundrechte der Europäischen Union*. In: Amtsblatt der Europäischen Gemeinschaften, 18.12.2000. (URL: [https://www.europarl.europa.eu/charter/pdf/text\\_de.pdf](https://www.europarl.europa.eu/charter/pdf/text_de.pdf) [letzter Zugriff: 02.12.2020]).

EU (2014): *Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG*. In: Amtsblatt der Europäischen Gemeinschaften, 28.08.2014, S. 73–114. (URL: [https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv%3AOJ.L\\_2014.257.01.0073.01.DEU&toc=OJ%3AL%3A2014%3A257%3AFULL](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv%3AOJ.L_2014.257.01.0073.01.DEU&toc=OJ%3AL%3A2014%3A257%3AFULL) [letzter Zugriff: 02.12.2020]).

EU (2018): *Verordnung (EU) 2017/670 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)*. (URL: <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679> [letzter Zugriff: 03.12.2020]).

EZB – Europäische Zentralbank (o. J.): *Electronic money*. (URL: [https://www.ecb.europa.eu/stats/money\\_credit\\_banking/electronic\\_money/html/index.en.html](https://www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html) [letzter Zugriff: 02.12.2020]).

FDA – U.S. Food & Drug Administration (2018): *HIPAA Compliance for Reporters to FDA Med-Watch*. Silver Spring (MD), 27.03.2018. (URL: <https://www.fda.gov/safety/reporting-series-problems-fda/hipaa-compliance-reporters-fda-medwatch> [letzter Zugriff: 03.12.2020]).

FIDO Alliance (o. J.): *FIDO2: WebAuthn & CTAP*. (URL: <https://fidoalliance.org/fido2/> [letzter Zugriff: 02.12.2020]).

Frankenfield, J. (2020): *Cryptocurrency*. Investopia, 05.05.2020. (URL: <https://www.investopedia.com/terms/c/cryptocurrency.asp> [letzter Zugriff: 02.12.2020]).

Fruhlinger, J. (2018): *What is network security? Definition, methods, jobs & salaries*. CSO, 03.07.2018. (URL: <https://www.csoonline.com/article/3285651/what-is-network-security-definition-methods-jobs-and-salaries.html> [letzter Zugriff: 02.12.2020]).

FTC – Federal Trade Commission (o. J.): *Privacy and Security Enforcement*. (URL: <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement> [letzter Zugriff: 02.12.2020]).

FTC (2019): *Google LLC and YouTube, LLC*. (URL: <https://www.ftc.gov/enforcement/cases-proceedings/172-3083/google-llc-youtube-llc> [letzter Zugriff: 02.12.2020]).

Gartner Glossary (o. J.): *Big Data*. (URL: <https://www.gartner.com/en/information-technology/glossary/big-data> [letzter Zugriff: 10.11.2020]).

Grassi, P. A./Garcia, M. E./Fenton, J. L. (2019): *Digital Identity Guidelines*. NIST Special Publication 800-63-3. (URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf> [letzter Zugriff: 02.12.2020]).

Gutmann, B./Roback, E. (1995): *An introduction to computer security. The NIST handbook*. NIST Special Publication 800.12. (URL: [https://books.google.de/books/about/An\\_Introduction\\_to\\_Computer\\_Security.html?id=Vyb\\_7hokxf4Crintsec=frontcover&source=kpr&read\\_buttonedir\\_esc=y&v=onepage=false](https://books.google.de/books/about/An_Introduction_to_Computer_Security.html?id=Vyb_7hokxf4Crintsec=frontcover&source=kpr&read_buttonedir_esc=y&v=onepage=false) [letzter Zugriff: 02.12.2020]).

Hansche, S. (2005): *Official (ISC<sup>2</sup>) guide to the CISSP-ISSEP CBK*. 2. Auflage, Auerbach, Boca Raton (FL)/New York.

Hern, A. (2018): *Cambridge Analytica: how did it turn clicks into votes?* In: The Guardian, 06.05.2018. (URL: <https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie> [letzter Zugriff: 02.12.2020]).

Hyperledger (2018): *An Introduction to Hyperledger*. (URL: [https://www.hyperledger.org/wp-content/uploads/2018/08/HL\\_Whitepaper\\_IntroductiontoHyperledger.pdf](https://www.hyperledger.org/wp-content/uploads/2018/08/HL_Whitepaper_IntroductiontoHyperledger.pdf) [letzter Zugriff: 14.12.2020]).

IBM – International Business Machines Corporation (2020): *An overview of the SSL or TLS Handshake*. (URL: [https://www.ibm.com/support/knowledgecenter/SSFKSJ\\_7.5.0/com.ibm.mq.sec.doc/q009930\\_.htm](https://www.ibm.com/support/knowledgecenter/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009930_.htm) [letzter Zugriff: 02.12.2020]).

InfoCuria (2019): *Urteil des Gerichtshofs (Große Kammer) vom 1. Oktober 2019 (Vorabentscheidungsersuchen des Bundesgerichtshofs – Deutschland) – Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V./Planet49 GmbH (Rechtssache C-673/17)*. (URL: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=221353&pageIndex=0&doctlang=DE&mode=req&dir=&oc=c=first&part=1&cid=4950930#1> [letzter Zugriff: 02.12.2020]).

ICO – Information Commissioner’s Office (2017): *Big data, artificial intelligence, machine learning and data protection*. (URL: <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> [letzter Zugriff: 03.12.2020]).

IISSCC – International Information System Security Certification Consortium (o. J.): *CISSP Domain Refresh FAQ*. (URL: <https://www.isc2.org/Certifications/CISSP/Domain-Refresh-FAQ> [letzter Zugriff: 03.12.2020]).

ISA 62443-4-1: *Standards – Secure Development Lifecycle (SDLC) Requirements*.

ISO 9001:2015: *Quality management systems – Requirements*.

ISO/IEC 15408:2009: *Information technology – Security techniques – Evaluation criteria for IT security*. (URL: <https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html> [letzter Zugriff: 22.01.2021]).

ISO/IEC 19941:2017: *Information technology – Cloud computing – Interoperability and portability*. (URL: <https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html> [letzter Zugriff: 22.01.2021]).

ISO/IEC 27001: *Information security management*.

ISO/IEC 27001:2013: *Information technology – Security techniques – Information security management systems – Requirements*.

ISO/IEC 27701:2019: *Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines*.

ISO/IEC 27002:2013: *Information technology – Security techniques – Code of practice for information security controls*.

ISO/IEC 29100:2011: *Information technology – Security techniques – Privacy framework*. (URL: <https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html> [letzter Zugriff: 22.01.2021]).

ISACA (2019): COBIT. (URL: <https://www.isaca.org/resources/cobit> [letzter Zugriff: 03.12.2020]).

Kalyani, C. (2017): *Various biometric authentication techniques: A review*. In: *Journal of Biometrics & Biostatistics*, 8. Jg., Heft 5. (URL: <http://doi.org/10.4172/2155-6180.1000371> [letzter Zugriff: 03.12.2020]).

- Karthikeyan, B./Gaëtan, L. (2016): *On the Practical (In-)Security of 64-bit Block Ciphers: Collision attacks on HTTP over TLS and OpenVPN*. In: Proceedings of the 2016 ACM Conference on Computer and Communications Security, Wien, Oktober 2016, S. 456–467. (URL: <https://hal.inria.fr/hal-01404208v2/document> [letzter Zugriff: 03.12.2020]).
- Kerckhoffs, A. (1883): *La cryptographie militaire*. In: Journal des sciences militaires, 9. Jg., Heft 1, S. 5–38. (URL: [https://www.petitolas.net/kerckhoffs/crypto\\_militaire\\_1.pdf](https://www.petitolas.net/kerckhoffs/crypto_militaire_1.pdf) [letzter Zugriff: 03.12.2020]).
- Kessler, G. C. (2020): An Overview of Cryptography. (URL: <https://www.garykessler.net/library/crypto.html> [letzter Zugriff: 03.12.2020]).
- Lake, J. (2019): *What is the Diffie–Hellman key exchange and how does it work?* Comparitech, 05.03.2019. (URL: <https://www.comparitech.com/blog/information-security/diffie-hellman-key-exchange/> [letzter Zugriff: 03.12.2020]).
- Lánský, J. (2018): *Possible state approaches to cryptocurrencies*. In: Journal of Systems Integration, 9. Jg., Heft 1, S. 19–31. <http://dx.doi.org/10.20470/jsi.v9i1.335> [letzter Zugriff: 03.12.2020]).
- Microsoft (2009): *The STRIDE Thread Model*. (URL: [https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878\(v=cs.20\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN) [letzter Zugriff: 03.12.2020]).
- Nakamoto, S. (2008): *Bitcoin: A Peer-to-Peer Electronic Cash System*. (URL: <https://bitcoin.org/bitcoin.pdf> [letzter Zugriff: 03.12.2020]).
- Neumann, C./Hartman, S./Raeburn, K. (2005): *The Kerberos network authentication service (V5)*. (URL: <https://tools.ietf.org/html/rfc4120> [letzter Zugriff: 03.12.2020]).
- Nian, L. P./Chuen, D. L. K. (2015): *Handbook of Digital Currency. Bitcoin, Innovation, Financial Instruments, and Big Data*. Elsevier, Amsterdam et al.
- Nieles, M./Dempsey, K./Pillitteri, V. (2017): *An introduction to information security*. NIST Special Publication 800.12. Revision 1. (URL: <https://doi.org/10.6028/NIST.SP.800-12r1> [letzter Zugriff: 03.12.2020]).
- NIST – National Institute of Standards and Technology (o. J.): *FISMA implementation project*. (URL: <https://csrc.nist.gov/projects/risk-management/detailed-overview>. [letzter Zugriff: 03.12.2020]).
- NIST (2018): *NIST Releases Version 1.1 of its Popular Cybersecurity Framework*. (URL: <https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cyber-security-framework> [letzter Zugriff: 03.12.2020]).
- NIST (2019): *Hash functions*. (URL: <https://csrc.nist.gov/projects/hash-functions> [letzter Zugriff: 03.12.2020]).

NIST (2020): *Draft NIST Special Publication 800-53 Revision 5 -Security and Privacy Controls for Information Systems and Organizations*. (URL: <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final> [letzter Zugriff: 03.12.2020]).

OpenStack (o. J.): *Security/OSSA-Metrics*. (URL: <https://wiki.openstack.org/wiki/Security/OSSA-Metrics#DREAD> [letzter Zugriff: 03.12.2020]).

Orcutt, M. (2018): *How secure is blockchain really?* In: MIT Technology Review, 25.04.2018. (URL: <https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/> [letzter Zugriff: 03.12.2020]).

OWASP – Open Web Application Security Project (2021): *OWASP Top 10 – 2021. The Most Critical Web Application Security Risks*. (URL: <https://owasp.org/www-project-top-ten/> [letzter Zugriff: 07.03.2024]).

Paar, C./Pelzl, J. (2010): *Understanding Cryptography. A Textbook for Students and Practitioners*. Springer, Heidelberg.

Parlament of India (2000): *The Information Technology Act*. (URL: <https://indiocode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf> [letzter Zugriff: 03.12.2020]).

PCI Security Standards Council (2018): *PCI DSS Quick Reference Guide. Understanding the Payment Card Industry Data Security Standard version 3.2.1*. (URL: [https://www.pcisecuritystandards.org/documents/PCI\\_DSS-QRG-v3\\_2\\_1.pdf?agreement=true&time=1607968598086](https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf?agreement=true&time=1607968598086) [letzter Zugriff: 14.12.2020]).

PDPC – Personal Data Protection Commission (o. J.): *PDPA Overview*. (URL: <https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act> [letzter Zugriff: 03.12.2020]).

PGP (2002): *An Introduction to Cryptography*. (URL: <https://www.cs.unibo.it/babaoglu/courses/security/resources/documents/intro-to-crypto.pdf> [letzter Zugriff: 03.12.2020]).

Raynaud, F. (2017): *DevSecOps Whitepaper*. DevSecCon (URL: <https://www.devseccon.com/wp-content/uploads/2017/07/DevSecOps-whitepaper.pdf> [letzter Zugriff: 13.03.2020]).

Roeder, T. (2020): *Symmetric-Key Cryptography*. (URL: <https://www.cs.cornell.edu/courses/cs5430/2010sp/TL03.symmetric.html> [letzter Zugriff: 03.12.2020]).

Seacord, R. (2018): *Top 10 Secure Coding Practices*. Carnegie Mellon University, 02.05.2018. (URL: <https://wiki.sei.cmu.edu/confluence/display/seccode/Top+10+Secure+Coding+Practices> [letzter Zugriff: 03.12.2020]).

UN – United Nations (1948): *The Universal Declaration of Human Rights*. (URL: <https://www.un.org/en/universal-declaration-human-rights/> [letzter Zugriff: 03.12.2020]).

Vacca, J. R. (2014): *Cyber Security and IT Infrastructure Protection*. Syngress, Waltham (MA).

VDE (2019): *IEC 62443: Die internationale Normenreihe für Cybersecurity in der Industrieautomation*. (URL: <https://www.dke.de/de/arbeitsfelder/core-safety/iec-62443> [letzter Zugriff: 02.12.2020]).

Villanova University (2019): *Perfect Forward Secrecy*. Philadelphia, 06.05.2019. (URL: <https://www.villanovau.com/resources/iss/perfect-forward-secrecy/> [letzter Zugriff: 03.12.2020]).

Vlasov, A. V. (2017): *The Evolution of E-Money*. In: European Research Studies Journal, 20. Jg., Heft 1, S. 215–224. (URL: [https://www.ersj.eu/repec/ers/papers/17\\_1\\_p21.pdf](https://www.ersj.eu/repec/ers/papers/17_1_p21.pdf) [letzter Zugriff: 03.12.2020]).

# ABBILDUNGSVERZEICHNIS

Abbildung 1: CIA-Triade der IT-Sicherheit .....	15
Abbildung 2: Lebenszyklus eines Sicherheitsvorfalls .....	21
Abbildung 3: Symmetrische Kryptografie .....	23
Abbildung 4: Asymmetrische Kryptografie .....	24
Tabelle 1: Nicht anonymisierte Feedback-Tabelle .....	51
Tabelle 2: Zwei-Anonymitäts-Feedback-Tabelle .....	51
Tabelle 3: Drei-Diversitäts-Feedback-Tabelle .....	52
Abbildung 5: Prozess des Zugriffs auf ein System .....	65
Abbildung 6: Beispielschritte in der MFA-Methode .....	67
Abbildung 7: Authentifizierung über das verbreitete SSO-Protokoll Kerberos .....	68
Abbildung 8: Konzept der Verwundbarkeit (Höhe des Risikos) .....	76
Abbildung 9: NIST-Rahmen für IT-Sicherheit .....	79
Abbildung 10: Ein Prozess des Risikomanagements .....	86
Abbildung 11: Qualitative Risikomatrix .....	87
Tabelle 4: Risikoregister .....	89
Tabelle 5: ISO-27k-Normen .....	91
Abbildung 12: PDCA-Zyklus .....	93
Tabelle 6: RACI-Diagramm .....	95
Abbildung 13: Ver- und Entschlüsselungsprozesse .....	101
Abbildung 14: Übersicht Kryptologie .....	102
Abbildung 15: Symmetrische Verschlüsselung .....	104

Tabelle 7: Häufigste symmetrische Verschlüsselungsalgorithmen .....	105
Abbildung 16: Asymmetrische Kryptografie (Kryptografie mit öffentlichem Schlüssel) ..	108
Abbildung 17: Beispiel einer elliptischen Kurve .....	109
Abbildung 18: Hash-Funktion .....	111
Tabelle 8: MD4-Familie von Hash-Funktionen .....	112
Tabelle 9: SHA-3-Familie .....	112
Abbildung 19: Wie digitale Signaturen funktionieren .....	120
Abbildung 20: Digitale Zertifikatskette .....	121
Abbildung 21: TLS/SSL Handshake .....	125
Abbildung 22: Blockchain-Schema .....	127
Abbildung 23: Transaktionen auf der Bitcoin-Blockchain .....	131



 **IU Internationale Hochschule GmbH**  
**IU International University of Applied Sciences**  
Juri-Gagarin-Ring 152  
D-99084 Erfurt

 **Postanschrift**  
Albert-Proeller-Straße 15-19  
D-86675 Buchdorf

 [media@iu.org](mailto:media@iu.org)  
[www.iu.org](http://www.iu.org)

 **Hilfe & Kontakt (FAQ)**  
Antworten rund um Dein Studium findest  
Du jederzeit auf myCampus.