Edition <kes>

Eberhard von Faber

IT und IT-Sicherheit in Begriffen und Zusammenhängen

Thematisch sortiertes Lexikon mit alphabetischem Register zum Nachschlagen

<kes>

EBOOK INSIDE

Springer Vieweg

Edition <kes>

Mit der allgegenwärtigen IT ist auch die Bedeutung der Sicherheit von Informationen und IT-Systemen immens gestiegen. Angesichts der komplexen Materie und des schnellen Fortschritts der Informationstechnik benötigen IT-Profis dazu fundiertes und gut aufbereitetes Wissen.

Die Buchreihe Edition <kes> liefert das notwendige Know-how, fördert das Risikobewusstsein und hilft bei der Entwicklung und Umsetzung von Lösungen zur Sicherheit von IT-Systemen und ihrer Umgebung.

Die <kes> – Zeitschrift für Informations-Sicherheit – wird von der DATAKONTEXT GmbH im zweimonatigen Rhythmus veröffentlicht und behandelt alle sicherheitsrelevanten Themen von Audits über Sicherheits-Policies bis hin zu Verschlüsselung und Zugangskontrolle. Außerdem liefert sie Informationen über neue Sicherheits-Hard- und -Software sowie die einschlägige Gesetzgebung zu Multimedia und Datenschutz. Nähere Informationen rund um die Fachzeitschrift finden Sie unter www.kes.info.

Weitere Bände in der Reihe http://www.springer.com/series/12374

Eberhard von Faber

IT und IT-Sicherheit in Begriffen und Zusammenhängen

Thematisch sortiertes Lexikon mit alphabetischem Register zum Nachschlagen

Springer Vieweg

Eberhard von Faber
Bornheim, Deutschland

ISSN 2522-0551 ISSN 2522-056X (electronic)
Edition <kes>
ISBN 978-3-658-33430-7 ISBN 978-3-658-33431-4 (eBook)
https://doi.org/10.1007/978-3-658-33431-4

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

Planung: David Imgrund
Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Dieses Buch und seine Nutzung

Sie wollen wissen, wie dieses Buch funktioniert? → Blättern Sie um!

Ich widme dieses Buch allen, die Klarheit lieben.

Im Buch „Secure ICT Service Provisioning for Cloud, Mobile and Beyond“ werden die Grundlagen für die Absicherung von IT-Services in einer *großtechnischen, industrialisierten IT-Produktion* gelegt, wo IT-Sicherheit so ganz anders organisiert werden muss, als man sich das lehrbuchhaft manchmal vorstellen mag.

Mit „Joint Security Management: organisationsübergreifend handeln“ blieben wir den Motiven „servicebezogen“ und „bezogen auf die marktwirtschaftliche Realität“ treu und verlagerten den Schwerpunkt weiter in Richtung *Anwenderorganisation*. Sicherheit entsteht nicht von alleine, sondern ist Ergebnis eines aktiven Managementprozesses, in dem die *Anforderungen der Anwender* berücksichtigt werden und durch die *Maßnahmen des IT-Dienstleisters* und seiner Zulieferer erfüllt werden.

In beiden Büchern (siehe Literaturhinweise in Kapitel 1.3) mussten wir viele Fachtermini benutzen und teils auf grundlegendem Wissen zu IT und IT-Sicherheit aufbauen.

Deshalb wurden wir gefragt, ob die verwendeten Begriffe nur unsere Sichtweise darstellen würden, und ob es nicht eine Möglichkeit gäbe, die vielen Termini einmal kurz und knapp nachlesen zu können. Und Studenten musste ich vertrösten, weil auch meine Vorlesungsskripte viele Erklärungen nicht enthielten.

So entstand die Idee zu diesem Buch.

> *Es erklärt fast alles, was Sie zum Thema IT und zum Thema IT- bzw. Cyber-Sicherheit wirklich wissen bzw. in Kürze parat haben sollten, um in Projekten und im sonstigen Tagesgeschäft stets aussagefähig und sachverständig zu sein, sodass Sie führend und vermittelnd tätig sein können.*

Fehlt etwas? Sind Sie anderer Meinung? Schreiben Sie an ESARIS@t-online.de!

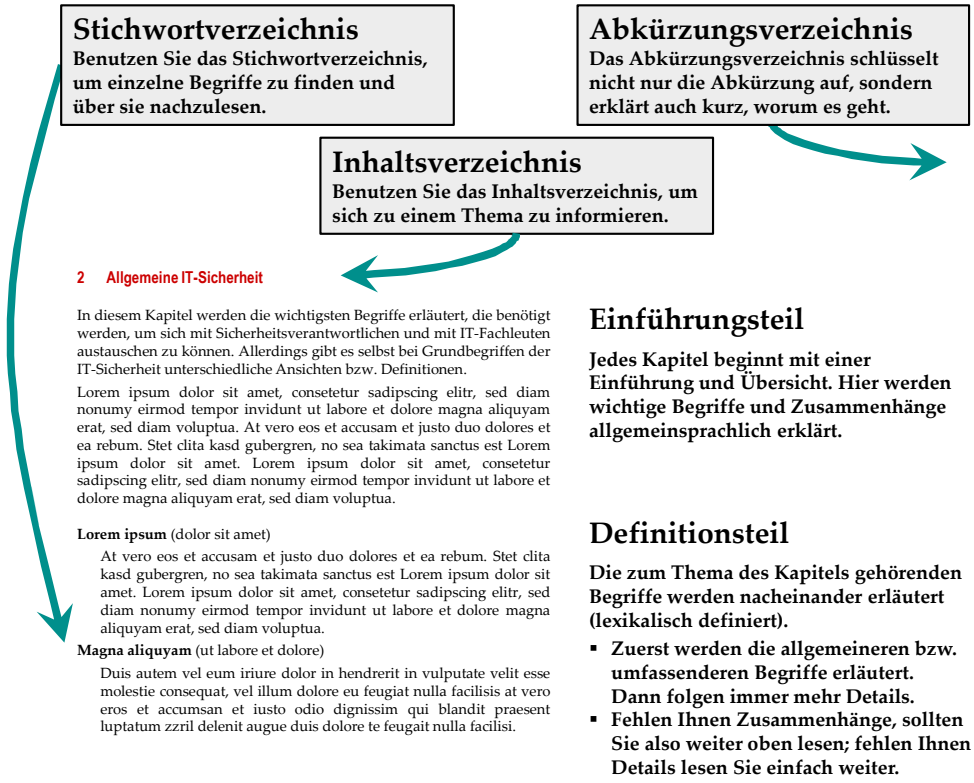
Alle 64 Abbildungen und eventuell weiteres Zusatzmaterial finden Sie in elektronischer Form über https://link.springer.com/ auf der Seite der eBook-Version.

Eberhard von Faber

Nutzungshinweise

A. Es gibt drei Einstiegsmöglichkeiten (siehe Darstellung).

Ihr Vorteil: 1) Sie können einzelne Begriffe nachschlagen. 2) Sie erkennen sofort den Kontext. Dank der Einführungsteile und der vielen Schaubilder sehen Sie Zusammenhänge und finden Begriffe zum gleichen Thema. Auf diese Weise können Sie sich systematisch in ein Thema einlesen. 3) Die Erklärungen der einzelnen Begriffe enthalten Verweise auf andere Begriffe. Da jeder Begriff in einem thematischen Kontext steht, weiß man immer, wo man gerade ist.



B. Alle Kapitel beginnen mit einem Einführungsteil. Erst dann folgen, wie man es von einem Lexikon erwartet, die Erklärungen einzelner Begriffe.

Ihr Vorteil: 4) Weder Wikipedia noch irgendein Glossar führt Sie allgemeinverständlich in ein Thema ein und strukturiert den Wald von Begriffen. 5) Die Begriffe sind logisch geordnet. Sie bauen aufeinander auf, und es wird schrittweise detaillierter.

C. Es gibt neben den Verzeichnissen (siehe oben) auch viele Verweise.

Ihr Vorteil: 6.) Achten Sie auf **Fettschrift**[1], wenn Sie einen Begriff bzw. dessen Erklärung suchen. 7.) Stoßen Sie auf *Kursivschrift*, so wissen Sie, dass dieser Begriff an anderer Stelle ausführlich erklärt bzw. definiert wird. Der eigentliche Begriff ist eventuell etwas weiter unten definiert (siehe Darstellung unten). 8.) Wichtige Wörter oder Sachverhalte sind unterstrichen.

D. Weitere Hinweise.

9.) Wenn Sie im Abkürzungsverzeichnis eine Abkürzung nachschlagen (zum Beispiel AAAAA), so finden Sie dort nicht nur die Langversion (im Beispiel: American Association Against Acronym Abuse), sondern auch eine kurze Erklärung.[2]
10.) Das Buch vereint Grundlagen der IT und der IT-Sicherheit. Denn IT-Sicherheit macht man nicht ohne IT. Und die IT-Sicherheit ist die im wirklichen Business.

Meine Bitte: Vielen Dank, wenn Sie dieses Buch bereits gekauft haben. Es macht sehr viel Arbeit, ein solches Buch zu schreiben. Empfehlen Sie das Buch gerne weiter, wenn Sie es nützlich finden. Aber kopieren Sie es bitte nicht. Danke.

---

1 Sind sowohl der deutsche als auch der englische Begriff gebräuchlich, so werden beide Begriffe fett gedruckt. Wird nur einer genutzt, so erscheint nur dieser in Fettschrift.

2 In diesem Fall müsste dort stehen, dass es diese Vereinigung nicht gibt und es sich um einen Scherz handelt (den einzig richtig komischen in diesem Buch).

Inhaltsverzeichnis

1 Einführung

Im privaten wie im geschäftlichen Leben kommt es eher häufig zu Missverständnissen. Im besten Fall können sie schnell geklärt werden. Wir lernen schon als Kinder und später in der Ausbildung, was einzelne Wörter wirklich bedeuten. Gibt es verschiedene Bedeutungen, so helfen die Umstände (der Kontext) dabei herauszufinden, welche Bedeutung gerade gemeint ist.

Aber es gibt auch unterschiedliche Sprachen. Will sich ein Niederländer mit einem Norweger verständigen, so müssen sie eine gemeinsame Sprache sprechen. Im beruflichen Leben stößt man mit der Alltagssprache schnell an Grenzen. Daher haben die verschiedenen Disziplinen Fachsprachen entwickelt. Das vorliegende Buch hilft, die „Sprache der IT-Sicherheit“ und der „Informationstechnik“ zu beherrschen. Das Buch enthält die wichtigsten Begriffe mit ausführlichen Erklärungen.

1.1 Begriffe, Sachverhalte, Fachsprache

Sprachen lernt man aber nicht mit einem Wörterbuch – also indem man Wörter einfach übersetzt. Vielmehr lernt man an Beispielsätzen, wie man sie einsetzt. Fachsprachen haben keine eigene Grammatik; aber eine Begriffserklärung allein sagt oft sehr wenig. Oft stößt man mit einem Wörterbuch oder Lexikon zudem schnell an Grenzen. Man steht auf verlorenem Posten, spätestens nachdem man dem zweiten Querverweis gefolgt ist. Die Erklärungen führen auf ein fremdes Territorium oder aber zu schnell zurück zum Ausgangspunkt. Wenig ist gewonnen. Oder, wie oft im Falle der Wikipedia, sind die Erklärungen viel zu lang, so dass die Übersicht verloren geht. Auch reichen Zeit und Aufmerksamkeit nicht aus, um dies alles zu lernen. Diese Formen der Erklärung sind also wenig effizient.

Deshalb ist dieses Buch nicht wie ein Wörterbuch oder ein Lexikon aufgebaut:

- Die Begriffe sind nicht alphabetisch geordnet, sondern thematisch. Es geht den meisten Nutzern nicht um eine einfache „Übersetzung“, sondern darum, eine „Angelegenheit“ zu verstehen.
- Ein Eintrag erklärt nicht nur einen Begriff. Anhand einzelner Begriffe wird eine „Angelegenheit“ erläutert, wobei mitunter auch weitere Begriffe vollständig erklärt werden, die in diesem Zusammenhang von Bedeutung sind.

E. von Faber, *IT und IT-Sicherheit in Begriffen und Zusammenhängen*,
Edition <kes>, https://doi.org/10.1007/978-3-658-33431-4_1

- Die einzelnen Begriffserklärungen sind lexikonartig, also kurz und präzise. Damit spart der Leser Zeit, und er kann seine Aufmerksamkeit dafür nutzen, sein eigentliches Thema zu bearbeiten.

Man kann über Themen einsteigen, wobei die Gliederung des Buches in Kapitel und Unterkapitel genutzt wird. Man kann aber auch über Begriffe einsteigen und dann eventuell die Erklärung weiterer Begriffe studieren. Die Begriffe findet man leicht über das alphabetische Stichwortverzeichnis, das alle erklärten Fachbegriffe enthält.

Vor allem im beruflichen Leben ist es aus folgenden Gründen wichtig, fachliche Begriffe richtig einordnen und verstehen zu können:

- Werden Begriffe richtig verstanden und verwendet, werden Missverständnisse vermieden. Dies ist ein Grunderfordernis einer guten, effektiven Kommunikation. Die Kommunikation kann auf viele zusätzliche Erklärungen verzichten und sich auf den eigentlichen Gegenstand konzentrieren.
- Nur wer die Spezifika einer Sache richtig versteht und sie von anderen ähnlichen Tatbeständen unterscheiden kann, kann einen echten Wertbeitrag liefern. Eigenschaften und Unterschiede sind der Stoff, der die Gedanken treibt, und Zusammenhänge und Muster bilden das Gewebe, das zu Lösungen führt.

Deshalb wird Ihnen dieses Lernwörterbuch oder Lexikon von Begriffen der Informationstechnik und der IT-Sicherheit nützliche Dienste leisten.

Sehr viele Begriffe unserer Fachsprache sind gar nicht genau definiert, so dass wir Stunden um Stunden verbringen, um sie zu schärfen. Nicht weil es um die Begriffe geht, sondern um die Sache, die wir verstehen und in den Griff bekommen wollen. Deshalb denken die Begriffsdefinitionen in diesem Buch die Sache manchmal auch weiter. Ein Beispiel: Wir sind uns alle einig, dass ein Sicherheitsvorfall ein Ereignis ist, bei dem es zu einem Schaden (besser: Verletzung von Sicherheitsrichtlinien) gekommen ist bzw. umgekehrt: Das Eintreten des Schadens nennen wir Sicherheitsvorfall. Doch warum werden Vorkehrungen getroffen, solche Vorkommnisse behandeln zu können? Wir sind uns abermals einig, dass diese Vorbereitungen die Reaktionsfähigkeit sicherstellen und damit helfen sollen, den sicheren Zustand baldmöglich wieder herstellen zu können. Wäre es dann aber nicht sinnvoll, schon dann zu reagieren, wenn die unmittelbare Gefahr besteht, dass es zu einem Schaden kommt? Konsequenterweise müsste dann die Definition für den Sicherheitsvorfall entsprechend erweitert werden. Genau dies erfolgt manchmal in diesem Buch.

Die Begriffsdefinitionen helfen auch dabei, das IT- und IT-Sicherheitsmanagement konkret auszugestalten. Ich habe an mehreren Projektbesprechungen teilgenommen, in denen es um die Ausgestaltung des Prozesses zur Behandlung von Sicherheitsvorfällen (security incident management) und genau um den gerade geschilderten Fall der Begriffsdefinition ging. Seine Schärfung hat Wesen und Charakter (scope) des zu definierenden Prozessablaufs verändert. Schließlich werden nun Meldungen in Empfang genommen, die auf eine unmittelbare Gefahr hinweisen. Das Ticketing-Tool muss nun andere Kategorien verarbeiten und bestimmte Felder erst

später als Pflichtfelder ansehen, die auszufüllen sind. Oder es müssen spätere Korrekturen möglich sein, weil der Schaden anfangs ja noch gar nicht feststeht, sondern allenfalls grob geschätzt werden kann. Mit den Begriffsdefinitionen profitieren Sie also, wie es sich für ein Fachbuch gehört, von der vielfältigen Erfahrung anderer.

Die Begriffe werden aber keinesfalls aufgebläht. Vielmehr steht lexikalische Kürze im Vordergrund. Manche Begriffe werden in der Tat etwas ausführlicher erklärt, niemals jedoch lang oder ausschweifend. Die Texte sollen immer wirkliche Erklärungen liefern – einen Lerneffekt inbegriffen. Zwei Zeilen oder ein paar wenige Wörter können das nicht leisten.

Ein anderer Grundsatz ist die wissenschaftliche Richtigkeit und Präzision. Die Texte versuchen niemals zu überzeugen oder gar etwas anzubieten oder zu verkaufen, wie man es häufig in Internettexten findet. Die Texte sind nicht werblich, sondern nüchtern. Zuweilen wirken sie dadurch etwas sperrig und sehr analytisch. Aber das war der Standard für Lexika. Dann begannen Sammlungen wie Wikipedia, alles verfügbare Wissen zu sammeln, was zum Teil zu ellenlangen Abhandlungen führt. Das vorliegende Buch liefert das notwendige Wissen in Form einer Essenz. Das Wichtigste kommt auch zuerst, sodass man auch aufhören kann zu lesen, wenn der Informationsbedarf gedeckt ist.

Anders als in einem Lexikon sind die Begriffserklärungen nicht alphabetisch, sondern thematisch sortiert. Ein alphabetisch sortiertes Stichwortregister ist aber ebenfalls verfügbar, wenn man über einen bestimmten Begriff einsteigen will. Während man sich bei einer alphabetischen Sortierung den Kontext oft erst mühsam erschließen muss, ist er durch die thematische Sortierung schon gegeben. Viel wichtiger ist aber, dass man sofort inhaltlich verwandte Begriffe finden kann. Sie blättern zurück und finden allgemeinere Zusammenhänge. Sie schauen sich die Begriffe davor und danach an und finden oft Parallelen. Sie lesen weiter und finden mehr Details. In einem alphabetisch sortierten Wörterbuch wissen Sie nach dem zweiten Verweis nicht mehr, wo Sie eigentlich sind und waren. Das Gleiche gilt für das Internet.

Das Buch enthält auch ein ausführliches alphabetisches Verzeichnis von Abkürzungen. Neben der einfachen Übersetzung wird eine kurze Erklärung geliefert, die oft die Qualität eines kurzen Lexikoneintrages erreicht.

Ein Schwerpunkt dieses Buches ist IT-Sicherheit und hierbei wiederum die Sicht der Praktiker und Anwender – und nicht so sehr die der Forscher und Kryptologen. Wenn es um IT-Sicherheit geht, muss man die IT verstehen. Deshalb wird der Erklärung der Informationstechnologie (Technik) und den Prozessen und Verfahren zur Konstruktion, zum Betrieb und zur Pflege von IT-Systemen genügend Raum gegeben. Anwender beziehen diese IT über den Markt und meist in Form von IT-Dienstleistungen. Sie zu verstehen und ihre Unterschiede und Besonderheiten einzuordnen ist deshalb von essentieller Bedeutung auch für IT-Sicherheitsexperten, die solche Services hinsichtlich ihrer IT-Sicherheit bewerten oder selbst für die IT-Sicherheit sorgen sollen.

Ich habe mich darum bemüht, dem Deutschen den Vorzug zu geben. Die englischen Begriffe sind zusätzlich angegeben. **Fettschrift** wird für den Begriff verwendet, wenn er an dieser Stelle erklärt wird. *Kursivschrift* weist darauf hin, dass der Begriff an anderer Stelle erklärt wird. Unterstreichungen werden als Hervorhebung genutzt. Sollte der Leser eine bestimmte Begriffsdefinition nicht finden können, empfehlen wir, das Stichwortregister (Index) am Ende des Buches zu befragen. Alle erklärten Stichworte sind dort aufgeführt.

1.2 Über den Autor und Danksagung

Beruflicher Lebenslauf: Eberhard von Faber

Quelle: privat

Eberhard von Faber studierte Theoretische Elektrotechnik sowie Physik und promovierte auf dem Gebiet der Halbleiterphysik. Er ist Chief Security Advisor, IT-Services, bei T-Systems. Als Professor für IT-Sicherheit lehrt er nebenberuflich an der Technischen Hochschule Brandenburg im Master-Studiengang Security Management.

Im Januar 1992 begann er seine berufliche Laufbahn in der Industrie als Entwickler von Sicherheitssystemen und -produkten.
Er entwickelte CryptCard, das weltweit erste, hardware-basierte Sicherheitssystem für Notebook-Computer. Das System umfasste eine 3,3 mm dicke, kreditkartengroße Einsteckkarte, in der ein vollständiger Microcomputer, der damals schnellste Kryptografie-Chip für DES-Operationen, ein weiterer von Herrn von Faber entwickelter ASIC, eine Echtzeituhr sowie Programm- und Schlüsselspeicher untergebracht waren.

Er verließ die Firma und wechselte zum debis Systemhaus, wo er auf verschiedenen Gebieten im Security-Engineering, Security-Consulting und der Evaluierung von Produkten und Lösungen tätig war.

Herr von Faber entwickelte die Basisspezifikation einer noch heute erfolgreich im Einsatz befindlichen "Wegfahrsperre" eines führenden Automobilkonzerns. Ein anderes großes Projekt im Bereich Security-Engineering war 1996 die Entwicklung einer Infrastrukturlösung für die sichere Kommunikation eines Zusammenschlusses von deutschen Banken. Das System wurde unter seiner Leitung von Grund auf spezifiziert und implementiert.

Eberhard von Faber führte 1995/1996 den Nachweis, dass der in der Finanzwirtschaft verwendete kryptografische Algorithmus DES durch einen Brute-Force-Angriff mit in Deutschland verfügbaren Technologien gebrochen werden kann. Die Kreditwirtschaft in Deutschland entschied daraufhin, den Algorithmus in allen Komponenten des kartenbasierten Zahlungsverkehrs wie ec-Karten, POS-Terminals und GAA-Pinpads (EPP) zu ersetzen. Die Angelegenheit wurde streng geheim

gehalten und wurde lange Zeit vor dem erst im Juni 1998 durchgeführten Brute-Force-Angriff "Deep Crack" abgeschlossen.

Herr von Faber war lange als Evaluator und Gutachter tätig. Speziell untersuchte er die Sicherheit von Chips, die im Zahlungsverkehr etwa in Form von Debit- und Kreditkarten weltweit zum Einsatz kamen. Er entwickelte einige ausgeklügelte, meist invasive neue Angriffstechniken. Er ist Hauptautor eines internationalen Standards für die Sicherheit von integrierten Schaltkreisen für Debit- und Kreditkarten.

Eberhard von Faber baute das Geschäft mit Evaluierungen gemäß ITSEC und später Common Criteria auf. Er leitete die Prüfstelle beim debis Systemhaus einige Jahre und war international als Evaluator bis 2003 tätig.

Inzwischen arbeitet Herr von Faber für T-Systems, wo er diverse Positionen innehatte. Als Stabsleiter der Geschäftsführung einer auf Sicherheitsdienstleistungen und -lösungen spezialisierten Geschäftseinheit war er für die strategische Ausrichtung, die Konsolidierung und den Ausgleich durch zukunftsträchtige Angebote verantwortlich. Er initiierte Innovationsprojekte und entwickelte selbst Lösungen. Weitere Stationen waren die Gestaltung des Angebotsportfolios (Offering Manager) und dessen Operationalisierung in einem deutlich größeren Verantwortungsbereich und die Arbeit als Executive Consultant für T-Systems.

Ende 2010 wurde Herrn von Faber die Aufgabe übertragen, die Absicherung aller IT/TK-Services von T-Systems zu verbessern und völlig neu zu organisieren. Er entwickelte Dutzende neuer Methoden (die unter dem Namen *ESARIS* firmieren), führte existierende Sicherheitsstandards zusammen und verbesserte Transparenz, Effektivität und Effizienz. Wichtige Ergebnisse und die Einführung von *ESARIS* bei T-Systems sind in seinem erstmals 2013 erschienenen Buch dokumentiert, das 2017 in vollständig neuer und erweiterter Auflage erschien.

Nach der erfolgreichen Einführung von *ESARIS* bei T-Systems (IT/TK-Dienstleister mit ca. 44.000 Mitarbeitern in 20 Ländern; Stand: 2016) wurde Eberhard von Faber zum Chief Security Advisor, IT Services ernannt. Seine aktuellen Interessen liegen in den folgenden Bereichen: Sicherheitsaspekte bei IT-Outsourcing-Modellen einschließlich aller Formen von Cloud-Computing, Metriken und Vertrauenswürdigkeitsmodelle, Enterprise Security Architecture sowie Sicherheitsmanagement in Zuliefernetzwerken und in der Beziehung zwischen Kunde und Dienstleister.

Die lexikalischen Erklärungen in diesem Buch basieren auf

- einer fast 30-jährigen beruflichen Tätigkeit auf dem Gebiet der IT-Sicherheit,
- unzähligen schriftlichen Arbeiten, Gutachten, Spezifikationen und Standards, für die der Autor verantwortlich zeichnet,
- weit mehr als 150 Veröffentlichungen und Vorträge auf internationalen und nationalen Fachkonferenzen und einigen Büchern,
- einer fast 15-jährigen Lehrtätigkeit zur IT-Sicherheit (im Masterstudiengang Security Management),

- vielleicht 1500 Antworten auf ebenso viele Fragen von Studierenden während der Lehrveranstaltungen,
- zig Vorbereitungen von Prüfungsfragen und tausende Bewertungen von Antworten darauf,
- der Tätigkeit als Ideengeber und Chief Security Advisor, IT Services, in einem Konzern, in dem der Autor zudem für die umfangreiche Bibliothek der firmeninternen Standards zur IT-Service-Sicherheit verantwortlich ist.

Danksagung

Ich danke meinem Freund und früheren Kollegen und Koautor Wolfgang Behnsen, dass er es sich nicht nehmen ließ, dieses Buch mit Akribie sprachlich und inhaltlich Korrektur zu lesen und mich, wo nötig, mit Rat zu unterstützen. Gerade bei derart dichtem Text wird der Autor sehr bald blind für Tipp- und andere Fehler. Die Verwendung zweier Sprachen und der vielen, oft zusammengesetzten Fachtermini stellt eine besondere Herausforderung hinsichtlich der Einheitlichkeit der Schreibweisen dar. Danke für deine Gründlichkeit.

Vielen Dank an Christian von Faber, der mir mit großer Geduld geholfen hat, mancher Widrigkeit bei der technischen Herstellung der elektronischen Buchversion zu trotzen. Danke für dein Ohr und manchen Tipp – auch bei diesem Buch wieder.

1.3 Literaturhinweise

Die folgende Aufstellung enthält einige Werke, in denen Begriffe meist in Form eines Glossars erklärt werden. Es gibt auch verschiedene Glossare und Wikis im Internet. Ich erlaube mir auch, auf meine beiden letzten Bücher zu verweisen, die viele Dinge viel ausführlicher erklären, als es in diesem Lernwörterbuch möglich ist. Die Liste ist in keiner Weise erschöpfend. Die Literaturangaben sind nicht als Quellen zu verstehen, obwohl sie neben einer Vielzahl anderer Quellen und Werke vom Autor genutzt wurden.

Weitere Quellen und Literaturhinweise findet man in den jeweiligen Kapiteln.

[1] ISO/IEC 15408 – Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model; 2009; und: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; April 2017, Version 3.1 Revision 5, https://commoncriteriaportal.org

[2] ISO/IEC 21827 – Information Technology – Systems Security Engineering – Capability Maturity Model (SSE-CMM); 2008

[3] ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements (ersetzt BS 25999-1:2006 seit 2012)

[4] ISO/IEC 27000 - Information technology — Security techniques — Information security management systems — Overview and vocabulary; 2016

[5] Kissel, Richard (ed.): Glossary of Key Information Security Terms; National Institute of Standards and Technology, U.S. Department of Commerce, NIST IR 7298, Rev. 2, May 2013

[6] Gartner: Gartner Glossary, Information Technology; https://www.gartner.com/en/information-technology/glossary

[7] WhatIs.com® (Referenz- und Selbstlernwerkzeug zum Thema Informationstechnologie (IT)); https://whatis.techtarget.com/de

[8] Thomas R. Köhler und Dirk Schürmann: automotiveIT®. Das Lexikon- Alle IT-Begriffe von A bis Z; Media-Manufaktur GmbH, Pattensen, 2012, ISBN 978-3-9814661-3-3

[9] Eberhard von Faber and Wolfgang Behnsen: Secure ICT Service Provisioning for Cloud, Mobile and Beyond (ESARIS: The Answer to the Demands of Industrialized IT Production Balancing Between Buyers and Providers); Springer Vieweg, Wiesbaden 2017, 383 pages, 159 figures, ISBN 978-3-658-16481-2, 2nd updated and extended Edition, https://doi.org/10.1007/978-3-658-16482-9; (Die Erstauflage von 2012 ist völlig anders organisiert und enthält vieles gar nicht.)

[10] Eberhard von Faber and Wolfgang Behnsen: Joint Security Management: organisationsübergreifend handeln (Mehr Sicherheit im Zeitalter von Cloud-Computing, IT-Dienstleistungen und industrialisierter IT-Produktion); Springer Vieweg, Wiesbaden 2018, 244 Seiten, 60 farbige Abbildungen, ISBN 978-3-658-20833-2, https://doi.org/10.1007/978-3-658-20834-9

Elektronisches Zusatzmaterial
Alle 64 Abbildungen dieses Buches sind als PowerPoint-Datei kapitelweise über https://link.springer.com/ auf der Seite des eBooks abrufbar.

2 Allgemeine IT-Sicherheit

In diesem Kapitel werden die wichtigsten Begriffe erläutert, die benötigt werden, um sich mit Sicherheitsverantwortlichen und mit IT-Fachleuten austauschen zu können. Allerdings gibt es selbst bei Grundbegriffen der IT-Sicherheit unterschiedliche Ansichten bzw. Definitionen. Auch deshalb wird geraten, dass Organisationen ein Glossar mit Begriffsdefinitionen anlegen und dieses im *Joint Security Management* mit den Partnern abstimmen.

Hinweis: Einige der in diesem Kapitel erklärten Begriffe sind bereits im Glossar (im Bonus-Teil meines letzten Buches) enthalten.[3] Um die Anzahl der Fußnoten zu begrenzen und auf das Wesentliche zu beschränken, wird dies nicht in jedem Einzelfall kenntlich gemacht.

2.1 Grundlagen der IT-Sicherheit

Sicherheit ist ein schwieriger Begriff mit begrenztem praktischen Wert. Man muss „Sicherheit" im Zusammenhang mit anderen Begriffen sehen. Einige davon sind in Abb. 1 dargestellt. Die Abbildung gibt auch die Gliederung innerhalb dieses Abschnittes wieder.

- Wir gehen von Anforderungen und Zielen der IT-Sicherheit aus (Kapitel 2.1.1).
- Um diese Ziele erreichen zu können, ist eine Analyse (Kapitel 2.1.2) erforderlich, die auch den wichtigen Begriff des Risikos einführt.
- Im Kapitel 2.1.3 wird erläutert, wie Sicherheitsmaßnahmen abgeleitet und spezifiziert werden.
- Es schließt sich ein Kapitel 2.1.4 an, in dem es um Eigenschaften von Sicherheitsmaßnahmen und deren Überprüfung geht.

---

[3] Eberhard von Faber und Wolfgang Behnsen: Joint Security Management: organisationsübergreifend handeln (Mehr Sicherheit im Zeitalter von Cloud-Computing, IT-Dienstleistungen und industrialisierter IT-Produktion); Springer Vieweg, Wiesbaden 2018, 244 Seiten, 60 farbige Abbildungen, ISBN 978-3-658-20833-2; https://doi.org/10.1007/978-3-658-20834-9; Kapitel 10, Seite 207-220

Zusatzmaterial online
Zusätzliche Informationen sind in der Online-Version dieses Kapitel (https://doi.org/10.1007/978-3-658-33431-4_2) enthalten.

E. von Faber, *IT und IT-Sicherheit in Begriffen und Zusammenhängen*,
Edition <kes>, https://doi.org/10.1007/978-3-658-33431-4_2

Die Begriffe bzw. Sachverhalte sind auf verschiedene Art und Weise miteinander verbunden. Die beiden wichtigsten Verbindungen sind in Abb. 1 durch gestrichelte Linien gekennzeichnet: Von Sicherheit spricht man, wenn keine nicht akzeptierten Risiken bestehen. Risiken können entstehen, wenn Sicherheitsmaßnahmen über Schwachstellen verfügen.

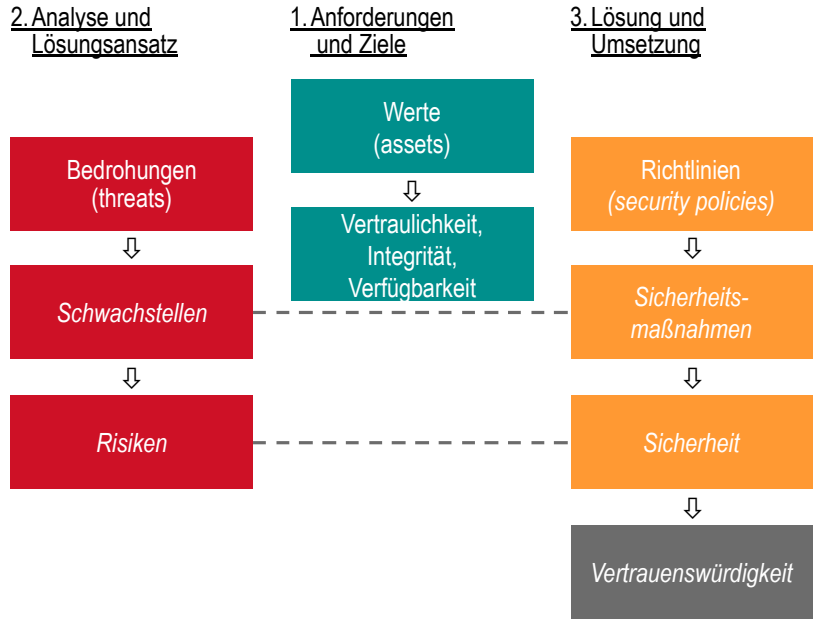


Abb. 1: Grundbegriffe – erste Annäherung und drei Themen

IT-Sicherheitsexperten beschäftigen sich nur zum Teil damit, für Sicherheit zu sorgen bzw. Risiken zu reduzieren! Sie haben nämlich die zweite wichtige Aufgabe, Informationen über die erreichte Sicherheit zu sammeln und zu kommunizieren. Dies steht mit dem Begriff Vertrauenswürdigkeit in Zusammenhang, der wegen seiner besonderen Rolle andersfarbig in Abb. 1 dargestellt ist.

2.1.1 Anforderungen und Ziele

Es folgen 6+1 Begriffserklärungen, die den Ausgangspunkt für die IT-Sicherheit bilden. Sie spielen auch eine wichtige Rolle bei der Erstellung von Sicherheitskonzepten, denn ganz zu Anfang stehen Fragen wie: Was soll erreicht werden? Welche Anforderungen müssen erfüllt werden?

Wert (asset)

> Ein Wert (asset) ist etwas, das für eine Organisation bzw. ein Unternehmen wichtig und unabdingbar ist, um die Geschäftsziele zu erreichen. Werte (assets) müssen daher geschützt werden. In der Informationsverarbeitung handelt es sich meist um immaterielle Werte (IT-Dienstleistung, Informationen/Daten). Solche Werte zu schützen bzw. zu erhalten, bedeutet daher vor allem, für die

Vertraulichkeit (confidentiality), *Integrität (integrity)* und *Verfügbarkeit (availability)* zu sorgen.

Vertraulichkeit (confidentiality)

Die Vertraulichkeit von Informationen drückt die Notwendigkeit aus, diese Informationen vor Zugriff durch oder Offenlegung gegenüber Unberechtigten (Personen oder Systemen) zu schützen. Die Vertraulichkeit wird zum Beispiel durch die Einschränkung von Zugriff, Lesbarkeit, Informationsfluss und Auffindbarkeit aufrechterhalten. Beispiele für zugehörige Sicherheitsmaßnahmen sind Rechteprüfung bzw. *Zugriffskontrolle* (Zugriff), *Verschlüsselung* (bzgl. Einschränkung der Lesbarkeit), *Enterprise Digital Rights Management* (bzgl. Informationsfluss) und *Steganographie* (bzgl. Auffindbarkeit).

Die Vertraulichkeit einer Information ist nicht wiederherstellbar, wenn sie verloren ging, die Information also Unberechtigten bekannt wurde. Das unterscheidet die Vertraulichkeit von allen anderen Sicherheitszielen und Qualitäten. Vertraulichkeit kann also nur durch vorsorgende Maßnahmen sichergestellt werden (Vorsorgeprinzip).

Integrität (integrity)

Die Integrität von Informationen, Systemen und Services bedeutet, dass diese nicht unberechtigt oder versehentlich geändert, beschädigt oder manipuliert wurden. Die Integrität kann aufrechterhalten werden, indem zum Beispiel Änderungsmöglichkeiten eingeschränkt werden. Die Verletzung der Integrität kann zum Beispiel durch einen Vergleich aufgedeckt werden.

Verfügbarkeit (availability)

Die Verfügbarkeit von Informationen, Systemen und Services bedeutet, dass (im Fall einer berechtigten Anfrage) auf sie zugegriffen werden kann und sie verwendet werden können. Die Verfügbarkeit wird zum Beispiel durch Redundanz, Kapazität und Ausfallsicherheit aufrechterhalten.

Authentizität (authenticity)

Die Authentizität von Informationen bedeutet, dass diese echt sind. Dies umfasst die *Integrität (integrity)*, beinhaltet jedoch zusätzlich, dass ihre Herkunft verifiziert ist. Die Authentizität eines Kommunikationspartners (Person oder IT-Komponente) kann durch die *Authentisierung* festgestellt werden, die von Daten beispielsweise mithilfe von Signaturen.

Verantwortlichkeit (accountability)

Die Verantwortlichkeit bedeutet (im Sinne eines weiteren Ziels der IT-Sicherheit), dass Handlungen einer Entität eindeutig auf diese identifizierbare Entität zurückgeführt werden können. Dies kann unterschiedlichen Zwecken dienen. Anwendungsbeispiele sind die Auswertung von *Protokolldaten* (Unleugbarkeit), die gerichtsfeste Identifikation eines Verursachers (*Forensik*) und die Erfassung

der Nutzung (zum Zwecke der Abrechnung oder auch der Ressourcenzuteilung und -optimierung).

CIA-Triade

Die Abkürzung bezieht sich auf die drei Anfangsbuchstaben der Aspekte „Confidentiality" *(Vertraulichkeit)*, „Integrity" *(Integrität)* und „Availability" *(Verfügbarkeit)*. Diese Aspekte werden verwendet, um *Sicherheitsanforderungen* oder *Bedrohungen* zu beschreiben, weshalb bisweilen auch der Terminus CIA-Sprache verwendet wird.

Es wurde darauf hingewiesen, dass die *Vertraulichkeit* einer Information nicht wiederherstellbar ist, wenn sie einmal verloren ging. Man kann davon ausgehen, dass diese Tatsache dazu geführt hat, dass das Vorsorgeprinzip in der IT-Sicherheit und auch im *Datenschutz* tief verankert ist. Da „Protect/Prevent" deshalb immer im Vordergrund steht, gelten IT-Sicherheitsexperten oft als neurotisch vorausschauend, gründlich und vorsichtig.[4] Im Unterschied dazu können IT-Experten fast immer davon ausgehen, dass Reparaturen und nachträgliche Verbesserungen möglich sind.

2.1.2 Analyse und Lösungsansatz

Eigentümer haben ein Interesse daran, Werte zu erhalten (bzw. zu schützen). Um zu wissen, was zu tun ist, ist eine Problemanalyse notwendig. Nur mit einer solchen „vorsorglichen Analyse" (links in Abb. 2) ist zielgerichtetes Handeln möglich. Es wird eine Bedrohungs- und Risikoanalyse durchgeführt: Werte sind Bedrohungen ausgesetzt. Deshalb werden Sicherheitsmaßnahmen implementiert, die jedoch lücken- und fehlerhaft sein können. Derartige Schwachstellen können die Urheber der Bedrohungen eventuell ausnutzen. Die Werte sind dann einem Risiko ausgesetzt. Um das Risiko zu bestimmen, wird die Wahrscheinlichkeit für das Eintreten eines potentiellen, bezifferbaren Schadens bestimmt bzw. abgeschätzt. Die Bewertung dieser Risiken ermöglicht es, Entscheidungen zu treffen hinsichtlich weiterer Handlungen.

Bei der „vorsorglichen Analyse" (links in Abb. 2) ist (a) die Kenntnis der verwendeten Informationstechnologie entscheidend, weshalb in diesem Buch auch das Thema „IT" vertieft wird. Für die Schadensabschätzung muss (b) die Rolle der verwendeten IT zur Erfüllung geschäftlicher Aufträge bekannt sein. Diese Informationen liefern die Geschäftseinheiten, was in diesem Buch nicht näher betrachtet wird.

Die Spalten 2 und 3 in Abb. 2 geben einen Ausblick auf das, was bei der Nutzung der IT wirklich geschieht bzw. geschehen kann. Es kommt zu Angriffen (Szenario 2 in Abb. 2), deren Ausgang man durch die Analyse vorwegzunehmen und durch die Implementierung von Sicherheitsmaßnahmen (Beseitigung von Schwachstellen) zu

---

[4] Nur in Bereichen wie dem Flugzeugbau hat sich eine ähnliche Qualitätskultur der Vorsorge etabliert, nachdem in den ersten Jahrzehnten der Luftfahrt viele Tote zu beklagen waren.

beeinflussen versucht. Gelingt das nicht oder nicht in ausreichender Weise, wird aus dem Angriff ein Einbruch und aus dem möglichen Schaden ein tatsächlicher.

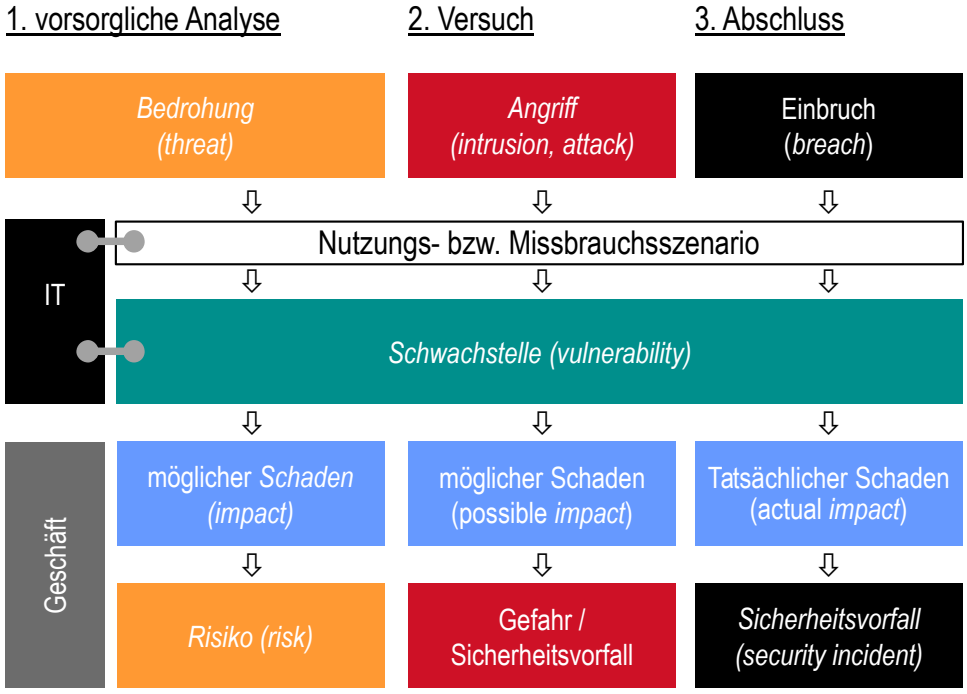


Abb. 2: Risikobewertung (Vorsorge) und zwei Abläufe bei der Nutzung der IT (*kursive Begriffe* sind gängig, andere nicht)[5]

Es folgt eine Detaillierung der „vorsorglichen Analyse“ (links in Abb. 2).

Bedrohung (threat)

Bedrohungen sind absehbare Szenarien oder Umstände, die das Potenzial aufweisen, eine *Sicherheitsrichtlinie (security policy)* zu verletzen. Bedrohungen richten sich auf *Werte (assets)*. Der Geschäftsbetrieb wird jedoch nur dann gestört, wenn eine *Schwachstelle (vulnerability)* existiert und die Bedrohung diese ausnutzt.

Risiko (risk)

Ein Risiko entsteht, wenn eine *Bedrohung* auf eine *Schwachstelle (oder Sicherheitslücke, vulnerability)* trifft und diese mit einer bestimmten Wahrscheinlichkeit (aus)nutzen kann, so dass dies den Geschäftsbetrieb beeinträchtigt bzw. beeinträchtigen kann.[6]

---

5 vergleiche: Eberhard von Faber: Vorlesungsskript; Technische Hochschule Brandenburg

6 vergleiche auch: SP 800-30: Guide for Conducting Risk Assessments; NIST (National Institute of Standards and Technology); Rev. 1, Sept. 2012

Es gibt vier Möglichkeiten der *Risikobehandlung*.[7]

Die Beeinträchtigung des Geschäftsbetriebes wird als **Schaden** (impact) bezeichnet und vorzugsweise in Euro oder anderer Währung gemessen, um Risiken direkt vergleichen zu können. Das ist für die *Risikobehandlung* wichtig, da hier in der Regel Prioritäten für die *Risikominderung* bestimmt werden müssen. Das Risiko wird oft als Produkt aus dem Schaden und dessen *Eintrittswahrscheinlichkeit* berechnet. Dies ist für nicht allzu große Schäden und nicht allzu kleine Eintrittswahrscheinlichkeiten ein guter Ansatz.

Unter **Risikomanagement** versteht man den Umgang mit Risiken. Das schließt die Identifikation von Risiken, deren Bewertung bzw. die Risikoabschätzung, die →*Risikobehandlung*, die Risikokommunikation und die Überwachung und Überprüfung von Risiken ein. Die **Risikoidentifikation** verbindet *Bedrohungen* mit Werten und betrachtet existierende *Sicherheitsmaßnahmen* und sucht nach *Schwachstellen*. Die Suche nach *Schwachstellen* bildet den Kern in dieser Analyse von Szenarien der Nutzung bzw. des Missbrauchs der IT.

Eintrittswahrscheinlichkeit

Der Begriff Eintrittswahrscheinlichkeit (likelihood, probability) wird im Risikomanagement verwendet und bezeichnet dort den Grad der Möglichkeit des Eintretens eines Schadens.

Geht die Bedrohung von (einem) Menschen aus, so spricht man häufig auch von **Angriffswahrscheinlichkeit**, obwohl sie die Wahrscheinlichkeit des Gelingens eines Angriffes misst.

Es gibt diverse Parameter, die die Angriffswahrscheinlichkeit beeinflussen und einzeln abgeschätzt und aggregiert werden, um sie zu bestimmen. Dabei geht man davon aus, dass Angreifer rational in dem Sinne handeln, dass sie Kosten und Nutzen abwägen. Zu den Parametern oder Einflussfaktoren gehören: prinzipieller Nutzen für den Angreifer; Wissen des Angreifers über diesen prinzipiellen Nutzen; Fähigkeit des Angreifers, daraus einen persönlichen Gewinn zu erzielen; Aufwand; Fähigkeit des Angreifers zum Angriff; Gelegenheit zum Angriff; Wahrscheinlichkeit entdeckt zu werden und Höhe der Sanktionen.

Der Aufwand gliedert sich weiter in Kapitalaufwendungen für notwendige Ausrüstungen (Werkzeuge usw.), die für den Angriff notwendige Zeit und die Zeit für die Vorbereitung. Hinsichtlich der Fähigkeiten des Angreifers können ferner betrachtet werden: sein Wissen über die Sicherheitsmaßnahmen; Expertise bezüglich der Nutzung der einzusetzenden Werkzeuge sowie Fähigkeiten zur Planung und Umsetzung.

---

[7] ISO/IEC 27005 – Information technology — Security techniques — Information security risk management; 2011

Risikobehandlung (risk treatment)

Es gibt vier Möglichkeiten der Risikobehandlung oder Risikobewältigung.[8]

(1) **Risikoakzeptanz** (risk retention; oft auch: risk acceptance). Risiken können akzeptiert werden. In diesem Fall sind keine weiteren Maßnahmen vorgesehen. Die Risikohöhe, bis zu der eine Organisation das Risiko akzeptiert, kann sehr unterschiedlich sein. Man spricht auch von unterschiedlichem **Risikoappetit** (risk appetite). Auch außerhalb der IT gehen zum Beispiel Start-up-Unternehmen in der Regel höhere Risiken ein als etablierte Marktführer.

(2) **Risikominderung** (risk reduction). Risiken können reduziert werden, indem *Sicherheitsmaßnahmen* implementiert oder verbessert werden. Dadurch werden *Schwachstellen* (vulnerabilities) beseitigt. Es verbleibt dann ein **Restrisiko** (residual risk). Kann dieses Restrisiko akzeptiert werden (siehe erste Möglichkeit zur Behandlung), so ist die Risikobehandlung abgeschlossen. Andernfalls wird nach weiteren Verbesserungen gesucht. Entscheidungen über die Risikominderung (Priorisierung der Umsetzung, Suche nach Alternativen) unterliegen in der Regel einer Kosten-Nutzen-Betrachtung. Dafür müssen *Risiken* einheitlich in Euro oder anderer Währung gemessen werden.

(3) **Risikoübertragung** (risk transfer). Risiken können übertragen bzw. abgewälzt werden. Die bekannteste Form der Risikoübertragung ist die Risikoversicherung, die es auch in Bezug auf die IT-Sicherheit gibt. Wie bei allen Versicherungen wird der Versicherungsvertrag nur dann zum Abschluss kommen, wenn das Risiko bekannt und beschränkt (klein, beherrschbar) ist. Oft ist es dazu nötig, dass der Versicherungsnehmer Sicherheitsvorkehrungen trifft, das Risiko also bereits reduziert hat. In diesem Sinne wird nur ein *Restrisiko* versichert.

(4) **Risikovermeidung** (risk avoidance). Risken können vermieden werden. Insbesondere wenn andere Methoden der Risikobehandlung zu teuer sind oder das Risiko generell nicht beherrschbar erscheint, kann versucht werden, die Einsatzumgebung oder die Art der Nutzung so zu verändern, dass das Risiko nicht mehr oder in verminderter Höhe auftritt. Zum Beispiel werden Daten an anderer Stelle verarbeitet, wo bestimmte Risiken nicht mehr auftreten.

Sicherheit (security)

Sicherheit bedeutet die Abwesenheit nicht-akzeptierter *Risiken (risks*). Alternative Formulierung: Sicherheit bedeutet, dass noch bestehende Risiken (für die die betreffende Organisation selbst die Folgen zu tragen hat) von dieser Organisation akzeptiert wurden (siehe *Risikoakzeptanz*). Dieser Zustand wird erreicht, wenn technische, prozessbezogene und organisatorische *Sicherheitsmaßnahmen* eingeführt und dauerhaft umgesetzt und aufrechterhalten werden.

---

[8] ISO/IEC 27005 – Information technology — Security techniques — Information security risk management; 2011

Die **IT-Sicherheit** bezieht sich auf die Sicherheit von Informationen/Daten, die mit elektronischen Systemen verarbeitet werden, und auf die Sicherheit der informationsverarbeitenden Systeme selbst. IT-Sicherheit ermöglicht es einem Anwender (Organisation oder Nutzer), IT-Services zu nutzen, obwohl damit *Risiken* verbunden sind.

Der Begriff **Cyber-Sicherheit** soll hervorheben, dass die IT-Sicherheit den gesamten „Cyber-Raum" im Auge behalten muss, da die IT-Systeme heutzutage hochgradig vernetzt und oft über das Internet erreichbar sind.

Klarstellungen:

Alle folgenden Begriffe beziehen sich auf den Bereich der elektronischen Informationsverarbeitung. In diesem Sinne ist der im Folgenden der Einfachheit halber oft verwendete Begriff „Sicherheit" mit IT-Sicherheit (bzw. Cyber-Sicherheit) gleichzusetzen.

Der Begriff Informationssicherheit bezieht sich dagegen auf Informationen, die in beliebiger Form gespeichert sein können, auch in Papierform. Die so verstandene Informationssicherheit wird im vorliegenden Buch nicht behandelt.

Sicherheitsziel (security objective)

Ein Sicherheitsziel beschreibt den zu erreichenden Zustand. In der Regel werden dabei ein bestimmtes Subjekt und eine bestimmte Umgebung mit den Zielen der Informationssicherheit verknüpft, also mit *Vertraulichkeit (confidentiality*), *Integrität (integrity*), *Authentizität (authenticity*), *Verfügbarkeit (availability)* und *Verantwortlichkeit (accountability*). Ein Sicherheitsziel kann darüber hinaus das Ergebnis einer Handlung vorgeben.

Sicherheitskategorie (security category)

Die Sicherheitskategorie verbindet die *Sicherheitsziele* für Informationen oder Systeme mit einer Einschätzung des möglichen *Schadens*. Die Sicherheitsziele sind *Vertraulichkeit (confidentiality*), *Integrität (integrity*) und *Verfügbarkeit (availability).*

Der mögliche Schaden wird zum Beispiel in den Stufen niedrig (low), mittel (moderate), hoch (high) und nicht anwendbar (not applicable) gemessen, wobei der letztgenannte Wert nur dann verwendet werden kann, wenn keine Einschränkungen hinsichtlich der Vertraulichkeit bestehen.

Das NIST konstruiert daraus Vektoren der folgenden Form:[9]

---

[9] FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems; NIST (National Institute of Standards and Technology); Gaithersburg, February 2004

Sicherheitskategorie = { (Vertraulichkeit, Schaden),
(Integrität, Schaden),
(Verfügbarkeit, Schaden) }

„Sicherheitskategorien können in Verbindung mit Informationen über Schwachstellen und Bedrohungen verwendet werden, um Risiken für eine Organisation zu bestimmen.“[10]

2.1.3 Lösung und Umsetzung

Nachdem die *Risiken* analysiert und eine Entscheidung zur *Risikominderung* getroffen wurde, geht es nun darum, mit Hilfe von Maßnahmen wirklich für Sicherheit zu sorgen.

Das heißt, es werden *Sicherheitsmaßnahmen* entwickelt bzw. ausgewählt und implementiert. Es gibt zwei Herangehensweisen für die Auswahl von Sicherheitsmaßnahmen und die Entscheidung über ihre Implementierung:

- Der risikobasierte Ansatz eignet sich für Verbesserungen und die Absicherung komplexer bestehender Systeme. Er basiert auf dem oben beschriebenen Risikobegriff (siehe Darstellung links in Abb. 2). Dabei werden möglichst alle Nutzungs- bzw. Missbrauchsszenarien untersucht, für die es eine Bedrohung (eines Wertes) gibt. Man sucht entlang des Informationsflusses nach Schwachstellen und ermittelt das Risiko. Dieses wird verglichen mit den Kosten für eine Maßnahme, die die Schwachstelle schließt. Das Vorgehen ist im Einzelnen zu kompliziert, um es hier praxisnah beschreiben zu können.[11] Der Ansatz wird weiter unten in der Erklärung des Begriffs *Sicherheitskonzept* skizziert.
- Ein einfacherer Ansatz[12] eignet sich für die Informationstechnik und folgt dem Entwicklungsprozess („grüne Wiese“). Die Analyse der Einsatzumgebung einschließlich der Bedrohungen führt im zweiten Schritt zur Definition von *Sicherheitszielen* (Was soll erreicht werden?). Daraus werden dann wiederum *Sicherheitsanforderungen* abgeleitet (Was wird benötigt?), die Eigenschaften der zu implementierenden *Sicherheitsmaßnahmen* beschreiben. Der Ansatz wird weiter unten in der Erklärung des Begriffs *Sicherheitsvorgaben* skizziert.

---

10 ebenda, Übersetzung vom Autor

11 Eberhard von Faber und Wolfgang Behnsen: Joint Security Management: organisationsübergreifend handeln (Mehr Sicherheit im Zeitalter von Cloud-Computing, IT-Dienstleistungen und industrialisierter IT-Produktion); Springer Vieweg, Wiesbaden 2018, 244 Seiten, 60 farbige Abbildungen, ISBN 978-3-658-20833-2; https://doi.org/10.1007/978-3-658-20834-9; Kapitel 7.8 (S. 149-153)

12 ISO/IEC 15408 – Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model; 2009; und: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; April 2017, Version 3.1 Revision 5, https://commoncriteriaportal.org

Im Unternehmenskontext werden immer *Sicherheitsrichtlinien* (Regelwerke) benötigt, die durch die Definition von Regeln und Kriterien eine Absicht und eine Richtung vorgeben. Siehe Abb. 3. Diese entfalten ihre Wirkung in der Regel erst dadurch, dass *Sicherheitsmaßnahmen* spezifiziert und implementiert werden. Wird von *Sicherheitsmaßnahmen* gesprochen, so kann die Spezifikation oder die Implementierung gemeint sein (Abb. 3). Im Allgemeinen gibt es zwischen beiden einen Kreislauf: Die Implementierung wird kontrolliert und gegebenenfalls korrigiert.

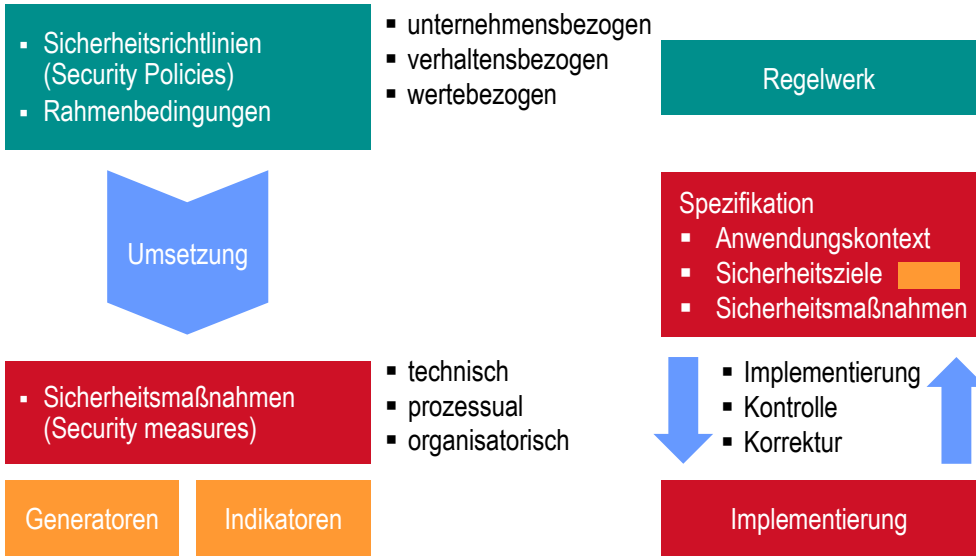


Abb. 3: Regelwerke und Sicherheitsmaßnahmen[13]

Es folgen zwei Empfehlungen, bevor wir mit den Begriffserklärungen fortfahren.

- Es wird dringend empfohlen, *Sicherheitsziele* zu definieren, bevor mit der eigentlichen Spezifikation der Sicherheitsmaßnahmen begonnen wird (siehe Abb. 3, gelbes Rechteck rechts in der Mitte). Aus Bedrohungen und Risiken sofort Sicherheitsmaßnahmen abzuleiten ist sehr fehleranfällig! Oft werden dann nämlich Maßnahmen ausgewählt, die ungeeignet, also nicht effektiv (wirksam) bezüglich der Abwehr der Bedrohung sind. Schnell wird beispielsweise erwartet, dass der Werkschutz auch gegen Innentäter hilft. Die explizite Ausarbeitung von Sicherheitszielen lenkt die Aufmerksamkeit auf die Absicht und den Zweck. Außerdem ist es dann besser möglich, die Eignung der definierten Sicherheitsmaßnahmen zu prüfen.
- Es wird ebenfalls empfohlen,[14] bei den Sicherheitsmaßnahmen zwischen *Generatoren* und *Indikatoren* zu unterscheiden und beide in gleicher Art und Weise zu

---

13 vergleiche: Eberhard von Faber: Vorlesungsskript; Technische Hochschule Brandenburg

14 Eberhard von Faber and Wolfgang Behnsen: Secure ICT Service Provisioning for Cloud, Mobile and Beyond (ESARIS: The Answer to the Demands of Industrialized IT Production

spezifizieren und zu implementieren. Siehe Abb. 3 (gelbe Rechtecke ganz unten links). Dafür gibt es im Wesentlichen zwei Gründe. Erstens werden dadurch Wirkungsketten besser sichtbar, sodass sich Regelkreise bilden lassen, ohne die zielgerichtete Verbesserungen nicht möglich sind. Zweitens benötigt man ein Lagebild zur IT-Sicherheit, und häufig müssen diese Informationen in Form betrieblicher Nachweise auch an Kunden, Geschäftseinheiten oder Interessengruppen weitergegeben werden, die diese für ihr Risikomanagement, zur Dokumentation von Compliance oder als Leistungsnachweise benötigen.

Die **„Generatoren"** „produzieren" Sicherheit. Sie arbeiten direkt gegen eine *Bedrohung* oder sie verringern die Wahrscheinlichkeit, dass ein Angriff erfolgreich durchgeführt wird und ein wirklicher Schaden entsteht. Es ist auch möglich, dass sie eine Schwachstelle beseitigen (so dass die Bedrohung ins Leere läuft) oder dass der Schaden verringert wird. Die **„Indikatoren"** „messen". Sie tragen, wenn auch indirekt, wesentlich zur Sicherheit bei, weil sie Informationen liefern über die Wirksamkeit bzw. Funktionsfähigkeit der „Generatoren". Oder sie liefern Informationen, die es gestatten, verdächtige oder feindliche Aktivitäten zu identifizieren. In beiden Fällen wehrt die Maßnahme (der „Indikator") keinen Angriff ab und verbessert die Sicherheit nicht direkt. Sie liefert aber Informationen und ermöglicht es damit, Gegenmaßnahmen zu ergreifen.

Werden die „Indikatoren" nicht ebenso wie die „Generatoren" spezifiziert, wird ihnen nicht die gleiche Bedeutung beigemessen werden. Auch ist es schwieriger, die Vollständigkeit der Maßnahmen zu gewährleisten und Abhängigkeiten zu erkennen und zu gestalten. Das *Zusammenwirken* der Sicherheitsmaßnahmen spielt eine entscheidende Rolle. Nur wenn dem Zusammenwirken genügend Aufmerksamkeit zuteil wird, kann ein integriertes, sicheres Ganzes entstehen.

Die Cloud Security Alliance (CSA) unterscheidet sogar drei Arten von Sicherheitsmaßnahmen:[15] Präventive Maßnahmen (preventive controls) entsprechen den Generatoren, sie verhindern etwas. Detektierende Maßnahmen (detective controls) identifizieren Vorfälle und charakterisieren sie dann. Die korrigierenden Maßnahmen (corrective controls) mindern den Schaden.

Sicherheitsrichtlinie (security policy)

Sicherheitsrichtlinien geben durch die Definition von Regeln und Kriterien eine Absicht und eine Richtung vor. In der Regel werden Sicherheitsrichtlinien unabhängig von der Technologie erarbeitet. Sie beziehen sich auf einen größeren

---

Balancing Between Buyers and Providers); Springer Vieweg, Wiesbaden 2017, 383 pages, 159 figures, ISBN 978-3-658-16481-2, 2nd updated and extended Edition, https://doi.org/10.1007/978-3-658-16482-9; Kap. 8.3.2 (Seite 153-155)

15 Cloud Security Alliance (CSA): Guide to the CSA Internet of Things (IoT) Security Controls Framework; 2019

Arbeitsbereich oder das ganze Unternehmen und werden häufig vom Management verbindlich eingeführt.

Sicherheitsrichtlinien sind sehr allgemeinen *Sicherheitszielen (security objectives)* ähnlich, wenn sie beschreiben, was erreicht werden soll. Sie ähneln eher *Sicherheitsanforderungen (security requirements)*, wenn sie wie allgemeine Handlungsempfehlungen formuliert sind.

Der Begriff Sicherheitsrichtlinie wird auch im technischen Kontext benutzt. Dann bezieht er sich meist auf eine spezifische Konfiguration einer IT-Komponente oder eines IT-Systems.

Sicherheitsmaßnahme (security measure, security control)

Sicherheitsmaßnahmen sind Vorkehrungen, die getroffen werden, um Risiken zu verringern. Sicherheitsmaßnahme ist gleichbedeutend mit Sicherheitskontrolle (oft deutsch für: security control). Sicherheitsmaßnahmen, können administrativer, organisatorischer oder prozessbezogener, technischer oder juristischer Art sein.

Der Begriff Sicherheitsmaßnahme ist hinsichtlich des Abstraktionsgrades bzw. Detaillierungsniveaus nicht genau gefasst. Sicherheitsmaßnahmen können sehr umfassend oder auch sehr implementierungsnah sein und reichen manchmal zum Beispiel von allgemein „Zugriffskontrolle“ bis zu detaillierten, beigeordneten Vorgaben wie der Festlegung einer Passwortlänge. Die Sicherheitsarchitektur *ESARIS* reserviert den Begriff Sicherheitsmaßnahme (security measure) daher auf Beschreibungen auf Ebene 4 der schrittweisen Verfeinerung in der „Hierarchie der Sicherheitsstandards (Hierarchy of Security Standards)“, die als „Orchestration Layer“ bezeichnet wird und in der die Abstimmung der Maßnahmen im Sinne einer übergreifenden Sicherheitskonzeption erfolgt.

Sicherheitsanforderung (security requirement)

Mit Hilfe von Sicherheitsanforderungen werden die Eigenschaften von *Sicherheitsmaßnahmen (security measures)* beschrieben. Sicherheitsanforderungen ergeben sich aus *Sicherheitszielen (security objectives)*, die wiederum als Antwort auf festgestellte Bedrohungen (*threats*) formuliert werden.

Sicherheitsanforderungen besitzen unterschiedlichen Detaillierungsgrad: Im Allgemeinen erfolgt deren Definition in einer Weise, dass die Flexibilität bei der Auswahl und Konzeption der Sicherheitsmaßnahmen gewahrt bleibt. Der Begriff Sicherheitsanforderung wird aber auch im Sinne von technischen Spezifikationen verwendet, die die Art und Weise der Implementierung (Umsetzung) exakt beschreiben.

Sicherheitsvorgaben (security target)

Sicherheitsvorgaben sind eine umfassende Sicherheitsspezifikation, die Folgendes beinhaltet: die Feststellung von *Bedrohungen (threats)* in einer definierten

Umgebung (Problembeschreibung), die Beschreibung von *Sicherheitszielen (security objectives)* als Reaktion auf diese Problembeschreibung sowie die Beschreibung der *Sicherheitsanforderungen (security requirements)*, mit deren Hilfe die *Sicherheitsziele (security objectives)* erreicht und die *Bedrohungen (threats)* abgewehrt werden sollen. Sicherheitsvorgaben sind auch der Ausgangspunkt der Common Criteria.[16]

Sicherheitskonzept (security concept)

Ein Sicherheitskonzept ist das Ergebnis eines definierten, systematischen Vorgehens, bei dem *Sicherheitsmaßnahmen* definiert bzw. spezifiziert werden, die in einer definierten Umgebung (System) implementiert werden sollen.

Typischerweise werden die Sicherheitsmaßnahmen wie folgt abgeleitet. 1) Es werden die *Werte* (assets) erfasst. 2) Vorab festgelegte, grundlegende *Bedrohungen* (threats) werden den Werten zugeordnet. Es wird untersucht, ob sie für diese relevant sind. Gegebenenfalls werden die Bedrohungen konkretisiert und auf das Szenario zugeschnitten. 3) Nun wird abgeschätzt, mit welcher Wahrscheinlichkeit welcher Schaden entsteht. Oft werden jeweils nur drei bis fünf Werte verwendet (zum Beispiel: niedrig, mittel, hoch bzw. unbedeutend, gering, mittel, groß, fatal oder ähnlich). 4) Die Kombination beider Werte (in einer **Risikomatrix**) zeigt den Schutzbedarf, der Ausdruck für die Dringlichkeit der Implementierung von Sicherheitsmaßnahmen ist. Die Positionierung der einzelnen Szenarien in der Risikomatrix erlaubt die Priorisierung und ergibt ein Gesamtbild der Risikosituation. 5) Es erfolgt die Auswahl von Sicherheitsmaßnahmen. Meist beginnt man mit den Szenarien mit dem höchsten Schutzbedarf. Liegt der Schutzbedarf unter einem bestimmten Schwellwert, so wird keine Maßnahme vorgesehen. 6) Die geplanten Sicherheitsmaßnahmen werden hinsichtlich ihrer Wirksamkeit, der Kosten usw. bewertet. 7) Zum Schluss wird das *Restrisiko* abgeschätzt. Kann es akzeptiert werden, ist die Konzepterstellung abgeschlossen. Ist das Restrisiko immer noch zu hoch, müssen weitere Sicherheitsmaßnahmen implementiert oder bestehende verbessert werden (siehe Punkt 5).

2.1.4 Qualitätssicherung und Vertrauenswürdigkeit

Sicherheitsmaßnahmen werden ausgewählt bzw. abgeleitet und implementiert, um für ein adäquates *Sicherheits*niveau zu sorgen (siehe Abb. 4). Das setzt aber voraus, dass die implementierten Sicherheitsmaßnahmen einige Bedingungen erfüllen bzw. bestimmte Eigenschaften oder Qualitäten aufweisen. In Abb. 4 sind dies die Haupteigenschaften *Wirksamkeit* und *Korrektheit*, denen jeweils weitere Kriterien zugeord-

---

[16] ISO/IEC 15408 – Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model; 2009; und: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; April 2017, Version 3.1 Revision 5, https://commoncriteriaportal.org

net sind. Nur durch ihre Wirksamkeit und Korrektheit reduzieren Sicherheitsmaßnahmen *Risiken* derart, dass ein System als sicher angesehen werden kann.

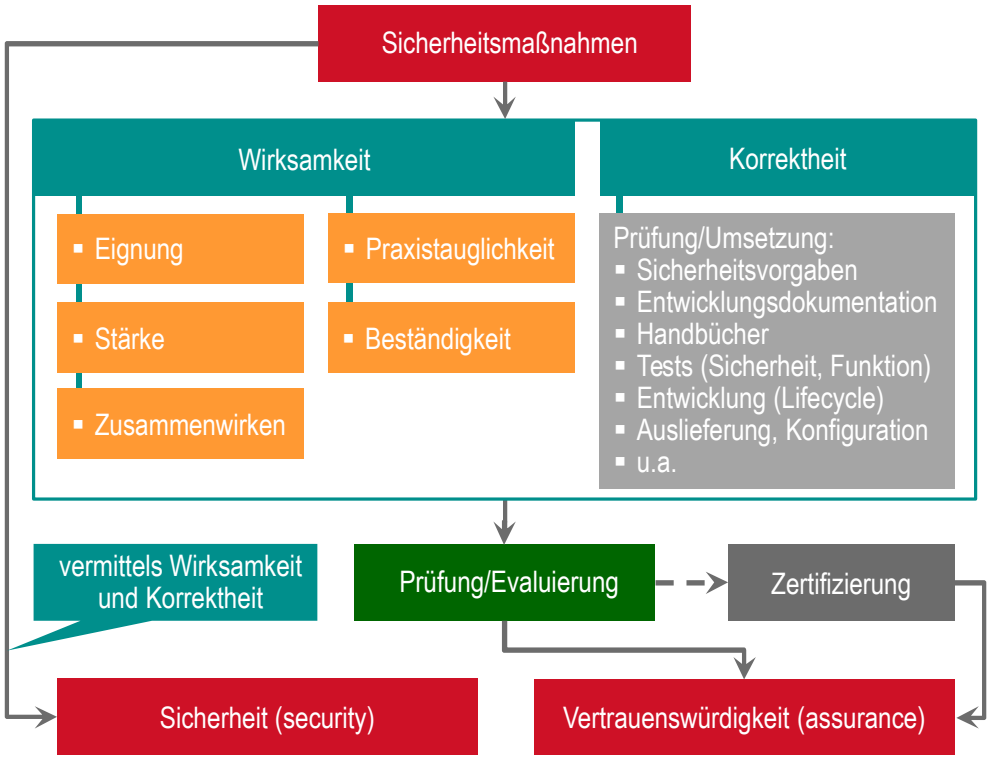


Abb. 4: Sicherheit und Vertrauenswürdigkeit

Anwender führen in der Regel keine aufwendige Bedrohungs- und Risikoanalyse durch, um auf Basis der dann festgestellten Risiken zu entscheiden, ob sie ein System nutzen oder eine Dienstleistung in Anspruch nehmen wollen. Vielmehr treffen sie ihre Entscheidung auf Basis der ihnen verfügbaren Informationen bezüglich der IT-Sicherheit des Systems oder der Dienstleistung oder, mit anderen Worten, aufgrund ihrer Einschätzung von dessen oder deren *Vertrauenswürdigkeit*. Die Vertrauenswürdigkeit steigt, wenn verlässliche Informationen über die Sicherheit vorliegen. Beides ist voneinander zu unterscheiden: Die Sicherheit kann hoch sein, während die Vertrauenswürdigkeit aufgrund mangelnder Informationen unzureichend ist. Da Anwender aufgrund der Vertrauenswürdigkeit entscheiden, müssen verlässliche Informationen bereitgestellt werden. Dies erfolgt durch Prüfung (und Bewertung) der Wirksamkeit und Korrektheit, die oft in Form einer formalisierten Evaluierung durch Experten erfolgt (siehe Abb. 4, grünes Rechteck „Prüfung/Evaluierung“). Der Umfang der Prüfung/Evaluierung kann äußerst unterschiedlich sein! Er reicht von einer Vergangenheitsbetrachtung („Uns ist kein größerer Sicherheitsvorfall bekannt“) über Entscheidungen aufgrund der Reputation („Die Firma ist für gute IT-Sicherheit bekannt“) bis hin zu detaillierten Untersuchungen durch

technisch versiertes Personal unter Verwendung vordefinierter Kriterien nach wissenschaftlichen Maßstäben (Begutachtung, Evaluierung). Eine *Zertifizierung* bescheinigt eine bestimmte, mit entsprechendem Testat erfolgreich abgeschlossene Prüfung/Evaluierung.

Warum ist dieser Unterschied zwischen Sicherheit und Vertrauenswürdigkeit sehr wichtig? IT-Sicherheitsmaßnahmen werden meist durch das IT-Personal implementiert und gepflegt (IT-Sicherheit). Viele IT-Sicherheitsexperten verbringen dagegen sehr viel Zeit damit, Informationen über die Sicherheit zu beschaffen, zu bewerten und zu kommunizieren. Dies ist eine sehr wichtige und sehr nützliche Arbeit (für die Vertrauenswürdigkeit). Allerdings führt eben nur ein sehr kleiner Teil dieser Arbeit zu einer Verbesserung der IT-Sicherheit, nämlich dann, wenn die Information (in Form einer *Schwachstellen*information) zurückfließt und IT-Personal und Prozessmanager die Lücken schließen und damit die IT-Sicherheit verbessern.

Die folgenden Begriffserklärungen beginnen mit den Kriterien für „gute" IT-Sicherheitsmaßnahmen. Dann folgen Begriffe wie Vertrauenswürdigkeit, die auch in das dann folgende Kapitel „Sicherheitsmanagement" (Kapitel 2.2) überleiten.

Wirksamkeit (Maßnahmen) (effectiveness)

Die inzwischen nicht mehr verwendeten „Information Technology Security Evaluation Criteria (ITSEC)"[17] unterscheiden zwischen der Wirksamkeit (effectiveness) und *Korrektheit* (correctness) von Sicherheitsmaßnahmen. Beides sind Kriterien für die Güte oder Qualität bzw. allgemeine Anforderungen an Sicherheitsmaßnahmen. Sicherheitsmaßnahmen sind wirksam, wenn sie die Kriterien Eignung, Stärke und Zusammenwirken erfüllen.

Eignung (suitability) drückt aus, inwieweit die Sicherheitsmaßnahme bzw. deren zugrunde liegenden sicherheitsspezifischen Funktionen und Mechanismen „den in den *Sicherheitsvorgaben* identifizierten Bedrohungen… tatsächlich entgegenwirken".[18] Gegenbeispiel: Ein *Einmalpasswortverfahren* ist nicht geeignet, einen Angriff mittels *Man-in-the-Middle* abzuwehren.

Stärke (strength) ist die Fähigkeit einer Sicherheitsmaßnahme, direkten Angriffen gegen zugrunde liegende Algorithmen, Prinzipien und Eigenschaften zu widerstehen. Beispiel: Der kryptografische Algorithmus ist stark, wenn er, nach dem Stand der Technik, einer Kryptoanalyse standhält und auch ein Ausprobieren der Schlüssel praktisch nicht möglich ist (das heißt, viel zu lange dauern würde). „Dieser Aspekt der Wirksamkeit unterscheidet sich von anderen Aspekten darin, dass er den Aufwand an Betriebsmitteln betrachtet, die ein

---

17 Europäische Kriterien für die Bewertung und Zertifizierung der IT-Sicherheit; Version 1.2, 28. Juni 1991; zu beziehen über: </Produktzertifizierung/ZertifizierungnachCC/ITSicherheitskriterien/ITSEC/itsec_node.html; inzwischen von den „Common Criteria for Information Technology Security Evaluation" abgelöst.

18 ebenda.

Angreifer benötigen würde, um einen erfolgreichen direkten Angriff durchzuführen."[19]

Zusammenwirken (binding) drückt aus, inwieweit die sicherheitsspezifischen Funktionen und Mechanismen sich gegenseitig unterstützen und „ein integriertes, wirksames Ganzes bilden".[20] Implementiert wird dies durch Kombination (Staffelung) von Sicherheitsmaßnahmen, durch Redundanzen (Parallelschaltung) und durch Prüfmechanismen. Beispiel für das Zusammenwirken: Die Verschlüsselung erfordert Mechanismen, die die Vertraulichkeit symmetrischer Schlüssel bzw. die Verwendung des authentischen öffentlichen Schlüssels sicherstellen.

Praxistauglichkeit ist die Eigenschaft von Sicherheitsmaßnahmen, unter Realbedingungen tatsächlich wirksam zu sein und nicht umgangen, gemieden, missachtet, ersetzt oder ignoriert zu werden. Dies wird zum Beispiel durch leichte Verständlichkeit von Regeln hinsichtlich von Zielen, Nutzen sowie notwendigen Aktionen bzw. Regeln erreicht oder dadurch, dass die Umsetzung erleichtert, unumgehbar implementiert oder automatisiert wird. In der Literatur wird der anders gelagerte Begriff **Benutzerfreundlichkeit** bzw. manchmal auch „Ease of use" (Einfachheit der Anwendung) verwendet. Er bedeutet, dass Anwender nicht versehentlich einen unsicheren Zustand herstellen, wobei sie jedoch annehmen, er wäre sicher.[21]

Beständigkeit bedeutet, dass die Sicherheitsmaßnahme insbesondere nicht unter der Last eines andauernden Angriffs ihre Wirksamkeit verliert oder einschränkt. Dies ist eine Frage der Ressourcen, der Mittel, des Durchhaltevermögens, der Stabilität und Ausdauer. Beständigkeit ist keine in der IT-Sicherheit übliche Anforderung.[22]

Korrektheit (Maßnahmen)

Die inzwischen nicht mehr verwendeten „Information Technology Security Evaluation Criteria (ITSEC)" [23] unterscheiden zwischen der *Wirksamkeit*

---

[19] ebenda.

[20] ebenda.

[21] Die Praxis zeigt jedoch: Die meisten derartigen Sicherheitsprobleme werden verursacht durch Unkenntnis, Unachtsamkeit, Bequemlichkeit und manchmal sogar durch selbstverschuldete Dummheit.

[22] Die Sicherheitskriterien ITSEC fordern als zusätzliches Kriterium, dass eine Liste von Schwachstellen vorliegt und deren mögliche Auswirkungen analysiert wurden.

[23] Europäische Kriterien für die Bewertung und Zertifizierung der IT-Sicherheit; Version 1.2, 28. Juni 1991; zu beziehen über: https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/ITSicherheitskriterien/ITSEC/itsec_node.html (zuletzt aufgerufen am 21.01.2021); inzwischen von den „Common Criteria for Information Technology Security Evaluation" abgelöst.

(effectiveness) und Korrektheit (correctness) von Sicherheitsmaßnahmen. Beides sind Kriterien für die Güte oder Qualität bzw. allgemeine Anforderungen an Sicherheitsmaßnahmen. Die Korrektheit wird im Rahmen einer Begutachtung (*Evaluierung*) geprüft. Dies schafft bzw. vergrößert die Gewissheit darüber, dass die Sicherheitsmaßnahme bzw. deren zugrunde liegenden sicherheitsspezifischen Funktionen und Mechanismen planungsgemäß entsprechend der Spezifikation implementiert wurden. Dadurch vergrößert sich die *Vertrauenswürdigkeit*.

Vertrauenswürdigkeit (assurance)

Vertrauenswürdigkeit bezeichnet das Maß an Wissen/Vertrauen, dass keine nicht-akzeptierten *Risiken (risks)* bestehen (bzw. die Sicherheit gewährleistet ist). Dies ist dann der Fall, wenn die *Sicherheitsvorgaben (security target)* umgesetzt und die *Sicherheitsziele (security objectives)* erreicht sind. Vertrauenswürdigkeit wird durch Techniken wie die Befolgung bestimmter Sicherheitsverfahren im Lebenszyklus und durch Transparenz hinsichtlich ihrer Einhaltung mit Hilfe von Untersuchungen durch Dritte erreicht.

Das heißt, ein System gilt dann als vertrauenswürdig, wenn dem Anwender genügend Informationen über die *Wirksamkeit* und *Korrektheit* der implementierten *Sicherheitsmaßnahmen* vorliegen.

Zertifizierung (certification)

Generell stellt eine Zertifizierung eine Bestätigung durch eine unabhängige Zertifizierungsstelle dar. Bestätigt werden kann zum Beispiel die Übereinstimmung mit Spezifikationen (*Compliance*). Im engeren Sinne verbirgt sich hinter Zertifizierung im Bereich Sicherheit aber fast immer, dass die *Vertrauenswürdigkeit (assurance)* in einem definierten Prozess mithilfe von vordefinierten Kriterien festgestellt wurde.

Häufig bestätigt die Zertifizierungsstelle dabei lediglich, dass die *Vertrauenswürdigkeit (assurance)* gemäß den Zertifizierungsanforderungen festgestellt wurde (d. h. gemäß den genannten Bedingungen der Befolgung eines definierten Prozesses und vordefinierter Kriterien). Die Beurteilung anhand der vordefinierten Kriterien selbst wird von einer weiteren Partei (der Evaluierungseinrichtung oder dem Prüflabor) durchgeführt. Die Evaluierungseinrichtung muss von der Zertifizierungsstelle akkreditiert sein, was die Prüfung und kontinuierliche Überwachung der Einrichtung und ihrer Tätigkeit erfordert.

2.2 Sicherheitsmanagement

Im vorangehenden Kapitel wurde zuletzt (Kapitel 2.1.4) der Begriff Vertrauenswürdigkeit eingeführt und es wurden Kriterien diskutiert, die für „gute“ Sicherheitsmaßnahmen stehen.

- Aber was passiert, wenn die Sicherheitsmaßnahmen nicht perfekt sind? Im folgenden **Kapitel 2.2.1** wird erklärt, wie solche Schwachstellen entdeckt werden und was man eigentlich unter einer Schwachstelle verstehen kann. Schwachstellen können zu Sicherheitsvorfällen führen, die entdeckt und bearbeitet werden müssen.
- Im **Kapitel 2.2.2** weiten wir den Blick und betrachten Tätigkeitsbereiche und weitere Themen für das Sicherheitsmanagement. Die IT-Sicherheit ist nämlich nur einer ihrer Arbeitsbereiche.

2.2.1 Schwachstellen auffinden, Vorfälle bearbeiten

Fehler in Design und Umsetzung zu finden, um Verbesserungen zu ermöglichen, gehört natürlich zu den wichtigen Aufgaben im Sicherheitsmanagement. Dabei muss systematisch vorgegangen werden. In der Praxis findet man verschiedenste Methoden und Vorgehensweisen. Die Zahl der hierbei verwendeten Begriffe ist groß, und es ist nicht einfach, diese in eine Struktur und auf einen gemeinsamen Nenner zu bringen. Abb. 5 ist der Versuch einer Übersicht. Sie ist nicht vollständig, und die Begriffsdefinitionen in diesem Kapitel können nicht alle Details beleuchten.

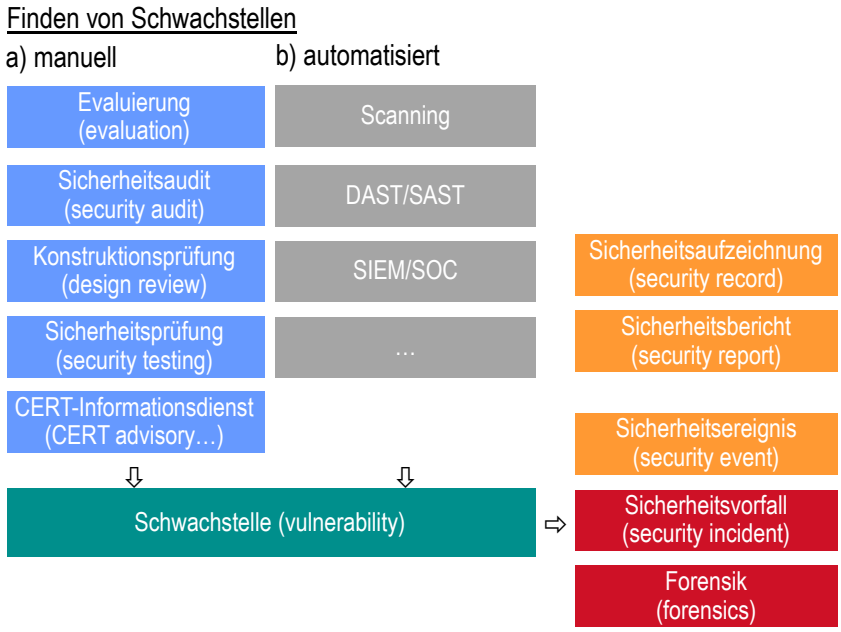


Abb. 5: Schwachstellen im Design und in der Umsetzung auffinden, Vorfälle bearbeiten

Wir werden uns auf diejenigen Methoden und Vorgehensweisen beschränken, die mit „manuell“ überschrieben sind, bei denen also Handarbeit im Vordergrund steht, die von Menschen geleistet wird (blaue Kästchen links in Abb. 5). Natürlich werden die Tests für die Suche nach Fehlern und Lücken auch automatisiert durchgeführt

(graue Kästchen). Die entsprechenden Produkte und Lösungen werden in **Kapitel 6** erläutert.

Das Fehlen oder die Unzulänglichkeit der Absicherung mit Sicherheitsmaßnahmen wird allgemein als Schwachstelle bezeichnet. Nachdem auch die damit zusammenhängenden Begrifflichkeiten geklärt sind, wenden wir uns dann den Konsequenzen zu: Das Sicherheitsmanagement muss sich mit Sicherheitsvorfällen beschäftigen (siehe Abb. 5).

Evaluierung (evaluation)

Eine Evaluierung ist eine systematische, um Vollständigkeit bemühte, unabhängige Überprüfung, Analyse und Bewertung von *Sicherheitsmaßnahmen (security measures)*. Sie wird von Dritten (d.h. von Organisationen/Institutionen, die nicht am Zustandekommen der Maßnahmen beteiligt waren) durchgeführt und verbindet fast immer die Prüfung und Analyse von Unterlagen mit der Durchführung und Bewertung praktischer Tests. Die Evaluierung erfolgt gemäß festgelegter Verfahren und definierter Kriterien.

Staaten und manche Branchen wie die Finanzindustrie haben Schemata aufgebaut, bei denen die Evaluierung nur durch zugelassene (akkreditierte) Prüflabors bzw. **Evaluierungsstellen** erfolgt. **Zertifizierungsstellen** wachen darüber, dass diese die Verfahren einhalten und die Kriterien anwenden und bestätigen das Evaluierungsergebnis (den Evaluierungsbericht) mit einem Zertifikat oder allgemein mit einer Urkunde, die den Evaluierungsgegenstand (das Produkt) für den Einsatz zulässt.

Bei Normen wie den Common Criteria[24] liegen der Evaluierung sogenannte *Sicherheitsvorgaben* (security target) zugrunde, die den Evaluierungsgegenstand (EVG) definieren und die zu prüfenden Sicherheitseigenschaften spezifizieren.

Sicherheitsaudit (security audit)

Ein Sicherheitsaudit ist eine stichprobenartige, unabhängige Überprüfung, Analyse und Bewertung von Aufzeichnungen, Berichten oder beobachteten Tatsachen. Der Fokus liegt auf dem Vergleich oder der *Übereinstimmung* (compliance) mit erwarteten oder zugesicherten Eigenschaften.[25] Es wird geprüft, ob Maßnahmen vorhanden und wirksam sind, Richtlinien und Verfahren einge-

---

[24] ISO/IEC 15408 – Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model; 2009; und: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; April 2017, Version 3.1 Revision 5, https://commoncriteriaportal.org

[25] Die betroffene Organisation kann sich grundsätzlich sogar gegen eine zu tiefe und zu umfangreiche Prüfung wehren. Bei einer Evaluierung hat sie dagegen eher nur Anspruch auf eine vergleichbare Bewertung (zum Beispiel im Vergleich zu Mitbewerbern oder Konkurrenzprodukten). Objektiv müssen natürlich beide Vorgehensweisen sein.

halten werden und Änderungen an Maßnahmen, Richtlinien oder Verfahren notwendig sind und, wenn ja, welche empfehlenswert sind.

Ein Sicherheitsaudit kann von organisationsinternen Organisationen (wie der Revisions- oder der Sicherheitsabteilung) durchgeführt werden oder durch Externe (Kunden, Prüfgesellschaften usw.).

Ein Audit wird in Form einer Begehung, Befragung und Auswertung von *Sicherheitsaufzeichnungen (security record)* durchgeführt und beinhaltet in der Regel Praxistests.

Konstruktionsprüfung (design review)

Der Begriff Konstruktionsprüfung wird nur selten benutzt, gibt aber gut wieder, was sich hinter dem englischen Begriff „Design review" verbirgt. Meist werden nämlich nicht nur Entwürfe und Pläne (design) geprüft, ob sie die Anforderungen korrekt umsetzten, sondern auch, ob dies ebenfalls für die dingliche Ausführung und Umsetzung (implementation) gilt – im IT-Jargon häufig auch Instanziierung genannt.

Die Prüfung der korrekten Umsetzung der Anforderungen bezieht sich nämlich meist nicht nur auf die Entwürfe und Pläne (design), sondern auch auf die Realisierung bzw. Umsetzung (implementation).

Solche Prüfungen erfolgen meist innerhalb der Organisation. Sie werden von oder unter Mitwirkung der Sicherheitsmanagementabteilung durchgeführt und sind oft notwendige Voraussetzung für die Produktionsfreigabe (Freigabe zum Produktivbetrieb, „ready for production", „ready to deliver" o.ä.).

Sicherheitsprüfung (security testing)

Der Begriff Sicherheitsprüfung ist sehr unscharf und steht hier für die Übersetzung des amerikanischen Begriffs „Security testing".

Mit Sicherheitsprüfung wird die unabhängige Untersuchung und praktische Überprüfung von IT-Komponenten und IT-Systemen bezeichnet, bei der die Suche nach *Schwachstellen* im Vordergrund steht. Sicherheitstests sind oft Teil von *Konstruktionsprüfungen* (design reviews).

Meist handelt es sich um **Penetrationstests** (penetration testing), auch „**Ethical Hacking**" oder „**White hat hacking"** genannt. Dabei wendet der Prüfende manuell und halbautomatisch Methoden und Werkzeuge an, von denen erwartet wird, dass sie auch ein Angreifer (Einbrecher, oft als „hacker" bezeichnet) anwenden würde. Es werden also Angriffe simuliert und tatsächlich durchgeführt.

CERT-Informationsdienst (CERT advisory service)

Ein CERT-Informationsdienst (manchmal auch als Schwachstelleninformationsdienst bezeichnet) informiert über *Schwachstellen* (Sicherheitslücken, Bugs) in IT-Produkten. Sie informieren dabei auch über das damit möglicherweise verbundene *Risiko* und geben Hinweise, wie die Schwachstelle ausgenutzt werden

kann (Angriffsszenario) und welche Abhilfe- oder Schutzmaßnahmen zur Verfügung stehen (zum Beispiel *Patching*). Entsprechende **CERT-Meldungen (CERT advisories)** werden über Mailinglisten (Newsletter, Rundschreiben) verteilt oder können bei entsprechenden Dienstleistern abonniert werden, die die Meldungen in einer Datenbank über das Internet bereitstellen.

Die Informationen stammen überwiegend von Herstellern, wobei die Schwachstellen durch *Konstruktionsprüfungen (design reviews)*, durch *Penetrationstests* oder durch Beobachtung und Analyse wirklicher Angriffe (siehe *Security Information and Event Management, SIEM,* bzw. die Tätigkeit eines *Security Operations Centers*, *SOC*) entdeckt werden.

Es ist gängige Praxis, entdeckte Schwachstellen zunächst an den Hersteller des Produktes zu melden, so dass dieser dem nachgehen und eine weiter qualifizierte Meldung herausgeben kann. Geschieht dies nicht so schnell wie erwartet, so tauchen die Informationen vorher als Warnung bei Online-Nachrichtendiensten oder an anderer Stelle im Internet auf.

Schwachstelle, allgemein (vulnerability, general)

Schwachstellen (oder Sicherheitslücken) weisen auf das Fehlen oder eine Unzulänglichkeit von *Sicherheitsmaßnahmen* (*security measures/controls*) hin. Unzulänglich sind *Sicherheitsmaßnahmen*, wenn sie nicht zweckdienlich sind (Mangel an *Eignung*, d.h., sie wirken nicht der identifizierten *Bedrohung* entgegen bzw. können umgangen werden) oder wenn sie nicht stark genug sind (Mangel an *Stärke*, d.h., sie können überwunden werden). *Sicherheitsmaßnahmen* als Ganzes sind unzulänglich, wenn sie sich nicht ausreichend gegenseitig unterstützen und somit kein sicheres, integriertes Ganzes bilden (Mangel am *Zusammenwirken*). Diese Mängel können konzeptioneller Natur sein, aber auch dadurch entstehen, dass die Konzepte nicht korrekt umgesetzt werden (→*Korrektheit*).

Technische Schwachstellen sind Lücken in Produkten, Systemen und dergleichen, die ein *Risiko* bedeuten bzw. zu einer Verletzung einer *Sicherheitsrichtlinie (security policy*) führen können, wenn sie ausgenutzt werden.

In gleicher Weise sollten Mängel an prozessualen und organisatorischen Sicherheitsmaßnahmen ebenfalls als Schwachstellen angesehen und entsprechend behandelt werden.[26]

Weicht die Implementierung von den Sicherheitsstandards des Unternehmens ab, so kann dies als Schwachstelle angesehen werden, weil die Standards ja

[26] Würde das Fehlen oder eine Unzulänglichkeit dieser Sicherheitsmaßnahmen nicht zu einem Risiko führen, so könnte man vermutlich auf ihre Implementierung verzichten. Allerdings sind die Wirkungen oft indirekt (vermittelt) und für die Ermittlung des Risikos müsste man eine eher abstrakte Bedrohung ansetzen.

Sicherheitsmaßnahmen definieren, die geeignet und stark sind und sich gegenseitig unterstützen.

Schwachstelle, technisch (vulnerability, technical)

Hierbei handelt es sich um Lücken in Produkten, Systemen und dergleichen, die zu *Risiken* bzw. einer Verletzung der *Sicherheitsrichtlinie (security policy)* führen können, wenn sie ausgenutzt werden. Technische Schwachstellen entstehen durch Mängel der Software, Fehlkonfigurationen oder allgemeine und architektonische Fehler in der Konzeption. Übliche Abhilfemaßnahmen sind *patches* (mit denen Software-Mängel beseitigt werden) sowie Konfigurationsänderungen (Entfernen oder Austauschen von Geräten, Ändern von Geräteeinstellungen).

Schwachstellen können aber auch durch unerwartete Veränderungen der Nutzung, durch Änderungen der Betriebsumgebung oder durch technologischen Fortschritt entstehen. Beispielsweise können kryptografische Algorithmen nicht mehr als sicher gelten, weil inzwischen höhere Rechenkapazitäten zur Verfügung stehen, die genutzt werden können, um sie zu brechen.

Schwachstellenbewertung (vulnerability assessment)

Die Schwachstellenbewertung setzt voraus, dass vorher *Schwachstellen (vulnerabilities*) identifiziert wurden. Diese Informationen können zum Beispiel über Benachrichtigungsdienste zu Sicherheitslücken (*CERT-Informationsdienste*) sowie Release-Hinweise von Herstellern, andere Nachrichtenquellen oder Ergebnisse aus *Sicherheitsprüfungen (security testing)* eingeholt werden. Letztere umfassen dabei ein Integritäts-Scanning, die Ermittlung von Abweichungen sowie automatisierte oder manuelle Penetrationstests.

Zur Schwachstellenbewertung gehören die Ermittlung der Ursachen, die Analyse der Auswirkungen und die Planung der *Risikobehandlung* (speziell der Risikominderung). Letztere umfasst Vorschläge für Abhilfemaßnahmen und die Beurteilung der geplanten und erzielten Ergebnisse.

Sicherheitsaufzeichnung (security record)

Eine Sicherheitsaufzeichnung ist ein Dokument in beliebigem Format, das Aktivitäten nachweist. Diese Aktivitäten können den Betrieb und die Nutzung von IT oder die Intervention durch Menschen betreffen. Die Sicherheitsaufzeichnung kann die Aktivität selbst oder ihr Ergebnis betreffen.[27]

Automatisch generierte Aufzeichnungen werden auch als Protokolldaten bezeichnet (→*Protokollierung*, Logging). Werden die Systemaktivitäten chronologisch aufgezeichnet, werden die Aufzeichnungen auch Auditdaten, Audit-Protokolle oder Audit-Trails genannt.

---

[27] NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations; April 2013 (updated 2015), Rev. 4

Sicherheitsbericht (security report)

Ein Sicherheitsbericht wird im Gegensatz zu einem Nachweis (wie einer *Sicherheitsaufzeichnung*) nur infolge einer gezielten Beauftragung erstellt (gegebenenfalls auch periodisch). Ein Sicherheitsbericht wird oft als Nachweis über einen geleisteten Service oder dessen Qualität erzeugt. In diesem Fall wird er oft für Dritte erstellt, also für Beteiligte außerhalb der Abteilung oder des Bereichs, in der der Bericht generiert wurde. Kern von Sicherheitsberichten sind Elemente wie Bedrohungssituation, (abgewehrte) Angriffe, *Sicherheitsvorfälle* und die Bearbeitung von *Schwachstellen*. Dadurch liefern sie ein Lagebild.

Die Sicherheitsberichterstattung ist der Kommunikationsprozess mit Auftraggebern und anderen Interessengruppen auf der Basis von Sicherheitsberichten. Ein Sicherheitsbericht wird auch für interne Zwecke erstellt. Hier soll er primär auf Fehler und Verbesserungsmöglichkeiten hinweisen.

Sicherheitsereignis (security event)

Sicherheitsereignisse sind sicherheitsbezogene oder sicherheitsrelevante Vorkommnisse, die durch einen Protokolleintrag, einen Alarm oder eine sonstige erfasste Beobachtung offenbar werden. Ein Sicherheitsereignis gilt in seiner Auswirkung als „neutral" bzw. als noch nicht bewertet. Es kann für eine kritische Sicherheitsverletzung oder auch nur für eine autorisierte Nutzung der IT stehen.

Sicherheitsvorfall (security incident)

Sicherheitsvorfälle sind *Sicherheitsereignisse (security events)*, die gegen eine *Sicherheitsrichtlinie (security policy)* verstoßen und ein Eingreifen erfordern, das über üblicherweise automatisierte Abhilfemaßnahmen hinausgeht. Sicherheitsvorfälle berücksichtigen auch das Eintreten einer unmittelbaren Gefahr der Verletzung einer Sicherheitsrichtlinie.

Ein Sicherheitsvorfall kann durch die Ausnutzung einer technischen *Schwachstelle (vulnerability)* oder einer sonstigen Schwachstelle bei der Organisation bzw. in Prozessen verursacht werden; er kann die Folge menschlichen Versagens oder Fehlverhaltens oder einer Kombination aus beidem sein. Bei IT-Sicherheitsvorfällen handelt es sich um Sicherheitsvorfälle, die sich auf die IT (und damit die IT-Services und/oder die verarbeiteten Daten) auswirken.

Reaktion auf einen Sicherheitsvorfall (security incident response)

Die Reaktion auf einen *Sicherheitsvorfall* umfasst die Benachrichtigung der betroffenen Anwender und anderer Gruppen sowie Maßnahmen, die zur Minimierung von Verlusten, Schäden, Systemausfällen oder anderen Auswirkungen auf die Geschäftstätigkeit dienen.

Oft wird im Rahmen der Behandlung eines Sicherheitsvorfalls nur eine provisorische Lösung („workaround") gefunden und deren Implementierung initiiert.

Allerdings werden durch diese Änderung der IT (→*Change Management*) nur die aktuellen Auswirkungen (Schäden) verringert. Um eine Wiederholung zu verhindern bzw. die Wahrscheinlichkeit für das erneute Auftreten zu verringern, müssen die eigentliche Ursache (root cause) gefunden (→*Problem Management*) und geeignete Abhilfemaßnahmen implementiert werden.

Forensik, forensische Analyse (forensics, forensic analyzes)

Bei der forensischen Analyse werden Ereignisse (speziell Sicherheitsereignisse) aus der Vergangenheit rekonstruiert, um deren Ursache zu ermitteln. Dazu werden Spuren analysiert, die während des Ereignisses erzeugt oder aufgezeichnet wurden. Die forensische Analyse erfolgt grundsätzlich ohne Änderungen an Systemen und Daten, die vom Ereignis betroffen sind oder während des Ereignisses genutzt wurden. Mithilfe der forensischen Analyse sollen Nachweise und Daten zur *Verantwortlichkeit (accountability* bzw. zum Verursacher gewonnen werden.

2.2.2 Tätigkeitsbereiche und weitere Themen

Die Aufgaben des Sicherheitsmanagements und die Themen, mit denen sich die beauftragten Abteilungen beschäftigen, sind vielfältig und daher oft unübersichtlich und schwer zu verstehen. Zudem haben gerade große Organisationen das Sicherheitsmanagement unterschiedlich organisiert und die einzelnen Aufgaben und Verantwortlichkeiten verschiedenartig zugeordnet.

Abb. 6 zeigt Beispiele für Tätigkeitsbereiche und weitere Themen für das Sicherheitsmanagement. Sie sind entlang von *Governance, Risk and Compliance (GRC)* angeordnet. GRC entstand und verbreitete sich in den frühen 2000er Jahren als Reaktion auf den Bedarf nach besserer interner Kontrolle und Steuerung, der durch Skandale wie den Bilanzfälschungen beim Energiekonzern Enron und deren Folgen entstanden war (Insolvenz von Enron und Untergang von Arthur Andersen, einer der damals fünf größten Wirtschaftsprüfungsgesellschaften). Ein anderes Ergebnis waren verschärfte gesetzliche Bestimmungen wie der bekannte „U.S. Sarbanes Oxley Act of 2002“, besser bekannt als SOX.

GRC definiert Handlungsebenen für die korrekte Unternehmensführung, denen, wie erwähnt, Tätigkeitsbereiche, Instrumente bzw. weitere Themen für das Sicherheitsmanagement zugeordnet werden. Bei weitem nicht alle sind dabei der IT-Sicherheit zuzurechnen. Das ist ein Grund dafür, dass sich die Lösungen der Organisationen mitunter unterscheiden. Je nach der Bedeutung der Informationstechnologie für die Organisation erscheint die IT-Sicherheit als eigener großer Bereich oder wird zum Beispiel vielleicht nur als Teilaufgabe der IT-Abteilung angesehen. Bei einem *IT-Dienstleister* ist die IT und damit die IT-Sicherheit jedoch Teil des Kerngeschäfts, so dass die IT-Sicherheit wiederum anders organisiert sein kann als bei einem Anwenderunternehmen (→auch: *Anwenderorganisation*). Die Bandbreite ist groß.

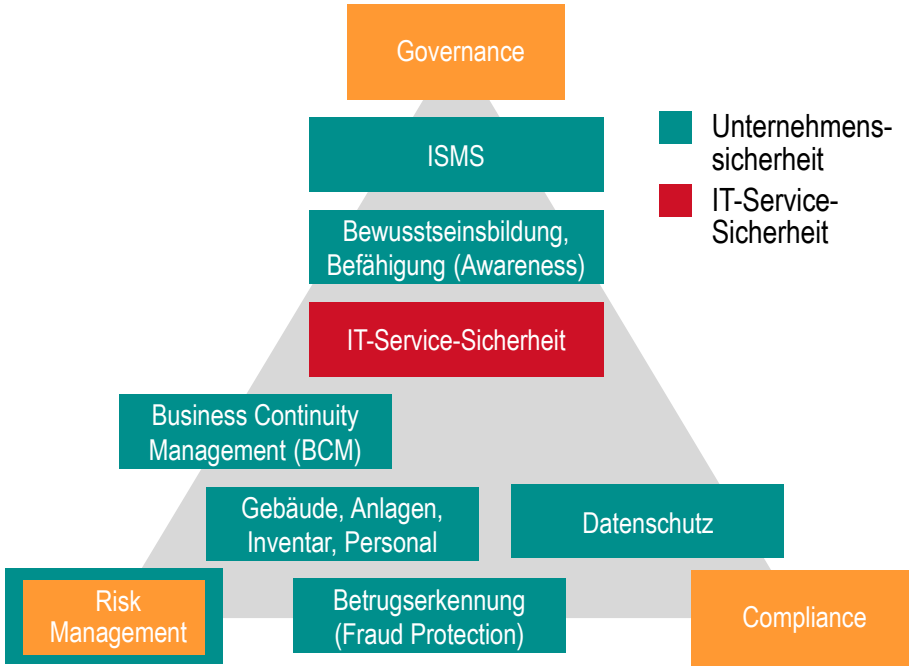


Abb. 6: Tätigkeitsbereiche und weitere Themen für das Sicherheitsmanagement

Abb. 6 zeigt einige Themen oder Arbeitsbereiche, die es auch geben würde, wenn gar keine Informationstechnologie zum Einsatz käme. Sie sind der „Unternehmenssicherheit (Corporate Security)" zugeordnet. Gerade bei größeren Organisationen ist es zu empfehlen, die „IT-Sicherheit" bzw. die „IT-Service-Sicherheit" als eigenständige Disziplin zu behandeln. Die hierbei notwendigen *Kompetenzen/Fähigkeiten*, *Reifegradmodelle*, *Verfahren* und *Prozesse* sind viel zu verschieden. (Diese Begriffe werden am Ende des Kapitels erklärt.) Bei IT-Dienstleistern ist die IT-Service-Sicherheit Teil der Produktsicherheit und genießt damit einen besonderen Stellenwert.[28]

Arbeitsbereiche, Themen

Governance, Risk and Compliance (GRC)

GRC (Governance, Risk and Compliance) bestimmt drei wichtige Aufgabengebiete: 1) **Governance** bedeutet, ein System zur effektiven Führung und Kontrolle etabliert zu haben, das Richtlinien und Methoden für die Kontrolle (im Sinne von Steuerung und Prüfung) ebenso umfasst wie die Einrichtung einer

[28] Zum Thema Unternehmens- versus Produktsicherheit siehe: Eberhard von Faber and Wolfgang Behnsen: Secure ICT Service Provisioning for Cloud, Mobile and Beyond (ESARIS: The Answer to the Demands of Industrialized IT Production Balancing Between Buyers and Providers); Springer Vieweg, Wiesbaden 2017, 383 pages, 159 figures, ISBN 978-3-658-16481-2, 2nd updated and extended Edition, https://doi.org/10.1007/978-3-658-16482-9; Kapitel 2.2 (Seite 30-32)

Unternehmensorganisation und passender Unternehmensprozesse. 2) Ein umfassendes **Risikomanagement** beinhaltet die Identifikation und Bewertung von Risiken für die Unternehmung einschließlich Ableitung und Vollzug adäquater Reaktionen und der abschließenden Umsetzungs- und Erfolgskontrolle. 3) Beim Thema *Compliance* schließlich geht es um die Einhaltung interner und externer Normen, Vorgaben und sonstiger Anforderungen zum Beispiel aus Verträgen. Compliance beinhaltet die Identifikation und Durchsetzung von Richtlinien, Gesetzen, vertraglichen Anforderungen usw. sowie die Kontrolle ihrer Einhaltung.

Übereinstimmung, Compliance

Im geschäftlichen Umfeld hat sich der englische Begriff eingebürgert. Auf technischer Ebene sind auch die Begriffe Übereinstimmung und Konformität (conformity) gebräuchlich.

a) Im Unternehmenskontext versteht man unter Compliance die Einhaltung interner und externer Normen, Vorgaben und sonstiger Anforderungen zum Beispiel aus Verträgen. Compliance beinhaltet die Identifikation und Durchsetzung von Richtlinien, Gesetzen, vertraglichen Anforderungen usw. sowie die Kontrolle ihrer Einhaltung.

b) Für Organisationen oder für ihre Mitarbeiter bedeutet Compliance, dass sie in Übereinstimmung mit bestimmten, festgelegten Standards handeln. Dies wird für gewöhnlich durch die Definition von Prozessen und Verfahren erreicht, die in der Praxis angewandt werden.

c) Eine physische Entität erfüllt die Compliance- oder **Konformitäts**-Anforderungen (conformity), wenn ihre Eigenschaften mit den vordefinierten Merkmalen oder Eigenschaften übereinstimmen oder wenn sie über eine vordefinierte Qualität oder vordefinierte Attribute verfügt. Eigenschaft kann hierbei auch bedeuten, in einer vordefinierten Art und Weise konstruiert zu sein.

Informationssicherheits-Managementsystem (ISMS) (Information Security Management System)

Ein Informationssicherheits-Managementsystem (ISMS) ist ein Modell, mit dessen Hilfe ein Unternehmen angemessen mit der Informationssicherheit umgehen kann. Es umfasst Richtlinien, Verfahren und Leitfäden und wird verwendet, um die allgemeine Informationssicherheit eines Unternehmens zu etablieren, zu überwachen und zu verbessern. Ein ISMS ist ein Handlungs-, Steuerungs- und Managementrahmen. Ein ISMS umfasst im Gegensatz zu einer *Sicherheitsarchitektur* nicht die spezifischen Sicherheitsmaßnahmen, mit denen ein angemessenes IT-Sicherheitsniveau erreicht wird.

Anforderungen an ein ISMS definiert ISO/IEC 27001.[29] Die konkrete Umsetzung und Ausgestaltung obliegt der jeweiligen Organisation. Viele Organisationen streben eine *Zertifizierung* ihres ISMS an. Die Institutionen (certification bodies), die solche Zertifizierungen anbieten und die dafür notwendigen *Audit*ierungen durchführen, müssen die Anforderungen von ISO/IEC 27006 erfüllen[30], die wiederum ISO/IEC 17021 verfeinert.[31]

Bewusstseinsbildung (awareness)

Weiterbildungs- und Schulungsmaßnahmen, Informationsangebote und andere Maßnahmen, die darauf abzielen, dass Mitarbeiter und Mitarbeiterinnen Situationen sowie die Auswirkungen von Handlungen bzw. deren Ausbleiben besser verstehen und befähigt und motiviert werden, in bestimmter Art und Weise zu agieren.

In der IT-Sicherheit besteht die Herausforderung, dass die Zusammenhänge häufig sehr abstrakt sind und dass Ursache-Wirkungsketten zu verstehen, technisches Wissen oder Einfühlungsvermögen erfordert.

Business Continuity Management (BCM)

Das Business Continuity Management (BCM) bzw. betriebliche Kontinuitätsmanagement steht im Zusammenhang mit *Verfügbarkeit (availability)*. Business Continuity Management (BCM) umfasst Vorkehrungen für die Minimierung von Auswirkungen als Folge von Unfällen, Pandemien usw. sowie dem Ausfall von Personal, Gebäudetechnik, Informationstechnologie usw.

Bezieht sich das BCM mehr auf den Ausfall von IT bzw. IT-Services, so ist auch der Begriff **IT Service Continuity Management (ITSCM)** gebräuchlich. Hier geht es um Vorkehrungen für die Minimierung von Auswirkungen als Folge von Ausfällen von IT-Services oder dem Verlust geschäftskritischer Daten und für die rechtzeitige und vollständige Wiederherstellung von IT-Services und Daten. Es gibt dazu zwei Standards, die Anforderungen definieren und Leitlinien enthalten.[32]

---

[29] ISO/IEC 27001 – Information technology – Security techniques – Information security management systems – Requirements; 2013

[30] ISO/IEC 27006 – Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

[31] ISO/IEC 17021 – Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements; 2015; Deutsch und Englisch verfügbar

[32] ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements (ersetzt BS 25999-1:2006 seit 2012); und ISO 22313:2020 Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301 (ersetzt BS 25999-2:2007 seit 2012)

Datenschutz (privacy)

Datenschutz ist ein interdisziplinäres Tätigkeitsfeld, das sich mit dem Schutz personenbezogener Daten beschäftigt. Unter **personenbezogenen Daten** fallen alle Informationen bzw. Angaben, die einer natürlichen Person zugeordnet sind und die sie durch ihre Verarbeitung identifizierbar machen kann.[33] Die technischen und organisatorischen Maßnahmen (TOM) des Datenschutzes haben ähnlich wie die Sicherheitsmaßnahmen der IT-Sicherheit das Ziel, die Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu gewährleisten. Dies soll durch Prinzipien wie „Data Protection by Design" (Berücksichtigung des Datenschutzes schon bei der Entwicklung) und „Data Protection by Default" (datenschutzfreundliche Voreinstellungen in Anwendungen) erreicht werden.

Der Datenschutz definiert Rechte für die Betroffenen (wie zum Beispiel zur Übertragung von Daten zu einem anderen Anbieter, Auskunftspflicht, Löschung). Der Datenschutz umfasst vor allem auch rechtliche Regelungen (Einwilligung, Verträge zur *Auftragsdatenverarbeitung, ADV*, usw.) sowie prozessuale Vorgaben (Meldeplichten).

Betrugserkennung (fraud protection)

Im engeren Sinne die Entwicklung, Implementierung und Nutzung von Maßnahmen, die sicherstellen sollen, dass unberechtigte Nutzung, Täuschung und Erschleichung von Rechten, Identitätsdiebstahl usw. verhindert oder zumindest erkannt werden können. Oft sind entsprechende Maßnahmen in den IT-Anwendungen oder IT-Systemen integriert. Dabei gibt es auch Verbindungen zu Maßnahmen, wie sie in der IT-Sicherheit verwendet werden. Bestimmte Maßnahmen der IT-Sicherheit helfen direkt dabei, Betrug zu verhindern und zu erkennen.

Unterbau, Voraussetzungen

Kompetenz, Fähigkeit (capability)

Kompetenzen ermöglichen es Organisationen oder ihren Mitarbeitern, zu erwartende Situationen zu meistern und ihre Kompetenzen schrittweise zu verbessern. Kompetenzen beziehen sich für gewöhnlich auf einen einzelnen, abgegrenzten Bereich. Kompetenzen können bestimmt werden; ihre Qualität ist messbar, zum Beispiel durch Betrachtung der Art und Weise, wie das Ergebnis erreicht wurde und wie sich dies gegenüber einer Zielgruppe belegen lässt. Siehe auch →*Reifegrad*.

Reifegrad (maturity)

Reifegrad bezieht sich auf die Art und Weise, wie bestimmte Situationen gemeistert bzw. definierte *Prozesse (processes)* und *Verfahren (procedures)* ange-

[33] Art. 4, Abs. 1 DSGVO (Datenschutzgrundverordnung)

wandt werden. Reifegrad ist dabei ein Qualitätsmerkmal, das zum Beispiel Selbständigkeit, Erfolg und Effizienz im Auge hat. Der Reifegrad erlaubt die Prognose allgemeiner Ergebnisse anstehender oder zukünftiger Projekte, Maßnahmen usw. Dies erfordert eine Messung des Reifegrads. Der Reifegrad bezieht sich normalerweise auf mehrere Bereiche.

ISO/IEC 21827 beschreibt ein **Reifegradmodell**,[34] das als „Systems Engineering – Capability Maturity Model© (SSE-CMM©)" bezeichnet wird. Es betrachtet auf der einen Seite grundlegende Methoden oder Verfahren (base practices) innerhalb von Bereichen (domains) und auf der anderen Seite allgemeingültige oder übergreifende Methoden oder Verfahren (generic practices), welche die Dimensionen der *Fähigkeiten (capabilities)* bilden. Beide werden zueinander in Beziehung gesetzt, um zu zeigen, ob eine Organisation dazu in der Lage ist, etwas in einem bestimmten Bereich (domain) zu tun. Die Messung erfolgt durch Bewertung, ob und in welchem Ausmaß vordefinierte Methoden oder Verfahren existieren und zur Anwendung kommen. Dies kann für Metriken der IT-Sicherheit eingesetzt werden.[35]

Verfahren (procedure)

Ein Verfahren ist eine spezifische und für gewöhnlich vorgeschriebene Art und Weise, einen *Prozess* oder Teile davon auszuführen.

Prozess (process)

Ein Prozess ist eine Reihe von aufeinanderfolgenden oder zusammenhängenden Aktivitäten, die einem gemeinsamen, übergeordneten Ziel dienen bzw. einen gemeinsamen Zweck verfolgen.

2.2.3 Sicherheitsprinzipien

Es gibt viele Prinzipien, die Hilfestellungen für die Entwicklung und Implementierung von Sicherheitsmaßnahmen bzw. für die Absicherung von IT-Systemen geben. Manche davon sind schon recht alt und in Vergessenheit geraten, obwohl sie auch heute noch wertvolle Dienste leisten können. Andere sind relativ neu und sollen auf die Besonderheiten im Cyberraum hinweisen. Abb. 7 zeigt eine Auswahl. Die einzelnen Begriffe werden im Folgenden erläutert.

---

[34] ISO/IEC 21827 – Information Technology – Systems Security Engineering – Capability Maturity Model© (SSE-CMM©); 2008

[35] Eberhard von Faber und Wolfgang Behnsen: Joint Security Management: organisationsübergreifend handeln (Mehr Sicherheit im Zeitalter von Cloud-Computing, IT-Dienstleistungen und industrialisierter IT-Produktion); Springer Vieweg, Wiesbaden 2018, 244 Seiten, 60 farbige Abbildungen, ISBN 978-3-658-20833-2; https://doi.org/10.1007/978-3-658-20834-9; Kapitel 9.3 (Seite 199-201)

Abb. 7: Auswahl an Sicherheitsprinzipien

Design-Prinzipien (Saltzer und Schroeder)

Die Arbeit von Saltzer und Schroeder aus dem Jahr 1975[36] enthält unter anderem acht fundamentale Prinzipien oder Regeln für den Entwurf und die Entwicklung von abwehrenden Sicherheitsmaßnahmen.

1. Sparsamkeit der Mechanismen (economy of mechanism) fordert, den Entwurf möglichst klein und einfach zu halten. Dies ist notwendig, damit eine Überprüfung der Sicherheitsfunktionen erfolgreich durchgeführt und Fehler gefunden werden können. Vergleiche →*Secure by Default*.

2. Sichere Voreinstellungen (fail-safe defaults): Die Grundeinstellung sollte sein, dass alle Zugriffe verboten sind. Das System prüft die Bedingungen, unter denen Zugriffe erlaubt werden und gibt diese dann frei. Die umgekehrte Vorgehensweise wird nicht empfohlen. Siehe →*Security by Default* (nicht: Secure by default).

3. Vollständige Vermittlung (complete mediation): Bei der Implementierung der Zugriffskontrolle ist darauf zu achten, dass die Quelle der Anforderung stets unzweifelhaft festgestellt werden kann und die Gültigkeit vorangegangener Prüfungen von Zugriffsrechten unbedingt sichergestellt sein muss.

---

[36] Saltzer und Schroeder: The Protection of Information in Computer Systems; Fourth ACM Symposium on Operating System Principles (October 1973), Revised version in Communications of the ACM 17, 7 (July 1974); revised April 17, 1975

4. Offenes Design (open design): Die Wirksamkeit von Sicherheitsmechanismen sollte nicht darauf beruhen, dass ihre Konstruktion geheim ist. Es kann nämlich nicht davon ausgegangen werden, dass die Konstruktion geheim bleibt. Außerdem erschwert eine Geheimhaltung der Konstruktion die Überprüfung.[37]

5. Aufteilung von Rechten (separation of privilege): Im weiteren Sinne bedeutet dieses Prinzip, falls möglich zwei Sicherheitsmechanismen zu nutzen statt nur einem. Die Begründung, die sich mehr auf Zugriffskontrolle bezieht, verweist darauf, dass das System dann weniger anfällig für Irrtümer, Fehler, Betrug und Vertrauensbruch ist.

Hinweis: Nicht wirklich in der Originalarbeit enthalten, aber in diesem Zusammenhang wichtig zu erwähnen, ist das wortähnliche Prinzip **Segregation of duties** oder **Separation of duties**. Es besagt, dass ein Nutzer in einem Kontext oder Aufgabenbereich nicht mehr als eine Rolle bekleiden bzw. eine Art von Verantwortlichkeit haben soll. Dadurch werden zum Beispiel Durchführung und Kontrolle personell getrennt.

Hinweis: Das Prinzip, zwei Sicherheitsmechanismen zu nutzen statt nur einem, ist allgemein als **Staffelung von Sicherheitsmaßnahmen** oder **Defense in depth** bekannt. Es bedeutet, dass Sicherheitsmechanismen in verschiedenen Ebenen angeordnet und hintereinandergeschaltet werden sollten. Versagt ein Mechanismus oder wird er überwunden, bietet der darauffolgende immer noch Schutz. Dies ist ein typisches Beispiel für das →*Zusammenwirken*.

6. **Minimale Rechte (least privilege)**: Programme und Nutzer sollten nur die Rechte haben, die sie für die Erfüllung der Aufgabe unbedingt benötigen. Das reduziert den Schaden im Fehlerfall und verringert die Anzahl der Interaktionen im System, so dass es unwahrscheinlicher wird, dass Rechte unabsichtlich, ungewollt oder fälschlich ausgeübt werden.

7. Minimierung gemeinsamer Mechanismen (least common mechanism) fordert, die Anzahl der Mechanismen zu minimieren, die für viele Nutzer angewendet werden.

8. Mentale Akzeptanz (psychological acceptability): *Benutzerfreundlichkeit*. Oberflächen von Programmen sollten so gestaltet sein, dass Nutzer die Sicherheitsmechanismen routinemäßig und automatisch richtig anwenden.

Security Development Lifecycle (SDL)

Der „Security Development Lifecycle (SDL)" erweitert bzw. modifiziert den Entwicklungsprozess für Software durch den Einsatz von Maßnahmen, die die

---

[37] Anmerkung des Autors: Dies bedeutet nicht, dass alle Konstruktionsdetails uneingeschränkt offengelegt werden müssen. Die Nichtverfügbarkeit solcher Informationen vergrößert durchaus den Aufwand für einen Angreifer (der sich diese zum Beispiel erst durch Reverse-Engineering erschließen muss) und damit das erreichte Sicherheitsniveau.

Sicherheit entscheidend verbessern. Der Prozess besteht aus 12 Stufen, die sich bei jeder Entwicklung wiederholen, plus einer Nullten Stufe (Education and Awareness), welche grundsätzlicher Natur ist. Der Prozess enthält eine Reihe von Praktiken, durchzuführenden Aktivitäten, Tipps, Verboten und Kontrollpunkten. Dazu gehört auch eine abschließende Sicherheitsüberprüfung (Final Security Review, FSR).[38]

Der SDL wurde von Microsoft entwickelt, eingeführt und genutzt. Als zugrunde liegende Prinzipien werden „Secure by Design", „Secure by Default", „Secure in Deployment" und "Communications" genannt.[39]

1. *Secure by Design* bedeutet, dass Software so konzipiert, entwickelt und implementiert sein soll, dass sie sich selbst schützt sowie die Daten, die sie verarbeitet.

2. *Secure by Default* besagt, dass die Software eine minimale Angriffsfläche bieten soll, um die Schwere eines Programmierfehlers zu begrenzen. Standard- bzw. Voreinstellungen einer Software sollten so gewählt sein, dass bei der Ausnutzung möglicher Softwarefehler der Schaden begrenzt bleibt.

3. **Secure in Deployment** fordert, dass zu einem Softwareprodukt Werkzeuge und Handbücher gehören, die es den Nutzern und Administratoren ermöglichen, sie sicher zu nutzen. Außerdem sollen Softwareaktualisierungen leicht zu implementieren sein.

4. **Communications** besagt, dass Softwareentwickler darauf vorbereitet sein sollen, dass Schwachstellen aufgedeckt werden. Sie sollten offen kommunizieren und Anwendern helfen, Abhilfemaßnahmen oder Provisorien zu implementieren.[40]

Hinweis: Man findet zum Beispiel auch den Begriff Secure Software Development Lifecycle (SSDL)[41] und andere Abkürzungen wie Secure SDLC oder SDLC. Dabei handelt es sich meist um Erweiterungen eines Software-Entwicklungsmodells, die jedoch nicht so detailliert ausgearbeitet zu sein scheinen, wie der Security Development Lifecycle (SDL) von Microsoft.

---

38 Michael Howard and Steve Lipner: The Security Development Lifecycle, SDL: A Process for Developing Demonstrably More Secure Software; Microsoft Press, Redmond, 2006, 343 Seiten, ISBN 978-07356-2214-2

39 Steve Lipner and Michael Howard: The Trustworthy Computing Security Development Lifecycle; März 2005, aktualisierte Version des gleichnamigen Artikels präsentiert auf der Annual Computer Security Applications Conference, Dezember 2004, https://docs.microsoft.com/en-us/previous-versions/ms995349(v=msdn.10)?redirectedfrom=MSDN; zuletzt aufgerufen am 21.01.2021

40 vgl. ebenda.

41 Noopur Davis: Secure Software Development Life Cycle Processes; Carnegie Mellon University, 2006

Secure by Design

„Secure by Design" ist eines der vier Grundprinzipien des *Security Development Lifecycle (SDL)*" und bedeutet, dass Software so konzipiert, entwickelt und implementiert sein soll, dass sie sich selbst schützt sowie die Daten, die sie verarbeitet.

Geläufig ist der Begriff **Security by Design**, der so verstanden wird, dass die Sicherheit bereits ganz am Anfang des Entwicklungsprozesses Teil der Anforderungen sein muss. Nur dann werden die Sicherheitsmaßnahmen wirklich umgesetzt, und nur dann wird die Sicherheit ein integraler Bestandteil des Produktes oder Systems werden können.

Secure by Default

„Secure by Default" ist eines der vier Grundprinzipien des *Security Development Lifecycle (SDL)*" und besagt, dass die Software eine minimale Angriffsfläche bieten soll, um die Schwere eines Programmierfehlers zu begrenzen. Standard- bzw. Voreinstellungen einer Software sollten so gewählt sein, dass bei der Ausnutzung möglicher Softwarefehler der Schaden begrenzt bleibt.

Geläufig ist der Begriff **Security by Default**, der vor allem auf die Standard- bzw. Voreinstellungen abhebt. Entsprechend sind auch die Begriffe **Privacy by Default** oder **Data Protection by Default** zu verstehen, die das gleiche für den *Datenschutz*, also „datenschutzfreundliche Voreinstellungen" fordern.

Secured by Definition

„Secured by Definition" integriert die Entwicklung, Umsetzung, Kontrolle und Verbesserung aller Maßnahmen zur Absicherung von IT-Systemen und IT-Komponenten in die Bereitstellungs- und Betriebsprozesse der IT entlang des gesamten Lebenszyklus (Plan-Build-Run[42]). Diese Integration von IT-Sicherheitsmanagement und IT-Service-Management betrifft insbesondere auch die Auslieferungs- und Betriebsphasen, was für die Aufrechterhaltung der IT-Sicherheit entscheidend ist. Als Bereitstellungs- und Betriebsprozesse der IT werden die IT-Service-Management-Prozesse zugrundegelegt, wie sie in ITIL®[43] bzw. ISO/IEC 20000[44] definiert sind.

---

[42] eingeführt von debis Systemhaus etwa 1995 als Ausdruck umfassender IT-Dienstleistungen; in den letzten Jahren in der Referenzarchitektur IT4IT auf Plan, Build, Deliver, Run bzw. Plan, Source, Offer, Manage erweitert

[43] IT Infrastructure Library®, eine Sammlung von vordefinierten Prozessen, Aktivitäten und Rollen entlang des Lebenszyklus von IT-Services, wobei die Betriebsphase besonders beachtet wird. Seit 2013 sind ITIL und IT Infrastructure Library eine Marke von Axelos.

[44] ISO/IEC 20000 – Information technology – Service management – Part 1: Service management system requirements, Part 2: Guidance on the application of service management systems; 2012

Der Ansatz „Secured by Definition“ wurde durch die Sicherheitsarchitektur →*ESARIS* eingeführt. ESARIS wurde von T-Systems eingeführt und genutzt. Teile davon wurden durch die Vereinigung „Zero Outage Industry Standard” übernommen und weiterentwickelt.[45]

„Secured by Definition“ betrachtet IT-Sicherheit als eine Qualität. Einer der Leitgedanken des „Total Quality Management (TQM)“ (1951) ist, Qualität zu erzeugen, statt sie später zu kontrollieren.[46] Entsprechend soll sich die IT-Sicherheit auf die Prozesse zur Erzeugung (von Produkten oder Services) konzentrieren und nicht auf Kontrollmaßnahmen eines separaten Sicherheitsprozesses. Das heißt, dass Menschen an jeder Stelle der Wertschöpfungskette vordefinierten Regeln (zur IT-Sicherheit) folgen müssen, die integraler Bestandteil aller IT-Produktionsprozesse sind.[47]

Protect, Detect, Respond bzw.
Prevent, Detect, Respond… oder **Identify, Protect, Detect…**

Bei diesen Leitmotiven handelt es sich um die Aufzählung von Kernfunktionen des IT-Sicherheitsmanagements bzw. eines Vorgehensmodells für die Cybersecurity. Es gibt sie mit drei bis fünf Begriffen, mit leicht unterschiedlichen Begrifflichkeiten und leicht abgewandelten Bedeutungen. Das NIST hat in Form des „Cybersecurity Frameworks“ ab 2015 ein einfaches, aber umfassendes Rahmenwerk veröffentlicht,[48] das zusätzlich „Identify“ einführt, wobei es um die Schaffung von Grundlagen, vor allem Bildung und Aufklärung, geht (also: Identify, Prevent, Detect, Respond, Recover). Die anderen vier Begriffe können wie folgt verstanden werden:

Protect / Prevent: Die wichtigsten bzw. primären Sicherheitsmaßnahmen sind präventiver Natur, das heißt, sie wirken Bedrohungen aktiv und unmittelbar entgegen.[49] Der erste Schritt ist daher „Verhindern“ (prevent) bzw. „Schützen“ (protect), was prinzipiell eine kontinuierliche Kontrolle und Verbesserung einschließt.

---

45 https://zero-outage.com/the-standard/security/; zuletzt aufgerufen am 21.01.2021

46 Phil Cosby, der die von US-Amerikanern in Japan erfolgreich eingeführte Methode in den USA verbreiten half.

47 Eberhard von Faber: Methoden: „Secured by definition“ und die Umsetzung von Prinzipien aus dem Qualitätsmanagement, Durchgängige IT-Sicherheit durch Integration in die IT-Produktionsprozesse; in: Datenschutz und Datensicherheit - DuD, 43(7), Juli 2019, Springer Fachmedien, Wiesbaden 2019, ISSN 1614-0702, pp 410-417; https://doi.org/10.1007/s11623-019-1136-0

48 NIST (National Institute of Standards and Technology): Framework for Improving Critical Infrastructure Cybersecurity; Version 1.1; April 16, 2018; https://www.nist.gov/cyberframework

49 Solche Sicherheitsmaßnahmen wurden weiter oben „Generatoren“ genannt.

Detect: Dadurch, dass viele IT-Systeme heute über das Internet erreichbar sind bzw. dass IT-Services einer Vielzahl von möglichen Nutzern angeboten werden, kommt der Erkennung von *Sicherheitsereignissen* (detect) eine größer werdende Rolle zu, da sie auf Angriffe hindeuten, einen *Sicherheitsvorfall* darstellen und Handlungsbedarf anzeigen können. Der Begriff "detect" lenkt die Aufmerksamkeit auf diesen Teil der IT-Sicherheit.

Respond: Entsprechend muss darauf reagiert werden, zum Beispiel indem schadensminimierende Sofortmaßnahmen ergriffen werden. Um eine Wiederholung des Sicherheitsvorfalls zu verhindern bzw. die Wahrscheinlichkeit für das erneute Auftreten zu verringern, müssen die eigentliche Ursache (root cause) gefunden und geeignete Abhilfemaßnahmen implementiert werden. Siehe auch: *Reaktion auf einen Sicherheitsvorfall* (Security incident response). Der Begriff "respond" weist vor allem darauf hin, dass entsprechende Vorbereitungen (Pläne, Prozesse, Werkzeuge, Ressourcen) nötig sind, die vor dem ersten Vorfall abzuschließen sind. Die Vorbereitungen und die Reaktionen im Falle eines Vorfalls bilden einen eigenständigen Teil des Sicherheitsmanagements.

Recover: Nach einem Sicherheitsvorfall ist es eventuell erforderlich, größere Schäden zu beseitigen. Auch muss der eigentliche Betrieb entsprechend den Vorgaben wiederhergestellt werden. Der Vorfall sollte analysiert werden, um Verbesserungsbedarf identifizieren und Maßnahmen implementieren zu können. Entsprechende Vorbereitungen (Pläne, Prozesse, Werkzeuge, Ressourcen) sind zu treffen.

Zero Trust

Zero Trust bedeutet, dass Nutzer und Geräte als potenziell unsicher bzw. nicht vertrauenswürdig angesehen werden, auch wenn sie sich logisch in einem bestimmten, meist internen Netzwerk befinden.[50] Dies erfordert eine neue Sicherheitsarchitektur, weil die Zulässigkeit des Zugriffs auf Ressourcen im Netzwerk bei jeder einzelnen Anforderung geprüft werden muss. Das schließt die Authentisierung von Nutzern und Geräten sowie die Prüfung weiterer kontextabhängiger Regeln ein.

Gegensatz: Die etablierten Sicherheitsarchitekturen messen dem Schutz der Außenlinie (perimeter) große Bedeutung bei. Entsprechend sind wichtige Sicherheitsmaßnahmen am Übergang vom äußeren, unsicheren Netzwerk zum inneren, als sicher geltenden Netzwerk angeordnet. – Sobald Nutzer und die von ihnen genutzten Geräte Zugang zu einem internen, als sicher angesehenen Netzwerk erhalten haben, erhalten sie ohne weitere Prüfungen Zugriff auf viele Ressourcen, die sich in diesem Netzwerk befinden.

---

[50] Der Begriff Zero Trust wurde von Forrester eingeführt.

2.3 Rahmenwerke und Architekturen

Die Anzahl von Handreichungen, Standards, Zusammenfassungen und Übersichten zum Thema IT-Sicherheit ist nur schwer überschaubar. Es ist sogar meist recht schwierig, diese zu klassifizieren und klar definierten Kategorien zuzuordnen. Zu unterschiedlich sind Gegenstand, Zweck, Zielgruppe, Detailtiefe usw. Hier sind zwei Beispiele solcher Dokumente oder Rahmenwerke:

- "The ISF Standard of Good Practice for Information Security 2018"[51] (ISF SOGP) umfasst die Themen der IT-Sicherheit und gibt praktische und verlässliche Hilfestellungen. Insbesondere enthält er eine Fülle von Sicherheitsmaßnahmen, die in Kategorien und Themen geordnet sind. Zu jedem Thema werden Maßnahmen beschrieben, die wiederum durch „Statements of good practice" verfeinert werden. Das Information Security Forum (ISF) ist eine Organisation, in der überwiegend Anwenderorganisationen vertreten sind, die gemeinsam Verfahren und Standards für die IT-Sicherheit entwickeln.
- Die „Security Guidance for Critical Areas of Focus in Cloud Computing"[52] der Cloud Security Alliance (CSA) ist eine Sammlung von Informationen und Meinungen von über 70 Experten aus der Industrie zum Thema Cloud-Security. Geordnet in 14 Bereichen werden verschiedenste bewährte Verfahren (best practices) beschrieben. Diese werden um praktische Empfehlungen erweitert sowie um Anforderungen, die gemessen und überprüft (auditiert) werden können. Viele Anbieter (IT-Dienstleister, Hersteller usw.) sind Mitglied der Cloud Security Alliance (CSA).

Weitere Institutionen, die solcherlei Dokumente und Rahmenwerke herausgeben, sind:

- NIST (National Institute of Standards and Technology); Bundesbehörde der USA vergleichbar mit der Physikalisch-Technische Bundesanstalt (PTB) in Deutschland bzw. auf dem Gebiet der IT-Sicherheit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI); https://www.nist.gov/ bzw. https://csrc.nist.gov/,
- Bundesamt für Sicherheit in der Informationstechnik (BSI); veröffentlich zum Beispiel die IT-Grundschutz-Kataloge mit Vorgehensweise und Kompendium[53],

---

[51] Information Security Forum (ISF): The ISF Standard of Good Practice for Information Security 2018; https://www.securityforum.org, 338 pages

[52] Cloud Security Alliance (CSA): Security Guidance for Critical Areas of Focus in Cloud Computing; Version 3.0, 2011, 177 pages

[53] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

die BSI-Standards [54] und den Kriterienkatalog Cloud Computing C5 [55]; https://www.bsi.bund.de,

- ENISA (European Network and Information Security Agency); deutsch: Agentur der Europäischen Union für Cybersicherheit; veröffentlicht zu sehr vielen Themen wie der Cloud-Security[56] und der Sicherheit im Internet-der-Dinge[57]; https://www.enisa.europa.eu.

In diesem Kapitel wird es nicht um solche Handreichungen, Standards, Hilfestellungen, Zusammenfassungen, Übersichten und Best Practices gehen, sondern um Strukturen und Verfahren, die im Folgenden als „Architekturen" definiert werden. Auch handelt es sich um eine Auswahl: Abb. 8 zeigt fünf Architekturen (rote Kästchen)[58] im Kontext anderer Entwicklungen entlang eines Zeitstrahls. Der Startpunkt eines Kastens markiert jeweils den etwaigen Beginn der Entwicklung und die Zeit, die die Ausarbeitung wahrscheinlich hauptsächlich in Anspruch genommen hat. Manche Rahmenwerke wurden kontinuierlich weiterentwickelt; auch dann endet der Kasten aus Platzgründen.

---

54 BSI-Standard 200-1: Managementsysteme für Informationssicherheit; BSI-Standard 200-2: IT-Grundschutz-Methodik; BSI-Standard 200-3: Risikomanagement; BSI-Standard 100-4: Notfallmanagement; https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/-ITGrundschutzStandards_node.html; zuletzt aufgerufen am 21.01.2021

55 https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Kriterienkatalog/Kriterienkatalog_Cloud_Computing.html; zuletzt aufgerufen am 21.01.2021

56 European Network and Information Security Agency (ENISA): Cloud Computing Information Assurance Framework; November 2009

57 European Network and Information Security Agency (ENISA): Good Practices for Security of IoT - Secure Software Development Lifecycle; November 2019

58 JSM: Das Joint Security Management erreicht nur bei Verwendung einzelner Methoden der Sicherheitsarchitektur ESARIS die Tiefe und Multi-Dimensionalität, wie sie für Architekturen typisch ist.

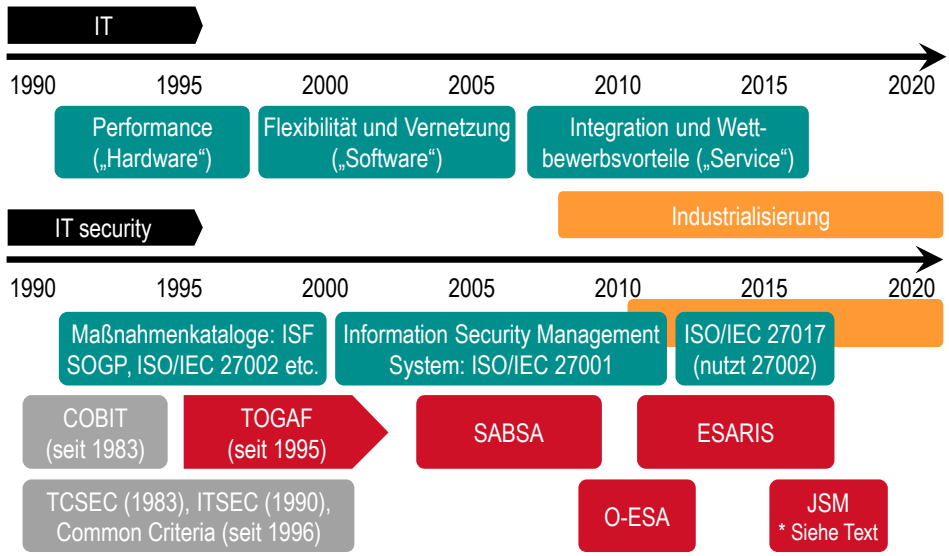


Abb. 8: Zeitstrahl mit fünf Architekturen und weiteren Orientierungspunkten[59]

Der obere Zeitstrahl soll andeuten, wie sich die Informationstechnologie von der Sicht auf die Bereitstellung über die Ausdehnung ihrer Nutzung bis zu IT als Dienstleistung (siehe Kapitel 4) entwickelt hat. Zuletzt hat sich auch die Art der Herstellung noch einmal deutlich geändert (Industrialisierung der IT). All dies hat Einfluss auf die IT-Sicherheit bzw. die Art und Weise, wie die Absicherung der IT zu erfolgen hat. Parallel hat sich die IT-Sicherheit entwickelt (siehe Abb. 8). Einige Standards, die auch heute noch zur Grundausstattung gehören, sind zur zeitlichen Orientierung ebenfalls aufgeführt (blaugrün/petrol bzw. grau).

Die Architekturen in den rot eingefärbten Kästchen werden im Folgenden erläutert. Aufgrund des großen Einflusses wird jedoch zu Anfang das COBIT®-Rahmenwerk vorgestellt. Allerdings gibt es noch zwei weitere Gründe dafür: Erstens ist IT-Sicherheit nur schwerlich möglich, ohne IT-Governance, um die es bei COBIT geht. Zweitens definiert COBIT die Informationssicherheit als eigenen Fokusbereich.

COBIT (Control Objectives for Information and Related Technology)

> COBIT® (es wird fast ausschließlich die Abkürzung benutzt) ist ein IT-Management-Rahmenwerk, das Unternehmen ermöglicht, Informationen und zugehörige Technologien ganzheitlich zu steuern und zu verwalten. COBIT unterstützt bei der Entwicklung, Implementierung und Nutzung eines dazu

[59] vergleiche: Eberhard von Faber and Wolfgang Behnsen: Secure ICT Service Provisioning for Cloud, Mobile and Beyond (ESARIS: The Answer to the Demands of Industrialized IT Production Balancing Between Buyers and Providers); Springer Vieweg, Wiesbaden 2017, pages XIV+369, figures 159, ISBN 978-3-658-16481-2, 2nd updated and extended Edition, https://doi.org/10.1007/978-3-658-16482-9

benötigten Governance-Systems. COBIT fokussiert auf alle Informationen, die ein Unternehmen erzeugt und verarbeitet bzw. verwendet, sowie auf die Technologien (vor allem Informationstechnologie, IT), die es dazu nutzt.

COBIT wurde von ISACA® entwickelt.

COBIT (2019) besteht aus folgenden Teilen bzw. Büchern.

- „Einführung und Methodik" ist der Hauptleitfaden und beschreibt die wesentlichen Konzepte und grundlegenden COBIT-Prinzipien.
- „Governance und Managementziele" beschreibt das COBIT-Kernmodell und enthält die 40 Governance- und Managementziele. Jedes Ziel definiert den Zweck und zeigt die Verbindung mit den Unternehmensprozessen und den übergreifenden Unternehmenszielen.
- Der „Entwurfsleitfaden" liefert eine ausführliche Anleitung für die Entwicklung eines eigenen, auf das Unternehmen zugeschnittenen Governance-Systems.
- Das „Implementierungshandbuch" führt das Unternehmen durch die Implementierung der Governance-Strategie. Es beschreibt bewährte Verfahren (best practices) und zeigt Möglichkeiten, Fallstricke zu vermeiden und dergleichen.[60]

COBIT bietet durch die sogenannten „Focus Areas" die Möglichkeit, das Governance-System auf unterschiedliche Bedürfnisse zuzuschneiden bzw. an diese anzupassen. Ein Fokusbereich beschreibt ein bestimmtes Thema, einen Bereich oder ein Problem.

Einer dieser Fokusbereiche ist „Informationssicherheit". COBIT bietet einen Leitfaden dafür und unterstützt bei der Anwendung von COBIT auf spezifische Informationssicherheitsthemen in einem Unternehmen. Der Leitfaden erweitert den Hauptleitfaden durch sicherheitsspezifische Praktiken und Metriken zur Informationssicherheit.

TOGAF (The Open Group Architecture Framework)

TOGAF® (es wird fast ausschließlich die Abkürzung benutzt) bietet einen umfassenden Ansatz für den Entwurf, die Planung, die Implementierung und die Verwaltung einer Informationsarchitektur für Unternehmen. TOGAF ist ein übergeordneter und ganzheitlicher Ansatz für das Design. Dabei wird typischerweise auf vier Ebenen modelliert: Geschäft, Anwendung, Daten und Technologie. TOGAF setzt auf Modularisierung, Standardisierung und die Nutzung bereits vorhandener, bewährter Technologien und Produkte.

TOGAF 9.2 besteht aus sechs Teilen:

- Part I – Introduction,
- Part II – Architecture Development Method (ADM),

---

60 ISACA, Why COBIT?; https://www.isaca.org/resources/cobit; aufgerufen am 02.02.2021

- Part III – ADM Guidelines and Techniques,
- Part IV – Architecture Content Framework,
- Part V – Enterprise Continuum and Tools und
- Part VI – Architecture Capability Framework.

Sicherheitsarchitektur

Nach einer Definition der Open Group bzw. *TOGAF*® (The Open Group Architecture Framework) ist eine Architektur „eine formale Beschreibung eines Systems oder ein detaillierter Plan des Systems auf Komponentenlevel für seine Implementierung." Alternativ versteht *TOGAF* darunter „die Struktur der Komponenten, ihre Wechselbeziehungen und die Prinzipien und Richtlinien, die das Design und die Entwicklung über die Zeit bestimmen."[61]

Sicherheitsarchitekturen und deren Teilarchitekturen sind Ordnungs- und Organisationsschemata, die einen komplexen Gegenstand in Teilaspekte aufgliedern und Zusammenhänge zwischen diesen aufzeigen (Verbindendes, Trennendes, Wechselwirkungen). Es können sechs Eigenschaften unterschieden werden:[62]

Eine Sicherheitsarchitektur leitet die Aktivitäten zur Absicherung von IT-Services in ganzheitlicher Weise

1. durch die Aufteilung des Fachgebietes in wohl definierte Grundbausteine (Dekomposition) und durch die Beschreibung von Regeln für ihr Zusammenwirken (Integration),
2. durch die Reduktion von Komplexität, die das Verstehen und die Anwendung fördert und erleichtert,
3. durch Hierarchie, weil die Darstellungen auf unterschiedlichen Ebenen der Abstraktion erfolgen und daher verschiedenen Zwecken dienen und zielgruppengerecht verfasst werden können,
4. durch Konsistenz und innere Logik, weil die Teile der Sicherheitsarchitektur widerspruchsfrei ineinandergreifen und sich gegenseitig unterstützen,
5. durch Wiederverwendung, weil durch die Dekomposition Grundbausteine entstehen, die wiederverwendet werden können, um gleiche oder ähnliche Probleme zu lösen,
6. durch Unterstützung der Arbeitsteilung und Spezialisierung.

---

61 Übersetzung des Autors aus den „TOGAF - Frequently Asked Questions"

62 Eberhard von Faber und Wolfgang Behnsen: Joint Security Management: organisationsübergreifend handeln (Mehr Sicherheit im Zeitalter von Cloud-Computing, IT-Dienstleistungen und industrialisierter IT-Produktion); Springer Vieweg, Wiesbaden 2018, 244 Seiten, 60 farbige Abbildungen, ISBN 978-3-658-20833-2; https://doi.org/10.1007/978-3-658-20834-9; Kapitel 2.2 (S. 24-28)

Enterprise Security Architecture (ESA)

Eine Enterprise Security Architecture (ESA) ist ein streng strukturierter Ansatz, mit dem in einem Unternehmen ein angemessenes Sicherheitsniveau (informations- oder IT-bezogen) erreicht werden soll. Die Sicherheitsarchitektur definiert und umfasst Elemente (zum Beispiel Methoden und Sicherheitsmaßnahmen), deren Beziehungen (zum Beispiel Schnittstellen, Interaktionen und Abhängigkeiten) und eine Taxonomie mit einer klaren Struktur und einem Ordnungsschema (zum Beispiel Hierarchien, Organisation, Konventionen). Die Sicherheitsarchitektur ordnet alle anzuwendenden Sicherheitsmaßnahmen (organisatorische, prozessbezogene und technische). Der Begriff deckt sich mit dem Begriff Enterprise Information Security Architecture (EISA), da in dieser Definition der Schwerpunkt auf der Minimierung von IT- oder informationsrelevanten Risiken liegt.

ESARIS (Enterprise Security Architecture for Reliable ICT Services)

Die Enterprise Security Architecture for Reliable ICT Services (ESARIS) ist eine Sicherheitsarchitektur speziell für Anbieter von ICT/IT-Services. Sie verfolgt den Zweck, den Kunden IT-Services mit einem angemessenen Sicherheitsniveau bereitstellen zu können, die dessen Anforderungen erfüllen. ESARIS reduziert Risiken für Kunden und den Anbieter selbst. Die Sicherheitsarchitektur vermittelt zwischen Anwender und Anbieter ebenso wie zwischen Anbieter und Zulieferern. ESARIS ist hochgradig strukturiert und modular, unterstützt die Arbeitsteilung und ist auf die industrialisierte IT-Produktion zugeschnitten. ESARIS unterstützt die Standardisierung und ist ein Mittel zur Erhöhung von Effektivität, Effizienz und Qualität. ESARIS wurde ab 2010 bei T-Systems entwickelt[63] und 2013 erstmals als Buch zugänglich gemacht, das 2017 in aktualisierter und erweiterter Auflage erschien.[64] Teile davon wurden durch die Vereinigung „Zero Outage Industry Standard" übernommen und weiterentwickelt.[65]

---

63 Eberhard von Faber and Wolfgang Behnsen: A Systematic Approach for Providers to Deliver Secure ICT Services; in: ISSE 2012 Securing Electronic Business Processes, Highlights of the Information Security Solutions Europe, ISSE 2012, Springer Vieweg, Wiesbaden, 2012, ISBN 978-3-658-00332-6, https://doi.org/10.1007/978-3-658-00333-3_9; p. 80-88

64 Eberhard von Faber and Wolfgang Behnsen: Secure ICT Service Provisioning for Cloud, Mobile and Beyond (ESARIS: The Answer to the Demands of Industrialized IT Production Balancing Between Buyers and Providers); Springer Vieweg, Wiesbaden 2017, 383 pages, 159 figures, ISBN 978-3-658-16481-2, 2nd updated and extended Edition, https://doi.org/10.1007/978-3-658-16482-9

65 Zero Outage Industry Standard: https://zero-outage.com/the-standard/security/; zuletzt aufgerufen am 21.01.2021

Open Enterprise Security Architecture (O-ESA)

Die Open Enterprise Security Architecture (O-ESA) gibt einen Überblick über wichtige Sicherheitsthemen, Prinzipien, Komponenten und Konzepte, die architektonischen Entscheidungen zugrunde liegen. O-ESA bietet Richtlinien und Vorlagen für die Entwicklung einer Enterprise Security Architecture. O-ESA ist selbst keine spezielle Enterprise Security Architecture.[66]

Die Open Enterprise Security Architecture (O-ESA) wurde von der Open Group entwickelt.

SABSA (Sherwood Applied Business Security Architecture)

Das SABSA®-Modell für „Security Architecture Development" hat sechs Ebenen: die kontextuelle Sicherheitsarchitektur – Sicht des Geschäfts, die konzeptionelle Sicherheitsarchitektur – Sicht des Architekten; die logische Sicherheitsarchitektur – Sicht des Entwicklers, die physische Sicherheitsarchitektur – Sicht des „Bauarbeiters", die Komponenten-Sicherheitsarchitektur – Sicht des Händlers sowie die betriebliche Sicherheitsarchitektur, deren Aspekte quer über die anderen fünf Ebenen gehen. Jede der sechs Ebenen wird weitergehend analysiert, indem jeweils sechs Fragen gestellt werden: was, warum, wie, wer, wo und wann. Die entstehende Matrix entspricht dem **Zachman Framework**, einer Enterprise-Architektur, die auf die 1980er Jahre zurückgeht und bei IBM entwickelt wurde.

SABSA basiert weiterhin auf ISO 7498-2.[67] Der Standard verbindet Sicherheitsdienste mit einer logischen Architektur, Sicherheitsmechanismen mit einer physischen Architektur und das Sicherheitsmanagement mit einer betrieblichen Architektur. Dem wurden oben zwei Ebenen hinzugefügt (kontextuell und konzeptionell), um den Geschäftsbezug abzubilden, sowie eine Ebene ganz unten (Komponenten-Architektur), um Werkzeuge und Produkte erfassen zu können.

SABSA hat einen starken geschäftlichen Bezug. SABSA liefert eine ganzheitliche Sicht und eine große Sammlung an bewährten Verfahren, Vorgehensweisen, Konzepten und Maßnahmen.

Hinweis: Diese kurze Zusammenfassung wurde auf Basis der Monographie zu SABSA verfasst.[68]

---

66 The Open Group: Open Enterprise Security Architecture (O-ESA), A Framework and Template for Policy-Driven Security; Van Haren Publishing, Zaltbommel, 2011, ISBN 978 90 8753 672 5, 142 pages

67 ISO 7498-2 – Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture; 1989

68 John Sherwood, Andrew Clark and David Lynas: Enterprise Security Architecture, A Business-Driven Approach; CRC Press, Boca Raton, 2005, ISBN 978 1 57820 318 5, 611 pages

Joint Security Management (JSM)

Das Joint Security Management (JSM) ist ein organisationsübergreifendes Sicherheitsmanagementsystem, das Anwenderorganisationen und IT-Dienstleister zusammenbringt und bei dem die Interaktion zwischen rechtlich verschiedenen Organisationen von vornherein im Mittelpunkt steht.[69]

Das Joint Security Management soll der Tatsache Rechnung tragen, dass die heutige IT-Industrie sehr arbeitsteilig organisiert ist und dass mehrere Firmen und Institutionen ihren Beitrag leisten müssen, damit IT-Services adäquat abgesichert sind und Sicherheitsvorfälle adäquat behandelt werden. Das Joint Security Management baut das Sicherheitsmanagement entlang der industriellen, marktwirtschaftlichen Prozesse und der für moderne IT charakteristischen Wertschöpfungsketten auf.

Das Joint Security Management unterscheidet die Vorbereitungsphase (mit vier Aufgabenbereichen) und die Betriebsphase (mit fünf Aufgabenbereichen). In der Vorbereitungsphase agieren Anwenderorganisation und IT-Dienstleister zunächst noch getrennt, kommen dann zusammen und schließlich übernimmt der IT-Dienstleister die Bereitstellung der IT-Services. In der Betriebsphase sind die sicherheitsbezogenen Aktivitäten beider Seiten miteinander verkoppelt. Für alle neun Aufgabenbereiche werden die Aufgaben für die Anwenderorganisation einerseits und den IT-Dienstleister andererseits dargestellt und deren Interaktionen und Abhängigkeiten beschrieben.

Hinweis: ISO/IEC 27017[70] gibt für einige Kontrollziele und Sicherheitsmaßnahmen der ISO/IEC 27002 eine Aufteilung bzw. Gegenüberstellung von Aufgaben des Kunden, der Cloud-Services nutzt, und des IT-Dienstleisters, der diese bereitstellt. Da ISO/IEC 27002 primär Anwenderorganisationen adressiert, die Informationstechnologie nutzen, wird der Bereich „Supplier Relationships" herangezogen, um die Cloud-Services zu integrieren. Die Detailtiefe entspricht der von ISO/IEC 27002.

Literatur und Bildnachweise

Besonders ein solches Buch, das sich zur Aufgabe macht, Definitionen von Fachbegriffen zu geben, kann nicht geschrieben werden, ohne dass der Autor vielfältige Literatur gelesen hätte – in der langen Zeit der Tätigkeit auf diesem Gebiet, bei der

---

69 Eberhard von Faber und Wolfgang Behnsen: Joint Security Management: organisationsübergreifend handeln (Mehr Sicherheit im Zeitalter von Cloud-Computing, IT-Dienstleistungen und industrialisierter IT-Produktion); Springer Vieweg, Wiesbaden 2018, 244 Seiten, 60 farbige Abbildungen, ISBN 978-3-658-20833-2, https://doi.org/10.1007/978-3-658-20834-9

70 ISO/IEC 27017 – Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Erstellung von Lehrunterlagen für Studierende und beim Schreiben dieses Buches. Die Definitionen sollen ja den Stand der Technik korrekt wiedergeben und konsensfähig sein. Das bedeutet auch, dass Begriffe und Zusammenhänge auch in anderen Veröffentlichungen so oder ähnlich vorkommen können – ja müssen.

Daher wurde wie folgt verfahren: (1) Literatur ist an den Stellen als Fußnote angegeben, wo ich sie direkt verwendet habe bzw. mir bewusst ist, dass Begriff, Definition oder sonstige Beschreibungen auf eine solche Quelle zurückgeführt werden können. (2) Gilt dies in gleicher Weise für Institutionen oder Einzelpersonen, so sind diese meist direkt im Text angegeben. (3) Die folgende Liste enthält Literaturhinweise und wiederholt nicht die Quellenangaben in diesem Kapitel. (4) Falls nicht anders angegeben, wurden Abbildungen extra für dieses Buch erstellt.

[1] ISO/IEC 15408 – Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model; 2009; and: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; April 2017, Version 3.1 Revision 5, https://commoncriteriaportal.org

[2] ISO/IEC 27000 - Information technology — Security techniques — Information security management systems — Overview and vocabulary; 2016

[3] Kissel, Richard (ed.): Glossary of Key Information Security Terms; National Institute of Standards and Technology, U.S. Department of Commerce, NIST IR 7298, Rev. 2, May 2013

[4] SP 800-30: Guide for Conducting Risk Assessments; NIST (National Institute of Standards and Technology); Rev. 1, Sept. 2012

[5] ISO/IEC 27005 – Information technology — Security techniques — Information security risk management; 2011

Elektronisches Zusatzmaterial
Die Abbildungen sind als PowerPoint-Datei kapitelweise über https://link.springer.com/ auf der Seite des eBooks abrufbar.

3 Identitäts- und Zugriffsmanagement (IAM)

Zweifelslos gehört die Frage „Wer darf was in einem IT-System?“ zu den wichtigsten der IT-Sicherheit. Wird das Identitäts- und Zugriffsmanagement (IAM) jedoch auf die „Abwehr der Bösen“ („Keep the bad guys out.“) fokussiert, so greift dies viel zu kurz. Die Komplexität der Aufgaben rückt erst dann ins Blickfeld, wenn man bedenkt, dass IAM die digitalisierten Geschäftsabläufe gestaltet. Es geht also primär um die „Unterstützung der Nutzer“ („Let the good guys in.“) und damit um mehr als um IT-Sicherheit.

Hinweis: Dieses Kapitel ist gewissermaßen die Ausformulierung einer Vorlesung, die ich jährlich gehalten und entsprechend aktualisiert habe. Quellen dafür sind am Ende des Kapitels angegeben.

Abb. 9 dient zur Orientierung und zeigt eine der Möglichkeiten, das Thema Identitäts- und Zugriffsmanagement (IAM) zu strukturieren. Die meisten Begriffe werden im Folgenden erklärt, wobei auf viele weitere Details eingegangen wird. In allen Beschreibungen werden sowohl die deutschen als auch die englischen Begriffe verwendet.

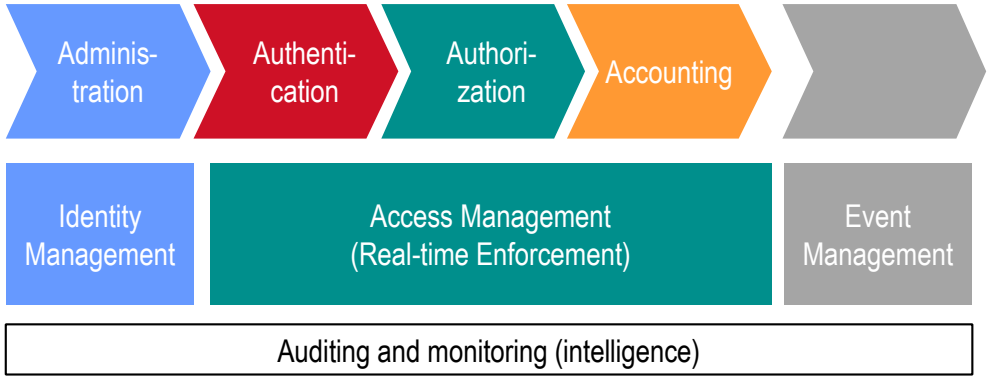


Abb. 9: IAM - Logische Sicht der Abläufe und Aufgaben[71]

Auf die Bereiche Ereignisverwaltung (event management, grau in Abb. 9) und Überwachung wird nicht weiter eingegangen, weil dies nicht zum eigentlichen Identitäts- und Zugriffsmanagement (IAM) gehört. Der englische Begriff „Intelligence“ ist

[71] Eberhard von Faber: Vorlesungsskript; Technische Hochschule Brandenburg

Zusatzmaterial online
Zusätzliche Informationen sind in der Online-Version dieses Kapitel (https://doi.org/10.1007/978-3-658-33431-4_3) enthalten.

E. von Faber, *IT und IT-Sicherheit in Begriffen und Zusammenhängen*,
Edition <kes>, https://doi.org/10.1007/978-3-658-33431-4_3

dem Sprachgebrauch der Geheimdienste entlehnt und bedeutet dort so etwas wie „Aufklärung“ im Sinne von „wissen, was passiert“. Das Prüfen und Überwachen erweist sich dabei als sehr komplexe Aufgabe, die weit über die Aufgaben und Kompetenzen des IT-Sicherheitsmanagements hinausgeht. Das ist der Grund, warum hier nicht weiter darauf eingegangen wird.

Abb. 10 zeigt eine etwas andere Darstellung, in der auch die wichtigsten verwendeten Daten zu sehen sind. Diese und weitere werden weiter unten erklärt.

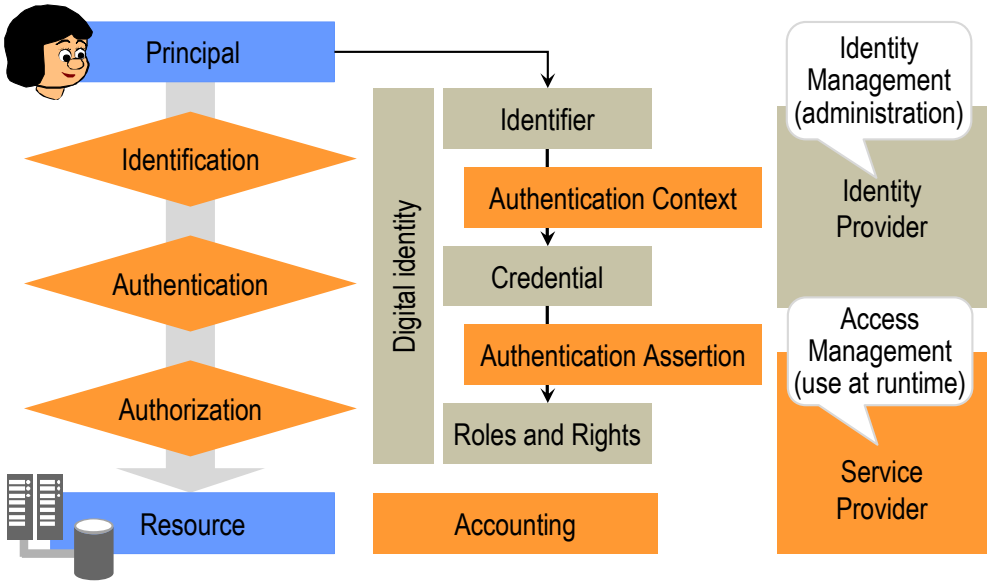


Abb. 10: IAM-Grundmodell[72]

3.1 Grundbegriffe

Identitäts- und Zugriffsmanagement (IAM) (Identity and Access Management)

Identitäts- und Zugriffsmanagement (IAM) umfasst Prozesse und IT-Lösungen für die Erzeugung, Verwaltung, Nutzung und Löschung von digitalen Identitäten (von Personen, Diensten, Geräten und anderen Objekten). Dabei geht es darum, den Zugriff auf Daten, Anwendungen und andere IT-Ressourcen so zu steuern, dass die Geschäftsprozesse gemäß der Business-Logik und den Sicherheitsrichtlinien ablaufen und erlaubte Zugriffe nachvollziehbar sind.

Das Identitäts- und Zugriffsmanagement besteht aus einem Verwaltungsteil, dem *Identitätsmanagement* (IdM, Administration), und einem Nutzungsteil, dem *Zugriffsmanagement (Access Management)*.

---

72 Eberhard von Faber: Vorlesungsskript; Technische Hochschule Brandenburg

Identitätsmanagement (IdM) (Identity Management)

Der Verwaltungsteil beim *Identitäts- und Zugriffsmanagement* (Identity and Access Management, IAM). Eine als **Identity provider** bezeichnete Rolle oder Entität verwaltet einen Bestand an digitalen Identitäten, indem sie diese erzeugt, aktualisiert und archiviert.

Digitale Identitäten werden im *Zugriffsmanagement (Access Management)* verwendet.

Zugriffsmanagement (Access Management)

Der Nutzungsteil beim *Identitäts- und Zugriffsmanagement* (Identity and Access Management, IAM). Eine als **Service provider** bezeichnete Rolle oder Entität stellt unter bestimmten, zu prüfenden Voraussetzungen IT-Ressourcen zur Verfügung.

Authentisierung (authentication), *Autorisierung* (authorization) und *Accounting* (Buchführung) sind die drei Maßnahmen, mit denen diese Einschränkungen im Zugriffsmanagement durchgesetzt werden.

Identifikation (identification)

Vorgang der Differenzierung von Subjekten bzw. Vorgang, bei dem sich die Instanz, die einen IT-Dienst nutzen möchte, gegenüber dem System, das den IT-Dienst anbietet, zu erkennen gibt.

Teil des *Zugriffsmanagements* (Access Management), der unmittelbar vor der *Authentisierung* (authentication) erfolgt. Synonym mit **Identifizierung**.

Achtung: Der hier gemeinte Vorgang darf nicht verwechselt werden mit der gleichnamigen Funktion eines IT-Systems, das zum Beispiel Menschen durch Analyse des Gesichts oder anderer biometrischer Merkmale in einer Menge erkennt.

Die Identifikation erfolgt mit Hilfe einer Eigenschaft, die Identität genannt wird. Außerhalb von IT-Systemen erfolgt die Identifikation anhand bzw. mit Hilfe einer „natürlichen" Identität, die bei Personen a priori gegeben ist und bei juristischen Personen (wie Unternehmen usw.) durch rechtliche Vorgänge etabliert wurde.

Innerhalb von IT-Systemen wird jeweils eine *digitale Identität* (digital identity) verwendet. Bei natürlichen Personen und juristischen „Personen" wird diese durch den *Identity provider* erzeugt oder bestätigt. Der Name und öffentliche Teil der Identität ist der **Identifikator** (identifier), der bei Personen **Benutzerkennung** genannt wird. Die Erzeugung bzw. Bestätigung erfolgt im Rahmen eines Vorgangs, der *Registrierung* genannt wird.

Bei technischen Komponenten (zunächst identischen Industrieprodukten) entsteht die digitale Identität im Rahmen der Herstellung ebenfalls durch eine „Registrierung", die hier jedoch *Personalisierung* (personalization) genannt wird.

Durch die Personalisierung werden aus technisch identischen Produkten unterscheidbare IT-Komponenten.

Registrierung (registration)

Herstellung der Verbindung zwischen „wirklicher oder natürlicher“ und „digitaler“ Identität.

Teil des *Identitätsmanagements* (identity management), also dem Verwaltungsteil des Identitäts- und Zugriffsmanagements (Identity and Access Management, IAM).

Bei der Registrierung erfolgt die Prüfung (Verifikation) der „wirklichen“ Identität. Diese Prüfung bestimmt die Qualität bzw. Verlässlichkeit der digitalen Identität und damit des gesamten *Zugriffsmanagements* (Access Management). Die digitale Identität ist das Resultat der Registrierung. Sie wird entweder nach der Prüfung erzeugt und zugewiesen oder aber nur bestätigt, weil sie bereits existiert.

Die Registrierung kann zum Beispiel durch persönliches Erscheinen erfolgen. Hier erfolgt die Prüfung der „wirklichen“ Identität unmittelbar. Bei der Selbstregistrierung erfolgt die Prüfung dagegen erst später, zum Beispiel indem eine Ware beschwerdefrei ausgeliefert und bezahlt wurde.

Das Ergebnis ist die Zuordnung eines *Identifikators* (identifier), der bei Personen *Benutzerkennung* genannt wird. Beispiele dafür sind Personalausweisnummer, Nutzername bzw. Nutzer-ID, Kürzel und E-Mail-Adresse. Damit wird im IT-System auch ein Konto (Nutzerkonto) erstellt, in dem mehr oder weniger umfangreiche Informationen über den Nutzer, allgemein als Principal bezeichnet, gespeichert werden.

Ebenfalls wird ein *Authentisierungsmerkmal* (credential) erzeugt und so im IT-System hinterlegt, dass eine spätere sichere Wiedererkennung des Nutzers, also die *Authentisierung* (authentication), möglich ist. Eventuell werden weitere Daten wie Name und Postadresse erfasst. All diese Daten bilden die sogenannte **digitale Identität**.

Personalisierung (personalization)

Einbringen von system- und/oder gerätespezifischen Informationen (Identitäten, Parameter, Schlüssel) in eine IT-Komponente.

Beim Identitäts- und Zugriffsmanagement geht es um eine Subjekt-Objekt-Beziehung, wobei dem Subjekt unter bestimmten, zu prüfenden Voraussetzungen Zugriff auf ein Objekt (IT-Ressource) gewährt wird. Handelt es sich um Personen, die den Zugriff anfordern, so erfolgt die Zuordnung der dafür benötigten digitalen Identität durch einen *Registrierung* genannten Vorgang. Aber auch die Kommunikation zwischen IT-Komponenten muss geregelt erfolgen. Durch den Vorgang der Personalisierung werden sie mit *digitalen Identitäten* ausgestattet.

Authentisierung (authentication) – Abkürzung: AuthN

Verifikation einer behaupteten Identität. Die erste der drei „A"-Aufgaben im *Zugriffsmanagement*. Synonym mit **Authentifizierung**.

Die Instanz, die einen IT-Dienst nutzen möchte, authentisiert sich mit Hilfe eines geheimen *Authentisierungsmerkmals* (credential) gegenüber dem System, das den IT-Dienst anbietet. Dieses System, das die anfordernde Instanz authentisiert, wird *Authentisierungsdienst* genannt, die entsprechende Rolle im Gesamtsystem *Authentication authority*.

Authentisierungsmerkmal (credential)

Daten zum Nachweis bzw. zur Feststellung einer behaupteten Identität.

Beispiele sind ein Passwort oder eine Chipkarte; aber auch kryptografische Schlüssel werden dafür eingesetzt. Ein Authentisierungsmerkmal wird im Rahmen der *Authentisierung* (authentication) von der Instanz, die einen IT-Dienst nutzen möchte, vorgelegt und geprüft, bevor der IT-Dienst zur Verfügung gestellt wird.

Autorisierung (authorization) – Abkürzung: AuthZ

Einräumung von Rechten (Ermöglichung des Zugriffs auf Ressourcen bzw. IT-Objekte) nach Überprüfung von Zugriffsregeln und Zugriffsrechten. Die zweite der drei „A"-Aufgaben im *Zugriffsmanagement*. Autorisierung ist in gewisser Weise synonym zum Begriff *Zugriffskontrolle*, der weiter unten verwendet wird, um die technische Umsetzung der Autorisierung zu erläutern.

Alternative Definition: Autorisierung ist der Vorgang, Subjekten den Zugriff auf Objekte zu gewähren.

Der Begriff Zugriff ist von zentraler Bedeutung und im Sinne der Informationstechnik zu verstehen: **Zugriff (access)** ist die Tatsache und Art der Interaktion zwischen Subjekt und Objekt mit dem Ergebnis, dass Informationen fließen.

Das Subjekt ist in diesem Sinne die aktive Entität, deren Identität bereits geprüft ist (siehe *Authentisierung*) und feststeht. Statt Subjekt wird häufig der Begriff *Principal* verwendet. Beide sind fast synonym und umfassen Personen, IT-Komponenten, IT-Services, Dateien, Geräte und dergleichen mehr. Das Objekt ist die passive Entität (resource), auf die Subjekte zugreifen (wollen).

Der Begriff Zugriff sollte allein für logische Vorgänge, wie oben definiert, reserviert bleiben. Für alle physischen Vorgänge (Betreten eines Gebäudes oder Raumes) sollte, um Missverständnisse zu vermeiden, stattdessen der Begriff **Zugang** verwendet werden.

Accounting (Buchführung)

Erzeugung von Daten, die die Nutzung von IT-Ressourcen betreffen. Die dritte der drei „A"-Aufgaben im *Zugriffsmanagement*.

Die Erfassung von Nutzungsdaten kann sehr unterschiedliche Zwecke verfolgen: IT-Sicherheitsexperten haben dabei primär das Erkennen von Sicherheitsverstößen und möglichen Schwachstellen im Auge. Entsprechende Daten dienen aber auch der Nachverfolgung und Beweissicherung für *Compliance*-Nachweise und Revisionszwecke. Manchmal dient die Erfassung von Verbrauchsdaten aber einfach der Kostenzuweisung (charging) oder der Rechnungsstellung (billing). In wieder anderen Fällen werden die Nutzungsdaten verwendet, um Kapazitäten der IT an den Bedarf anzupassen. Sie werden aber auch für Trendanalysen zum Beispiel für die Pflege der Kundenbeziehung (CRM) genutzt.

3.2 Weitere Bestandteile und Umsetzung

3.2.1 Von Subjekten bis zur Informationsflusskontrolle

Principal

Das *Zugriffsmanagement* ist eine Subjekt-Objekt-Beziehung: Das anfordernde Subjekt verlangt Zugriff auf ein Objekt (IT-Ressource). Das Subjekt (anfordernde Instanz) wird oft als Principal bezeichnet. Dabei kann es sich um einen Menschen, eine Rolle, eine Institution wie eine Firma, eine IT-Komponente oder einen IT-Dienst bzw. eine IT-Anwendung und dergleichen handeln. Menschen greifen häufig nicht direkt auf IT-Systeme zu bzw. authentisieren sich nicht selbst, sondern nutzen eine IT-Komponente, die als Stellvertreter fungiert. Falls dies bei der Entwicklung oder beim Betrieb der IAM-Lösung eine Rolle spielt, kann dieser Stellvertreter extra eingeführt und als „**Principal agent**“ bezeichnet werden.

Nutzer, Arten von ~

Nutzer sind Personen, die als Subjekt Zugriff auf Objekte (IT-Services bzw. IT-Ressourcen) benötigen. Die Steuerung des Zugriffs ist Gegenstand des Identitäts- und Zugriffsmanagements (IAM). Bei den Nutzern handelt es sich in der Regel jeweils um Einzelpersonen (Individuen). Ausnahmen bilden die sogenannten **funktionalen Nutzerkonten** (functional accounts), bei denen sich mehrere Nutzer eine digitale Identität teilen und damit die Zugriffsmöglichkeiten gemeinsam nutzen können. Funktionale Nutzerkonten werden vor allem zur Durchführung administrativer, meist automatisierter Aufgaben verwendet.

Grundsätzlich muss zwischen normalen Nutzern und privilegierten Nutzern unterschieden werden. Erstere verwenden IT-Services bzw. allgemein IT-Ressourcen, um anderweitige private oder geschäftliche Tätigkeiten durchzuführen. Sie können die Art und Weise, ob, in welcher Form und wem IT-Ressourcen zur Verfügung gestellt werden, nicht beeinflussen. Insbesondere können sie ihre eigenen Rechte und die anderer nicht verändern.

Privilegierte Nutzer werden meist als **Administratoren** bezeichnet. Sie verwalten Computersysteme oder Netzwerke. Im Unterschied zu normalen Nutzern

verfügen sie über eine oder mehrere der folgenden Fähigkeiten: Privilegierte Nutzer sorgen für die reibungslose Bereitstellung von IT-Services bzw. allgemein IT-Ressourcen. Sie müssen dazu auf IT-Systeme und IT-Komponenten zugreifen, die normalen Nutzern nicht zugänglich sind, und Tätigkeiten zur Verwaltung der IT ausführen, die normalen Nutzern verwehrt sind. Privilegierte Nutzer sorgen für den ordnungsgemäßen Betrieb des Identitäts- und Zugriffsmanagements (IAM) und aller dafür benötigten IT-Systeme und IT-Komponenten. Privilegierte Nutzer verwalten die digitalen Identitäten der normalen Nutzer. Besonders privilegierte Nutzer verwalten die digitalen Identitäten anderer privilegierter Nutzer (Administratoren). Solche Systeme sind hierarchisch aufgebaut. Durch die Verwaltung von digitalen Identitäten bestimmen sie ganz oder teilweise über die Zugriffsmöglichkeiten anderer Nutzer.

Privilegierte Nutzer besitzen also umfangreiche Rechte bezüglich der Verwaltung von IT-Services bzw. IT-Ressourcen und aller zugrunde liegenden IT-Komponenten, der Verwaltung des Identitäts- und Zugriffsmanagements (IAM) und aller dafür benötigten IT-Systeme und IT-Komponenten und/oder der Verwaltung von digitalen Identitäten und der darin enthaltenen Rechte. Deshalb müssen diese Privilegien besonders sorgfältig zugewiesen (und entzogen) werden; und es müssen besonders sichere Verfahren zum Beispiel für die Authentisierung (siehe *Authentisierungsverfahren*) verwendet werden.

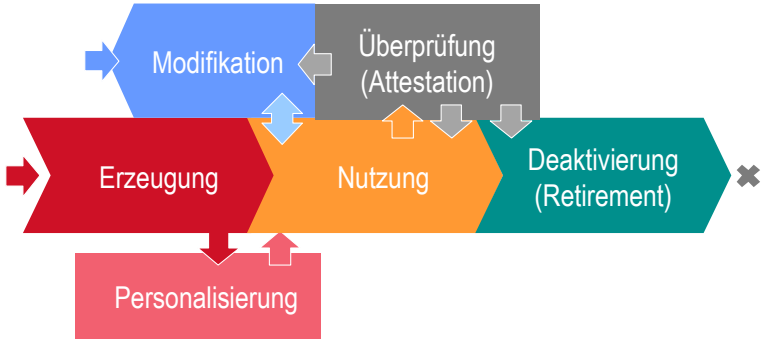


Abb. 11: Lebenszyklus digitaler Identitäten

Lebenszyklus digitaler Identitäten

Gegenstand des *Identitätsmanagements* (Verwaltungsteil des Identitäts- und Zugriffsmanagements).

Generell folgt der Lebenslauf digitaler Identitäten den realen Veränderungen bezüglich der dahinterstehenden Personen außerhalb des IT-Systems. Bei den digitalen Identitäten von IT-Komponenten usw. gilt dies entsprechend.

Grob unterscheidet man folgende Phasen (Abb. 11): Erzeugung (Beispiel: Mitarbeiter tritt ins Unternehmen ein), Nutzung (Identität und verbundene Rechte sind aktiv und können genutzt werden), Modifizierung (Beispiel: Mitarbeiter wird befördert oder nimmt andere Aufgaben wahr, so dass sich seine Rechte

ändern) und Löschung bzw. Deaktivierung (Beispiel: Mitarbeiter verlässt das Unternehmen). Die erste Phase (Erzeugung) korrespondiert mit dem Vorgang der *Registrierung*.

Die letzte Phase der Löschung bzw. Deaktivierung, für die sich der englische Begriff **Retirement** eingebürgert hat, ist besonders wichtig. Immer wieder kommt es zu Sicherheitsvorfällen, weil digitale Identitäten immer noch verwendbar sind, obwohl die Personen das Unternehmen längst verlassen haben oder in gänzlich anderer Funktion tätig sind und sich daher für die bestehenden Zugriffsmöglichkeiten nicht mehr verantwortlich fühlen.

Daher muss regelmäßig überprüft werden, ob die digitale Identität (einschließlich der enthaltenen Rollen und Rechte) die aktuellen Erfordernisse in der Organisation und in deren Geschäftsablauf korrekt widerspiegelt. Für diesen Überprüfungsvorgang bzw. die neuerliche Bestätigung der digitalen Identität hat sich der englische Begriff **Attestation** eingebürgert. Oft wird auch von **Rezertifizierung** gesprochen.

Authentisierungsdienst

Die Entität, die die *Authentisierung* durchführt. Wenn weniger das IT-System, sondern eine Rolle im Gesamtsystem gemeint ist, wird der Begriff **Authentication authority** verwendet.

Der Authentisierungsdienst prüft die Korrektheit des geheimen *Authentisierungsmerkmals* (credential) durch Vergleich mit einem gespeicherten Vergleichswert. Um beide Werte in Verbindung bringen zu können, wird auch der *Identifikator* (identifier) des *Principals* bzw. Nutzers benötigt. Für den Schutz des geheimen *Authentisierungsmerkmals* gegen Abhören und Wiedereinspielen werden vor oder bei der Übertragung teils umfangreiche zusätzliche Sicherheitsmaßnahmen ergriffen. Das Gleiche gilt für die Speicherung der Vergleichswerte.

Abhängig vom gewählten *Authentisierungsverfahren* und weiteren Anforderungen wird das System zur Authentisierung (Authentisierungsdienst) unterschiedlich realisiert. Beispiele sind *LDAP*, *Kerberos*, *RADIUS* und zertifikatsbasierte Systeme (*Public-Key-Infrastructures, PKI).*

Als Ergebnis der Authentisierung erzeugt der Authentisierungsdienst die **Authentication assertion**" (Feststellung). Die Authentication assertion ist die Basis für die nachfolgende Autorisierung. Sogenannte **SAML-Token** oder bestimmte *Cookies* sind Vertreter einer Authentication assertion.

Dieser Datensatz enthält (neben dem Ergebnis der Authentisierung) oft auch Informationen, die als **Authentication context** bezeichnet werden. Dabei handelt es sich um Parameter wie zum Beispiel die Zeit der Authentisierung, den Ort bzw. die Umstände der Netzverbindung oder den maximalen Transaktionswert. Dies bestimmt, inwieweit die (erfolgte) Authentisierung gültig ist bzw. bleibt und wann eine Neu-Authentisierung erforderlich ist.

Abb. 12: Schema der Umsetzung der Zugriffskontrolle[73]

Zugriffskontrolle (access control)

Der Vorgang der Beschränkung des Zugriffs (der Interaktion zwischen Subjekt und Objekt). Zugriffssteuerung wäre eine bessere Übersetzung des englischen Begriffs. Oft werden neben der Beschränkung des Zugriffs zusätzlich alle unterstützenden Maßnahmen wie die Authentisierung und sogar das Identitätsmanagement subsummiert. Bei der hier verwendeten, engeren Definition bezieht sich der Begriff Zugriffskontrolle auf den Vorgang der *Autorisierung* oder dessen Umsetzung und ist in diesem Sinne synonym dazu.

Betrachtet man die technische Umsetzung näher, so werden Grenzen und Probleme der Zugriffskontrolle sichtbar. Grundsätzlich besteht die Zugriffskontrolle aus zwei Vorgängen (siehe Abb. 12): der Entscheidung (decision) und der Durchsetzung (enforcement). Auch im IT-System erfolgt dies getrennt, oft in zwei vollständig voneinander entfernten Systemen, was die Übertragung der Entscheidung bzw. Feststellung an den Durchsetzungspunkt in Form eines gesicherten Datensatzes (authorization assertion) erforderlich macht.

Während der Entscheidungspunkt die *Rechte* prüft, kann man sich den Durchsetzungspunkt als eine Schranke vorstellen, die nur bei einem positiven Bescheid (Feststellung, englisch: assertion) aufgeht und sonst den Zugriff unmöglich macht. Doch mit dieser Architektur sind Einschränkungen und weitere Probleme verbunden. Die Zugriffskontrolle ist nämlich nur dann wirksam, wenn der Zugriff über den Weg (Kanal) erfolgt, der mit dem Durchsetzungspunkt (enforcement point) standardmäßig versperrt ist. Das kann in vielen Fällen nicht als gegeben angenommen werden und ist Ursache für viele Sicherheitsprobleme. Mehr dazu finden Sie unter *Grenzen der Zugriffskontrolle*.

[73] Eberhard von Faber: Vorlesungsskript; Technische Hochschule Brandenburg; modifiziert

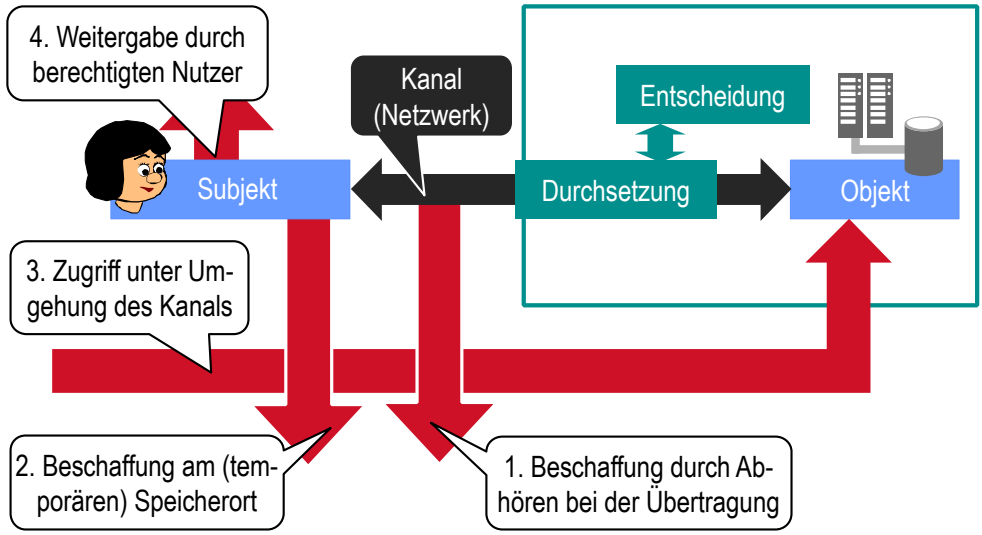


Abb. 13: Grenzen der Zugriffskontrolle

Grenzen der Zugriffskontrolle

Übliche IT-Systeme sind so aufgebaut, dass der Nutzer (Subjekt in Abb. 13) über ein Netzwerk verbunden auf das System zugreift, das den IT-Dienst bzw. die IT-Ressource (Objekt) bereitstellt. In der Shannon'schen Informationstheorie wird der Kanal (siehe Abb. 13) durch das das Netzwerk gebildet, aber es kommt im Folgenden nicht darauf an, ob es sich wirklich um ein Netzwerk handelt. Wichtig ist, dass der Durchsetzungspunkt des Zugriffsmanagements auf diesem Kanal liegt und nur dort den Zugriff beeinflussen kann (siehe *Zugriffskontrolle)*.

Die Zugriffskontrolle erlaubt oder verbietet einem (authentisierten) Subjekt eine definierte Aktion (wie Lesen, Verändern und Löschen) auf ein definiertes Objekt (Datei oder andere Ressource) durchzuführen. Dabei gelten folgende Voraussetzungen/Randbedingungen (siehe Abb. 13): Der Zugriff erfolgt stets über einen bestimmten Kanal und das Objekt verbleibt im Einflussbereich der Zugriffskontrolle.

Praktisch ergeben sich folgende Probleme oder Fragestellungen, die weitere, über die Zugriffskontrolle hinausgehende Sicherheitsmaßnahmen erforderlich machen können: Angreifer könnten die Informationen am Kanal abhören (siehe Nr. 1 in Abb. 13). Dieses Problem kann durch Verschlüsselung der Kommunikation gelöst werden. Angreifer könnten die Informationen auf dem Bildschirm oder von der Festplatte bzw. aus dem Hauptspeicher des Rechners des Nutzers (wo sie temporär gespeichert sind) abgreifen (siehe Nr. 2 in Abb. 13). Auch dieses Problem kann durch zusätzliche Sicherheitsmaßnahmen gelöst werden. Das Gleiche gilt für den Fall, dass Angreifer versuchen könnten, auf anderem Wege als über den geschützten Kanal auf das Objekt zuzugreifen (siehe Nr. 3 in Abb. 13). Angreifer könnten sich zum Beispiel physischen Zugang zum

Computer bzw. zur Festplatte des Servers verschaffen, auf dem das Objekt verfügbar ist. Demzufolge ist auch dieser Rechner entsprechend zu schützen.

Etwas problematischer ist der vierte Fall (siehe Nr. 4 in Abb. 13). Hier ist es so, dass der berechtigte Nutzer die für ihn verfügbare Information aus Versehen (unsachgemäß, fehlerhaft) oder sogar mit Absicht an unberechtigte Dritte weitergibt. Lösungen hierfür sind generell schwierig in der Anwendung und im Unterhalt. Beispiele für Produktgruppen, die gegen dieses Szenario schützen, sind DLP-Produkte (*Data Loss/Leakage Prevention*) und EDRM-Lösungen (*Enterprise Digital Rights Management*).

Generell würde eine umfassende Implementierung einer *Informationsflusskontrolle* (information flow control) alle Probleme lösen, die mit der Zugriffskontrolle inhärent verbunden sind.

Informationsflusskontrolle (information flow control)

Der Begriff Informationsflusskontrolle stammt aus dem militärischen Bereich und ist umfassender als die praktische Umsetzung einer *Zugriffskontrolle*. *Vertraulichkeit* von Informationen gewährleisten bedeutet im Kern eigentlich, dass kein Subjekt diese Informationen bekommen darf bzw. kann, das nicht dazu berechtigt ist. Der Ansatz zur Umsetzung muss hier also darin bestehen, die Möglichkeiten zur Weitergabe von Informationen derart einzuschränken, dass Subjekte ohne Berechtigung nicht in den Besitz der zu schützenden Informationen gelangen können gleich welchen Weg sie durch das IT-System nehmen.

Während bei der Zugriffskontrolle die Zugriffsmöglichkeiten an den Speicherort gebunden sind, sind sie bei der Informationsflusskontrolle unabhängig davon. Entsprechende EDRM-Lösungen (*Enterprise Digital Rights Management*) binden die „Zugriffsrechte“ untrennbar an die Information (an die Datei) und verhindern durch Verschlüsselung deren Umgehung.

3.2.2 Implementierung der Zugriffskontrolle

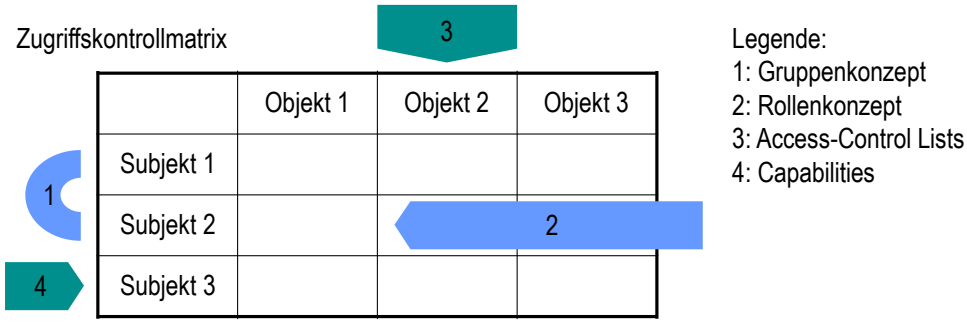


Abb. 14: Access-Control-Matrix und Andeutung der vier Vereinfachungen (siehe Text)[74]

[74] vergleiche: Eberhard von Faber: Vorlesungsskript; Technische Hochschule Brandenburg

Rechte (rights)

Eine Beziehung zwischen Subjekt, Objekt und der Art des gewünschten Zugriffs, die bestimmt, ob und unter welchen Bedingungen diese Aktion erlaubt wird.

Die Begriffe Recht und Zugriffsrecht sind im Zusammenhang mit dem Identitäts- und Zugriffsmanagement (IAM) synonym. Im Englischen ist neben dem Wort „rights" auch „entitlement" gebräuchlich.

Alle Subjekte und Objekte besitzen einen eindeutigen *Identifikator* (zum Beispiel eine Nutzer-ID bzw. *Benutzerkennung* bei Personen). Diese Werte werden bei der Definition von Rechten als Verweis auf das Subjekt herangezogen. Bei der Art des gewünschten Zugriffs unterscheidet man zum Beispiel zwischen Lesen, Schreiben und Ausführen. Die Kombination der drei Werte definiert ein Recht. Man kann sich die Rechte in einer **Access-Control-Matrix** bzw. **Zugriffskontrollmatrix** angeordnet vorstellen. Siehe Abb. 14. Das Recht oder Zugriffsrecht, das ein Subjekt in Bezug auf ein Objekt besitzt, ist am Kreuzungspunkt der jeweils zugehörigen Zeile bzw. Spalte in der Tabelle verzeichnet.

Bei komplexeren Systemen bestehen Probleme hinsichtlich Pflege und Konsistenz infolge der Anfälligkeit gegenüber Administrationsfehlern. Der Ansatz skaliert nicht.[75] Üblicherweise wird die Matrix daher vereinfacht und aufgeteilt. Dafür gibt es vier Ansätze: *Gruppen*, *Rollen*, *Access-Control Lists* und *Capabilities*.

Nicht zuletzt werden Regeln für die Vergabe der Rechte benötigt. Ein solches Regelwerk wird **Zugriffskontrollpolitik** genannt. Werden die Rechte allen Regeln folgend korrekt definiert und durchgesetzt, werden alle Zustände des Systems im Einklang mit der Zugriffskontrollpolitik stehen. Unterschiedliche Ansätze, zu solchen Regeln zu kommen, stellen die Zugriffskontrollstrategien *Eigentümerprinzip (Discretionary Access Control, DAC)* und *Vorschriftsprinzip (Mandatory Access Control, MAC)* dar.

Gruppen (groups)

Das Konzept der Gruppen stellt eine der vier Ansätze zur Vereinfachung und Aufteilung einer *Zugriffskontrollmatrix* (Access-Control-Matrix) und zur Anordnung von Zugriffsrechten dar. Siehe hierzu Nr. 1 in der Darstellung der Access-Control-Matrix in Abb. 14. Bei Gruppen werden Nutzer zusammengefasst und mit gleichen Rechten ausgestattet.

---

75 50.000 Mitarbeiter und 500 wichtige Programme oder Daten führen zu 25 Millionen Einträgen. Allerdings werden einige der IT-Services und Programme, die zunächst als Objekte auftauchen, ihrerseits wiederum auf andere Objekte zugreifen müssen. Tauchen bei den 500 Objekten 250 im ersten und 250 im zweiten Zugriffsschritt als Objekte auf, so hat die dreidimensionale Matrix rein rechnerisch über 3 Milliarden Einträge.

Die Nutzer in einer Unternehmung lassen sich typischerweise Kategorien zuordnen wie zum Beispiel IT-Administrator, Führungskraft, Mitarbeiter und Innenrevision. Dem Gruppenkonzept folgend werden alle Nutzer (Principals) einer solchen Kategorie zugeordnet und dann gleichbehandelt, d.h., mit den gleichen Zugriffsrechten ausgestattet. Beispiel: Administrator, Nutzer, Gast.

Hinweis: Im Unterschied zum *Rollen*konzept werden beim Gruppenkonzept zuerst Nutzer zusammengefasst. Dann werden Rechteprofile zugewiesen. Das Rollenkonzept bearbeitet die Matrix dagegen von rechts nach links (Abb. 14).

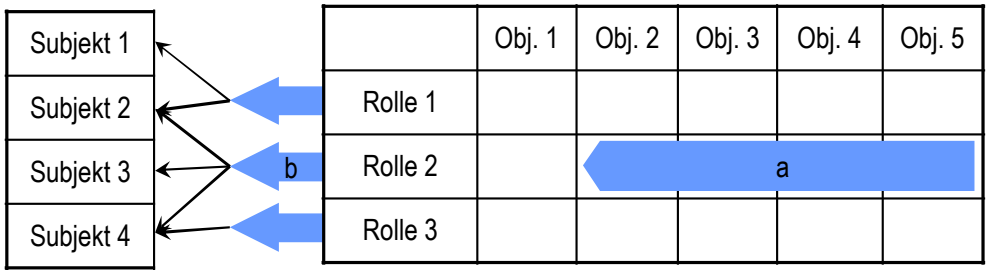


Abb. 15: Veranschaulichung des Rollenkonzepts[76]

Rollen (roles)

Das Konzept der Rollen stellt eine der vier Ansätze zur Vereinfachung und Aufteilung einer *Zugriffskontrollmatrix (Access-Control-Matrix)* und zur Anordnung von Zugriffsrechten dar. Siehe hierzu Nr. 2 in der Darstellung der Access-Control-Matrix in Abb. 14.

In einer Unternehmung gibt es typische Aufgaben und Arbeitsabläufe, für deren Ausführung bestimmte Zugriffsrechte erforderlich sind. Daher würden sich bestimmte Muster in den Zeilen der Matrix (Abb. 14) in Form von Rechteprofilen wiederholen. Das schafft Möglichkeiten zur Vereinfachung der Matrix: Es werden Rechteprofile geschaffen, die Rollen genannt bzw. diesen zugewiesen werden (Abb. 15). In einem zweiten Schritt werden die Rollen (Rechteprofile) nun den Nutzern zugewiesen (Abb. 15), wobei ein Nutzer eine oder mehrere Rollen haben kann.

Das Rollenkonzept hat viele Vorteile. Es unterstützt eine Trennung zwischen der organisatorischen Verantwortung samt unternehmensinternem Genehmigungsprozess und der technischen Umsetzung durch IT-Personal. Führungskräfte weisen allein tätigkeitsbezogene Rollen zu, was keine IT-Kenntnisse verlangt. Die Zeit für die Zuweisung der Rechte durch das IT-Personal wird sehr verkürzt, weil nur eine Rolle oder einige wenige Rollen zugewiesen werden. Das führt zu Kostenersparnis, Zeitgewinn, einer besseren Einhaltung von Richtlinien und Regularien sowie zu mehr Transparenz.

---

[76] Eberhard von Faber: Vorlesungsskript; Technische Hochschule Brandenburg; modifiziert

Access-Control Lists (ACL)

Das Konzept der Access-Control-Lists stellt eine der vier Ansätze zur Vereinfachung und Aufteilung einer *Zugriffskontrollmatrix (Access-Control-Matrix)* und zur Anordnung von Zugriffsrechten dar. Siehe hierzu Nr. 3 in der Darstellung der Access-Control-Matrix in Abb. 14.

Bei Access-Control Lists (ACL) werden die Rechte den Objekten zugeordnet und dort gespeichert. Jedem Objekt werden Werte einer Spalte der Access-Control-Matrix zugeordnet (siehe Abb. 14). Diese Anordnung korrespondiert sehr gut mit der Zugriffskontrollstrategie *Eigentümerprinzip (Discretionary Access Control, DAC)*.

Schwierig gestalten sich das Hinzufügen bzw. Entfernen von Nutzern (was allerdings auch durch Deaktivierung der digitalen Identität möglich ist), aber auch Prüfschritte, bei denen festgestellt werden soll, über welche Rechte ein bestimmter Nutzer verfügt (siehe auch *Verantwortlichkeit* (Accountability)).

Capabilities

Das Konzept der Capabilities stellt eine der vier Ansätze zur Vereinfachung und Aufteilung einer *Zugriffskontrollmatrix (Access-Control-Matrix)* und zur Anordnung von Zugriffsrechten dar. Siehe hierzu Nr. 4 in der Darstellung der Access-Control-Matrix in Abb. 14.

Bei Capabilities werden die Rechte den Subjekten zugeordnet und dort gespeichert. Jedem Subjekt werden Werte einer Zeile der Access-Control-Matrix zugeordnet (siehe Abb. 14).

Im Prinzip sind die Stärken und Schwächen entgegengesetzt zu den der *Access-Control Lists*. Das Hinzufügen und Entfernen von Objekten gestalten sich aufwendig. Auch ist es schwieriger herauszufinden, welche Nutzer auf ein bestimmtes Objekt Zugriff haben.

Windows (ab der Version 2000) nutzt sowohl die *Access-Control Lists* als auch die Capabilities. Dadurch soll das Beste aus beiden Welten erreicht werden. Das ist nur deshalb möglich, weil die Capabilities dynamisch vergeben werden.

3.2.3 Zugriffskontrollstrategien

Eigentümerprinzip (Discretionary Access Control, DAC)

Zugriffskontrollstrategie. Der Eigentümer/Erzeuger (einer Information, einer Datei) bestimmt die Regeln und definiert die Rechte. Wie dies erfolgt, soll bestimmten Regeln folgen, liegt aber häufig im persönlichen Ermessen des Nutzers. Damit ist die Gewährleistung einer übergreifenden, widerspruchsfreien und konsequenten *Zugriffskontrollpolitik* kaum möglich.

Subjekte können Zugriffsberechtigungen an andere Subjekte weitergeben. Die Administration ist sehr einfach. Das Betriebssystem Unix implementiert diese Zugriffskontrollstrategie.

Vorschriftsprinzip (Mandatory Access Control, MAC)

Zugriffskontrollstrategie. Nach dem Vorschriftsprinzip ergeben sich aus einer „Klassifikation" bestimmte Regeln und nachfolgend die Rechte. Dabei wird die verbindliche, übergeordnete Einstufung durch das System oder ein Klassifizierungsschema bestimmt und dann durchgesetzt. Damit wird eine übergreifende, widerspruchsfreie und konsequente *Zugriffskontrollpolitik* durchgesetzt. Zum Beispiel im Umfeld geschäftlicher Anwendungen gilt die Implementierung dagegen als zu unflexibel.

Role Based Access Control (RBAC)

Zugriffskontrollstrategie. Es werden Aufgaben und Arbeitsabläufe identifiziert und die zu ihrer Ausführung erforderlichen Rechte zu entsprechenden aufgabenbezogenen Rechteprofilen zusammengefasst. Das definiert die *Rollen*. Diese Rollen werden (ggf. dynamisch) Nutzern zugeordnet, wobei ein Nutzer eine oder mehrere Rollen wahrnehmen kann.

Bei sorgfältiger Implementierung ist die Durchsetzung einer übergreifenden, widerspruchsfreien und konsequenten Zugriffskontrollpolitik möglich. Allerdings erweisen sich das Rollenkonzept bzw. die entsprechende Zugriffskontrollstrategie in sehr dynamischen Umgebungen manchmal als zu unflexibel. Dies ist dann der Fall, wenn sich die Aufgaben bzw. die verwendete Informationstechnologie (wie Anwendungssoftware) zu schnell verändern.

Attribute Based Access Control (ABAC)

Zugriffskontrollstrategie. Ähnelt in gewisser Weise dem *Role Based Access Control (RBAC)*. Allerdings werden den Nutzern hier nicht Rollen (Rechteprofile) zugewiesen, sondern allgemein Eigenschaften (Attribute), die in ihren digitalen Identitäten enthalten sind bzw. daraus ermittelt werden können. Die Zugriffskontrolle erfolgt dann entsprechend dieser Attribute.

3.3 Authentisierungsverfahren und -systeme

Bei der Realisierung der Authentisierung kann unterschieden werden A) hinsichtlich der Art des verwendeten Authentisierungsmerkmals und B) hinsichtlich der Architektur und Arbeitsweise des Authentisierungssystems. Zur ersten Gruppe A, die im Folgenden mit „Authentisierungsverfahren" bezeichnet und in Kapitel 3.3.1 behandelt wird, gehören Passwortverfahren, Einmalpasswortverfahren, TANs, Grid-Cards und dergleichen. Die zweite Gruppe B, mit „Authentisierungssysteme" überschrieben, ist Gegenstand von Kapitel 3.3.2.

3.3.1 Authentisierungsverfahren

Authentisierungsverfahren

Der Begriff Authentisierungsverfahren bezieht sich (in diesem Buch) auf Unterschiede in der Realisierung der *Authentisierung* durch unterschiedliche Arten von Authentisierungsmerkmalen *(credentials)*. Architektur und Arbeitsweise des Authentisierungssystems als Ganzes werden nicht betrachtet.

Beispiele für Authentisierungsverfahren sind *Passwortverfahren*, *Einmalpasswortverfahren*, *TANs*, *Grid-Cards*, *biometrische Authentisierungsverfahren* wie zum Beispiel Fingerabdrücke und kryptografische *Challenge-Response-Verfahren*.

Passwortverfahren

Zur *Authentisierung* (von Nutzern) wird eine geheime Parole verwendet (Folge von Buchstaben, Ziffern und Sonderzeichen). Um eine ausreichende Sicherheit gegen Ausprobieren bzw. Erraten zu erreichen, bestimmen **Passwortrichtlinien** (password policy) die minimale Länge des Passwortes, die zugelassenen Zeichen, welche Zeichengruppen mindestens vertreten sein müssen und wie oft das Passwort gewechselt werden muss. Außerdem werden manche Zeichenkombinationen ganz verboten. Angriffe durch systematisches Ausprobieren des Passwortes werden dadurch abgewehrt, dass die Anzahl der Versuche (Eingaben, Authentisierungsversuche) begrenzt und das Konto ganz oder für eine gewisse Zeit gesperrt wird oder indem die Antwortzeit des Authentisierungssystems bei jedem Fehlversuch erhöht wird.

Werden Passwörter (unverschlüsselt) über potentiell unsichere Kanäle (Netze) übertragen, so besteht das Risiko, dass sie abgehört und dann missbräuchlich verwendet werden. In diesem Fall kann die Sicherheit durch **Dynamisierung der Passwörter** erhöht werden, was auch gegen systematisches Ausprobieren schützt. Dynamisierung bedeutet, dass das Passwort bei jeder Authentisierung gewechselt wird. Dafür gibt es sehr unterschiedliche Implementierungen wie *Einmalpasswortverfahren*, *TANs* oder *Grid-Cards*.

Die Dynamisierung schützt nicht vor dem Angriffsszenario „Man-in-the-Middle“. Beim →*Man-in-the-Middle*-Angriff unterbricht der Angreifer die laufende Kommunikation zwischen Nutzer (Principal) und Authentisierungssystem. Dem Nutzer (Principal) wird die Rolle des Authentisierungssystems vorgespielt, sodass der Angreifer an das Passwort gelangt und dann gegenüber dem wirklichen Authentisierungssystem als Nutzer (Principal) mit dem gestohlenen Passwort auftritt.

Oft werden Passwörter auch durch Trickbetrug („social engineering“ oder „phishing“) erbeutet.

Einmalpasswortverfahren

Methode zur *Dynamisierung* von Passwörtern. Sie schützt davor, dass Passwörter abgehört und missbräuchlich eingesetzt werden, nachdem der rechtmäßige Nutzer sie verwendet hat. Sie schützt nicht vor dem Angriffsszenario *Man-in-the-Middle*, weil bei diesem Angriff der Missbrauch unmittelbar auf den Passwortdiebstahl folgt und der rechtmäßigen Nutzung zuvorkommt.

Die Einmalpasswörter werden durch Hardware/Software auf Seiten des Nutzers und auf Seiten des Authentisierungssystems jeweils synchron und unabhängig voneinander für den folgenden Authentisierungsvorgang neu berechnet, wodurch gesendetes Passwort und Vergleichswert stets übereinstimmen. Ein bereits verwendetes Passwort wird nicht erneut akzeptiert, da das Authentisierungssystem ja schon das nächste Passwort erwartet. Die Art der kryptografischen Berechnung stellt sicher, dass aus einem abgehörten Passwort nicht auf folgende geschlossen werden kann.

Die Synchronisierung beider Seiten erfolgt durch Zeitmessung oder durch die Authentisierungsvorgänge. In beiden Fällen kann es zum Auseinanderlaufen (Asynchronität) kommen, was durch Fangbereiche ausgeglichen wird, also indem Passwörter in einem bestimmten Bereich (Zeit oder Authentisierungsversuche) akzeptiert werden.

TANs

Methode zur *Dynamisierung* von Passwörtern, wobei hier Transaktionsnummern (TANs) genannte PINs (mit meist vier oder sechs Ziffern) zum Einsatz kommen. Jede TAN kann (in der Regel) nur einmal zur Authentisierung verwendet werden. Damit soll die missbräuchliche Nutzung abgehörter TANs verhindert werden.

Die Transaktionsnummern (TANs bzw. PINs zur Authentisierung) wurden anfangs in Form einer Liste an den Nutzer ausgeliefert. Trickbetrügern gelang es jedoch häufig, Nutzer zur Herausgabe bisher nicht genutzter TANs zu bewegen. Deshalb wurden die Listen zu indizierten TAN-Listen weiterentwickelt (**iTAN**). Hierbei fordert das Authentisierungssystem statt der nächsten TAN diejenige an, die an einer bestimmten Stelle in der Liste steht. Herausgabe zum Beispiel der nächsten fünf TANs kann so ins Leere laufen. Einen besseren Schutz gegen Diebstahl der TAN-Liste oder Teilen davon bietet die Verwendung eines zusätzlichen Mediums. Hierbei wurde zum Beispiel der Index (Stelle der TAN in der Liste) per Mobilfunk an ein Handy des berechtigten Nutzers gesendet.

Diese Formen der Dynamisierung schützen weitgehend davor, dass die PINs/TANs abgehört und missbräuchlich eingesetzt werden, nachdem der rechtmäßige Nutzer sie verwendet hat. Sie schützen auch weitgehend davor, dass Angreifer in den Besitz von Teilen einer TAN-Liste oder sogar der kompletten TAN-Liste gelangen. Sie schützen aber nicht vor dem Angriffsszenario

Man-in-the-Middle, bei dem der Angreifer die Kommunikation zwischen Nutzer und Authentisierungssystem manipuliert. So kann er versuchen, zum Beispiel die Kontonummer einer beglaubigten Überweisung während der Übertragung durch seine eigene zu ersetzen. Dem hat man durch sogenannte kontogebundene TANs (**eTANs**) einen Riegel vorgeschoben. Die Server-Seite berechnet einen Kontrollwert, den der Nutzer für eine eigene Berechnung auf einem separaten TAN-Generator verwendet und zurücksendet. Da dieser Vorgang jeweils unter Einschluss der Kontonummer erfolgt, können Manipulationen aufgedeckt werden. Die Überweisung wird nicht abgeschlossen.

Grid-Cards

Die patentgeschützten Grid-Cards sind nicht besonders verbreitet, aber ein Anschauungsbeispiel für ein einfaches Authentisierungsverfahren mit *Dynamisierung* (wechselnde Passwörter) und einem Challenge-Response-Ansatz (Dialogfunktion). Der Nutzer besitzt eine Plastikkarte, eine Darstellung in einer Datei oder sieht eine Webseite, auf der eine mit Zeichen gefüllte Tabelle zu sehen ist. Der Authentisierungsdienst schickt dem Nutzer eine „Challenge" die den Inhalt von drei Zellen der Tabelle abfragt. Die Zelle wird jeweils identifiziert durch Angabe der Spalte und der Zeile. Der Authentisierungsdienst verfügt ebenfalls über die Tabelle und kann daher die Angaben des Nutzers überprüfen und ihn authentisieren.

Das Verfahren schützt weitgehend gegen Abhören, da die abgefragten Zellen jeweils zufällig gewählt werden und wechseln. Erst nach dem Abhören sehr vieler Authentisierungsdialoge könnte der Angreifer so viele Informationen gesammelt haben, dass er eine Authentisierungsanfrage mit einer gewissen Wahrscheinlichkeit richtig beantworten könnte.

biometrische Authentisierungsverfahren

Viele äußere Merkmale des Menschen sind genügend spezifisch (sie diskriminieren, sodass sich Menschen erkennbar unterscheiden) und stabil (sodass eine spätere Wiedererkennung möglich ist), dass sie als *Authentisierungsmerkmal* eingesetzt werden können. Diese Merkmale sind messbar (weshalb sie „biometrisch" genannt werden) und können während der *Registrierung* einer Person als Vergleichswert erfasst werden.

Bei der Verwendung biometrischer Merkmale muss zwischen der Anwendung zur Identifikation und der zur *Authentisierung* klar unterschieden werden. Bei der Identifikation muss der aktuell erfasste Wert mit allen gespeicherten Vergleichswerten verglichen werden. Bei der Authentisierung, bei der sich die Person bereits zu erkennen gegeben hat (*Identifikation*) genügt ein Vergleich mit einem Vergleichswert. Daher ist die Authentisierung stets genauer als die Identifikation. Beiden Verfahren haftet jedoch eine Unschärfe an, da biometrische Merkmale analog verteilt sind und einer gewissen Variabilität unterliegen. Deshalb gibt es immer Übereinstimmungen, die nicht erkannt werden (Falsche

Zurückweisung, **False Rejection Rate, FRR**, ist größer Null) und Unterschiede, die als Übereinstimmungen erkannt werden (Falsche Akzeptanz, **False Acceptance Rate, FAR**, ist größer Null).

Zu den physiologischen Merkmalen zählen Gesichtsgeometrie, Fingerabdruck, Handgeometrie bzw. Venenmuster, Augennetzhaut, Regenbogenhaut, DNA. Verhaltenstypische Charakteristiken von Personen sind zum Beispiel Stimme, Tastenanschläge, Schrift und deren Dynamik, Lippendynamik, Mimik und Bewegungsprofil. Merkmale sind statisch oder dynamisch.

Challenge-Response-Authentication

Bei der *Authentisierung* erhält die Instanz, die einen IT-Dienst nutzen möchte, eine Aufforderung, ihre Identität zu beweisen (Challenge). Die Instanz beweist ihre Identität durch Übersendung einer Nachricht (Response), die nur mit Hilfe eines geheimen *Authentisierungsmerkmals* (credential) erzeugt werden konnte, das der Instanz zugeordnet ist. Bei der Challenge-Response-Authentication unterscheidet sich diese Nachricht (Response) bei aufeinanderfolgenden Authentisierungsvorgängen. Sie hängt von der Anfrage bzw. Aufforderung zur Authentisierung (Challenge) ab. Damit wird erreicht, dass eine einmal abgehörte Nachricht nicht einfach genutzt werden kann, wenn der Authentisierungsdienst eine andere Challenge schickt.

Bei der kryptografischen Challenge-Response-Authentication (siehe →*Challenge-Response-Verfahren* ist die Challenge zufällig und damit ebenso wie die Response bei praktisch jeder Authentisierung verschieden. Das geheime Authentisierungsmerkmal wird dabei nicht übertragen, so dass es auch nicht abgehört werden kann. Das Verfahren schützt auch gegen ein *Man-in-the-Middle*-Szenario, denn der Angreifer erhält keine Information, die es ihm gestattet, sich gegenüber dem Authentisierungsdienst als der Principal (Nutzer) auszugeben.

Bei einer passwortbasierten Challenge-Response-Authentication (siehe →*Passwortverfahren*) kommen mehrere oder viele Passwörter zum Einsatz. Bei *TAN*-Listen und *Einmalpasswortverfahren* werden sie sequentiell abgefragt, bei *iTANs*, *Grid-Cards* und Sicherheitsfragen zur Passwortzurücksetzung erfolgt die Abfrage zufällig.

3.3.2 Authentisierungssysteme

Authentisierungssysteme

Der Begriff Authentisierungssystem bezieht sich (in diesem Buch) auf die unterschiedlichen Realisierungen der *Authentisierung* hinsichtlich der technischen Realisierung und Architektur des *Authentisierungsdienstes*. Die Art des verwendeten *Authentisierungsmerkmals* (credential) spielt hingegen keine oder eine untergeordnete Rolle.

Beispiele für Authentisierungssysteme sind *LDAP*, *Kerberos* und *RADIUS*.

LDAP

Bei LDAP handelt es sich um einen **Verzeichnisdienst (directory)**, also eine auf Abfragen spezialisierte zentrale *Datenbank*. LDAP wird sehr häufig bei passwortbasierter Authentisierung eingesetzt.

LDAP ist die Abkürzung für Lightweight Directory Access Protocol. Der Name des Kommunikationsprotokolls wird häufig einfach für den *Authentisierungsdienst* bzw. das *Authentisierungssystem* verwendet.

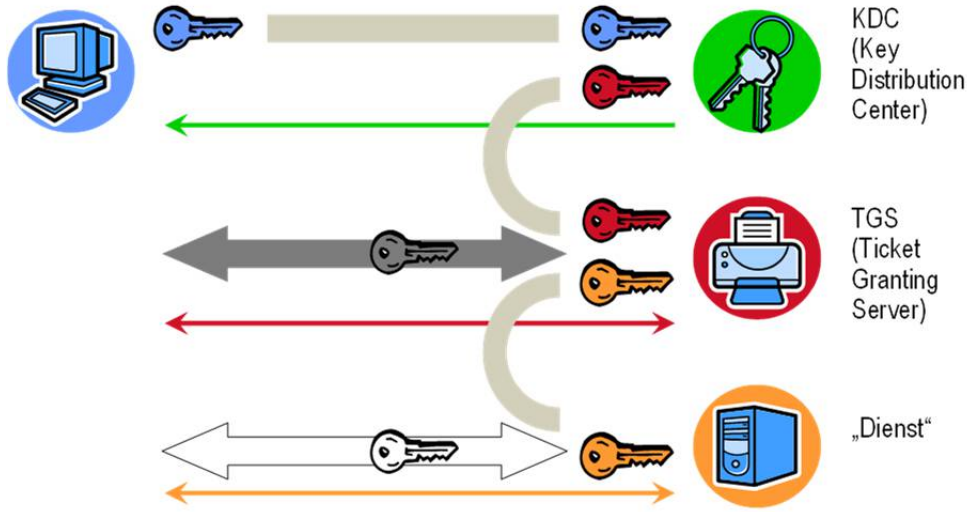


Abb. 16: Kerberos-Architektur mit drei Vertrauensbeziehungen (farbig) und der dreistufigen Kommunikation (Zeilen) des Nutzers („PC des Nutzers“ links)[77]

Kerberos

Kerberos ist ein auf Kryptgrafie basierendes System zur sicheren Verbindung mit meist entfernten IT-Services/IT-Komponenten in einem dynamischen Umfeld gegebenenfalls wechselnder IT-Services/IT-Komponenten.

Das System kennt drei Vertrauensbeziehungen, die wie folgt genutzt werden (siehe Abb. 16): 1. Nutzer sind einem Key-Distribution-Center (KDC bzw. Kerberos-Server) bekannt und werden dort authentisiert. Neue bzw. wegfallende Nutzer werden dort hinzugefügt bzw. entfernt. 2. Key-Distribution-Center (KDC) sind einem Ticket-Granting-Server (TGS) bekannt und werden dort authentisiert. Neue bzw. wegfallende KDC werden dort hinzugefügt bzw. entfernt. 3. IT-Services bzw. IT-Ressourcen sind einem Ticket-Granting-Server (TGS) bekannt und werden dort authentisiert. Neue bzw. wegfallende IT-Services bzw. IT-Ressourcen werden dort hinzugefügt bzw. entfernt.

---

[77] Eberhard von Faber: Vorlesungsskript; Technische Hochschule Brandenburg

Dadurch können Nutzer in einem dynamischen Umfeld auf IT-Services/IT-Komponenten (allgemein Ressourcen) zugreifen. Dies erfolgt in drei Schritten (siehe Abb. 16): 1. Nutzer fordern den Zugriff bei ihrem KDC bzw. Kerberos-Server an und müssen sich dafür beim KDC authentisieren. Das KDC beglaubigt die Anforderung in Form eines „Tickets“, das der Nutzer erhält und entsprechend der Instruktion des KDC an einen TGS weiterleitet. 2. Damit fordert der Nutzer den Zugriff bei diesem TGS an, der das „Ticket“ im Sinne einer Authentisierung auf Echtheit prüft. Das TGS beglaubigt die Anforderung in Form eines „Tickets“, das der Nutzer erhält und entsprechend der Instruktion des TGS an den gewünschten IT-Dienst weiterleitet. 3. Damit fordert der Nutzer den Zugriff beim gewünschten IT-Dienst an, der das „Ticket“ im Sinne einer Authentisierung auf Echtheit prüft. Der IT-Dienst erfährt auf diese Weise, dass die Kommunikation mit dem Nutzer „erlaubt“ ist. Kerberos sorgt ebenfalls dafür, dass der Nutzer neben dem „Ticket“, das er nur weitergibt, auch eine „Bestätigung“ erhält, die er öffnen kann. Auf diese Weise können die neu zusammengeführten Kommunikationspartner auch kryptografisch gesichert miteinander kommunizieren.

Kerberos ist in einer speziellen Form zum Beispiel fester Bestandteil des Windows-Betriebssystems.

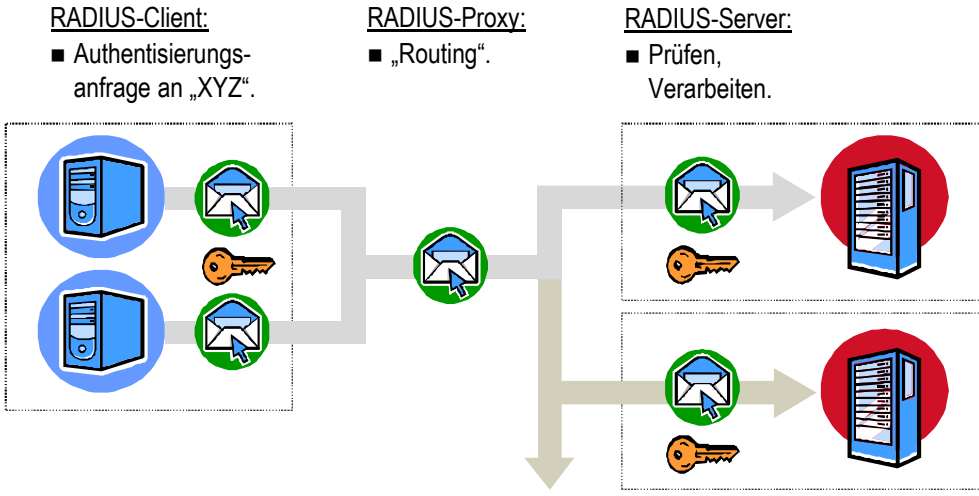


Abb. 17: Architektur von RADIUS mit optionalen Komponenten[78]

RADIUS

RADIUS ist die Abkürzung für Remote Authentication Dial In User Service. Es ist ein sehr mächtiges System (siehe Abb. 17), das neben der *Authentisierung* auch andere Funktionen bereitstellt. Besondere Merkmale der Authentisierung

78 Eberhard von Faber: Vorlesungsskript; Technische Hochschule Brandenburg

sind die Unterstützung mehrerer Nutzerdomänen und ein entsprechendes, sehr leistungsfähiges Routing zum *Authentisierungsdienst* der richtigen Domäne, die Unterstützung verschiedener *Authentisierungsverfahren* sowie die Möglichkeiten, die Kommunikation mit dem RADIUS-Authentisierungsserver zu verschlüsseln.

Single Sign-On (SSO)

Single-Sign-On-Lösungen dienen dazu, dem Nutzer eine Einmalanmeldung (Single Sign-On) zu bieten, obwohl die *Authentisierungsverfahren* der Zielsysteme nicht miteinander kompatibel sind. Manche SSO-Lösungen unterstützen verschiedene Authentisierungsverfahren, andere nur die Authentisierung mit Passwörtern, deren *Passwortrichtlinien* (password policies) nicht miteinander verträglich sind. Dies kommt vor allem dann vor, wenn Altsysteme (legacy systems) im Einsatz sind und nicht ersetzt werden können.

Der SSO-Client fungiert als Authentisierungsmedium (siehe *Principal agent*), das den Nutzer automatisch mit den darin gespeicherten Authentisierungsmerkmalen (credentials) anmeldet. Der SSO-Client erkennt zum Beispiel auch Aufforderungen (Masken) zum Passwortwechsel und führt diesen selbständig durch. Vor der Verwendung wird der SSO-Client durch den Nutzer freigeschaltet, indem er sich gegenüber dem Medium authentisiert.

Passwort-Manager speichern Nutzername und Passwörter für unterschiedliche Anwendungen (Konten) in einer mit einem Masterpasswort verschlüsselten Form. Sie fungieren jedoch nicht als Authentisierungsmedium und melden den Nutzer nicht automatisch an.

Federation (Föderation)

Federation (Föderation) erlaubt Nutzern, IT-Services aus einer anderen Domäne zu verwenden als aus der, in der ihre digitale Identität gepflegt wird. Dazu werden Informationen über das Ergebnis der Authentisierung (*Authentication assertion*, Feststellung) aus der Heimatdomäne (*Identity Provider*) in die Zieldomäne (Service Provider) übertragen. Der *Service Provider* akzeptiert diese, weil zwischen beiden Providern (Domänen) eine Vertrauensbeziehung besteht, die durch den Austausch kryptografischen Materials manifestiert wurde.

Die digitale Identität, die es erlaubt, Nutzer zu identifizieren und zu authentisieren, wird vom Identity Provider verwaltet. Der *Service Provider* führt und verwaltet ein Nutzerkonto, das im Kontext einer speziellen Applikation wichtig ist und deren Nutzung steuert. Föderation ersetzt nicht das Identitätsmanagement, sondern nutzt es in einer anderen Domäne bzw. aus einer anderen Domäne.

Man unterscheidet zwei Formen der Föderation (Federation): Bei der **Outbound Federation** bietet eine Organisation, die als Identity Provider agiert, seinen Nutzern einen Mehrwert, indem sie Dienste eines externen Service Providers zu nutzen erlaubt (ohne eine Registrierung/Anmeldung dort). Bei der **Inbound**

Federation bietet eine Organisation, die als Service Provider agiert, den Nutzern einen Mehrwert, indem sie ihre IT-Services (ohne Registrierung/Anmeldung) anderen Nutzern aus anderen Organisationen zu nutzen ermöglicht.

Föderation beginnt mit der Herstellung einer Vertrauensbeziehung zwischen zwei Parteien (Übereinkünfte treffen und Vertrag schließen). Dann wird kryptografisches Material ausgetauscht, das die Anerkennung von Authentication assertions ermöglicht, und ein Konnektor zu deren Austausch installiert. Benutzerkonten werden automatisch mit Daten angelegt, die aus der Heimatdomäne übertragen werden. Die Autorisierung ist nicht Gegenstand der Föderation.

3.4 Vertrauensbeziehungen und Public-Key-Infrastructure (PKI)

Um einzelne Daten vor unberechtigtem Zugriff zu schützen, ist *Zugriffskontrolle* nicht die einzige und nicht unbedingt die beste Methode. Daten können zum Beispiel, wie unter *Grenzen der Zugriffskontrolle* beschrieben, von berechtigten Nutzern aus dem Einflussbereich der Zugriffskontrolle gebracht werden. Bei der Kommunikation mit anderen (berechtigten) Anwendern passiert das regelmäßig.

Alternativ schützt man Daten mittels Verschlüsselung. Details werden in Kapitel 8 ausführlich behandelt. Bei der Anwendung sogenannter asymmetrischer Verfahren kommt es zu einer Problemstellung, die im Rahmen des *Identitätsmanagements* gelöst wird. Es werden digitale Ausweise (sogenannte Zertifikate) erzeugt und verwaltet. Dies ist der Hauptgrund, warum das Thema in diesem Kapitel „Identitäts- und Zugriffsmanagement (IAM)“ besprochen wird. Der zweite Grund besteht darin, dass die *Authentisierung* oftmals mittels kryptografischer Schlüssel erfolgt. Basiert die *Authentisierung* auf asymmetrischen Verfahren, spielen meist auch Zertifikate eine Rolle.

3.4.1 Das Problem asymmetrischer Kryptografie

Deshalb müssen wir uns kurz mit Kryptografie bzw. kryptografischen Schlüsseln beschäftigen, wobei die Analogie zu einem Haustürschlüssel hier völlig ausreichen wird. Natürlich kommt es auf die Güte des Schlosses an. Doch wenn man die Schlüssel nicht gut verwahrt (zum Beispiel im Schloss stecken lässt), nützt das beste Schloss nichts. Deshalb geht es, auch in den Anwendungen der Kryptografie, vor allem um die Verwaltung und Verwendung der Schlüssel. Noch näher ist man in der Analogie, wenn das Haus mit einem Zahlenschloss gesichert ist. Der Schlüssel ist dann eine Zahl, genau wie bei kryptografischen Verfahren, um die es jetzt geht. Die Zahlen sind sehr groß, was für Computer kein Problem darstellt. Sollen Menschen sie verwenden, so werden die Zahlen (Schlüssel) auf Token gespeichert, wie zum Beispiel einer Chipkarte, die die Person besitzt (siehe rechts oben in Abb. 18).

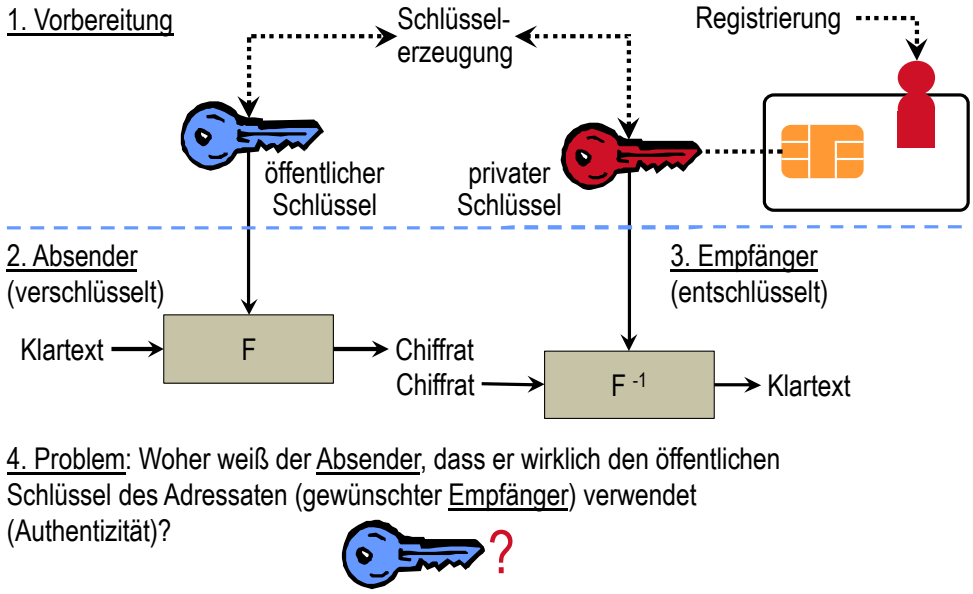


Abb. 18: Problemstellung bei Anwendung asymmetrischer Kryptografie (Verschlüsselung)[79]

Bei sogenannten *asymmetrischen Verschlüsselungs*verfahren, die im Folgenden ausschließlich betrachtet werden, unterscheidet sich der Schlüssel (Zahlencode) für das Zuschließen (Verschlüsseln von Daten) und das Aufschließen (Entschlüsseln von Daten). Siehe oben in Abb. 18. Beide Werte (Schlüssel) hängen zusammen. Damit die Kommunikationspartner ad hoc sicher kommunizieren können, d.h., ohne dass sie vorher Codes (Schlüssel) sicher austauschen müssen, wird einer der Codes (Schlüsselkomponenten) öffentlich gemacht.

3.4.2 Die Authentizität des öffentlichen Schlüssels

Der springende Punkt besteht darin, dass der Absender einer verschlüsselten Nachricht genau den Zahlencode (öffentlicher Schlüssel) verwenden muss, der zu dem Zahlencode (privater Schlüssel) des beabsichtigten Empfängers gehört. Denn anders als in unserem mechanischen Analogon (Zahlenschloss) sind alle Schlösser gleich; das kryptografische Rechenverfahren unterscheidet sich nicht. Verwendet der Absender einen falschen Code, so kann eventuell jemand anders die Daten entschlüsseln. Deshalb muss sichergestellt sein, dass es nicht zu Verwechselungen oder Manipulationen kommt (Angreifer gibt seinen Schlüssel als den eines andern aus).

Jeder öffentliche Schlüssel muss daher mit dem Namen des Besitzers (des zugehörigen privaten Schlüssels) versehen werden. Der Inhaber kann eine Person, eine Institution oder eine IT-Komponente usw. sein. Die Verbindung muss allerdings fälschungssicher sein, und auch der Zahlenwert des öffentlichen Schlüssels muss vor

[79] Eberhard von Faber: Vorlesungsskript; Technische Hochschule Brandenburg; modifiziert

Manipulationen geschützt sein. Dafür gibt es zwei grundsätzlich verschiedene Herangehensweisen. Bei einem *Web-of-Trust* muss jeder Teilnehmer für die *Integrität* der gespeicherten Schlüssel sorgen. Der Zusammenhang zwischen öffentlichem Schlüssel und Teilnehmer wird durch das Sammeln von Bestätigungen von Teilnehmern hergestellt und durch die wiederholte erfolgreiche Benutzung immer verlässlicher. Einen anderen Weg geht man mit einer *Public-Key-Infrastructure (PKI)*, die im Folgenden ausführlich erläutert wird. Das Grundprinzip ihrer Anwendung ist in Abb. 19 dargestellt. Die Verbindung zwischen (gewünschtem) Empfänger und dem richtigen Wert des öffentlichen Schlüssels wird hier durch ein sogenanntes *Zertifikat* hergestellt. Bei diesem „digitalen Ausweis" handelt es sich um einen digital signierten Datensatz, der neben Angaben zum Besitzer der Schlüssel (insbesondere des privaten Schlüssels) auch den öffentlichen Schlüssel enthält. Der Datensatz ist durch eine Signatur vor Manipulationen geschützt. Er wird von einer *Zertifizierungsstelle* (certification authority, eine Art Einwohnermeldeamt im Internet) erzeugt und herausgegeben, weshalb „digitaler Ausweis" sicher eine passendere Bezeichnung gewesen wäre. Allerdings hat sich die Übertragung des amerikanischen Ausdrucks „Certificate" eingebürgert, wohl auch, weil die USA keine Ausweiskultur besitzen. Wie bei anderen Ausweisen ist dessen Inhalt im sicherheitstechnischen Sinne nicht geheim, sondern hier sogar öffentlich. Absender verschlüsselter Nachrichten verwenden ihn wie in Abb. 19 dargestellt.

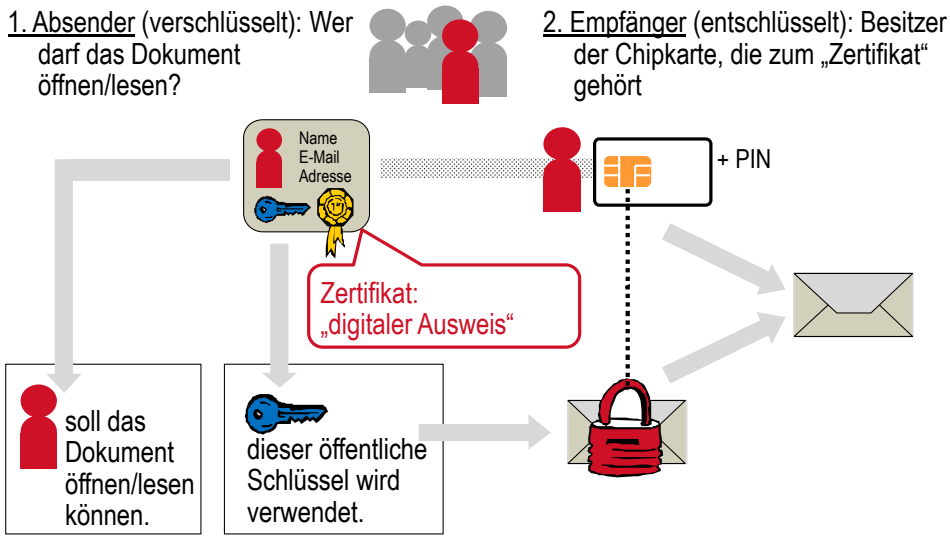


Abb. 19: Lösung des Problems asymmetrischer Kryptografie mit „Zertifikaten"[80]

[80] Eberhard von Faber: Vorlesungsskript; Technische Hochschule Brandenburg; modifiziert

Mit der Erzeugung der Schlüssel und des *Zertifikats* („digitaler Ausweis“) ist auch verbunden, dass der private Schlüssel entsprechend geschützt gespeichert wird. In Abb. 19 ist eine Chipkarte als Schlüsselträger zu sehen, was aber nur ein Beispiel ist.

Asymmetrische Kryptografie kann neben der Verschlüsselung (Schutz der *Vertraulichkeit*) auch für die Signatur (*Authentizität*) verwendet werden. Die obige Argumentation gilt analog für die Signatur, nur dass das „Problem“ diesmal beim Empfänger liegt. Dieser muss die Signatur mit dem richtigen (authentischen) öffentlichen Schlüssel prüfen, um den Datenursprung und die Integrität der Daten eindeutig feststellen zu können. Auch hier können Zertifikate bzw. eine Public-Key-Infrastructure (PKI) eine Lösung bieten.

Man kann die Zusammenhänge und die Funktion einer PKI auch ganz ohne kryptografische Schlüssel beschreiben.[81] Allerdings geht dann natürlich etwas an Tiefe verloren.

3.4.3 Implementierung

Web-of-Trust

Bei der Verwendung *asymmetrischer Verschlüsselungs*verfahren besteht das Problem der *Authentizität des öffentlichen Schlüssels*. Bei einem Web-of-Trust wird die Authentizität des öffentlichen Schlüssels bzw. der Zusammenhang zwischen öffentlichem Schlüssel und Teilnehmer (Besitzer) durch das Sammeln von Bestätigungen von Teilnehmern hergestellt und durch die wiederholte erfolgreiche Benutzung des öffentlichen Schlüssels in einer Kommunikation immer verlässlicher.

Die Bestätigungen von Teilnehmern werden durch Signaturen vor Manipulationen geschützt und ähneln daher Zertifikaten in einer *Public-Key-Infrastructure (PKI)*. Die Bestätigungen sind jedoch nicht Ergebnis einer standardisierten Prüfung, sondern geben den Grad des Vertrauens in die Authentizität eines Schlüssels wieder. Die gesammelten Werte werden bei jedem Anwender genutzt, um einen Gesamtwert (Key Legitimacy) zu errechnen. Datenformate sind in **OpenPGP** spezifiziert. Die bekanntesten Produkte sind **Pretty Good Privacy (PGP)** und **GnuPGP**.

Public-Key-Infrastructure (PKI)

Bei *asymmetrischen Verschlüsselungs*verfahren wird beim Absenden oder Abspeichern von Daten ein anderer Code (Schlüssel) verwendet als beim Empfangen oder Lesen. Beide Codes (Schlüsselkomponenten) gehören aber zusammen. Damit die Kommunikationspartner ad hoc sicher kommunizieren können, d.h., ohne dass sie vorher Codes (Schlüssel) sicher austauschen müssen, wird einer

---

[81] Benutzerhandbuch T-TeleSec Signet, Verschlüsselung, Signatur, Authentisierung, Vielfältige Anwendungen; T-Systems, 2004, ISBN 3-00-013243-0 (Autor: Eberhard von Faber)

der Codes (Schlüsselkomponenten) öffentlich gemacht. Dieser wird für die kritischen Aktionen, das Verschlüsseln und das Prüfen des Datenursprungs, genutzt. Würde der öffentliche Code (Schlüssel) zum Beispiel durch den eines Angreifers ersetzt, so kann dieser die Daten anstelle des rechtmäßigen Empfängers entschlüsseln, oder er kann die Daten manipulieren, gleichwohl sie von jemand anderem zu stammen scheinen. Eine Public-Key-Infrastructure (PKI) löst dieses Problem der **Authentizität des öffentlichen Schlüssels**, indem sie den öffentlichen Schlüssel zusammen mit Informationen zum rechtmäßigen Besitzer (der anderen Schlüsselkomponente) in einem digital signierten Datensatz fälschungssicher speichert, der einen digitalen Ausweis darstellt und *Zertifikat* genannt wird. Die Kommunikationsteilnehmer prüfen die Echtheit des Zertifikats ihres darin angegebenen Kommunikationspartners und verwenden dann den beglaubigten öffentlichen Code (öffentliche Schlüsselkomponenten) aus dem Zertifikat. Eine PKI erfordert eine vertrauenswürdige dritte Partei, die *Zertifizierungsstelle* (certification authority, CA), die die Zugehörigkeit der Schlüsselkomponenten zu einem Kommunikationspartner prüft und in Form eines Zertifikats bestätigt.

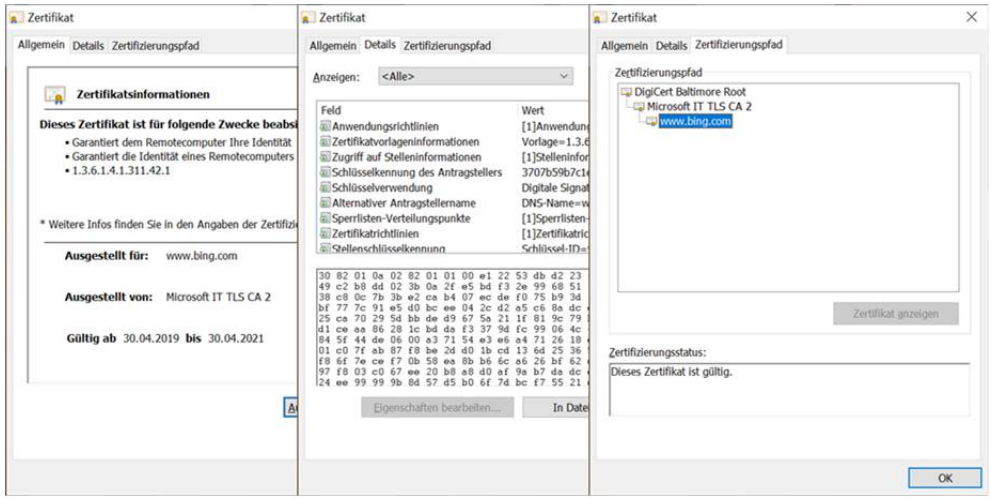


Abb. 20: Drei Teile des Zertifikats der Internet-Seite www.bing.com[82]

Zertifikat (certificate; digitaler Ausweis)

Ein Zertifikat ist ein fälschungssicherer Datensatz, der einen öffentlichen Schlüssel dem Inhaber (Person, Instanz, IT-Komponente) zuordnet, der auch den zugehörigen privaten Schlüssel besitzt. Ein Zertifikat wird von einer *Zertifizierungsstelle* (certification authority) erstellt, digital signiert und in der Regel auch

[82] Links: die für einen Ausweis typischen Angaben; Mitte: der öffentliche Schlüssel (unten) sowie Angaben zur Ausstellung und Nutzung (Auswahlfeld oben); Rechts: Zertifizierungspfad (Auswahl weiterer Zertifikate möglich)

veröffentlicht bzw. im Rahmen des Nutzungsbereichs der *Public-Key-Infrastructure (PKI)* verfügbar gemacht. Es enthält neben Informationen zum Inhaber und den öffentlichen Schlüssel nebst Hinweisen für seine Verwendung auch Angaben zur *Zertifizierungsstelle* (der Herausgeberin) und Details zur Ausstellung des Zertifikats. Siehe Abb. 20.

Zertifikate werden von Absendern verschlüsselter Daten, den Empfängern signierter Daten und von *Authentisierungsdiensten* (Server-Komponente der Authentisierung) verwendet. Sie enthalten keine geheimen Informationen und eignen sich nicht als *Authentisierungsmerkmal* (credential).

Das Datenformat ist in X.509 und ISO/IEC 9594-8 spezifiziert.[83]

Zertifizierungsstelle (certification authority, CA))

Eine Zertifizierungsstelle ist die Instanz in einer *Public-Key-Infrastructure (PKI)*, die *Zertifikate* erstellt und verwaltet. Mit einem Zertifikat bestätigt sie die Zuordnung eines öffentlichen Schlüssels zu einem Inhaber, der im Besitz des zugehörigen privaten Schlüssels ist. Die Verwaltung von Zertifikaten umfasst auch die Bereitstellung von *Sperrlisten* (certificate revocation lists) und die Bereitstellung von *Verzeichnisdiensten*. Verzeichnisdienste machen Zertifikate verfügbar, damit Teilnehmer ad hoc sicher kommunizieren können, d.h., ohne dass sie vorher Schlüsselmaterial austauschen müssen. Manchmal werden auch *Onlinestatusprüfungen (OCSP)* angeboten.

Die Erstellung und Verwaltung von Zertifikaten gehört zum *Identitätsmanagement* (identity management). Die Erstellung eines Zertifikats erfolgt auf Basis einer *Registrierung*. Bei höherwertigen Zertifikaten wird dabei die wirkliche Identität des Antragstellers (Schlüsselinhabers) überprüft. Ebenfalls wird überprüft, ob der Antragsteller wirklich im Besitz des privaten Schlüssels ist. Das Schlüsselmaterial kann vom Antragsteller erzeugt werden, der der Zertifizierungsstelle nur den öffentlichen Schlüssel aushändigt. Oft wird das Schlüsselmaterial von der Zertifizierungsstelle erzeugt. Dann muss der private Schlüssel über einen sicheren Weg (zum Beispiel auf einem physischen Schlüsselträger gespeichert per Post) versandt werden.

Registrierung sowie Erstellung und Verwaltung von Zertifikaten erfolgen nach Regeln, die (bei höherwertigen Zertifikaten) in *Zertifikatsrichtlinien* (Certificate Practice Statement, CPS) und *Certificate Policies (CP)* festgelegt sind.

Registrierungsstelle (registration authority, RA)

Die Registrierungsstelle ist die Instanz in einer *Public-Key-Infrastructure (PKI)*, die Anträge zur Erstellung von *Zertifikaten* bearbeitet und dabei insbesondere die *Registrierung* vornimmt. Bei höherwertigen Zertifikaten wird bei der Regis-

---

[83] ISO/IEC 9594-8:2017 — Information technology — Open Systems Interconnection — The Directory — Part 8: Public-key and attribute certificate frameworks

trierung die wirkliche Identität des Antragstellers überprüft. Unterbleibt eine solche Prüfung bzw. erfolgt sie nur oberflächlich, wird auch das Zertifikat keinen oder nur einen geringeren Nutzen haben. Nach der Registrierung erstellt die *Zertifizierungsstelle* (certification authority, CA) das Zertifikat. Werden dem Antragsteller Schlüsselträger übergeben, so erfolgt dies in der Regel durch die Registrierungsstelle. Die Registrierungsstelle nimmt auch Anträge zum Sperren von Zertifikaten entgegen.

Trust Center

Im engeren Sinne werden in einem Trust Center die besonders sicherheitskritischen Operationen in einer *Public-Key-Infrastructure (PKI)* durchgeführt. Dazu gehören die Erzeugung von Schlüsseln (Schlüsselpaaren), die Herstellung von Schlüsselträgern (bzw. deren *Personalisierung*), die Erzeugung von *Zertifikaten*, die Signatur von *Sperrlisten* und die Bereitstellung eines Dienstes zur *Onlinestatusprüfung (OCSP)*.

In einem allgemeineren Sinne bezieht sich der Begriff Trust Center auf eine vertrauenswürdige dritte Partei, die die kryptografisch gesicherte Kommunikation anderer Parteien unterstützt und ermöglicht.

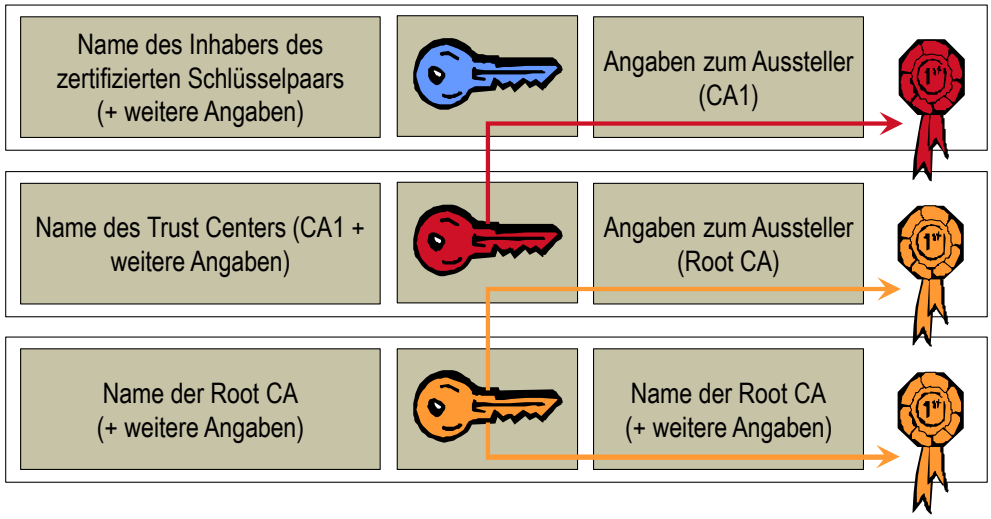


Abb. 21: Zertifizierungspfad mit Anwender-, Zertifizierungsstellen- und Root-Zertifikat

Zertifizierungspfad

Eine *Public-Key-Infrastructure (PKI)* löst das Problem der *Authentizität des öffentlichen Schlüssels*, indem sie den öffentlichen Schlüssel zusammen mit Informationen über den rechtmäßigen Besitzer (der anderen Schlüsselkomponente) in einem digital signierten Datensatz fälschungssicher speichert, der einen digitalen Ausweis darstellt und *Zertifikat* genannt wird. Allerdings muss sich der Nutzer dieses Zertifikates von dessen Echtheit durch Prüfung der Signatur überzeugen. Dafür wird der (authentische) öffentliche Schlüssel der *Zertifizierungsstelle*

(certification authority, CA) benötigt, die das Zertifikat ausgestellt hat. Dieser öffentliche Schlüssel kann wiederum in Form eines Zertifikats vorliegen, dessen Echtheit auf die gleiche Weise zu prüfen wäre. Diese in Abb. 21 veranschaulichte Kette von Zertifikaten, deren Echtheit mit öffentlichen Schlüsseln zu prüfen ist, die wiederum in anderen Zertifikaten enthalten sind, nennt man Zertifizierungspfad.

Die Kette endet an einer Wurzel mit dem Zertifikat der sogenannten **Root-CA**. Ein solches Zertifikat ist selbstbezüglich (siehe Abb. 21). Das Zertifikat bzw. der entsprechende öffentliche Schlüssel muss im System des Anwenders sicher gespeichert sein. In diesem Sinne reduziert eine *Public-Key-Infrastructure (PKI)* die Zahl der sicher zu speichernden öffentlichen Schlüssel auf einen (den der Wurzel). Siehe Abb. 22a.

Eine Wurzel (root) kann mehrere *Zertifizierungsstellen* (Domänen) und deren Nutzer unterstützen. Durch eine gegenseitige Anerkennung (**Cross-Zertifizierung** oder Überkreuz-Zertifikate) ist eine sichere Ad-hoc-Kommunikation über Domänengrenzen hinaus auch ohne eine zentrale Wurzel möglich. Siehe Abb. 22b.

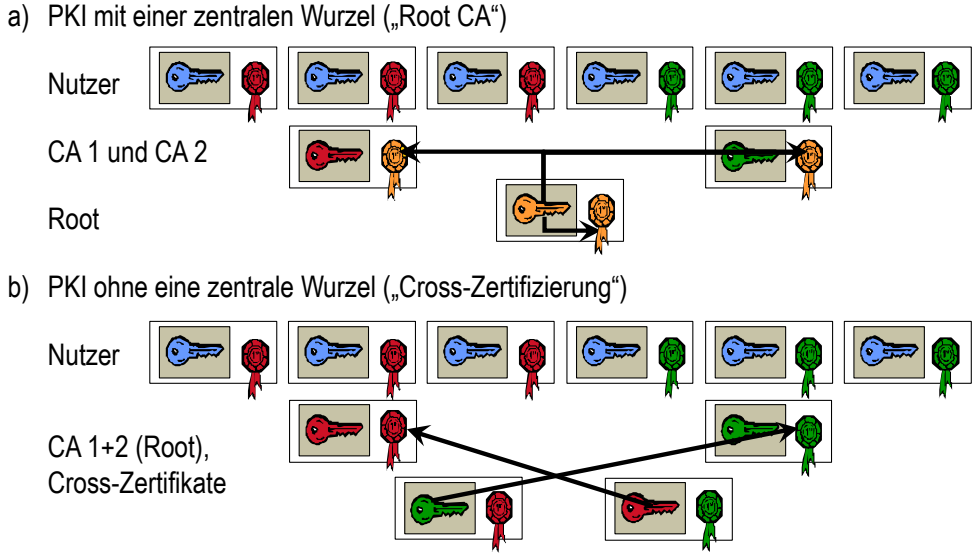


Abb. 22: Zertifizierungspfad (a) mit und (b) ohne zentrale Wurzel[84]

Zertifikatsrichtlinie

Ein **Certificate Practice Statement (CPS)** beschreibt die Verfahren und Regeln, die angewendet werden, wenn eine *Zertifizierungsstelle* (certification authority, CA) ein *Zertifikat* ausstellt (erzeugt), veröffentlicht, sperrt bzw. zurückzieht,

[84] vergleiche: Eberhard von Faber: Vorlesungsskript; Technische Hochschule Brandenburg

erneuert und archiviert. Anhand der Zertifikatsrichtlinien können Anwender einer *Public-Key-Infrastructure (PKI)* das Vertrauenswürdigkeitsniveau von Zertifikaten erkennen. Ein CPS weist auch Ähnlichkeiten mit einer Service-Beschreibung einerseits und mit einem Anwenderhandbuch andererseits auf und ist damit besonders dann von Nutzen, wenn Anwender und Zertifizierungsstelle zu unterschiedlichen Organisationen gehören.

Zertifikate unterscheiden sich hinsichtlich ihrer Anwendung, Qualität, Bereitstellung und rechtlichen Stellung. Solche Spezifika werden in einzelnen, zertifikatsspezifischen **Certificate Policies (CPs)** beschrieben.

Höherwertige Zertifikate enthalten einen Verweis auf die CPS und die CPs in Form von URLs (siehe Abb. 20, Mitte). Damit kann der Nutzer eines Zertifikates vorher die Bedingungen studieren, die der Erzeugung des Zertifikates zugrunde lagen, und dann eine Entscheidung treffen, ob er das Zertifikat (Echtheit vorausgesetzt) für seine Zwecke nutzen will.

Für den Betrieb einer PKI oder eines Trust Centers werden weitere interne Unterlagen benötigt, wie Organisationshandbücher (Abläufe, Schnittstellen, Rollen), Betriebshandbücher (Anweisungen im Betrieb), Sicherheitskonzepte und Notfallkonzepte. Diese sind im Gegensatz zur CPS und zu CPs nicht öffentlich.

Verzeichnisdienst (Zertifikate)

Ein Verzeichnisdienst in einer *Public-Key-Infrastructure (PKI)* stellt die öffentlichen Schlüssel von Nutzern in Form von *Zertifikaten* abrufbar bereit. Anwender, die Zugriff auf den Verzeichnisdienst haben, können ad hoc sicher miteinander kommunizieren, d.h., ohne vorher Schlüsselmaterial austauschen zu müssen.

Oft ist der Verzeichnisdienst mit einem weiteren Service, der **Onlinestatusprüfung (OCSP)** bzw. dem **Validierungsdienst** (der Validation Authority, VA), verbunden. Die Abkürzung OCSP steht für Online Certificate Status Protocol, wird aber oft auch für den Dienst selbst benutzt. Die Statusprüfung umfasst die Prüfung der Echtheit und der Gültigkeit, kann jedoch inhaltliche Aspekte wie die Verlässlichkeit des Anbieters und des Zertifikats selbst nicht umfassen.

Sperrliste (revocation list)

Eine Sperrliste verzeichnet *Zertifikate*, die vor Ablauf ihrer Gültigkeit zurückgezogen wurden und damit ungültig geworden sind. Sperrlisten werden von einer *Zertifizierungsstelle* (certification authority, CA) zur Verfügung gestellt. Ihre *Authentizität* (Ursprung und Integrität) wird durch eine digitale Signatur gewährleistet. Die Prüfung der Sperrliste ergänzt die Prüfung eines Zertifikats (auf Echtheit und Inhalt) vor seiner Nutzung. Alternativ kann die *Onlinestatusprüfung (OCSP)* genutzt werden, da sie die Sperrlistenprüfung einschließt, nicht jedoch die inhaltliche Prüfung des Zertifikats.

Literatur und Bildnachweise

Besonders ein solches Buch, das sich zur Aufgabe macht, Definitionen von Fachbegriffen zu geben, kann nicht geschrieben werden, ohne dass der Autor vielfältige Literatur gelesen hätte – in der langen Zeit der Tätigkeit auf diesem Gebiet, bei der Erstellung von Lehrunterlagen für Studierende und beim Schreiben dieses Buches. Die Definitionen sollen ja den Stand der Technik korrekt wiedergeben und konsensfähig sein. Das bedeutet auch, dass Begriffe und Zusammenhänge auch in anderen Veröffentlichungen so oder ähnlich vorkommen können – ja müssen.

Ab Mitte der 2000er Jahre habe ich mich beruflich mit dem Thema Identitäts- und Zugriffsmanagement in Unternehmen beschäftigt (siehe [4]). Auch habe ich eine Vorlesung zum Thema entwickelt, die ich jährlich gehalten und entsprechend aktualisiert habe (siehe [3]). Das vorliegende Kapitel kann gewissermaßen als Ausformulierung dieser Vorlesung angesehen werden.

Meine wesentlichen Quellen waren die Konferenzen der Technologieberatungsfirma Gartner (Gartner Security Summit ab 2006 sowie der Gartner IAM Summit ab 2007) und die Gartner Research-Paper (nicht öffentlich; kostenpflichtig). Beispielhaft sei die Zusammenfassung „IAM Foundations“ [1] genannt. Viele Begriffe wurden auch zum Beispiel durch das Liberty Alliance Project [2] eingeführt und standardisiert.

[1] Perry Carpenter: IAM Foundations: Part 1 - So You've Been Handed an IAM Program ... Now What?; 5 May 2010; Part 2 - Part 2: Tools and Technologies; 29 July 2010; Part 3: Developing Your IAM Plan; 6 August 2010; Part 4: Building the Business Case for IAM; Part 5: Building Your IAM Team; Part 6: Tips for Choosing an IAM Vendor; Part 7: IAM Best Practices; Part 8: IAM FAQs; Gartner

[2] Liberty Alliance Project, diverse Spezifikationen; www.projectliberty.org

[3] Eberhard von Faber: Vorlesungsskript; Technische Hochschule Brandenburg

[4] Eberhard von Faber: Identity and Access Management, Gain Agility through IAM – in Companies and Complex Supply Chains; White-Paper, T-Systems Enterprise Services, www.t-systems.com/whitepapers, October 2007; deutsche Version: Identity und Access Management (IAM), Steigerung der Agilität – in Unternehmen und komplexen Zulieferketten; Juli 2007

Elektronisches Zusatzmaterial
Die Abbildungen sind als PowerPoint-Datei kapitelweise über https://link.springer.com/ auf der Seite des eBooks abrufbar.

4 IT/TK-Services und Informationstechnologie

In den Kapiteln 4.1 bis 4.4 geht es um den Liefergegenstand der IT-Dienstleister. Deren Leistung besteht meist in der Bereitstellung eines IT-Service bzw. einer IT-Dienstleistung. Anwender haben äußerst unterschiedliche Bedarfe und Ansprüche. Das führt zu einer Vielzahl an IT-Services. Die wichtigsten Arten dieser Dienstleistungen werden erklärt und die ihnen zugrunde liegenden Architekturen vorgestellt. Bei der Aufgliederung der IT-Services spielen die Aufteilung der Verantwortlichkeiten und die Art der Nutzung durch die Anwender eine entscheidende Rolle. Dies charakterisiert die Service-Modelle und Bereitstellungsvarianten; ihr Verständnis ist wichtig für jedwede Tätigkeit als IT-Experte oder IT-Sicherheitsexperte, die über die bloße Durchführung vorgegebener, standardisierter Abläufe hinausgeht.

Das Kapitel 4.5 widmet sich dem Aufbau von Informationstechnologie, also den IT-Komponenten, die zum Teil auch als Produkte angeboten und für die Bereitstellung von IT-Services benötigt und genutzt werden. Dabei werden aber auch wichtige Zusammenhänge erklärt wie zum Beispiel die Funktionsweise verschiedener Formen der Virtualisierung und der Cloud bzw. des Cloud-Computings. Zum Abschluss wird das Wichtigste zum Thema Rechenzentrum zusammengefasst. Im Kapitel 4.6 geht es schließlich um Netzwerke. Dabei wird die Sichtweise auf Services mit der Beschreibung von Produkten und Netzwerkkomponenten verbunden.

IT-Sicherheitsexperten sollten sich nicht nur mit Bedrohungen beschäftigen und Risiken verwalten. Sie sollten sich vor allem mit dem Gegenstand beschäftigen, den sie beschützen (absichern) sollen bzw. von dem sie wollen, dass ihn jemand absichert: Dieser Gegenstand sind die IT/TK-Komponenten bzw. IT/TK-Services. Nur dafür bezahlen Anwender. Deshalb ist dieses Kapitel den Leistungen gewidmet, die Dienstleister bereitstellen. IT-Sicherheit macht man nicht ohne IT.

IT-Experten sind oft hoch spezialisiert. Bei der Beschäftigung mit den technischen Details geraten jedoch manchmal diejenigen Merkmale aus dem Blick, die für die Anwender primär wichtig sind. Die Anwender schauen auf die Funktionalitäten und die Qualitäten des gesamten Liefergegenstands. Sie nutzen oft facettenreiche Dienstleistungen, die aus dem komplexen Zusammenspiel zwischen den verschiedensten IT/TK-Komponenten einerseits und zwischen diesen und verschiedenen, auf die IT/TK bezogenen Tätigkeiten andererseits entstehen. Eine IT-Komponente macht noch keinen IT-Service.

Zusatzmaterial online
Zusätzliche Informationen sind in der Online-Version dieses Kapitel (https://doi.org/10.1007/978-3-658-33431-4_4) enthalten.

E. von Faber, *IT und IT-Sicherheit in Begriffen und Zusammenhängen*,
Edition <kes>, https://doi.org/10.1007/978-3-658-33431-4_4

4.1 Einführung und Übersicht

4.1.1 Parteien, Liefergegenstände, Dienstleistungsarten, Merkmale

Der erste Teil dieser Einführung verschafft Übersicht in vier Schritten (siehe Abb. 23). Nacheinander werden besprochen: (1) die beteiligten Parteien, (2) die Liefergegenstände und ihre prinzipiellen Unterschiede, (3) die Arten von IT-bezogenen Dienstleistungen sowie (4) die Kennzeichen oder Unterscheidungsmerkmale.

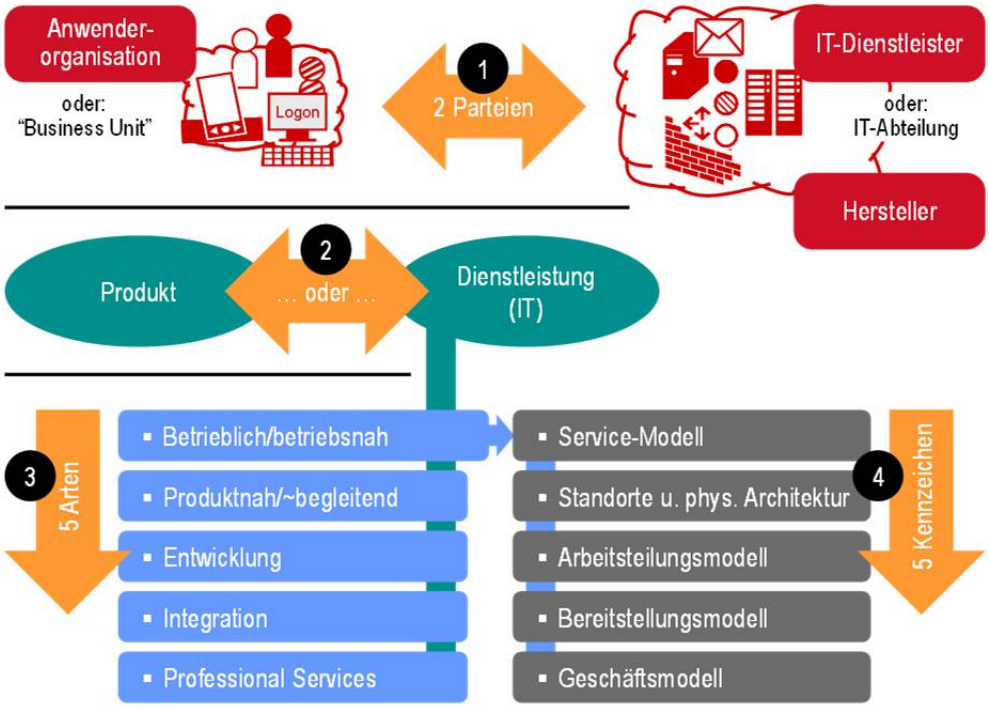


Abb. 23: Parteien, Liefergegenstand sowie Arten und Kennzeichen von IT-Dienstleistungen

Für die IT-Sicherheit ist es enorm wichtig, insbesondere die Besonderheiten der Liefergegenstände und die Kennzeichen zur Unterscheidung von IT-Services zu verstehen.

Handelnde Parteien

Die Aufgliederung der handelnden Parteien spielt eine große Rolle, weil Aufgaben und Zuständigkeiten zugewiesen werden müssen. Ohne eine klare Vorstellung der Arbeitsteilung fehlt jeglichen Spezifikationen der Anknüpfungspunkt zu deren Umsetzung, und ohne die Zuweisung der Verantwortlichkeit bleibt die Kontrolle der Umsetzung folgenlos.

Bezüglich der handelnden Parteien wird in diesem Kapitel ein einfaches Modell zugrunde gelegt mit der Anwenderorganisation bzw. dem Anwender als Konsumenten auf der einen Seite und dem IT-Dienstleister als dem Anbieter und Produzenten

auf der anderen. Daneben gibt es noch Hersteller. In konkreten Anwendungsfällen muss dieses Modell gegebenenfalls erweitert werden.

Anwenderorganisation

Anwenderorganisationen bilden die konsumierende Partei (Nachfrage), die IT-Dienstleistungen (IT-/TK-Services) als Mittel zur Unterstützung ihrer Geschäftstätigkeit nutzt. Wird „die IT" in einer Organisation (Konzern, Firma, Behörde usw.) intern von einer IT-Abteilung (einem internen *IT-Dienstleister*) zur Verfügung gestellt (Angebot), so verbergen sich hinter dem Terminus Anwenderorganisation die Geschäftseinheiten (business units) der Organisation. Häufig werden IT-Dienstleistungen von spezialisierten Firmen (externen *IT-Dienstleistern*) eingekauft. In diesem Fall bezieht sich der Begriff Anwenderorganisation auf die gesamte Organisation mit allen ihren Geschäftseinheiten (business units).

Nutzer sind Personen, die IT-Dienstleistungen verwenden. Kommt es nicht auf den Unterschied zwischen Anwenderorganisation und Nutzer an, kann der Begriff **Anwender** verwendet werden, der beides umfasst.

IT-Dienstleister

Ein IT-Dienstleister stellt als produzierende Partei (Angebot) IT-Dienstleistungen (IT-/TK-Services) im Rahmen seiner primären Geschäftstätigkeit zur Verfügung. Seine Kunden sind *Anwenderorganisationen*, wenn er den Unternehmens- bzw. Geschäftskundenmarkt bedient, und *Nutzer*, wenn er im Privatkundenmarkt tätig ist. Das Geschäftsmodell ist fast immer „one-to-many": Er stellt seine IT-Dienstleistungen also vielen Kunden in meist gleicher oder ähnlicher Form zur Verfügung.

Hersteller (manufacturer, vendor)

Der Begriff Hersteller wird im Kontext der Informationstechnologie für Firmen verwendet, die *IT-Dienstleistern* als ihren Kunden IT-Komponenten, IT-Systeme, *Produkte* und dergleichen zur Verfügung stellen. Auch *Nutzer* stellen Kunden von Herstellern dar, sofern der Hersteller den Privatkundenmarkt bedient.

Produkte und Dienstleistungen

Bevor im Folgenden beständig von Dienstleistungen bzw. Services die Rede sein wird, ist es angebracht, das Besondere herauszuarbeiten und mit herkömmlichen Vorstellungen zu vergleichen. Sind es nicht einfach Produkte, die die IT-Industrie bereitstellt? Warum ist von Dienstleistungen die Rede? Besonders im geschäftlichen Bereich ist der Unterschied wichtig, wobei es gar nicht so sehr um die Begriffe selbst geht. Doch dazu gleich später; zunächst die Definitionen.

Produkt

Ein Wirtschaftsgut, das durch Fertigung hergestellt wurde zur bestimmungsgemäßen, vorhersehbaren Verwendung. Da die Verwendung klar bestimmt ist, kann ein Produkt (im Gegensatz zur *Dienstleistung*) im Prinzip genau und vollständig spezifiziert werden.

Produkte haben einen Preis, der in der Regel in zeitlichem Zusammenhang mit der Bestellung oder Übergabe zu zahlen ist. Betriebswirtschaftlich ist die Beschaffung eines Produktes mit fixen *Kosten* verbunden, die in Form von Abschreibungen auf das Anlagevermögen anfallen. Produkte sind lagerfähig, oft weiter veräußerbar, veralten aber häufig.

Dienstleistung

Ein Wirtschaftsgut, das durch eine über einen längeren Zeitraum erbrachte Leistung erbracht wird. Der Nutzen entsteht, anders als bei *Produkten* bzw. Sachgütern, zeitgleich mit der Herstellung (Produktion) und nicht erst danach.

Im geschäftlichen Umfeld werden Dienstleistungen oft über Jahre erbracht und müssen entsprechend aufrechterhalten werden. Aber auch in kürzeren Zeiträumen kommt es zu Änderungen im Geschäft, im Markt, in der Technik, oder neue Bedrohungen und Risiken treten auf. Dienstleistungen werden also typischerweise in einem sich wandelnden Umfeld erbracht. Das führt dazu, dass sie nicht genau und nicht vollständig spezifiziert werden können. Trotzdem sind Käufer (*Anwender*) und Dienstleister, ungeachtet üblicher Ausstiegsklauseln, vertraglich eng aneinander gebunden und aufeinander angewiesen. Das hat zur Folge, dass das Verhältnis der Parteien viel enger ist als das zwischen dem Käufer und dem Hersteller eines Produktes. Dies gilt auch, wenn Produkte mit produktbegleitenden Dienstleistungen (zum Beispiel Gewährleistung) verbunden sind.

Betriebswirtschaftlich entstehen bei Dienstleistungen für den Käufer (Anwender) variable *Kosten* (laufende Kosten) und keine Anschaffungskosten.

Immer mehr Organisationen (Anwenderorganisationen) nutzen Informations- und Kommunikationstechnologie für ihre Geschäftsprozesse. Sie kaufen heutzutage jedoch immer weniger die IT-Produkte, um sie dann zu Systemen zu integrieren, die sie selbst betreiben. Stattdessen kaufen sie fertige IT-Dienstleistungen bzw. IT-Services. Umgekehrt hat sich die IT-Industrie dahingehend gewandelt, dass IT-Dienstleistungen einen immer breiteren Raum einnehmen. Häufig werden selbst Produkte in eine Dienstleistung überführt und entsprechend vermarktet, indem sie mit einem Mietmodell einschließlich eines Versprechens zur Aufrechterhaltung der Qualität versehen werden.

IT-Sicherheitsexperten müssen sich dieser Gegebenheiten bewusst sein und die marktwirtschaftlichen Realitäten und vertraglichen Konstellationen berücksichtigen. Im Folgenden wird statt IT-Dienstleistung sehr oft und später ausschließlich der synonyme Begriff IT-Service verwendet.

Eingrenzung und Übersicht

Eine grobe Einteilung könnte folgende fünf Kategorien von „Services“ verwenden:

1. Betriebliche und betriebsnahe Services: Darunter werden im Folgenden Dienstleistungen verstanden, die von einem Anwender bzw. Anwenderunternehmen direkt konsumiert werden können („customer-facing services“). Ebenfalls hinzugezählt werden Dienstleistungen, die benötigt werden, um die „customer-facing services“ herzustellen. Man spricht von „supporting services“. Diese „Services“ stellen IT-Funktionalitäten bereit und umfassen weitere Leistungen, die in direktem Zusammenhang mit Funktionen der Datenverarbeitung, -speicherung und -übertragung stehen. Das vorliegende Kapitel konzentriert sich auf diese erste Kategorie von „Services“ und wird nur diese im Detail betrachten.
2. Produktnahe und produktbegleitende Services: Hersteller von Produkten (manufacturer, vendor) stellen nicht nur das aus Hardware und Software bestehende Produkt zur Verfügung, sondern bieten verschiedene unterstützende Leistungen an, die sich auf die Inbetriebnahme, die Pflege und die Beseitigung von Störungen und Fehlern beziehen. Die Notwendigkeit, diese anzubieten, kann sich aus gesetzlichen Regelungen (zum Beispiel Gewährleistung) oder durch die Komplexität des Produktes ergeben. Oft handelt es sich aber um eine Leistung zur Entlastung des Anwenders des Produktes oder um eine Möglichkeit für den Hersteller, kontinuierliche Einnahmen zu erzielen.

Daneben gibt es weitere Leistungen, die meist einfacher zu verstehen und einzuordnen sind. Dazu gehören alle Arten von Entwicklungs- und Integrationsleistungen sowie die sogenannten „Professional Services“.

3. **Entwicklungsleistungen:**

   Der Liefergegenstand von Entwicklungsleistungen sind Pläne, Konstruktionszeichnungen und dergleichen. Entwicklungsleistungen produzieren oft auch ein Produkt bzw. einen Prototypen eines Produktes. Ein typisches Beispiel ist die Auftragsentwicklung von Software, oft auch Systems Integration bezeichnet. Der Begriff System ist sehr vielschichtig; hier bezieht er sich auf Softwarekomponenten.

4. **Integrationsleistungen:**

   Liefergegenstand von Integrationsleistungen sind Systeme, die aus einzelnen Komponenten zusammengefügt und entsprechend konfiguriert wurden. Die Integrationsleistung besteht im sachgerechten Zusammenfügen, also dem Aufbau des Systems oft einschließlich Test und Inbetriebnahme.

5. **Professional Services:**

   Professional Services umfassen viele Arten von Unterstützung durch Experten wie zum Beispiel Beratung, Bewertung, Schulung oder Projektmanagement (Wahrnehmung organisatorischer Aufgaben). Gerade der Bereich der Beratung

ist sehr vielfältig und umfasst Marktanalysen, Anbieterbewertungen, Technologiebewertungen, Entwicklung von Geschäftsplänen, Betriebsprüfung, Identifizierung von Problemen, Unterstützung bei der Problemlösung, Erarbeitung von Konzepten und Hilfe bei deren Umsetzung.

Im Folgenden wird nur die erste Gruppe (Nr. 1) detailliert betrachtet. Alle darunterfallenden Dienstleistungen werden einfach als IT-Services bzw. TK-Services oder kombiniert als IKT-Services bezeichnet.

Fünf Aspekte zum Verständnis aller IT-/TK-Services

IT- bzw. TK-Services dienen verschiedenen Zwecken und sind verschieden aufgebaut. Geht es zum Beispiel um die IT-Sicherheit von IT- bzw. TK-Services, ist es sehr wichtig zu verstehen, aus welchen Komponenten sie bestehen und wer für welche dieser Komponenten welche Verantwortung übernimmt und welche Leistung erbringt.

Will man IT- bzw. TK-Services verstehen, so hilft es, generell folgende Fragen zu stellen und zu beantworten. Sind alle Fragen beantwortet, ist der Service soweit charakterisiert, dass die Grundlagen für Diskussionen über seine IT-Sicherheit geschaffen sind:

1. Service-Modell: Welche Funktionalitäten bzw. Tätigkeiten bietet der Service und aus welchen Komponenten besteht er, um diese Funktionalitäten bereitstellen zu können? Funktionalitäten umfassen viele Formen der Verarbeitung, Speicherung und Übertragung von Daten, die letztlich nur verstanden werden können, wenn man die IT-Komponenten betrachtet, die Verwendung finden. Tätigkeiten umfassen die Entwicklung, den Betrieb, die Instandhaltung und Wiederherstellung sowie gegebenenfalls auch die Weiterentwicklung.
2. Standorte und physische Architektur: Auch wenn es in Zeiten von *Software-Defined Data Centers* altmodisch klingen mag: Für das Verständnis mancher Architekturen mit Hilfe der Informationen aus dem Service-Modell ist es mehr als nur hilfreich zu wissen, welche IT-Komponenten sich wo befinden. Wird ein (echtes) Rechenzentrum vorausgesetzt? Handelt es sich um das des IT-Dienstleisters oder das des Anwenderunternehmens? Oder stehen die IT-Komponenten einfach am Standort im lokalen Netz des Anwenderunternehmens mit Netzverbindung zum IT-Dienstleister? Ohne solche Details wird man *Hyper-Converged-Systems* und Modelle wie *Edge-Computing* kaum verstehen bzw. von anderen Lösungen unterscheiden können. Ohne den Standort (geografisch und politisch) zu kennen, wird es kaum möglich sein, die Einhaltung zum Beispiel von Gesetzen oder staatlichen Regularien einschätzen oder sicherstellen zu können.

3. Arbeitsteilungsmodell: Betrachtet man die Nutzung des IT-/TK-Service durch den/die Anwender als Ganzes und während der gesamten Vertragslaufzeit, so gibt es häufig Funktionalitäten und immer Leistungen, die der Dienstleister nicht liefert, gleichwohl sie Teil des Nutzungsszenarios sind. Für diese noch fehlenden muss der Anwender selbst sorgen oder sie anderweitig beschaffen. Selbst beim umfassendsten IT-/TK-Service muss der Anwender diesen in richtiger und sicherer Weise nutzen können, und er sollte dem Dienstleister auch melden, wenn der IT-/TK-Service fehlerhaft arbeitet oder gar nicht verfügbar ist. Oft muss der Anwender aber einen Teil der IT-Ausstattung selbst beisteuern bzw. anderweitig beschaffen. Ebenso häufig muss er Leistungen zur Instandhaltung und Wiederherstellung selbst erbringen oder den Dienstleister im Rahmen von Mitwirkungspflichten dabei unterstützen.
4. Bereitstellungsmodell: Wie wird der IT-/TK-Service bereitgestellt? Erfolgt die Bereitstellung individuell für einen Kunden oder teilen sich mehrere Kunden den Service oder Teile davon? Wie soll seine Nutzung erfolgen und welche (technischen) Voraussetzungen muss der Anwender erfüllen bzw. welche findet er vor?
5. Geschäftsmodell: Welchen Nutzer- bzw. Kundengruppen (Personen, mittelständische Betriebe, große Institutionen und Firmen) wird der IT-/TK-Service angeboten? Wie erfolgt die Bezahlung? Welche Art von Verträgen bilden die Grundlage für die Nutzung des Service?

Jeder der fünf Aspekte ist von enormer Wichtigkeit, um Maßnahmen der IT-Sicherheit planen, umsetzen, verstehen und kontrollieren zu können. Insbesondere das Arbeitsteilungsmodell wird selten richtig analysiert; aber auch das Geschäftsmodell wird häufig nicht ausreichend im Hinblick auf Auswirkungen auf IT-Sicherheit und Datenschutz untersucht.

Das erkennt man schon daran, dass „Arbeitsteilungsmodell“ und „Geschäftsmodell“ in der Literatur zur IT-Sicherheit keine feststehenden Begriffe sind bzw. gar nicht Verwendung finden. Auch der Begriff „Standort“ wird oft zu eng gefasst.

4.1.2 Einteilung der IT-/TK-Services

Abb. 24 gibt einen groben Überblick über die IT-/TK-Services und zeigt eine mögliche Einteilung in Form einer Taxonomie.

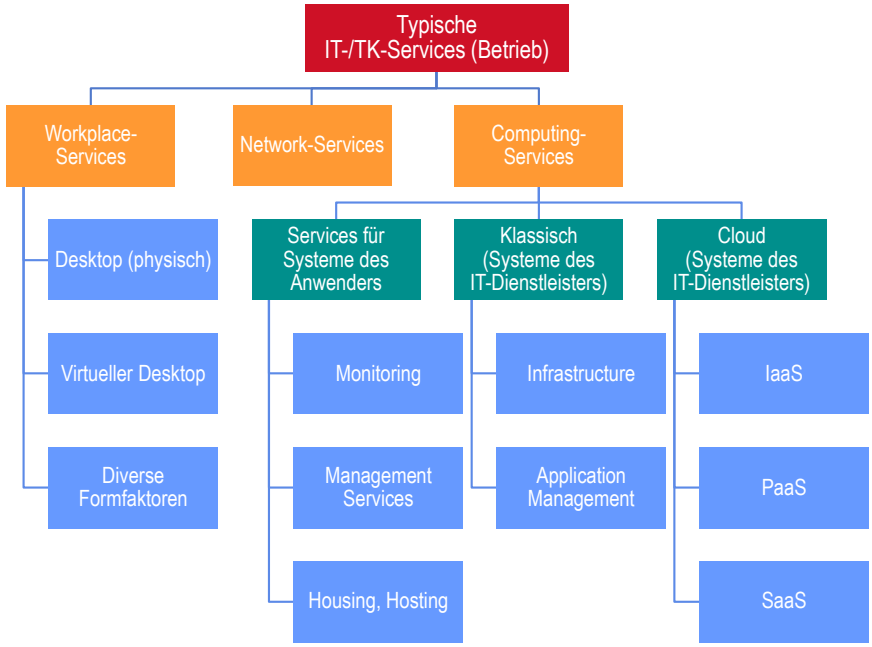


Abb. 24: Übersicht über typische betriebliche Dienstleistungen

ICT/IKT-Services, IKT-Dienstleistungen (Übersicht)

ICT bzw. IKT steht für Informations- und (Tele-)Kommunikationstechnologie. Ein ICT-Service oder IKT-Dienst bzw. eine ICT-Dienstleistung ist eine über einen längeren Zeitraum mit Hilfe von ICT/IKT erbrachte Leistung. Der Nutzen entsteht, anders als bei Sachgütern, zeitgleich mit der Produktion. Die Abkürzungen ICT und IKT sind wenig geläufig.

Man unterscheidet *Workplace-Services*, *Computing-Services* und *Network-Services*. Jede dieser Gruppen umfasst verschiedene Arten spezieller Dienstleistungen.

Workplace-Services

Workplace-Services umfassen Leistungen rund um einen Computer-Arbeitsplatz, mit dem Personen Arbeiten durchführen können. Wird ein physischer Computer wie ein Desktop, ein Notebook oder ein Tablet bzw. Smartphone als Teil der Dienstleistung zur Verfügung gestellt, so wird die benötigte Software oft darauf installiert und mitsamt der Hardware und Firmware gewartet.

Virtuelle Arbeitsplätze nutzen eine bereits vorhandene Hardware. Software und Speicher werden für die Dauer der Dienstleistung aus einem Rechenzentrum des IT-Dienstleisters heraus zur Verfügung gestellt; der Computer des Nutzers fungiert im Wesentlichen als Ein- und Ausgabegerät.

Computing-Services

Computing-Services umfassen Leistungen für den Betrieb einer Anwendungssoftware (*Anwendung*, Applikation) in einem Rechenzentrum. Bei Infrastrukturdienstleistungen stellt der IT-Dienstleister die Anwendung nicht selbst bereit, sondern betreibt diese nur mit Hilfe diverser IT- und Netzwerkkomponenten. Solche Dienstleistungen besitzen im Wesentlichen drei Leistungsparameter bzw. Grundbausteine: Rechenkapazität (compute), Speicherkapazität (storage) und Netzwerkkapazität (network). Gemessen wird die Rechenkapazität typischerweise in der Anzahl von CPU-Kernen (zum Beispiel 32) und der Größe des flüchtigen Hauptspeichers (zum Beispiel 128 Gigabyte). Die Speicherkapazität misst man zum Beispiel in Terabyte nichtflüchtigen Speichers in einem (Festplatten)-Speichersystem (storage). Dazu kommen Angaben bezüglich Aufbewahrungszeiten und der Art und Weise der Datensicherung bis hin zum Desaster-Recovery (Datenwiederherstellung im Katastrophenfall). Bei der Netzwerkkapazität wird die Bandbreite (Geschwindigkeit der Datenübertragung zwischen Computer und dessen Außenwelt in Mega- oder Gigabit pro Sekunde) angegeben.

Computing-Services werden häufig auch einfach **IT-Services** genannt. Sie sind sehr vielfältig und unterscheiden sich vor allem hinsichtlich der Leistung, die der IT-Dienstleister dem Anwender bzw. der Anwenderorganisation zur Verfügung stellt. Die →*Service-Modelle* gliedern die IT-Services und definieren die wichtigsten Gruppen oder Arten.

Network-Services

Network-Services umfassen Leistungen zur Übertragung von Daten bzw. zur Verbindung von bzw. mit Computern oder Computer-Netzen. Anwenderorganisationen benötigen in der Regel Network-Services mit garantierten Leistungsparametern (**Quality of Service, QoS**). Zu diesen Leistungsparametern können Bandbreite, Latenz und Netzwerkqualität gehören. Die *Bandbreite* betrifft die maximale Geschwindigkeit der Datenübertragung bzw. den Durchsatz (Bit pro Zeiteinheit) im Netz. Die *Latenz (latency)* betrifft die Antwortzeit (Verzögerung bis zur Antwort) bzw. die Zeit, die das Netz beansprucht, um Anfrage und Antwort zu übertragen. Mit *Netzwerkqualität* ist gemeint, wie viele Fehler bei der Datenübertragung durch das Netz verursacht werden.

Eine normale Internetverbindung hat normalerweise keine garantierten Leistungsparameter (Quality of Service, QoS), allenfalls werden typische Grenzwerte angegeben. Anwenderorganisationen sind für den reibungslosen Ablauf ihrer elektronischen Geschäftsprozesse aber in der Regel auf Garantien angewiesen. **Telekommunikationsanbieter** stellen solche Verbindungen als Netzwerk-Service oder TK-Service zur Verfügung.

Netzwerke werden ausführlich in Kapitel 4.6 behandelt.

4.2 Computing-Modelle

„Computing-Modell“ ist kein feststehender Begriff. Er wird hier verwendet, um eine erste grobe Einteilung vornehmen zu können. Das Kriterium ist hierbei die physische Verteilung und Vernetzung von Computern. Abb. 25 zeigt die fünf bzw. vier Modelle, die im Folgenden erklärt werden.

Anwendereigene Systeme (im Rechenzentrum der Anwenderorganisation) können ebenfalls Gegenstand von IT-Services eines IT-Dienstleisters sein, der in diesem Fall nur Leistungen wie die Überwachung oder die Pflege erbringt. Die Systeme selbst stellt der Anwender. Die entsprechenden IT-Dienstleistungen werden im nächsten Kapitel 4.3 behandelt.

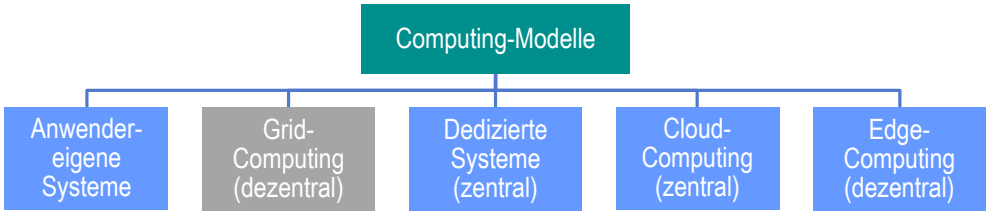


Abb. 25: Methoden zur Verteilung und Vernetzung von Computern

Im Folgenden geht es um die drei Modelle auf der rechten Seite von Abb. 25. Zusätzlich wird das Grid-Computing erklärt, obwohl es sich nicht so sehr um einen Service, sondern um eine Art der Nutzung von Computern handelt. Hier sieht man jedoch sehr schön den Unterschied zum Cloud-Computing.

Viele der genutzten Fachbegriffe wie etwa Middleware werden in Kapitel 4.5 definiert. In vielen Fällen wird darauf verzichtet, sie kursiv zu setzen, da ein genaues Verständnis dieser Termini an dieser Stelle nicht erforderlich ist.

Dediziertes System (dedicated system)

> Computersysteme mit Anwendungssoftware, Middleware, Betriebssystem und Hardware, die sich im Rechenzentrum eines IT-Dienstleisters befinden, aber nur für eine Anwenderorganisation bereitgestellt und betrieben und nur von dieser genutzt werden. Nur die Netzwerke sowie das physisch geschützte Rechenzentrum mit Klimaanlagen, Stromversorgung usw. sind geteilt (shared), werden also auch von anderen Anwendern genutzt.
>
> Dedizierte Systeme waren in den 1990er Jahren vorherrschend, als Organisationen (vor allem große Firmen) begannen, ihre IT an spezialisierte IT-Dienstleister auszulagern. Für die Auslagerung in ein Rechenzentrum des IT-Dienstleisters bzw. die Übernahme ganzer Rechenzentren wurde der Begriff **(klassisches) Outsourcing** geprägt. Erst später wurden Kosten reduziert, indem Computersysteme, die oft nur zu etwa 15% ausgelastet waren, simultan durch mehrere Anwender genutzt wurden (→*Geteiltes/Shared System*).

Dedizierte Systeme gibt es auch heute. Meist spielen bei der für dedizierte Systeme typischen Isolation Sicherheitsgründe die wichtigste Rolle.

Geteiltes/Shared System

Man spricht von einem geteilten System (shared system) oder einer geteilten Umgebung (shared environment), wenn die entsprechenden physischen IT-Systeme gleichzeitig die Daten verschiedener Anwender verarbeiten oder speichern. In vielen Fällen befinden sich auf dem physischen IT-System (wie einem *Server*) *Anwendungen* verschiedener Anwenderorganisationen. Die verschiedenen Anwender werden oft als **Mandanten** bezeichnet, da sie vom selben IT-Dienstleister unter Nutzung derselben Ressourcen versorgt werden.

Wird ein Computersystem nur von einer Anwendung oder einem Anwender genutzt, so ist dessen Auslastung oft sehr gering. Das heißt, die Leistungsfähigkeit des Computers wird meist nicht ausgeschöpft, was unwirtschaftlich ist. Soll die Auslastung der Computersysteme erhöht werden, so muss die Last der verschiedenen Anwendungen einer oder mehrerer Anwenderorganisationen dynamisch auf mehrere, physische Computersysteme verteilt werden. Ein solcher Computerverbund nutzt die →*Virtualisierung* und das „Verschieben" von Software auf andere Computer mit freien Ressourcen.

In Kapitel 4.5.1 werden die einzelnen, eingesetzten IT-Komponenten näher erklärt.

Grid-Computing

Eine Anwendung bzw. die Durchführung einer Berechnung (Datenverarbeitung) wird auf viele Rechner verteilt, die über ein Netzwerk (meist das Internet) miteinander verbunden bzw. erreichbar sind (grid), wodurch große Rechenkapazitäten erschlossen werden. Im Unterschied zum *Cloud-Computing* spielt die Rechenleistung des einzelnen Computers eine untergeordnete Rolle; es können auch leistungsschwächere Computer eingesetzt werden. Auch erfolgt die Vernetzung vorrangig über das Internet, während eine Cloud primär einen Verbund physischer Rechner innerhalb eines Rechenzentrums darstellt.

Cloud-Computing

Beim Cloud-Computing werden IT-Services in einem (zentralen) Rechenzentrum produziert und den Nutzern in der Regel über Weitverkehrsnetze wie dem Internet bereitgestellt. Im Gegensatz zu den entsprechenden klassischen IT-Services teilen sich mehrere Anwenderorganisationen bzw. deren Anwendungsprogramme (*Anwendungen*, Applikationen) nicht nur Rechenzentrum und Netze, sondern mindestens auch die physischen Computersysteme (compute) und die Speichersysteme (storage) im simultanen Betrieb. Den Anwendungsprogrammen können je nach Bedarf dynamisch Ressourcen wie Rechenkapazität und Kurzzeitspeicher zugewiesen werden. Durch die Verbindung sehr vieler Computersysteme ergibt sich eine große Elastizität hinsichtlich der für ein Anwendungsprogramm (Anwendung, Applikation) verfügbaren

Ressourcen. Dabei ist eine verbrauchsabhängige Zuweisung und Abrechnung der Kosten möglich. Die Anwendungsprogramme werden automatisiert auf den Computersystemen „installiert". In vielen Fällen wird das dazu genutzt, dass Anwender ihre Anwendungsprogramme und weitere Softwarekomponenten über ein Selbstbedienungsportal selbst verwalten, also „installieren" und starten sowie stoppen.

Wie die „Cloud" funktioniert, wird ausführlich in Kapitel 4.5.2 behandelt.

Edge-Computing

Während das Cloud-Computing mit einer Zentralisierung der Datenverarbeitung und -speicherung beim IT-Dienstleister verbunden ist, stellt Edge-Computing den gegenteiligen Trend dar. Die IT ist dezentral verteilt und befindet sich räumlich im Bereich der Anwenderorganisation. Im Unterschied zum Eigenbetrieb (on-premise) wird die IT jedoch vom IT-Dienstleister verwaltet und in der Regel auch gestellt.

Für diese (aus Sicht des IT-Dienstleisters) dezentrale Aufstellung der IT gibt es technische und rechtliche Gründe. Zu den technischen Gründen gehören a) Latenz, b) Bandbreite, c) Sicherheit, d) Anschlussmöglichkeit (connectivity) und e) Netzwerkqualität.

Latenz: Bei Anwendungen im Internet-der-Dinge (IoT) bzw. betrieblichen Anwendungen (Operational Technology, OT) gibt es harte Anforderungen an die Antwortzeit (Verzögerung bis zur Antwort) bzw. an die Zeit, die das Netz beansprucht, um Anfrage und Antwort zu übertragen. Im Bereich der einzelnen Geräte muss die Verzögerung oft unter einer Millisekunde, im Nahbereich (near edge) unter 5 Millisekunden und weiter entfernt (far edge) immer noch deutlich unter 50 Millisekunden liegen. Die **Bandbreite** betrifft die maximale Geschwindigkeit der Datenübertragung bzw. den Durchsatz (Bit pro Zeiteinheit) im Netz. Diese muss aufgrund der hohen Anzahl von Geräten bzw. des enormen Datenaufkommens sehr groß sein. Oft erfolgt eine Vorverarbeitung (preprocessing) der Daten nahe an den Geräten, um die Datenmenge frühzeitig zu verringern. Auch die Sicherheit kann ein Grund sein, die Daten bei der Anwenderorganisation zu verarbeiten. Hier spielen Kontrollmöglichkeiten die wichtigste Rolle. Hinzu kommen gegebenenfalls gesetzliche und andere Vorschriften. Auch gibt es gegebenenfalls Beschränkungen aufgrund der **Anschlussmöglichkeiten** (connectivity). Manche Geräte können aufgrund baulicher Einschränkungen zum Beispiel nur mit lokalen drahtlosen Netzen (wie WLANs) verbunden werden. Oder es werden lokale Netze genutzt, die auf bestimmte Netzanforderungen optimiert sind. Deren Vorteile würden verschwinden, wenn die Daten zwecks Verarbeitung erst an ein weiteres Netz übertragen würden. Mit **Netzwerkqualität** ist gemeint, wie viele Fehler bei der Datenübertragung durch das Netz verursacht werden. Auch hier ist damit zu rechnen, dass die Fehlerrate steigt, je komplexer und ausgedehnter die Netzwerkinfrastruktur ist.

Hyper-Converged-Systems

Bei einem hyperkonvergenten System werden Rechenkapazität (compute), Speicherkapazität (storage) und Netzwerkdienste (network) in einem einzigen kompakten physischen System zusammengefasst. Ebenfalls wird eine Control-Komponente integriert, die es dem IT-Dienstleister erlaubt, das gesamte System und alle seine aufeinander abgestimmten Komponenten über eine einzige Schnittstelle zu verwalten und zu pflegen. Hyperkonvergente Systeme zeichnen sich durch ihre hohe Effizienz der Ressourcennutzung und durch Einheitlichkeit verschiedener Schnittstellen (APIs) aus.

Hyperkonvergente Systeme haben zum Teil eine enorm große Rechenkapazität (sehr viele CPUs) und sehr große Speicherkapazitäten (Tera- bis Petabyte), sodass man sie als Mini-Rechenzentren ansehen kann. Sie sind mit *Virtualisierungs*technologien ausgestattet, sodass ein solches System eine sogenannte *Private Cloud* bildet.

Aufgrund der hohen Integration der Hardwarekomponenten ist es möglich, die Hardware durch ein zusammenhängendes System von Software zu abstrahieren und zu nutzen. Man spricht in diesem Zusammenhang auch vom →*Software-Defined Data Center (SDDC)*. Das ermöglicht eine bessere Automation. Die Möglichkeit, Module hinzuzufügen, ermöglicht einen Ausbau der Ressourcen.

4.3 Service-Modelle (IT)

Die nun folgende Unterscheidung von IT-Services nach Service-Modellen ist die wohl wichtigste. Hierbei geht es um nichts anderes als um den Liefergegenstand selbst. Allerdings sind Begriffe wie „Infrastructure“ oder „Management“ nicht sehr eindeutig bzw. eingängig, und es kommt immer wieder zu Missverständnissen und Fehlurteilen. Die hier ausgewählten Begrifflichkeiten schaffen Klarheit und zeigen, worauf es, insbesondere auch für IT-Sicherheitsexperten, ankommt. Es geht um die Arbeitsteilung und damit um Verantwortlichkeiten – auch für die IT-Sicherheit.

Bevor es um die einzelnen Service-Modelle selbst gehen kann, müssen die Begriffe IT-Stack und Service-Modell definiert werden.

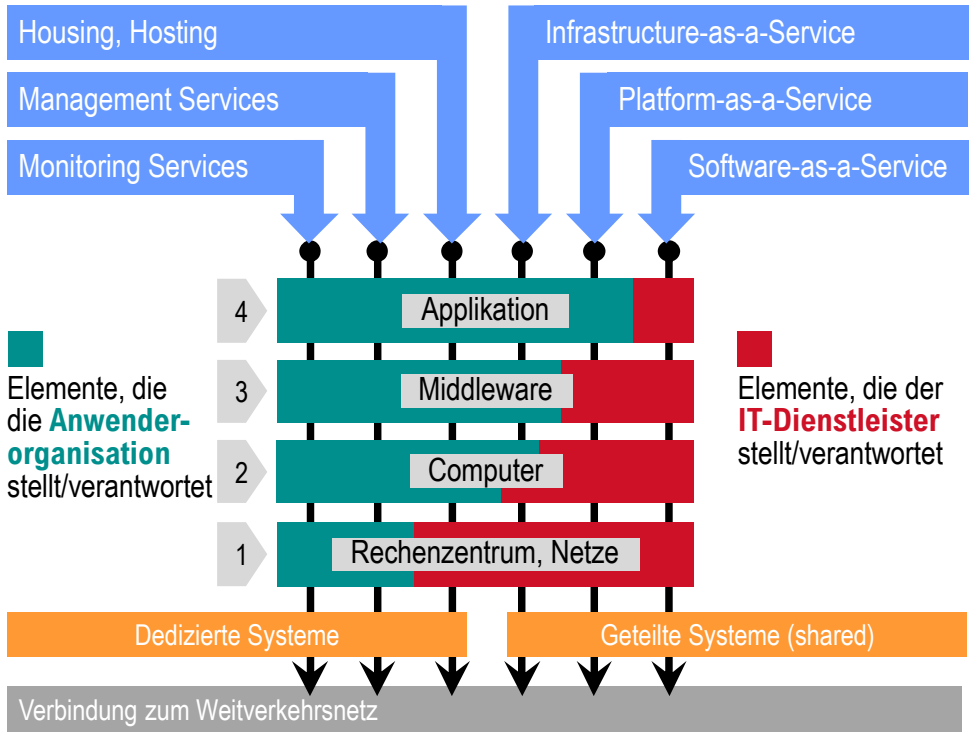


Abb. 26: Service-Modelle: Arbeitsteilung im IT-Stack[85]

IT-Stack

Eine Hierarchie von IT-Komponenten in einem Computersystem, bei dem die Anwendungsprogramme (*Anwendungen*, Applikationen) Dienste der darunterliegenden *Middleware* nutzen, die wiederum auf Funktionen des *Betriebssystems* zurückgreifen. Siehe Abb. 26 Mitte.

IT-Systeme sind generell so aufgebaut, dass sehr häufig verwendete Funktionen und solche, die allgemeinen Zwecken dienen, in Form von Unterprogrammen und IT-Komponenten gekapselt werden. Bei der Implementierung spezifischerer Funktionen wird auf diese zurückgegriffen; ihre Funktionen werden wiederverwendet. Dadurch entsteht eine Hierarchie von Elementen (Systeme, Subsysteme, Komponenten), die man sich meist als Stapel von Elementen vorstellt, bei

---

[85] vom Autor in ähnlicher Form wahrscheinlich erstmalig veröffentlicht in: Eberhard von Faber: Auslagerung von IT Services: Klassifikation und Risikomodell, Leitlinien für Anwender im "global sourcing"; E. von Faber und F. Holl (Hrsg.): The Bulletin Security Management, BSM Anwender 201, 25. Sept. 2009, ISSN 1869-2125; sowie danach in: Eberhard von Faber and Michael Pauly: User Risk Management Strategies and Models – Adaption for Cloud Computing; in: Securing Electronic Business Processes, Proceedings of the Information Security Solutions Europe, ISSE 2010, Vieweg+Teubner, Wiesbaden, 2010, ISBN 978-3-8348-1438-8, https://doi.org/10.1007/978-3-8348-9788-6_8; p. 80-90

denen die allgemeineren, wiederverwendbaren Elemente unten angeordnet sind und die eher spezifischen Funktionen bzw. Elemente oder Komponenten weiter oben liegen. Bei Computersystemen ergibt sich die bereits erwähnte Struktur des Stapels, bei dem die Anwendungen oben angeordnet sind.

Bei Mikroprozessoren (CPU) und in der Programmierung wird der Begriff **Stack** dagegen anders verwendet. Dort bezeichnet er einen Stapel von Daten (Stapelspeicher), der nach dem Prinzip „Last-in First-out (LIFO)" gefüllt bzw. geleert wird. Ebenfalls eingebürgert hat sich der Begriff Stack bei Warteschlangen, wie sie in Übertragungsprotokollen vorkommen. Dort wird der Datenstapel aber nach dem Prinzip „First-in First-Out (FIFO)" gefüllt bzw. geleert.

Service-Modell

Das Service-Modell ist ein Charakteristikum eines IT-Service. Es gibt verschiedene Service-Modelle. Jedes Service-Modell charakterisiert, welche Tätigkeiten Bestandteil der Dienstleistung sind und welche IT-Komponenten Funktionalitäten bereitstellen, die direkt Teil der Dienstleistung sind. Hinsichtlich der Tätigkeiten, Funktionalitäten und IT-Komponenten wird stark abstrahiert, sodass sich etwa ein Dutzend Typen bzw. Modelle unterscheiden lassen. Abb. 26 zeigt einige Beispiele.

Unabhängig vom Service-Modell ist der →*IT-Stack* (Schichten 1-4 in Abb. 26) immer vollständig: Anwendungen/Applikationen (4) benötigen in vielen Fällen Middleware (3). Beide Schichten nutzen Funktionen eines Betriebssystems und werden auf physischen Computern ausgeführt (2), die sich in einem Rechenzentrum befinden und mit Netzwerken verbunden sind (1). Die Aufteilung kann auch etwas anders gewählt werden. Gedanklich sollte man den IT-Stack (IT-Stapel) noch um Tätigkeiten bzw. betriebliche und betriebsnahe Services ergänzen wie zum Beispiel die Überwachung (Monitoring) und die Pflege (Management). Auch solche Tätigkeiten sind immer zu erbringen.

Die Service-Modelle unterscheiden sich darin, für welche IT-Komponenten und Tätigkeiten der IT-Dienstleister die Verantwortung trägt. Da der IT-Stack immer vollständig ist und auch die meisten Tätigkeiten immer zu erbringen sind, muss der Anwender bzw. die Anwenderorganisation für die fehlenden IT-Komponenten und Tätigkeiten sorgen. In diesem Sinne definiert das Service-Modell auch das **Arbeitsteilungsmodell**: Meist trägt die Anwenderorganisation zum Beispiel für die Anwendungssoftware (*Anwendung*, Applikation, Schicht 4 in Abb. 26) die Verantwortung. Sie wird auf der Infrastruktur und im Rechenzentrum (Schicht 1) des IT-Dienstleisters ausgeführt. Service-Modelle unterscheiden sich dann weiterhin darin, für welche Teile der IT-Infrastruktur der IT-Dienstleister die Verantwortung trägt.

Bei den Service-Modellen *Monitoring-Services* und *Management-Services* wird der gesamte IT-Stack samt Rechenzentrum (Schicht 1-4) von der Anwenderorganisation gestellt bzw. zumindest gegenüber dem IT-Dienstleister verantwortet.

Der IT-Dienstleister bietet Tätigkeiten (Leistungen) zu dessen Überwachung bzw. Pflege. In diesem Sinne liefert das Service-Modell auch Informationen zu den Standorten der IT-Komponenten bzw. zur physischen Architektur. Siehe Abb. 26.

Infrastructure-as-a-Service (IaaS)

Ein *Service-Modell*, bei dem der IT-Dienstleister ein Minimum an IT-Komponenten bereitstellt, die es dem Anwender erlauben, seine eigene Anwendungssoftware betreiben zu lassen. Der zur Verfügung gestellte IT-Stack enthält physische Server (Computer) und Zugang zu einem Speicher (storage). Eine Zeit lang war der Begriff **Utility-Computing** gebräuchlich.

Der Anwender kombiniert seine Anwendungssoftware (Anwendung, Applikation) und gegebenenfalls zusätzliche Middleware mit einem Betriebssystem zu einem Paket, das als →*Virtuelle Maschine (VM)* bzw. *Container* auf dem physischen Server zur Ausführung gebracht wird. Die Installation, Ausführung und Stilllegung dieses oberen Teils des *IT-Stacks* (VM) wird durch die *Virtualisierungs*schicht (*Hypervisor*) ermöglicht, die der IT-Dienstleister auf dem physischen Server installiert hat und ebenfalls verwaltet und pflegt. Die Installation, Ausführung und Stilllegung übernimmt entweder der Anwender über ein Selbstbedienungsportal (self-service portal) des IT-Dienstleisters, oder der IT-Dienstleister erledigt dies für die Anwenderorganisation mit Hilfe eigener Systeme.

Meist bietet der IT-Dienstleister ein fertig konfiguriertes Betriebssystem als zusätzlichen optionalen Service an. Beim persistenten Speicher (storage) hat der Anwender neben der Kapazität meist auch die Wahl zwischen verschiedenen Backupmöglichkeiten und Verfügbarkeitsklassen.

In fast allen Fällen bezieht sich Infrastructure-as-a-Service (IaaS) auf einen echten *Cloud-Computing*-Service. Das heißt, dass viele physische Server (Computer) bzw. deren *Virtualisierungs*schicht (*Hypervisor*) miteinander verbunden bzw. vernetzt sind. Abhängig von Anforderungen an Rechenleistung (compute) und flüchtigem Hauptspeicher (Kurzzeitspeicher) können auf einem physischen Server (Computer) mehrere Virtuelle Maschinen (VM) laufen. Reichen die Ressourcen des Servers (Computers) nicht mehr aus, so können VM (workload) im laufenden Betrieb auf andere Server (Computer) mit freien Ressourcen umgezogen werden. Dadurch können die physischen Ressourcen optimal ausgenutzt und dem Anwender dynamisch und skalierbar zur Verfügung gestellt werden.

Abhängig vom *Bereitstellungsmodell* teilen sich verschiedene Anwender gegebenenfalls ein physisches System.

Platform-as-a-Service (PaaS)

Ein *Service-Modell*, bei dem der IT-Dienstleister so gut wie alle Komponenten des IT-Stacks bereitstellt, jedoch nicht die Anwendungssoftware (Applikation). Der

zur Verfügung gestellte IT-Stack enthält physische Server (Computer), Zugang zu einem Speicher (storage) und diverse *Middleware* wie Laufzeitumgebungen (runtime environments; zum Beispiel .Net oder Java), verschiedene *Datenbanksysteme* sowie manchmal ganze Programmier- bzw. Entwicklungsumgebungen. Platform-as-a-Service (PaaS) ist etwa gleich *Infrastructure-as-a-Service (IaaS)* plus Betriebssystem und teils komplexer Middleware.

Der Anwender steuert die Installation, Ausführung und Stilllegung seiner Anwendungssoftware über eine Schnittstelle, die der IT-Dienstleister anbietet.

Platform-as-a-Service (PaaS) ist ein *Cloud-Computing*-Service. Das heißt, dass viele physische Server (Computer) bzw. deren *Virtualisierungs*schicht (*Hypervisor*) miteinander verbunden bzw. vernetzt sind. Dadurch können die physischen Ressourcen optimal ausgenutzt und dem Anwender dynamisch und skalierbar zur Verfügung gestellt werden. Dies wird wie für *Infrastructure-as-a-Service (IaaS)* beschrieben realisiert. Abhängig vom *Bereitstellungsmodell* teilen sich auch hier verschiedene Anwender gegebenenfalls ein physisches System.

Software-as-a-Service (SaaS)

Ein *Service-Modell*, bei dem der IT-Dienstleister eine Anwendungssoftware (Applikation) bzw. deren Nutzung einschließlich Speicher (storage) und weiterer gegebenenfalls benötigter Softwarekomponenten zur Verfügung stellt. Nutzer verwenden ihre Arbeitsplatzcomputer oder mobilen Systeme, um über Netze auf die Anwendung zuzugreifen, die der Anwender nicht selbst beschaffen und auch nicht selbst verwalten und pflegen muss.

Software-as-a-Service (SaaS) ist ein *Cloud-Computing*-Service. Das bedeutet, dass die Software und die dazu verwendeten Ressourcen, wie zum Beispiel Speicher, den Anwendern dynamisch und in der Regel auch skalierbar zur Verfügung gestellt werden.

Besonders bei Angeboten für Konsumenten, aber in der Regel auch bei webbasierten Anwendungen im Geschäfts- und Großkundenmarkt, nutzen verschiedene Anwender eine Instanz der Software, die hierfür mandantenfähig ausgelegt ist. **Mandantenfähigkeit** ist eine Architektureigenschaft der Software und bedeutet, dass sie Zugang, Nutzung und Datenspeicherung für jeden Anwender getrennt verwalten kann. Hinsichtlich der Nutzung unterstützen manche Angebote anwenderspezifische Konfigurationen. Die Daten der verschiedenen Anwender sind in einer gemeinsamen Datenbank, einer gemeinsamen Datenbank mit anwenderspezifischem Schema oder in einer anwenderspezifischen Datenbank gespeichert.

Um die für Cloud-Computing-Services typische *Skalierbarkeit* zu erreichen, wird die Software auf mehrere Server (Computer) verteilt oder die Software wird für hinzukommende Anwender(-gruppen) auf anderen noch freien Servern (Computern) installiert.

Die Fähigkeit, die Software vielen Anwendern zur Verfügung zu stellen, kann alternativ zur Mandantenfähigkeit der Software auch durch *Virtualisierung* erreicht werden, die ebenfalls für eine Trennung der Anwender sorgt. Hier erhält jede Anwenderorganisation eine eigene Instanz der Software. Die verschiedenen Instanzen sind in Form Virtueller Maschinen (VM) voneinander getrennt, wie es bei *Infrastructure-as-a-Service (IaaS)* üblich ist. Solche Modelle weisen Ähnlichkeiten zu früheren Angeboten der Application Service Provider (ASP) auf, die Software bzw. deren Nutzung in herkömmlicher Weise zur Verfügung stellen, also nicht als Cloud-Computing-Service. Andere Bezeichnungen sind Software-on-Demand oder manchmal auch Mietsoftware.

Housing

Der IT-Dienstleister stellt Fläche im Rechenzentrum zur Aufstellung von Serverschränken (racks) sowie Strom- und Notstromversorgung (uninterruptable power supply, UPS) und Klimatisierung zur Verfügung. Natürlich wird auch ein Anschluss an ein Weitverkehrsnetz benötigt, damit die Anwenderorganisation die eigene Rechentechnik (IT) auch nutzen kann. Die Anwenderorganisation nutzt auch die physischen Sicherheitsmaßnahmen des →*Rechenzentrums* wie Zutrittskontrolle, Brand- und Blitzschutzanlagen, Videoüberwachung, Bewachung usw. Zusätzliche Maßnahmen wie eigene Räume, Trennung in Brandschutzzonen und Käfige sind oft optional erhältlich.

Für die Unterbringung eigener Rechentechnik in einem fremden Rechenzentrum ist auch der Begriff **Co-location** gebräuchlich.

Hosting

Beim Hosting stellt der IT-Dienstleister physische Server (Computer) in seinem Rechenzentrum bereit. Als zusätzliche, nicht enthaltene Leistung bietet er meist weitere IT-Komponenten wie Betriebssysteme, Speicher (storage) und andere Software wie Datenbanken und Webserver an. Daraus und aus Komponenten, die der Anwender bereitstellt, entsteht eine anwenderspezifische IT-Lösung, die auch nur von diesem genutzt wird.

Mit anderen Anwendern (Kunden des IT-Dienstleisters) werden nur die Rechenzentrumsinfrastruktur und der Anschluss an ein Weitverkehrsnetz geteilt, über das der Anwender die eigene Anwendung bzw. IT-Lösung nutzen kann. Zur Rechenzentrumsinfrastruktur gehören Strom- und Notstromversorgung (uninterruptable power supply, UPS), Klimatisierung und physische Sicherheitsmaßnahmen, wie sie unter *Housing* aufgezählt sind.

Beim **Web-Hosting** stellt der Anwender die Internet-Applikation oder die Daten (zum Beispiel für eine Webseite) zur Verfügung. Der IT-Dienstleister übernimmt den Betrieb. Der Begriff lässt offen, ob die zugrunde liegende IT-Infrastruktur exklusiv für die Anwenderorganisation zur Verfügung gestellt

wird (*Dediziertes System*) oder ob sie mit anderen Anwendern geteilt wird, wie es beim *Cloud-Computing* üblich ist.

Management Services

Im Bereich der IT-Services versteht man unter „Management" diverse Tätigkeiten, die der Verwaltung, Bereitstellung, Aufrechterhaltung und der Verbesserung von IT-Services dienen. Daher spricht man auch von →*IT-Service-Management (ITSM)*.

Management-Services im engeren Sinne umfassen solche Tätigkeiten, ohne dass der IT-Dienstleister die Funktionalitäten und IT-Komponenten bereitstellt.

Entsprechend versteht man unter dem Begriff *Managed Services* solche, bei denen der IT-Dienstleister die Funktionalitäten einschließlich der dafür notwendigen IT-Komponenten bereitstellt und diese auch verwaltet und pflegt. Die Verwaltung ist Teil des IT-Services.

Für die Aktivitäten rund um Planung, Umsetzung und Integration, also bis zur Erstbereitstellung, hat sich kein einheitlicher Begriff eingebürgert. Man kann die Prozesse, Abläufe und Aktivitäten während der Entwicklung und Implementierung aber auch als Teil des IT-Service-Managements ansehen.

Managed Service (verwalteter IT-Service)

Managed Services sind IT-Services, die IT-Funktionalitäten zur Verarbeitung, Speicherung und Übertragung von Daten umfassen und bei denen der IT-Dienstleister die dafür notwendigen IT-Komponenten als Teil der Dienstleistung ebenfalls verwaltet und pflegt.

Unmanaged Services sind IT-Services, die IT-Funktionalitäten zur Verarbeitung, Speicherung und Übertragung von Daten umfassen, bei denen der IT-Dienstleister die dafür notwendigen IT-Komponenten jedoch nicht verwaltet und pflegt bzw. dafür kein Serviceversprechen gibt.

Monitoring-Services

Ein *Service-Modell*, bei dem der IT-Dienstleister fremde IT-Systeme überwacht. IT-Services müssen ständig überwacht werden, um Beeinträchtigungen der Service-Qualität erkennen und Gegenmaßnahmen ergreifen zu können. Diese Überwachung hinsichtlich der Verfügbarkeit und der Einhaltung von Leistungsparametern ist Gegenstand der Monitoring-Services.

Diese können auch die Überwachung hinsichtlich der IT-Sicherheit einschließen (siehe auch →*Security Operations Center, SOC)*. Dann werden *Sicherheitsereignisse* (security events) laufend analysiert. Kommt die Analyse zu dem Ergebnis, dass es sich um einen *Sicherheitsvorfall* (security incident) handeln könnte, wird in der Regel nur die beauftragende Organisation alarmiert, die dann die weiteren Schritte übernimmt. Monitoring-Services sind automatisiert, erfordern jedoch immer manuelle Eingriffe und die Bewertung von Experten.

4.4 Bereitstellungsmodelle (Cloud)

Parameter wie der Produktionsort, die Form des Netzzugangs und sogar die Art der Nutzer beeinflussen beim *Cloud-Computing* das *Risiko*profil, meist auch das *Sicherheits*niveau sowie immer die *Vertrauenswürdigkeit*, die letztlich darüber entscheidet, ob Anwender den IT-Service verwenden und für welchen Zweck.

Abb. 27 zeigt drei Bereitstellungsmodelle und den Eigenbetrieb zum Vergleich. Die vier Eigenschaften werden bei den Erklärungen eine wichtige Rolle spielen. Doch zunächst wird der Begriff Bereitstellungsmodell selbst erklärt. Auf die Hybrid-Clouds und sogenannte Community-Clouds wird ebenfalls eingegangen.

Modell → Eigenschaft ↓	On-premise (Eigenbetrieb)	Private Cloud	Virtual Private Cloud	Public Cloud
Anwender (Nutzer)	Betreiber selbst	assoziiert	assoziiert	ohne Bindung
	vertrauenswürdig	vertrauenswürdig	vertrauenswürdig	unbekannt
Anwender teilen Cloud mit	niemandem	niemandem	mehreren	vielen
Zugang (Netz)	lokales Netz, Campus-Netz u.a.	Weitverkehrsnetz mit beschränktem Zugang	Weitverkehrsnetz mit beschränktem Zugang	öffentliches Internet
Produktionsort (Lokation)	bei der Anwender-organisation	beim IT-Dienstleister	beim IT-Dienstleister	beim IT-Dienstleister

Abb. 27: Bereitstellungsmodelle beim Cloud-Computing (Eigenbetrieb zum Vergleich)

Bereitstellungsmodell (deployment model)

Bereitstellungsmodelle sind unterschiedliche Formen der Nutzung und der Nutzungsmöglichkeiten von *Cloud-Computing*-Systemen. Sie unterscheiden sich nicht primär hinsichtlich ihres technischen Aufbaus und der integrierten Sicherheitsmaßnahmen, sondern darin, a) welchen Nutzergruppen die IT-Services angeboten werden, b) in wieweit Teile der IT gemeinsam genutzt werden (shared), c) wie der Zugang dazu erfolgt und d) wo die Produktion und Datenverarbeitung und -speicherung erfolgt. Unterschiede in diesen vier Eigenschaften führen zu einem unterschiedlichen Risikoprofil.

Bei den Nutzergruppen wird zum Beispiel unterschieden zwischen Firmenkunden, die dem IT-Dienstleister bekannt sind und als verlässlich gelten, und der nicht näher definierten Allgemeinheit. Hinsichtlich der gemeinsamen bzw. geteilten Nutzung von IT (shared) sollte es eigentlich keine Unterschiede geben, es werden jedoch auch sogenannte private Infrastrukturen als Cloud bezeichnet, die nur von einem Unternehmen genutzt werden. Die Art des Zugangs hängt mit dem Produktionsort zusammen. Die Clouds sind über das Internet, spezielle

Weitverkehrsnetze oder Unternehmensnetze (Intranet) erreichbar. Die IT befindet sich beim IT-Dienstleister oder beim Anwenderunternehmen.

Die gängigsten Bereitstellungsmodelle sind *Private Cloud*, *Virtual Private Cloud*, *Public Cloud* und *Hybrid Cloud*. Zum Vergleich siehe auch *Edge-Computing* und *Hyper-Converged-Systems*.

Private Cloud

Eine Private Cloud ist ein komplexes, aus sehr vielen Komponenten bestehendes System für das *Cloud-Computing*, das ein *IT-Dienstleister* für eine *Anwenderorganisation* betreibt. Das System ist komplex und besteht aus sehr vielen Komponenten. IT-Dienstleister und Anwenderorganisation schließen einen meist individuellen Vertrag und arbeiten im Rahmen der Service-Erbringung sehr eng zusammen.

Der IT-Dienstleister stellt IT-Services genau einer Anwenderorganisation bzw. den von ihr autorisierten Nutzern bereit, wobei sich die für die IT-Services benötigten Computersysteme im Rechenzentrum des IT-Dienstleisters befinden und nur für die eine Anwenderorganisation verwendet werden. Der Zugang erfolgt über ein (sicheres) Weitverkehrsnetz mit beschränktem Zugang. Dabei kann es sich um ein spezielles Hochgeschwindigkeitsnetz eines Netzbetreibers für solche geschäftlichen Anwendungen oder um ein Virtual Private Network (VPN) handeln.

Während sich bei einer typischen Cloud mehrere Anwenderorganisationen insbesondere die physischen Computersysteme (compute) teilen, ist dies bei der Private Cloud nicht der Fall. Das im Vergleich zu anderen Cloud-Modellen bessere Risikoprofil zählt zu den Vorteilen der Private Cloud.

Die Einschränkung auf eine Anwenderorganisation bedeutet aber, dass die Anwenderorganisation dem IT-Dienstleister die gesamte Private Cloud und ihr Management unabhängig von ihrer Auslastung vergüten muss. Im Vergleich zu dedizierten Systemen ergeben sich bei einer genügend großen und vielschichtigen Anwendungslandschaft aber trotzdem beträchtliche *Skaleneffekte*, und es kommt eingeschränkt auch zu einer Elastizität hinsichtlich der Ressourcen, weil Belastungsspitzen einer Anwendung durch den Minderbedarf anderer Anwendungen ausgeglichen werden können.

Beauftragt die Anwenderorganisation keinen externen, sondern einen internen zur eigenen Organisation gehörenden IT-Dienstleister, so spricht man auch von einer **internen Cloud**.

Virtual Private Cloud

Eine Virtual Private Cloud ist ein komplexes, aus sehr vielen Komponenten bestehendes System für das *Cloud-Computing*, mit dessen Hilfe ein *IT-Dienstleister* IT-Services für mehrere *Anwenderorganisationen* bereitstellt. Die physischen Computersysteme werden gemeinsam genutzt (shared). Der IT-Dienstleister

und die jeweilige Anwenderorganisation schließen einen Vertrag und arbeiten im Rahmen der Service-Erbringung zusammen.

Der IT-Dienstleister stellt IT-Services mehreren genau bekannten Anwenderorganisationen bzw. den von diesen autorisierten Nutzern bereit, wobei sich die für die IT-Services benötigten Computersysteme im Rechenzentrum des IT-Dienstleisters befinden und gleichzeitig für mehrere Anwenderorganisationen verwendet werden. Der Zugang erfolgt über ein (sicheres) Weitverkehrsnetz mit beschränktem Zugang. Dabei kann es sich um ein spezielles Hochgeschwindigkeitsnetz eines Netzbetreibers für solche geschäftlichen Anwendungen oder um ein Virtual Private Network (VPN) handeln.

Im Vergleich zu dedizierten Systemen und zur *Private Cloud* sind beträchtliche Skaleneffekte und eine große Elastizität hinsichtlich der Ressourcen möglich, weil Belastungsspitzen einer Anwenderorganisation oder einer Anwendung durch den Minderbedarf anderer Anwenderorganisationen bzw. den Minderbedarf von deren Anwendungen ausgeglichen werden können.

Public Cloud

Eine Public Cloud ist ein komplexes, aus sehr vielen Komponenten bestehendes System für das *Cloud-Computing*, mit dessen Hilfe ein *IT-Dienstleister* IT-Services für in der Regel sehr viele Anwender bereitstellt. Zu den Anwendern können Personen und jede Art von Organisation gehören. Sie teilen sich alle IT-Systeme, die für die Service-Erbringung benötigt werden (shared). Der Zugang erfolgt über das öffentliche Internet.

Der Vertrag zwischen IT-Dienstleister und Anwender kommt in der Regel durch das Akzeptieren der Allgemeinen Geschäftsbedingungen (AGB) des IT-Dienstleisters zustande. Eine Zusammenarbeit im Rahmen der Service-Erbringung ist in der Regel nicht vorgesehen. Der IT-Dienstleister stellt die IT-Services sehr vielen Anwendern (Nutzern, Anwenderorganisationen) bereit, über die er in der Regel keine Informationen besitzt, die über den standardisierten Vertragsabschluss hinausgehen bzw. zu dessen Erfüllung direkt notwendig sind.

Hybrid Cloud

Eine Hybrid Cloud ist kein einzelnes System für das *Cloud-Computing*, sondern die Bezeichnung für die parallele Nutzung von IT-Services aus einer *Private Cloud*, *Virtual Private Cloud* und/oder *Public Cloud*.

Jede der genutzten Cloud-Umgebungen behält dabei die für sie charakteristischen Eigenschaften, d.h., welchen Nutzergruppen die IT-Services angeboten werden, welche Teile der IT gemeinsam genutzt werden (shared), wie der Zugang dazu erfolgt und wo die Produktion und Datenverarbeitung und -speicherung erfolgt.

Community Cloud

Eine Community Cloud entspricht von der Konstruktion und vom Nutzungsmodell weitgehend einer *Virtual Private Cloud*. Der einzige Unterschied besteht darin, dass die Gruppe der Anwender weiter eingeschränkt ist auf bestimmte Organisationen, die zu einer Branche, einer Wertschöpfungskette o.ä. gehören oder deren Anforderungen sich decken hinsichtlich IT-Sicherheit, *Compliance*, Technik o.ä.

Eine Community Cloud wird von einem beauftragten IT-Dienstleister (spezialisierte IT-Firma oder IT-Abteilung eines Mitglieds der „Community") nach diesen Anforderungen betrieben und befindet sich in dessen Rechenzentrum oder auf einer dafür angemieteten Rechenzentrumsfläche (*Housing*).

4.5 Informationstechnologie (Technik)

Es ist sehr wichtig, dass sich auch IT-Sicherheitsverantwortliche mit den verschiedenen IT-Services und ihren Schattierungen auskennen, denn es sind die IT-Services, auf die sich die Anforderungen der Anwender beziehen. Dieser direkte Servicebezug scheint allgemeingültigen Standards wie ISO/IEC 27001/2[86] oder dem ISF Standard of Good Practice[87] zu fehlen; aber letztlich geht es nur um die IT-Services, unter all den potentiell möglichen, die der Anwender konsumiert. Die Sicherheitsarchitektur *ESARIS* stellt den Bezug zu den IT-Services an den Anfang und entsprechende Werkzeuge dafür bereit.

Die Kenntnis dieser IT-Services ist aber nicht ausreichend. Deshalb werfen wir in diesem Kapitel einen Blick unter die Motorhaube oder in den Maschinenraum und schauen uns an, aus welchen Komponenten die IT-Services aufgebaut sind und wie die Komponenten zusammenwirken. Denn nur die Kenntnis aller Komponenten und der Informationsflüsse zwischen ihnen ermöglicht es, mögliche Sicherheitsprobleme zu erkennen und geeignete Sicherheitsmaßnahmen auszuwählen (siehe dazu Kapitel 2.1).

Wir verwenden das in Abb. 28 dargestellte, generische Architekturmodell (physische Sicht).[88] Es baut auf einem einfachen Modell mit drei Bereichen auf:

---

[86] ISO/IEC 27001 – Information technology – Security techniques – Information security management systems – Requirements; 2013
ISO/IEC 27002 – Information technology – Security techniques – Code of practice for information security management; 2013

[87] Information Security Forum (ISF): The ISF Standard of Good Practice for Information Security 2018; https://www.securityforum.org, 338 pages

[88] IT-Architekturen zeigen sehr oft eine funktionale Sicht, die in mehreren Schichten (meist horizontal) aufgebaut ist, sowie zentrale oder übergreifende Funktionen, die oft etwas abgesetzt zum Beispiel am Rand (vertikal) zu sehen sind. Das hier verwendete generische

1. IT beim Anwender (links in Abb. 28): Anwender nutzen ihre Endgeräte und eventuell zusätzlich weitere IT-Services, die mit Hilfe von IT-Komponenten erbracht werden, die sich in dem lokalen Netz befinden, an das das Endgerät angeschlossen ist. Die Anwender greifen mit ihren Endgeräten (mobile und stationäre) aber auch auf entfernte, zentrale IT-Services zu.

2. IT im Rechenzentrum (rechts in Abb. 28): Die zentralen IT-Services werden mit Hilfe von IT-Komponenten wie Servern produziert, die sich in einem Rechenzentrum befinden.

3. Netzwerke (Abb. 28, Mitte bzw. unten in Blau): Die notwendige Verbindung zwischen Endgeräten (1) und der IT im Rechenzentrum (3) stellen Netzwerke wie das Internet her.

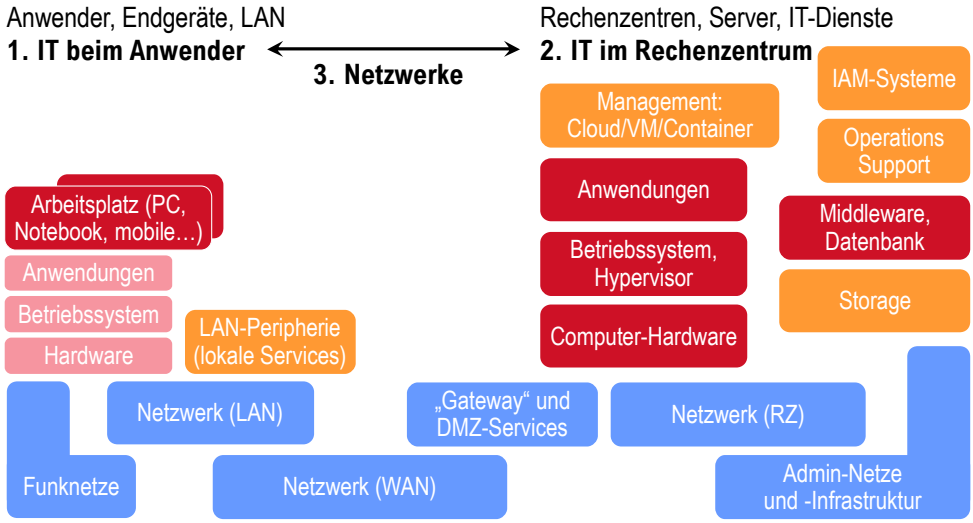


Abb. 28: Generisches Architekturmodell der Informationstechnologie (physische Sicht)[89]

Auf beiden Seiten befinden sich also Computersysteme, die Informationen verarbeiten und speichern. In Abb. 28 sind die primären Computersysteme (links) bzw. deren Komponenten (rechts) in Rot dargestellt. Bei der Betrachtung der *Service-Modelle* (Kapitel 4.3) wurde bereits der →*IT-Stack* eingeführt (siehe auch Abb. 26, Seite 98). Die Computersysteme beinhalten den kompletten IT-Stack, der im Kern durch die

Modell ist allgemeiner und komponentenorientiert, wobei die Komponenten allgemeine, sich wiederholende Funktionen wahrnehmen.

89 Die Darstellung geht auf die „ESARIS Security Taxonomy“ zurück, die 2010 firmenintern entwickelt und erstmals 2012 veröffentlicht wurde in: Eberhard von Faber and Wolfgang Behnsen: A Systematic Approach for Providers to Deliver Secure ICT Services; in: ISSE 2012 Securing Electronic Business Processes, Highlights of the Information Security Solutions Europe, ISSE 2012, Springer Vieweg, Wiesbaden, 2012, ISBN 978-3-658-00332-6, https://doi.org/10.1007/978-3-658-00333-3_9; p. 80-88

rot dargestellten IT-Komponenten (rechts in Abb. 28) und die darunterliegenden Netze (blaue Kästchen) gebildet wird. Der IT-Stack wiederholt sich bei den Endgeräten (rote Kästchen links in Abb. 28) prinzipiell. Auch bei den meisten zusätzlichen, in Gelb dargestellten Komponenten handelt es sich in Wirklichkeit um solche Computersysteme mit einer speziellen Software (zum Beispiel: einen File-Server als lokaler Service im LAN). Ihr innerer Aufbau wird hier nicht betrachtet.

Im Folgenden werden einige der am häufigsten verwendeten Begriffe im Bereich IT bzw. IT-Komponenten erläutert. Die Netzwerke und deren Komponenten (blaue Kästchen in Abb. 28) werden in Kapitel 4.6 behandelt.

4.5.1 Server und sonstige Komponenten

Host

Computersystem, das einen Endpunkt in einem Netzwerk bildet und nicht Teil des Netzes selbst ist, also keinen Netzknoten (node) darstellt. Meist handelt es sich um einen *Server* oder einen Arbeitsplatzrechner (*Client*) wie zum Beispiel einen PC. Ein Host-Computer dient zur Ausführung einer *Anwendung*, die er gewissermaßen als „Gastgeber bewirtet“ (englisch: Host = Gastgeber).

Server

Computersystem, das Funktionalitäten für viele andere Computersysteme bereitstellt, wobei letztere als **Clients** („Kunden“) eine Anfrage stellen, die vom Server („Bediener“) bearbeitet und beantwortet wird. Dieses **Client-Server**-Paradigma entstand mit der zunehmenden Vernetzung von Computern und der Verlagerung von Aufgaben bzw. Funktionalitäten an eine zentrale Stelle (Zentralisierung der IT). Client-Rechner sind meist **Arbeitsplatzrechner**, die über eine Eingabemöglichkeit (Tastatur, Bildschirmtastatur, Maus usw.) und eine Ausgabe (Bildschirm) verfügen. Demgegenüber werden Server über ein Netzwerk ferngesteuert. Sie stehen typischerweise in einem Rechenzentrum und verfügen weder über eine physische Tastatur noch über einen Bildschirm.

Server nehmen meist eine bestimmte Aufgabe wahr. Entsprechend spricht man zum Beispiel von einem Anwendungs-Server, wenn er allgemein Anwendungen betreiben soll, oder von einem Web-Server, wenn er Web-Seiten ausliefern und Web-Anfragen beantworten soll. Es gibt weiterhin zum Beispiel Datenbank-Server, File-Server, Mail-Server, Print-Server usw. Der Begriff Server ist dahingehend unscharf, als dass er in manchen Fällen (Beispiel: Anwendungsserver) nur die Komponenten umfasst, die später die Software mit der anwendungsspezifischen Funktionalität aufnehmen, und in anderen Fällen letztere bereits Teil des Servers sind (Beispiel: File-Server, Print-Server).[90]

---

[90] Server-Komponenten: in Rot rechts in Abb. 28

Häufig wird auch eine einzelne Software als Server bezeichnet, wenn sie mit einer anderen Software wie oben beschrieben interagiert, die als Client operiert.

Anwendung, Anwendungssoftware, Applikation (application)

Eine Anwendung (auch: Anwendungssoftware oder Applikation) ist Software, die den Endanwender als Konsumenten oder als Teil eines geschäftlichen Arbeitsablaufs direkt bei der Erledigung spezifischer Aufgaben unterstützt. Die Anwendung befindet sich ganz oben im *IT-Stack*. Sie dient dem eigentlichen Zweck, für den das Computersystem betrieben wird; während darunterliegende Software-Layer lediglich unterstützende Funktionalitäten bereitstellen.

Man kann Anwendungen in „Allzwecksoftware" und „Business-Software" einteilen. Zur ersten Gruppe gehören zum Beispiel Standard-Bürosoftware (Schreiben, Präsentieren, Rechnen), E-Mail und Kalender und Kontaktverwaltung sowie Programme für das Projekt- und Dokumentenmanagement. Die zweite Gruppe von Anwendungsprogrammen dient der Beschleunigung und Verbesserung von Geschäftsprozessen oder geschäftlichen Vorgängen und ermöglicht oft, ganz neue Geschäftsmöglichkeiten zu erschließen und zu nutzen. Dadurch finden die geschäftlichen Tätigkeiten und ihre Ergebnisse ihren Niederschlag in digital gespeicherten und verarbeiteten Informationen, weshalb man von **Digitalisierung** spricht. Diese „Business-Software" ist oft sehr spezifisch für eine Anwenderorganisation und ihre aktuelle Geschäftstätigkeit. Sie wird daher kundenspezifisch entwickelt, wobei oft auch standardisierte Basiskomponenten zum Einsatz kommen, die entsprechend konfiguriert und ergänzt werden. Beispiele solcher Anwendungsprogramme sind Lösungen für die Ressourcenplanung (ERP), das Kundenbeziehungsmanagement (*Customer Relationship Management, CRM*) und das Lieferkettenmanagement (SCM).

Middleware

Die Middleware stellt Funktionen bereit, die viele *Anwendungen* (Anwendungssoftware) benötigen, die aber nicht durch das *Betriebssystem* bereitgestellt werden. Daher werden diese Funktionen in Programmpakete gebündelt, die wie das Betriebssystem einmal installiert und regelmäßig aktualisiert werden. Die Middleware befindet sich logisch „zwischen" Anwendung und Betriebssystem, was ihren Namen erklärt. Beispiele sind Java-Runtime-Environment (JRE) und .Net (gesprochen Dot-Net). Middleware steht in der Regel allen installierten Anwendungen zur Verfügung. Doch es gibt Ausnahmen, da auch *Datenbanken* zur Middleware gerechnet werden.

Betriebssystem (operating system)

Das Betriebssystem ermöglicht es, *Anwendungen* (und *Middleware*) auf einem Computer zu installieren und zu nutzen. Dazu stellt das Betriebssystem eine Vielzahl von Funktionen zur Verfügung, die von der Ein- und Ausgabe (Tastatur, Maus und Bildschirm) über die Verwaltung von Dateien und Verbindungen

(Netze) bis hin zum Anschluss von Peripheriegeräten (wie Druckern) und entfernten Servern einschließlich ihrer Dateien und Dateistrukturen reichen.

Computer wie zum Beispiel PCs weisen Unterschiede in Bezug auf ihre Hardware auf. Sie werden darüber hinaus mit unterschiedlichen Peripheriegeräten verbunden und genutzt (wie Druckern). Um dies zu ermöglichen, wird gerätespezifische Software installiert, die **Treiber** genannt werden. Bei quelloffenen Betriebssystemen wie Linux wird manchmal auch der Betriebssystemkern (kernel) selbst angepasst, damit das Betriebssystem auf einer bestimmten Computerhardware lauffähig ist.

Damit das Betriebssystem auf einem Computer installiert und später jeweils gestartet werden kann, stattet der Hersteller des Computers diesen mit einer **Firmware** aus, die fest (englisch: firmly) im Computer integriert ist. Bei PCs hieß diese Software früher **BIOS** (Basic Input Output System), heute **UEFI** (Unified Extensible Firmware Interface), wobei es sich bei letzterem genauer gesagt nur um die Software-Schnittstelle zwischen Betriebssystem und der eigentlichen Firmware handelt.

Damit Fehler beseitigt und Verbesserungen implementiert werden können, bieten die Hersteller des Betriebssystems, der Peripheriegeräte und der Computer-Hardware die Möglichkeit an, die entsprechende Software zu aktualisieren (Update).

Bei einfachen bzw. stark integrierten Computersystemen lassen sich Firmware und Betriebssystem oft gar nicht genau voneinander trennen. Das Betriebssystem und manchmal auch die Anwendungen sind zum Beispiel „fest" eingebaut. Gerade bei Massenprodukten für das Internet-der-Dinge[91] (IoT-Geräte) führt dies häufig dazu, dass Aktualisierungsmöglichkeiten nicht oder nur eingeschränkt zur Verfügung stehen bzw. genutzt werden. Solcherlei Verhältnisse stellen Probleme für die IT-Sicherheit dar.

Moderne Betriebssysteme insbesondere für *Arbeitsplatzrechner* (workplace computer) enthalten oft eine Reihe von *Anwendungen*, die im eigentlichen Sinne nicht Teil des Betriebssystems sind, aber mit diesem ausgeliefert werden.

Hardware (Computer)

Die Elektronik eines Computers (Server oder Arbeitsplatzrechner) enthält eine Hauptplatine (motherboard, main board), auf die elektronische Schaltkreise (Chips), Steckverbinder und andere Bauelemente aufgelötet und dadurch miteinander verbunden werden. Der wichtigste Schaltkreis ist die **CPU** (Central Processing Unit), die die Software ausführt und mit internen und extern

---

[91] IoT: Internet of Things (Internet der Dinge). Gegenstände des täglichen Lebens, im öffentlichen Raum und in Bereichen wie dem Gesundheitswesen werden mit Computertechnik ausgestattet und über Netzwerke mit zentralen Anwendungen verbunden.

angeschlossenen Geräten kommuniziert. Ein sogenannter Chipsatz, das heißt weitere Chips, die untereinander und mit der CPU abgestimmt sind, übernehmen spezielle Funktionen und verbinden die CPU mit diversen Geräten (Speicher, Laufwerke, Netzwerke, USB, Ein- und Ausgabegeräte) über spezielle Bussysteme. Auf der Hauptplatine befindet sich ein Festwertspeicher mit der *Firmware* (*BIOS* bzw. *UEFI*), die der Computer beim Einschalten ausführt. Spezielle Steckverbinder nehmen die Module mit dem flüchtigen Speicher (RAM) auf, andere ermöglichen die Verbindung mit einer Festplatte, einer Grafikkarte oder einem anderen Gerät wie einer Tastatur, einem Netzwerk oder einem USB-Gerät.

Dem verwendeten Prozessor entsprechend gibt es im Wesentlichen zwei unterschiedliche Architekturen: x86/x64 und ARM. Software (einschließlich Betriebssystem) ist abhängig von dieser Architektur und nicht kompatibel (austauschbar).

Datenbank

Eine Datenbank ist ein System, das Daten in strukturierter Weise speichert und zu verarbeiten und abzurufen gestattet. Eine Datenbank besteht aus dem **Datenbankmanagementsystem (DBMS)** und der eigentlichen Datenbank bzw. der Datenbankbasis mit den Daten. Die meisten Datenbanksysteme sind relationale Datenbanken mit einem „Relational Data Base Management System (RDBMS)“. Die Daten sind dabei in Tabellen enthalten, die aus Zeilen und Spalten bestehen. Jede Zeile stellt einen Eintrag (record) dar; die einzelnen Spaltenwerte in jeder Zeile heißen Attribute (attributes) des Eintrags. Jede Zeile einer Tabelle besitzt einen Identifikator (key). Beziehungen (relations) werden dadurch hergestellt, dass eine Tabelle eine zusätzliche Spalte erhält, die Identifikatoren (keys) einer anderen Tabelle enthält. Die Tabellen, die Bedeutung der Einträge und Attribute sowie die Verbindung durch Beziehungen bilden zusammen das **Datenbankmodell**.

Anwendungen greifen auf die Daten in einer Datenbank über eine standardisierte Schnittstelle (API) zu, das heißt, sie senden bestimmte Befehle an das DBMS und erhalten als Antwort entsprechende Daten. Die Befehle umfassen solche für das Auffinden von Daten bzw. Informationen, für das Schreiben und die Veränderung von Daten und für die Verwaltung der Datenbank. Die bekannteste Syntax einer solchen Schnittstelle ist SQL.

Bei vielen Anwendungen ist die Festlegung eines Datenbankmodells bereits ein wichtiger Schritt bei der Entwicklung der entsprechenden Anwendung. Von **strukturierten Daten** spricht man, wenn diese in Datenbanken entsprechend einem vorab definierten Datenbankmodell abgelegt sind. Daten in Dateien, werden als **unstrukturierte Daten** bezeichnet.

Wichtige Funktionen des DBMS umfassen die Sicherstellung der Datenintegrität und die Umsetzung von Zugriffsrechten.

Storage (-System)

Ein großer, persistenter (nicht-flüchtiger), zentraler Speicher in einem Rechenzentrum. Ein Storage-System besteht aus sehr vielen Festplatten (FDD), die aber auch als Flashspeicher ausgeführt sein können, bei dem die Daten in Chips gespeichert sind (SSD). Der zentrale Storage wird von sehr vielen Computersystemen (Servern bzw. Anwendungen) zur Speicherung von Daten genutzt, sodass die physischen Server dafür keine eigene Festplatte (FDD, SSD) mehr besitzen müssen.

Die Zentralisierung des Speichers hat viele Vorteile bezüglich der Ausfallsicherheit und des Backups. Die Zentralisierung wird aber notwendig, sobald statt *dedizierter Systeme* geteilte Systeme (shared) zum Einsatz kommen, wie es beim *Cloud-Computing* der Fall ist. Abhängig von der Auslastung der Computersysteme und den Leistungsanforderungen der Anwendungen wird eine Anwendung nämlich gegebenenfalls auf ein anderes physisches Computersystem verschoben. Die zentrale Speicherung der Daten der Anwendung in einem Storage-System erleichtert bzw. ermöglicht einen solchen Umzug, da nur die Verbindung zum Storage auf das neue System übertragen werden muss.

Es gibt grundsätzlich zwei Arten von Storage: *Network Attached Storage (NAS)* und *Storage Area Network (SAN)*.

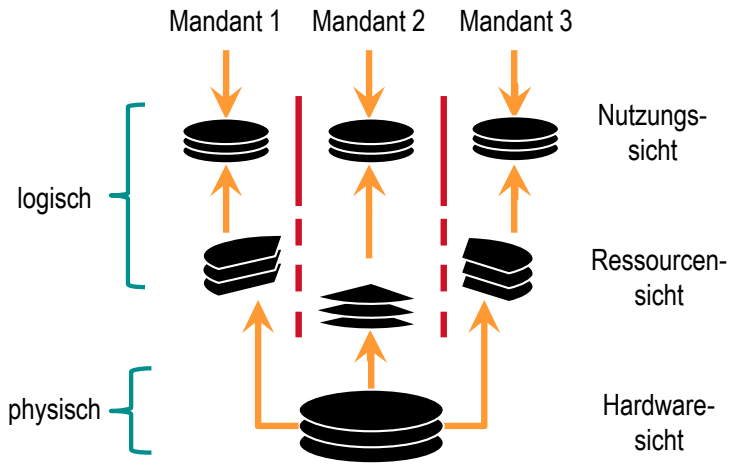


Abb. 29: Storage-Virtualisierung – Veranschaulichung

Network Attached Storage (NAS)

Beim Network Attached Storage (NAS) stellt das Computersystem (Server) zum Storage-Laufwerk (volume) eine Verbindung her (mount), um Zugriff auf dort gespeicherte Dateien (files) zu erhalten. Das Dateisystem (file system) befindet sich im Storage und wird von dort „exportiert". Mittels **Storage-Virtualisierung** (siehe Abb. 29) kann der Storage bzw. der Speicher in Form von Dateisystemen zwischen mehreren bzw. vielen Anwendern (Mandanten) aufgeteilt werden.

Dazu werden „virtual filers“ bzw. „virtual file systems (VFS)“ genutzt. Das gesamte Storage-System besteht aus vielen wirklichen Dateisystemen, die die Daten der Mandanten enthalten. Jedes wirkliche Dateisystem wird mit dem logischen bzw. virtuellen Netzwerk (VLAN) verbunden, das einem Mandanten zugeordnet und für diesen reserviert ist (NAS, links in Abb. 30). Nur die Computersysteme in diesem Netz können auf diesen Teil des Storage (mit dem Dateisystem) zugreifen, die Dateisysteme anderer Mandanten bleiben verborgen. Durch diese Storage-Virtualisierung kann jeder Mandant das Storage-System ansprechen als bestünde es nur aus einem, nämlich seinem eigenen Dateisystem bzw. den damit verwalteten Daten.

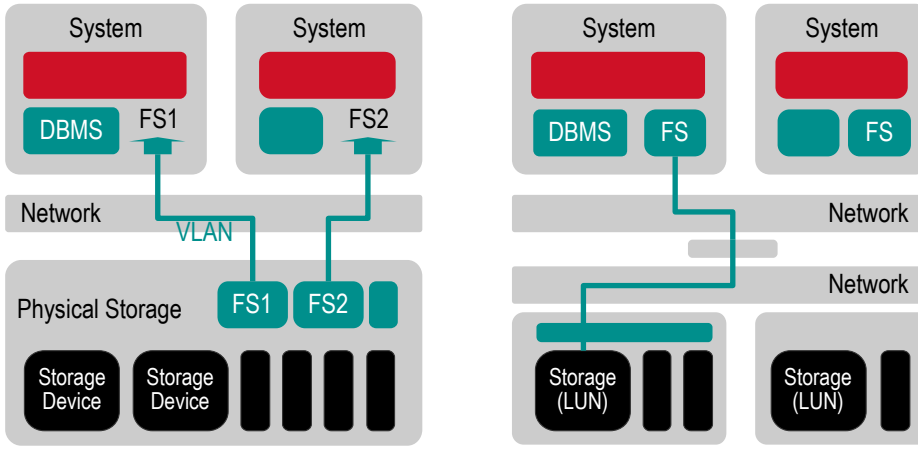


Abb. 30: Network Attached Storage (NAS, links) und Storage Area Network (SAN, rechts)[92]

Storage Area Network (SAN)

Bei einem Storage Area Network (SAN) (rechts in Abb. 30) stellt das Computersystem (Server) zum Storage-System eine Verbindung über ein Netzwerk (zum Beispiel Fibre Channel) her, um Zugriff auf dort gespeicherte Speicherblöcke zu erhalten. Das Dateisystem (Verwaltung der Dateien) befindet sich auf dem Computersystem (Server). Das Storage ist in verschiedene logische Einheiten (LUNs) geteilt, die den Speicher zwischen mehreren bzw. vielen Anwendern (Mandanten) aufzuteilen gestatten.

Storage-Systeme integrieren meist Funktionen für die Datensicherung. Dabei gibt es grundsätzlich zwei verschiedene Methoden. Beim vollständigen Sichern wird der gesamte Datenbestand auf ein anderes Medium (Festplatten oder

[92] Eberhard von Faber and Wolfgang Behnsen: Secure ICT Service Provisioning for Cloud, Mobile and Beyond (ESARIS: The Answer to the Demands of Industrialized IT Production Balancing Between Buyers and Providers); Springer Vieweg, Wiesbaden 2017, 383 pages, 159 figures, ISBN 978-3-658-16481-2, 2nd updated and extended Edition, https://doi.org/10.1007/978-3-658-16482-9; modifiziert

Magnetbänder) kopiert. Beim inkrementellen Sichern (snapshot integrated) werden Veränderungen aufgezeichnet. Beim Wiederherstellen (recovery) werden alle Veränderungen abgearbeitet, um den Zustand wiederherzustellen. Eine echte *Sicherheitskopie (Backup)* entsteht hierbei erst, wenn der gesamte Inhalt des Mediums (einschließlich aller Snapshots) auf ein anderes Medium kopiert wird und dort nicht den gleichen Risiken ausgesetzt ist. Für eine genauere Erklärung siehe →*Data backup and recovery*.

4.5.2 Virtualisierung und Cloud

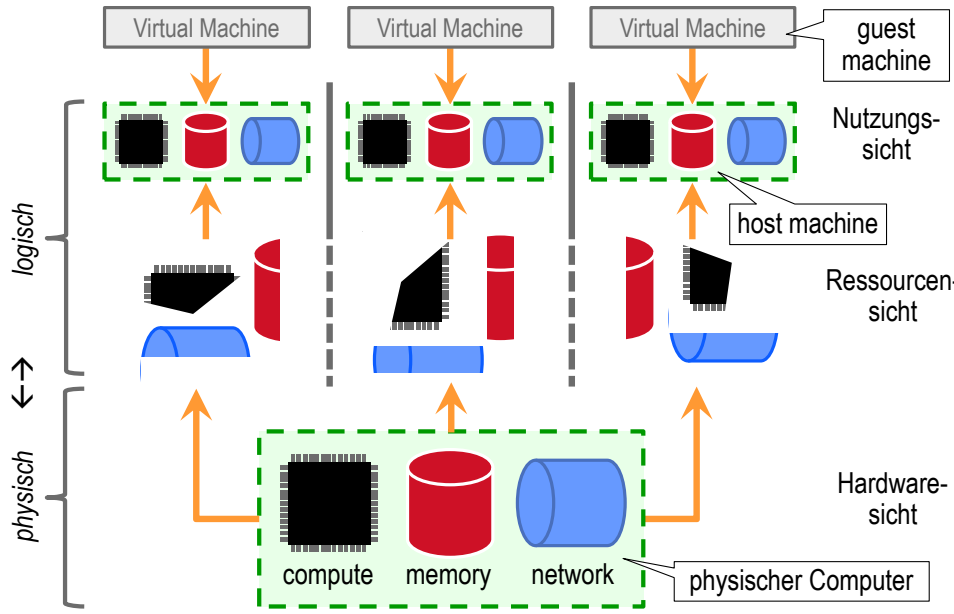


Abb. 31: Server-Virtualisierung – Veranschaulichung und Wirkungsweise der Virtualisierungsschicht (Virtual Machine Monitor bzw. Hypervisor)

Virtualisierung (virtualization)

Bei der (vollständigen) Virtualisierung (siehe Abb. 31) erzeugt eine **Virtualisierungsschicht** (Software) aus einer physischen Instanz mehrere logische Instanzen, die viele oder alle Eigenschaften der physischen Instanz besitzen. Software, die eine logische Instanz verwendet, kann (im Idealfall) nicht feststellen, ob sie eine logische oder die physische Instanz nutzt und dass es noch andere logische Instanzen gibt, die anderweitig genutzt werden.

Durch die Virtualisierung können physische Ressourcen besser genutzt und ausgelastet werden. Mitunter wird auch angestrebt, dass die logischen Instanzen eine bessere Kompatibilität bieten als die physischen.

Bei der **Server-Virtualisierung** wird die Virtualisierungsschicht als *Virtual Machine Monitor (VMM)* oder →*Hypervisor* bezeichnet. Dieser ist auf einem physischen Server installiert und erzeugt mehrere logische Instanzen dieses

Computersystems (host machines), die jeweils wie eigenständige Computersysteme erscheinen und entsprechend genutzt werden können. Siehe Abb. 31.

Bei der *Storage-Virtualisierung* wird ein physisches Speichersystem (*Storage)* in mehrere, logische Abteilungen (Einheiten) geteilt. Die Kommunikation mit einer solchen logischen Instanz erfolgt wie mit einem kompletten (physischen) Storage-System. Die Verbindung zwischen Anwender (Mandant) und zugehöriger logischer Instanz (Storage) erfolgt durch Konfiguration des Netzwerkes.

Bei der **Netzwerk-Virtualisierung** werden Datenströme verschiedener Anwender (Mandanten) in einem physischen Netzwerk getrennt, ohne dass dies vom Anwender beeinflusst werden kann. In Rechenzentren werden die lokalen Netze (LANs) in mehrere, *virtuelle lokale Netzwerke (VLANs, Virtual Local Networks)* aufgeteilt, die jeweils nur von einem Anwender (Mandanten) verwendet werden. Die Aufteilung erfolgt durch Anbringung von Schildchen (tagging). In Weitverkehrsnetzen funktioniert *MPLS (Multiprotocol Label Switching)* im Prinzip ähnlich.

Bezüglich der Virtualisierung auf Betriebssystemebene siehe →*Container*.

Emulation

Bei der Emulation wird im Unterschied zur *Virtualisierung* eine logische Instanz erzeugt, die andere Eigenschaften hat als das zugrunde liegende physische System. Es wird auch meist nur eine logische Instanz erzeugt. Bei der Emulation wird das Ziel verfolgt, die Eigenschaften eines Systems in die Eigenschaften eines anderen Systems zu übersetzen, um zum Beispiel Software ausführen zu können, die für ein physisches System entwickelt wurde, das nicht verfügbar ist.

Hypervisor

Ein Hypervisor oder **Virtual Machine Monitor (VMM)** ist eine Software, die die *Virtualisierungsschicht* bei der Server-*Virtualisierung* bildet. Mit einem Hypervisor können auf einem physischen Computersystem gleichzeitig mehrere *Virtuelle Maschinen (VM)* (Gastmaschinen) laufen, die wie eigene Computersysteme erscheinen und logisch vollständig voneinander getrennt sind. Siehe Abb. 31.

Ähnlich wie ein *Betriebssystem* verwaltet der Hypervisor die Virtuellen Maschinen, die jedoch selbst eine vollständige Computerinstallation darstellen und aus Betriebssystem und Anwendungen bestehen. Der Hypervisor verteilt die Ressourcen der Hardware (Rechenkapazität (compute), Speicherkapazität (storage) und Netzwerkkapazität (network)) dynamisch auf die laufenden Virtuellen Maschinen (VMs) (Gastmaschinen).

Durch diese dynamische Ressourcenzuteilung können physische Ressourcen besser genutzt und ausgelastet werden. Sie ist eine der Grundlagen für das *Cloud-Computing*. Zur Funktionsweise siehe unter →*Cloud-Management*. Daneben unterstützt der Hypervisor weitere Funktionen wie das Laden, Starten und

Stoppen von Virtuellen Maschinen und die Speichersynchronisation. Derartige Funktionen werden vom Cloud-Management-System über die Konsole des Hypervisors aufgerufen.

Virtuelle Maschine (VM) (virtual machine)

Eine sogenannte Virtuelle Maschine stellt eine Arbeitslast (workload) für einen virtualisierten Server dar und enthält neben der *Anwendung* und der zugehörigen *Middleware* auch ein *Betriebssystem*. Eine VM kann als Gastsystem (guest machine) angesehen werden, das auf einer virtuellen „host machine" läuft, die ein *Hypervisor* für diese VM (auf einem physischen Server) erzeugt hat. Siehe Abb. 31.

Eine Virtuelle Maschine wird auf dem Server nicht in herkömmlicher Weise installiert. Vielmehr wird ein lauffähiger Speicherabzug (image) erstellt und durch den Hypervisor in den Hauptspeicher kopiert und gestartet.

Container

Bei Containern steht die Portabilität (Anwendbarkeit auf verschiedenen Laufzeitumgebungen) im Vordergrund. „Container-Images" werden dazu zur Laufzeit umgewandelt und angepasst. Ein Container enthält die ausführbare Anwendung, Middleware, Werkzeuge und Bibliotheken und Einstellungen, also Software (code) und deren Abhängigkeiten.

Auf einem physischen Computersystem (Server) können mehrere Container ausgeführt werden. Sie teilen sich das Betriebssystem bzw. dessen Kern. Die verschiedenen Container werden isoliert bzw. voneinander getrennt, indem sie vom Betriebssystem als getrennte Prozesse mit eigenem Anwenderbereich (user space) ausgeführt werden. Das Betriebssystem oder eine Erweiterung des Betriebssystems weist den Containern Ressourcen zu und steuert den Zugriff auf Geräte. Mit Hilfe dieser **Virtualisierung auf Betriebssystemebene (OS-Level Virtualization)** können Container separiert und deren Kommunikation untereinander erlaubt und gesteuert werden.

Anhand von Abb. 32 und dem Begriff „Cloud-Management" soll nun die Funktionsweise einer „Cloud" skizziert werden.

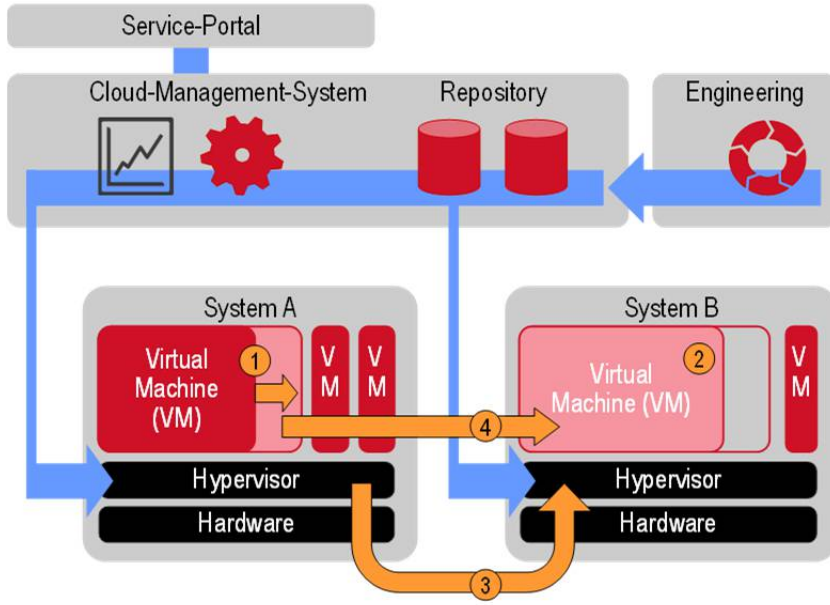


Abb. 32: Cloud-Management und Funktionsweise der Cloud[93]

Cloud-Management

Eine Cloud-Installation besteht aus sehr vielen physischen Systemen auf denen sehr viele *Virtuelle Maschinen (VMs)* ausgeführt werden. Der Ressourcenbedarf jeder einzelnen VM kann variieren. Es ist die Aufgabe des Cloud-Managements, alle VMs vertragsgemäß zu betreiben und dabei sicherzustellen, dass die Auslastung der physischen Computersysteme stets optimal ist. Nur dann können möglichst viele VMs auf einer Infrastruktur betrieben werden.

Zu den wesentlichen Aufgaben bei der Verwaltung bzw. dem Betrieb einer Cloud-Infrastruktur gehören (a) die Erzeugung von virtuellen Maschinen (VMs) auf einem Server, (b) die Zuweisung bzw. Anpassung von Ressourcen für die VM, (c) die Verschiebung einer VM und (d) die Außerbetriebnahme einer VM. Dies erfolgt über ein Cloud-Management-System (siehe Abb. 32).

Ausführbare Software (code image) für eine VM wird durch Entwickler (engineering) erzeugt und zur Verfügung gestellt und abrufbar gehalten (repository). Dazu gehört meist auch ein „golden image" für das Betriebssystem sowie weitere Komponenten (wie Datenbanken und andere Middleware). Die Anwendung wird in vielen Fällen von der Anwenderorganisation gestellt. Die

[93] Eberhard von Faber and Wolfgang Behnsen: Secure ICT Service Provisioning for Cloud, Mobile and Beyond (ESARIS: The Answer to the Demands of Industrialized IT Production Balancing Between Buyers and Providers); Springer Vieweg, Wiesbaden 2017, 383 pages, 159 figures, ISBN 978-3-658-16481-2, 2nd updated and extended Edition, https://doi.org/10.1007/978-3-658-16482-9; modifiziert

Zusammenstellung der Komponenten erfolgt in der Regel über ein Service-Portal, das die Administratoren des IT-Dienstleisters oder Experten der Anwenderorganisation bedienen. Die Virtuelle Maschine (VM) wird erzeugt, indem das lauffähige Image mit allen ausgewählten Software-Komponenten an den Hypervisor des physischen Zielsystems (System A in Abb. 32) übertragen und von diesem in den Hauptspeicher kopiert und gestartet wird.

Die Zuweisung von Ressourcen bzw. ihrer Maximalwerte erfolgt auf die gleiche Weise. (In Abb. 32 soll die Breite der VM ein Maß für den Ressourcenverbrauch sein.) Im Rahmen der vertraglichen Zusicherung weist der Hypervisor den VMs die benötigten Ressourcen dynamisch zu (siehe (1) in Abb. 32).

Können keine weiteren Ressourcen auf dem Ursprungssystem (System A) mehr bereitgestellt werden, so wird eine Kopie der VM (siehe (2) in Abb. 32) auf einem anderen physischen Computer (System B) erzeugt, der noch über ausreichend Ressourcen verfügt. Diese neue VM bleibt zunächst inaktiv. Allerdings werden die beiden Hypervisoren veranlasst, den Speicherinhalt (Daten) der VM von System A in den Speicher der VM auf dem System B zu kopieren und laufend zu synchronisieren (siehe (3) in Abb. 32). Nun wird die VM auf dem System B gestartet und die Netzwerkverbindung mit dem Anwender von System A auf das System B umgeschaltet (siehe (4) in Abb. 32). Dies geschieht durch Umkonfiguration virtueller Switches (Netzwerk an den Hypervisoren; nicht in der Abbildung dargestellt) und zwar so, dass keine Veränderung von Daten infolge einer Anwenderaktion oder durch die Ausführung der VM verlorengeht. Die ursprüngliche VM auf dem System A wird angehalten und gelöscht, der Arbeitsspeicher wiederaufbereitet und freigegeben.

4.5.3 Rechenzentrum (physisch)

Die Wolke (cloud) ist natürlich nur eine Metapher für die Datenverarbeitung mit entfernten Computern, die wir nicht sehen. Daten werden elektronisch immer von physischen Computern verarbeitet. Sie sind in zum Teil sehr großen, speziell für diesen Zweck errichteten Gebäuden (*Rechenzentren*) untergebracht. Gerade für das *Cloud-Computing* werden sehr viele Computersysteme benötigt, um die große Elastizität hinsichtlich der verfügbaren Ressourcen (wie Rechenkapazität und Kurzzeitspeicher) erreichen zu können.

Die *Server* (Computer), die in Rechenzentren verwendet werden, sind für den dortigen Einsatz optimiert und in großen Schränken (*racks*) untergebracht, die wiederum in langen Reihen angeordnet sind. Die Versorgung mit Strom und die Verbindung mit Netzwerken erfolgen über einen Doppelfußboden unter den Racks. Da die Hochleistungscomputer sehr viel Strom (Energie) verbrauchen, die letztlich in Wärme umgesetzt wird, ist die Klimatisierung bzw. Kühlung ein entscheidendes Element in einem Rechenzentrum. Die Leistungsfähigkeit der Kühlung bestimmt neben dem Stromverbrauch der Computer selbst wesentlich die mögliche

Packungsdichte der Computer. Platzverbrauch und Stromverbrauch für Kühlung und Rechentechnik sind Faktoren, die die Kosten beeinflussen.

Moderne Rechenzentren sind daher technisch hoch entwickelte Systeme, die auf Kosteneffizienz getrimmt sind. Ein anderer wichtiger Faktor ist die Zuverlässigkeit bzw. Verfügbarkeit. Deshalb kommt der Standortwahl große Bedeutung zu. Große Mengen von Strom (Energie) müssen zu einem günstigen Preis dauerhaft zur Verfügung stehen. Von der Umgebung ausgehende Katastrophen wie Überschwemmungen oder Großbrände müssen unwahrscheinlich sein. Gleichzeitig muss im Rechenzentrum selbst einiges getan werden, um die Zuverlässigkeit bzw. Verfügbarkeit sicherzustellen. Notstromaggregate schützen vor möglichem Stromausfall, und Batterien versorgen die Rechentechnik, bis die Aggregate hochgelaufen sind. Auch der Brandschutz spielt eine große Rolle. Dazu gibt es Brandschutzzonen und diverse Maßnahmen der Branderkennung und -meldung sowie zum manuellen und automatischen Löschen.

Aufgrund des Wertes der verbauten Rechentechnik werden zudem Maßnahmen ergriffen, um unberechtigtes Eindringen und Diebstahl zu verhindern. Diese Maßnahmen der physischen Sicherheit kommen auch der Zuverlässigkeit und IT-Sicherheit zugute.

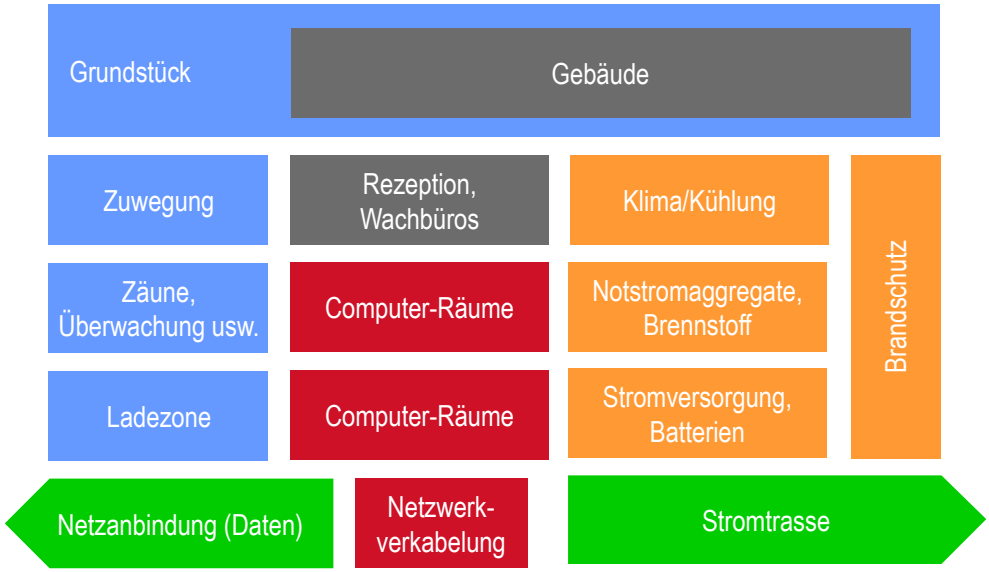


Abb. 33: Aufbau eines Rechenzentrums (schematisch)

Abb. 33 zeigt schematisch wichtige Teile eines großen Rechenzentrums. Oft wird der Begriff Rechenzentrum allgemein für den Ort verwendet, wo die zentrale Rechentechnik untergebracht wird. Die obige Beschreibung und die Abbildung beziehen sich auf die industrialisierte Produktionsweise von *ICT-Services* bzw. *Computing-* oder IT-Services. Die Computer-Räume sind mit Schränken (Racks) gefüllt.

Racks und die Baugruppen, die sie enthalten, sind schematisch weiter unten in Abb. 34 dargestellt und werden dort ebenfalls erläutert.

Rechenzentrum (data center)

Ein Rechenzentrum ist ein Gebäude für die Unterbringung und den Betrieb zentraler Rechentechnik (vor allem *Server*, aber auch *Storage* und Netzwerkkomponenten), das in der Regel genau für diesen Zweck konstruiert und gebaut wurde. Oft werden aber auch dafür hergerichtete Gebäude oder Räumlichkeiten als Rechenzentrum bezeichnet.

Moderne Rechenzentren sind optimiert auf hohe Zuverlässigkeit und Effizienz. Eine hohe Zuverlässigkeit bedeutet, dass die Wahrscheinlichkeit für Ausfälle im IT-Betrieb gering ist, die mit dem Rechenzentrum selbst in Verbindung stehen und durch materielle Vorfälle (zum Beispiel Feuer oder Stromausfall) oder durch Wartungsarbeiten verursacht werden. Rechenzentren unterscheiden sich hinsichtlich ihrer Ausstattung und erreichten Zuverlässigkeit. Das Uptime Institute teilt Rechenzentren diesbezüglich in vier Ebenen ein (Tier I - IV), die Telecommunications Industry Association (TIA) in vier Stufen (Level 1 – 4). Dabei werden die Ausstattung, Redundanz, Fehlertoleranz, die Auswirkungen von Wartungsarbeiten sowie der Schutz gegen bzw. die Anfälligkeit bei materiellen Vorfällen (physical events) wie Feuer, Stromausfall oder Unwetter bewertet.[94]

Um den störungsfreien Betrieb gewährleisten zu können, ist neben Brandschutzmaßnahmen und Maßnahmen zur physischen Sicherheit (Barrieren, Zutrittskontrolle, Überwachung mittels Kameras, Wachpersonal) auch die Standortwahl entscheidend. Darüber hinaus sind eine ausfallsichere Stromversorgung und die ausreichende Klimatisierung entscheidend. Zur ausfallsicheren **Stromversorgung** gehören Notstromaggregate mit ausreichendem Kraftstoffvorrat und Batterien, die die Versorgung übernehmen, bis die Aggregate die volle Leistung erreicht haben. Die Notstromaggregate stellen eine **Ersatzstromversorgung** dar, die längere Ausfälle überbrückt, während die Batterien Teil der **unterbrechungsfreien Stromversorgung (USV)** sind, die kurzfristige Beeinträchtigungen ausgleicht. Aber auch die Zuleitungen vom Energieversorgungsunternehmen (EVU) in der Umgebung des Rechenzentrums einschließlich Trafostationen, Verteilern usw. sowie im Rechenzentrum selbst müssen entsprechend gestaltet sein. Dazu kann auch gehören, dass das Rechenzentrum redundant aus zwei verschiedenen Umspannwerken versorgt wird.

Eine ausreichende **Klimatisierung** (Kühlung) ist für eine hohe Zuverlässigkeit unerlässlich und hat gleichzeitig großen Einfluss auf die Effizienz. Die Computersysteme (vor allem Server) verbrauchen viel Strom (Energie) und müssen beständig gekühlt werden. Der Energieverbrauch der Klimatisierung übersteigt

94 BITKOM: Betriebssicheres Rechenzentrum, Leitfaden; Version Dezember 2013

den der Rechentechnik. Die Computersysteme sind in hohen Server-Schränken (*Racks*) untergebracht, die in langen Reihen angeordnet sind. Unter dem Doppelfußboden (raised floor) befindet sich die Verkabelung für Strom und Daten. Der Doppelfußboden wird auch für die Klimatisierung genutzt. Das Einblasen kalter Luft sorgt zusammen mit den Lüftern der Computersysteme für die Durchströmung der Schränke mit den Computersystemen und damit für deren Kühlung. Es bildet sich ein kalter Gang (cold aisle) auf der einen Seite der Schränke und ein warmer (warm aisle) auf der anderen. Die warme Luft steigt nach oben und wird abgesaugt.

Die Technik der Rechenzentren einschließlich der Klimatisierung ist einer steten Weiterentwicklung unterworfen. Rechenzentren werden normalerweise nur dann betreten, wenn Komponenten neu installiert oder ausgetauscht werden oder wenn andere größere Wartungsarbeiten anstehen. Nur das Wachpersonal hält sich in seinen Räumlichkeiten und auf dem Gelände auf. Die Wartung der IT erfolgt auf elektronischem Wege aus der Ferne („remote“). Rechenzentren sind in Sicherheitszonen gegliedert, die mit abgestuften Beschränkungen verbunden sind und unterschiedlich stark gesichert sind. Hochsicherheitsrechenzentren befinden sich an besonders geschützten Orten in Stollen, Bunkern und dergleichen.

Notfallrechenzentrum

Notfallrechenzentren oder **Ausweichrechenzentren** sind Rechenzentren, die die Bereitstellung der IT-Services im Falle eines Ausfalls des produktiven (primären) Rechenzentrums übernehmen können, dazu an dieses entsprechend angebunden sind und laufend Daten zur Synchronisation erhalten. Um den Betrieb übernehmen zu können, muss die gesamte benötigte IT einschließlich der Anwendungen vorhanden sein und gepflegt werden. Das Notfallrechenzentrum muss sich je nach betrachteten Ausfallszenarien geographisch weit entfernt vom primären Rechenzentrum befinden.

Es gibt auch mobile oder portable Notfallrechenzentren zum Beispiel in Form eines Containers, die vor Ort gebracht und in kurzer Zeit angeschlossen werden können. Sie dienen vor allem der Datensicherung im Notfall. Als vorbeugende Maßnahmen werden üblicherweise regelmäßig Sicherungskopien angefertigt. Die entsprechenden Datenträger müssen sich jedoch an einem anderen Ort (oder in einem anderen Rechenzentrum) befinden, um einen Schutz gegen Datenverlust im Katastrophenfall zu bieten.

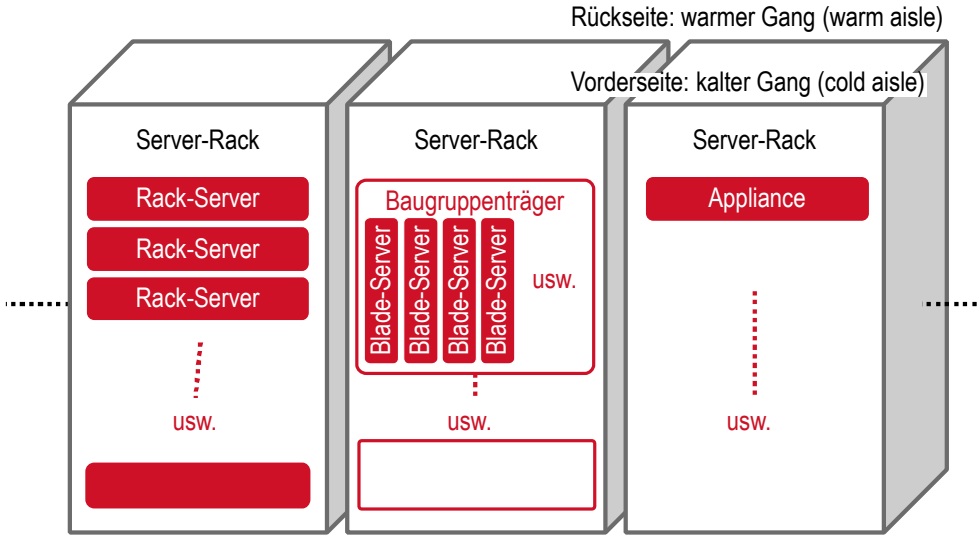


Abb. 34: Schränke (Racks) und enthaltene Baugruppen in einem Rechenzentrum

Rack (Server-Rack)

Die Technik in den Computer- oder Server-Räumen eines *Rechenzentrums* ist in Schränken, Gestellen bzw. Haltevorrichtungen untergebracht, die allgemein als Rack bezeichnet werden. Je nach Zweck bzw. untergebrachter Technik wird auch zwischen Server-Racks, Netzwerk-Racks und Stromversorgungs- und Stromverteilungs-Racks unterschieden. Die einzelnen technischen Komponenten werden waagerecht als Einschübe, ähnlich wie Schubladen, in den Rack eingeschoben und verschraubt.

Die meisten IT-Systeme wie *Rack-Server* und Systeme aus *Blade-Servern* sind für den Einbau in einen Rack mit einer Breite des Einbauchassis von ca. 48 cm (19 Zoll) vorgesehen, dessen lichte, nutzbare Breite ca. 45 cm beträgt. Die meisten der in Rechenzentren eingesetzten Racks sind daher die sogenannten **19-Zoll-Racks**. Die vertikale Höhe eines Racks wird in nutzbaren Innenmaßen angegeben, die in Höheneinheiten gemessen werden. Eine Höheneinheit misst ca. 4,4 cm (1,75 Zoll). Üblich für den Einsatz im Rechenzentrum sind Racks mit einer Höhe von ca. 2 Metern (42 Höheneinheiten).

Ein Rack muss große Lasten tragen und entsprechend stabil sein. Da außerdem oft Raum für Verkabelung benötigt wird, übersteigen die Außenmaße die gerade angegebenen Maße zum Teil beträchtlich. Manche Racks besitzen auch Türen, um sie verschließen zu können. Ein 19-Zoll-Rack kann außen zum Beispiel 60 oder sogar 80 cm breit sein. Die Tiefe liegt zwischen 60 und 120 cm.

Rack-Server

Ein für den Einsatz in *Rechenzentren* optimiertes Computersystem (Server), das waagerecht in einen Serverschrank (*Rack*) eingeschoben wird. Ein etwa 2 Meter

(42 Höheneinheiten) hoher Serverschrank (Rack) kann etwa 14 Rack-Server aufnehmen. Bei einer Höhe von ca. 9 cm (2 Höheneinheiten) passen rein rechnerisch sogar 20 Systeme in einen solchen Rack, der meist eine Breite von ca. 48 cm (19 Zoll) hat.

Blade-Server

Ein für den Einsatz in *Rechenzentren* optimiertes Computersystem (Server), das senkrecht zunächst in einen Baugruppenträger (Blade Center oder Blade Enclosure) eingeschoben wird. Bei einer Breite des Serverschranks von ca. 48 cm (19 Zoll) kann ein Baugruppenträger 14 Blade-Server aufnehmen. Etwa sechs Baugruppenträger passen übereinander in einen etwa 2 Meter (42 Höheneinheiten) hohen Serverschrank (*Rack*), wenn die Blade-Server als Platinen im Doppel-Europa-Format ausgeführt sind.

Appliance

Der Begriff Appliance bezeichnet kompakte IT-Systeme oder Geräte bestehend aus Hardware und Software, die vom Hersteller als Fertiglösung geliefert werden und vom Anwender nicht oder kaum verändert oder angepasst werden können. Oft vereinigt eine Appliance mehrere Funktionalitäten bzw. kombiniert die Funktion verschiedener Geräte. Die Wahl des Begriffs ist auf Ähnlichkeiten mit Haushaltsgeräten (home appliances) zurückzuführen, die ebenfalls kompakt, verschlossen und meist sogar versiegelt sind und bestimmte Funktionalitäten für einen festgelegten Zweck bereitstellen, die vom Anwender nicht verändert oder modifiziert werden können. Enthält das Gerät Software, so kann auch diese ohne den Hersteller nicht modifiziert oder erweitert werden, wie dies im Gegensatz dazu zum Beispiel bei einem PC (Personal Computer) möglich ist. Eine Appliance ist weiterhin dadurch gekennzeichnet, dass Hardware, Betriebssystem und Anwendungssoftware in einem Gerät fest integriert und von vornherein aufeinander abgestimmt sind. Dies erleichtert den Einsatz als schlüsselfertige Lösung (turnkey solution).

Ein typisches Beispiel für eine **Network appliance** kombiniert einen Router mit Firewall-Funktionen sowie Lösungen für die Authentisierung und die Adressumsetzung und -verwaltung. Beispiele für eine **Security appliance** sind Geräte, die Funktionen wie *Firewall*, *Anti-Malware* und *Content filtering* vereinen und bereitstellen. Solche Security appliances werden auch unter der Bezeichnung *Unified Threat Management (UTM)* speziell für kleine und mittelgroße Unternehmen angeboten und enthalten typischerweise Lösungen aus den drei Bereichen Netzwerksicherheit (*Firewall*, *Intrusion Prevention System (IPS)*, *Virtual Private Network (VPN)*), sicherer Internet-Zugang (*URL-Filter*, *Anti-Virus*) und Datensicherheit (*Spam-Filter*, *Anti-Virus* für E-Mail).

Software-Defined Data Center (SDDC)

Ein softwaredefiniertes Rechenzentrum oder auch virtuelles Rechenzentrum (**virtual data center, VDC**) bezeichnet eine vollständig virtualisierte IT-Infrastruktur bestehend aus *Server-Virtualisierung*, *Storage-Virtualisierung* und *Netzwerk-Virtualisierung*, d.h., virtualisierten Compute-Ressourcen, virtualisiertem Speicher und virtualisierten Datenverbindungen. Dabei werden Steuerungs- bzw. Anwendungsebene von der Daten- bzw. Ressourcenebene getrennt. Die Steuerung bzw. Anwendung erfolgt über Softwareschnittstellen (APIs) ohne direkte Eingriffe auf die IT-Ressourcen, wodurch so etwas wie **IT-as-a-Service (ITaaS)** entsteht.

4.6 Netzwerke und Kommunikationstechnologie (Technik)

Netzwerke sind ein nahezu unerschöpfliches Thema. Dieses Kapitel gibt nur einen Überblick. Oft werden nur kurze Beschreibungen gegeben, sodass, um ein vollständigeres Verständnis zu erlangen, weitere Literatur herangezogen werden muss. Schon der Begriff „Netzwerk" kann zu falschen Assoziationen führen. Gemeinhin verbindet man mit dem Begriff viele Verbindungen, die an Knoten zusammenlaufen und Maschen bilden. Computernetzwerke gleichen aber eher Straßen, an denen sich Häuser befinden. Am Rand des Viertels oder des Ortes sind diese Straßen oder Straßensysteme zu Ende. Land- und Bundesstraßen sowie Autobahnen übernehmen dann und schaffen weitere Verbindungen (Netzwerke).

Physische Netze bestehen aus elektrischen Leitungen oder Kabeln aus Metall oder Glasfaser sowie aus elektronischen Systemen an deren Enden. Physische Netze haben immer einen Besitzer und Betreiber. Logische Netze haben Anwender. Sie bestehen in gewisser Weise aus Adressen und Verbindungsmöglichkeiten.

Zunächst geht es um Netze, die sich hinsichtlich ihrer Reichweite und ihrem grundsätzlichen Aufbau unterscheiden. Dabei werden auch virtualisierte, „software-defined" Varianten beschrieben, und auch der Aufbau des Internets kommt nicht zu kurz (Kapitel 4.6.1). Die wichtigsten grundlegenden Komponenten folgen (Kapitel 4.6.2). Auf die Beschreibung von Übertragungsprotokollen wird verzichtet. Soweit fürs Verständnis wichtig, werden sie an verschiedenen Stellen in diesem Buch erwähnt.

4.6.1 Netzwerke

Weitverkehrsnetz (WAN) (Wide Area Network)

Netzwerk, das geografisch größere Distanzen überwindet. Seine Nutzung wird von Dienstleistern als *Network-Service* angeboten und verkauft. Damit werden Standorte bzw. ihre *lokalen Netzwerke (LANs)* verbunden oder Verbindungen zu Rechenzentren bzw. IT-Services (Computersystemen) hergestellt. Anwender-

organisationen werden in der Regel Leistungsparameter garantiert (→*Quality of Service, QoS*).

Damit der Anbieter und Betreiber des WAN (*Netzbetreiber*, auch *Carrier* genannt) die WAN-Verbindung selbst bereitstellen kann, muss er vor Ort vertreten sein (**Point of Presence, PoP**) und einen Übergabepunkt (Provider Edge oder Service Point) anbieten, an dem der Anwender die Verbindung mittels sogenannter **Customer Premises Equipment (CPE)** herstellen kann. Generell setzen sich WAN-Verbindungen aber aus Leistungen verschiedener Netzbetreiber oder Carrier zusammen, die von der Anwenderorganisation selbst, meist aber von einem der beteiligten Carrier zusammengeführt werden.

Grundsätzlich gibt es **Standleitungen (Direct Network Link, DNL)**), d.h. physische Netzwerkverbindungen, die einer Anwenderorganisation exklusiv zur Verfügung stehen.

Multiprotocol Label Switching (MPLS) ist ein Standard für die Übertragung von Daten verschiedener Anwenderorganisationen über ein physisches Netz. Die Datenströme werden durch Anbringen eines Etiketts (Labels) unterschieden. Auf die gleiche Art können auch Datenströme für verschiedene Anwendungen (Konferenzen, Ton, Daten usw.) unterschieden werden, damit sie mit einer unterschiedlichen Dienstgüte (Quality of Service, QoS) übertragen werden bzw. übertragen werden können.

Eine andere Möglichkeit, Weitverkehrsverbindungen herzustellen, bietet das *Internet* selbst. Das Internet vernetzt weltweit und ist daher auch ein (logisches) WAN (manchmal aber auch als GAN (Global Area Network) eingeordnet). Leistungsparameter (QoS) beziehen sich hier nur auf den Zugang zu diesem Netz und nicht zu den Systemen in diesem Netz. Neben dieser fehlenden Garantie kann auch kein Einfluss auf die Übertragung (zum Beispiel eine Priorisierung von Paketen) genommen werden. Aus Sicherheitsgründen werden Internet-Verbindungen sehr häufig über ein *Virtual Private Network (VPN)* genutzt.

Lokales Netzwerk (LAN) (Local Area Network)

Netzwerk, das örtlich beschränkt ist und sich zum Beispiel nur auf ein Gelände oder ein Gebäude erstreckt. Es gibt kabelgebundene Netzwerke, in denen hauptsächlich Ethernet als Übertragungsprotokoll (IEEE-802.3) zum Einsatz kommt, und kabellose oder drahtlose Netzwerke (**Wireless LAN, WLAN**), in denen die Informationen mittels elektromagnetischer Wellen übertragen werden. Letztere basieren auf dem Übertragungsstandard IEEE-802.11. Ein angehängter Buchstabe (b, g, n, ac, ax) kennzeichnet die Geschwindigkeit des Netzes.

Eine besondere Form eines LANs bzw. eines Systems von LANs stellen die Netzwerke in Rechenzentren (**RZ-Netze**) dar. Diese sind in einzelne Netze segmentiert und physisch und logisch für verschiedene Verwendungszwecke getrennt.

Die zur Übertragung von Nutzdaten verwendeten RZ-Netze sind für sehr hohe Geschwindigkeiten ausgelegt und unterstützen die Übertragung von Daten verschiedener Anwenderorganisationen über ein physisches Netz mittels VLAN-Technologie (siehe auch *Netzwerk-Virtualisierung*). Dabei wird das physische Netz in logische Teilnetze aufgespaltet, die jeweils ein eigenes **VLAN** (virtual local area network) bilden. Die Kommunikation über das (physische) Netz ist nur über *Switches* möglich, die sicherstellen, dass Datenpakete nur an Systeme zugestellt werden, die zu diesem VLAN gehören. In virtualisierten Server-Umgebungen (siehe *Server-Virtualisierung*) sind die Switches Teil des Hypervisors und als Software ausgeführt (Virtual Switch).

Software-defined Networking (SDN)

Architektur zur Optimierung von Netzwerken, bei der über die ursprünglichen Netzwerke (data layer, data plane) eine zusätzliche Steuerungsebene (control layer, control plane) in Form einer Software-Abstraktionsschicht gelegt wird. Durch die Nutzung mehrerer paralleler oder alternativer Übertragungswege und die intelligente Steuerung der Datenströme kann die Netzwerkqualität bzw. Dienstgüte (Quality of Service, QoS) verbessert werden.

In einem solchen Netz können auch Netzwerkkomponenten virtualisiert werden, die eine oder mehrere **Virtual Network Function (VNF)** realisieren. Eine VNF[95] ist eine Komponente ähnlich einer *Virtuellen Maschine (VM)* (virtual machine), die Netzwerkfunktionen realisiert wie *Firewall*, *Switch* oder Load Balancer. Das Konzept wird als **Network Function Virtualization (NFV)** bezeichnet.

Die bekannteste Anwendung von Software-defined Networking (SDN) ist *SD-WAN*.

SD-WAN (Software-defined Wide Area Network)

Nutzung eines Systems von →*Weitverkehrsnetzen (WANs)* bzw. Weitverkehrsnetzwerkdienstleistungen (underlay: data layer, data plane) mit Hilfe einer darüberliegenden, zusätzlichen Steuerungsebene (overlay: control layer, data plane). Diese Netzwerkarchitektur realisiert *Netzwerk-Virtualisierung* für Weitverkehrsdienstleistungen im großen Maßstab, um die Nutzung für die Anwenderorganisationen zu vereinfachen, und/oder um, falls alternative Übertragungswege (MPLS, Internet) genutzt werden können, Bandbreite zu gewinnen oder die Dienstgüte (*Quality of Service, QoS)* zu verbessern. Diese Architektur und die Prinzipien wurden unter dem Namen *Software-defined Networking (SDN)* entwickelt und bekannt gemacht.

Durch die gleichzeitige Nutzung zweier Übertragungswege (WAN) kann gegebenenfalls die Qualität verbessert werden hinsichtlich der *Latenz (latency)* oder

---

[95] Wikipedia; https://en.wikipedia.org/wiki/Network_function_virtualization; zuletzt aufgerufen am 21.01.2021

Antwort- bzw. Durchlaufzeit, der Varianz der Verzögerung (jitter oder delay variation) und der Fehlerrate (packet loss). Zeitkritische Anwendungen wie Telefonie, Videokonferenzen und Media Streaming verlangen geringe Werte für Jitter und Packet Loss.

An den mit SD-WAN verbundenen Lokationen wird ein **SD-WAN Edge** genanntes System installiert, das Ähnlichkeiten zu einem *Customer Premises Equipment (CPE)* hat bzw. dieses darstellt und dessen Funktion im SD-WAN übernimmt. Jede SD-WAN-Lösung besitzt einen **SD-WAN Orchestrator**, der Entscheidungen über sämtliche Datenströme entsprechend vordefinierter Regeln trifft. Die Regeln verarbeiten Anforderungen an die Leistungsparameter (*Quality of Service, QoS)*. Diese erhalten **SD-WAN Controller** von den mit ihnen verbundenen SD-WAN Edges, die sie auch steuern (konfigurieren usw.).

Internet

International allgegenwärtiges Netzwerk, das Anwendern den Zugang zu den unterschiedlichsten IT-Services bietet, die Firmen, Behörden, Institutionen, Organisationen, Vereine, Personen usw. anbieten und nutzen.

Internet Service Provider (ISP), auch kurz Internetprovider genannt, sind Firmen, die Anwender mit dem Internet verbinden. Sie besitzen eigene Netze und/oder treten als Wiederverkäufer auf. Oft wird nicht zwischen Internet Service Provider (ISP) und *Netzbetreiber* unterschieden.

Die im Internet angebotenen IT-Services umfassen kostenlose und bezahlte Dienste sowie solche, die Waren und Dienstleistungen gegen Bezahlung im Internet anbieten. Im Internet sind diverse Geschäftsmodelle vertreten. Die (kommerziellen) Anbieter von Inhalten und anderen IT-Services werden **Internet-Dienstleister** genannt.

Der Zugang zum Internet erfolgt direkt über das Endgerät (zum Beispiel über Mobilfunk oder DSL), über ein *lokales Netzwerk (LAN)* mit Internetanbindung, über das *Backbone* eines WAN/MPLS-Netzes oder über Server in einem Rechenzentrum, die über eine zusätzliche, separate Verbindung zum Internet verfügen. Bei den beiden letztgenannten Varianten spricht man im engeren Sinne von Internet-Breakout, weil es sich um eine weitere, hinzugefügte Verbindung handelt.

Das Internet besteht aus vielen sogenannten **Autonomen Systemen (AS)**, die von **Netzbetreibern** (gegebenenfalls im Auftrag von großen Firmen oder Organisationen) betrieben werden. Netzbetreiber oder **Carrier** verfügen über eigene Netze und steuern den Netzwerkverkehr zunächst innerhalb ihrer Autonomen Systeme (AS). Sie bieten aber eine Kommunikationsdienstleistung innerhalb des gesamten Internets und zwar durch Wahl der besten Route durch das Internet bzw. durch eine Kette von Autonomen Systemen (AS). Diese Kette wird durch das **Border Gateway Protocol (BGP)** gesteuert, das das Routing-Protokoll des

Internets darstellt. Netzbetreiber bzw. Internet Service Provider (ISPs) tauschen den Datenverkehr untereinander an Internet-Knoten (physisch und logisch) aus, die **Austauschpunkt** genannt werden. Die größeren, kommerziellen Austauschpunkte werden **Commercial Internet eXchange (CIX)** genannt. Besonders bekannt ist der weltweit größte Austauschpunkt DE-CIX in Frankfurt am Main.

Intranet

Ein firmen- oder organisationseigenes Netzwerk, das Technologien des Internets wie beispielsweise das Internet Protokoll (IP) verwendet.

Backbone

Der Hochgeschwindigkeits- (high-speed) Kernbereich eines großen physischen *Weitverkehrsnetzes (WAN)*. Das Backbone (englisch für Rückgrat) bildet den Kern (das **Core network**) in einer Hierarchie von Netzwerken unterschiedlicher Reichweite.

Content Delivery Network (CDN)

Bezeichnung für Dienstleister, die Inhalte wie Filme, Webseiten, Software usw. für bzw. im Namen der eigentlichen Anbieter im Internet bereitstellen. Sie duplizieren diese Inhalte in verteilte, lokale Rechenzentren, um die Wege zu den Anwendern und die Ladezeiten zu verkürzen.

4.6.2 Netzwerkkomponenten

Es gibt eine Vielzahl von Netzwerkkomponenten. Die wichtigsten werden im Folgenden kurz vorgestellt. Abb. 35 zeigt das OSI-Schichtenmodel, das zunächst erklärt wird. Die Abbildung ordnet einigen Schichten Komponenten zu. Die verschiedenen *Firewalls* und Lösungen für ein *Virtual Private Network (VPN)* werden jedoch nicht hier, sondern in Kapitel 6 ausführlich beschrieben.

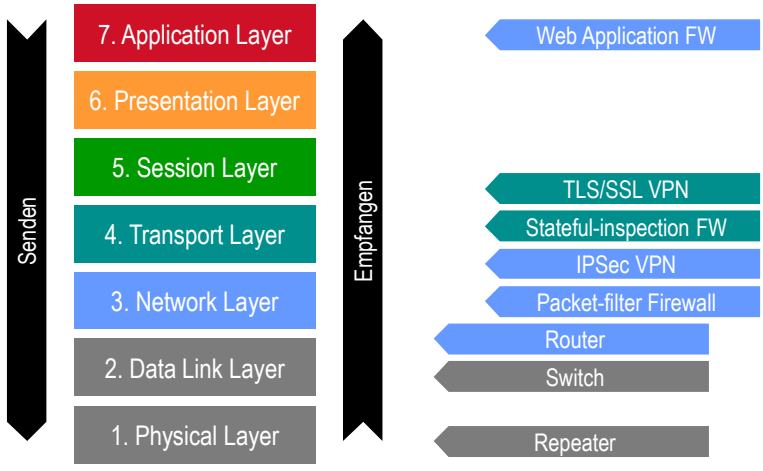


Abb. 35: OSI-Modell und Auswahl an Netzwerkgeräten

OSI-Modell (ISO/OSI-Referenzmodell)

Modell zur Einordnung von Protokollen, die für den Austausch von Daten zwischen diversen informationsverarbeitenden Systemen verwendet werden. Das Modell besteht aus sieben Kategorien von Protokollen. Siehe Abb. 35.

In der Regel können sich die Systeme nicht direkt über die Protokollschicht verbinden, die sie zur Kommunikation nutzen. Dann werden einzelne Protokolle verschachtelt (Zwiebelschalenmodell). Beim Senden von Daten werden höhere Schichten in die nächst niedrigere verpackt, sodass die höhere Schicht als Nutzdaten der niedrigeren übertragen wird. Die Verschachtelung kann sich bis zur niedrigsten Schicht fortsetzen. Beim Empfangen wird das jeweils außen liegende Protokoll verarbeitet, und die übertragenen inneren Daten werden weitergereicht.

Repeater

Netzverlängerung oder Netzwerkverstärker. Ein Repeater verteilt Daten (OSI-Layer 1) an alle Teilnehmer im Netz (über alle Ports).

Switch

Netzwerkweiche oder Netzwerkverteiler, der Netzwerksegmente verbindet bzw. die Segmentierung von Netzwerken ermöglicht. Ein Switch verteilt Datenpakete (Frames, OSI-Layer 2) an genau einen der Netzwerkanschlüsse (Ports, Hardware), an die Geräte angeschlossen werden, die eine eindeutige MAC-Adresse haben.

Es gibt auch Layer-3-Switches und Multi-Layer-Switches.

Router

Netzwerkweiche oder Netzwerkverteiler, verteilt Datenpakete (IP-Pakete, OSI-Layer 3) an genau einen der Netzwerkanschlüsse bzw. an das Netzwerk, über das der Empfänger erreichbar ist.

Router können angeschlossenen Geräten (mittels DHCP) eine IP-Adresse zuweisen und bauen damit ein eigenes Netz auf. Der Router vermittelt dann zum Beispiel zwischen dem Internet und den angeschlossenen Geräten. Dabei können Router die IP-Adressen der angeschlossenen Geräte in öffentliche übersetzen.

Gateway

Eine aktive Komponente, die eine Verbindung zwischen zwei Netzen herstellt und dabei die Daten auf einer Schicht im OSI-Modell bearbeitet. d.h., in der Regel verändert. Je nach der Schicht gibt es verschiedene Gateways. So ist ein *Router* ein Layer-3-Gateway und ein *Proxy* oder *Reverse Proxy* ist ein Application Layer Gateway (Layer-7-Gateway).

Literatur und Bildnachweise

Besonders ein solches Buch, das sich zur Aufgabe macht, Definitionen von Fachbegriffen zu geben, kann nicht geschrieben werden, ohne dass der Autor vielfältige Literatur gelesen hätte – in der langen Zeit der Tätigkeit auf diesem Gebiet, bei der Erstellung von Lehrunterlagen für Studierende und beim Schreiben dieses Buches. Die Definitionen sollen ja den Stand der Technik korrekt wiedergeben und konsensfähig sein. Das bedeutet auch, dass Begriffe und Zusammenhänge auch in anderen Veröffentlichungen so oder ähnlich vorkommen können – ja müssen.

Daher wurde wie folgt verfahren: (1) Literatur ist an den Stellen als Fußnote angegeben, wo ich sie direkt verwendet habe bzw. mir bewusst ist, dass Begriff, Definition oder sonstige Beschreibungen auf eine solche Quelle zurückgeführt werden können. (2) Gilt dies in gleicher Weise für Institutionen oder Einzelpersonen, so sind diese meist direkt im Text angegeben. (3) Die folgende Liste enthält Literaturhinweise und wiederholt nicht die Quellenangaben in diesem Kapitel. (4) Falls nicht anders angegeben, wurden Abbildungen extra für dieses Buch erstellt.

[1] Cloud Security Alliance (CSA): Security Guidance for Critical Areas of Focus in Cloud Computing; Version 3.0, 2011, 177 pages

[2] BITKOM: Eckpunkte für sicheres Cloud Computing, Leitfaden für die Auswahl vertrauenswürdiger Cloud Service Provider; 2013, 48 Seiten

[3] BITKOM: Cloud Computing – Was Entscheider wissen müssen, Ein ganzheitlicher Blick über die Technik hinaus Positionierung, Vertragsrecht, Datenschutz, Informationssicherheit, Compliance; Leitfaden; 2010, 116 Seiten

[4] Torsten Gründer (Hrsg.): IT-Outsourcing in der Praxis, Strategien, Projektmanagement, Wirtschaftlichkeit; Erich Schmidt Verlag, Berlin, 2011, 2. Auflage, ISBN 978-3-503-09015-0, 479 Seiten

[5] WhatIs.com® (Referenz- und Selbstlernwerkzeug zum Thema Informationstechnologie (IT)); https://whatis.techtarget.com/de

[6] Gartner: Gartner Glossary, Information Technology; https://www.gartner.com/en/information-technology/glossary

Elektronisches Zusatzmaterial
Die Abbildungen sind als PowerPoint-Datei kapitelweise über https://link.springer.com/ auf der Seite des eBooks abrufbar.

5 IT-Verfahren, Abläufe und Prozesse

In diesem Kapitel wird die Organisation des IT-Betriebs beschrieben. Sie folgt in der Regel standardisierten IT-Verfahren, die Abläufe in Form von ausdefinierten Prozessen festlegen. Diese unter dem Begriff „IT-Service-Management" zusammengefassten Prozesse werden in Kapitel 5.2 im Detail erläutert. Doch zuvor liefert das folgende Kapitel 5.1 eine Darstellung der wichtigsten Grundbegriffe. Das Kapitel 5.3 widmet sich abschließend einem meist unterschätzten Thema, der Berücksichtigung der IT-Sicherheit in den Prozessen des IT-Service-Managements.

Sobald eine bestimmte Technologie eine bestimmte Komplexität erreicht hat oder besonders belastet wird, sind regelmäßige Reparatur- und Wartungsarbeiten nötig. Die kontinuierliche Überwachung und eine regelmäßige Überprüfung sind dann erforderlich, wenn die Anwender von der fehlerfreien Funktion in besonderer Weise abhängig sind. All dies trifft auf Autos ebenso zu wie auf Verkehrsflugzeuge. Autos müssen zur Inspektion. Verkehrsflugzeuge werden vor jedem Start untersucht. Wichtige Funktionen werden jedoch auch während der Nutzung kontinuierlich überwacht. Das Auto zeigt den Ölstand an und warnt, wenn der Sensor der Abstandsregelung (Abstandsregeltempomat, Adaptive Cruise Control) kein verlässliches Signal liefern kann. Die Triebwerke von Verkehrsflugzeugen werden besonders intensiv überwacht, um mögliche Probleme frühzeitig erkennen zu können. Wichtige oder kritische Daten werden während des Fluges an das Service-Center am Boden übermittelt, sodass Reparatur- oder Instandhaltungsmaßnahmen vorbereitet und nach der Landung so bald wie möglich durchgeführt werden können.

Bei Computersystemen und Netzwerken werden ähnliche Vorkehrungen getroffen. Schließlich hängt das reibungslose Funktionieren von Fertigung, Verwaltung, medizinischer Versorgung, Handel und vielen anderen gesellschaftlichen Bereichen davon ab, dass auch die Informationstechnologie (IT) ihren Dienst tut. Die zunehmende Digitalisierung verstärkt diese Abhängigkeit.

Deshalb spielen Instandhaltung, Fortentwicklung und Fehlerbehandlung auch in der IT eine große Rolle. Dazu kommt, dass die IT „niemals fertig ist". Immer wieder werden Änderungen gefordert und implementiert. Das liegt nicht allein an der manchmal schlechten Qualität der Software, sondern daran, dass die Anforderungen der Anwender einem steten Wandel unterworfen sind.

Zusatzmaterial online
Zusätzliche Informationen sind in der Online-Version dieses Kapitel (https://doi.org/10.1007/978-3-658-33431-4_5) enthalten.

E. von Faber, *IT und IT-Sicherheit in Begriffen und Zusammenhängen*,
Edition <kes>, https://doi.org/10.1007/978-3-658-33431-4_5

5.1 Grundbegriffe

Abb. 36 fasst wichtige Begriffe im IT-Betrieb zusammen, die in diesem Kapitel erläutert werden. Der Schwerpunkt liegt hierbei allerdings nicht bei den IT-Verfahren, Abläufen und Prozessen der eigentlichen Bereitstellung von IT-Services, sondern auf

- der Instandhaltung und Fortentwicklung (Kapitel 5.1.1) und
- der Fehlerbehandlung (Kapitel 5.1.2).

Die zugehörigen Prozesse werden im Kapitel 5.2 (5.2.6 bzw. 5.2.7) beschrieben.

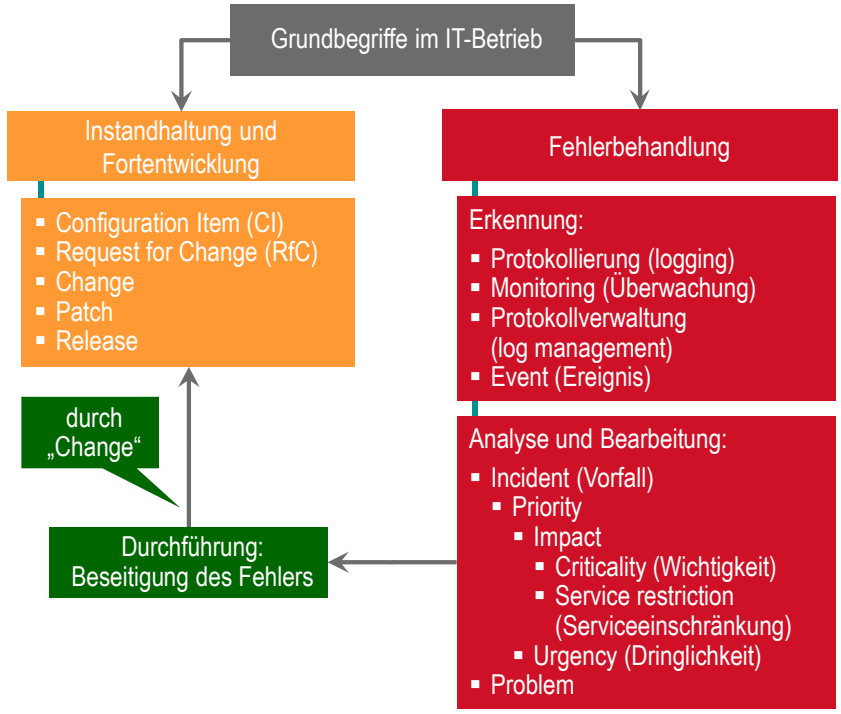


Abb. 36: Einige Grundbegriffe im IT-Betrieb

5.1.1 Instandhaltung und Fortentwicklung

Während der Phase des Normalbetriebs müssen beständig Änderungen vorgenommen werden, um die Bereitstellung der IT-Services sicherzustellen und um Verbesserungen zu implementieren.

Configuration Item (CI) (Konfigurationselement)

> Mit Configuration Item (CI, Konfigurationselement) werden jedwede Komponenten bezeichnet, die verwaltet werden müssen, um den IT-Service bereitstellen zu können. Ein zu einem IT-Service gehörendes Konfigurationselement ist für seine Bereitstellung erforderlich oder nimmt wesentlich Einfluss auf die Bereitstellung.

Beispiele für Konfigurationselemente sind IT-Services, IT-Systeme, Hardware, Software und formale Dokumentationen wie die Prozessdokumentation und *Service Level Agreements (SLAs)*. Informationen zu den einzelnen CIs werden in einem Konfigurationsdatensatz in einer Datenbank (*Configuration Management Database, CMDB*) erfasst und über den gesamten Lebenszyklus hinweg vom →*Configuration Management* verwaltet.

Request for Change (RfC) (Änderungsantrag)

Ein Request for Change (RfC) (Änderungsantrag) ist ein offizieller Vorschlag bzw. eine Beantragung zur Einleitung einer Änderung (*Change*). Ein RfC enthält eine Beschreibung der angefragten Maßnahmen. Mit diesem Begriff wird weder die Änderung selbst (Change) noch eine Aufzeichnung darüber (Change Ticket) bezeichnet.

Ein RfC ist der Startpunkt im Prozess →*Change Management*, in dem die Änderung durchgeführt wird.

Change (Änderung)

Ein Change (eine Änderung) ist eine Umgestaltung der IT, genauer gesagt eines *Configuration Items* (Konfigurationselements). Dazu gehört das Hinzufügen, Modifizieren oder Entfernen von IT-Services, von freigegebenen oder unterstützten Komponenten, von Hardware, Netzwerken, Software, Anwendungen, Systemen, Arbeitsplätzen, der Einsatzumgebung oder der zugehörigen Dokumentation.

Patch

Patches sind Software-Elemente, die entwickelt werden, weil der vorhandene Code einer Software mangelhaft oder verbesserungswürdig ist. Sie ergänzen oder ersetzen diesen. Mit Patches werden vorhandene Mängel in einer Software beseitigt oder zusätzliche Funktionen eingeführt. Unter **Patching** versteht man die Aktualisierung von Software bzw. einer Softwareinstallation (Instanz), ohne dass die Software vollständig neu installiert wird.

Viele Patches bessern Fehler aus, die Schwachstellen beim Informationsschutz darstellen. Manche dieser **Security Patches** (Sicherheitsaktualisierungen) sollen mit Vorrang und unverzüglich installiert werden; sie werden auch als **Hotfix** bezeichnet.

Release

Ein Release ist eine Sammlung von Hardware, Software, Dokumentation, Prozessen oder anderen Komponenten, die benötigt werden, um einen oder mehrere freigegebene *Changes* (Änderungen) an IT-Services vorzunehmen. Die Inhalte eines einzelnen Release werden zusammengefasst und als Ganzes verwaltet, getestet und implementiert.

Ein Release wird im Rahmen des Prozesses *Release and Deployment Management* geplant und umgesetzt.

5.1.2 Fehlerbehandlung

Zur besseren Übersicht sind die folgenden Begriffserklärungen sortiert in die, die sich a) auf die „Erkennung von Fehlern" beziehen und b) in jene, die die „Analyse und Bearbeitung von Fehlern" betreffen.

Die Fehlerbehandlung schließt im vorliegenden Kontext des IT-Service-Managements (Kapitel 5.2) die Behebung der Fehler nicht mit ein. Die Fehlerbehebung erfolgt nach Verfahren, die auch für anderweitig veranlasste Änderungen verwendet werden. Die diesbezüglichen Begrifflichkeiten wurden bereits im Kapitel 5.1.1 erläutert.

Erkennung von Fehlern

Protokollierung (logging)

Die Protokollierung bezeichnet den Prozess der Erstellung von Protokolldaten. **Protokolldaten** sind Aufzeichnungen, die von IT-Systemen und IT-Komponenten im Einsatz bzw. Betrieb erstellt werden. Die Protokollierung dient der Informationsbeschaffung über die Nutzung und den Betrieb dieser IT-Systeme und IT-Komponenten.

Die Protokollierung dient verschiedenen Zwecken. Dazu gehören die Erkennung von Engpässen und die Anpassung von Kapazitäten, die Zuweisung von Kosten und deren Abrechnung sowie die Erkennung von Fehlern und das Auffinden von deren Ursachen. Für das Sicherheitsmanagement am relevantesten sind die Protokolldaten zu *Sicherheitsereignissen (security events)*.

Monitoring (Überwachung)

Die Überwachung bezeichnet die Beobachtung von IT-Systemen und IT-Komponenten im laufenden Einsatz bzw. Betrieb durch ein zusätzliches IT-System. Letzteres protokolliert die Ergebnisse oder generiert einen Alarm.

IT-Systeme und IT-Komponenten erzeugen *Protokolldaten*, die Informationen über deren Nutzung und Betrieb liefern (eigene Aufzeichnungen). Werden beim Monitoring Protokolldaten erzeugt, so enthalten diese Informationen über das überwachte IT-System (Aufzeichnungen über ein Fremdsystem).

Protokollverwaltung (log management)

Die Protokollverwaltung (log management) beinhaltet die Analyse und Verarbeitung von *Protokolldaten*. Sie dient dem Auffinden von Systemfehlern und deren Ursachen, der Prüfung der Einhaltung von Richtlinien und Vorschriften (*Compliance*), der Ermittlung von und der Reaktion auf *Sicherheitsereignisse (security events)* und *Sicherheitsvorfälle (security incidents)* sowie der Durch-

führung von Sicherheitsuntersuchungen, speziell von forensischen Analysen (*forensic analyses*).

Event (IT-Betrieb) (Ereignis)

Events sind Vorkommnisse oder Zustandsänderungen, die durch einen Protokolleintrag, einen Alarm oder eine sonstig erfasste Beobachtung offenbar werden. Ein Event gilt in seiner Auswirkung zunächst als „neutral" bzw. als noch nicht bewertet. Erst nach der Bewertung, die auf eine Filterung und die Korrelation mit anderen Events erfolgt, wird offenkundig, ob das Ereignis für eine Einschränkung der IT-Service-Erbringung oder für dessen normale Nutzung steht. Die Erfassung von Events kann aber bereits mit einem Filter eingeschränkt sein, was eine erste Bewertung impliziert.

In ITIL®[96] gibt es einen eigenen Prozess **Event Management**, der sicherstellt, dass alle IT-Services und *Configuration Items (CIs)* (Konfigurationselemente) überwacht werden und dass die Events gefiltert, mit anderen Events korreliert und kategorisiert werden. Dies ist die Voraussetzung dafür, dass im Rahmen des Prozesses die Bedeutung des Ereignisses verstanden und der nächste Schritt bestimmt werden kann.

Analyse und Bearbeitung von Fehlern

Wie die folgenden Begriffe zusammenhängen, kann Abb. 36 (Seite 134) entnommen werden.

Incident (Vorfall)

Incidents sind Ereignisse *(events)*, bei denen ein IT-Service nicht mehr oder nur eingeschränkt erbracht wird, sodass ein Eingreifen erforderlich ist, das über üblicherweise automatisierte Abhilfemaßnahmen hinausgeht. Ein Incident liegt auch dann vor, wenn die unmittelbare Gefahr eines Ausfalls oder von Qualitätseinbußen von IT-Services besteht und bemerkt wird.

Die damit verbundene Nichtverfügbarkeit bzw. die Einschränkungen oder Einbußen können sich auf den IT-Service selbst oder auf das Leistungsversprechen in Bezug auf die Bereitstellung des IT-Services (*Service Level Agreement, SLA*) beziehen. Siehe auch →*Service Level Management (SLM)*. Eine spezielle Form von Incidents stellen *Sicherheitsvorfälle (security incidents)* dar.

Um die Behandlung von Incidents zu planen, wird die Priorität der Behandlung bestimmt. Siehe →*Priorität*. Die zunächst unbekannte Ursache von Incidents oder eine Ursache, für die keine Abhilfe bekannt ist, wird →*Problem* genannt.

---

[96] IT Infrastructure Library®, eine Sammlung von vordefinierten Prozessen, Aktivitäten und Rollen entlang des Lebenszyklus von IT-Services, wobei die Betriebsphase besonders beachtet wird. Seit 2013 sind ITIL und IT Infrastructure Library eine Marke von Axelos.

Priorität (Incident)

Die Priorität (1), mit der ein *Incident* (Vorfall) behandelt und gelöst werden soll, kombiniert

- (2) das Ausmaß der Auswirkungen (Impact) für die Anwender und
- (3) die sogenannte Dringlichkeit (Urgency).

(2) Die Kenngröße „Auswirkung des Incidents" bzw. **Impact** misst inwieweit die Anwender durch den Vorfall Einschränkungen oder Beeinträchtigungen in ihrem Geschäftsbetrieb erleiden. Der Impact wird unterschiedlich gemessen. D.h., IT-Dienstleister definieren ihre eigene Metrik (Messverfahren). Als bewährtes Verfahren kann gelten, dass die Auswirkung (Impact) wiederum aus zwei Kenngrößen ermittelt wird und zwar aus:[97]

- (2a) der *Serviceeinschränkung (service restriction)*, die primär misst, inwieweit der IT-Service noch verfügbar ist (Totalausfall, teilweiser Ausfall, Leistungseinschränkung usw.), und
- (2b) der *Kritikalität (criticality)*, die die Abhängigkeit der Anwender von der uneingeschränkten Verfügbarkeit des IT-Service hinsichtlich der Aufrechterhaltung des Geschäftsbetriebs misst.

(3) Die Dringlichkeit bzw. **Urgency** betrachtet den zeitlichen Schadensverlauf und misst den Zeitdruck, unter dem die Behandlung des Vorfalls steht.

Der Impact berücksichtigt erst einmal keine Sicherheitsaspekte wie den Verlust der *Vertraulichkeit (confidentiality)* oder der *Integrität (integrity)*. Die Sicherheitsarchitektur *ESARIS* integriert das IT-Sicherheits-Management und das IT-Service-Management, zu dem das *Incident Management* (Vorfallmanagement) gehört.[98] Um das Ausmaß der Auswirkungen eines *Sicherheitsvorfalls (security incident)* bestimmen zu können, werden dort die *Serviceeinschränkung (service restriction)* und die *Kritikalität (criticality)* entsprechend erweitert.[99]

Kritikalität (criticality)

Die Kritikalität (criticality) misst die Abhängigkeit des Anwenders vom reibungslosen Betrieb eines IT-Services. Sie ist als Eigenschaft von verwendeten IT-Elementen (*Configuration Items*, Konfigurationselementen) anzusehen, die zur Bereitstellung eines bestimmten IT-Services für bestimmte Anwender benötigt

---

97 Stephan Kasulke und Jasmin Bensch: Zero Outage, Kompromisslose Qualität in der IT im Zeitalter der Digitalisierung; Springer Gabler, Wiesbaden, 2016, 205 Seiten, ISBN 978-3-658-14221-6

98 Eberhard von Faber and Wolfgang Behnsen: Secure ICT Service Provisioning for Cloud, Mobile and Beyond (ESARIS: The Answer to the Demands of Industrialized IT Production Balancing Between Buyers and Providers); Springer Vieweg, Wiesbaden 2017, 383 pages, 159 figures, ISBN 978-3-658-16481-2, 2nd updated and extended Edition, https://doi.org/10.1007/978-3-658-16482-9

99 Siehe auch Kapitel 5.3.2.

werden. Die Kritikalität spielt eine Rolle bei der Bestimmung der Auswirkung (→*Impact*) eines *Incidents* (Vorfalls).

Es kann als bewährtes Verfahren gelten, die Kritikalität explizit als Eingangsgröße zur Bestimmung des Impacts zu verwenden.[100] Entsprechend wird der Wert im Konfigurationsdatensatz abgespeichert und in der *Configuration Management Database (CMDB)* abrufbar gehalten.

Beispiele für Parameter, die die Kritikalität beeinflussen sind: Anzahl der Kunden (Anwenderorganisationen), die auf das CI angewiesen sind; Anzahl der Anwender (Nutzer), die auf das CI angewiesen sind; Bedeutung des Geschäftsprozesses, für das der IT-Service mit dem CI eingesetzt wird. Es können auch finanzielle Verluste beim Ausfall und Auswirkungen auf die Reputation berücksichtigt werden.

Für die Kritikalität kann ein einfaches Raster verwendet werden, da sie letztendlich nur als eine Eingangsgröße für die Bestimmung der *Priorität* verwendet wird, mit der ein *Incident* (Vorfall) behandelt und gelöst werden soll.

Um das Ausmaß der Auswirkungen eines *Sicherheitsvorfalls (security incident)* bestimmen zu können, sollte die Kritikalität nicht nur den Verlust der *Verfügbarkeit* berücksichtigen, sondern auch den der *Vertraulichkeit* und *Integrität*. Diese Erweiterung gegenüber ISO/IEC 20000 und ITIL wird insbesondere in der Sicherheitsarchitektur *ESARIS* definiert.

Serviceeinschränkung (service restriction)

Die Serviceeinschränkung (service restriction) misst das Ausmaß der Verschlechterung (Degradierung; degradation) der Serviceerbringung im Falle eines *Incidents* (Vorfalls). Sie berücksichtigt nicht die Nutzung des IT-Services oder der IT-Systeme im Geschäftskontext des Anwenders (Kunden). Die Serviceeinschränkung spielt eine Rolle bei der Bestimmung der Auswirkung eines Incidents (*impact*).

Es kann als bewährtes Verfahren gelten, die Serviceeinschränkung explizit als Eingangsgröße zur Bestimmung des Impacts zu verwenden und dafür eine einheitliche Metrik (Messverfahren) zu definieren.

Für die Serviceeinschränkung kann ein einfaches Raster verwendet werden, da sie letztendlich nur als eine Eingangsgröße für die Bestimmung der *Priorität* verwendet wird, mit der ein Incident (Vorfall) behandelt und gelöst werden soll.

Die Serviceeinschränkung (service restriction) betrachtet lediglich die Verfügbarkeit (siehe auch *Service Availability*) und Einschränkungen der Service-Qualität. Um auch das Ausmaß der Auswirkungen eines *Sicherheitsvorfalls (security*

---

[100] Stephan Kasulke und Jasmin Bensch: Zero Outage, Kompromisslose Qualität in der IT im Zeitalter der Digitalisierung; Springer Gabler, Wiesbaden, 2016, 205 Seiten, ISBN 978-3-658-14221-6

incidents) bestimmen zu können, sollte die Serviceeinschränkung nicht nur den Verlust der Verfügbarkeit berücksichtigen, sondern auch den der *Vertraulichkeit* und *Integrität*. Diese Erweiterung gegenüber ISO/IEC 20000 und ITIL wird insbesondere in der Sicherheitsarchitektur *ESARIS* definiert.

Problem

Ein Problem bezieht sich auf die Ursache von *Incidents (Vorfällen)*, einer schlechten Performance, unzureichender Kapazität oder mangelhafter Funktionen. Ein Problem erfordert eine Lösung. Die Ursache (root cause) ist jedoch zum Zeitpunkt der Erstellung der Problem-Meldung bzw. der Problem-Aufzeichnung noch nicht bekannt. Für die weitere Untersuchung ist der Prozess *Problem Management* verantwortlich.

Der Problem-Management-Prozess wird nicht notwendigerweise durch das Auftreten eines Incidents (Vorfalls) angestoßen. Es kann sich auch um vorbeugende Aktivitäten handeln oder um Verbesserungen, die nur den IT-Dienstleister selbst betreffen und den Anwendern nicht als Leistungsparameter garantiert werden.

5.2 IT-Service-Management (ITSM)

Um IT-Services effizient und mit gleichbleibend guter Qualität herstellen zu können, wurden die dazu notwendigen Aktivitäten strukturiert und standardisiert.

Es wurden allgemeine Ziele bzw. übergeordnete Absichten identifiziert und zu einer überschaubaren Anzahl von Aufgaben zusammengefasst. Für jede dieser Aufgaben wurden Aktivitäten definiert, die erforderlich sind, um die Ziele zu erfüllen. Da die Aktivitäten Abhängigkeiten besitzen und in einer logischen Reihenfolge abzuarbeiten sind, spricht man von *Prozessen*, genauer von **IT-Service-Management**- oder kurz ITSM-Prozessen.

ITIL®[101] wurde als Sammlung bewährter Verfahren („best practices“) entwickelt und mehrfach den Erfordernissen angepasst und aktualisiert. Die Bereitstellungs- und Betriebsprozesse der IT sind auch als internationaler Standard in ISO/IEC 20000-2[102] spezifiziert. Die folgende Beschreibung der wichtigsten IT-Service-Management-Prozesse bezieht sich auf die Standardreihe ISO/IEC 20000. Abb. 37 bietet eine Übersicht über die Prozessstruktur.

---

[101] IT Infrastructure Library®, eine Sammlung von vordefinierten Prozessen, Aktivitäten und Rollen entlang des Lebenszyklus von IT-Services, wobei die Betriebsphase besonders beachtet wird. ITIL und IT Infrastructure Library sind eingetragene Warenzeichen der Axelos Ltd.

[102] ISO/IEC 20000-2 - Information technology — Service management — Part 2: Guidance on the application of service management systems

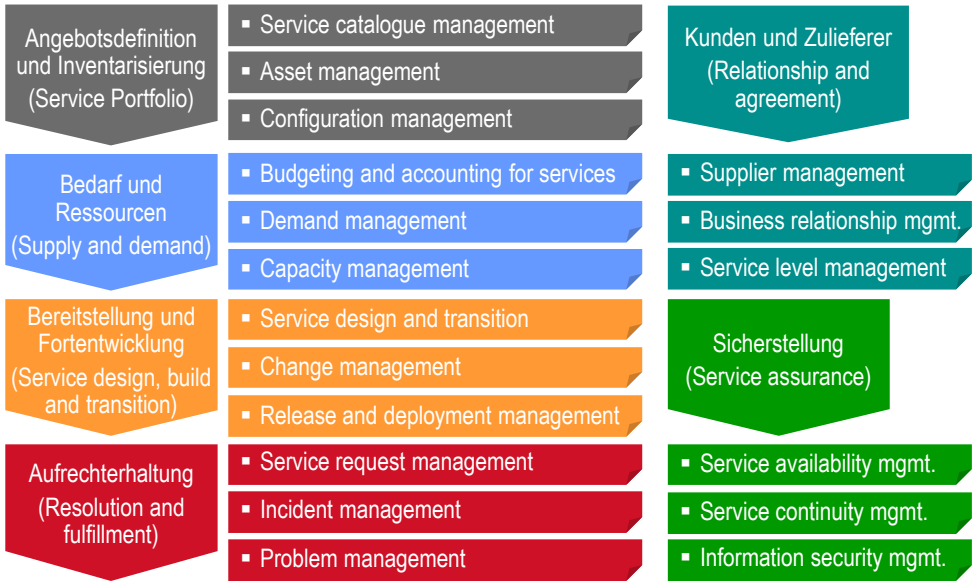


Abb. 37: Grundsätzliche Struktur der ITSM-Prozesse nach ISO/IEC 20000

5.2.1 Anmerkungen zum Lebenszyklus

ITIL Version 3 teilt die Prozesse in fünf Bereiche oder Bücher ein: Strategy, Design, Transition, Operation und Continuous Improvement. Alle fünf werden durch Prozesse näher spezifiziert. Damit werden die Prozesse anscheinend entlang eines Lebenszyklus angeordnet. Allerdings liegt der Schwerpunkt auf den IT-Verfahren, Abläufen und Prozessen für den IT-Betrieb.

ISO/IEC 20000 betont, dass sich der Standard auf alle Aktivitäten entlang des Lebenszyklus eines IT-Services bezieht, die zusätzlich zu den täglichen betrieblichen Aktivitäten durchgeführt werden, und dass der Lebenszyklus die Planung (planning), Implementierung (transition), Bereitstellung (delivery) und Verbesserung (improvement) umfasst.[103] ISO/IEC 20000 definiert einen Prozess *Service Design and Transition*, der sich zusammen mit dem Änderungswesen in einer Prozessfamilie befindet (siehe Kapitel 5.2.6). Trotzdem liegt der Fokus sehr klar auf Prozessen, die sich im weitesten Sinne auf die Aufrechterhaltung der Serviceerbringung beziehen. Manche Prozesse haben einen planerischen und einen operativen Anteil. Manche erstrecken sich über einen weiten Teil des Lebenszyklus der IT-Services, andere auf einen kürzeren Abschnitt. Die einzelnen Prozesse sollten als Aufgaben verstanden werden, die in einzelne Aktivitäten aufgegliedert sind, die wiederum auszuführen sind, damit IT-Services gemäß den Anforderungen über einen längeren Zeitraum bereitgestellt werden können.

---

[103] ISO/IEC 20000-1 Information technology — Service management — Part 1: Service management system requirements

Für das Gesamtverständnis wichtig ist aber auch die Tatsache, dass der IT-Dienstleister im Rahmen der Entwicklung der Service-Strategie (ITIL) nach Marktchancen und Absatzmöglichkeiten sucht und Geschäftsfelder und angebotene IT-Services danach ausrichtet. Das Ergebnis ist ein **Service Portfolio**, das eine Aufstellung aller Angebote des IT-Dienstleisters darstellt und laufend über den gesamten Lebenszyklus angepasst und aktualisiert wird. Der ITIL-Prozess für die Entwicklung und Pflege des Portfolios heißt Service Portfolio Management:

Service Portfolio Management (ITIL)

Portfoliomanagement ist ein systematischer Ansatz der Unternehmensplanung. Dabei werden Geschäftsmöglichkeiten analysiert und bewertet. Schließlich wird eine Entscheidung getroffen, welche Geschäftsmöglichkeiten genutzt und in den Katalog der Angebote aufgenommen werden sollen, das Portfolio genannt wird.

Das Service Portfolio umfasst alle IT-Services, die der IT-Dienstleister anbietet. Der Service-Portfolio-Management-Prozess entwickelt und pflegt das Portfolio und sorgt dafür, dass alle IT-Services den versprochenen bzw. erwarteten Nutzen bei entsprechenden Kosten erbringen. Der Prozess erstreckt sich über den gesamten Lebenszyklus der IT-Services.

5.2.2 Angebotsdefinition und Inventarisierung (service portfolio)

Vom Service Portfolio Management (Kapitel 5.2.1) gibt es einem direkten Zusammenhang zur Verwaltung der Service-Kataloge. Dabei handelt es sich um eine Übersicht über alle angebotenen IT-Services, die auch unterstützende Leistungen beschreibt. Diese Kataloge sind die Grundlage dafür, die Konfiguration der IT-Services für den Kunden zusammenzustellen. Sie dienen aber auch der Unterstützung des internen Bestellwesens und der Organisation der internen Lieferkette.

Neben dem Service Catalogue Management ordnet ISO/IEC 20000 dieser Prozessfamilie auch die Prozesse zur Inventarisierung zu, was die aktive Verwaltung von Unternehmenswerten, IT-Komponenten, Dokumenten und dergleichen umfasst. Siehe Abb. 37 auf Seite 141.

Service Catalogue Management

Liefert und pflegt den Service-Katalog, der alle Informationen über zwei Arten von IT-Services enthält: die für Kunden nutzbaren und die unterstützenden IT-Services, die für erstere benötigt werden. Für die beiden Arten sind die Begriffe „customer-facing“ und „supporting“ IT-Services gebräuchlich.

Der **Service Catalogue** (Service-Katalog) definiert und beschreibt alle für Anwenderorganisationen (Kunden des IT-Dienstleisters) buchbaren IT-Services mit allen auswählbaren Optionen. Er ist meist Grundlage für die Beschaffung durch die Kunden. Der Service-Katalog ist auch die Basis für die Beschaffung

beim IT-Dienstleister, d.h. die Organisation der internen Lieferkette und den Einkauf bzw. die Beschaffung von Leistungen Dritter.

Asset Management

Verwaltet Werte, die für die Bereitstellung von IT-Services nötig sind. Dies umfasst zum Beispiel Hardware, Geräte, Lizenzen und Gebäude. Viele der zu verwaltenden Werte sind zugleich *Configuration Items (CIs)* und werden entsprechend durch das →*Configuration Management* verwaltet.

Configuration Management

Dieser Prozess verwaltet Informationen über →*Configuration Items (CIs)* und ihre Beziehungen zueinander und stellt damit über deren gesamten Lebenszyklus hinweg verlässliche Informationen über IT-Services und alle Service-Komponenten bzw. ihre Bestandteile bereit.

Der Prozess bildet eine wichtige Grundlage für andere Prozesse wie das Vorfallmanagement (*Incident Management*), denn insbesondere bei der Fehlersuche und -beseitigung werden Informationen über die Zusammensetzung, Konstruktion und Einrichtung der IT, über Versionsstände von Software und Hardware und dergleichen benötigt. Diese Informationen werden in Form von Konfigurationsdatensätzen in einer Konfigurationsdatenbank (**Configuration Management Database, CMDB**) gespeichert und abrufbar gehalten.

Der Prozess stellt auch sicher, dass Änderungen an Configuration Items (CIs) autorisiert sind und dass die Produktionsumgebung korrekt in der CMDB abgebildet ist.

Der Prozess ist auch unter den Namen **Service Asset Configuration Management** und **Asset and Configuration Management** bekannt.

5.2.3 Kunden und Zulieferer (relationship and agreement)

Ein IT-Dienstleister ist einerseits auf Lieferanten angewiesen, die IT-Komponenten oder sogar komplette IT-Services beisteuern, und andererseits gibt es Abhängigkeiten zu den Kunden, für die er die IT-Services produziert. Entsprechend definiert ISO/IEC 20000 zwei Prozesse, die dabei helfen, die externen Beziehungen erfolgreich zu gestalten. Ein weiterer Prozess regelt Übereinkünfte bzw. das Vertragswesen. Siehe Abb. 37 auf Seite 141.

Die Unterhaltung der Geschäftsbeziehungen (Relationship Processes) spielt eine wichtige Rolle für die Aufrechterhaltung der Serviceerbringung im Betrieb (Operations). Allerdings muss der IT-Dienstleister die Beziehungen sowohl zu den Anwendern bzw. Kunden (Business Relationship Management, BRM) als auch zu den Zulieferern (Supplier Management) schon bei der Entwicklung und vor der Überführung in den Normalbetrieb gestaltet haben. Und eigentlich spielt das Beziehungsmanagement zu möglichen Kunden ja eine entscheidende Rolle dabei, überhaupt Geschäft einwerben und Verträge schließen zu können. Das ändert aber nichts

daran, dass die Geschäftsbeziehungen ihre Bewährungsprobe häufig erst in der Betriebsphase bei der Fortentwicklung und Aufrechterhaltung der IT-Services bestehen müssen.

Supplier Management

Dieser Prozess stellt sicher, dass die von Dritten (den Zulieferern) bezogene Hardware, Software sowie Komponenten, Systeme, IT-Services oder sonstige Dienstleistungen die erforderlichen Eigenschaften wie Funktionalität und Qualität aufweisen. Er stellt auch sicher, dass Verträge vereinbart und vom Lieferanten eingehalten werden. Der Prozess umfasst aber auch die Anpassung der Verträge, Ausnahmeregelungen, Streitschlichtungen und dergleichen und erstreckt sich auch auf Sublieferanten (Lieferanten der Lieferanten).

Das Ziel besteht darin, dass die Leistungen der Zulieferer so abgestimmt und integriert werden, dass der IT-Dienstleister die IT-Services einschließlich ihrer Service-Levels vertragsgemäß erbringen kann.

Business Relationship Management (BRM)

Dieser Prozess gestaltet die Beziehung zu den Kunden des IT-Dienstleisters, also zu Anwenderorganisationen. Der IT-Dienstleister soll das geschäftliche Umfeld verstehen, in dem der Kunde die IT-Services einsetzt. Dies soll ihn in die Lage versetzen, die Anforderungen und Erwartungen des Kunden und eventueller weiterer Interessengruppen zu verstehen und entsprechend darauf reagieren zu können. Das Beziehungsmanagement beschränkt sich nicht auf die Geschäftsanbahnung und endet nicht mit dem Vertragsabschluss. Vielmehr sind die Behandlung von Beschwerden im Betrieb und auch Änderungen des Umfangs der IT-Services, der Service-Levels sowie des Vertrages insgesamt ausdrücklich eingeschlossen.

Der Prozess steht in enger Beziehung mit dem *Service Level Management (SLM)*, da in diesem Prozess a) die Service-Kataloge (*Service Catalogues)* herangezogen werden und b) kundenbezogen die zu erbringenden IT-Services und ihre Zielgrößen definiert werden. Das SLM bezieht sich auf die betriebliche Umsetzung („operational"), während sich das Business Relationship Management (BRM) auf die geschäftlichen Aspekte bezieht.

Service Level Management (SLM)

Dieser Prozess sorgt für den Abschluss von drei Arten von Verträgen, vor allem aber für deren Konsistenz und Einhaltung. Im Vordergrund stehen die Verträge mit Anwenderorganisationen (Kunden des IT-Dienstleisters). Dazu kommen sogenannte **Operational Level Agreements (OLAs)** oder Vereinbarungen auf Betriebsebene). Das sind Verträge, die der IT-Dienstleister intern mit Einheiten schließt, die IT-Services bereitstellen. Drittens werden Verträge mit Lieferanten geschlossen, die auch **Underpinning Contracts (UC**) genannt werden. Den Verträgen liegen Anforderungen zugrunde, die im Rahmen des Prozesses erfasst

und dokumentiert werden. Der Prozess arbeitet eng mit dem *Business Relationship Management (BRM)* und auch mit dem *Supplier Management* zusammen.

In herkömmlichen IT-*Outsourcing*-Verträgen wird unterschieden zwischen Service-Beschreibung einerseits (**Statement of Work**, auch **Leistungsschein** genannt) und dem Leistungsversprechen in Bezug auf die Bereitstellung des IT-Services (**Service Level Agreement, SLA**) anderseits. Während eine Service-Beschreibung definiert, „was" geliefert wird, definiert das Leistungsversprechen (SLA) das „Wie", also die Qualität und die Leistungsparameter. ISO/IEC 20000 spricht von „Service" und „Service targets". ITIL verfährt ähnlich und unterscheidet zwischen **Utility**) (erforderlicher Funktionalität) und **Warranty** (zu erreichenden Service Levels).

Der Prozess ist auch für die Überwachung der Einhaltung insbesondere der SLAs verantwortlich. In ITIL umfasst der Prozess auch das *Service Reporting* (Berichtswesen), während er in früheren Versionen der ISO/IEC 20000 als eigener Prozess definiert wurde.

Service Reporting

Dieser Prozess[104] erzeugt aussagekräftige und verlässliche Berichte (reports) für den IT-Dienstleister, seine Kunden und weitere interessierte Parteien. Ihr Inhalt deckt den identifizierten Informationsbedarf der Adressaten und unterstützt, diese dabei, in ihrem Aufgabenbereich Entscheidungen zu treffen.

Die Berichte basieren auf der Erfassung betrieblicher Daten (Monitoring) und führen einen Soll-/Ist-Vergleich durch. Es gibt reaktive und proaktive Berichte. Reaktive Berichte informieren über den Verlauf von Kenngrößen nach einem Ereignis oder Vorfall. Proaktive Berichte geben Warnhinweise, sodass vorbeugende Maßnahmen ergriffen werden können.

5.2.4 Bedarf und Ressourcen (supply and demand)

In dieser Prozessfamilie befinden sich drei Prozesse. Siehe Abb. 37 auf Seite 141.

Budgeting and Accounting for Services

Budgets werden auf Basis von Kostenabschätzungen festgelegt. Die Buchführung (accounting) ermittelt die wirklichen Ausgaben und vergleicht sie mit den Budgets. Abweichungen von den Budgets werden ermittelt, gelöst und die betroffenen Parteien werden darüber informiert. Die buchhalterischen Verfahren sind an denen des IT-Dienstleisters bzw. des gesamten Unternehmens ausgerichtet.

---

[104] In der aktuellen Version von ISO/IEC 20000 nicht mehr als eigenständiger Prozess definiert. Er ist daher in Abb. 37 auch nicht dargestellt.

Demand Management (Nachfragemanagement)

In diesem Prozess werden die Anforderungen und Erwartungen der Kunden (Nutzer und Anwenderorganisationen) gesammelt, verstanden, analysiert, beurteilt und intern kommuniziert, sodass die notwendigen Kapazitäten (capacity) bereitgestellt werden können. Im Vordergrund stehen die Vorhersage und Verbrauchserfassung.

Capacity Management (Kapazitätsmanagement)

Der Prozess soll sicherstellen, dass ausreichende Kapazitäten (capacity) zur Verfügung stehen, um die vereinbarten Leistungsparameter der IT-Services einhalten zu können. Dabei werden die aktuell genutzten Kapazitäten überwacht und zukünftige Bedarfe ermittelt und bereitgestellt. Dabei spielt die Kapazitätsplanung eine wichtige Rolle.

Der Begriff Kapazität (capacity) bezieht sich auf menschliche und technische Ressourcen sowie auf Informationen und die finanzielle Ausstattung. Das Kapazitätsmanagement hat eine reaktive und eine proaktive Komponente. Bei der reaktiven liegt der Fokus auf der Erfassung betrieblicher Daten (Monitoring), der Anpassung, Analyse und Verbesserung der Kapazitäten. Der proaktive Teil des Kapazitätsmanagements konzentriert sich auf die Planung, um zukünftige Bedarfe abdecken zu können.

5.2.5 Sicherstellung (service assurance)

Diese Prozessfamilie besteht aus drei Prozessen, wobei das „Information Security Management“ eine Sonderrolle einnimmt und in ISO/IEC 20000 ähnlich unspezifisch gestaltet ist wie in ITIL. Siehe Abb. 37 auf Seite 141.

Service Availability Management (Verfügbarkeitsmanagement)

Eine eher technische bzw. auf die IT-Infrastruktur bezogene Disziplin, die das Ziel verfolgt, durch Verfahrensweisen und technische Merkmale die Verfügbarkeit, die Ausfallsicherheit und die Wiederherstellung so zu gestalten, dass die Dienstleistungsgüte (Service Level) sichergestellt und das Leistungsversprechen (Service Level Agreement) eingehalten werden kann.

Unter **(Service) Availability** (Verfügbarkeit) wird hier die Eigenschaft eines IT-Services oder einer Service-Komponente verstanden, seine bzw. ihre geforderte Funktion zu einem vereinbarten Zeitpunkt oder über einen vereinbarten Zeitraum zu erbringen.[105]

[105] ISO/IEC 20000-1 Information technology — Service management — Part 1: Service management system requirements

Service Continuity Management

Konzentriert sich auf die Bewältigung eher außergewöhnlicher Vorfälle wie Katastrophen und verfolgt das Ziel, Risiken beherrschen zu können und die Auswirkungen möglicher Unterbrechungen der IT-Services oder eines Datenverlusts zu minimieren, was eine rechtzeitige und vollständige Wiederherstellung der Dienste und Daten einschließt.

Das Service Continuity Management kann als eine Teilmenge des *Business Continuity Managements (BCM)*[106] angesehen werden.[107]

Unter **Service Continuity** versteht man die Fähigkeit, Risiken und Vorkommnisse beherrschen zu können, die ernsthafte Auswirkungen auf einen IT-Service haben können, damit die IT-Services kontinuierlich entsprechend den Vereinbarungen geliefert werden.[108]

Information Security Management

Dieser Prozess soll sicherstellen, dass Sicherheitsmaßnahmen (security controls) implementiert sind, um Informationen zu schützen, und dass die entsprechenden Anforderungen bei der Entwicklung und Implementierung von neuen IT-Services und größeren Änderungen berücksichtigt werden.

Die Darstellung des Prozesses Information Security Management hier und auch im Standard umfasst bei weitem nicht alle Aufgaben. Ausführlicher sind diese in ISO/IEC 27001 beschrieben.[109]

5.2.6 Bereitstellung und Fortentwicklung (service design, build and transition)

Die drei Prozesse umfassen Aufgaben, bei denen die Informationstechnologie bzw. die IT-Services direkt verändert werden. Siehe Abb. 37 auf Seite 141. Dabei wird dem Entwurf bzw. der Entwicklung (design) und der Implementierung (transition) ein eigener Prozess gewidmet.[110] Prinzipien dafür werden in ISO/IEC 20000 auch unter der Überschrift „Service portfolio“ (siehe Kapitel 5.2.2) beschrieben.

---

106 ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements (ersetzt BS 25999-1:2006 seit 2012)

107 ISO/IEC 20000-1 Information technology — Service management — Part 1: Service management system requirements

108 ebenda.

109 ISO/IEC 27001 – Information technology – Security techniques – Information security management systems – Requirements; 2013

110 In früheren Versionen von ISO/IEC 20000 waren „Entwicklung und Implementierung“ nicht als ein eigenständiger Prozess ausgebildet. Der Standard definierte generelle Leitlinien dafür. Diese sollten explizit sowohl für neue als auch für Änderungen bestehender IT-Services gelten. Änderungen (gemeint sind größere Änderungen) sollten also ganz

Zugehörige Grundbegriffe sind in Kapitel 5.1.1 zu finden.

Service Design and Transition

Dieser Prozess stellt sicher, dass Planung (planning), Entwicklung (design), Implementierung (build) und Überführung in den Betrieb (transition) auf der Grundlage von definierten und vereinbarten Anforderungen an die IT-Services erfolgen. Der Prozess bezieht sich auf die Einführung neuer IT-Services, die Änderung existierender, das Einstellen (Entfernen) eines IT-Services und die Übertragung eines IT-Services zu einem anderen IT-Dienstleister. Die Aktivitäten erstrecken sich von der Anforderungsanalyse über die Konzeptionierung bis hin zum Betrieb und letztendlich dessen Einstellung oder Übertragung.[111]

Die Planungsphase umfasst Themen wie Verantwortlichkeiten, Ressourcen, Abhängigkeiten, Anforderungen (auch an das Testen), Abnahmekriterien, Risikomanagement und Ergebnisdefinition.

Die Designphase produziert Entwicklungsunterlagen und umfasst diverse Aufgaben, wie zum Beispiel Änderungen im Vergleich zur Planungsphase in Bezug auf Ressourcen zu identifizieren. Weiterhin werden Schulungsanforderungen definiert, Service-Kataloge aktualisiert sowie Auswirkungen auf Verträge, SLAs usw. untersucht.

In der Implementierungsphase werden Komponenten zusammengefügt, getestet und entsprechend der definierten Kriterien abgenommen.

Die Überführung in den Betrieb erfolgt, Freigabe durch das *Change Management* vorausgesetzt, im Rahmen des *Release and Deployment Management*s.[112]

Change Management

Dieser Prozess hat die Aufgabe, die Durchführung von Änderungen (Changes) zu koordinieren und dabei für minimale Beeinträchtigungen und Risiken zu sorgen. Auslöser ist ein Änderungsantrag (*Request for Change, RfC*). Alle Änderungsanträge müssen bewertet und freigegeben werden; dann werden die Änderungen implementiert und überprüft.

Alle Änderungen werden durch ein **Change Advisory Board (CAB)** der Produktionseinheit explizit freigegeben. Davon können nur geringfügige Änderungen (**Standard changes**) ausgenommen werden, die vorab autorisiert wurden und mit geringem Risiko standard- bzw. routinemäßig umgesetzt werden können. Alle anderen Änderungen sind entweder geplante Änderungen (**Normal changes**) oder zeitkritische Änderungen (**Emergency changes**). Für besonders

---

ähnlich behandelt und durchgeführt werden wie die „Entwicklung und Implementierung" neuer IT-Services.

111 ISO/IEC 20000-2 - Information technology — Service management — Part 2: Guidance on the application of service management systems

112 ebenda.

umfangreiche, komplexe und risikoreiche Änderungen wird die Überprüfung und Freigabe oft erweitert (zum Beispiel um ein Central Change Advisory Board, CCAB).[113] Im Falle von zeitkritischen Änderungen (Emergency changes) wird die Freigabe verkürzt und zum Beispiel einem Manager on Duty (MoD) übertragen[114] oder einem Emergency Change Advisory Board (ECAB) mit hoher Verfügbarkeit und schneller Reaktionsweise.

Die geplanten Änderungen (Normal changes) werden hinsichtlich ihrer Komplexität bzw. des Risikos von Fehlern kategorisiert in Major, Significant und Minor Changes.

Der Prozess ist, insbesondere bei umfangreicheren Änderungen, auch dafür verantwortlich, dass Vorkehrungen getroffen werden, den ursprünglichen Zustand wiederherstellen zu können (back-out), falls die Änderung nicht erfolgreich umgesetzt werden konnte (Contingency and back-out/roll-back planning).

Alle Informationen zu einem Change und alle Vorgänge bei der Umsetzung werden in einem **Change Record** (einem Datensatz, der auch Ticket genannt wird) aufgezeichnet. Ein **Change Model** bezeichnet eine Beschreibung in Form einer Vorlage (template), nach der alle gleichartigen Änderungen durchgeführt werden.

Nach erfolgreicher Umsetzung der Änderung wird die neue Konfiguration in der *Configuration Management Database (CMDB)* (Konfigurationsdatenbank) vermerkt.

Release and Deployment Management

Dieser Prozess stellt sicher, dass ein →*Release* (Sammlung von Hardware, Software, Dokumentation, Prozessen oder anderen Komponenten) in der Zielumgebung korrekt eingerichtet oder installiert wird (**Deployment**).

Dabei werden typischerweise mehrere Änderungen (Changes) umgesetzt. Der Prozess koordiniert die Planung und steuert die Implementierung, das Testen, die Freigabe und den Betriebsübergang. Die Aufgaben umfassen aber auch zum Beispiel die Schulung und die Dokumentation. Pilot- und Versuchsphasen können dem Betriebsübergang vorausgehen.

5.2.7 Aufrechterhaltung (resolution and fulfillment)

Die Prozesse dieser Familie beschäftigen sich mit der Erfüllung von Kundenaufträgen gemäß Vertrag (service requests), der Behandlung von Vorfällen und der Lösung von Problemen. Die dafür notwendigen Änderungen an der IT werden aber

---

[113] Stephan Kasulke und Jasmin Bensch: Zero Outage, Kompromisslose Qualität in der IT im Zeitalter der Digitalisierung; Springer Gabler, Wiesbaden, 2016, 205 Seiten, ISBN 978-3-658-14221-6

[114] ebenda.

weiterhin durch die Bereitstellungsprozesse (Kapitel 5.2.6) durchgeführt. Siehe Abb. 37 auf Seite 141.

Zugehörige Grundbegriffe sind in Kapitel 5.1.2 zu finden.

Service Request Management

Dieser Prozess, auch **Request Fulfillment** genannt, sorgt für die Bearbeitung von Aufträgen der Anwender durch den IT-Dienstleister. Dabei handelt es sich in der Regel um Standardaufgaben (laut Vertrag), wie zum Beispiel das Anlegen eines neuen Nutzers oder das Zurücksetzen eines Passwortes. Letzteres erklärt die Nähe zum *Incident Management*, weshalb beide Prozesse in derselben Familie zu finden sind.

Incident Management (Vorfallmanagement)

Dieser Prozess hat die Aufgabe, den IT-Service nach Bekanntwerden eines Vorfalls (→*Incidents*) so schnell wie möglich und in einer Weise wiederherzustellen, dass die Auswirkungen auf den Geschäftsbetrieb minimiert werden und er schließlich nicht mehr beeinträchtigt ist. Dies erfolgt durch eine provisorische Lösung (workaround) oder die Implementierung einer endgültigen Lösung, die die Ursache der Störung beseitigt.

Der Prozess wird durch das Auftreten bzw. die Meldung eines Vorfalls ausgelöst, bei dem es sich um eine ungeplante Unterbrechung oder eine Minderung der Qualität eines IT-Services handelt. Der Prozess erfasst Informationen über den Vorfall und ordnet dem Vorfall Kategorien zu, die den möglichen Fehlerort bzw. die Fehlerursache eingrenzen.

Dann erfolgt ein Vergleich mit bereits bekannten Fehlern unter Zuhilfenahme der „*Known Error Database*“ (Datenbank bekannter Fehler), die vom *Problem Management* gepflegt wird. Sind Fehler und Lösung bekannt, so wird die Implementierung der Maßnahmen zur Fehlerbehebung in der Regel durch einen *Emergency Change* veranlasst. In einfachen Fällen, zum Beispiel, wenn der Anwender den Fehler selbst beseitigen kann und muss, führt der sogenannte **1st Level Support** den Anwender zur Lösung.

Sind Fehler bzw. Ursache und Lösung dafür nicht bekannt, so wird zunächst die →*Priorität* des Incidents bestimmt, da in einem größeren IT-Betrieb oft viele Störungen zugleich auftreten und sich die begrenzten Ressourcen zuerst den dringendsten Fällen mit den größten Auswirkungen widmen müssen. Die Suche nach einer Lösung wird Spezialisten übertragen (**2nd Level Support**), die falls nötig, auch Lieferanten und Hersteller heranziehen (**3rd Level Support**). Die Priorität bestimmt den Ablauf im Detail.

Major Incidents sind schwerwiegende Vorfälle mit der höchsten Priorität. Sie bedeuten meist eine vollständige Unterbrechung eines kritischen Geschäftsprozesses des Anwenders und werden deshalb nach einem anderen Verfahren behandelt als dem im Standardprozess definierten. Der wesentliche Unterschied

besteht darin, dass der Incident nicht mehr allein durch die betriebsverantwortliche Einheit selbst behandelt wird. Es werden Ressourcen und Instrumente genutzt, über die nur die Gesamtorganisation verfügt bzw. die nur sie heranziehen kann. Manche Organisationen nutzen einen vergleichbar verstärkten Prozess auch für Vorfälle der zweithöchsten Priorität.

Der Prozess besitzt eine Schnittstelle mit dem Anwender, die auch als **Service Desk** bezeichnet wird. Handelt es sich bei den Kunden des IT-Dienstleisters um Anwenderorganisationen wie zum Beispiel große Firmen, so ist die Interaktion der beteiligten Parteien komplex und umfasst mehr als nur den Austausch von Meldungen.

Alle Informationen zu einem Incident und alle Vorgänge bei dessen Bearbeitung werden in einem **Incident Record** (einem Datensatz, der auch Ticket genannt wird) aufgezeichnet.

Problem Management

Das Ziel dieses Prozesses ist, die Ursache eines Incidents (Vorfalls) zu finden, um durch eine gefundene Lösung das wiederholte Auftreten des Vorfalls verhindern zu können. Diese Fehlersuche erfolgt nach einem Vorfall zum Beispiel dann, wenn nur eine provisorische Lösung (workaround) implementiert wurde, die eigentliche Ursache des Vorfalls aber noch nicht bekannt ist (reaktives Problem Management). Generell werden dabei mögliche Schwachpunkte gesammelt und Verbesserungspotenziale identifiziert. Gefundene Fehlerursachen bzw. deren Lösungen werden in der **Known Error Database** (Datenbank bekannter Fehler) abgelegt und dem *Incident Management* zur Verfügung gestellt, um die Beseitigung erneuter Störungen zu beschleunigen.

Das proaktive Problem Management sucht nach Mustern, analysiert Beschwerden und sonstige Hinweise und führt Erfahrungen aus früheren Vorfällen plattformübergreifend zusammen, um daraus Maßnahmen abzuleiten, die das Auftreten von Vorfällen vermeiden helfen. Stützt sich dieses Verfahren überwiegend auf Informationen, die automatisch erhoben und ausgewertet werden, so gibt es Ähnlichkeiten zu vorausschauender Instandhaltung (predictive maintenance), die im Maschinen- und Anlagenbau verbreitet ist, und auch zum Beispiel bei Storage-Systemen mit Festplatten längst Einzug in die IT gehalten hat.

Alle Informationen zu einem *Problem* und alle Ergebnisse bei dessen Analyse werden in einem **Problem Record** (einem Datensatz, der auch Ticket genannt wird) aufgezeichnet. Das Problem Management benötigt Zugriff auf die *Configuration Management Database (CMDB)* (Konfigurationsdatenbank) und andere Details zum Beispiel über Prozesse, Abläufe und Verfahren.

5.3 IT-Sicherheit im IT-Service-Management (ITSM)

5.3.1 Secured by Definition

Praktisch alle größeren IT-Organisationen setzen ISO/IEC 20000 oder ITIL ein bzw. orientieren sich bei der Gestaltung ihres IT-Betriebes an den dort definierten Prozessen des IT-Service-Managements (ITSM). Doch das Thema IT-Sicherheit ist sowohl in ISO/IEC 20000 als auch in ITIL nur oberflächlich vertreten.

Daher werden in diesem Kapitel einige Erweiterungsmöglichkeiten beschrieben. Die Darstellung folgt dem in diesem Buch in Kapitel 2.2.3 bereits beschriebenen Sicherheitsprinzip →*Secured by Definition*". Das Konzept ist Teil der Sicherheitsarchitektur →*ESARIS*,[115] die ab 2010 entwickelt und 2013 erstmals als Buch zugänglich gemacht wurde, das 2017 in aktualisierter und erweiterter Auflage erschien.[116] ESARIS integriert IT-Security-Management (ISO/IEC 27001) und IT-Service-Management (ISO/IEC 20000, ITIL) erstmals konsequent: Alle ablauf- oder prozessbezogenen Sicherheitsmaßnahmen einschließlich aller Schritte zur Implementierung und Aufrechterhaltung technischer Sicherheitsmaßnahmen werden Teil der ITSM-Prozessschritte, der dort verwendeten Tools sowie der Anweisungen für das IT-Personal und decken alle Abschnitte des erweiterten Lebenszyklus (Vertrieb, Angebotsmanagement, Bereitstellung mit Migration und Betrieb) ab.

Warum? Es ist erstens so, dass die IT-Organisation die Verantwortung für die Bereitstellung der IT-Services gemäß den Anforderungen trägt und sehr wohl in der Lage ist, für ein adäquates Sicherheitsniveau selbst zu sorgen, vorausgesetzt, dass dieses samt der zu implementierenden Maßnahmen definiert ist. Entsprechend ergibt sich die in Abb. 38 schematisch dargestellte Arbeitsteilung zwischen IT-Organisation einerseits und der IT-Sicherheitsorganisation andererseits. Zweitens ist es oft gar nicht möglich, Sicherheit und IT zu trennen. Man denke an Härtung und andere Konfigurationsaktivitäten, an Vorfälle einschließlich Systemausfällen oder an das Patchen. Die Berücksichtigung von Sicherheit in allen Prozessschritten entlang der (internen) Lieferkette hilft, nachträgliche Korrekturen sowie Doppelarbeit und

---

[115] Eberhard von Faber and Wolfgang Behnsen: A Systematic Approach for Providers to Deliver Secure ICT Services; in: ISSE 2012 Securing Electronic Business Processes, Highlights of the Information Security Solutions Europe, ISSE 2012, Springer Vieweg, Wiesbaden, 2012, ISBN 978-3-658-00332-6, https://doi.org/10.1007/978-3-658-00333-3_9; p. 80-88

[116] Eberhard von Faber and Wolfgang Behnsen: Secure ICT Service Provisioning for Cloud, Mobile and Beyond (ESARIS: The Answer to the Demands of Industrialized IT Production Balancing Between Buyers and Providers); Springer Vieweg, Wiesbaden 2017, 383 pages, 159 figures, ISBN 978-3-658-16481-2, 2nd updated and extended Edition, https://doi.org/10.1007/978-3-658-16482-9

Widersprüche zu vermeiden. Das senkt die Kosten und erhöht Geschwindigkeit und Qualität.[117]

Abb. 38: Arbeitsteilung zwischen IT-Organisation und IT-Sicherheitsorganisation bzgl. der IT-Sicherheit[118]

Aber es gibt noch einen dritten Grund.[119] Eine der wichtigen Einsichten von William Edwards Deming (1900-1993) und auch des „Total Quality Managements" (1951) besteht in Folgendem: Qualität muss erzeugt und nicht nur kontrolliert werden. Sie ist das Ergebnis aktiven Handelns eines jeden Mitarbeiters. Was bedeutet dies übertragen auf die IT-Sicherheit? Die IT-Sicherheit muss sich auf die Prozesse zur Erzeugung von Produkten und IT-Services konzentrieren – also auf das IT-Service-Management. Die Leitung (Unternehmensführung, Management) muss einen Rahmen definieren, der Qualität ermöglicht – also Regeln definieren, damit jeder Mitarbeiter an jeder Stelle der Wertschöpfungskette das für die IT-Sicherheit Notwendige tun kann. „Business Process Reengineering" (1993) war in den 1990er Jahren eine viel genutzte Methode. Sie fordert, parallele Aktivitäten zu verbinden, statt nur ihre Ergebnisse zu integrieren: Entsprechend sollten Aktivitäten zur IT-Sicherheit Teil des IT-Service-Managements werden.

---

[117] Eberhard von Faber und Wolfgang Behnsen: Joint Security Management: organisationsübergreifend handeln (Mehr Sicherheit im Zeitalter von Cloud-Computing, IT-Dienstleistungen und industrialisierter IT-Produktion); Springer Vieweg, Wiesbaden 2018, 244 Seiten, 60 farbige Abbildungen, ISBN 978-3-658-20833-2, https://doi.org/10.1007/978-3-658-20834-9, Kapitel 2.5

[118] Eberhard von Faber: Methoden: „Secured by definition" und die Umsetzung von Prinzipien aus dem Qualitätsmanagement, Durchgängige IT-Sicherheit durch Integration in die IT-Produktionsprozesse; in: Datenschutz und Datensicherheit - DuD, 43(7), Juli 2019, Springer Fachmedien, Wiesbaden 2019, ISSN 1614-0702, pp 410-417; https://doi.org/10.1007/s11623-019-1136-0

[119] ebenda.

5.3.2 Erweiterungen des IT-Service-Managements

Um IT-Sicherheit im Sinne von *Secured by Definition* aktiv als Qualität zu erzeugen oder zu erreichen, müssen die Prozesse des IT-Service-Managements erweitert werden. Damit schafft die Unternehmensführung den Rahmen, den Mitarbeiter brauchen, um Qualität erzeugen zu können.

Abb. 39 zeigt das *Vulnerability Management* (Schwachstellenmanagement) als einen neuen Prozess,[120] der eingeführt werden kann, um die allfälligen Maßnahmen zur Reparatur mangelhafter IT-Sicherheit besser koordinieren zu können.

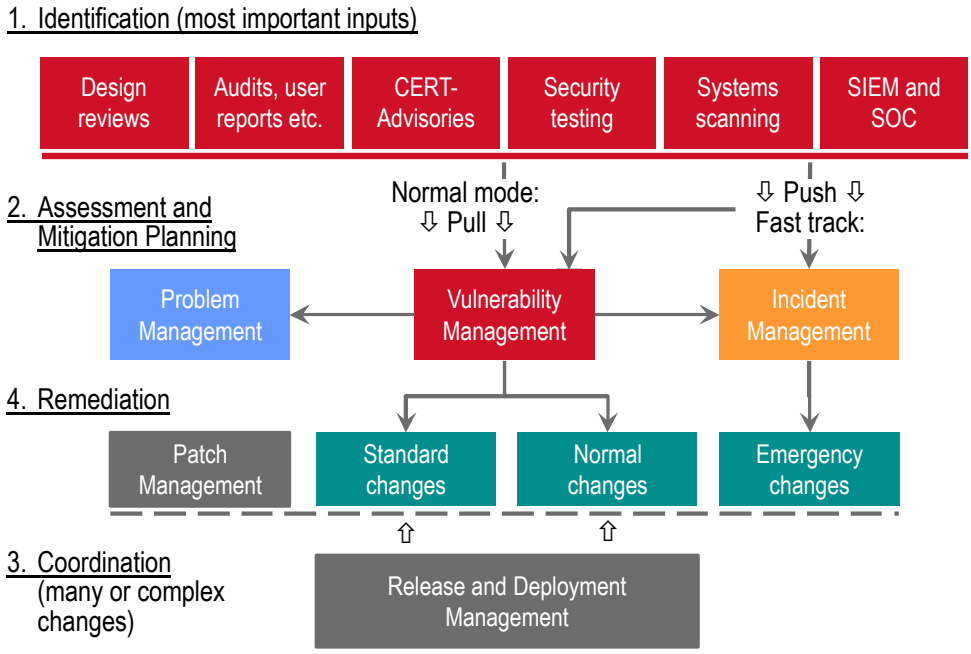


Abb. 39: Das Schwachstellenmanagement und seine Beziehung zu anderen Kernprozessen

Die oberste Zeile zeigt sechs Quellen, die solche →*Schwachstellen* identifizieren und Informationen über die fehlerhafte Komponente (Produkt, Verfahren o.ä.) und mögliche Auswirkungen bereitstellen (siehe auch Kapitel 2.2.1, Schwachstellen auffinden, Vorfälle bearbeiten):

- *Konstruktionsprüfungen* (Design reviews) decken Schwachstellen auf, die auf Fehler im Entwurf und dessen Umsetzung zurückzuführen sind.

---

[120] Eberhard von Faber and Wolfgang Behnsen: Secure ICT Service Provisioning for Cloud, Mobile and Beyond (ESARIS: The Answer to the Demands of Industrialized IT Production Balancing Between Buyers and Providers); Springer Vieweg, Wiesbaden 2017, 383 pages, 159 figures, ISBN 978-3-658-16481-2, 2nd updated and extended Edition, https://doi.org/10.1007/978-3-658-16482-9; Kap. 5.3 (Seite 91ff.) und Kap. 12.1.2 (Seite 216f.)

- *Sicherheitsaudits* (Security audits) prüfen, ob Verfahren eingehalten und Maßnahmen implementiert wurden und wirksam sind.
- *CERT-Informationsdienste* (CERT advisory services) liefern Informationen (CERT Advisories) über Bugs in Software- und Hardware-Produkten und deren Behebung.
- Bei *Sicherheitsprüfungen* (Security testing) bzw. *Penetrationstests* (penetration testing) suchen Experten werkzeuggestützt und teilautomatisiert gezielt nach Schwachstellen in IT-Komponenten und IT-Systemen.
- *Systems scanner* sind Softwareagenten, die auf IT-Komponenten und IT-Systemen Soll-Ist-Vergleiche durchführen bzw. Daten für solche Vergleiche beschaffen. Dadurch können Konfigurationsfehler und auch Rückstände bei Softwareaktualisierungen festgestellt werden.
- *Security Operations Center (SOC)* entdecken mit Hilfe einer SIEM-Infrastruktur wirkliche Angriffe, deren Analyse Hinweise auf Schwachstellen liefert, die der Angreifer im konkreten Fall auszunutzen versucht hat.

Diese Quellen liefern alle Informationen zu Schwachstellen. Allerdings sind der Informationsgehalt, die Qualität, der Kontext, die Art des betroffenen Objekts sowie die Zeit und Frequenz der Meldungen sehr unterschiedlich. Alle Meldungen sollen aber zu Änderungen in den Systemen führen, die in koordinierter Art und Weise, nach Priorität geordnet und nach einheitlichen Verfahren durchgeführt werden sollen. Dies vorzubereiten, ist die Aufgabe des Vulnerability Managements (Schwachstellenmanagements). Siehe Abb. 39.

Vulnerability Management (Schwachstellenmanagement)

Dieser Prozess hat die Aufgabe, den IT-Betrieb mit ausführbaren Anweisungen (Qualified instructions) bezüglich der Behandlung von *Schwachstellen* (Vulnerabilities) zu versorgen, die auf die Belange des IT-Betriebes zugeschnitten sind, also relevant sind und konkretisiert wurden.

Der Prozess sammelt Meldungen über Schwachstellen aus verlässlichen, relevanten Quellen und überprüft die zur Verfügung gestellten Informationen auf Relevanz für den eigenen IT-Betrieb und gegebenenfalls erneut auf Validität (bei Quellen, die außerhalb des IT-Betriebs liegen, zu dem der Prozess gehört). Die Meldungen werden konsolidiert (Doppel werden entfernt bzw. zusammengeführt), und es werden fehlende Informationen ergänzt. Dazu gehören, sofern verfügbar, umsetzbare Anweisungen, wie die Schwachstelle beseitigt werden kann.

Dann erfolgt die Bewertung hinsichtlich der Schwere (Degree of vulnerability) im Zusammenhang mit bzw. für den eigenen IT-Betrieb. Daraus wird nach einer einheitlichen Metrik (Messverfahren) eine Empfehlung oder Anweisung zur Behandlung der Schwachstelle ermittelt, die Informationen über die Dringlichkeit enthält.

Optionen: Der Prozess sollte bei dieser Bewertung auch Informationen über die Verbreitung der betroffenen Produkte im eigenen IT-Betrieb heranziehen (Implementation gap). Außerdem sollte der Prozess gegebenenfalls Informationen über bestimmte, besonders kritische Schwachstellen zusätzlich in einer Form zur Verfügung stellen, die von Entscheidungsträgern beim IT-Dienstleister und beim Anwender verstanden werden kann und sich als Grundlage für Entscheidungen eignet.

Wie in Abb. 39 zu sehen ist, führen die ausführbaren Anweisungen (Qualified instructions) bezüglich der Behandlung von Schwachstellen in der Regel zu *Standard Changes* oder *Normal Changes*. Da diese nicht zeitkritisch sind, werden insbesondere die Normal Changes gesammelt und vom *Release and Deployment Management* koordiniert als Paket implementiert. Dringend zu beseitigende Schwachstellen werden als *Sicherheitsvorfall (security incident)* eingestuft und mit einem *Emergency Change* behoben. Grundsätzlich kann es auch Schwachstellen geben, für die noch keine Lösung gefunden wurde. Diese können an das *Problem Management* übergeben werden.

Abb. 39 zeigt auch das *Patch Management* als einen neuen Prozess,[121] der eingeführt werden sollte, damit Softwareaktualisierungen nach einheitlichen Regeln vorbereitet und durchgeführt werden.

Patch Management

Dieser Prozess hat die Aufgabe, die Aktualisierung von Software bzw. einer Softwareinstallation (Instanz), auch *Patching*) genannt, adäquat vorzubereiten und zu begleiten. Die Nutzung einheitlicher Verfahren verfolgt das Ziel, Fehler zu vermeiden, Risiken zu mindern und die Effizienz zu erhöhen. Die Installation eines *Patches* selbst erfolgt mit einem *Change* im Rahmen des *Change Managements*.

Der Prozess umfasst das Einsammeln von Patches (aus validierten Quellen), deren Qualitätsüberprüfung, die Paketierung (Zusammenstellung zu Paketen), die Planung und das Testen und schließt mit der Initiierung von Changes bzw. deren Umsetzung ab. Für die Planung benötigt das Patch Management die Festlegung von Umsetzungsfristen, die je nach „Change Type“ und eventuell auch nach Zielsystemen variieren. Der Prozess kann als Teil vom *Release and Deployment Management* angesehen und implementiert werden, da beide zum Teil ähnliche Abläufe realisieren.

---

[121] Eberhard von Faber and Wolfgang Behnsen: Secure ICT Service Provisioning for Cloud, Mobile and Beyond (ESARIS: The Answer to the Demands of Industrialized IT Production Balancing Between Buyers and Providers); Springer Vieweg, Wiesbaden 2017, 383 pages, 159 figures, ISBN 978-3-658-16481-2, 2nd updated and extended Edition, https://doi.org/10.1007/978-3-658-16482-9; Kap. 5.3 (Seite 91ff.) und Kap. 12.2.4 (Seite 244f.)

Die beiden Prozesse *Vulnerability Management* und *Patch Management* hinzuzufügen reicht aber bei weitem nicht aus, um das benötigte Sicherheitsniveau im Betrieb aufrechtzuerhalten.

Einige Erweiterungen für die IT-Sicherheit wurden oben schon erwähnt; zum Beispiel bei der Priorisierung von Vorfällen (Incidents). Siehe →*Priorität (Incident)*. Hier folgen weitere Beispiele: Eingehende Meldungen eines Vorfalls (Incidents) werden im *Incident Management* zunächst eingeordnet, d.h., kategorisiert. Die zur Auswahl stehenden Kategorien müssen um solche ergänzt werden, die sich auf Sicherheitsvorfälle beziehen und diese zu unterteilen bzw. einzuordnen gestatten. Die Bewertung der Auswirkungen (Impact) sollte aus den Größen *Serviceeinschränkung (service restriction)* und *Kritikalität (criticality)* gebildet werden. Die Serviceeinschränkung muss dann auch den Verlust der Vertraulichkeit und Integrität zu messen gestatten. Für die Kritikalität des IT-Services gilt dies analog, nur dass hier die Wichtigkeit von Vertraulichkeit und Integrität für den Anwender gemessen wird. Das *Problem Management* übernimmt Daten aus dem Incident Management und nimmt ebenfalls eine Priorisierung vor. Daher sind ähnliche Anpassungen auch im Problem Management und dem dort genutzten Ticketing-System nötig. Die Kritikalität muss in der *Configuration Management Database (CMDB)* vorgehalten werden, was Anpassungen im *Configuration Management* nach sich zieht. Doch auch das *Change Management* muss erweitert werden und zum Beispiel nicht nur das Installationsrisiko, sondern auch die Informationssicherheitsrisiken (mögliche Auswirkungen auf die IT-Sicherheit) bewerten.

Die Einführung des *Vulnerability Managements* (Schwachstellenmanagements) hat Auswirkungen auf andere Prozesse. Die benötigten SIEM-Funktionalitäten sind gegebenenfalls Teil des *Event Managements*, so dass dort Anpassungen nötig sind. Auditing-Funktionen mit Scannern usw. sind eventuell mit dem *Configuration Management* verbunden, das sicherstellen muss, dass die Produktionsumgebung korrekt in der CMDB abgebildet ist. Wird bei der Bewertung von Schwachstellen nicht nur die Schwere, sondern auch ihre Verbreitung (Implementation gap) gemessen, so muss das Configuration Management auch eine Statistik darüber liefern können, wie viele Instanzen einer bestimmten Software, eines Produktes usw. im Einsatz sind. Obwohl die Aktualisierung von Software fast tägliche Praxis im IT-Betrieb ist, findet man das Wort „Patch“ sowohl in ISO/IEC 20000 als auch in ITIL kaum. Die notwendige Einführung eines Prozesses oder Verfahrens zum *Patch Management* nimmt durch die Definition von Umsetzungsfristen deutlichen Einfluss auf den IT-Betrieb und die Abläufe im *Release and Deployment Management*, mit dem das Patch Management wechselwirkt oder in das es sogar vollständig integriert wird.

Dies sind nur die augenfälligsten Beispiele für die Umsetzung der IT-Sicherheit durch die IT-Service-Management-Prozesse gemäß *Secured by Definition*!

IT-Dienstleister, die Geschäfts- bzw. Enterprise-Kunden bedienen, müssen die Prozesse *Service Portfolio Management (ITIL)* und *Service Catalogue Management (ITIL)*

entsprechend ausrichten, damit dort die IT-Service-Sicherheit angemessen und kundenorientiert berücksichtig wird. Das hat Einfluss auf die Struktur der gesamten Dokumentation zur IT-Service-Sicherheit.[122] Zudem muss die IT-Service-Sicherheit Teil aller Verträge sein, was die „Relationship"-Prozesse *Supplier Management* und *Business Relationship Management (BRM)* und betrieblich auch das *Service Level Management (SLM)* betrifft.

Die „Berücksichtigung der IT-Sicherheit" passiert aber nicht von allein. Das Vorgehen muss in Standards bzw. Arbeitsanleitungen festgehalten werden. Es sind Schulungen nötig, sodass die Mitarbeiter wissen, was von ihnen erwartet wird. Blaupausen (Vorlagen) müssen erstellt und verbreitet, und Software muss angepasst werden. An vielen Stellen werden Sicherheitsexperten benötigt, die als Multiplikatoren wirken, Hilfe anbieten und korrigierend eingreifen können. Schließlich müssen die Security-Management-Organisation und die Führungsebene im IT-Betrieb alle Beteiligten regelmäßig ermutigen, das Notwendige umzusetzen. – Die Liste der betroffenen Prozesse ließe sich erweitern. Doch von den IT-Service-Management-Prozessen alleine wird nicht einmal alles erfasst. Als Beispiel sei nur an die Gestaltung von Vertrieb und Marketing erinnert.

Die Nutzung bewährter Praktiken (best practices) hat aber gegenüber der eigenen Entwicklung nicht nur den Vorteil der höheren Geschwindigkeit und der geringeren Kosten. Vielmehr bauen die bewährten Praktiken auf vielen Erfahrungen aus Irrtümern und Fehlversuchen auf. Sie sind häufig evolutionär über lange Jahre gewachsen. Insbesondere größere Organisationen müssen solche bewährten Praktiken trotzdem an die eigenen Gegebenheiten anpassen und weiterentwickeln.

Literatur und Bildnachweise

Besonders ein solches Buch, das sich zur Aufgabe macht, Definitionen von Fachbegriffen zu geben, kann nicht geschrieben werden, ohne dass der Autor vielfältige Literatur gelesen hätte – in der langen Zeit der Tätigkeit auf diesem Gebiet, bei der Erstellung von Lehrunterlagen für Studierende und beim Schreiben dieses Buches. Die Definitionen sollen ja den Stand der Technik korrekt wiedergeben und konsensfähig sein. Das bedeutet auch, dass Begriffe und Zusammenhänge auch in anderen Veröffentlichungen so oder ähnlich vorkommen können – ja müssen.

In Kapitel 5.2 (bei der Beschreibung der ITSM-Prozesse) wurde von der unten aufgeführten Literatur ausführlich Gebrauch gemacht.

---

[122] Eberhard von Faber: Methoden: „Secured by definition" und die Umsetzung von Prinzipien aus dem Qualitätsmanagement, Durchgängige IT-Sicherheit durch Integration in die IT-Produktionsprozesse; in: Datenschutz und Datensicherheit - DuD, 43(7), Juli 2019, Springer Fachmedien, Wiesbaden 2019, ISSN 1614-0702, pp 410-417; https://doi.org/10.1007/s11623-019-1136-0

Für das gesamte Kapitel 5 gilt, dass Literatur an den Stellen als Fußnote angegeben ist, wo ich sie direkt verwendet habe bzw. mir bewusst ist, dass Begriff, Definition oder sonstige Beschreibungen primär auf diese Quelle zurückgeht. Falls nicht anders angegeben, wurden Abbildungen extra für dieses Buch erstellt.

Die folgende Liste wiederholt nicht alle bereits angegebenen Quellen.

[1] ISO/IEC 20000-1 Information technology — Service management — Part 1: Service management system requirements

[2] ISO/IEC 20000-2 - Information technology — Service management — Part 2: Guidance on the application of service management systems

[3] Stephan Kasulke und Jasmin Bensch: Zero Outage, Kompromisslose Qualität in der IT im Zeitalter der Digitalisierung; Springer Gabler, Wiesbaden, 2016, 205 Seiten, ISBN 978-3-658-14221-6

[4] IT Process Wiki - das ITIL®-Wiki: Das Wiki zur IT Infrastructure Library ITIL® (ITIL 4, V3 und V2) und zu IT-Service-Management (ITSM): https://wiki.de.it-processmaps.com/ (Deutsch) und https://wiki.en.it-processmaps.com/ (Englisch)

[5] itsmprocesses.com, ...Ihr Portal für ITSM Prozesse und Tools...: https://www.itsmprocesses.com/

[6] 20000Academy, ITIL® and ISO 20000 Online Consultation Center: https://advisera.com/20000academy/knowledgebase/incident-classification/

[7] ISO Online browsing platform: http://www.iso.org/obp

Elektronisches Zusatzmaterial
Die Abbildungen sind als PowerPoint-Datei kapitelweise über https://link.springer.com/ auf der Seite des eBooks abrufbar.

6 Produktgruppen der IT-Sicherheit

Die Vielzahl der IT-Sicherheitsprodukte erscheint schwer überschaubar. Das gilt noch viel mehr für die ihnen zugrunde liegenden Funktionen. Es gibt diverse Bemühungen, Ordnungsschemata zu schaffen. Vor allem Marktforschungsinstitute bzw. Analysten wie Forrester Research, Gartner, IDC, Frost & Sullivan, ISG und früher Datamonitor untersuchen den Markt für Sicherheitsprodukte und -lösungen. Um zu Trendaussagen kommen zu können, werden Kategorien und Produktgruppen geschaffen und Entwicklungen bei Herstellern und Anwendern aggregiert. Besonders in neu entstehenden oder sich wandelnden Marktsegmenten werden dagegen eher Technologien oder Funktionen untersucht, da noch nicht viele Produkte verfügbar sind bzw. noch nicht erkennbar ist, wie sich der Markt für diese konsolidieren wird.

In Bereichen, wo der Markt besonders entwickelt ist, gibt es eine Reihe von Produkten, die unabhängig vom Hersteller ähnliche Funktionalitäten haben und ähnlich bezeichnet werden. Sie lösen allgegenwärtige und häufig wiederkehrende Sicherheitsprobleme und werden standardmäßig eingesetzt. Solche Produkte bzw. Produktgruppen werden im vorliegenden Kapitel behandelt.

Die Klassifikation und Gruppierung von Produkten ist ein wichtiges Element, um eine gemeinsame Sprache zu finden, die die Angebots- und Nachfrageseite zusammenbringt. D.h., Hersteller und Anwender können sich verständigen und sich über Probleme, Bedarfe und Lösungen austauschen. Klassifikationsschemata und Übersichten helfen den Anwendern, die Vielfalt der potentiell verfügbaren Lösungen kennenzulernen und Produkte entsprechend ihren Anforderungen auszuwählen.

6.1 Abgrenzung, Charakterisierung und Taxonomie

Die Komplexität von IT-Sicherheit und Informationstechnologie bietet vielerlei Ansätze für eine Systematisierung. Hinsichtlich Wirkung und Effekt im allgemeinen Sinne können Sicherheitsprodukte Folgendem dienen:

- Abwehr bzw. Verhinderung (prevention),
- Eindämmung (containment),
- Überprüfung (auditing, compliance scanning etc.),
- Erkennung (detection of attacks, monitoring, event collection and analysis),
- Alarmierung (notification, alerting),
- Reaktion und Wiederherstellung (reaction and recovery/restoration).

Zusatzmaterial online
Zusätzliche Informationen sind in der Online-Version dieses Kapitel (https://doi.org/10.1007/978-3-658-33431-4_6) enthalten.

E. von Faber, *IT und IT-Sicherheit in Begriffen und Zusammenhängen*,
Edition <kes>, https://doi.org/10.1007/978-3-658-33431-4_6

Abgrenzung

In diesem Kapitel werden Produkte bzw. Produktgruppen betrachtet, die vorrangig in IT-Systeme und IT-Infrastrukturen integriert werden bzw. eng mit diesen zusammenspielen. Nicht betrachtet werden im Folgenden Produkte, die das Sicherheitsmanagement im Allgemeinen unterstützen, also die Organisation und die Prozesse, das Risikomanagement, das Verwalten von Informationen über Bedrohungen, Sicherheitsvorfälle und bekannte Fehler und dergleichen. Nicht betrachtet werden auch Produkte bzw. Lösungen, die in der IT-Produktion zusätzlich benötigt werden wie zum Beispiel Werkzeuge zur Analyse von Logdaten, von Ports und zur sonstigen Gewinnung von Informationen über Konfigurationen und Ereignisse sowie Werkzeuge zur Unterstützung von Prozessen und Arbeitsabläufen wie der sicheren Entwicklung zum Beispiel von Software oder deren Aktualisierung im Wirkbetrieb. Ebenfalls nicht berücksichtigt werden Werkzeuge zur Verfügbarkeitsüberwachung (wie Heartbeat-Monitoring), zur Lastkontrolle oder die Steuerung und Verbesserung der Performance.

Im Allgemeinen werden *Dienstleistungen* in diesem Kapitel nicht behandelt, sondern primär *Produkte* im allgemeinen Sinne.

Charakterisierung

Über ein Sicherheitsprodukt bzw. eine Gruppe von Sicherheitsprodukten sollte man Folgendes wissen:

- das Sicherheitsproblem, das es zu lösen verspricht,
- Grundlegendes über die Sicherheitsfunktion, mit der das Produkt das Sicherheitsproblem adressiert und beseitigt oder löst,
- den Anwendungsbereich und die wichtigsten Anwendungsbedingungen.

Sicherheitsprodukte lösen Sicherheitsprobleme immer nur in einem spezifischen Kontext unter bestimmten Bedingungen. Dies sind Informationen, die zum Anwendungsbereich gehören. Siehe Abb. 40.

Sicherheitsprodukte sorgen dafür, dass bestimmte Entitäten bestimmte Sicherheitseigenschaften erhalten. Es gibt viele verschiedene zu schützende Entitäten (Objekte, Zusammenhänge, Vorgänge) und noch mehr unterschiedliche Situationen, in denen sie eine Rolle spielen. Daher werden sehr viele Sicherheitsprodukte benötigt, obwohl es vergleichsweise wenig unterschiedliche Sicherheitseigenschaften gibt.

Um ein Sicherheitsprodukt zu verstehen, ist es unerlässlich, das Sicherheitsproblem und den Kontext zu verstehen, in dem es gelöst werden soll.

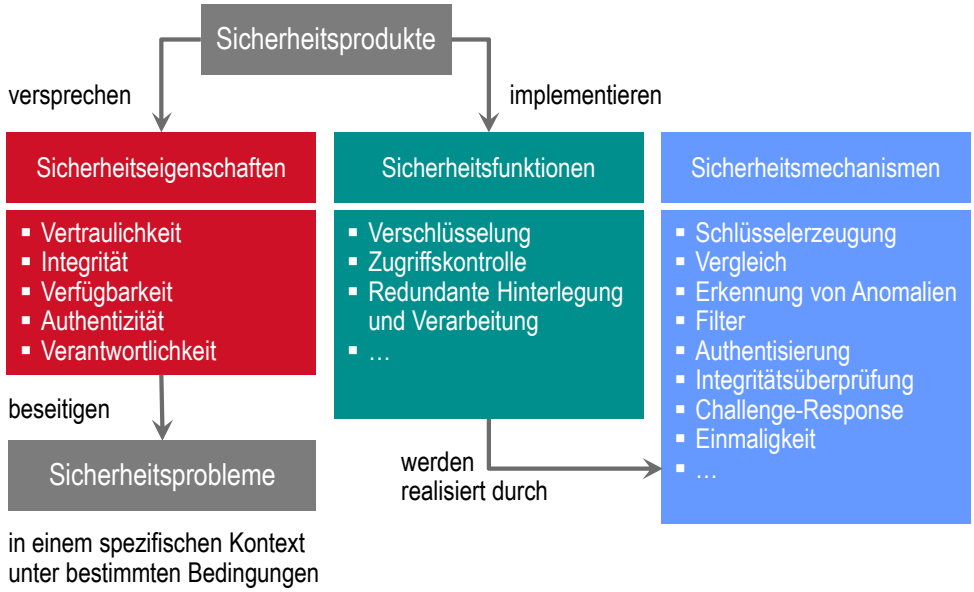


Abb. 40: Wie Sicherheitsprodukte Sicherheitsprobleme lösen (Schema)

Sicherheitsprodukte implementieren Sicherheitsfunktionen, die wiederum durch eine Reihe von Sicherheitsmechanismen realisiert werden (siehe Abb. 40). Die Zahl der Sicherheitsfunktionen und mehr noch die der Sicherheitsmechanismen ist schwer zu überschauen. Die Common Criteria[123] bieten im Teil 2 einen Katalog von Sicherheitsfunktionen. Das NIST hat mit der Special Publication 800-53[124] ebenfalls einen solchen Katalog vorgestellt, der auch das Security-Management umfasst. Die „Taxonomy of ICT Security Solutions“[125] wählt eine Reihe von Kategorien (Funktionsweisen von Produkten und Services) sowie Unterkategorien (Details zur Funktionsweise), die, mit einem Einsatzgebiet kombiniert, dann Klassen oder Gruppen von Produkten und Services ergeben.

Abb. 41 zeigt eine vereinfachte Darstellung mit nur sieben generischen Sicherheitsfunktionen bzw. Funktionsweisen und einigen Hilfsfunktionen, die nur indirekt zur Sicherheit beitragen. Die Sicherheitsfunktionen sind unabhängig von einem Anwendungskontext definiert und eignen sich dafür, das Verständnis eines Sicherheitsproduktes zu vertiefen.

---

123 ISO/IEC 15408 – Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components; July 2008; and: Common Criteria for Information Technology, Security Evaluation, Part 2: Security functional components; April 2017, Version 3.1, Revision 5, https://commoncriteriaportal.org

124 NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations; April 2013 (updated 2015), Rev. 4

125 Inteco: Information Security Taxonomy Handbook; National Institute for Communications Technologies (INTECO), León (Spain), 2010

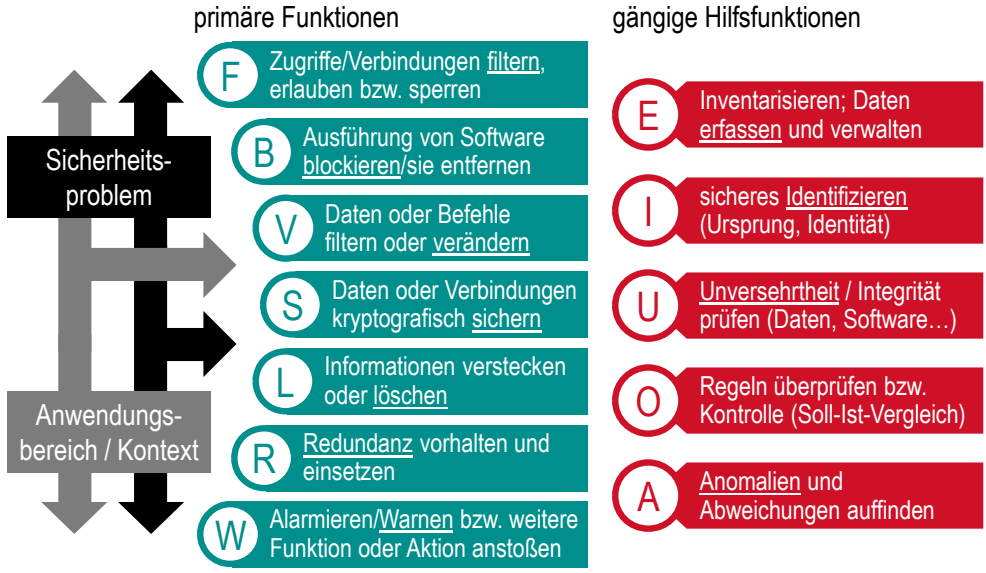


Abb. 41: Was man über die hier betrachteten Produkte wissen sollte (Schema)[126]
(Die Schildchen mit den Buchstaben dienten zur Kommunikation in der Lehre.)

Die Abbildung zeigt die drei Begrifflichkeiten Sicherheitsproblem, Sicherheitsfunktion und Anwendungsbereich, die bei der Betrachtung von Sicherheitsprodukten eine wichtige Rolle spielen.

Ordnungsschema (Taxonomie)

Es gibt verschiedene Ansätze, um ein Ordnungsschema (Taxonomie) für Sicherheitsprodukte zu entwickeln. Da die Produkte an einer bestimmten Stelle in der IT-Infrastruktur (etwa auf Arbeitsplatzrechnern, im Netz oder auf Servern) installiert werden, liegt es nahe, den Anwendungsbereich als hauptsächliches Ordnungskriterium zu verwenden. Dabei zeigt sich jedoch, dass bestimmte Produktarten mehrfach auftauchen würden, da sie in ähnlicher Form an verschiedenen Stellen installiert werden. Rückt man dagegen die Sicherheitsfunktionalität in den Vordergrund, zerfallen die Produkte zu Bausteinen, da die Produkte meist mehrere Funktionen in unterschiedlicher Weise kombinieren.

Das im Folgenden verwendete Ordnungsschema ist ein Kompromiss (siehe Abb. 42). Es verwendet sieben Bereiche, die Zweck und Anwendungsbereich kombinieren.

[126] Eberhard von Faber: Vorlesungsskript; Technische Hochschule Brandenburg; modifiziert

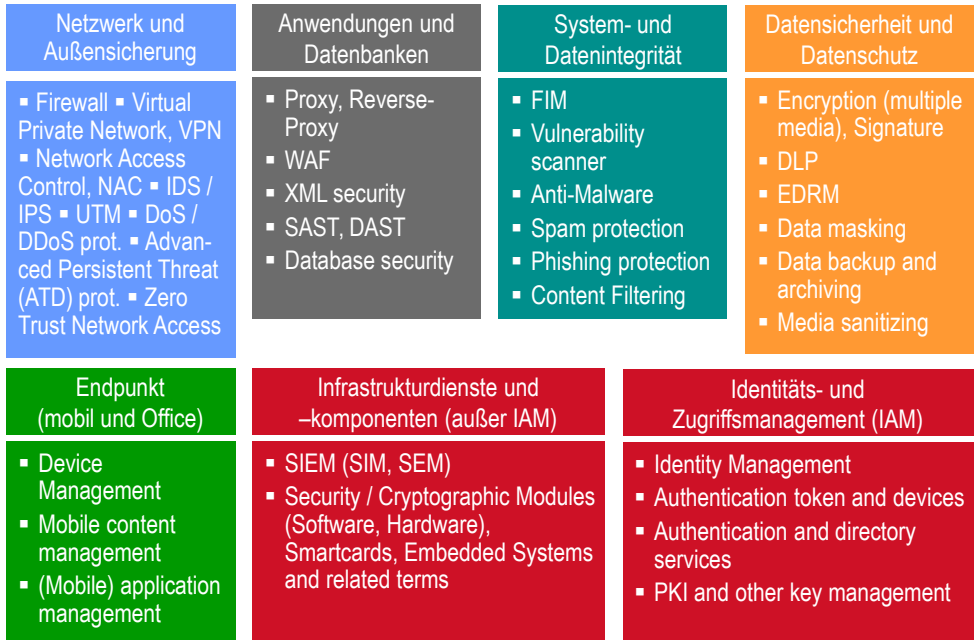


Abb. 42: Taxonomie für IT-Sicherheitsprodukte und -lösungen[127]

Hinweis: Die im Folgenden verwendete Kapitelstruktur (6.2 - 6.7) entspricht der Einteilung in Abb. 42.

Bezüglich Identitäts- und Zugriffsmanagement (IAM) siehe Kapitel 3.

Die Abbildung zeigt Beispiele für Produkte und Lösungen, die im Folgenden beschrieben werden.

Hinweis: In Kapitel 2.1.2 und 2.1.3 wurden Begriffe, wie *Bedrohung* (threat), *Schwachstelle* (vulnerability), Angriff (intrusion, attack), *Schaden* (impact) und *Risiko* (risk) eingeführt und definiert. Siehe auch Abb. 2 auf Seite 13. Bei der Bezeichnung von Produkten und deren Beschreibung werden Begrifflichkeiten verwendet, die zu Missverständnissen führen können. Der Begriff „threat detection/protection" bezieht sich zum Beispiel nicht unbedingt auf die Erkennung einer Bedrohung („threat intelligence") bzw. die Erkennung oder Verhinderung des Eindringens („intrusion") eines „threat agents", sondern oft auf die Erkennung von Schwachstellen („vulnerabilities"), die zu einer Gefahr werden können und deren Beseitigung („remediation") zu einem besseren Schutz („protection") führt.

6.2 Netzwerk und Außensicherung

Wie Abb. 43 erwarten lässt, werden in diesem Kapitel zunächst verschiedene Typen von Firewalls behandelt. Danach geht es um sichere Netzverbindungen, sicheren

[127] Eberhard von Faber: Vorlesungsskript; Technische Hochschule Brandenburg; modifiziert

Netzwerkzugang, Einbruchserkennung sowie verschiedene Arten, Einbrüche abzuwehren. Abschließend wird eine Umsetzung von *Zero Trust* vorgestellt, die nicht die in Abb. 43 dargestellte Architektur zur Grundlage hat.

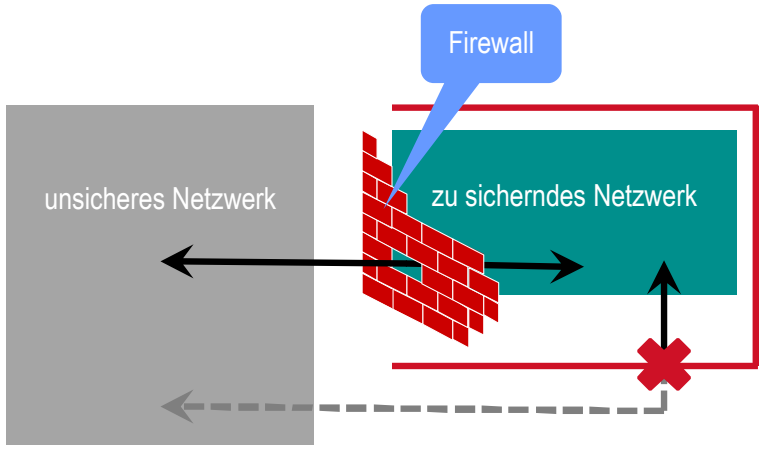


Abb. 43: Firewalls sind nur dann wirksam, wenn sie nicht umgangen werden können

Firewall

Eine Firewall verbindet zwei Netzwerke mit unterschiedlichem Sicherheitsniveau und ermöglicht die Kommunikation zwischen ihnen, indem der Netzwerkverkehr nach vordefinierten Regeln gefiltert wird.

Um von einem Netzwerk A aus mit Teilnehmern oder IT-Services in einem Netzwerk B kommunizieren zu können, müssen beide Netzwerke verbunden werden. Hat Netzwerk A höhere Sicherheitsanforderungen bzw. ein höheres Sicherheitsniveau als Netzwerk B, so werden Bedrohungen aus dem Netzwerk B (meist als äußeres bezeichnet) die Sicherheit des Netzwerks A gefährden (das dann als inneres Netzwerk bezeichnet wird). Dieses Problem wird durch eine Firewall, genauer eine Netzwerk-Firewall (**Network Firewall**) gelöst, die als *Gateway* (Tor bzw. Verbindung) zwischen beiden Netzwerken wirkt und dort den Netzwerkverkehr filtert.

In ähnlicher Weise kann ein Computersystem (*Host*) gefährdet werden, wenn es mit einem Netzwerk verbunden wird. Dies zu verhindern, ist Aufgabe einer auf dem Computersystem installierten Firewall, die **Personal Firewall** genannt wird.

Eine weitere Form stellt **Firewall-as-a-Service (FWaaS)** dar, auch **Cloud Firewall** genannt. Hier wird der gesamte Datenverkehr auf einen Cloud-Service des Anbieters umgeleitet und dort geprüft und gesteuert.

Eine Firewall untersucht die IP-Adresse der Quelle und die des Empfängers sowie den genutzten Netzwerkdienst (Protokoll, Port) und prüft, ob diese Angaben den in der Firewall eingestellten Regeln entsprechen. Entsprechend wird die Kommunikation (Austausch der IP-Pakete) erlaubt oder unterbunden. Man

spricht daher auch von **packet filter (firewalls)**. Eine höhere Sicherheit bieten **stateful inspection firewalls**. Sie merken sich den Zustand (state) der Kommunikation und können daher zum Beispiel feststellen, ob eine Antwort auf eine Anfrage folgt oder ob eine Nachricht ohne Anlass und damit möglicherweise in böser Absicht gesendet wird.

Zusätzliche Funktionalitäten bieten →*Application-level Firewalls*.

Next-Generation Firewall (NGFW)

Next-Generation Firewalls bieten im Vergleich zu Paketfilter-Firewalls zusätzliche Funktionen. Sie untersuchen die übertragenen Daten auf dem Anwendungslevel (im Sinne des *OSI-Modells*/OSI-Referenzmodells) und können dadurch Angriffsmuster erkennen und Angriffe abwehren (intrusion prevention) sowie Schadsoftware erkennen und differenzierte Entscheidungen über auszuschließende Formen der Kommunikation treffen (wie der Nutzung bestimmter Anwendungen).

Während *Packet filter (firewalls)* (einschließlich *Stateful inspection firewalls*) nur die Steuerungsinformationen (Header) der zwischen zwei Netzen ausgetauschten IP-Pakete untersuchen, inspizieren sogenannte **Deep-inspection firewalls** auch die übertragenen (Nutz-)Daten im Datenteil der IP-Pakete, um unerwünschte oder falsche Protokolle und Schadsoftware aufspüren sowie Angriffe erkennen zu können. Diese **Deep Packet Inspection (DPI)** erfolgt auf dem Anwendungslevel (im Sinne des OSI-Referenzmodells).

Ports können für mehrere verschiedene Zwecke bzw. Dienste (Protokolle) genutzt werden, was durch einfachere Paketfilter nicht erkannt bzw. unterschieden werden kann. Diese können auch nicht feststellen, von welchem Service bzw. welcher (Internet-)Anwendung ein Paket stammt, und sie können daher entsprechende Regeln nicht umsetzen. Angriffsmuster können ebenfalls nur erkannt werden, wenn die verschiedenen IP-Pakete inspiziert und im Zusammenhang miteinander untersucht werden.

Um die genannten Vorteile gegenüber herkömmlichen Firewalls wirklich realisieren zu können, werden Next-Generation Firewalls (NGFW) von externen Quellen mit Informationen über neue Bedrohungen versorgt.

Application-level Firewall

Eine Application-level Firewall hat große Ähnlichkeiten mit einer →*Deep-inspection firewall*. Meist wird unter einer Application-level Firewall jedoch eine Lösung verstanden, die auch aktiv als *Proxy* arbeitet, also die anfragende Verbindung unterbricht, selbst eine Verbindung zum Zielsystem aufbaut und den Datenverkehr als Stellvertreter modifiziert, filtert und dergleichen. Siehe auch →*Web Application Firewall*.

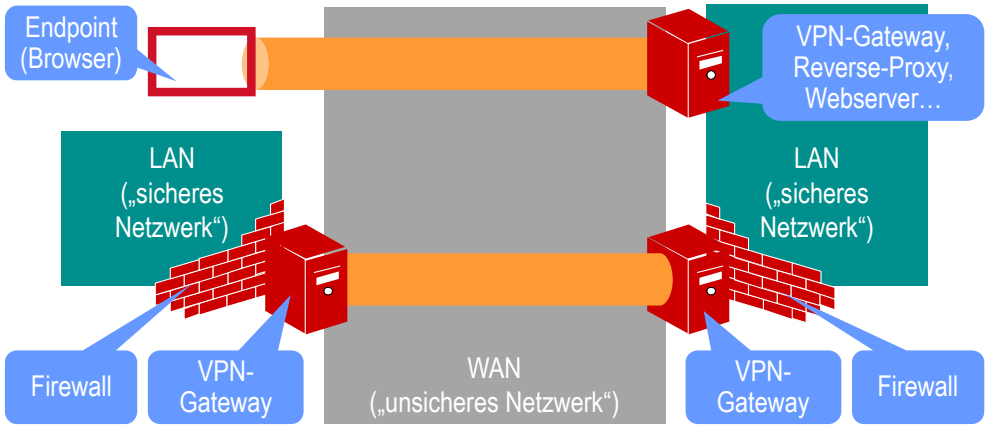


Abb. 44: VPN-Installationen (schematisch, vereinfacht ohne DMZ)

Virtual Private Network (VPN)

Ein Virtual Private Network (VPN) schafft eine gesicherte Verbindung zwischen zwei IT-Komponenten in einem unsicheren Netz. Bei einem VPN im engeren Sinne entsteht der sichere „Tunnel“ („Netz im Netz“) durch Verschlüsselung des gesamten, zwischen den beiden IT-Komponenten ausgetauschten Datenverkehrs.

Wird der sichere Kanal in einem unsicheren Netz dynamisch aufgebaut (und abgebaut), so ist ergänzend zwingend die *Authentisierung* (sichere Identifikation) mindestens einer der IT-Komponenten nötig. Andernfalls könnte ein Angreifer die Rolle dieser Komponente übernehmen und eine verschlüsselte Verbindung zur anderen IT-Komponente aufbauen, die ihre Daten dann dem Angreifer preisgibt.

Ein VPN im weiteren Sinne kommt ohne Verschlüsselung aus. Auch bei einem VPN mit Verschlüsselung muss die Netzwerktechnik dafür sorgen, dass Daten gemeinsam durch das Netz bewegt werden, am Ende jedoch nur dem Adressaten zugestellt werden. Den „Tunnel“ (das „Netz im Netz“) erzeugt die Netzwerktechnik. Diese Netzwerklösung (ohne Verschlüsselung) schützt nicht gegen Abhören oder Manipulation der Datenverbindung. Dieses Szenario spielt jedoch bei physisch gesicherten Netzen (wie zum Beispiel jenen innerhalb eines Rechenzentrums) keine Rolle.

Für ein VPN werden immer zwei Komponenten benötigt: eine für das Senden (und Verschlüsseln) von Daten und eine fürs Empfangen (und Entschlüsseln) der Daten. Werden zwei Netze über ein drittes miteinander verbunden, so spricht man von einem **Site-to-Site-VPN**. Da meist zwei lokale Netzwerke (LANs) über ein Weitverkehrsnetz (WAN) verbunden werden, wird auch der Begriff **LAN-to-LAN-VPN** verwendet. Von einem **End-to-Site-VPN** spricht man, wenn ein Endgerät (Arbeitsplatzcomputer, Smartphone oder dergleichen)

über ein WAN mit einem LAN verbunden wird. Bei diesen Lösungen (**IPSEC VPN**) wird das gesamte Netzwerk im anderen LAN bzw. im Endgerät sichtbar. Die IT-Komponente des VPNs am Übergang zwischen WAN und LAN heißt **VPN-Gateway**. Die IT-Komponente des VPNs auf einem Endgerät wird **VPN-Client** genannt.

Geht es nur darum, eine Verbindung zu einem Server oder einem speziellen IT-Service herzustellen, so kommt meist ein **TLS VPN** bzw. **SSL VPN** zum Einsatz, das TLS (Transport Layer Security) bzw. früher SSL (Secure Sockets Layer) für die Herstellung des verschlüsselten VPNs verwendet. Die IT-Komponente des VPN auf einem Endgerät ist dann oft ein Browser.

Die VPN-Gateways befinden sich genauso wie die *Firewalls* am Übergang zwischen (sicherem) LAN und (unsicherem) WAN. Siehe Abb. 44. Die Firewall soll den gesamten Netzwerkverkehr prüfen, kann dies aber nur dann, wenn der VPN-Tunnel (vom WAN aus gesehen) vor der Firewall terminiert wird. Firewall und VPN-Gateway werden daher oft derart kombiniert, dass der VPN-Tunnel „in" der Firewall terminiert wird. Auch im Falle einer TLS/SSL-Verbindung mit einer Web-Anwendung endet der VPN-Tunnel meist nicht erst im sicheren LAN, sondern davor.

Demilitarisierte Zone (DMZ)

Eine DMZ ist kein Produkt, sondern ein architektonisches Konzept. Der Übergang zwischen dem sicheren bzw. vertrauenswürdigen lokalen Netzwerk (LAN) und dem unsicheren Weitverkehrsnetz (WAN) wird durch (mindestens) zwei, hintereinander geschaltete *Firewalls* gesichert. Der Bereich zwischen den beiden Firewalls bzw. wird Demilitarisierte Zone (DMZ) genannt. IT-Komponenten in diesem Bereich sind aus dem WAN leicht erreichbar, ohne dass dies die Sicherheit des inneren LANs gefährdet, das hinter einer weiteren Firewall liegt und von ihr geschützt wird.

In einer vereinfachten Variante wird der Netzübergang zwischen sicheren bzw. vertrauenswürdigen lokalen Netzwerk (LAN) und dem unsicheren Weitverkehrsnetz (WAN) nur durch eine Firewall gesichert, an die ein eigenes Netzsegment angeschlossen ist, das man ebenfalls als Demilitarisierte Zone (DMZ) bezeichnet.

Network Access Control (NAC)

Network Access Control (NAC), auch als **Network Admission Control (NAC)** bezeichnet, prüft Bedingungen für den Zugang zu einem Netzwerk und setzt sie durch. In der Regel gehen diese über die *Authentisierung* von Geräten und Nutzern hinaus und betreffen den Sicherheitsstatus eines Endgerätes, das sich dynamisch mit einem Netzwerk verbinden möchte (Remote Access).

Sind Endgeräte nicht dauerhaft mit dem als sicher geltenden Netzwerk verbunden, kann deren Konfiguration eventuell nicht ständig den aktuellen

Anforderungen angepasst und aktualisiert werden. Es ist auch möglich, dass die ursprünglich sichere Konfiguration des Gerätes durch Fehler oder feindliche Einwirkung verändert wurde. Wenn ein solches Gerät mit einem als sicher geltenden Netzwerk verbunden wird, könnte die Sicherheit dieses Netzwerks beeinträchtigt oder kompromittiert werden. Network Access Control (NAC) sorgt dafür, dass der erforderliche Sicherheitsstatus des Gerätes geprüft und gegebenenfalls hergestellt wird, bevor die Verbindung zum Netzwerk vollständig hergestellt wird.

NAC besteht aus zwei Komponenten: Der Agent auf dem Gerät überprüft die Konfiguration (scanner) und ist in der Lage, den Sicherheitsstatus herzustellen, also zum Beispiel Einstellungen zu ändern und die Aktualisierung von Software oder der Anti-Malware-Informationen zu veranlassen. Während dieser Zeit besteht für den Nutzer keine vollständige Netzwerkverbindung; das Gerät befindet sich in **Quarantäne**. Die zweite Komponente befindet sich im Netzwerk, zu dem die Verbindung hergestellt werden soll. Sie versorgt den Agenten auf dem Endgerät mit den Bedingungen oder Vorgaben (policies) und erwartet die positive Nachricht des Agenten zur Freischaltung des Netzwerkzugangs.

Intrusion Detection/Prevention System (IDS/IPS)

Ein Intrusion Detection System (IDS) identifiziert Versuche, in ein Netzwerk oder ein Computersystem einzubrechen und generiert in diesem Falle unverzüglich einen Alarm. Ein Intrusion Prevention System (IPS) geht darüber hinaus und greift aktiv ein, um den Einbruch zu verhindern.

Die Einbruchserkennung basiert auf Mustererkennung sowie heuristischen und statistischen Methoden. Mit Hilfe von statistischen Methoden werden Anomalien gefunden, die auf Angriffe hindeuten. IDS und IPS können fehlerhaft anschlagen (false positive) oder Einbruchsversuche übersehen (false negative). Dies kann insbesondere dann auftreten, wenn sich der überwachte Informationsaustausch in Folge geänderter IT (zum Beispiel Neuinstallation einer Anwendung) oder geänderten Nutzerverhaltens stark verändert. Ein IPS besitzt einen Lernmodus, in dem nur die IDS-Funktion freigeschaltet ist.

Sind die Systeme Teil eines Netzwerks, das sie überwachen, so handelt es sich um **Network IDS/IPS**. Systeme, die auf einem Computersystem installiert sind, überwachen den Informationsaustausch zwischen diesem *Host* und den angeschlossenen Netzwerken und werden als **Host IDS/IPS** bezeichnet.

Unified Threat Management (UTM)

Bei *Unified Threat Management (UTM)* handelt es sich um Produkte, die typischerweise Lösungen aus den folgenden drei Bereichen integrieren: Netzwerksicherheit (*Firewall*, *Intrusion Prevention System (IPS)*, *Virtual Private Network (VPN)*), sicherer Internet-Zugang (Internet-Gateway, *URL-Filter*) und Daten-

sicherheit (*Spam-Filter*, *Anti-Malware* für E-Mail). UTM wird häufig als *Appliance* angeboten und von kleinen und mittelgroßen Unternehmen genutzt.

(Distributed)-Denial-of-Service-Protection (DoS/DDoS)

Diese Lösungen bieten Schutz gegen Angriffe auf die Verfügbarkeit, bei denen ein Netzwerk bzw. eine Netzwerkkomponente oder ein Server bzw. eine Anwendung gezielt überlastet wird und schließlich nur eingeschränkt nutzbar ist oder vollständig ausfällt, also „den Dienst verweigert" (**Denial-of-Service, DoS**). Der Angreifer schickt dabei Anfragen mit besonders hoher Frequenz (viele Anfragen innerhalb kurzer Zeit). Werden dabei sehr viele Computer genutzt, um die Frequenz der Anfragen massiv zu erhöhen, spricht man von einem DDoS-Angriff, wobei DDoS für **Distributed-Denial-of-Service** steht.

Intrusion Detection/Prevention Systems (IDS/IPS) bieten bereits einen gewissen Schutz gegen einen DoS-Angriff. Allerdings besitzen derartige Systeme selbst nur eine begrenzte Kapazität und können daher Angriffe mit sehr hoher Frequenz nicht mehr verarbeiten, die in der Regel über das Internet erfolgen. Dies gilt grundsätzlich für alle Systeme am Übergang vom Internet zum eigenen Netz oder im eigenen Netz. Massive DDoS-Angriffe können daher am besten durch Internet- bzw. Netzbetreiber in deren *Backbone*, dem Hochgeschwindigkeits-Kernbereich des Netzes, abgefangen werden.

Advanced Threat Detection (ATD)

Advanced Threat Detection (ATD) sind Lösungen, die ausführbaren Code, allgemein Dateien sowie Netzwerkverkehr besonders gründlich untersuchen, sodass hochentwickelte und vielschichtige Angriffe erkannt werden können. Da verdächtiger Code zum Beispiel in simulierten Laufzeitumgebungen getestet wird (sandboxing), sind die Analysen rechenintensiv, weshalb die Lösungen als *Appliance* angeboten werden. Auch werden mehrere Informationen zum Beispiel über die Quelle, den Code und die Art der Kommunikation miteinander korreliert.

Zero Trust Network Access (ZTNA)

Produkt oder Service, der als alleiniger Vermittler den Zugriff auf bestimmte *Anwendungen* (Applikationen) steuert, indem er die Nutzer und gegebenenfalls auch die von ihnen genutzten Geräte bei jedem Zugriff authentisiert sowie Kontext und weitere Regeln prüft.

Diese Lösung folgt dem Prinzip des *Zero Trust*, nach dem Nutzer und Geräte als unsicher bzw. nicht vertrauenswürdig angesehen werden, auch wenn sie sich logisch in einem bestimmten, meist internen Netzwerk befinden. D.h., ein solches internes Netzwerk wird ebenfalls als nicht sicher angesehen. Die Ver-

teidigungslinie wird mit Zero Trust Network Access (ZTNA) nahe an die Anwendungen gelegt.[128]

Auf diese Weise definiert ZTNA einen Software-Defined Perimeter (SDP). Wird der Zugriff erlaubt, so stellt die Lösung gegebenenfalls auch eine sichere Verbindung her; eine zusätzliche Lösung auf Netzwerkebene (wie ein *Virtual Private Network (VPN)*) ist dann nicht mehr erforderlich.

Gegensatz: Die etablierten Sicherheitsarchitekturen messen dem Schutz der Außenlinie (perimeter) große Bedeutung bei. Entsprechend sind wichtige Sicherheitsmaßnahmen am Übergang vom äußeren, unsicheren Netzwerk zum inneren, als sicher geltenden Netzwerk angeordnet. – Sobald Nutzer und die von ihnen genutzten Geräte Zugang zu einem internen, als sicher angesehenen Netzwerk erhalten haben, erhalten sie ohne weitere Prüfungen Zugriff auf viele Ressourcen, die sich in diesem Netzwerk befinden.

6.3 Anwendungen und Datenbanken

In diesem Kapitel werden Produktgruppen betrachtet, die

- der Anwendungssicherheit dienen
  (dazu gehören: *Proxy*, *Reverse Proxy*, *Web Application Firewall (WAF)* und *XML-Firewall* sowie *Static Application Security Testing (SAST)* und *Dynamic Application Security Testing (DAST)*, zwei Diensten bzw. Produkten für die Überprüfung von Anwendungssoftware)

  und solche,

- die Datenbanken absichern
  (das sind: *Database Activity Monitoring (DAM)*, *Database Audit and Protection (DAP)* und *Database encryption* (Datenbankverschlüsselung).

Zur Verschlüsselung von Storage, Cloud, Dateien, E-Mails und Medien siehe Kapitel 6.5.

Abb. 45 zeigt schematisch und stark vereinfachte Architekturmodelle, die die Verwendung der im Folgenden beschriebenen Lösungen für die Anwendungssicherheit (erste Abteilung) veranschaulichen.

[128] Zero Trust wurde von Forrester eingeführt; der Begriff „Zero Trust Network Access (ZTNA)“ geht auf Gartner zurück.

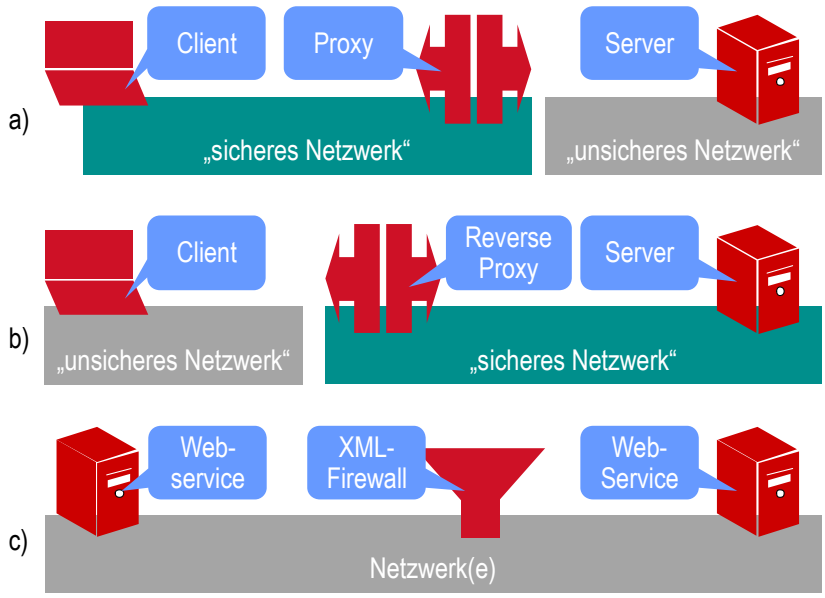


Abb. 45: Proxy (a), Reverse Proxy bzw. WAF (b) und XML-Firewall (c)

Proxy

Ein Proxy (englisch für Stellvertreter), auch **Forward Proxy** genannt, ist eine Instanz, die zwischen Client (aufrufende Entität) und Server (ausführende Entität) geschaltet ist, um den Client vor Gefahren aus dem Netz zu schützen, in dem sich der oder die Server befinden, um die IP-Adresse des Clients zu verbergen oder um Daten oder Protokolle umzusetzen. Siehe Abb. 45(a).

Ein Proxy verhält sich gegenüber dem Client wie ein Server und gegenüber dem Server wie ein Client. Damit ist er in der Lage, die Kommunikation des Clients bzw. die Kommunikation mit dem Client entsprechend seiner Aufgaben zu beeinflussen. Das Netz, in dem sich der Client befindet, gilt als das vertrauenswürdigere und wird oft als „internes“ Netz bezeichnet. Es gibt diverse Arten von Proxys für verschiedene Anwendungsfälle, die sich in ihrer Funktionsweise und ihrer Form der Integration in die IT zum Teil sehr deutlich unterscheiden.

Reverse Proxy

Ein Reverse Proxy (englisch für umgekehrter Stellvertreter) ist eine Instanz, die zwischen Client (aufrufende Entität) und Server (ausführende Entität) geschaltet ist, um den Server vor Gefahren aus dem Netz zu schützen, in dem sich der Client befindet, um die IP-Adresse des Servers zu verbergen oder (Sicherheits-) Funktionalitäten zu ergänzen, über die der Server selbst nicht verfügt. Siehe Abb. 45(b).

Ein Proxy verhält sich gegenüber dem Client wie ein Server und gegenüber dem Server wie ein Client. Damit ist er in der Lage, die Kommunikation zwischen Client und Server entsprechend seiner Aufgaben zu beeinflussen. Das Netz, in

dem sich der Server befindet, gilt als das vertrauenswürdigere und wird oft als „internes" Netz bezeichnet. Ein Reverse Proxy kann verschiedene Aufgaben übernehmen, zum Beispiel auch Lastverteilung und Entlastung des Servers durch Zwischenspeicherung bestimmter Antworten. Typische Sicherheitsfunktionen sind Malwareschutz, Transportverschlüsselung zum Client, Nutzer-Authentisierung und Schutz vor Angriffen auf den Server (hierzu siehe auch *Web Application Firewall (WAF)*.

Web Application Firewall (WAF)

Eine Web Application Firewall (WAF) funktioniert wie ein →*Reverse Proxy*. Siehe Abb. 45(b). Sie schützt eine Web-Anwendung vor Gefahren aus dem Netz, in dem es die Web-Anwendung oder den gesamten Web-Server abschirmt (nicht direkt erreichbar macht) und alle Kommunikation zur Web-Anwendung und zurück untersucht und gegebenenfalls verändert.

Insbesondere werden Angriffe wie SQL-injection, Command Injection, *Session Hijacking*, Cross-Site Scripting abgewehrt. Eine Web Application Firewall überprüft Eingabeparameter, überwacht den Inhalt von Protokollen und Formaten (insbesondere XML) und wehrt *Denial-of-Service*-Angriffe ab.

Mit Hilfe von Scannern können Schwachstellen der Web-Anwendung aufgespürt und in Profile für Aktionen der Web Application Firewall umgewandelt werden.

Web Application Firewalls gibt es als Erweiterung (Plug-in), als eigenständige *Appliance* oder in Form eines Internet- bzw. Cloud-Service.

XML-Firewall

Eine XML-Firewall überprüft die mittels XML zwischen Anwendungen ausgetauschten Daten, filtert diese und steuert den Zugriff auf Ressourcen, die mittels XML angesteuert werden. XML-Firewalls schützen die Machine-to-Machine (M2M) – Kommunikation zwischen Webservices (Web-Dienste bzw. Web-Anwendungen). XML-Firewalls bieten Zugriffskontrolle auf angefragte Webservices und Funktionen abhängig von der anfragenden Entität und der XML-Nachricht. Letztere können vollständig verschlüsselt sein oder Daten enthalten, die verschlüsselt sind. XML unterstützt auch digitale Signaturen. Aufgrund der Vielfalt dieser Funktionen können XML-Firewalls sehr komplex sein. Sie werden auch als **Webservice Firewalls** oder **Webservice Security Gateways** bezeichnet.

XML (Extensible Markup Language) ist eine Metasprache bzw. ein Format zur Darstellung und Übertragung von strukturierten Daten, das ein einfaches Textformat für die Daten selbst, deren Beschreibung sowie die Beziehungen unter ihnen verwendet. XML ermöglicht den Austausch von Daten zwischen Anwendungen bzw. Webservices.

Eine Serviceorientierte Architektur (SOA) strukturiert und modularisiert Dienste (IT-Services), um deren Wiederverwendbarkeit zu erhöhen. Diese strukturierten und modularisierten Dienste werden **Webservices** genannt. Letztere tauschen XML-Daten aus und ermöglichen es, andere Webservices aufzurufen. Diese Funktionen unterstützt das Netzwerkprotokoll SOAP (Simple Object Access Protocol).

Abb. 46 zeigt zwei wichtige Lösungen für die Anwendungssicherheit (erste Abteilung) und drei Produktgruppen für die Absicherung von Datenbanken (zweite Abteilung von Lösungen). Die drei Begrifflichkeiten für die Absicherung von Datenbanken wurden von Gartner geprägt.[129]

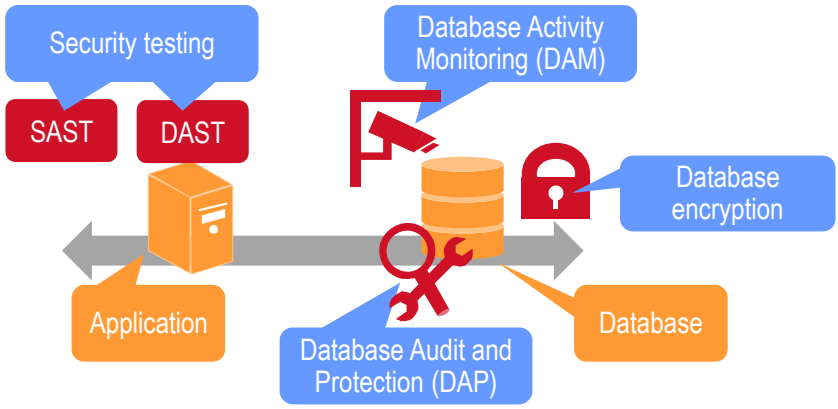


Abb. 46: Sicherheitsüberprüfung von Anwendungen und Datenbank-Sicherheitslösungen

Static Application Security Testing (SAST)

Überprüfung von Source-Code, Bytecode oder Binärcode auf Schwachstellen. SAST ermöglicht es, Fehler frühzeitig während der Entwicklung zu finden und zu beseitigen. SAST ist prinzipiell als Software verfügbar, wird aber in der Regel als Service angeboten, bei dem der Programmcode auf einen Server geladen und dort analysiert wird. Der Kunde erhält einen Bericht mit den Schwachstellen.

Dynamic Application Security Testing (DAST)

Überprüfung von Software, um Schwachstellen zu finden, während sie ausgeführt wird. Dabei werden dem Programm Nachrichten oder Aufforderungen übergeben, und es werden die Antworten analysiert. Dadurch wird geprüft, ob Eingabeparameter richtig überprüft werden, und es können auch Schwachstellen gefunden werden wie Cross-Site Scripting, Buffer overflow und SQL-injection. DAST arbeitet also wie ein automatisierter (blackbox) Penetrationstest.

---

[129] Siehe auch: Gartner: Gartner Glossary, Information Technology; https://www.gartner.com/en/information-technology/glossary; zuletzt aufgerufen am 21.01.2021

Database Activity Monitoring (DAM) (Datenbanküberwachung)

Transparent im Hintergrund laufende Überwachung einer *Datenbank* im Betrieb, um feindliche, betrügerische, unerlaubte und unerwünschte Aktivitäten identifizieren zu können. Außerdem werden Aufzeichnungen (log data, audit data) darüber angefertigt, durch wen wann auf welche Daten zugegriffen wurde.

Database Audit and Protection (DAP)

Kann als Erweiterung von *Database Activity Monitoring (DAM)* verstanden werden, bietet aber vor allem Datenanalyse und deren Klassifikation, Schwachstellenanalyse sowie Einbruchserkennung und -verhinderung (intrusion prevention, früher auch als **Database IPS** bezeichnet).

Ein Scanner sucht zum Beispiel nach unplausiblen Nutzerrechten, nicht mehr aktiven Nutzerkonten, fehlerhaften Konfigurationen und anderen Schwachstellen. Die Software korrigiert Schwachstellen zum Beispiel bei der Verarbeitung von Eingabeparametern bzw. gibt Hinweise zur Verbesserung der Konfiguration.

Database encryption (Datenbankverschlüsselung)

Die Verschlüsselung der in einer *Datenbank* gespeicherten Daten kann mit Werkzeugen der Datenbank bzw. des *Datenbankmanagementsystems (DBMS)* selbst erfolgen oder mit Hilfe von zusätzlichen Produkten, die die Verschlüsselung durchführen. Die Verschlüsselung kann die ganze Datenbank, ausgewählte Spalten oder einzelne Felder betreffen. Sie kann innerhalb des DBMS, im Datenfluss zum Speichermedium, auf dem Speichermedium bzw. im *Storage-System* oder auf Applikationsniveau (d.h. im Datenfluss bei Aufruf der Datenbank) erfolgen. Nicht alle Varianten bzw. Kombinationen sind möglich, da die Datenbank die meisten Operationen nur mit unverschlüsselten Daten ausführen kann.

Die Verschlüsselung soll die Daten vor unberechtigtem Zugriff schützen. Datenbanken enthalten oft sensible Daten, die nicht in fremde Hände fallen dürfen. Auch Personal, das berechtigt und beauftragt ist, die IT-Installation mit der Datenbank zu administrieren, soll nicht auf solche Daten zugreifen können. Insbesondere wenn *Hardware-Sicherheitsmodule (HSMs)* für die Verschlüsselung verwendet werden, sind die Administration der Datenbank und der Zugriff auf die gespeicherten Daten auch physisch voneinander getrennt.

Die Verschlüsselung kann nur dann ihren Zweck erfüllen, wenn für die sichere Speicherung und Verwendung des dafür nötigen geheimen Parameters (des kryptografischen Schlüssels) gesorgt ist. Die Verwaltung der Schlüssel (*key management*) ist deshalb ein entscheidender Aspekt bei der Konzeption der Datenbankverschlüsselung.

Weitere Verschlüsselungslösungen und Maßnahmen für den Datenschutz werden in Kapitel 6.5 beschrieben.

6.4 System- und Datenintegrität

Die *Integrität (integrity)* wird in der IT-Sicherheit manchmal ein wenig unterschätzt. Oft steht die Vertraulichkeit im Rampenlicht. Allerdings muss erst einmal die Integrität sichergestellt werden, bevor auch für die Vertraulichkeit gesorgt werden kann. Entsprechend findet man in der Kategorie „System- und Datenintegrität" diverse Scanner und Filter mit und ohne Reinigungsfunktion einschließlich der weit verbreiteten Anti-Malware- bzw. Anti-Virus-Lösungen.

Auch Maßnahmen der physischen Sicherheit sorgen für die Unversehrtheit von IT-Systemen. Auf Sicherheitsmodule wird jedoch in Kapitel 6.7 eingegangen. Darüber hinaus gibt es für den Schutz innerhalb des Rechenzentrums zum Beispiel Käfige, die einzelne Systeme zusätzlich schützen, sowie diverse Maßnahmen der Gebäude- und Umgebungssicherheit wie zum Beispiel zur Zutrittskontrolle und der Überwachung. Diese Maßnahmen werden, auch wenn manche in Produktform existieren, hier nicht behandelt.

File Integrity Monitoring (FIM)

Überwacht die Integrität von Dateien und erkennt und meldet Veränderungen an diesen. Dazu erfasst die Lösung initial die (kryptografischen) Prüfsummen und weitere Attribute der unversehrten, später zu überwachenden Dateien. Prüfsummen und Attribute werden als Referenzwerte gespeichert. In der Überwachungsphase werden die Prüfsummen der zu überwachenden Dateien erneut berechnet und Attribute werden erneut erfasst und jeweils mit den gespeicherten Referenzwerten verglichen.

Ausführbare Programme und Daten, die auch die Programmausführung steuern bzw. beeinflussen können, werden vom Betriebssystem in Form von Dateien (files) gespeichert. Änderungen können auf Manipulationen von Systemeinstellungen oder das Einschleusen von Malware hindeuten.

Da die Zahl der Dateien sehr groß ist und sich ihre Inhalte und ihre Attribute mitunter sehr häufig ändern, erfasst die Lösung weitere Kontextinformationen, die dazu genutzt werden, die identifizierten Änderungen daraufhin zu bewerten und zu filtern, ob sie durch eine möglicherweise feindliche Manipulation oder die sachgemäße Nutzung verursacht wurden.

Auf jedem der zu überwachenden Computersysteme wird eine Software installiert. Die Konfigurations- und Dashboard-Funktionen (Konsole) können auf einem separaten Computersystem installiert werden oder online als Cloud-Service genutzt werden.

File Integrity Monitoring kann die *Trusted Computing Platform (TCP)* mit dem *TPM (Trusted Platform Module)* verwenden, um kryptografische Operationen durchzuführen und Daten sicher zu speichern.

Vulnerability scanner (Schwachstellen-Scanner)

Software, die im Betrieb befindliche IT-Komponenten untersucht und bekannte *technische Schwachstellen* (Vulnerabilities, technical) automatisiert ermittelt. Schwachstellen-Scanner sind für den wiederholten bzw. regelmäßigen Einsatz konzipiert und meist in die Betriebsumgebung integriert.

Auf jedem zu prüfenden Computersystem wird ein Software-Agent installiert, der den Scan lokal durchführt, durch eine zentrale Komponente gesteuert wird und seine Ergebnisse dorthin übermittelt.

Bei anderen Lösungen nutzt eine zentrale Software eine Standardschnittstelle, um mit den Computersystemen zu kommunizieren. In diesem Fall wird durch Absuchen des Netzes ermittelt, welche Computersysteme sich im Netzwerk befinden. Dies wird als **Network Discovery** bezeichnet. **Network port and service identification** liefert weitere Informationen über Schnittstellen und Protokolle, die von den zu prüfenden Systemen unterstützt werden. Schwachstellen-Scanner verwenden die so ermittelten Informationen oder können sie durch eigene Funktionen selbst ermitteln.[130]

Schwachstellen-Scanner ermitteln Schwachstellen wie folgt: a) Die detaillierte Version einer Software oder eines Systems, auch als **Patch-Level** bezeichnet, zeigt unter Verwendung von anderen Informationen (*CERT-Meldungen, CERT advisories)*, welche Schwachstellen in dem System noch nicht beseitigt, also noch vorhanden sind. b) Es wird durch Ausprobieren ermittelt, ob Funktionen, Schnittstellen oder Protokolle verfügbar sind, die durch Härtung (Hardening: sicherheitskonforme Konfiguration) eigentlich entfernt und nicht verfügbar sein sollten. c) Konfigurationen (Systemeinstellungen) werden ausgelesen und einem Soll-Ist-Vergleich unterzogen.

Ein **Compliance scanner** untersucht, ob die Implementierung einem Standard entspricht. Er ist in gewisser Hinsicht ebenfalls ein Vulnerability scanner, nämlich dann, wenn dieser nach Unterschieden zu einem Sicherheitsstandard sucht, denn solche Abweichungen können in vielen Fällen Schwachstellen bedeuten.

Anti-Malware/Anti-Virus

Software, die nach Schadsoftware (malware) sucht, diese aufspürt und ihre Ausführung verhindert, indem sie die Schadsoftware entfernt, blockiert oder isoliert (in Quarantäne bringt). Meist wird dann der Anwender informiert. Die Software untersucht kontinuierlich oder regelmäßig die Speicher von Computersystemen sowie den Informationsaustausch innerhalb des Systems und mit dessen Außenwelt.

---

[130] NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations; April 2013 (updated 2015), Rev. 4

Schadsoftware wird in Systeme eingeschleust, um unautorisiert Zugang zu Daten oder IT-Services zu erhalten, um Daten oder Systeme zu manipulieren oder um zu verhindern, dass Berechtigte auf Informationen, Systeme und Services zugreifen können. Oft dient eine Schadsoftware nur der Vorbereitung eines solchen Angriffs. Sogenannte Spyware wird zum Beispiel genutzt, um Passwörter auszuspionieren. Schadsoftware wird auch als **Malware** (Abkürzung für „malicious software") oder Virus bezeichnet, sowie nach der Verbreitungsform in Viren, Würmer und Trojaner eingeteilt.

Die Anti-Malware- oder Anti-Virus-Lösung erkennt Schadsoftware an Merkmalen wie Codesequenzen oder an ihrem Verhalten. Da ständig neue Schadsoftware in Verkehr gebracht wird und sich modifiziert, muss der Schutz- bzw. Erkennungsmechanismus kontinuierlich aktualisiert werden. Bei Enterprise-Installationen mit sehr vielen Computersystemen (Endgeräte, Server, Netzwerkkomponenten) wird ein eigenes System für die Aktualisierung bzw. die Verteilung der Signaturen bzw. „anti-virus pattern" genutzt. Endverbraucher beziehen die Aktualisierungen direkt vom Anbieter über das Internet.

Es gibt Lösungen für Computersysteme allgemein, für den Schutz auf E-Mail-Servern und E-Mail-Clients sowie für weitere spezielle Anwendungszwecke wie zum Beispiel das Laden und die Verarbeitung von Internetinhalten im Browser. E-Mail spielt eine besondere Rolle, weil sie ein häufig genutztes Eingangstor für das Einschleusen von Schadsoftware darstellt.

Spam-Schutz

Spam bezeichnet unerwünschte E-Mail, die massenhaft verbreitet wird, die die Produktivität des Empfängers beeinträchtigt, die IT-Systeme unnötig belastet sowie auch häufig der Verbreitung von Schadsoftware dient.

Spam-Schutz oder **Spam-Filter** sind Lösungen, die derartige Nachrichten (E-Mails) von anderen unterscheiden und entsprechend kennzeichnen oder isolieren (in einen Spam-Ordner verschieben) können. Die Lösung erkennt Spam anhand von Merkmalen wie Texten oder Mustern, die in sehr vielen E-Mails zu finden sind. Solche Merkmale können bei der Analyse von sehr vielen E-Mails identifiziert werden, die dann an die Spam-Schutz-Lösung zur Erkennung von Spam übermittelt werden.

Phishing protection

Software, die verhindert, dass Nutzer vertrauliche Daten wie Passwörter an einen Trickbetrüger verraten, der sich als legitimierter, vertrauenswürdiger Empfänger (Unternehmen, Institution oder Person) ausgibt.

Diese Lösung ist oft in eine *Anti-Malware*/*Anti-Virus*-Lösung integriert. Sie basiert auf folgenden Funktionen:

a) Erkennen von Webseiten, die für Phishing benutzt werden, und Blockieren des Zugriffs darauf. Dazu werden E-Mails, deren Anhänge, Dateien, Eingaben des Nutzers usw. überprüft.
b) Prüfen von Webseiten und Erkennen, das es sich zum Beispiel um gefälschte, in betrügerischer Absicht erstellte Webseiten handelt.
c) Erkennen von E-Mails, die für Phishing benutzt werden, mit ähnlichen Techniken, wie sie beim *Spam-Schutz* zum Einsatz kommen.

Content-Filter

Software, die unerwünschte Inhalte bzw. Inhaltstypen blockiert, sodass sie nicht genutzt werden können. Abhängig vom Einsatzszenario kann es sich dabei um Inhalte handeln, die illegal sind, die gegen moralische oder rechtsstaatliche Prinzipien verstoßen, die die öffentliche Ordnung gefährden können, deren Nutzung nicht im Interesse zum Beispiel des Arbeitgebers liegt (zum Beispiel, weil die Produktivität sinken kann), die nicht jugendfrei sind oder die IT-Sicherheit gefährden können. Lösungen, die Reklame (Werbung, englisch: „ad" bzw. „advertising") herausfiltern, sind ebenfalls Content-Filter.

Der Content-Filter kann Webseiten bzw. ihre URL mit Positiv- oder Negativlisten vergleichen (white/black listing), Stichwörter oder Textphrasen erkennen sowie Bilder und Darstellungen prüfen. Je nach Konfiguration und Einsatzszenario kann die Software die Nutzung unterbinden oder den Nutzer warnen und um seine explizite Zustimmung ersuchen. Eine einfache Form eines Content-Filters ist ein **URL-Filter**, der mit Positiv- oder Negativlisten der Internetadressen arbeitet.

Content-Filter sind als **Secure Web Gateway (SWG)** und zur Installation auf Endgeräten verfügbar und werden in beiden Fällen dort mit einer *Anti-Malware/Anti-Virus*-Lösung verbunden. Content-Filter sind auch als Plug-in (Zusatzsoftware) zum Beispiel für Browser erhältlich oder werden als Zusatz zum Internet-Zugang als Web-/Cloud-Lösung angeboten.

6.5 Datensicherheit und Datenschutz

Bei vielen IT-Sicherheitsprodukten und IT-Sicherheitslösungen gibt es verschiedene Varianten. Das macht die Verständigung manchmal schwierig und erschwert das Verständnis. Dies gilt für manche Produktgruppen, die im letzten Kapitel 6.4 beschrieben wurden ebenso wie für die, die jetzt folgen. Abb. 47 zeigt Beispiele für sechs Eigenschaften, die dabei helfen, Varianten von Produkten zu unterscheiden.

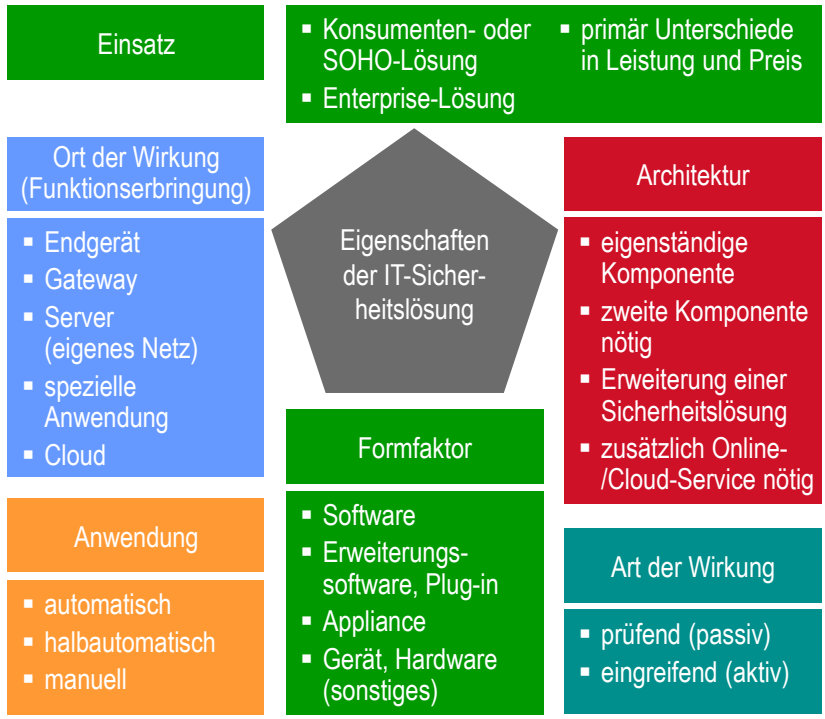


Abb. 47: Beispiele für Eigenschaften, die helfen, Varianten von Produkten zu unterscheiden (Mehrfachnennungen teilweise möglich)

Zum Beispiel gibt es Anti-Malware/Virus-Lösungen für den Einsatz auf Arbeitsplatzrechnern, solche für E-Mail-Server, und die Anti-Malware/Virus-Funktionalität wird auch in Gateways zur Verfügung gestellt. Auch Content-Filter werden in verschiedenen Formen angeboten. Das Gleiche gilt für Verschlüsselungslösungen. Einige Varianten werden im Folgenden beschrieben. Abb. 48 zeigt eine Übersicht über die in diesem Kapitel vorgestellten Produkte und Lösungen. Varianten sind nicht aufgeführt, aber im Text beschrieben.

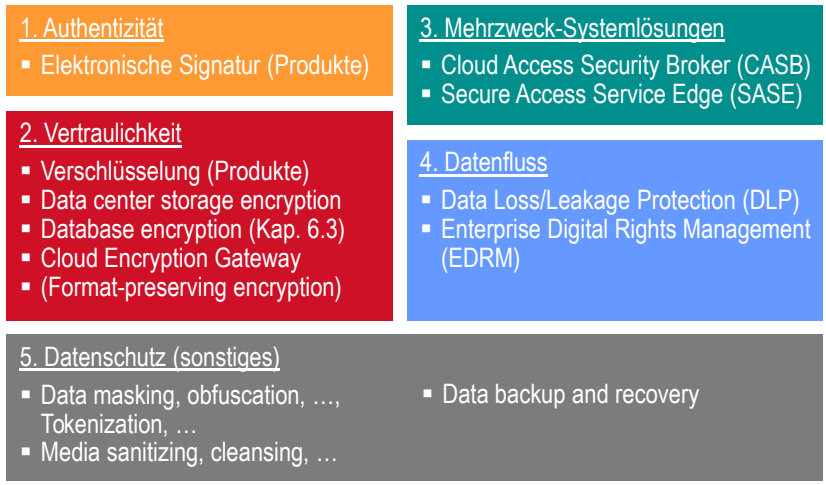


Abb. 48: Produkte und Lösungen zu „Datensicherheit und Datenschutz“ (Übersicht)

Elektronische Signatur (Produkte)

Produkte, Komponenten und Lösungen, die es ermöglichen, die *Authentizität (authenticity)* von Daten sicher feststellen zu können, indem sie die Daten beim Absenden (oder Schreiben) mit einer elektronischen (digitalen) Signatur versehen und diese beim Empfangen (oder Lesen) wieder kontrollieren. Die Authentizität umfasst die *Integrität (integrity)* oder Unversehrtheit sowie den Nachweis der Herkunft von Daten (Datenursprung).

Die Produktarten sind ähnlich denen für die →*Verschlüsselung (Produkte)*. Häufig werden von solchen Produkten beide Funktionalitäten angeboten. Komponenten für die Signatur sind ebenso wie die für die Verschlüsselung in großer Zahl in den verschiedensten IT-Systemen (zum Beispiel Betriebssystemen) und in vielen Sicherheitslösungen enthalten. Mit der Signatur als sichtbarer, primärer Funktionalität werden sie zum Beispiel für den Schutz von Dateien (files), E-Mails und XML-Daten angeboten.

Signaturen werden mittels kryptografischer Algorithmen wie RSA, DSA und EC (Elliptischen Kurven) erzeugt und verifiziert.

Verschlüsselung (Produkte)

Produkte, Komponenten und Lösungen, die die *Vertraulichkeit (confidentiality)* von Daten sicherstellen, indem sie diese in eine Form konvertieren (verschlüsseln), die für Unberechtigte (Personen oder Systeme) nicht verwendbar ist. Die Wiederherstellung der ursprünglichen Form (Entschlüsselung) ist nur unter Verwendung eines Geheimnisses (Schlüssels) möglich, das die Produkte, Komponenten und Lösungen vor unberechtigtem Zugriff und unautorisierter Verwendung ebenfalls schützen. Manchmal sind jedoch zusätzliche Komponenten oder Lösungen nötig, um dies zu bewerkstelligen.

Üblicherweise wird bei dieser Form der Datensicherheit unterschieden, ob die Daten gerade gespeichert sind, also ruhen (**Data at rest**), kommuniziert bzw. übertragen werden (**Data in transit**, **Data in motion**) oder gerade verarbeitet werden (**Data in use**, **Data in process**). Entsprechend werden die Verschlüsselungslösungen bezeichnet, wobei es entweder „Data encryption at rest" oder „Data at rest encryption" und dergleichen heißen kann.

Produkte der Kategorie „Data at rest encryption" gliedern sich in solche, die spezielle Daten verschlüsseln wie Dateien (files) oder E-Mails und solche, die ein spezielles Speichermedium als Ganzes oder logische Teile davon (zum Beispiel Partitionen) sichern. Zu den unterstützten Speichermedien gehören Festplatten (hard disks), Speichersysteme (storage) oder Magnetbänder (tapes). Die „Data in transit encryption" ist Teil von Lösungen zur sicheren Kommunikation und der Absicherung von Netzwerken wie zum Beispiel Lösungen für ein *Virtual Private Network (VPN)*. Zur "Data in use encryption" gehört die Verschlüsselung von Hauptspeicher (memory).

Neben der technischen Umsetzung der Verschlüsselung muss auch für die Verwaltung der verwendeten Schlüssel (*key management*) gesorgt werden. Produkte können automatisch verschlüsseln bzw. die Entscheidung darüber selbst treffen oder sie dem Nutzer überlassen. Die Entscheidung sollte Regeln für die Klassifikation von Daten folgen.

Details zu den zugrunde liegenden kryptografischen Algorithmen und Verfahren sowie ihren Anwendungen enthält Kapitel 8.

Data center storage encryption

Für die Verschlüsselung von Daten, die in einem → *Storage (-System)* gespeichert sind, gibt es im Prinzip drei Möglichkeiten:

Bei der serverseitigen Verschlüsselung (**Server-side encryption, SSE**) verschlüsselt eine Software des Anwenders die Daten auf dem Computersystem (host), bevor sie zum Storage-System übertragen werden. Die Verschlüsselung kann alle Daten betreffen, oder es werden nur einzelne Datenelemente (wie Dateien) verschlüsselt. Siehe auch *Database encryption*.

Die Verschlüsselung kann zweitens im Datenfluss zum Speichermedium erfolgen und im Netzwerk (switching fabric) des Rechenzentrums implementiert sein. Eine Implementierung an der Schnittstelle des Hosts zum Storage-Netzwerk ist ebenfalls möglich.

Drittens kann die Verschlüsselung im Storage-System selbst erfolgen, die der Hersteller dort implementiert. Sogenannte **Self-Encrypting Drives (SED)** sind Festplatten (hard disk drives, HDDs), die den gesamten Inhalt der Festplatte (Full Disk Encryption, FDE) verschlüsseln können. Die Verschlüsselung ist in der Steuerungseinheit (Controller) der Festplatte implementiert; der Schlüssel

ist wählbar. Soll die Festplatte wiederverwendet oder verschrottet werden, so löscht der Administrator vorher den Schlüssel in der Festplatte.

„Data center storage encryption“[131] bezieht sich im engeren Sinne auf Produkte, die verschiedene, in einem Rechenzentrum eingesetzte Verschlüsselungsprodukte bzw. -lösungen zu konfigurieren und zu verwalten gestatten.

Cloud Encryption Gateway

Computersystem, das aus Anwendersicht einem *Cloud-Computing*-Service vorgeschaltet ist und dessen Nutzung ermöglicht. Es arbeitet als →*Proxy* und verschlüsselt und/oder anonymisiert (→*Data masking*) Datenelemente auf dem Weg vom Anwender zum Server bzw. in die Cloud.

Wird cloudbasierte *Software-as-a-Service (SaaS)* genutzt, so besteht das Problem, dass die verschlüsselten Datenelemente den Formatanforderungen der Cloud-Anwendung entsprechen müssen. Es muss dann eine formaterhaltende Verschlüsselung (*Format-preserving encryption)* verwendet werden.

Format-preserving encryption (formaterhaltende Verschlüsselung)

Kein Produkt, sondern eine Art der Verschlüsselung. Um die Vertraulichkeit von Daten gewährleisten zu können, kann die Anforderung bestehen, dass ein Anwendungsprogramm oder eine Datenbank mit verschlüsselten Daten arbeitet statt mit den lesbaren und verwendbaren Originaldaten. Dies ist (ohne große Änderungen an der datenverarbeitenden Software) nur dann möglich, wenn bestimmte Eigenschaften der lesbaren und verwendbaren Originaldaten (Eingabe) auch nach der Verschlüsselung (Ausgabe) vorhanden sind, also bestehen bleiben. Erwartet die datenverarbeitende Software zum Beispiel einen Wert einer bestimmten Länge, so müssen auch die Ersatzdaten diese Länge haben. Das Gleiche gilt für die Kodierung also zum Beispiel die Einschränkung auf alphanumerische Zeichen. Eventuell sollen die Daten auch zu einer bestimmten Kategorie gehören bzw. eine bestimmte Bedeutung haben, wie zum Beispiel lesbare Worte enthalten. Solche Eigenschaften werden hier als „Format“ bezeichnet, und die Verschlüsselung ist „formaterhaltend“, wenn die verschlüsselten Ersatzdaten das „Format“ der Originaldaten haben.

Eine formaterhaltende Verschlüsselung ist zum Beispiel für ein *Cloud Encryption Gateway* nützlich, das die Originaldaten konvertiert und dann an eine cloudbasierte Anwendung weiterleitet.

Eine formaterhaltende Verschlüsselung ist immer mit Einschränkungen für die Verarbeitung der Daten verbunden. Sogar die Einhaltung der Länge kann ein Problem darstellen, selbst wenn ein Blockverschlüsselungsalgorithmus zum Einsatz kommt, der die Länge an sich nicht verändert. Die lesbaren und verwendbaren Originaldaten können Muster aufweisen, zum Beispiel Teile

[131] Der Begriff wurde von Gartner geprägt.

enthalten, die in anderen Daten enthalten sind (Beispiel: „Metallschraube“ und „Holzschraube“). Diese Muster gehen verloren, sodass die Software nicht nach ihnen suchen kann. Andererseits können solche Muster durchaus ein Problem für die Vertraulichkeit darstellen. Zum Beispiel könnten gleichlautende Felder „Nachname“ eine mögliche Zugehörigkeit zu einer Familie zeigen, auch wenn die Daten verschlüsselt wurden. Deshalb verwendet man Blockverschlüsselungsalgorithmen häufig im CBC-Modus (Cipher Block Chaining), bei dem Eingangsdaten, die gleichlautend beginnen, zu verschlüsselten Daten führen, die nicht gleichlautend beginnen.

Cloud Access Security Broker (CASB)

Lösung, die aus Anwendersicht den *Cloud-Computing*-Services eines IT-Dienstleisters vorgeschaltet ist und deren Nutzung gemäß den Sicherheitsrichtlinien des Anwenders dadurch ermöglicht, dass die Lösung Sicherheitsfunktionen wie *Authentisierung*, *Autorisierung*, *Verschlüsselung*, *Anonymisierung*, Schutz vor *Malware* und dergleichen erbringt.[132]

Secure Access Service Edge (SASE)

Kombiniert a) *Cloud Access Security Broker (CASB)* zur Durchsetzung von Sicherheitsrichtlinien, die der Cloud-Computing-Service nicht unterstützt, b) *Secure Web Gateway (SWG)*, damit unerwünschte Inhalte bzw. Inhaltstypen blockiert werden (*Content-Filter*), c) *Zero Trust Network Access (ZTNA)*, eine Lösung, die die Verteidigungslinie vom Netzwerkzugang bis vor die Anwendungen verlegt und d) *Firewall-as-a-Service (FWaaS)*.[133]

SASE wird “sässi” ausgesprochen.

Data Loss Protection (DLP), Data Leakage Prevention

Diese Lösungen finden vertrauliche Informationen, die gespeichert, verarbeitet oder übertragen werden bzw. werden sollen, und verhindern unautorisierte Zugriffe auf diese Informationen und absichtliche oder unabsichtliche Versuche, diese unerlaubt zu übertragen.

DLP schränkt die Möglichkeiten zur Weitergabe von Informationen derart ein, dass unautorisierte Nutzer nicht in den Besitz dieser Informationen gelangen können. Die Lösung teilt Ziel und Funktionalität mit der *Informationsflusskontrolle* (information flow control) und setzt diese im Wirkungsbereich der DLP-Lösung um. Lösungen, die mehr als einen bzw. mehrere Übertragungskanäle

---

[132] Der Begriff „Cloud Access Security Broker (CASB)“ wurde von Gartner geprägt.

[133] Andrew Lerner: Say Hello to SASE (Secure Access Service Edge); Gartner, blog post, December 23, 2019, https://blogs.gartner.com/andrew-lerner/2019/12/23/say-hello-sase-secure-access-service-edge/; zuletzt aufgerufen am 21.01.2021
Der Begriff „Secure Access Service Edge (SASE)“ wurde von Gartner geprägt.

überwachen, kombinieren verschiedene Funktionalitäten und integrieren oft weitere Lösungen, die nicht für DLP entwickelt wurden.

Zu den wiederkehrenden DLP-Funktionalitäten gehören unter anderem: Nutzer werden gewarnt und explizit um Freigabe gebeten. In anderen Fällen wird die Nutzung oder Übertragung unterbunden, oder es erfolgt eine Zwangsverschlüsselung vor der Übertragung. Um Datenverlust zu vermeiden, werden Daten automatisch gesichert. Dazu werden Ports und Schnittstellen ebenso überwacht wie der Netzwerkverkehr. Regeln werden situationsbedingt und unter Verwendung verschiedener Kontextinformationen (authentisierter Nutzer, Gerät, Anwendung, Zugriff, Zeit, Ort usw.) angewandt. Solche und ähnliche Funktionen werden auf jedem Endgerät und in Netzwerkverbindungen implementiert. Vor allem bei Unternehmenslösungen werden auch umfangreiche Berichtsfunktionen (reporting) integriert.

Enterprise Digital Rights Management (EDRM)

Diese Lösungen, auch als **Rights Management Service (RMS)** bezeichnet, binden Rechte, wie die Nutzung oder Lesbarkeit von Informationen und das Kopieren oder Drucken, an den Datensatz (Datei, E-Mail). Damit bleiben die definierten Beschränkungen erhalten, auch wenn der Datensatz elektronisch übermittelt und andernorts gespeichert wird. Autorisierte Nutzer können die ihnen eingeräumten Rechte nicht an andere übertragen.

Im Prinzip kann dies auch durch eine *Zugriffskontrolle* erreicht werden – allerdings nur dann, wenn der Datensatz nicht aus dem Einflussbereich der Zugriffskontrolle gebracht werden kann. Bei der Benutzung vernetzter Computersysteme ist dies jedoch kaum gegeben (→*Grenzen der Zugriffskontrolle*). Mit EDRM bleibt die Sicherheit einschließlich der Vertraulichkeit dagegen trotzdem gewährleistet. Das Ziel, die Informationen unabhängig vom Speicherort zu schützen, teilt EDRM mit der *Informationsflusskontrolle* (information flow control).

Kern der Lösung ist die Verschlüsselung des Datensatzes und ein Integritätsschutz der darin gegebenenfalls gespeicherten Rechte. Berechtigte Nutzer authentisieren sich gegenüber einem zentralen Server. Dieser überträgt den Schlüssel an die zum System gehörende Client-Komponente, die den Datensatz dann entschlüsseln kann. Sie sorgt ebenfalls für die Durchsetzung der weiteren Rechte wie Kopieren und Drucken. Die Rechte können im Datensatz selbst oder auf dem zentralen Server gespeichert sein.

Einen anderen Ansatz, vertrauliche Daten vor Offenlegung durch autorisierte Nutzer zu schützen, verfolgt *Data Loss Protection (DLP)/Data Leakage Prevention*.

EDRM darf nicht mit DRM verwechselt werden. **Digital Rights Management (DRM)** soll die Nutzung illegaler Kopien verhindern bzw. mindestens deren Verteilung erkennbar machen.

Data masking

Verhindert, dass datenschutzrelevante Daten missbraucht werden, indem die Originaldaten (in der Regel Daten in Tabellen bzw. in Feldern von Datenbanken) durch andere ersetzt werden. D.h., es werden die Werte wiederkehrender Parameter manipuliert. Zum Beispiel werden Namen von Personen durch andere mögliche Familien- und Vornamen ersetzt und Geburtsdaten durch willkürliche Kalenderdaten. Andere Begriffe sind **data obfuscation**, **deidentification**, **deauthorization** und **data scrambling**.

Beim **Static data masking** erfolgt der Austausch bleibend. Dadurch entsprechen die Daten strukturell den Originaldaten, sodass sie für Testzwecke verwendet werden können. Spielt dies keine Rolle, so können die Daten auch durch Platzhalter, Sterne oder andere feste Zeichen ersetzt werden.

Beim **Dynamic data masking** werden die Daten typischerweise vor dem Speichern (in einer Datenbank) ersetzt und nach dem Lesen für die Verarbeitung durch das Anwendungsprogramm wiederhergestellt. Das bedeutet, dass die Übersetzungstabelle ebenfalls gespeichert und entsprechend geschützt werden muss. Im Amerikanischen ist auch der Begriff **Tokenization** üblich, weil ein Token (eine Übersetzungstabelle zwischen zwei Referenzwerten) benutzt wird, um den Bezug zwischen Daten und den Identitäten herzustellen, die verborgen werden sollen.

Wenn vorrangig Namen von Personen geschützt werden sollen, spricht man weiterhin auch von **Pseudonymisierung** und **Anonymisierung**. Bei der Pseudonymisierung kann der Bezug zur Person, wie bei den obigen Begriffen, wiederhergestellt werden. Bei der Anonymisierung wird dagegen jeglicher Bezug in einer nicht wiederherstellbaren Form entfernt.

Media sanitizing

Software oder Hardware, die Daten von einem Datenträger (medium) so entfernt, dass diese nicht wiederhergestellt oder rekonstruiert werden können (**sanitization** oder **cleansing**). Dadurch wird verhindert, dass vertrauliche Daten in unautorisierte Hände gelangen, wenn Datenträger wiederverwendet oder entsorgt werden sollen.

Die Lösung gibt es für verschiedene Typen von Medien wie Magnetbänder, Festplatten (magnetisch/HDD, solid-state/SSD), optische Speichermedien (CD-ROM, DVD), Halbleiterspeicher (Module, USB-Sticks usw.) u.a.

Die Methoden können zerstörend sein. Hier kommen Geräte (Hardware) zum Einsatz, die Speichermedien bis zur Unbrauchbarkeit zerkleinern (schreddern). Sollen die Medien wiederverwendet werden, so spricht man auch von **Wiederaufbereitung**.

Data backup and recovery

Software, die Daten auf zusätzlichen, sekundären Speichermedien wie Festplatten (hard disk), Magnetbändern (tapes) oder optischen Speichern (DVDs usw.) sichert und die Wiederherstellung der Daten am ursprünglichen, primären Speicherort ermöglicht. Dadurch wird ein Schaden durch Datenverlust (Nichtverfügbarkeit) am primären Speicherort vermindert oder sogar ganz vermieden.

Solche Lösungen sichern Daten automatisch oder auf Veranlassung des Nutzers nach Bedarf. Nur beim vollständigen Sichern entsteht eine Sicherheitskopie, weil der gesamte Datenbestand auf ein anderes Medium kopiert wird.

Beim inkrementellen Sichern (snapshot integrated) werden Veränderungen aufgezeichnet, die beim Wiederherstellen (recovery) nacheinander abgearbeitet werden, um den Anfangszustand wiederherzustellen. Neue Daten (Veränderungen) werden an eine andere Stelle auf dem gleichen Datenträger oder Storage-Bereich geschrieben; die alten Daten bleiben dort gespeichert und werden nicht verändert. Der Schnappschuss (snapshot) erfasst, welche Datenblöcke existieren und zu welcher Version der Daten sie gehören.[134] Deshalb spricht man hier auch von einem virtuellen Abbild. Eine echte Sicherheitskopie (physisches Abbild bzw. Kopie) entsteht erst, wenn die Informationen auf einem anderen Medium liegen und dort nicht den gleichen Risiken ausgesetzt sind.

6.6 Endgeräte (mobil und Office)

Viele der in den letzten Kapiteln beschriebenen Produktgruppen oder Produkte werden auch für den Schutz von Endgeräten angeboten. In diesem Kapitel werden solche Varianten nicht noch einmal beschrieben. Allerdings bilden die Produkte für Endgeräte („endpoints“) schon eine eigenständige Kategorie auf dem Markt, und es gibt Besonderheiten, die es hervorzuheben gilt. Im Folgenden geht es um letzteres.

Unter einem „endpoint“ wird meist ein Arbeitsplatzrechner (Desktop oder Notebook), ein Tablet oder Smartphone verstanden. Generell handelt es sich aber um einen *Host*.

Device management

Lösung, mit der die Softwareausstattung und die Konfiguration von Endgeräten entsprechend zentral definierter Vorgaben verwaltet wird. Mit Hilfe der Lösung wird Standardsoftware über die Netzwerkverbindung auf die Endgeräte verteilt und dort installiert. Das Gleiche gilt für Patches, für reguläre Aktualisierungen von Betriebssystemen, Treibern, Anwendungssoftware, von Sicherheitssoftware und von Konfigurationseinstellungen einschließlich von Sicherheitsrichtlinien. Die Nutzer der Endgeräte verfügen dabei meist nur über eingeschränkte

---

134 Tim Chien: Snapshots Are NOT Backups; Oracle, https://www.oracle.com/database/technologies/rman-fra-snapshot.html; zuletzt aufgerufen am 21.01.2021

Rechte (keine Administratorrechte), sodass sie diese Vorgänge entsprechend vorgegebener Regeln nicht oder nur bedingt beeinflussen können. Damit wird ein einheitlicher (Sicherheits-)Standard aller Endgeräte erreicht und die Nutzer werden entlastet. Die Lösung führt ein Inventar der installierten Software und ihrer Versionen.

Derart verwaltet (administriert) werden vor allem Arbeitsplatzrechner (Desktop oder Notebook), aber auch Tablets und Smartphones sowie virtuelle Geräte. Bei Smartphones und bestimmten Tablets spricht man auch von **Mobile Device Management (MDM)**.

Insbesondere für mobile Geräte (bzw. Geräte ohne Verschlüsselung aller Nutzerdaten) bietet die Lösung eine **Fernlöschung (Kill pill**), die bei Verlust des Gerätes ebenfalls aus der Ferne ausgelöst werden kann, da die Komponente auf dem Endgerät sich (Netzwerkverbindung vorausgesetzt) automatisch mit der zentralen Komponente verbindet, von dort die Aufforderung zum Löschen erhält und die Daten auf dem Gerät löscht.

Mobile Content Management (MCM)

Lösungen, die die sichere Nutzung von Unternehmens- oder geschäftlichen Daten auf mobilen Endgeräten ermöglichen. Das schließt den sicheren Zugang zu Daten ein, die auf zentralen Servern der Anwenderorganisation gespeichert sind, als auch die sichere Speicherung und Verwaltung der Daten auf dem Endgerät. Die Lösungen verschlüsseln die Übertragung von Daten. Die Dokumentenverwaltung reicht von einem globalen Zugangsschutz bis zum granularen Rechtemanagement und Funktionen, die Daten aktiv verteilen oder löschen.

Bei der dualen Nutzung mobiler Endgeräte für private und geschäftliche Zwecke werden die Daten in jeweils getrennten, verschlüsselten Datenbereichen verwaltet.

Mobile Application Management (MAM)

Eine unternehmens- bzw. organisationsspezifische Plattform für den Erwerb und die Verteilung von Anwendungssoftware und Softwarewerkzeugen, auch als „**Enterprise app store**“ bezeichnet. Dieser ersetzt die für Konsumenten über das Internet erreichbaren „App stores“ bei zentral verwalteten Endgeräten (→*Device management*) und enthält nur Software, die von der Anwenderorganisation (Unternehmen, Behörde o.ä.) freigegeben wurde.

Endpoint Protection, Detection and Response (EPDR)

Dem Schutz des Endgerätes (Endpoint Protection, vornehmlich Anti-Malware/Anti-Virus-Lösungen) werden die Funktionalitäten der Erkennung

(Detection) und der Reaktion (Response) hinzugefügt.[135] Die Erkennung betrifft das Verhalten von Malware nach der Infektion, bezieht sich aber auch auf die Integration einer Einbruchserkennung (Host Intrusion Detection, HIP). Der Begriff **Advanced Threat Protection (ATP)** steht hierbei für die Erkennung von Angriffen mit Kombinationen von Malware bzw. unterschiedlichen Angriffen, die mehrere Schwachstellen auszunutzen versuchen. Solche Angriffe werden auch **Blended attacks** (bzw. **Blended threats**) genannt. Die Komponente der Reaktion untersucht das Endgerät auf Schwachstellen (*Vulnerability scanner*) und ist in der Lage, diese durch Aktualisierungen zu beheben bzw. den Nutzer dabei zu unterstützen.

6.7 Infrastrukturdienste und -komponenten

Infrastrukturdienste

Hinweis: Das gesamte Kapitel 3 ist dem *Identitäts- und Zugriffsmanagement* (IAM, Identity and Access Management) gewidmet. IAM ist oft als Infrastrukturdienst implementiert. Siehe dort.

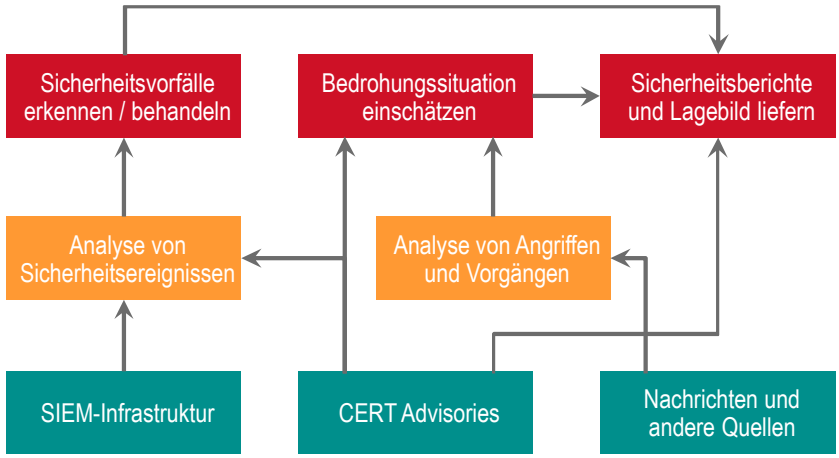


Abb. 49: Hauptaufgaben eines SOC und ihre Grundlagen

Security Operations Center (SOC)

Abteilung oder Organisation, die erstens (aus der Ferne) Applikationen, IT-Systeme und Netzwerke überwacht, um *Sicherheitsereignisse (security events)* zu finden, die ein Eingreifen erfordern, also *Sicherheitsvorfälle* darstellen. Zweitens werden laufend Informationen über vergangene und aktuelle Angriffe und andere Vorgänge gesammelt und ausgewertet, um die Bedrohungssituation

[135] Christopher Schuetze: The Evolution of Endpoint Security: Beyond Anti-Malware; KuppingerCole, Posted on Oct 29, 2020, https://www.kuppingercole.com/blog/schuetze/evolution-endpoint-protection-beyond-anti-malware; zuletzt aufgerufen am 21.01.2021

einschätzen zu können (**Threat intelligence**). Drittens werden *Sicherheitsberichte (Security reports)* erstellt. Vergleiche Abb. 49.

Ein SOC verwendet für die genaue Analyse viertens Informationen über *Schwachstellen (vulnerabilities)*, die in Form von *CERT-Meldungen* (*CERT advisories*) bezogen und/oder selbst zusammengestellt und bewertet werden.

Mitunter übernimmt ein SOC fünftens auch die Pflege („management") bestimmter Sicherheitslösungen (wie Firewalls oder IPS) im Tagesgeschäft. In Ausnahmefällen übernimmt das SOC sechstens auch die Beseitigung von Schwachstellen. Diese Aktivitäten müssen in die standardisierten Arbeitsabläufe des IT-Service-Managements (ITSM) eingebettet sein, sodass die Koordination mit anderen Änderungen sichergestellt ist.

Das SOC greift auf →*Security Information and Event Management (SIEM)* als Basisinfrastruktur zurück, nutzt also Mittel zur Protokollierung und Überwachung, die in die IT-Infrastruktur integriert sind. Ein SOC nutzt auch den Rat von Sicherheitsexperten, die Schwachstellenanalysen, Forensik, Bedrohungsanalysen, Penetrationstests und ähnliches durchführen. Das SOC arbeitet 7x24 und ist mit technischen Experten ausgestattet.

SOC-Leistungen werden in standardisierter Form, ähnlich einem Produkt, auch von Dienstleistern angeboten.

Security Information and Event Management (SIEM)

SIEM sammelt Logdaten (log data; siehe *Protokollierung*) und Alarme (siehe *Monitoring (Überwachung)*) von sehr unterschiedlichen Quellen, verarbeitet und verknüpft diese mit anderen Ereignisdaten und Informationen über die Umgebung und liefert schließlich a) Informationen bezüglich der Einhaltung von Regeln (compliance) und b) Informationen über mögliche *Sicherheitsvorfälle (security incidents)*.

Der erste Anwendungsfall (**Security Information Management (SIM)**) analysiert eher historische Daten, der zweite (**Security Event Management (SEM)**) arbeitet in Realzeit oder nahe „real-time".[136]

Zu den Quellsystemen gehören diverse Sicherheitsprodukte und Lösungen wie *Firewalls*, *Intrusion Detection/Prevention Systems (IDS/IPS)*, *Anti-Malware*-Lösungen, *Vulnerability scanner (Schwachstellen-Scanner)* sowie solche, die Nutzer und Geräte authentisieren (*Authentisierung*) und deren Zugriffe steuern (*Zugriffsmanagement*). Andere Datenlieferanten sind *Betriebssysteme*, *Datenbanken*, *Anwendungen* u.v.a.m.

---

[136] Der Begriff „Security Information and Event Management (SIEM)" wurde von Gartner geprägt und in die beiden Teildisziplinen SIM und SEM eingeteilt bzw. aus diesen zusammengesetzt.

Die Verarbeitung der Quelldaten erfolgt grob in folgenden Schritten: Normalisierung (normalization), Filtern, Korrelation (correlation) und Analyse (analysis). Für jeden Anwendungsfall (use case) werden einmalig Sätze von Regeln definiert, die das SIEM in die Lage versetzen, die gesuchten Ketten von Ereignissen in der konkreten IT-Umgebung aufzufinden und zu analysieren. Diese Regelsätze werden bei Änderungen der Einsatzumgebung oder der Anwendungsfälle aktualisiert und, wenn nötig, optimiert. SIEM-Lösungen verwenden Such- und andere Algorithmen sowie statistische Analysen und/oder Big-Data-Methoden.

SIEM-Lösungen liefern *Sicherheitsberichte (Security reports)* und verfügen über eine Übersichtsfunktion in Form eines Dashboards.

Infrastrukturkomponenten

Es gibt einige häufig wiederkehrende Komponenten, die keinem der bisherigen Kategorien zugeordnet werden können, also nicht in eines der obigen Kapitel 6.2-6.6 zu passen scheinen und/oder dort den Rahmen gesprengt hätten. Diese Komponenten und einige mit ihnen im Zusammenhang stehende Begriffe werden im Folgenden erläutert.

Sicherheitsmodul (security module)

Im Allgemeinen versteht man unter einem Sicherheitsmodul eine Funktionseinheit, die geeignet gekapselt, also von ihrer Umgebung in klarer Weise abgetrennt ist. Sicherheitsmodule führen kryptografische Operationen und andere Sicherheitsfunktionen aus und speichern kryptografische Schlüssel und andere sicherheitsrelevante Daten so, dass diese vor unbefugter Verwendung und Manipulation geschützt sind. Die Funktionen werden über eine Programmierschnittstelle (API) zur Verfügung gestellt, die typischerweise vor unberechtigter Nutzung geschützt ist.

Sicherheitsmodule sind die Basis für die Anwendung von Kryptografie in IT-Systemen und IT-Anwendungen. FIPS PUB 140[137] und ISO/IEC 19790[138] verwenden die Bezeichnung **Cryptographic Module**.

Meist wird von einem Sicherheitsmodul erwartet, dass es über Mechanismen verfügt, die einen gewissen Schutz vor Angriffen auf seine Struktur und Funktion sowie auf gespeicherte Daten bieten. Einen solchen Schutz gegen *Tampering* bieten *Hardware-Sicherheitsmodule (HSM)* immer. Sicherheitsmodule, die nur in Software ausgeführt sind, benötigen diesbezüglich Unterstützung durch ihre Einsatzumgebung.

---

[137] National Institute of Standards and Technology (NIST): Security Requirements for Cryptographic Modules, FIPS 140-3; March 22, 2019

[138] ISO/IEC 19790 – Information technology — Security techniques — Security requirements for cryptographic modules

Hardware-Sicherheitsmodul (HSM) (Hardware Security Module)

Ein Hardware-Sicherheitsmodul oder kurz HSM ist ein physisch gekapseltes *Sicherheitsmodul*, das Schutz gegen Angriffe (siehe *Tampering*) auf seine Struktur und Funktion sowie auf gespeicherte Daten bietet. HSMs gibt es in sehr verschiedenen Bauformen, die von einer *Appliance* bis zu verschiedensten Typen von *Embedded Systems* reichen, also zum Beispiel von einem kompakten IT-System oder Gerät in Form einer Fertiglösung bis zu einer Single-Chip-Lösung, die in Form einer Scheck- oder SIM-Karte ausgeliefert wird.

Tampering

Tampering ist ein Sammelbegriff für feindliche Handlungen, die das Ziel verfolgen, Veränderungen an IT-Systemen und Komponenten vorzunehmen oder hervorzurufen, die deren Funktionsweise beeinflussen oder es erlauben, Daten zu manipulieren oder auszulesen. Meist bezieht sich der Begriff auf *Sicherheitsmodule* bzw. *Hardware-Sicherheitsmodule (HSMs)*, da vornehmlich physische bzw. physikalische und chemische Wirkungsmechanismen betrachtet werden.

Tampering bedeutet etwa „sich an etwas zu schaffen machen oder etwas verfälschen". Der Schutz dagegen wird wie folgt klassifiziert:[139] **Tamper resistance** (Manipulationsschutz) bewirken Mechanismen, die einem Angriffsversuch Widerstand entgegensetzen, ihn damit erschweren oder unmöglich machen sollen. **Tamper evidence** (Manipulationserkennung) ist gegeben, wenn ein für den Nutzer außen sichtbares bzw. erkennbares Zeichen die Manipulation bzw. den Manipulationsversuch verrät. **Tamper detection** bezeichnet die automatische Erkennung eines Angriffsversuchs. Im Falle von **Tamper response** werden automatisch Gegenmaßnahmen eingeleitet, wenn ein Angriffsversuch (automatisch) erkannt wurde.

Der Begriff **physical protection** (physischer Schutz) ist unspezifisch und kann verschiedene Formen des Schutzes gegen physische bzw. physikalische und chemische Manipulationen umfassen.

Eine besondere Form solcher Manipulationen nutzt aus, dass das Sicherheitsmodul bzw. seine sicherheitsrelevanten Funktionen unter bestimmten physikalischen Einsatz- bzw. Betriebsbedingungen (zum Beispiel Temperatur, Bestrahlung oder Spannungsversorgung) eventuell nicht mehr ordnungsgemäß funktioniert bzw. funktionieren. Unter **Environmental failure protection (EFP)** versteht man die Eigenschaft des Sicherheitsmoduls gegen solche Änderungen unempfindlich zu sein. **Environmental failure testing (EFT)** überprüft, dass mögliche Manipulationen der Einsatz- bzw. Betriebsbedingungen nicht zur Kompromittierung der Sicherheit führen.

---

[139] National Institute of Standards and Technology (NIST): Security Requirements for Cryptographic Modules, FIPS 140-3; March 22, 2019

Embedded System (eingebettetes System)

Ein eingebettetes System hat vier Eigenschaften:[140]
a) Es handelt sich um ein Computersystem oder das System beinhaltet ein solches.
b) Es ist für einen bestimmten Zweck bzw. eine bestimmte Anwendung konstruiert – also nicht beliebig oder frei programmierbar und nicht oder nur beschränkt neu programmierbar.
c) Es ist in besonderem Maße konstruktiven Beschränkungen unterworfen aufgrund von Kostendruck (weil es sich zum Beispiel um ein Massenprodukt handelt), aufgrund beschränkter Größe (weil es sich bei der Bauform zum Beispiel um ein Single-chip-, Multi-chip- oder Kleinstgerät handelt) oder aufgrund der vorhandenen Leistungsfähigkeit, des maximal möglichen Stromverbrauchs usw.
d) Es reagiert auf Umgebungsveränderungen und das meist mit Echtzeitanforderungen.

Viele Gegenstände des täglichen Lebens sind eingebettete Systeme oder enthalten diese. Beispiele sind Kameras, Navigationssysteme, medizinische Geräte, Chipkarten und Chipkartenterminals. Eingebettete Systeme sind typische Bestandteile vom Internet-der-Dinge (IoT).

Chipkarte

Eine meist kreditkartengroße Plastikkarte, in die ein Chip (Integrierter Schaltkreis) eingebettet ist, dessen Funktionalität von einem einfachen, nichtflüchtigen Datenspeicher mit Ausleselogik über einen Datenspeicher mit zusätzlicher Sicherheitslogik bis zu einem vollständigen Mikrocomputer mit Sicherheitsmechanismen reichen kann. Chipkarten der letztgenannten Ausbaustufe werden als Prozessorchipkarten (**Smartcards**) bezeichnet und oft als *Sicherheitsmodule* verwendet. Dabei kommen sie zum Beispiel als Debit- oder Kreditkarte im Zahlungsverkehr oder als Authentisierungsmedium in der IT und im Mobilfunk zum Einsatz.

Chipkarten können unterschiedliche Formate haben, die von der Kreditkartengröße (85 mm x 54 mm) über die SIM-Kartengröße (25 mm x 15 mm) bis zu Micro- und Nanoformaten reicht. Die Kommunikation zwischen der Chipkarte und der Gegenstelle (**Terminal**) kann kontaktbehaftet oder kontaktlos sein. Bei der kontaktlosen Kommunikation befindet sich im Kartenkörper aus Plastik eine Antenne, die zur Stromversorgung und zur Datenübertragung dient.

Chipkarten sind *Embedded Systems* (eingebettete Systeme).

---

[140] Frank Vahid and Tony Givargis: Embedded Systems, A unified Hardware/Software Introduction; John Wiley & Sons, Inc., 2002

TPM (Trusted Platform Module)

Ein TPM ist ein *Hardware-Sicherheitsmodul (HSM)*, das in Computer verschiedenster Bauformen eingebaut wird und zusammen mit spezieller Software eine **Trusted Computing Platform (TCP)** bildet, die auf dem Computer kryptografische Operationen sowie sicheren Speicher zur Verfügung stellt. Die Elektronik des TPMs ist in einem Chip (Integriertem Schaltkreis) untergebracht.

Anwendungen sind zum Beispiel die Überwachung des Computer-Starts (Überprüfung der Systemintegrität beim Booten), Computer-Identifikation, Einsatz als Prozessorchipkarten (*Smartcard*, die hier aber an den Computer gebunden ist), Verschlüsselung und Entschlüsselung von Daten, Erzeugen und Prüfen von Signaturen.

Literatur und Bildnachweise

Besonders ein solches Buch, das sich zur Aufgabe macht, Definitionen von Fachbegriffen zu geben, kann nicht geschrieben werden, ohne dass der Autor vielfältige Literatur gelesen hätte – in der langen Zeit der Tätigkeit auf diesem Gebiet, bei der Erstellung von Lehrunterlagen für Studierende und beim Schreiben dieses Buches. Die Definitionen sollen ja den Stand der Technik korrekt wiedergeben und konsensfähig sein. Das bedeutet auch, dass Begriffe und Zusammenhänge auch in anderen Veröffentlichungen so oder ähnlich vorkommen können – ja müssen.

Daher wurde wie folgt verfahren: (1) Literatur ist an den Stellen als Fußnote angegeben, wo ich sie direkt verwendet habe bzw. mir bewusst ist, dass Begriff, Definition oder sonstige Beschreibungen auf eine solche Quelle zurückgeführt werden können. (2) Gilt dies in gleicher Weise für Institutionen oder Einzelpersonen, so sind diese meist direkt im Text angegeben. (3) Die folgende Liste enthält Literaturhinweise und wiederholt nicht die Quellenangaben in diesem Kapitel. (4) Falls nicht anders angegeben, wurden Abbildungen extra für dieses Buch erstellt.

[1] Information Security Taxonomy Handbook; National Institute for Communications Technologies, INTECO, León (Spain), 2010

[2] ISO/IEC 15408 – Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components; July 2008; and: Common Criteria for Information Technology, Security Evaluation, Part 2: Security functional components; April 2017, Version 3.1, Revision 5, https://commoncriteriaportal.org

[3] NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations; April 2013 (updated 2015), Rev. 4

[4] Gartner: Gartner Glossary, Information Technology; https://www.gartner.com/en/information-technology/glossary

[5] National Institute of Standards and Technology (NIST): Security Requirements for Cryptographic Modules, FIPS 140-3; March 22, 2019

[6] National Institute of Standards and Technology (NIST): Glossary; https://csrc.nist.gov/glossary

[7] Celia Paulsen and Robert Byers: Glossary of Key Information Security Terms, NISTIR 7298; National Institute of Standards and Technology (NIST); Rev. 3, July 2019, https://csrc.nist.gov/glossary

Elektronisches Zusatzmaterial
Die Abbildungen sind als PowerPoint-Datei kapitelweise über https://link.springer.com/ auf der Seite des eBooks abrufbar.

7 Kunden, Verträge und Geschäfte

Auch ein IT-Dienstleister ist ein Hersteller und in vielen Fällen ein eigenständiges Unternehmen. Beides führt dazu, dass allgemeine betriebswirtschaftliche Regeln und Prozesse zur Anwendung kommen. Das Gleiche gilt für Anwenderorganisationen, die IT-Services einkaufen. In diesem Kapitel werden einige Themen wie das Vertragswesen und die unternehmerische Organisation behandelt, weil diese Themen als wichtiges Hintergrundwissen angesehen werden und in der gewählten Breite und Tiefe auch für IT- und IT-Sicherheitsmanager von Belang sind. Häufig sind technische Entscheidungen schließlich mit betriebswirtschaftlichen Rahmenbedingungen verknüpft. Dazu kommt, dass IT-Services für Anwenderunternehmen bereitgestellt und abgesichert werden, die Kunden der IT- und IT-Sicherheitsexperten darstellen.

Der Autor dieses Buches ist kein Betriebswirtschaftler. Die Erklärungen folgen den beruflichen Erfahrungen und betonen Aspekte, die im Kontext dieses Buches für wichtig erachtet werden. Der Umfang dieses Kapitels ist eher darauf ausgerichtet, eine minimale Grundausstattung zu liefern, statt die einzelnen Themen umfassend zu würdigen.

Im Kapitel 7.1 geht es im weitesten Sinne um das Vertragswesen, also um verschiedenste Formen von Übereinkünften, die Anbieter und ihre Kunden treffen. Zu den Verträgen gehören auch Vertragsbedingungen. Auch wird kurz beleuchtet, wie IT-Dienstleister bestimmte Vorteile erwirtschaften. Kapitel 7.2 fasst wichtige betriebswirtschaftliche Begriffe zusammen. In Kapitel 7.3 erfolgt dies für das Thema IT-Outsourcing. In Kapitel 7.4 werden einige Begriffe aus dem Bereich Unternehmensstrategie definiert, die von Formen von Zieldefinitionen bis zu Methoden für Bewertungen reichen.

7.1 Übereinkünfte, Verträge und Vertragsbedingungen

In diesem Kapitel werden einige wichtige Begriffe erklärt, die mit Übereinkünften und Verträgen im Zusammenhang stehen. Siehe Abb. 50. Die Begriffe in der oberen Hälfte werden in Kapitel 7.1.1, die gelb hinterlegten Begriffe der unteren Hälfte in Kapitel 7.1.2 erläutert.

Zusatzmaterial online
Zusätzliche Informationen sind in der Online-Version dieses Kapitel (https://doi.org/10.1007/978-3-658-33431-4_7) enthalten.

E. von Faber, *IT und IT-Sicherheit in Begriffen und Zusammenhängen*,
Edition <kes>, https://doi.org/10.1007/978-3-658-33431-4_7

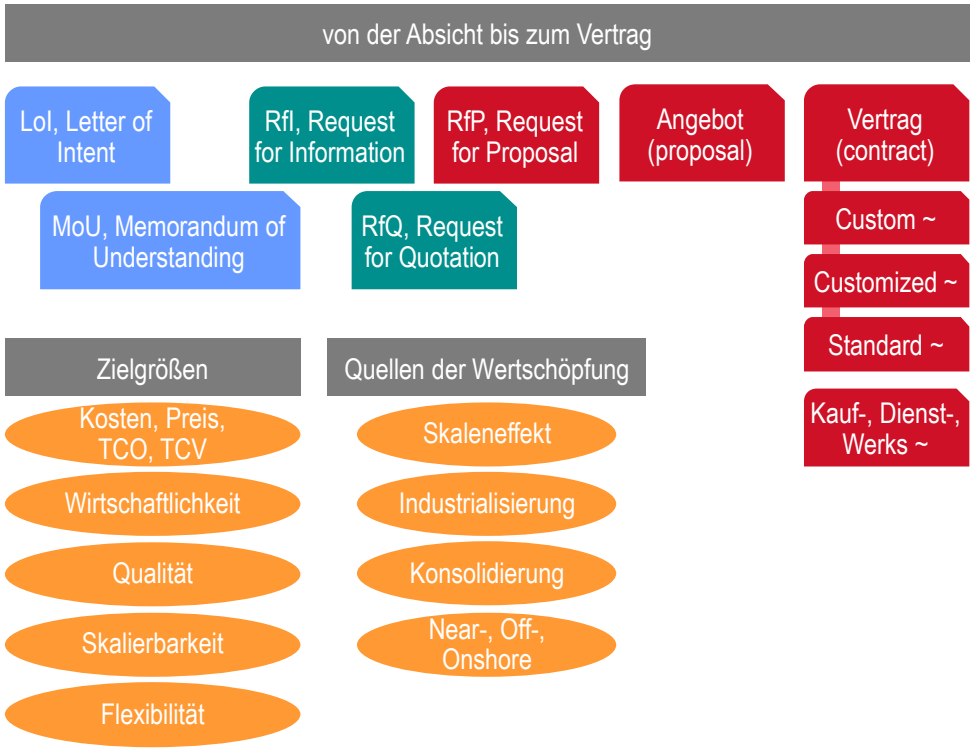


Abb. 50: Einige Begriffe zu Übereinkünften zwischen Käufer und Anbieter

7.1.1 Geschäftsanbahnung und Vertragsabschluss

LoI, Letter of Intent

Unverbindliche Absichtserklärung zweier Parteien. Sie dient der Abstimmung gemeinsamer Ziele und der Vorbereitung bzw. Planung gemeinsamer Aktivitäten meist in Form von Projekten. Oft bildet sie die Grundlage für spätere Verträge. LoI wird oft synonym zum *MoU (Memorandum of Understanding)* verwendet. Beide können Passagen enthalten, die rechtlich bindend sind, wie zum Beispiel Vertraulichkeitserklärungen.

MoU, Memorandum of Understanding

Offizielle Absichtserklärung zweier oder mehrerer Parteien. Sie ist (wie ein *LoI, Letter of Intent*) rechtlich nicht bindend. Oft wird auch hier ein Vertragsabschluss vorbereitet und angestrebt bzw. das MoU ersetzt einen formalen Vertrag, weil die Parteien sich nicht rechtlich binden wollen oder können. Letztlich entscheidet jedoch der Text selbst über den Charakter eines MoU. MoU wird oft synonym zum LoI verwendet. Beide können Passagen enthalten, die rechtlich bindend sind, wie zum Beispiel Vertraulichkeitserklärungen.

RfI, Request for Information

Aufforderung an Anbieter, Informationen bereitzustellen, anhand derer der Kreis der Anbieter auf diejenigen eingeschränkt wird, die eine Aufforderung erhalten, ein Angebot abzugeben (*RfP, Request for Proposal)*. Ein RfI kann aber auch einfach der Marktsondierung dienen, oder es werden geschäftliche Möglichkeiten getestet, oder es wird Material für die Strategiebildung oder für geschäftliche Entscheidungen gesammelt. Eine ähnliche Funktion hat ein **Request for Qualification (RfQ)**; diese Aufforderung konzentriert sich aber vor allem auf den Anbieter und seine Fähigkeiten, Qualitäten usw.

RfP, Request for Proposal

Ausschreibung bzw. Aufforderung, ein *Angebot (proposal)* abzugeben. Sie enthält Informationen zum Ablauf, beschreibt die aktuelle Situation und den Bedarf und definiert die geforderte Leistung sowie Anforderungen an den Anbieter und die Leistungserbringung.[141] Die Beschreibung der geforderten Leistung wird, insbesondere bei Auftragsarbeiten, auch als **Pflichtenheft** oder **Lastenheft** bezeichnet.

Anbieter, die ein RfP erhalten, befinden sich auf der sogenannten Long-List. Die eingereichten Angebote (proposals) werden nach vordefinierten Kriterien bewertet. Nur einige der Anbieter werden weiter berücksichtigt, so dass sich die Liste der möglichen Anbieter verkürzt (Short-List). Mit letzteren wird weiter verhandelt, um zum Beispiel weitere Details zu klären. Die Phase heißt (beim IT-*Outsourcing*) **Due Diligence**. Während der Due Diligence erhalten die Parteien die Möglichkeit, erhaltene Informationen zum Beispiel durch Begehungen und Befragungen zu erweitern. Die verbliebenen Anbieter erhalten auch weitere Informationen sowie oft auch die Gelegenheit, ihr Angebot zu schärfen und ein finales und endgültig bindendes Angebot abzugeben, das **Best and Final Offer (BAFO)** genannt wird.

Ausschreibungen der öffentlichen Hand unterliegen besonderen Regelungen.

RfQ, Request for Quotation

Preisanfrage, die an mögliche Anbieter versendet wird, wenn Leistung und Liefergegenstand bereits klar definiert und abgegrenzt sind und insbesondere der Preis der primär entscheidende Faktor bei der Vergabe eines Auftrages ist. Die Preisangabe ist in der Regel nicht verbindlich. Ein RfQ wird eventuell auch versendet, um allgemeine Preisinformationen zu erhalten, bevor eine Ausschreibung (*RfP, Request for Proposal)* gestartet wird.

---

[141] Torsten Gründer: OMIT – IT-Outsourcing mit Methode planen, umsetzen und steuern; in: Torsten Gründer (Hrsg.): IT-Outsourcing in der Praxis, Strategien, Projektmanagement, Wirtschaftlichkeit; Erich Schmidt Verlag, Berlin, 2011, 2. Auflage, ISBN 978-3-503-09015-0, 479 Seiten

Angebot (proposal)

Aufgrund einer formalen Ausschreibung (*RfP, Request for Proposal*) oder einer einfachen Anfrage bereitgestellte Beschreibung einer Lieferung oder Leistung einschließlich aller Bedingungen für die Lieferung bzw. die Erbringung der Leistung. Angebote, die auf Ausschreibungen reagieren, müssen sich in Inhalt und Form meist sehr genau an den Ausschreibungstext und die Ausschreibungsbedingungen halten. Hier spricht man auch von Bieten (bidding, bid). Andere Angebote erstellt der Anbieter nach seinen eigenen Standards.

Vertrag (contract)

Dokumentiert eine Übereinkunft zwischen Käufer und Anbieter. Insbesondere wird der Liefer- bzw. Leistungsgegenstand definiert, was überwiegend Anforderungen an den Anbieter stellt. Bei Dienstleistungen werden Mitwirkungspflichten für den Käufer definiert, die notwendig sind, damit der Anbieter die Leistung im geforderten Umfang und in der geforderten Qualität erbringen kann. Weitere Inhalte eines solchen Vertrags sind das Vergütungsmodell, die Vertragslaufzeit oder -dauer, Bedingungen für eine vorzeitige Vertragsbeendigung, die Möglichkeiten einer Vertragsverlängerung sowie Vertraulichkeitsklauseln.

Der für einen Kunden individuell ausgefertigte Vertrag bzw. ein für einen Kunden maßgeschneiderter IT-Service heißt **Custom (IT-Service)**. Ein für den Kunden angepasster Vertrag oder IT-Service heißt **Customized (IT-Service)**. Das schließt die Wiederverwendung von IT-Komponenten bzw. Textbausteinen bei Verträgen nicht aus. Einzelne Service-Leistungen bzw. deren Beschreibungen sind oft Kopien aus IT-Service-Katalogen (*Service Catalogues)* oder daraus abgeleiteten Dokumenten. Maßgeschneiderte und angepasste IT-Services werden oft als *Dedizierte Systeme* (dedicated systems) aufgebaut; aber nicht jedes dedizierte System liefert einen kundenspezifischen IT-Service.

Um die Vertragserstellung und -erfüllung weiter zu vereinfachen, werden neben individuellen Vertragsabreden auch Allgemeine Geschäftsbedingungen (AGB) (engl.: General Terms and Conditions) verwendet, die einer der beiden Vertragspartner stellt.

Bei der Bereitstellung von IT-Services sind weitere Begriffe üblich, die unter →*Service Level Management (SLM)* beschrieben werden.

Grundsätzlich gibt es Kaufverträge (Überlassung bzw. Übergabe eines *Produktes*) und Verträge über *Dienstleistungen*. Letztere existieren in Form von Dienstverträgen und Werkverträgen. Ein **Dienstvertrag** verpflichtet den Anbieter zu einer definierten Leistung; er ist tätigkeitsbezogen. Ein **Werkvertrag** verpflichtet zur Herstellung eines Guts; er ist erfolgsbezogen. Die Unterscheidung spielt bei *Professional Services* eine wichtige Rolle.

7.1.2 Vertragsbedingungen und Vertragserfüllung

In diesem Kapitel werden die gelb hinterlegten Begriffe in der unteren Hälfte der Abb. 50 erläutert. Bei den Erklärungen werden, wie stets, weitere Begriffe eingeführt.

Zielgrößen

Kosten

Im Sinne der Buchführung sind Kosten die finanziellen Ausgaben des Käufers. Im Hinblick auf die IT ist die Unterscheidung zwischen fixen und variablen Kosten wichtig.

Fixe Kosten bzw. sprungfixe Kosten verändern sich nicht, wenn nur der betrachtete Zeitraum variiert wird. Die entsprechenden Ausgaben entstehen bei der Anschaffung eines Guts (Produkts), das damit (als Anlagevermögen) in Besitz und Eigentum des Käufers übergeht. Man spricht von Investitionsausgaben, englisch **CAPEX** (Capital Expenses).

Variable Kosten ändern sich, wenn der Betrachtungszeitraum verändert wird. Wird eine Dienstleistung über einen längeren Zeitraum eingekauft und genutzt, so sind regelmäßige (zum Beispiel jährliche) Zahlungen zu leisten. Der Käufer erwirbt kein Eigentum und vergrößert sein Anlagevermögen nicht. Man spricht von Betriebskosten oder auch laufenden Kosten, englisch **OPEX** (Operational Expenses).

Will eine Organisation IT-Services selbst produzieren, so muss sie die dazu benötigten IT-Komponenten in der Regel anschaffen (CAPEX). Bilanztechnisch anders verhält es sich, wenn die Organisation die IT-Services von einem IT-Dienstleister einkauft und zum Beispiel eine jährliche Bezahlung vereinbart wird (OPEX). Ein weiterer Vorteil für den Käufer entsteht dadurch, dass er vertragsgemäß kündigen kann, wodurch die Kosten sofort verschwinden, während bei einer Anschaffung die Wertminderung erst nach dem Ende des Abschreibungszeitraums nicht mehr zu Buche schlägt.

Die Vergütung bzw. Bezahlung kann nach unterschiedlichen Modellen erfolgen: Bei einem **Festpreis (firm fixed-price)** oder **Pauschalpreis (lump sum)** schätzt der Anbieter die Kosten und errechnet daraus den Gesamtpreis, der zu zahlen ist, unabhängig davon, welche Kosten dem Anbieter bei der Leistungserbringung wirklich entstehen. Werden Kosten nach Aufwand verrechnet (**Time and Materials, T&M**), so sind alle anfallenden, nachgewiesenen Kosten zu vergüten. Von solchen **Preismodellen** unabhängig zu sehen sind die **Zahlungsmodalitäten**, die in einem Vertrag regeln, wann und unter welchen Bedingungen welche Vergütungen zu erfolgen haben.

Total Cost of Ownership (TCO)

Konzept für einen Gesamtkostenansatz, bei dem alle Aufwände und Ausgaben entlang des gesamten Lebenszyklus und auch indirekte Kosten berücksichtigt werden. Insbesondere werden neben den Anschaffungskosten auch die Kosten für die Einführung (einschließlich Schulungen), für den Betrieb, den Erhalt und die Ausmusterung berücksichtigt.

Total Contract Volume (TCV)

Einnahmen eines Dienstleisters, die über die gesamte Laufzeit des Vertrages berechnet wurden und insgesamt als Einnahmen erzielt werden, wenn der Vertrag bis zum Ende der Vertragslaufzeit bestehen bleibt.

Wirtschaftlichkeit

Ergebnis des Handelns, bei dem der Effekt, Nutzen, Erfolg oder Gewinn den Aufwand oder Mitteleinsatz übersteigt oder ein vorgegebenes Ziel mit einem vergleichsweise geringeren Aufwand oder Einsatz von Mitteln erreicht wird.

Qualität (IT)

Gesamtheit von inhärenten, sekundären bzw. nicht-funktionalen Eigenschaften, die dazu führen, dass ein IT-Service, ein Produkt oder eine Dienstleistung den Erwartungen oder Anforderungen des Anwenders entspricht oder diese übertrifft. Demgegenüber sind primäre, funktionale Eigenschaften solche, die erforderlich sind, damit der IT-Service, das Produkt oder die Dienstleistung seinen bzw. ihren Zweck erfüllt. Qualität differenziert mehrere Angebote, die sich hinsichtlich ihrer Zweckdienlichkeit nicht unterscheiden oder unterscheiden würden.

Skalierbarkeit

Skalierbarkeit ist eine Eigenschaft von Systemen (wie Produktionsanlagen und IT), bei wachsenden Aufgaben und Leistungsanforderungen so erweitert werden zu können, dass die Aufgaben erfüllt und die Leistungen erbracht werden können. Das System kann also mitwachsen und stößt nicht frühzeitig an Grenzen. Skalierbarkeit und *Skaleneffekt* beziehen sich auf zwei unterschiedliche Sachverhalte. Während es bei der Skalierbarkeit um die Möglichkeit einer Erweiterung geht, bezieht sich der Begriff Skaleneffekt auf die Entwicklung des damit verbundenen Aufwands.

Skalierbarkeit von Softwareanwendungen basiert auf Lastverteilung und erfordert, dass eine Aufgabe in Teilaufgaben zerlegt werden kann, die ganz oder teilweise simultan durchgeführt werden können.

Flexibilität

Möglichkeit bzw. Fähigkeit, sich veränderten Rahmenbedingungen anzupassen. Aus Sicht einer *Anwenderorganisation* setzt dies voraus, dass der *IT-Dienstleister* dazu technisch und organisatorisch in der Lage ist und dass die

Vertragsbedingungen dies ermöglichen. *Verträge (contracts)* für die langjährige Erbringung umfangreicher IT-Services enthalten deshalb oft Klauseln, die eine Vertragsänderung bzw. -erweiterung (zum Beispiel für die Modernisierung oder den Ausbau der IT) explizit und gegen zusätzliche Vergütung vorsehen. Damit bekundet der Anbieter nicht nur seine Bereitschaft, sondern geht auch Verpflichtungen ein, dies im Rahmen seines Geschäftsmodells auch umsetzen zu können.

Ein insbesondere im Zusammenhang mit Cloud-Computing oft diskutiertes Problem ist der sogenannte **Vendor lock-in**. Dies bedeutet, dass die Anwenderorganisation den Anbieter nicht oder nur unter hohem Aufwand wechseln kann, zum Beispiel, weil Inkompatibilitäten auftreten würden oder keine geeignete Schnittstelle zur Verfügung steht, um Daten beim aktuellen IT-Dienstleister exportieren zu können.

Quellen der Wertschöpfung

Skaleneffekt (Economies of scale)

Bezeichnet die Eigenschaft, dass die benötigten Ressourcen (Aufwand) langsamer wachsen als die erbrachten Leistungen (Nutzen), wenn letztere ausgedehnt werden. Das führt dazu, dass die spezifischen Kosten pro Leistung sinken, wenn mehr Leistungen erbracht werden. Dieser Kostenvorteil bildet eine wichtige Geschäftsgrundlage für IT-Dienstleister. Andere Vorteile im Vergleich zur Eigenherstellung sind höhere *Flexibilität* und das Vorhandensein benötigter *Fähigkeiten* (Kompetenzen) sowie, damit verbunden, ausreichende Kapazitäten und *Qualität*.

Industrialisierung

Produktionsweise, die durch a) Standardisierung (Verringerung der Varianten bzw. Vorab-Festlegung und Modularisierung), b) Wiederverwendung (Serienfertigung mit gleichen Elementen und nach gleichen Verfahren) und c) Automatisierung (Reduktion menschlicher Eingriffe) gekennzeichnet ist.

Mit dem Aufkommen der Vorläufer des Cloud-Computings (etwa ab 2005) hielt die Industrialisierung auch in der Informationstechnologie Einzug. Bereits vorher erfolgte mit ITIL[142] (in den 1990er Jahren) und ISO/IEC 20000 (2005) eine Standardisierung der Prozesse des *IT-Service-Managements (ITSM)*, die eine wesentliche Grundlage der industrialisierten IT-Produktion darstellen.

---

142 IT Infrastructure Library®, eine Sammlung von vordefinierten Prozessen, Aktivitäten und Rollen entlang des Lebenszyklus von IT-Services, wobei die Betriebsphase besonders beachtet wird. Seit 2013 sind ITIL und IT Infrastructure Library eine Marke von Axelos.

Konsolidierung

Zusammenlegen von Vorgängen oder Reduktion von Varianten (zum Beispiel von IT-Komponenten) mit dem Ziel, Kosten zu sparen und/oder die Qualität zu erhöhen. Oft werden dabei Systeme oder Komponenten durch fortschrittlichere, leistungsfähigere ersetzt.

Nearshore, **Offshore**, **Onshore**

Kennzeichnet die geografische Lage des *IT-Dienstleisters* relativ zu der der *Anwenderorganisation* (Auftraggeber). Beim Nearshoring wird die Leistung in einem Nachbarland bereitgestellt, beim Offshoring in weiter entfernten Ländern. Onshoring bezeichnet entsprechend den Bezug von Leistungen aus dem eigenen Land. Die geografische Lage beeinflusst (vor allem aus Sicht der entwickelten Industriestaaten) die Kosten, spielt aber häufig auch hinsichtlich verfügbarer Kapazitäten und der Einhaltung von Gesetzen und Regularien eine wichtige Rolle.

7.2 Etwas Betriebswirtschaft

Erst in den 1930er Jahren entwickelten Nordsieck und Henning das Konzept einer prozessorientierten Organisation. Genauer gesagt sollte die produktbezogene Organisation (Aufbauorganisation) durch eine weitere Organisation (Ablauforganisation) ergänzt werden, die sich an der zeitlichen Abfolge von Arbeitsleistungen orientiert, die wir heute als Geschäftsprozesse kennen. Siehe Abb. 51.

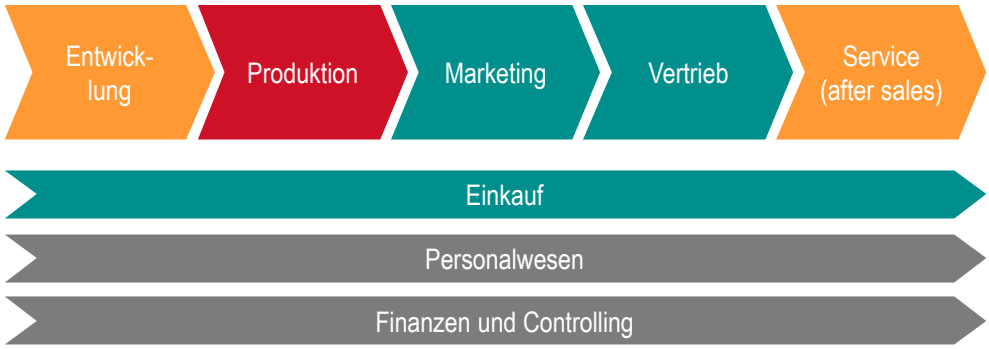


Abb. 51: Typischer Aufbau einer Unternehmung

Doch noch lange hat sich eine vertikale, produktorientierte Organisation gehalten. In diesen „Silos“ (wegen der vertikalen Lage) wurde ein Produkt über seinen gesamten Lebenszyklus betreut. Hier liefen die Fäden zusammen, hier war das für Werbung, Vertrieb und Herstellung notwendige Know-how konzentriert. Dies hat sich in der IT aufgrund der teilweise komplizierten und in schnellem Wandel begriffenen Technologie teilweise gehalten.

Die Organisation von Entwicklung, Produktion und Service (vergleiche Abb. 51) wurde schon in Kapitel 5 anhand der *IT-Service-Management*-Prozesse *(ITSM)* sehr

ausführlich diskutiert. Andere Bereiche wie Marketing und Vertrieb gibt es aber auch in einem IT-Unternehmen. In großen Firmen sind derartige Bereiche meist zentralisiert. Worauf es hier aber ankommt ist, dass es zwischen diesen Bereichen und der Bereitstellung und Absicherung der IT-Services sehr große Wechselbeziehungen und Abhängigkeiten gibt. Deshalb ist ein Basiswissen über diese überwiegend nicht-technischen Bereiche auch für Techniker unabdingbar. Das Gleiche gilt für betriebswirtschaftliche Kenngrößen, die Verhalten und Entscheidungen beeinflussen und steuern. Sie werden anschließend erläutert.

7.2.1 Prozesse

Marketing

Ausrichtung an Bedingungen, Anforderungen und dergleichen, die ihren Ursprung im Marktgeschehen haben. Beispiele sind Kundenwünsche und -anforderungen, aber auch Preise, Leistungen und Qualitäten der Mitbewerber. Marketing passt Produkte, Leistungen sowie Prozesse, die deren Herstellung und Verkauf beeinflussen, an. Das Marketing verfolgt das Ziel, Produkte und Leistungen erfolgreich zu verkaufen. Das bekannteste Beispiel ist die Werbung, die die Präsentation von Produkten und Leistungen so gestaltet, dass diese auf dem Markt bestmöglich verkauft werden können.

Vertrieb (sales)

Vertrieb (als Organisation) ist diejenige Einheit in einem Unternehmen, die konkrete, potenzielle Kunden bis zum Abschluss eines Vertrages führt. Oft hat der Vertrieb auch die Aufgabe, Bestandskunden zu Vertragsverlängerungen und weiteren Abschlüssen zu bewegen.

Vertrieb (als Prozess) führt von der Möglichkeit, einem konkreten Kunden ein Produkt oder eine Leistung zu verkaufen (opportunity), bis zum Abschluss des Vertrages. Für jeden Schritt werden Vorgehen, Verantwortlichkeiten, Werkzeuge und Regeln definiert.

Häufig wird die Ausfertigung komplexer *Verträge (contracts)* und Verhandlungen darüber von einer anderen Einheit des Unternehmens wahrgenommen (deal management, contracting).

Customer Relationship Management (CRM)

Gesamtheit aller Verfahren für die Interaktion mit potentiellen Kunden und Bestandskunden. Dies beginnt mit der Verwaltung von Informationen über Kunden und reicht von der Einschätzung von Entwicklungen und möglichem Kundenverhalten bis zur Gewinnung von Vorhersagen zum Beispiel über die Wahrscheinlichkeit eines Abschlusses und den erwarteten *Auftragseingang (order entry)*. Damit dient CRM auch der bedarfsgerechten Anpassung von Ressourcen in *Vertrieb* und Produktion.

Order to Cash (process)

Prozess der Abwicklung einer Bestellung bis zum Zahlungseingang. Dabei werden die Bestellung bzw. der Auftrag angelegt, notwendige Ressourcen und Komponenten ermittelt, die Auftragsbestätigung und die Rechnungen verschickt sowie der Zahlungseingang kontrolliert. Die Bestimmung der notwendigen Ressourcen und Komponenten steht in engem Zusammenhang mit den IT-Service-Katalogen (*Service Catalogues)*, auf denen der Vertrag in der Regel basiert.

Order Management (process)

Prozess der internen Beauftragung der Produktion, was die Identifikation und Bereitstellung aller notwendigen Ressourcen umfasst und externe Beschaffungsvorgänge erforderlich machen kann. Der Prozess wird in der Regel durch den Abschluss eines Vertrages mit einem Kunden angestoßen bzw. steht damit in Verbindung. Er löst ganz unterschiedliche Aktivitäten aus, die für die Bereitstellung der Leistung gemäß Vertrag nötig sind. Bei einem IT-Dienstleister können dazu die Beschaffung von IT-Komponenten zur Ausweitung von Kapazitäten gehören sowie Projekte zur Datenübernahme oder die Einrichtung von IT-Systemen. Die notwendigen IT-Komponenten werden aus der Bestellung und den Stücklisten ermittelt, die den IT-Service-Katalogen (*Service Catalogues)* zugrunde liegen.

Einkauf (procurement)

Organisation und Prozess, der für die Beschaffung von Produkten und Leistungen nach einheitlichen Richtlinien sorgt. Bei größeren Unternehmen werden meist nur vorqualifizierte Lieferanten berücksichtigt und angefragt. Auch werden meist nur bestimmte Produkte zugelassen, was die Heterogenität der Ausstattung reduziert und Betriebs- und Servicekosten senkt. Die Bündelung der Beschaffung reduziert den Aufwand, führt meist zu Preisvorteilen (Kostenreduktion) und unterstützt Standardisierung und Qualitätsmanagement.

7.2.2 Kenngrößen

Betriebswirtschaftliche Kenngrößen steuern und beeinflussen betriebliche Entscheidungen und Abläufe. Die allerwichtigsten werden im Folgenden in einer Form erläutert, die eher auf IT-Dienstleister zugeschnitten ist.

Auftragseingang (order entry)

Der Auftragseingang ist die Summe der Preise aller im Abrechnungszeitraum verkauften Leistungen und Produkte. Dabei ist es im Unterschied zum *Umsatz (revenue)* unerheblich, ob die Leistungen im Abrechnungszeitraum auch erbracht wurden.

Umsatz (revenue)

Der Umsatz ist die Summe der Preise aller im Abrechnungszeitraum erbrachten Leistungen und verkauften Produkte. Läuft ein Dienstleistungs- oder Servicevertrag über drei Jahre, so sind in einem Jahr nur ein Drittel des Gesamtpreises (*Total Contract Volume, TCV*) umsatzwirksam.[143] Bei Produkten erfolgt die Leistung durch die Übergabe, so dass ihr Preis im Jahr des Verkaufs vollständig umsatzwirksam wird.

Rohertrag (gross profit)

Der Rohertrag oder das Bruttoergebnis ist der *Umsatz (revenue)* vermindert um die direkten *Kosten*, die durch die Herstellung und den Verkauf der Produkte und Leistungen entstehen, mit denen der Umsatz generiert wurde. Um Vergleiche zu ermöglichen, wird er oft in Prozent als Anteil am Umsatz gemessen.

Gewinn…

EBIT, Gewinn vor Zinsen und Steuern („Earnings before Interest and Taxes"), ist die Differenz aller Einnahmen (*Umsatz, revenue*) und aller *Kosten* im gleichen Abrechnungszeitraum, ohne dass Zinsen und Steuern berücksichtigt wurden. Diese Kosten sind also nicht berücksichtigt, da sie zum Beispiel von Land zu Land schwanken können, sodass Vergleiche schwierig wären. Alle anderen Kosten wie zum Beispiel für die Betriebsführung werden berücksichtigt. Das EBIT ist eine Kennzahl für die Wirtschaftlichkeit einer bestimmten Einheit für die das EBIT berechnet wurde. Um Vergleiche zu ermöglichen, wird er oft in Prozent als Anteil an den Einnahmen (Umsatz) gemessen (EBIT-Marge).

Beim **EBITDA** („Earnings before Interest, Taxes, Depreciation and Amortization") werden auch Amortisierungen und Abschreibungen (Kosten bzw. Verluste durch Wertminderung des Anlagevermögens) nicht berücksichtigt.

Der **Jahresüberschuss** ist die Differenz zwischen allen Einnahmen (Umsatz) und wirklich aller Kosten innerhalb eines Geschäftsjahres.

7.3 IT-Outsourcing

Der Einkauf bzw. Verkauf von IT-Services folgt im Grunde immer einem einfachen Muster.[144] Wechselt jedoch eine komplexere IT-Landschaft den Betreiber, so gibt es einige Vorgänge und entsprechende Begriffe, die für einen solchen Übergang

---

[143] Zahlungsmodalitäten wie Zahlungsziele („Wann zahlt der Kunde?") werden hier zunächst nicht berücksichtigt.

[144] Ausschnitt aus: Eberhard von Faber und Wolfgang Behnsen: Joint Security Management: organisationsübergreifend handeln (Mehr Sicherheit im Zeitalter von Cloud-Computing, IT-Dienstleistungen und industrialisierter IT-Produktion); Springer Vieweg, Wiesbaden 2018, 244 Seiten, 60 farbige Abbildungen, ISBN 978-3-658-20833-2, https://doi.org/10.1007/978-3-658-20834-9

typisch sind. Das gilt insbesondere dann, wenn dabei eine ererbte, historisch gewachsene IT-Landschaft (legacy) modernisiert werden soll. Siehe Abb. 52.

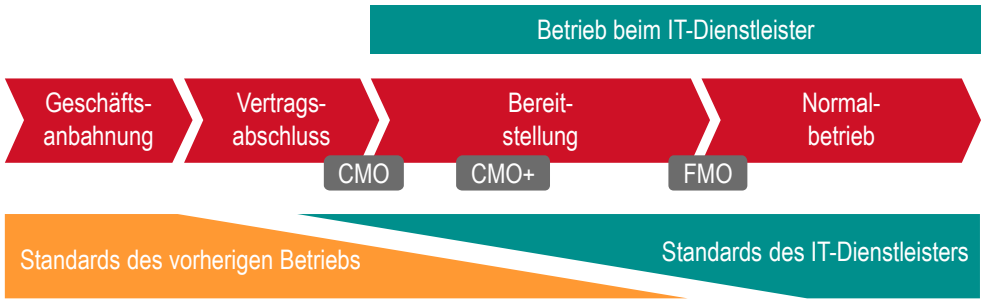


Abb. 52: Tätigkeiten und Ablauf der Geschäftsbeziehung

Outsourcing

Nutzung von Leistungen Dritter. Beim IT-Outsourcing kauft die *Anwenderorganisation IT-Services* von einem oder mehreren *IT-Dienstleistern*, die diese auf dem Markt anbieten.

Oft wird der Begriff IT-Outsourcing primär mit der Auslagerung der eigenen IT an einen IT-Dienstleister in Verbindung gebracht, was für den in den 1990er Jahren aufkommenden Markt für IT-Dienstleistungen typisch war (klassisches Outsourcing). Diese Auslagerung führte dazu, dass die IT-Dienstleister sehr heterogene Systeme, Technologien, Produkte und Prozesse zu meistern hatten, wodurch der Kostenreduktion durch *Skaleneffekte* Grenzen gesetzt waren.

Der Begriff Outsourcing wird oft mit weiteren Attributen verbunden, die den Gegenstand der eingekauften Leistungen, die zugrunde liegende Geschäftsidee oder den Leistungserbringer näher charakterisieren. Ein Beispiel ist Selektives Outsourcing, bei dem Leistungen nur begrenzt und fokussiert an Dritte vergeben und von diesen erbracht werden. Im Interesse einer klaren Abgrenzung wird dafür häufig auch der Begriff **Outtasking** verwendet. Hierbei verbleiben die Steuerung und Kontrolle meist vollständig beim Auftraggeber.

Transition

Die Transition (Übergang) ist der Prozess bis zur Erstbereitstellung von IT-Services und der Übertragung der Betriebsverantwortung auf einen IT-Dienstleister. Wechselt der IT-Dienstleister, wird die Übertragung aller definierten *Configuration Items (CIs)* und Werte (Assets), Mitarbeiter und/oder IT-Services auf den IT-Dienstleister vorbereitet und durchgeführt. Der Zustand, in dem IT-Services übernommen werden (Ist-Zustand), wird *Current Mode of Operation (CMO)* genannt. In der Regel werden Anpassungen und kleinere Verbesserungen bereits während der Transition vorgenommen. Der CMO des IT-Betriebs geht damit in einen anderen, verbesserten Betriebsmodus über (*Current Mode of Operation plus, CMO+).*

Transformation

Die Transformation hat die Modernisierung der Bereitstellung von IT-Services durch den IT-Dienstleister zum Inhalt. Bei der Transformation werden vertraglich festgelegte Projekte ausgeführt, um das Service-Level-Agreement (SLA) umzusetzen, die Gesamtbetriebskosten zu senken und bestehende IT-Services zu erweitern oder neue einzuführen. Der Schwerpunkt liegt dabei auf der Standardisierung, Zentralisierung und Integration. Mit der Transformation wird der IT-Service in den sogenannten *Future Mode of Operation (FMO)* versetzt. Die Transformation folgt zeitlich der *Transition*.

Current Mode of Operation (CMO)

Der Current Mode of Operation (CMO) ist der IT-Betriebsmodus vor der *Transition* (Übergang). Anders ausgedrückt werden die IT-Systeme des Kunden im Ist-Zustand ohne Änderungen durch den IT- Dienstleister betrieben.

Current Mode of Operation plus (CMO+)

Der CMO+ ist der IT-Betriebsmodus nach Abschluss der *Transition* (Übergang) und vor Beginn der *Transformation*. Der CMO+ unterscheidet sich vom CMO: Bei der Übertragung der IT-Services auf den IT-Dienstleister werden die Dienste angepasst und in gewissem Umfang verbessert. Auch der Betrieb geht vollständig in die Zuständigkeit des IT-Dienstleisters über.

Future Mode of Operation (FMO)

Der Future Mode of Operation (FMO) ist der IT-Betriebsmodus nach Abschluss der *Transformation*. Er folgt auf den CMO+. Der optimierte Betrieb nach den Standards des IT-Dienstleisters wird erreicht, nachdem alle durchzuführenden Projekte ausgeführt wurden.

7.4 Unternehmensstrategie

IT-Sicherheitsexperten verlangen von ihrer Geschäftsführung, die IT-Sicherheit in der Geschäftsstrategie zu verankern. Sie selbst interessieren sich meist sehr wenig dafür. – Das Wohl und Wehe mancher IT-Experten hängt am Erfolg eines IT-Services; doch den Marktchancen und den Aussagen ihres Managements bringen sie oft wenig Interesse entgegen. Dabei kann man aus den strategischen Aussagen eines Unternehmens manches ableiten. Vieles haben die Experten auch selbst in der Hand: Sie sind selber involviert in die Formulierung der Leistungsversprechen (value proposition) und der Alleinstellungsmerkmale (unique selling points, USPs), was rückwirkt auf die Marktchancen und eventuell auch auf die Unternehmensstrategie.

Es folgt eine kurze Darstellung einiger Begriffe der strategischen Planung. Der grundsätzliche Aufbau ist in Abb. 53 dargestellt.

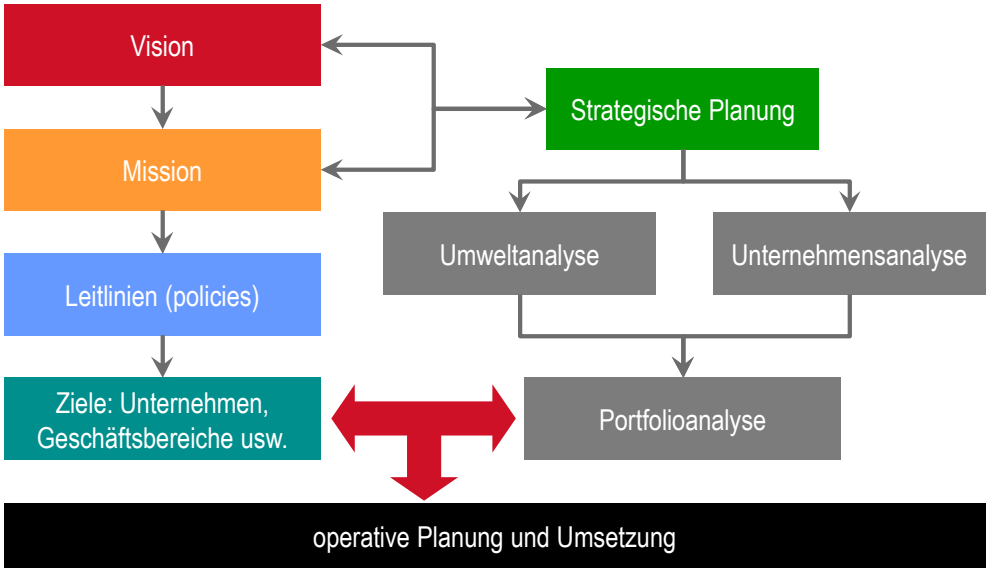


Abb. 53: Strategische Planung (einfache Grundstruktur)

Ziele

Vision

> Definition von Zielen auf der obersten Ebene der Zielehierarchie eines Unternehmens, in denen die zukünftige, angestrebte Rolle des Unternehmens beschrieben wird. Die Vision soll richtungsweisend wirken. Meist handelt es sich dabei um eine sehr kurze und prägnante Formel.

Die Vision ist oft sehr kurz und allgemein gefasst: „Wir werden die Nummer Eins im XY-Markt und der führende Anbieter von Z." Wird zusätzlich eine Mission definiert, so liefert diese eine Vorstellung davon, wie die Vision erreicht werden soll.

Mission

> Eine Mission fasst in sehr kurzer und prägnanter Form zusammen, worin die Bestimmung des Unternehmens liegt bzw. wie der Geschäftsauftrag zu verstehen ist. Die Mission beschreibt bzw. skizziert dabei, was das Unternehmen für welche Kunden oder Zielgruppen leistet und wie dies erfolgt. Oft wird dabei ein bestimmtes Leistungsversprechen (value proposition) hervorgehoben.

Nicht immer existiert eine Mission. Sie wird häufig mit der Vision verbunden, obwohl beide unterschiedliche Funktionen haben. An der Mission kann zum Beispiel erkannt werden, welche Bereiche zum Kerngeschäft gehören und welche möglicherweise nicht. Ähnliches gilt für Regionen oder Länder, in denen das Unternehmen geschäftlich tätig ist oder die es als Zielmärkte ansieht.

Unternehmensrichtlinien (policies)

Unternehmensrichtlinien bieten Orientierungshilfen für Führungskräfte und andere Mitarbeiter des Unternehmens. Sie stellen grundsätzliche Verhaltensregeln dar.

Unternehmensrichtlinien fassen zusammen, welche Verhaltensweisen positiv bewertet und „gelebt" und gefördert werden sollen. Außerdem werden bestimmte Themen wie Leistung, Zusammenarbeit, Fähigkeiten oder Innovationen hervorgehoben. Unternehmensrichtlinien reflektieren auch die (gewünschte) Unternehmenskultur. Es sollte jedoch immer bedacht werden, dass Vision, Mission sowie Unternehmensrichtlinien öffentlich zugängliche Informationen darstellen, so dass davon auszugehen ist, dass sie auch werblichen Zwecken (Imagepflege) dienen können.

Unternehmensziele

Die Definition von Zielen dient einerseits der Lenkung bzw. Steuerung und andererseits der Kontrolle bzw. Überprüfung, inwieweit das Gewünschte wirklich erreicht wurde. Dazu müssen die Ziele in konkreter Form abgefasst sein und es muss erkennbar sein, in welchem definierten Zeitraum sie erreicht werden sollen. Zieldefinitionen auf Unternehmensebene haben oft noch strategischen Charakter, solche für Geschäfts- und Funktionsbereiche verwenden oft konkrete Kennzahlen.

Ziele können weitere Funktionen erfüllen:[145] Sie können Entscheidungen ermöglichen, indem sie Kriterien für die Bewertung von Alternativen liefern. Sie wirken koordinierend, indem sie Aktivitäten auf ein Ziel ausrichten. Und sie legitimieren, indem sie Aktivitäten rechtfertigen.

Planung

Umweltanalyse

Um zu verstehen, wie ein Unternehmen bestmöglich agieren sollte, muss es seine Umwelt, speziell die Märkte untersuchen, in denen es tätig ist und sein will. Dabei spielt die Untersuchung der Marktattraktivität (Marktstruktur, Marktgröße, Marktwachstum) eine große Rolle und die der Marktdynamik (Veränderungen im Markt). Aus dieser **Marktanalyse** werden Chancen (Opportunities) und Risiken (Threats) für das Unternehmen abgeleitet, die eine Hälfte der Bewertung einer *SWOT-Analyse* ergeben. Dabei soll der Blick nicht nur aus dem Unternehmen nach außen („inside-out") gerichtet sein. Vielmehr wird dabei untersucht, wie das Unternehmen durch die Umwelt (Markt) wahrge-

---

[145] Franz Xaver Bea und Jürgen Haas: Strategisches Management; UTB für Wissenschaft: Uni-Taschenbücher 1458, Lucius & Lucius, 2001, 3. neu bearbeitete Auflage, ISBN 3-8252-1458-3, 601 Seiten

nommen wird und welche Chancen dadurch wirklich bestehen bzw. welche Risiken sich ergeben.

Unternehmensanalyse

Die Unternehmensanalyse untersucht, welche Möglichkeiten (Potenziale) das Unternehmen im Markt hat. Dies erfolgt dadurch, dass die Stärken (Strengths) und Schwächen (Weaknesses) des Unternehmens analysiert werden. Um zu realistischen Einschätzungen zu kommen, sollten auch Mitbewerber (Konkurrenten) untersucht und zum Vergleich herangezogen werden. Die Stärken und Schwächen des Unternehmens ergeben eine Hälfte der Bewertung in einer *SWOT-Analyse*.

SWOT-Analyse

Die SWOT-Analyse kombiniert Ergebnisse aus der *Umweltanalyse* und der *Unternehmensanalyse*. Die Unternehmensanalyse liefert die Stärken (Strengths) und Schwächen (Weaknesses) des Unternehmens, die Umweltanalyse die Chancen (Opportunities) und Risiken (Threats). Die Abkürzung SWOT ergibt sich aus den Anfangsbuchstaben der englischen Begriffe. Die SWOT-Analyse geht davon aus, dass ein Unternehmen die Gelegenheiten (Chancen versus Risiken) nur nutzen kann, wenn es über die erforderlichen Mittel (Stärken versus Schwächen) verfügt.

Portfolioanalyse

Die Portfolioanalyse ist ein Mittel der **strategischen Planung**. Dabei werden einzelne Angebote analysiert und bewertet, die strategischen Geschäftsfeldern zugeordnet sind. Die Gesamtheit aller Angebote (Produkte und Dienstleistungen) bildet das **Portfolio** oder **Offering Portfolio**. Die Bewertung ist die Grundlage für Entscheidungen hinsichtlich der Entwicklung, Weiterführung, Förderung oder Einstellung des jeweiligen Angebotes (Portfolioelementes). Weitverbreitete Methoden der Portfolioanalyse und der Art der Darstellung der Ergebnisse sind die *BCG-Matrix* und die *McKinsey-Matrix*.

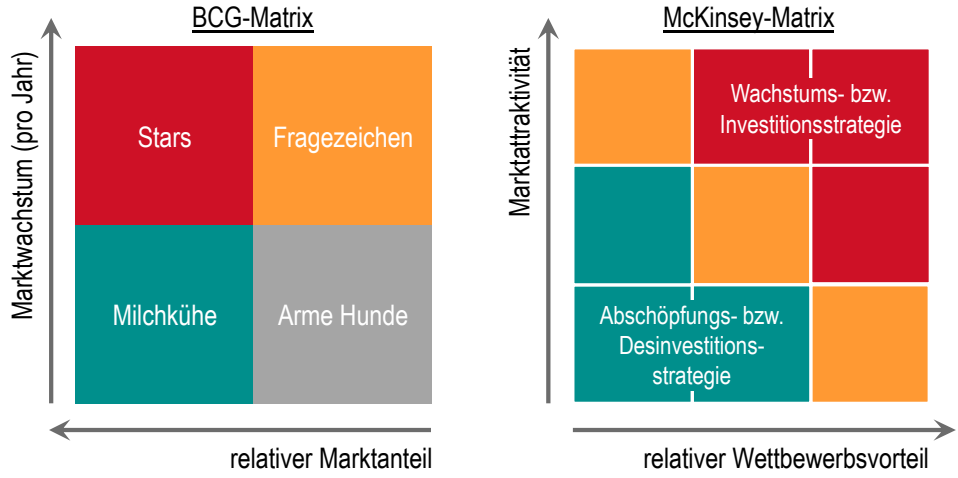


Abb. 54: Portfolioanalyse, BCG-Matrix (links) und McKinsey-Matrix (rechts)

BCG-Matrix

Die von der Unternehmensberatungsfirma Boston Consulting Group (BCG) entwickelte BCG-Matrix ist ein Verfahren zur *Portfolioanalyse*. Sie ordnet die Angebote (Portfolioelemente) in zwei Dimensionen an (Abb. 54, links): dem Marktwachstum und dem „relativen Marktanteil". Der relative Marktanteil ist der eigene, mit dem Angebot erzielte *Umsatz* geteilt durch den Umsatz des größten Wettbewerbers. Bildet das Marktwachstum die Y-Achse und der relative Marktanteil die X-Achse (mit in Richtung Koordinatenursprung wachsenden Werten), dann fallen die Angebote in einen von vier Quadranten, die wie folgt bezeichnet werden: Stars (hohes Marktwachstum, hoher relativer Marktanteil), Nachwuchs oder Fragezeichen (hohes Marktwachstum, geringer relativer Marktanteil), Milchkühe (geringes Marktwachstum, hoher relativer Marktanteil) und Auslaufmodelle oder arme Hunde (geringes Marktwachstum, geringer relativer Marktanteil). Für jeden Quadranten gibt es eine Empfehlung (Normstrategie). Die BCG-Matrix hilft dabei, den Cashflow zu optimieren.

McKinsey-Matrix

Die von der Unternehmensberatungsfirma McKinsey entwickelte McKinsey-Matrix ist ein Verfahren zur *Portfolioanalyse*. Sie ordnet die Angebote (Portfolioelemente) in zwei Dimensionen an (Abb. 54, rechts): der Marktattraktivität (Y-Achse) und dem relativen Wettbewerbsvorteil (X-Achse). Sind beide Werte zusammengenommen gering (Portfolioelement ist dem Koordinatenursprung relativ nahe), so wird eine Abschöpfungsstrategie empfohlen. Sind die Werte zusammengenommen hoch (Portfolioelement ist relativ weit entfernt vom Koordinatenursprung), so soll auf Wachstum und Investitionen gesetzt werden. Als dritte Möglichkeit wird eine sogenannte Selektionsstrategie empfohlen. Die McKinsey-Matrix hilft dabei, den Return on Investment (RoI) zu optimieren.

Literatur und Bildnachweise

Besonders ein solches Buch, das sich zur Aufgabe macht, Definitionen von Fachbegriffen zu geben, kann nicht geschrieben werden, ohne dass der Autor vielfältige Literatur gelesen hätte – in der langen Zeit der Tätigkeit auf diesem Gebiet, bei der Erstellung von Lehrunterlagen für Studierende und beim Schreiben dieses Buches. Die Definitionen sollen ja den Stand der Technik korrekt wiedergeben und konsensfähig sein. Das bedeutet auch, dass Begriffe und Zusammenhänge auch in anderen Veröffentlichungen so oder ähnlich vorkommen können – ja müssen.

Daher wurde wie folgt verfahren: (1) Literatur ist an den Stellen als Fußnote angegeben, wo ich sie direkt verwendet habe bzw. mir bewusst ist, dass Begriff, Definition oder sonstige Beschreibungen auf eine solche Quelle zurückgeführt werden können. (2) Gilt dies in gleicher Weise für Institutionen oder Einzelpersonen, so sind diese meist direkt im Text angegeben. (3) Die folgende Liste enthält Literaturhinweise und wiederholt nicht die Quellenangaben in diesem Kapitel. (4) Falls nicht anders angegeben, wurden Abbildungen extra für dieses Buch erstellt.

[1] Torsten Gründer (Hrsg.): IT-Outsourcing in der Praxis, Strategien, Projektmanagement, Wirtschaftlichkeit; Erich Schmidt Verlag, Berlin, 2011, 2. Auflage, ISBN 978-3-503-09015-0, 479 Seiten

[2] Investopedia Dictionary; https://www.investopedia.com/financial-term-dictionary-4769738

[3] Rechnungswesen verstehen.de, Wirtschaft verständlich erklärt; https://www.rechnungswesen-verstehen.de/lexikon/ebit.php

[4] Franz Xaver Bea und Jürgen Haas: Strategisches Management; UTB für Wissenschaft: Uni-Taschenbücher 1458, Lucius & Lucius, 2001, 3. neu bearbeitete Auflage, ISBN 3-8252-1458-3, 601 Seiten

[5] Edward Russel-Walling: 50 Schlüsselideen Management; Spektrum Akademischer Verlag, Heidelberg, 2011, ISBN 978-3-8274-2636-9, 207 Seiten

Elektronisches Zusatzmaterial
Die Abbildungen sind als PowerPoint-Datei kapitelweise über https://link.springer.com/ auf der Seite des eBooks abrufbar.

8 Kryptografie

Die wichtigsten Prinzipien und Verfahren der Kryptografie zu kennen, gehört heute zum informationstechnologischen Grundwissen. Leider wird bei der Wissensvermittlung nicht immer zwischen Anwendern und Gelehrten unterschieden, sodass die Darstellung für die erste Zielgruppe, zu denen auch Programmierer zählen, unnötig kompliziert wird. Die Darstellung in diesem Kapitel versucht, diesen Fehler zu vermeiden und dennoch viel Interessantes auch für diejenigen zu bieten, die mit vielen Begriffen aus der Kryptografie bereits sicher umgehen können.

Physische Werte können hinter Mauern, Türen und gesicherten Tresoren verborgen und so vor unberechtigtem Zugriff geschützt werden. Handelt es sich bei den Werten um elektronisch gespeicherte Informationen, so kann das Computersystem, das sie speichert, so konstruiert werden, dass es wie die Mauern, Türen und gesicherten Tresore wirkt. Doch elektronische Informationen werden bewegt, sie werden über Netzwerke übertragen und per elektronischer Post verschickt. Dabei können sie in unberechtigte Hände gelangen oder verfälscht werden. Sie können als eigene Daten ausgegeben oder verfälscht und anderen untergeschoben werden. Gelangen sie in fremde Hände, so kann dies unbemerkt geschehen, weil Daten beliebig oft kopiert werden können. Werden sie verfälscht, indem das Original überschrieben wird, so fehlt der Vergleichswert, um die Fälschung aufdecken zu können.

Wie kann Vertrauen entstehen in diesem Umfeld? Wie können verlässliche Verabredungen und geschäftliche Vereinbarungen getroffen werden? Wie wird bezahlt? Wie werden Rechte gewahrt? Wie können Fehler entdeckt und Betrüger entlarvt werden?

Die Antwort lautet: durch Mathematik. Informationen werden in eine für Uneingeweihte unbrauchbare Form gebracht, die nur von Berechtigten wiederhergestellt werden kann. Informationen werden mit Zahlenwerten ergänzt, die die Richtigkeit und Echtheit der Informationen zu prüfen gestatten. Dabei handelt es sich um verschiedenste Verschlüsselungsverfahren und andere Berechnungsschemata mit besonderen Eigenschaften wie der Unumkehrbarkeit. Die Wissenschaft dieser Verfahren ist die Kryptografie. Kryptografische Verfahren oder Algorithmen sind heute in jedem Computersystem hundert- oder tausendfach implementiert. Ohne sie ist das Internet in seiner heutigen Form nicht denkbar.

Zusatzmaterial online
Zusätzliche Informationen sind in der Online-Version dieses Kapitel (https://doi.org/10.1007/978-3-658-33431-4_8) enthalten.

E. von Faber, *IT und IT-Sicherheit in Begriffen und Zusammenhängen*,
Edition <kes>, https://doi.org/10.1007/978-3-658-33431-4_8

Hinweis: Probleme bei der Anwendung asymmetrischer Verschlüsselungsverfahren und deren Lösung (primär mit Public-Key Infrastructures, PKI) werden sehr ausführlich in Kapitel 3.4 behandelt. Siehe dort.

8.1 Einführung und Übersicht

Kryptografie ist nicht gleich IT-Sicherheit, aber die IT-Sicherheit wäre ein stumpfes Schwert ohne Kryptografie. Viele Studienkurse und auch Lehrbücher konzentrieren sich daher darauf, kryptografische Verfahren bzw. kryptografische Algorithmen, wie sie auch genannt werden, im Detail zu erklären. Für fast alle Experten wird es jedoch mit Blick auf ihre berufliche Tätigkeit ausreichend sein, die wichtigsten Klassen solcher Verfahren und deren Eigenschaften zu kennen.

Wir werden also im Folgenden nur Klassen von Verfahren bzw. Algorithmen beschreiben und diese weitgehend als Blackbox betrachten (Kapitel 8.2). Die sieben Klassen, die beschrieben werden, sind in Abb. 55 aufgeführt.

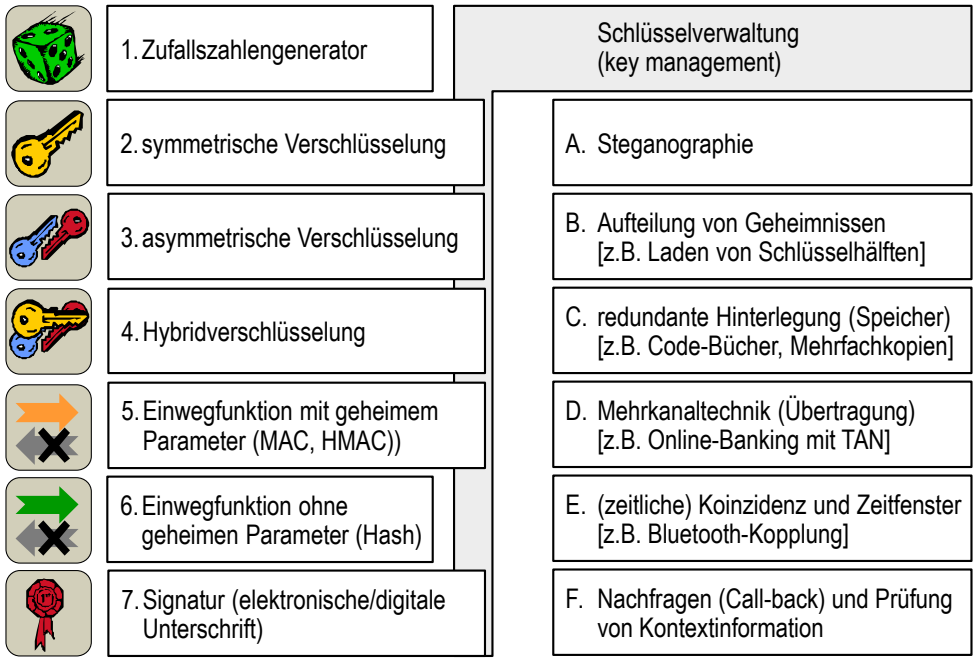


Abb. 55: Kryptografische Verfahren (links) und zusätzliche Techniken (rechts)[146]

Viele kryptografische Verfahren verwenden geheime Parameter, die Schlüssel genannt werden. Was es mit ihnen auf sich hat, wird im Kapitel 8.3 über Schlüsselverwaltung (key management) beschrieben (siehe rechts oben in Abb. 55).

[146] Eberhard von Faber: Vorlesungsskript; Technische Hochschule Brandenburg; modifiziert

Die Beschreibung der Verfahren wird ergänzt durch die Betrachtung einiger Anwendungen (Kapitel 8.4), bei denen es sich vor allem um ein paar Protokolle handeln wird.

Eine sehr große Herausforderung bei der Implementierung kryptografischer Verfahren besteht darin, die gerade erwähnte Schlüsselverwaltung (key management) zu meistern. Zusätzlich kommen aber oft weitere Techniken zum Einsatz, von denen einige rechts in Abb. 55 dargestellt sind (Buchstaben A-F).

Wir werden nur den Begriff Steganographie erklären (Buchstabe A). Auf die Kryptoanalyse wird ebenfalls nicht näher eingegangen. Damit sind wir bereits bei den ersten vier Oberbegriffen: Steganographie, Kryptografie, Kryptoanalyse und Kryptologie.

Steganographie

Methoden, bei denen die Existenz von Informationen verborgen wird, um sie zu schützen. Ist die Existenz prinzipiell bekannt, so wird das Auffinden der Information derart erschwert, dass ein Schutz gegeben ist, den die *Kryptografie* mit anderen Mitteln und höherer Sicherheit erreicht, ohne die Existenz der Informationen bzw. der Kommunikation in irgendeiner Weise zu verbergen.

Kryptografie (cryptography)

Gesamtheit mathematischer Methoden und ihrer Anwendung zum Schutz von digital vorliegenden Informationen und der digitalen Kommunikation.

Im Vordergrund steht dabei die Sicherstellung der *Vertraulichkeit* (confidentiality), der *Integrität* (integrity), der *Authentizität* (authenticity) sowie der *Verantwortlichkeit* (accountability) bzw. der Nicht-Abstreitbarkeit oder Unleugbarkeit (non-repudiation).

Kryptografie ist damit auch ein Mittel, Vertrauensbeziehungen abzubilden und verschiedene Formen von Übereinkünften elektronisch nachprüfbar zu besiegeln.

Kryptoanalyse

Verfahren und Versuche, ohne Kenntnis des Schlüssels Daten zu entschlüsseln, die mit Hilfe kryptografischer Algorithmen gesichert wurden. Die Kryptoanalyse umfasst also alle analytischen und praktischen Verfahren, um kryptografische Algorithmen zu brechen oder Schwächen aufzuzeigen.

Kryptoanalyse und *Kryptografie* bilden zusammen die **Kryptologie**.

8.2 Kryptografische Verfahren

Es werden Typen oder Klassen kryptografischer Verfahren oder Algorithmen beschrieben und weitgehend als Blackbox betrachtet. Die sieben Klassen sind links in Abb. 55 aufgeführt.

Hinweis: Die folgende Darstellung ist natürlich, schon aufgrund ihrer zusammenfassenden kurzen Darstellungsweise, vereinfachend. Es gibt eine Vielzahl von Verfahren und Algorithmen, sodass es hier nicht möglich ist, die vielen Unterschiede aufzuzeigen. Stattdessen stehen gemeinsame Grundprinzipien im Vordergrund.

Zufallszahlengenerator (random number generator)

Produziert Zahlen, die nicht vorhersehbar sind. Echte Zufallszahlengeneratoren erzeugen Zahlen zudem in einer Weise, die nicht reproduzierbar ist. D.h., ein Neustart oder dergleichen erzeugt eine andere Folge von Zahlen.

Zufallszahlen spielen eine große Rolle in der Kryptografie, weil die Sicherheit vieler Algorithmen darauf beruht, dass ein Parameter (Schlüssel) geheim bleibt, also auch nicht erraten oder rekonstruiert werden kann. Zufallszahlen werden für die Erzeugung von kryptografischen Schlüsseln verwendet, als Saatwert (seed) für die Verschlüsselung (CBC-Modus), als Challenge für die Authentisierung (siehe *Challenge-Response-Verfahren*) oder als *Authentisierungsmerkmal* selbst.

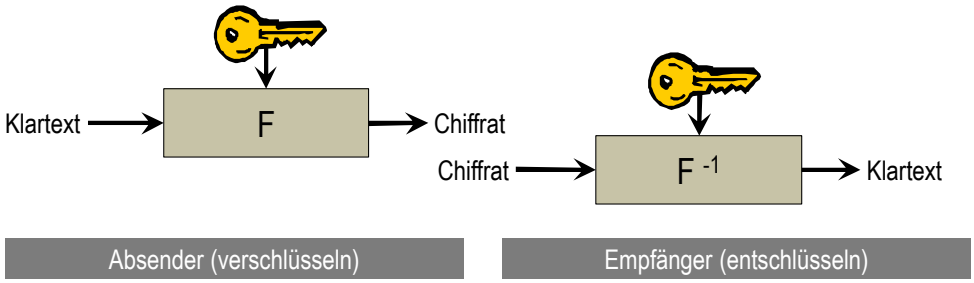


Abb. 56: Symmetrische Verschlüsselung (schematischer Ablauf)[147]

Symmetrische Verschlüsselung

Verfahren oder Algorithmus, um Daten von ihrer Ursprungsform (Klartext) in eine Form zu transformieren (Chiffrat), die für alle unautorisierten Empfänger unbrauchbar ist, aber vom Besitzer (von Besitzern) eines geheimen Schlüssels (Zahl) wiederhergestellt werden kann. Symmetrisch heißt diese Form der Transformation (Verschlüsselung) deshalb, weil für die Transformation vom Klartext zum Chiffrat und zurück der gleiche Schlüssel verwendet wird.[148] Absender und Empfänger (die identisch sein können) teilen sich also einen Schlüssel. Siehe Abb. 56.

Die wichtigsten Eigenschaften der symmetrischen Verschlüsselung sind:
a) Die Wiederherstellung der Klartextdaten ist nur mit dem Schlüssel möglich.

---

147 Eberhard von Faber: Vorlesungsskript; Technische Hochschule Brandenburg; modifiziert

148 Genauer gesagt können sie verschieden sein; aber sie können voneinander abgeleitet werden.

b) Dieser Schlüssel ist mit realistischem Aufwand in realistischer Zeit nicht rekonstruierbar, auch nicht durch die Analyse sehr vieler echter Klartext-Chiffrat-Paare.
c) Die Verschlüsselung mit bekanntem Schlüssel ist rechentechnisch vergleichsweise wenig aufwendig (schnell).

Bei symmetrischen Verschlüsselungsverfahren handelt es sich meist um eine **Blockverschlüsselung**. D.h., die Algorithmen verarbeiten Daten (Zahlen) einer bestimmten Länge (in Bits). Kürzere Daten werden aufgefüllt (padding), längere werden in Blöcke aufgeteilt. Die Blöcke werden unabhängig voneinander verschlüsselt (Electronic Codebook Mode, ECB) oder verkettet verschlüsselt (Cipher Block Chaining Mode, CBC). Neben der Blockverschlüsselung gibt es auch **Stream Cipher**, die bitweise arbeiten. Ein Beispiel ist One-time Pad, der einzig beweisbar sichere Algorithmus.

Bekannte Algorithmen sind AES (Advanced Encryption Standard), der von diesem abgelöste DES (Data Encryption Standard) sowie Triple-DES, IDEA, RC5 usw.

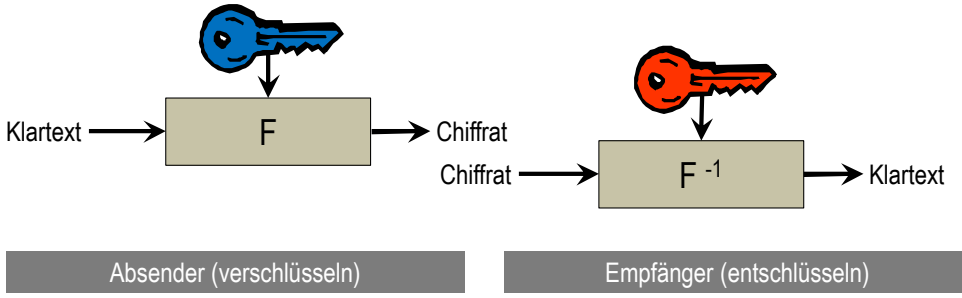


Abb. 57: Asymmetrische Verschlüsselung (schematischer Ablauf)[149]

Asymmetrische Verschlüsselung

Verfahren oder Algorithmus, um Daten von ihrer Ursprungsform (Klartext) in eine Form zu transformieren (Chiffrat), die für alle unautorisierten Empfänger unbrauchbar ist, aber vom Besitzer (von Besitzern) eines geheimen privaten Schlüssels (Zahl) wiederhergestellt werden kann. Asymmetrisch heißt diese Form der Transformation (Verschlüsselung) deshalb, weil für die Transformation vom Klartext zum Chiffrat ein anderer Schlüssel verwendet wird als bei der Wiederherstellung des Klartexts. Der Absender verwendet den sogenannten öffentlichen Schlüssel, der Empfänger seinen privaten, der geheim zu halten ist. Beide werden auch als Komponenten eines **Schlüsselpaares** bezeichnet. Die asymmetrische Kryptografie wird auch als **Public-Key Cryptography** bezeichnet. Siehe Abb. 57.

[149] Eberhard von Faber: Vorlesungsskript; Technische Hochschule Brandenburg; modifiziert

Mit einer asymmetrischen Verschlüsselung ist eine Ad-hoc-Kommunikation möglich: Teilnehmer können sicher miteinander kommunizieren, ohne dass sie vorher Schlüssel sicher austauschen müssen. Die öffentliche Schlüsselkomponente wird dazu allgemein zugänglich gemacht.

Die wichtigsten Eigenschaften der asymmetrischen Verschlüsselung sind:
a) Die Wiederherstellung der Klartextdaten ist nur mit dem privaten Schlüssel (der privaten Schlüsselkomponente) möglich.
b) Dieser Schlüssel ist mit realistischem Aufwand in realistischer Zeit nicht rekonstruierbar, nimmt man an.
c) Die Berechnungen sind im Vergleich zu symmetrischen Verschlüsselungsverfahren sehr aufwendig (langsamer).

RSA (1977, benannt nach seinen Erfindern Rivest, Shamir und Adleman) ist das bekannteste Public-Key-Kryptoverfahren. Es geht auf die Grundidee von Diffie und Hellmann (1976) zurück, die kryptografische Sicherheit an ein bekannt schwieriges Berechnungsproblem zu koppeln.[150] So ist es weitaus schwieriger bzw. aufwendiger, echte Teiler einer natürlichen Zahl zu finden, als ein Produkt zu berechnen. Arbeitet man mit genügend großen Zahlen, so sind Probedivisionen genügend langwierig. Daher sind die RSA-Schlüssel immer sehr viel länger (in Bits) als die Schlüssel symmetrischer Verfahren.

Die mit der Nutzung bzw. Veröffentlichung der öffentlichen Schlüsselkomponente im Zusammenhang stehenden Probleme und Lösungen werden ausführlich in Kapitel 3.4 beschrieben. Daher wird an dieser Stelle auf *Public-Key-Infrastructures (PKIs)* und dergleichen nicht eingegangen.

[150] Die zweite Idee ist folgende: Wer eine Nachricht verschlüsselt versendet, braucht diese nicht entschlüsseln zu können – er kennt den Inhalt ohnehin. Daher kann für die Verschlüsselung ein anderer Schlüssel verwendet und dieser öffentlich zugänglich gemacht werden.

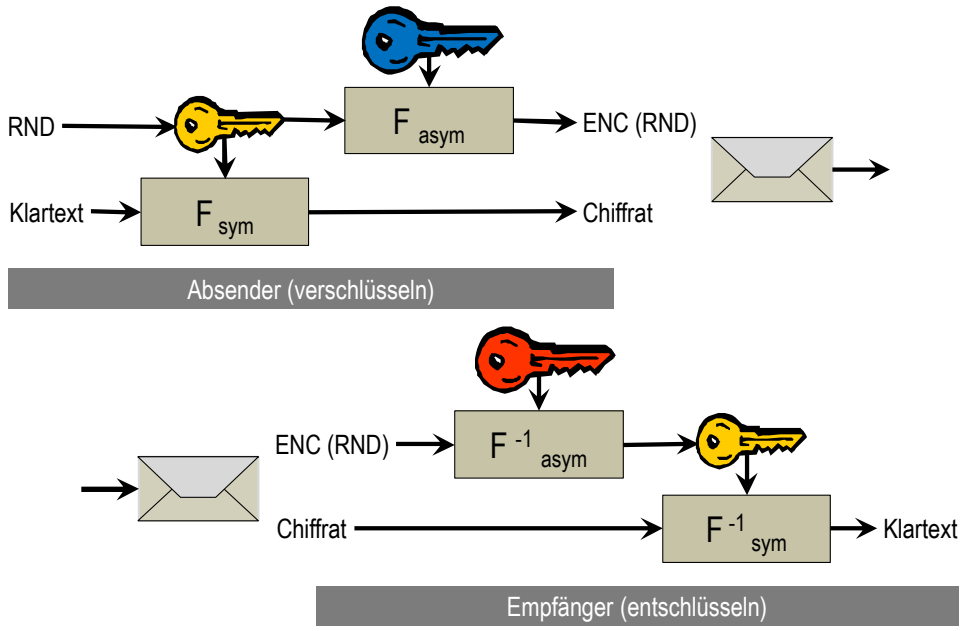


Abb. 58: Hybridverschlüsselung (schematischer Ablauf)[151]

Hybridverschlüsselung

Kombination von symmetrischer und asymmetrischer Verschlüsselung, wobei das symmetrische Verfahren aufgrund seiner hohen Effizienz (Geschwindigkeit) für die Verschlüsselung der Daten zum Einsatz kommt und die asymmetrische Verschlüsselung genutzt wird, um den dafür verwendeten symmetrischen Schlüssel sicher zu übertragen. Siehe Abb. 58.

Der für die Verschlüsselung der Daten verwendete symmetrische Schlüssel wird mit Hilfe eines *Zufallszahlengenerator*s erzeugt und nur einmal verwendet. Der Absender benötigt weiterhin den öffentlichen Schlüssel des Empfängers. Wurde dieser allgemein zugänglich gemacht, ist eine vertrauliche Ad-hoc-Kommunikation möglich, ohne dass die Kommunikationspartner vorher einen Schlüssel auf sicherem Wege austauschen müssen.

[151] Eberhard von Faber: Vorlesungsskript; Technische Hochschule Brandenburg; modifiziert

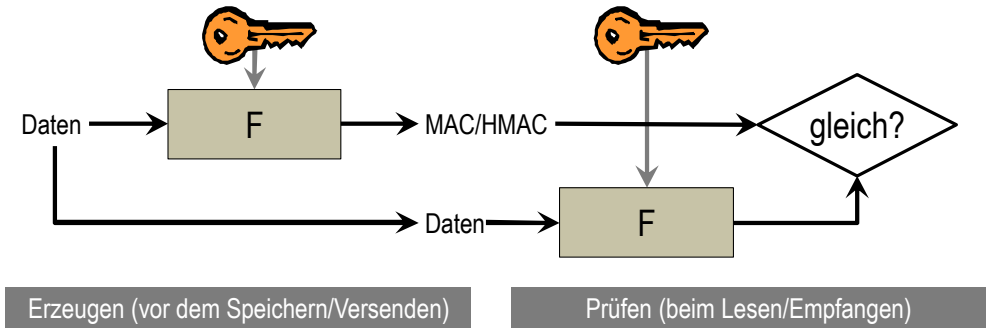


Abb. 59: Einwegfunktion mit geheimem Parameter (MAC, HMAC) (schematischer Ablauf)

Einwegfunktion mit geheimem Parameter (MAC, HMAC)

Erzeugt eine kryptografische Prüfsumme (charakteristische Kurzform) von Daten unter Verwendung eines geheimen Schlüssels, anhand derer die *Integrität* (integrity) nachgeprüft werden kann. Die Prüfsumme, die auch **Message Authentication Code (MAC)** genannt wird, wird zusätzlich zu den Daten gespeichert bzw. übertragen. Kommt es zu Veränderungen an den Daten, so stimmt die nachberechnete Prüfsumme nicht mit der ursprünglichen, gespeicherten bzw. übertragenen Prüfsumme überein. Siehe Abb. 59.

Die Daten können beliebig lang sein; die Prüfsumme hat eine feste Länge und ist (fast immer) kürzer. Allein daraus ergibt sich eine Einwegeigenschaft: Es ist nicht möglich, die Daten aus der Prüfsumme zu rekonstruieren. Der MAC kann mit Hilfe eines *Blockverschlüsselungs*algorithmus im CBC-Modus erzeugt werden, dessen Blocklänge die Länge des MACs vorgibt. Es wird von einem **Keyed-Hash MAC (HMAC)** gesprochen, wenn statt des Blockverschlüsselungsalgorithmus eine →*Hashfunktion* zum Einsatz kommt.

Bei der Beschreibung der Hashfunktion werden auch weitere Eigenschaften der Einwegfunktionen bzw. der erzeugten Prüfsummen (*Kollisionsresistenz* und *Urbildresistenz*) erläutert.

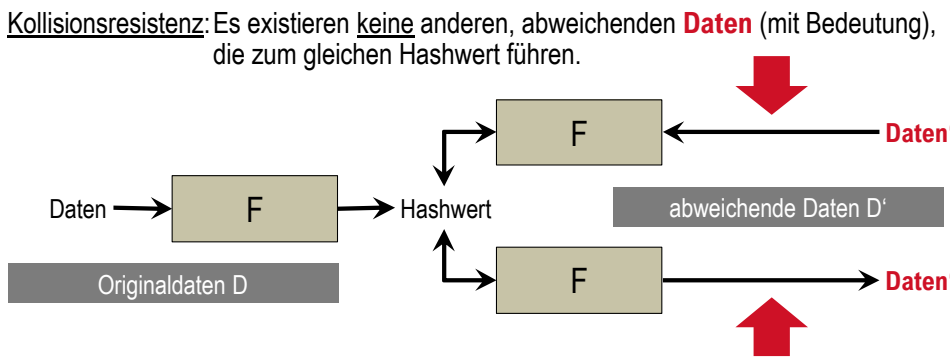


Abb. 60: Einwegfunktion ohne geheimen Parameter (Hash): Eigenschaften

Einwegfunktion ohne geheimen Parameter (Hash)

Erzeugt eine kryptografische Prüfsumme (charakteristische Kurzform, meist **Hash** genannt) von Daten (ohne die Anwendung eines Schlüssels). Der Hash bzw. Hashwert kann verwendet werden, um die *Integrität* (integrity) nachzuprüfen. Der Ablauf entspricht dann dem in Abb. 59 (ohne die Schlüssel). Hauptanwendung ist aber die Verwendung als charakteristische Kurzform („fingerprint“), um einen Datensatz wiedererkennen zu können, ohne ihn untersuchen zu müssen bzw. sogar, ohne ihn zu kennen. So kann sich ein System den Hashwert eines korrekten Passwortes merken und eine erneute Eingabe durch Vergleich der Hashwerte überprüfen, ohne das Passwort selbst zu besitzen.

Die Daten können beliebig lang sein; die Prüfsumme hat eine feste Länge und ist (fast immer) kürzer. Allein daraus ergibt sich eine Einwegeigenschaft:
a) Es ist nicht möglich, die Daten aus der Prüfsumme zu rekonstruieren. Die beiden anderen, wichtigen Eigenschaften einer **Hashfunktion** sind Kollisionsresistenz und Urbildresistenz.
b) Über **Kollisionsresistenz** verfügt die Funktion dann, wenn es praktisch unmöglich ist, verschiedene Daten zu finden, die zum gleichen Hashwert führen.[152]
c) Die **Urbildresistenz** ist dann gegeben, wenn es praktisch unmöglich ist, einen weiteren Datensatz zu finden, der den gleichen Hashwert hat, wie ein anderer, gegebener Datensatz.[153] Siehe Abb. 60.

Hashfunktionen bzw. -algorithmen sind zum Beispiel SHA-2, SHA-3 und MD5. Die Abkürzungen stehen für „Secure Hash Algorithm“ bzw. „Message Digest“.

---

[152] Kollisionsresistenz: D und D‘ existent mit H(D)=H(D‘)? Siehe Abb. 60.

[153] Urbildresistenz: D‘ finden mit H(D‘)=H(D), wobei H(D) gegeben ist. Siehe Abb. 60.

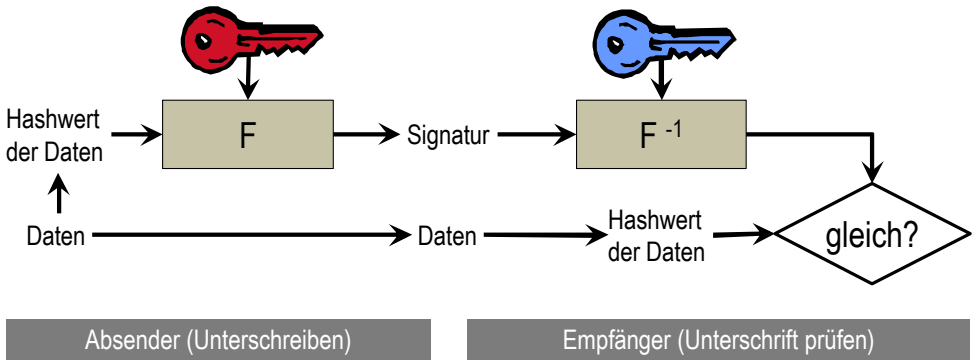


Abb. 61: Digitale Signatur bzw. elektronische Unterschrift (schematischer Ablauf)[154]

Signatur (elektronische/digitale Unterschrift)

Erzeugt eine kryptografische Prüfsumme (Signatur) von Daten unter Verwendung eines geheimen Schlüssels, anhand derer die *Authentizität* (der Datenursprung) eindeutig festgestellt werden kann. Die Signatur wird zusätzlich zu den Daten gespeichert bzw. übertragen.

Variante 1: Die Bildung einer Signatur kann mittels *asymmetrischer Verschlüsselung* durch Verschlüsselung des *Hash*wertes der Nachricht erfolgen. Dabei kommt der private Schlüssel des Absenders und Unterzeichners zum Einsatz. Siehe Abb. 61. Bei der Prüfung der Herkunft wird die Signatur mit dem öffentlichen Schlüssel des Unterzeichners[155] entschlüsselt. Stimmt dieser Wert mit dem neu berechneten Hashwert der Daten überein, gilt die Herkunft als bestätigt und die Daten sind unversehrt.

Als Algorithmen sind einsetzbar: RSA, DSS (Digital Signature Algorithm), ECC (Elliptic Curve Cryptography).

Variante 2: Eine Lösung mit *symmetrischer Kryptografie* verwendet einen *Message Authentication Code (MAC)* und benötigt eine unabhängige, vertrauenswürdige Partei als Treuhänder.[156] Jeder Teilnehmer teilt sich einen symmetrischen Schlüssel mit dem Treuhänder. Der Unterzeichner schickt die mit einem MAC versehenen Daten an den Treuhänder. Der Treuhänder prüft den MAC und stellt damit fest, dass die Daten vom Unterzeichner kamen. Nun fügt er den Daten die Information hinzu, dass sie vom Unterzeichner stammen und generiert einen MAC für den eigentlichen Empfänger. Der kann den MAC und damit die Unversehrtheit der Übertragung prüfen und sieht an der vom Treuhänder hinzugefügten, ebenfalls vom MAC gesicherten Information, dass die Daten vom

---

[154] Eberhard von Faber: Vorlesungsskript; Technische Hochschule Brandenburg; modifiziert

[155] Wie der Prüfer den öffentlichen Schlüssel erhält, wird ausführlich in Kapitel 3.4 diskutiert.

[156] Bruce Schneier: Applied Cryptography, Protocols, Algorithms, and Source Code in C; Wiley, 1996, 2nd Edition, 675 pages, ISBN 0-471-12845-7

Unterzeichner stammen. Da er dem Treuhänder vertraut, gilt die Herkunft für ihn als bestätigt und die Daten sind unversehrt.

Man sieht an diesen Beispielen, dass der Übergang von einem kryptografischen Verfahren zu einem Protokoll fließend ist. Einige *Protokolle* werden später in Kapitel 8.4 bei den Anwendungen vorgestellt.

8.3 Schlüsselverwaltung (key management)

Rolle der Kryptografie

Kerckhoffs-Prinzip

Auguste Kerckhoff[157] formulierte 1883 unter anderem das folgende Prinzip: Die Sicherheit soll nur auf der Geheimhaltung der Schlüssel beruhen und nicht auf der Geheimhaltung des Algorithmus selbst.

Daraus ergeben sich weitreichende Konsequenzen: Durch den Einsatz kryptografischer Verfahren verlagert sich der Schutzbedarf von den Daten auf die kryptografischen Schlüssel. Die Sicherheit der Daten bzw. der kryptografisch gesicherten Kommunikation kann nicht höher sein als die der verwendeten Schlüssel.

Unter der Annahme, dass starke kryptografische Verfahren und wasserdichte Protokolle zum Einsatz kommen, verbleibt die Aufgabe, die kryptografischen Schlüssel zu sichern. Diese Aufgabe wird als Schlüsselmanagement oder Schlüsselverwaltung (key management) bezeichnet.

Key management

Der mit dem Schlüsselmanagement (key management) verbundene Aufwand wird häufig unterschätzt. Nicht der Einsatz einzelner Algorithmen beeinflusst das Systemdesign und die Gesamtarchitektur, sondern die Notwendigkeit, die Schlüssel zu verwalten. Und Letzteres ist eine komplexe Aufgabe. Dafür gibt es eine Reihe von Gründen:

- Aus Sicherheitsgründen soll ein Schlüssel nur für einen Zweck verwendet werden. Man will Nebeneffekte ausschließen. Dadurch steigt die Zahl der Schlüssel.
- Maschinen verstehen nicht und können vorhandene Kontextinformationen nicht würdigen. Die Kommunikation zwischen ihnen erfolgt aus technischen Gründen durch nacheinander wechselseitig ausgetauschte Nachrichten. Die Kommunikation ist sehr stark formalisiert. Die sogenannten Protokolle, die dies abbilden, führen zu einem nochmaligen Anstieg der Anzahl der benötigten Schlüssel, weil nicht nur die übertragenen Daten, sondern auch das Protokoll selbst Fehlern und Angriffen ausgesetzt sein kann.

---

[157] Auguste Kerckhoff, niederländischer Militärkryptologe

- Oft bestehen Systeme aus einer großen Anzahl von Geräten, die jeweils eigene, individuelle Schlüssel benötigen. Oder Systeme haben eine Vielzahl von Nutzern, die selbst Schlüssel benötigen oder über Geräte verfügen, die Schlüssel nutzen. Das multipliziert oder potenziert die Anzahl der Schlüssel.
- Jeder Schlüssel hat einen eigenen Lebenszyklus, der möglicherweise an jeder Stelle Lücken aufweisen oder sogar angegriffen werden kann.
- An einer bestimmten Stelle enden Technik und Automatisierung und der Mensch muss aktiv werden (eingreifen). Um seinen Einfluss auf die Sicherheit zu beschränken, sind weitere Vorkehrungen bei der Verwaltung der Schlüssel nötig.

Doch was ist Schlüsselmanagement?

Schlüsselmanagement (key management)

Gesamtheit der auf kryptografische Schlüssel und ihren gesamten Lebenszyklus bezogenen Aufgaben, bei denen der Sicherheit der Schlüssel ausnahmslos Aufmerksamkeit zu schenken ist.

Das Schlüsselmanagement oder die Schlüsselverwaltung (key management) umfasst die Erzeugung, Ableitung, Verteilung, Speicherung, Verwendung, Aktualisierung, Archivierung, und Vernichtung.

Diese acht Teilaufgaben werden nachfolgend beschrieben. Die Einteilung des Schlüsselmanagements bzw. die Aufteilung der Aufgaben kann je nach verwendeter Literatur auch anders ausfallen. Bei der Beschreibung kann bei weitem nicht auf alle Facetten eingegangen werden.

Schlüsselerzeugung

Teilaufgabe des *Schlüsselmanagements (key managements)*. Schlüssel für symmetrische Verschlüsselungsverfahren werden mit Hilfe von *Zufallszahlengeneratoren* erzeugt. Dies muss so erfolgen, dass der Schlüssel für einen Beobachter bzw. Angreifer nicht vorhersagbar ist und alle Werte gleich wahrscheinlich sind. Schlüssel für die asymmetrischen Verfahren RSA und DSS werden unter Verwendung von sehr großen Primzahlen erzeugt bzw. aus sehr großen Zahlen erzeugt, von denen man hinreichend sicher annehmen kann, dass sie Primzahlen sind. Die Erzeugung sollte sicherstellen, dass Schlüssel nicht doppelt vorkommen, da dies festgestellt und ausgenutzt werden kann.

Schlüsselableitung

Teilaufgabe des *Schlüsselmanagements (key managements)*. Schlüssel werden zum Beispiel berechnet, indem eine meist nicht geheime Information mit einem geheimen Systemschlüssel (master key) verschlüsselt wird. Wird ein abgeleiteter Schlüssel kompromittiert, so wird nicht die Sicherheit des gesamten Systems kompromittiert. Abgeleitete Schlüssel verringern also Risiken.

Mitunter werden Schlüssel auch aus völlig anderen geheimen Informationen wie zum Beispiel Passwörtern abgeleitet. Dann muss dabei sichergestellt werden, dass die abgeleiteten Schlüssel die kryptografisch erforderlichen Eigenschaften besitzen.

Schlüsselverteilung

Teilaufgabe des *Schlüsselmanagements (key managements).* Werden Schlüssel nicht am Ort ihrer Verwendung erzeugt, so müssen sie in elektronischer oder anderer Form dorthin übertragen werden. Dabei müssen Maßnahmen ergriffen werden, um die *Integrität* und in der Regel auch die *Vertraulichkeit* der Schlüssel zu gewährleisten. Die Gewährleistung der Integrität schließt auch das Ersetzen eines Schlüssels durch einen anderen aus.

Die Herstellung von Schlüsselträgern und die Einbringung von Schlüsseln in die IT-Komponenten und IT-Systeme, die sie verwenden werden, →*Personalisierung* genannt, sind generell kritische Vorgänge, die entsprechend abzusichern sind. Hier stößt die Absicherung mittels Kryptografie meist an ihre Grenzen und muss durch organisatorische und personelle Maßnahmen ergänzt bzw. sogar ersetzt werden.

Schlüsselspeicherung

Teilaufgabe des *Schlüsselmanagements (key managements).* Am Speicherort muss verhindert werden, dass Schlüssel unautorisiert ausgelesen, ersetzt oder verändert werden. Es ist die Aufgabe von →*Sicherheitsmodulen*, dies mittels eigener technischer Maßnahmen sicherzustellen, wobei gegebenenfalls auch auf organisatorische und personelle Maßnahmen in der Einsatzumgebung des Sicherheitsmoduls zurückgegriffen wird. *Hardware-Sicherheitsmodule (HSMs)* bieten einen physischen Schutz. Die für die Schlüssel erreichte Sicherheit ergibt sich immer aus der Gesamtbetrachtung der Bedrohungssituation und der Sicherheitsmaßnahmen des IT-Systems, das die Schlüssel speichert, und solchen, die die Einsatzumgebung bereitstellt.

Schlüsselverwendung

Teilaufgabe des *Schlüsselmanagements (key managements).* Primär geht es hierbei darum, die unautorisierte Nutzung der Schlüssel zu verhindern (falls sich dadurch ein Risiko ergibt). Dies erfolgt mit Mitteln wie der *Zugriffskontrolle*. Außerdem können während der Verwendung der Schlüssel Informationen über sie abfließen (*Inherent Information Leakage*) oder mit Hilfe zusätzlicher Manipulationen beschaffbar sein (*Forced Information Leakage*). Man spricht von Seitenkanalangriffen (side channel attacks). Sie werden durch die Art und Weise der Implementierung der kryptografischen Algorithmen und der Speicherung und Verwendung der Schlüssel abgewehrt.

Schlüsselaktualisierung

Teilaufgabe des *Schlüsselmanagements (key managements)*. Bei der Schlüsselaktualisierung wird ein Schlüssel gewechselt. Schlüssel können prinzipiell durch Ausprobieren gefunden werden (*Brute-Force Attacks*). Diese und andere Angriffe auf Schlüssel nehmen jedoch Zeit in Anspruch. Die Sicherheit eines Schlüssels wird daher erhöht, wenn die Dauer seiner Verwendung beschränkt wird und kürzer ist als ein Angriff in Anspruch nehmen würde.

Die Schlüsselaktualisierung kann dadurch erfolgen, dass die Kette *Schlüsselerzeugung - Schlüsselverteilung* erneut durchlaufen wird. Alternativ können die Kommunikationspartner einen neuen Schlüssel aus dem alten ableiten (*Schlüsselableitung*).

Schlüsselarchivierung

Teilaufgabe des *Schlüsselmanagements (key managements)*. Schlüssel sind systemkritische Daten, die für die reibungslose Funktion (*Verfügbarkeit* von IT-Services) benötigt werden. Daher werden gegebenenfalls Sicherheitskopien der Schlüssel angefertigt, oder sie sind Teil einer Sicherheitskopie, einer Auslagerungsdatei oder dergleichen. In diesen Fällen wirken die ursprünglich für die *Schlüsselspeicherung* definierten Sicherheitsmaßnahmen meist nicht mehr. Um den gleichen Schutz zu erreichen, müssen im Rahmen der Schlüsselarchivierung andere, wirksame Maßnahmen implementiert werden.

Eine spezielle Form der Schlüsselarchivierung ist die **Schlüsselhinterlegung (key escrow)**, bei der der Schlüssel zusätzlich einem Treuhänder ausgehändigt wird. Dieser darf den Schlüssel entsprechend vorher klar definierter Regeln verwenden. Mit der Schlüsselhinterlegung kann sich ein Unternehmen beispielsweise vor dem Verlust von Daten schützen, die Angestellte regelkonform mit den bereitgestellten Werkzeugen verschlüsselt haben.

Schlüsselvernichtung

Teilaufgabe des *Schlüsselmanagements (key managements)*. Nicht mehr benötigte Schlüssel müssen gelöscht werden, um Missbrauch zu verhindern. Löschmethoden, wie sie Betriebssysteme anbieten, löschen aber oft nur logische Zugriffsmöglichkeiten statt den eigentlichen Speicherort. Wird der eigentliche Speicherort gelöscht, so schützt auch das eventuell nicht ausreichend gegen Rekonstruktion des Schlüssels. Daher sind wirksame Maßnahmen nötig, um alle Speicherorte vollständig zu säubern. Man spricht auch von der *Wiederaufbereitung* von Speicher, die bei Schlüsseln besonders hohe Anforderungen zu erfüllen hat. Siehe dazu →*Media sanitizing*. Das Gleiche gilt, wenn *Hardware-Sicherheitsmodule* aus dem Verkehr gezogen und verschrottet werden. Hier kommen oft auch Verfahren der physischen Zerstörung des Moduls bzw. der Speichermedien zum Einsatz.

Schlüsselarten und Schlüsselattribute

Es gibt verschiedene Arten von Schlüsseln, und sie haben Attribute, wodurch sie sich weiter unterscheiden. Die damit verbundene Vervielfältigung der Anzahl der Schlüssel ist auf Regeln für ihre Verwendung zurückzuführen. Beispiele dafür sind:
a) Es soll auf universell genutzte Master-Keys verzichtet werden.
b) Jeder Schlüssel sollte nur zu einem Zweck verwendet werden.
c) Verschiedene Geräte sollen unterschiedliche Schlüssel verwenden.
d) Schlüssel dürfen nicht in unterschiedlichen Umgebungen eingesetzt werden, die ihnen unterschiedliche Schutzniveaus bieten.

Schlüsselarten

Unterscheidung von Schlüsseln hinsichtlich ihres Schutzbedarfes oder hinsichtlich des für ihre Einsatzumgebung charakteristischen Schutzniveaus.

IT-Systeme durchlaufen verschiedene Phasen in ihrem Lebenszyklus. Für den gleichen kryptografischen Zweck müssen unterschiedliche Werte für einen Schlüssel verwendet werden, damit die Phase mit einem geringeren Schutz eine andere Phase mit einem höheren nicht negativ beeinflussen kann. Man unterscheidet beispielsweise Testschlüssel und Produktionsschlüssel: Da mit Testschlüsseln keine wirklich kritischen Daten gesichert werden, ist ihr Schutzbedarf geringer als bei Produktionsschlüsseln, sodass davon auszugehen ist, dass ihr Sicherheitsniveau auch geringer ist. Zudem bieten Testsysteme und Produktivsysteme in der Regel unterschiedliche Schutzniveaus.

In vielen IT-Systemen bilden Schlüssel in der Weise eine Hierarchie, dass ihre Kompromittierung unterschiedlich große Auswirkungen haben würde. So gibt es zum Beispiel Systemschlüssel, die für die Absicherung sehr grundlegender Funktionen verwendet werden, und andere, die für sehr spezielle, stark eingegrenzte Zwecke eingesetzt werden. Systemschlüssel werden also besser geschützt werden als Anwendungsschlüssel, deren Einfluss auf einen einzelnen Vorgang beschränkt ist. Master-Keys oder Pre-Shared Keys werden zum initialen Aufbau einer sicheren Kommunikation genutzt, andere Schlüssel für die sichere Kommunikation von Daten.

Schlüsselattribute

Unterscheidung von Schlüsseln hinsichtlich ihrer Nutzung bzw. der Funktion, die sie in einem System übernehmen. Jeder Schlüssel soll nur zu einem Zweck verwendet werden. Schlüsselattribute kennzeichnen diese Zwecke.

Key-Encryption-Keys sind Schlüssel, die für die Verschlüsselung anderer Schlüssel verwendet werden, um letztere sicher zu übertragen (→*Schlüsselverteilung*). **Data Keys** (Daten-Schlüssel) werden dagegen verwendet, um Nutzdaten (Informationen) zu schützen. Diese können weiter unterschieden werden in solche, die für die Verschlüsselung, für einen *Message Authentication Code (MAC)* oder für die Authentisierung genutzt werden.

Schlüssel unterscheiden sich hinsichtlich ihrer Nutzungsdauer (oder Gültigkeitsdauer). **Sitzungsschlüssel (session keys)** sind kurzlebig; sie werden für eine bestimmte Kommunikation neu erzeugt (*Schlüsselerzeugung*) und danach gelöscht. Allgemein kann zwischen temporären und permanenten Schlüsseln unterschieden werden.

Für den Einsatz in *Sicherheitsmodulen* werden Schlüssel mit weiteren Attributen versehen. Beispielsweise wird zwischen Schlüsseln unterschieden, die **exportierbar** sind und unter bestimmten Bedingungen das Sicherheitsmodul verlassen dürfen und solchen für die dies nicht gilt (**nicht exportierbare Schlüssel**).

8.4 Anwendung und logische Angriffe

Zwei Anschauungsbeispiele

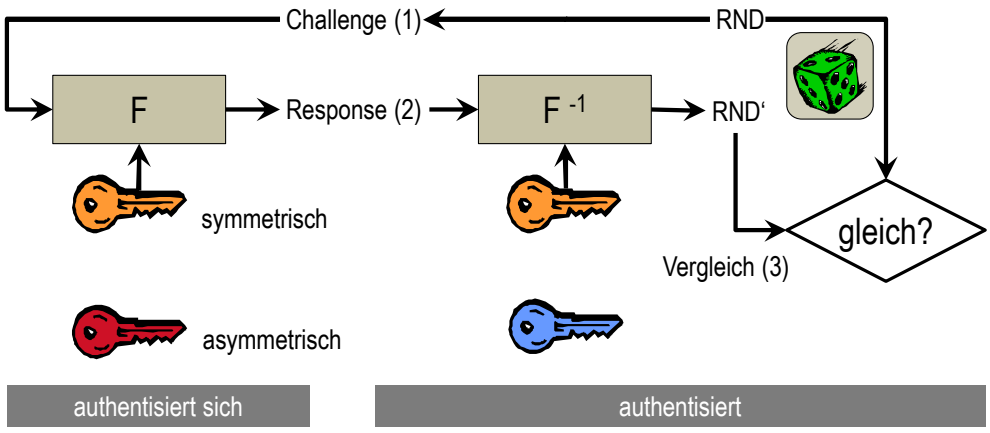


Abb. 62: Kryptografisches Challenge-Response-Verfahren

Challenge-Response-Verfahren

Das kryptografische Challenge-Response-Verfahren dient der *Authentisierung* eines Systems (links in Abb. 62) gegenüber einem anderen (rechts im Bild) durch den Besitz eines kryptografischen Schlüssels.

Es können symmetrische oder asymmetrische Verschlüsselungsalgorithmen zum Einsatz kommen. Siehe Abb. 62. Die Challenge ist eine Zufallszahl, die der Teilnehmer (links) mit der Aufforderung erhält, sie mit dem geheimen bzw. privaten Schlüssel zu verschlüsseln und zurückzusenden. Der andere Teilnehmer (rechts) führt die Entschlüsselung mit dem vereinbarten Schlüssel durch und vergleicht das Ergebnis mit der Challenge. Stimmen beide Werte überein, gilt der Teilnehmer (links) als authentisiert.

Ist die Authentisierung nicht nur einseitig, sondern beidseitig, so tauschen beide Parteien im nächsten Schritt die Rollen bzw. die zweite Challenge wird bereits zusammen mit der ersten Antwort versendet.

Bei dieser Form der Authentisierung wird das geheime Authentisierungsmerkmal nicht übertragen, sodass es auch nicht abgehört werden kann. Das Verfahren schützt auch gegen ein *Man-in-the-Middle*-Szenario, denn der Angreifer erhält keine Information, die es ihm gestattet, sich als rechtmäßige Partei auszugeben.

Wir führen das gerade verwendete Modell fort und stellen uns vor, dass die rechte Seite ein zentrales Authentisierungssystem ist, das sehr viele, eventuell tausende Geräte (links in Abb. 62) authentisieren soll, wobei ein symmetrisches Verschlüsselungsverfahren eingesetzt werden soll. Gemäß den Prinzipien des Schlüsselmanagements müssen alle Geräte einen eigenen Schlüssel verwenden. Ständig kommen jedoch Geräte hinzu und andere fallen aus und werden ersetzt. Das Problem: Die Schlüssel der Geräte müssten im zentralen Authentisierungssystem ständig nachadministriert werden. Doch es geht auch anders. Abb. 63 zeigt eine bessere Lösung in schematischer Weise.

Das Authentisierungssystem benötigt nur einen Schlüssel statt 1000 Schlüssel, um mit jedem der beispielsweise 1000 Geräte sicher zu kommunizieren, wie man es bei symmetrischer Verschlüsselung erwarten würde. Wie gelingt das?

- Die entscheidende Idee liegt nicht in der Änderung des Verfahrens zur Authentisierung, sondern in der Einbeziehung der Produktion der Geräte, während der die Geräte mit individuellen Schlüsseln ausgestattet werden (→*Personalisierung*).
- Dies unterstreicht einmal mehr die Bedeutung des *Schlüsselmanagements (key managements)*, das die Voraussetzungen für die sichere Kommunikation im Betrieb schafft und sich hier, leicht erkennbar, außerhalb des primären IT-Systems, in der Produktion der Geräte befindet. Schon in diesem sehr einfachen Fall nimmt das Schlüsselmanagement als vorbereitende Tätigkeit einen beträchtlichen Raum ein.
- Das hier verwendete Verfahren ist eine *Schlüsselableitung*. Jedes Gerät erhält einen individuellen Schlüssel, der durch Verschlüsselung der Seriennummer SN(x) des Gerätes x mit einem Systemschlüssel entsteht. Das zentrale Authentisierungssystem kann den Schlüssel eines jeden Gerätes wiederherstellen, indem es die Schlüsselableitung nachvollzieht.

Der übrige Teil ist eine normale Authentisierung mit dem kryptografischen *Challenge-Response-Verfahren* (vergleiche Abb. 62 und Abb. 63). Nur die Seriennummer SN(x) wird zusätzlich übertragen.

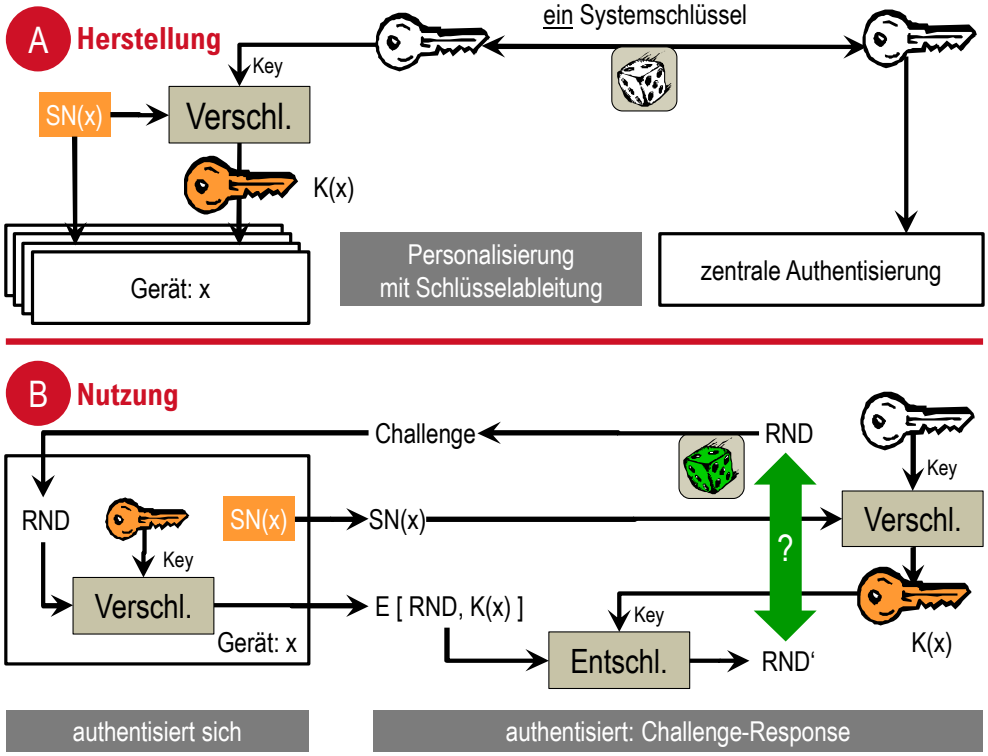


Abb. 63: Schlüsselableitung und Authentisierung sehr vieler Geräte

Protokoll, Nachrichten und Angriffe

Protokoll

Standardisierter Ablauf einer elektronischen Kommunikation zwischen Parteien. In jedem Schritt werden Nachrichten zwischen den Parteien ausgetauscht. Jede **Nachricht** ist in ihrer Form und Semantik (Bedeutung) einschließlich ihrer Bestandteile festgelegt. Die Nachrichtenbestandteile sind Nutzdaten, kryptografische Daten und gegebenenfalls Steuerinformationen. Für jede Nachricht ist außerdem spezifiziert, welche Operationen Sender und Empfänger ausführen. Das Gleiche gilt für den Ausgangszustand (Daten und Schlüssel vor Beginn der Kommunikation) und Endzustand einschließlich der Fehlerzustände (Daten und Schlüssel nach Abschluss der Kommunikation).

Es gibt zustandsbehaftete und zustandslose Protokolle. Bei **zustandsbehafteten Protokollen** hängt die Interpretation einer Nachricht durch den Empfänger von vorher ausgetauschten Nachrichten bzw. dem Status (Zustand) der Kommunikation ab. Bei **zustandslosen Protokollen** wird jede Nachricht eigenständig und unabhängig von vorher ausgetauschten Nachrichten behandelt. Im einfachsten Fall kann dies dadurch erreicht werden, dass der aktuelle Zustand und der Kontext der Kommunikation in jeder Nachricht mitgeführt werden.

Jetzt folgen einige Beispiele dafür, wie (kryptografisch gesicherte) Protokolle manipuliert werden können.

Man-in-the-Middle

Angriff auf ein Protokoll, bei dem sich der Angreifer („Mann in der Mitte") zwischen zwei Kommunikationsparteien stellt und die Kommunikation zwischen ihnen manipuliert. Er gibt sich gegenüber dem Sender als rechtmäßiger Empfänger und gegenüber dem Empfänger als rechtmäßiger Sender aus. Ein solcher Angriff ist immer dann möglich, wenn die Kommunikationsparteien ihr rechtmäßiges Gegenüber nicht oder noch nicht authentisiert haben.

Reflection

Angriff auf ein *Challenge-Response-Protokoll*, bei dem der Angreifer versucht, eine Kommunikationspartei dazu zu bringen, die Antwort (Response) auf die eigene Challenge zu liefern. Wird der Angreifer von der Kommunikationspartei zur Authentisierung aufgefordert, so sendet er die erhaltene Challenge an diese als Challenge (Aufforderung zur Authentisierung) zurück (reflection). Erhält er die richtige Antwort (response), so kann er sich seinerseits als rechtmäßiger Kommunikationspartner ausweisen. Dazu müssen zwei spiegelbildliche Protokolle parallel ablaufen. Bei der ersten Kommunikation will die zu betrügende Kommunikationspartei die andere Partei authentisieren, bei der zweiten wird er aufgefordert, sich zu authentisieren.

Wiedereinspielen (Replay)

Angriff auf ein Protokoll, bei dem der Angreifer Nachrichten einer Kommunikation zwischen rechtmäßigen Teilnehmern aufzeichnet und diese dann verwendet (wiedereinspielt), wenn er sich selbst als rechtmäßige Kommunikationspartei ausgibt. Dem wird dadurch begegnet, dass Nachrichten aus früheren Kommunikationen als fehlerhaft oder bereits genutzt erkannt werden. Das Konzept wird **Freshness** genannt. Dabei wird sichergestellt, dass ein schon verwendeter Sitzungsschlüssel (session key) nicht wiederverwendet wird. Oder es werden Folgenummern (Sequenzzähler) oder Zufallszahlen in gesicherter Form mitgeführt oder Zeitstempel verwendet.

Sitzungsübernahme (Session Hijacking)

Angriff auf ein Protokoll, bei dem der Angreifer eine rechtmäßig zustande gekommene Kommunikationsverbindung (session) analysiert, stört und schließlich die Rolle eines der Kommunikationspartner übernimmt bzw. eigene Datenpakete in die Kommunikation einschleust.

Dabei werden Schwächen in der Authentisierung der Kommunikationspartner ausgenutzt. Oft wird die Bestätigung der erfolgreichen Authentisierung (meist in Form eines „session cookie") gestohlen und missbräuchlich verwendet. **Cookies** werden verwendet, um in einem zustandslosen Protokoll den Zustand der Kommunikation zu speichern. Der Server erzeugt diese

Zustandsinformation, signiert sie und überträgt sie an den Client, der den Cookie mit der darin verpackten Zustandsinformation bei der nächsten Anfrage an den Server zurücksendet. Das (positive) Ergebnis der Authentisierung (*Authentication Assertion*) zählt auch zu den möglichen Zustandsinformationen.

Manipulation (Protokoll)

Angriff auf ein Protokoll, bei dem der Angreifer Nachrichtenteile verfälscht oder ersetzt, Fehler provoziert oder auf andere Weise auf eine Kommunikation zwischen rechtmäßigen Kommunikationsparteien Einfluss nimmt, um die Sicherheit der Kommunikation zu brechen.

Brute-Force Attack

Angriff auf ein Protokoll oder einen kryptografischen Algorithmus, bei dem der Angreifer ein Geheimnis (Schlüssel oder Passwort) durch systematisches Ausprobieren zu finden versucht. Dabei wird eine Testfunktion benötigt, die anzeigt, dass der richtige Wert gefunden wurde.

Besteht das Geheimnis aus Wörtern oder enthält es möglicherweise solche (wie es bei Passwörtern oft der Fall ist), so kann die Suche mit einem sogenannten **Wörterbuchangriff (dictionary attack)** erfolgen. Grundlage ist eine vorbereitete Wortliste (oder Liste bekannter Passwörter), die automatisiert abgearbeitet wird, wobei Varianten automatisch erzeugt werden.

8.5 Physische Angriffe

Im vorhergehenden Kapitel 8.4 wurden bereits einige Angriffe vorgestellt. Sie können in der Regel durchgeführt werden, ohne dass sich Angreifer oder seine Werkzeuge in räumlicher Nähe zu den *Sicherheitsmodulen* befinden müssen, die die Schlüssel speichern und kryptografische Operationen ausführen. Daher wurden sie als logische Angriffe bezeichnet. Bei den im Folgenden beschriebenen Angriffen ist dies nicht der Fall. Der Angreifer muss grundsätzlich direkten physischen Zugang zum Sicherheitsmodul haben.

Die fünf grundlegenden Angriffstypen sind auch im „Smartcard IC Platform Protection Profile“ beschrieben.[158] Weitere, spezielle Angriffe wie DPA und DFA werden dabei ebenfalls kurz erläutert. Danach werden Fragen der Modellierung diskutiert und exemplarisch ein Bedrohungsmodell für Embedded Systems vorgestellt.

---

[158] Smartcard IC Platform Protection Profile; BSI-PP-0002-2001 für die Version 2.1 der Common Criteria (CC), aktualisiert zu BSI-CC-PP-0035-2007 für Version 3.1 R1 der CC und aktualisiert zu BSI-CC-PP-0084-2014 für Version 3.1 R4 der CC.
Der Autor dieses Buches hat BSI-PP-0002 im Auftrag von und in Zusammenarbeit mit den Herstellern Atmel Smart Card ICs, Hitachi Europe Ltd., Infineon Technologies AG und Philips Semiconductors entwickelt.

Malfunction

Angriff auf die korrekte Funktionsweise eines Sicherheitsmoduls durch Manipulation seiner Betriebsbedingungen mit dem Ziel, Sicherheitsfunktionen temporär unwirksam zu machen oder dauerhaft für anschließende Angriffe zu schwächen. Der Angreifer betreibt das Sicherheitsmodul außerhalb der spezifizierten Bedingungen in der Einsatzumgebung (zum Beispiel Temperatur), stört die Spannungsversorgung (zum Beispiel durch Glitches) oder manipuliert den zeitlichen Verlauf der elektronischen Kommunikation mit dem Modul.

Physical Manipulation

Angriff auf die physische Integrität eines Sicherheitsmoduls durch mechanisches, physikalisches und chemisches Einwirken mit dem Ziel, Sicherheitsfunktionen meist dauerhaft unwirksam zu machen oder zu schwächen. Der Angriff zielt auf Hardware, Software und/oder Daten. Der gezielten Manipulation geht eine Analyse der Konstruktion voraus (reverse engineering), da diese aus Sicherheits- und anderen Gründen vom Hersteller nicht offengelegt wird. Die Analyse der Konstruktion erfordert oft ebenfalls physische Manipulationen, die nicht selten zerstörerisch sind.

Physical Probing

Angriff auf die Vertraulichkeit von Daten oder Teilen einer Software durch physikalische Messungen mit dem Ziel, die Daten missbräuchlich zu verwenden oder anhand der Software Hilfestellungen für nachfolgende Angriffe zu erhalten. Der Angreifer kontaktiert hierzu Leitungen im Inneren des Sicherheitsmoduls elektrisch, misst Potenziale auf andere Weise oder analysiert Stoffe, Geometrien oder andere Größen, die genutzt werden, um Informationen zu kodieren. Die Messungen erfolgen, während das Sicherheitsmodul in Betrieb ist oder im ausgeschalteten, stromlosen Zustand. Den Messungen geht eine Analyse der Konstruktion voraus (reverse engineering), da diese aus Sicherheits- und anderen Gründen vom Hersteller nicht offengelegt wird. Oft sind zur Analyse der Konstruktion oder zur Vorbereitung der Messungen *physische Manipulationen* am Sicherheitsmodul nötig.

Abuse Functions

Angriff auf die Vertraulichkeit oder Integrität von Daten und die Integrität (Funktionsweise) von Sicherheitsfunktionen durch die missbräuchliche Nutzung von Funktionen des Sicherheitsmoduls mit dem Ziel, Daten missbräuchlich zu verwenden oder Sicherheitsfunktionen zu deaktivieren oder zu modifizieren, um nachfolgende Angriffe zu ermöglichen. Bei den missbräuchlich genutzten Funktionen des Sicherheitsmoduls handelt es sich zum Beispiel um solche, die der Hersteller für Testzwecke oder für die Fehlersuche implementiert hat. Sind diese im Auslieferungszustand des Sicherheitsmoduls deaktiviert, so ist eine Manipulation nötig, um sie wieder verfügbar zu machen.

Inherent Information Leakage

Angriff auf die Vertraulichkeit von Daten durch Analyse von kontaktbehaftet oder kontaktlos erfassbaren Messwerten, die das Sicherheitsmodul zwangsläufig im Betrieb erzeugt, mit dem Ziel, die Daten missbräuchlich zu verwenden. Eine kontaktlos erfassbare Messgröße ist die elektromagnetische Abstrahlung. Zu den Größen die kontaktbehaftet messbar sind, gehören Variation des Stromverbrauchs, Dauer oder Zeit zwischen Ereignissen und dergleichen. Solche Größen müssen ursächlich mit den verarbeiteten Daten verbunden sein, d.h., mit ihnen korrelieren (direkt oder statistisch).

Diese Form des Angriffs zählt zu den Seitenkanalangriffen (side channel attacks).

Bei Verfahren wie der **Simple Power Analysis (SPA)** genügen wenige Datenpunkte (Wiederholungen der Messung), da nur das unvermeidliche Rauschen rechnerisch beseitigt werden muss. Das Prinzip beruht darauf, dass ein Transistor oder eine elektronische Schaltung einen anderen Stromverbrauch hat, wenn sie eine Null oder eine Eins verarbeitet. Wenn der Ablauf der Operation genau bekannt ist und mit dem zeitlichen Verlauf des Stromverbrauchs übereinandergelegt werden kann, kann ein Bit oder das Hamming-Gewicht eines Bytes oder Wortes bestimmt werden. Das **Hamming-Gewicht** ist die Anzahl der Einsen in einem Byte, Wort usw.

Bei der **Differential Power Analysis (DPA)** werden sehr viele Datenpunkte (Millionen oder Milliarden Messungen des Stromverbrauchs beim gleichen Vorgang) benötigt, die statistisch analysiert werden. Dabei wird die Berechnung der kryptografischen Operation mit einer gewählten Schlüsselhypothese (mathematisches Modell) mit dem zeitlichen Verlauf des gemessenen Stromverbrauchs (reale Berechnung) korreliert. Dies wird für alle Schlüsselhypothesen und Bits wiederholt. Deutlich hervorstechende starke Korrelationen zeigen, dass die Hypothese richtig war und weisen auf den Schlüsselwert.

Timing Attacks nutzen den Umstand aus, dass die Zeit für die Ausführung einer Operation im gegebenen Fall vom Eingabewert abhängt. Da zum Beispiel bei einer Exponentialfunktion der Exponent bitweise verarbeitet wird, ist die Verarbeitung einer Null viel schneller als die einer Eins.

Forced Information Leakage

Angriff auf die Vertraulichkeit von Daten durch Analyse von Ausgaben des Sicherheitsmoduls oder von kontaktlos erfassbaren Messwerten, die das Sicherheitsmodul zwangsläufig im Betrieb erzeugt, mit dem Ziel, die Daten missbräuchlich zu verwenden. Normalerweise gibt das Sicherheitsmodul keine vertraulichen Informationen preis, tut dies jedoch, weil der Angreifer Fehlfunktionen herbeiführt (→*Malfunction*) oder das Sicherheitsmodul manipuliert hat (→*Physical Manipulation*).

Diese Form des Angriffs zählt zu den Seitenkanalangriffen (side channel attacks).

Differential Fault Analysis (DFA) ist ein konkretes Beispiel.[159] Dabei werden bei der Wiederholung einer kryptografischen Berechnung mit gleichen Eingangsparametern Fehler induziert, die möglichst am Ende der Berechnung auftreten und nicht den Schlüssel treffen. Aus dem Vergleich der verschiedenen Ausgabedaten (fehlerfreie und fehlerbehaftete Chiffrate) können Rückschlüsse auf den verwendeten Schlüssel gezogen bzw. dieser berechnet werden. DFA beruht im Wesentlichen auf den bekannten Prinzipien der Differentiellen Kryptoanalyse.

Funktionsprinzip: Ein Element für die Sicherheit von kryptografischen Algorithmen besteht beispielsweise darin, dass man allein aus dem Ergebnis einer Exklusiv-Oder-Verknüpfung (XOR) nicht auf einen der beiden Eingangswerte schließen kann. Dadurch ist auch der Rückschluss auf den Pfad mit dem Schlüssel versperrt. Ist der andere Eingangswert jedoch gleich und das beobachtete Ergebnis der Exklusiv-Oder-Verknüpfung (XOR) durch den Fehler verschieden, so kann die Unkenntnis des gleichen Eingangswertes eliminiert und der Pfad zum Schlüssel verfolgt werden.

Messung und Analyse vereinfachen sich, wenn es gelingt, permanente Fehler herbeizuführen, bestimmte Datenleitungen also zu kappen.[160] Solche Angriffe könnte man entsprechend **Permanent Fault Analysis (PFA)** nennen, obwohl auch diesem Angriff Differenzen zugrunde liegen.

Um solche physischen Angriffe durchführen und zum Beispiel temporäre Fehler hervorrufen zu können, müssen geeignete Methoden gefunden werden, dies zu erreichen. Ein Modell kann dabei helfen, in systematischer Weise nach Wegen zu suchen.

Bedrohungsmodell

Ein Bedrohungsmodell fasst aus Sicht eines Angreifers potentielle Möglichkeiten und Umstände zusammen, die ausgenutzt werden könnten, um die Sicherheit zu kompromittieren.

Ein vollständiges (Angriffs-)Szenario entsteht erst durch die Aneinanderreihung von sehr vielen einzelnen Aktivitäten. Werden diese in Form einer logischen Folge und Hierarchie strukturiert, spricht man auch von einem **Bedrohungsbaum**. Einzelne Wege durch diesen Baum bilden Angriffspfade.

---

[159] Eli Biham, Adi Shamir: Research Announcement: A New Cryptographic Attack on DES; a) Notiz vom Freitag, 18. Oktober 1996, 16:58:50 (+0200); Risk Digest 18.54 und b) Entwurf vom 18. Oktober 1996

[160] Eli Biham und Adi Shamir: Differential Fault Analysis Revisited; Beitrag auf dem Fast Software Encryption Workshop (FSE4); 20.-22. Januar 1997, Haifa, Israel

Abb. 64 zeigt ein Bedrohungsmodell für Eingebettete Systeme (*Embedded Systems).* Die meisten →*Sicherheitsmodule* sind eingebettete Systeme.

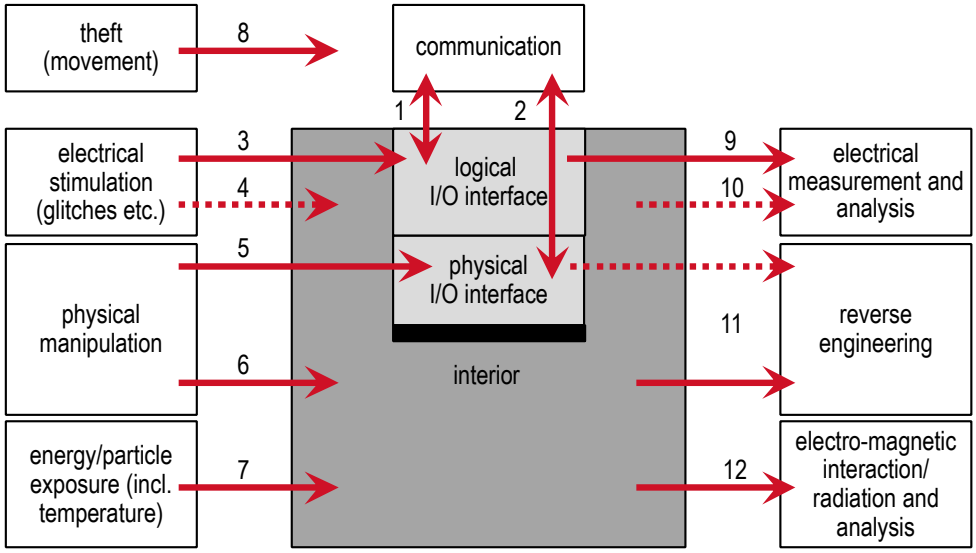


Abb. 64: Bedrohungsmodell für Embedded Systems[161]

Mit Hilfe dieses Modells können diverse Angriffsszenarien (Bedrohungsszenarien) entwickelt werden. Elektronikingenieure wissen mit Nr. 3 und 9 in Abb. 64 umzugehen. Physiker entwickeln Ideen, wie Nr. 7 und 12 genutzt werden könnten. Informatiker bedienen Nr. 1 und 2. Chipdesigner und Halbleiter-Prozesstechnologen sind für die Arbeit an Nr. 6 und 11 prädestiniert. Und Mathematiker (Kryptologen) liefern Basisideen, wo Algorithmen möglicherweise Schwachstellen aufweisen.

Abb. 64 fasst nur Einflussmöglichkeiten und Möglichkeiten zur Informationsgewinnung zusammen. Für jede dieser Kategorien können diverse Verfahren entwickelt werden, die, für sich allein genommen, bereits komplex sein können. Oft müssen jedoch mehrere Verfahren kombiniert werden. Eine solche Kombination stellt dann ein Angriffsszenario dar, wobei keinesfalls garantiert ist, dass dieses durch einen Angreifer erfolgreich durchgeführt werden kann. Dies korrekt einzuschätzen, obliegt den Verteidigern.

Literatur und Bildnachweise

Besonders ein solches Buch, das sich zur Aufgabe macht, Definitionen von Fachbegriffen zu geben, kann nicht geschrieben werden, ohne dass der Autor vielfältige Literatur gelesen hätte – in der langen Zeit der Tätigkeit auf diesem Gebiet, bei der Erstellung von Lehrunterlagen für Studierende und beim Schreiben dieses Buches.

---

[161] Eberhard von Faber: Vorlesungsskript; Technische Hochschule Brandenburg

Die Definitionen sollen ja den Stand der Technik korrekt wiedergeben und konsensfähig sein. Das bedeutet auch, dass Begriffe und Zusammenhänge auch in anderen Veröffentlichungen so oder ähnlich vorkommen können – ja müssen.

Daher wurde wie folgt verfahren: (1) Literatur ist an den Stellen als Fußnote angegeben, wo ich sie direkt verwendet habe bzw. mir bewusst ist, dass Begriff, Definition oder sonstige Beschreibungen auf eine solche Quelle zurückgeführt werden können. (2) Gilt dies in gleicher Weise für Institutionen oder Einzelpersonen, so sind diese meist direkt im Text angegeben. (3) Die folgende Liste enthält Literaturhinweise und wiederholt nicht die Quellenangaben in diesem Kapitel. (4) Falls nicht anders angegeben, wurden Abbildungen extra für dieses Buch erstellt.

[1] Bruce Schneier: Applied Cryptography, Protocols, Algorithms, and Source Code in C; Wiley, 2015, 784 pages, ISBN 978-1-119-09672-6

[2] Norbert Pohlmann: Cyber-Sicherheit, Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung; Springer-Vieweg, Wiesbaden, 2019, 620 Seiten, 348 Abbildungen, ISBN 978-3-658-25397-4

[3] Security IC Platform Protection Profile with Augmentation Packages Version 1.0; BSI-CC-PP-0084-2014, EUROSMART für Inside Secure, Infineon Technologies AG, NXP Semiconductors Germany GmbH und STMicroelectronics.

[4] Claudia Eckert: IT-Sicherheit, Konzepte – Verfahren - Protokolle; Oldenburg Wissenschaftsverlag, München, 2018, ISBN 978-3-11-055158-7

Elektronisches Zusatzmaterial
Die Abbildungen sind als PowerPoint-Datei kapitelweise über https://link.springer.com/ auf der Seite des eBooks abrufbar.

9 Kommentiertes Abkürzungsverzeichnis

Tipp für eBook-Leser:

> Suchen Sie nach „>“-**Buchstabe** (zum Beispiel „**>B**“ oder „**>H**“), um zu dem entsprechenden Buchstaben bzw. der Rubrik zu gelangen. Diese Lösung funktioniert von jeder Stelle im eBook aus und ist wahrscheinlich schneller und für die meisten Leser einfacher, als zwischen 26 Lesezeichen zu navigieren (die daher im eBook nicht angelegt wurden).
>
> (Um im Stichwortregister (Kapitel 10) zu navigieren, suchen Sie bitte nach „**=B**“ oder „**=H**“ usw.)

In allen Branchen und zu allen Themen verwenden Fachleute Abkürzungen. Sie sind kurz. Wortungetüme werden ersetzt. Aneinanderreihungen von Wörtern schrumpfen zu einem Begriff zusammen. Die Nutzung von Abkürzungen beschleunigt die Kommunikation und hilft dabei, sich auf das Wesentliche zu konzentrieren.

Auf der anderen Seite führen Abkürzungen leicht zu Missverständnissen, weil manche Abkürzungen mehrere Bedeutungen haben. Das macht auch eine Suche im Internet schwierig. Versuchen Sie doch einmal, eine harmlose Abkürzung wie AMS zu suchen, ohne dass Sie die Suche mit einem Zusatz eingrenzen können. Sie wissen ja schließlich nicht, was AMS bedeutet. Die Vieldeutigkeit stellt in diesem Buch kaum ein Problem dar, da im Wesentlichen nur die Informationstechnologie und die IT-Sicherheit betrachtet werden.

Dennoch gibt es viele Verzeichnisse – auch im Internet. Viele erklären jedoch nur, wofür die Buchstaben stehen, und nicht, was der Begriff bedeutet. Das folgende Abkürzungsverzeichnis bietet beides. Suchen Sie dagegen in elektronischen Dokumenten, so ergibt sich ein weiteres Problem, weil Abkürzungen mit zwei oder drei Buchstaben oft viele falsche Treffer liefern. „IP“ ist ein gutes Beispiel dafür.

Natürlich musste die in diesem Buch verwendete thematische Sortierung aufgegeben werden. Man lernt Abkürzungen ja nicht systematisch, man schlägt sie gegebenenfalls nach. Es gibt einige Überschneidungen mit den anderen Kapiteln in diesem Buch: Einige Abkürzungen werden natürlich schon in den anderen Kapiteln aufgeschlüsselt und erklärt. Dieses Kapitel eignet sich zum Nachschlagen und enthält aber weit mehr Abkürzungen als im ersten Teil des Buches zu finden sind.

E. von Faber, *IT und IT-Sicherheit in Begriffen und Zusammenhängen*,
Edition <kes>, https://doi.org/10.1007/978-3-658-33431-4_9

Katalog (A bis Z)

>>1-10 und Sonderzeichen

2G	Mobilfunknetze der zweiten Generation (GSM: Global System for Mobile Communications)
3G	Mobilfunknetze der dritten Generation (UMTS: Universal Mobile Telecommunication System)
4G	Mobilfunknetze der vierten Generation (LTE-Advanced: Long Term Evolution)
4EP	Four eyes principle; Vieraugenprinzip; Vorsichtsmaßnahme, die für die Durchführung einer Aktion die Zustimmung von zwei Personen verlangt
5G	Mobilfunknetze der fünften Generation; baut auf LTE auf
.Net	gesprochen: Dot Net; *Middleware* für Computersysteme; stellt *Anwendungen* diverse Funktionen zur Verfügung, die das *Betriebssystem* nicht bietet

>>A<<

ABAP	Advanced Business Application Programming; Programmiersprache für die Herstellung und Anpasssung von geschäftlichen SAP-Anwendungen
ACL	*Access Control List* (Zugangsliste); enthält die Rechte für die Zugriffskontrolle und speichert sie objektbezogen
AES	Advanced Encryption Standard; symmetrischer Chiffrieralgorithmus; ersetzte ab 2000 den bis dahin dominierenden DES (Data Encryption Standard); der AES ist in FIPS 197 spezifiziert
AMS	Application Management Service; Verwaltung und Pflege von Anwendungssoftware
ANSI	American National Standards Institute; US-amerikanisches Normungsinstitut (dem DIN in Deutschland ähnelnd)
API	Application Programming Interface; Schnittstelle einer Software, über die andere Programme mit der Software kommunizieren können
APT	Advanced Persistent Threat; Angriff auf ein IT-System, der sich dadurch auszeichnet, dass er lange dauert, aus mehreren systematisch aufeinander aufbauenden Schritten besteht und zum Teil ausgeklügelte Methoden verwendet

ARM Advanced RISC Machines; Architektur von Prozessoren (CPU), die unter anderem bei Smartphones, Tablets, eingebetteten Systemen und sogar Servern und Höchstleistungsrechnern sehr verbreitet ist

ASP Application Service Provider; IT-Dienstleister, der die Nutzung von Anwendungssoftware auf Mietbasis bzw. als Dienstleistung anbietet

ATM Asynchronous Transfer Mode; Technologie (Protokoll) für Weitverkehrsnetze (WAN), das virtuelle Kanäle unterstützt und damit erlaubt, dass sich mehrere (Anwender-)Unternehmen eine Verbindung teilen können

>>B<<

BAFO *Best and Final Offer*; verbessertes, finales und endgültig bindendes Angebot

BCM Business Continuity Management; umfasst Vorkehrungen für die Minimierung von Auswirkungen als Folge von Unfällen, Pandemien usw. sowie dem Ausfall von Personal, Gebäudetechnik, Informationstechnologie usw.

BDSG Bundesdatenschutzgesetz; Gesetz der Bundesrepublik Deutschland

BIOS Basic Input Output System; Firmware älterer PCs, siehe →*BIOS*

BNetzA Bundesnetzagentur; Regulierungsbehörde (der Bundesrepublik Deutschland); früher: Regulierungsbehörde für Post und Telekommunikation (RegTP)

BRM *Business Relationship Management*; IT-Service-Management-Prozess in ISO/IEC 20000 und ITIL®[162]

BSI Bundesamt für Sicherheit in der Informationstechnik; Bundesbehörde (der Bundesrepublik Deutschland), die u.a. Handreichungen zur IT-Sicherheit veröffentlicht, Sicherheitsstandards für Behörden in Deutschland herausgibt und sich an der Standardisierung und Überprüfung von Verfahren der Kryptografie beteiligt

BSI British Standards Institute; Normungsinstitut

BYOD Bring Your Own Device; erlaubte Nutzung privater Geräte im geschäftlichen Umfeld

>>C<<

CA *Certification Authority*; Stelle, die digitale (Schlüssel-)Zertifikate ausstellt

[162] ITIL® und IT Infrastructure Library® sind seit 2013 eine Marke von Axelos.

CAB	*Change Advisory Board*; Gremium der betriebsverantwortlichen Einheit zur Freigabe von normalen Änderungen (Changes) im IT-Betrieb
CAN	Controller Area Network; Bussystem für die Verbindung von Komponenten in einem Kraftfahrzeug
CAPEX	Capital Expenses (siehe auch unter *CAPEX*); Kapitalausgaben, Einmalkosten bzw. Investitionen; Gegensatz: OPEX, laufende Betriebsausgaben
CASB	*Cloud Access Security Broker*; Lösung, die Sicherheitsrichtlinien durchsetzt, die der Cloud-Computing-Service nicht unterstützt
CBI	Customer Business Impact; misst die Schwere eines Vorfalls (Ausfall oder Beeinträchtigung) für den Anwender
CC	Common Criteria for Information Technology Security Evaluation; internationale Kriterien für die Bewertung und Zertifizierung der IT-Sicherheit vor allem von Produkten
CCAB	Central Change Advisory Board; zentrales Gremium zur Freigabe komplexerer und risikobehafteter Änderungen (Changes) im IT-Betrieb
CERT	Computer Emergency Response Team; verwaltet Informationen über Schwachstellen, bewertet diese und unterstützt bei deren Behebung; manche Teams übernehmen weitere Aufgaben und gleichen eher einem →*Security Operations Center (SOC)*
CI	*Configuration Item*; Komponenten in einem bzw. für ein IT-System
CIA	*Confidentiality*, *Integrity*, *Authenticity*
CI/CD	Corporate Identity/Corporate Design; Idee, einer Firma oder Institution einen individuellen Charakter im Sinne einer Persönlichkeit zu geben und diesen durch Stilvorgaben auszudrücken und zu kommunizieren zum Beispiel durch firmenspezifische Schriftarten und Farben, Logos und Gestaltungsrichtlinien für Schriftsätze sowie die Verwendung bestimmter Bilderwelten
CIO	Chief Information Officer; höchste Führungskraft, die für die Informations- und Kommunikationstechnologie verantwortlich ist
CISO	Chief Information Security Officer; höchste Führungskraft, die für die Informationssicherheit bzw. IT-Sicherheit verantwortlich ist
CIX	Commercial Internet eXchange (CIX); größerer, kommerzieller *Austauschpunkt* im Internet
CMDB	Configuration Management Database; Verzeichnis aller Configuration Items (Komponenten in einem bzw. für ein IT-System) und ihrer Beziehungen untereinander; siehe auch →*CMDB*
CMO	*Current Mode of Operation*; aktueller Betriebsmodus, beim Outsourcing der Zustand der IT bei der Übernahme durch den IT-Dienstleister

CMS Configuration Management System; System zur Verwaltung von Versionen, zur Identifikation und zum Nachvollziehen von Änderungen und Freigaben sowie zur Identifikation von Komponenten und Systemen

COBIT Control Objectives for Information and Related Technology; COBIT (es wird fast ausschließlich die Abkürzung benutzt) wurde durch die ISACA entwickelt; COBIT wurde entwickelt, um Unternehmen ein umfassendes Rahmenwerk zur Verfügung zu stellen, das es ihnen ermöglicht, Informationen und zugehörige Technologie ganzheitlich zu regeln und zu verwalten - einschließlich der IT-Sicherheit.

COTS Component off-the-shelf oder: Commercial off-the-shelf; in Serie gefertigtes gleichartiges Produkt

CPE Customer Premise Equipment; Bezeichnung von Telekommunikationsunternehmen bzw. Internet Service Providern für Geräte, die beim Kunden stehen

CPU Central Processing Unit; Zentraleinheit und Herzstück eines Computers

CRM *Customer Relationship Management*; Verwaltung von Kundendaten und Informationen über Geschäftsbeziehungen bzw. Anwendungssoftware dafür

CSC Cloud Service Customer; Anwender eines *Cloud-Computing*-Service und Kunde des Cloud Service Providers (CSP)

CSO Chief Security Officer; höchste Führungskraft, die für die Sicherheit verantwortlich ist

CSP Cloud Service Provider; der IT-Dienstleister, der den *Cloud-Computing*-Service herstellt

>>D<<

DBMS Database Management System; Datenbankverwaltungssystem: Software, die die Speicherung von Daten in einer →*Datenbank* bewerkstelligt; das DBMS umfasst nicht den Datenspeicher (Datenbank)

DE-CIX Deutscher Commercial Internet Exchange; größter Internetknoten, über den Internet Service Provider (ISP) Daten austauschen

DES Data Encryption Standard; symmetrischer Chiffrieralgorithmus; wurde ab 2000 durch den AES (Advanced Encryption Standard) ersetzt; der DES ist in FIPS 81 spezifiziert

DFA *Differential Fault Analysis (DFA)*; Seitenkanalangriff (side channel attack), bei dem der Angreifer Fehler induziert, um an Informationen über geheime Schlüssel zu gelangen

DDoS Distributed Denial-of-Service Attack; Angriff, der von mehreren Punkten aus versucht, ein System durch eine hohe Zahl von Anfragen in kurzer Zeit durch Überlastung zum Erliegen zu bringen; siehe auch: *Denial-of-Service-Protection*

DHCP Dynamic Host Configuration Protocol; über das Protokoll bzw. den DHCP-Server wird einem Gerät eine Internet-Adresse (IP-Adresse) dynamisch zugewiesen

DMS Document Management System; Dokumentenmanagementsystem: Kombination von Abläufen, Regeln und Werkzeugen für die Verwaltung von Dokumenten; meist ist nur das Werkzeug (Verwaltungssoftware) gemeint

DMZ Demilitarized Zone; demilitarisierte Zone; Netzwerkbereich zwischen dem unsicheren externen Weitverkehrsnetz (meist Internet) und dem internen Netz, der aus dem Weitverkehrsnetz zwar erreichbar, aber bereits abgeschirmt ist; durch die Verlagerung in die DMZ werden Services extern verfügbar, ohne das interne Netz dazu öffnen zu müssen und so zu gefährden; außerdem können dort Angriffe erkannt werden, bevor sie das interne Netz erreichen.

DNL Direct Network Link; Standleitung: physische Netzwerkverbindung, die einer Anwenderorganisation exklusiv zur Verfügung steht

DNS Domain Name System; hierarchisches, verteiltes System von Servern, die es insbesondere gestatten, mit einem Netzwerk verbundene Computer und andere Ressourcen zu erreichen, indem ihre Namen in deren numerische IP-Adressen umgewandelt werden, die auf der Ebene der Kommunikationsprotokolle benötigt werden

DoS Denial-of-Service Attack; Angriff, bei dem versucht wird, ein System durch eine hohe Zahl von Anfragen in kurzer Zeit durch Überlastung zum Erliegen zu bringen; siehe auch DDoS bzw. *Denial-of-Service-Protection*

DPA *Differential Power Analysis*; Angriff, bei dem der Stromverbrauch analysiert wird, um Informationen über den geheimen Schlüssel zu erhalten

DRM Digital Rights Management; Verfahren, um die unerlaubte Weitergabe von Medieninhalten zu verhindern bzw. mindestens erkennen zu können; siehe auch EDRM

DSGVO Datenschutz-Grundverordnung; eine Verordnung der Europäischen Union zum Datenschutz (englisch: General Data Privacy Protection, GDPR)

DSS Digital Signature Algorithm; kryptografischer Algorithmus, mit dem digitale *Signaturen* erzeugt und verifiziert werden können

DSL Digital Subscriber Line; digitale Teilnehmerleitung; breitbandiger Anschluss von Teilnehmern in der Regel an das Internet bzw. bis zur

nächsten Vermittlungsstelle, die dann die Verbindung zum Internet herstellt

>>E<<

ECAB — Emergency Change Advisory Board; Gremium zur Freigabe von zeitkritischen Änderungen (Emergency Changes) im IT-Betrieb

ECC — Elliptic Curve Cryptography; elliptische Kurven; kryprographischer Algorithmus, mit dem digitale *Signaturen* erzeugt und verifiziert werden können

EDIFACT — Electronic Data Interchange for Administration, Commerce and Transport; branchenübergreifender Standard für den elektronischen Austausch von geschäftlichen Dokumenten

EDRM — *Enterprise Digital Rights Management*; Verfahren, das verhindert, dass autorisierte Nutzer Dateien einschließlich E-Mails an unautorisierte Nutzer weitergeben; die Daten sind beim Speichern und Übertragen verschlüsselt; um sie verarbeiten (anzeigen, drucken usw.) zu können, stellt ein Server den Schlüssel zur Verfügung, nachdem der Nutzer als autorisiert erkannt wurde

EFT — Electronic Funds Transfer; Verfahren zum Austausch von Zahlungsinformationen zwischen Banken

EMV — Elektromagnetische Verträglichkeit sowie frühere Abkürzung für Europay, Mastercard, VISA, einem Verbund von Zahlungsverkehrsdienstleistern bzw. Bezeichnung für die Standards im Zahlungsverkehr, den diese entwickelt haben

ERP — Enterprise Resource Planning; System bzw. Software für die Verwaltung (Bedarf, Bestand, Planung) von Material, Personal, Kapital und sonstigen Ressourcen in unternehmerischen Produktionsprozessen

ESARIS — Enterprise Security Architecture for Reliable ICT Services (→*ESARIS*)

ETSI — European Telecommunications Standards Institute; europäische Normungsorganisation

>>F<<

FAQ — Frequently Asked Questions; Sammlung von Antworten auf (häufig gestellte) Fragen; dient der Selbsthilfe von Nutzern und reduziert damit die Anfragen bei der Hotline bzw. dem Support

FIPS — Federal Information Processing Standard; Standards der US-Bundesbehörde NIST für Behörden in den USA, die jedoch auch international Bedeutung haben; Beispiele sind FIPS 81, der den Verschlüsselungsalgorithmus DES spezifiziert, sowie FIPS 197 für den AES

FMO Future Mode of Operation; Zustand nach der *Transformation*, d.h. nach Abschluss aller Modernisierungs- und Anpassungsmaßnahmen

FLOPS Floating Point Operations per Second; Fließkommaoperationen pro Sekunde; Maß für die Rechenleistung eines Computers

FTA Fault Tree Analysis; Fehlerbaumanalyse; Methode zur Bestimmung der Ausfallwahrscheinlichkeit bzw. zur Analyse der Verfügbarkeit oder Zuverlässigkeit

FTP File Transfer Protocol; Protokoll zum Austausch von Dateien über das Internet

>>G<<

GDPR General Data Privacy Protection; Datenschutz-Grundverordnung (DSGVO), eine Verordnung der Europäischen Union zum Datenschutz

GNU UNIX-ähnliches Betriebssystem auf Basis quelloffener Software (Open-Source); das Projekt ist auch Urheber der GNU Public License (GPL)

GRC *Governance, Risk and Compliance*; definiert Handlungsebenen für die korrekte Unternehmensführung

GSM Global System for Mobile Communication; Mobilfunkstandard der zweiten Generation (2G)

GPL GNU Public License; Softwarelizenz, die sehr weitreichende Nutzungsrechte gewährt (geringe Einschränkungen) und verlangt, diese Rechte bei der Weitergabe der Software ebenfalls weiterzugeben

GPRS General Packet Radio Service; Standard zur Datenübertragung im Mobilfunkstandard der zweiten Generation (GSM)

GPS Global Positioning System; Positionsbestimmungssystem; Satelliten senden Signale, anhand derer ein auf der Erde befindliches Gerät seine Position bestimmen kann; vom Militär der USA betrieben; das System der Europäischen Union heißt Galileo, das der Russischen Föderation heißt GLONASS und das der Volksrepublik China Beidou

GUI Graphical User Interface; grafische Benutzeroberfläche von Programmen

>>H<<

HDD Hard Disk Drive; Festplattenlaufwerk; Festplatten sind starre Scheiben, während die früher üblichen Disketten (FDD, Flexible Disk Drive) aus biegsamen Folien bestanden; heute sind HDD oft als Flashspeicher ausgeführt, wo die Daten in Chips gespeichert sind (SSD); statt der FDD kommen heute u.a. USB-Sticks (mit Flashspeichern) zum Einsatz

HIP Host Intrusion Detection; ein *Intrusion Detection System (IDS)*, das auf einem *Host* installiert ist

HMAC *Keyed-Hash MAC*, Keyed-Hash Message Authentication Code; kryptografische Prüfsumme, die mit einem Hashalgorithmus gebildet wird und einen geheimen Schlüssel verwendet

HTML Hypertext Markup Language; Sprache bzw. Codierung für Seiten im Internet bzw. World Wide Web

HTTP Hypertext Transfer Protocol; Protokoll für die Kommunikation mit Web-Anwendungen bzw. Web-Servern/-Diensten im Internet bzw. World Wide Web; auf Seiten des Nutzers kommt meist ein Webbrowser zum Einsatz; das Protokoll erkennt man an dem Präfix http:// im Eingabefenster, der jedoch vom Browser oft automatisch ergänzt wird

HTTPS Hypertext Transfer Protocol Secure; sicheres Protokoll für die Kommunikation mit Web-Anwendungen; Variante von HTTP, die zusätzlich eine Verschlüsselung der übertragenen Daten bietet und eine Authentisierung der Gegenstelle; verwendet der Nutzer einen Webbrowser, so steht im Eingabefenster der Präfix https://; moderne Webbrowser zeigen weiterhin zum Beispiel ein Schlüsselsymbol an, das darauf hinweist, dass Prüfungen und kryptografische Operationen erfolgreich durchgeführt wurden und die Adresse des Web-Servers im Eingabefenster der im *Zertifikat* (Schlüsselzertifikat) entspricht, der Nutzer also „an der richtigen Adresse“ ist

>>I<<

IaaS *Infrastructure-as-a-Service*; *Service-Modell*, bei dem der IT-Dienstleister ein Minimum an IT-Komponenten bereitstellt

ICT Information and Communication Technology; Informations- und Kommunikationstechnologie (IKT); etwa: Computertechnik und Netzwerke und deren Komponenten

IdM *Identity Management*; Identitätsmanagement; Verwaltungsteil beim Identitäts- und Zugriffsmanagement (IAM)

IDS *Intrusion Detection System*; identifiziert Versuche, in ein Netzwerk oder ein Computersystem einzubrechen und generiert in diesem Falle unverzüglich einen Alarm

IEC International Electrotechnical Commission; internationale Normungsorganisation

IEEE Institute for Electrical and Electronics Engineers; internationaler Berufsverband und Veranstalter

IKT Informations- und Kommunikationstechnologie (IKT); etwa: Computertechnik und Netzwerke und deren Komponenten; englisch: Information and Communication Technology, ICT

IoA Indicator of Attack; Anzeichen dafür, dass ein Angriff auf ein Computersystem stattgefunden hat

IoT Internet of Things; Internet der Dinge; Gegenstände des täglichen Lebens (privat oder öffentlich) werden im und mit dem Internet verbunden; ihre Zahl ist üblicherweise größer als die der ebenfalls verbundenen echten Computersysteme

IoC Indicator of Compromise; Anzeichen dafür, dass die Sicherheit eines Computersystems durch einen erfolgreichen Angriff kompromittiert wurde; der Begriff wird in der IT-Forensik verwendet

IP Internet Protocol; Standard zur Datenübertragung in Form einzelner Pakete; das Protokoll TCP (Transmission Control Protocol) übernimmt die Zusammensetzung in der richtigen Reihenfolge und die Quittierung des Empfangs, weshalb oft von TCP/IP gesprochen wird

IP Intellectual Property; geistiges Eigentum wie zum Beispiel Lösungen von Aufgaben und Problemen, Verfahren, Konstruktionsprinzipien und dergleichen, aber auch Software zählt zum immateriellen Eigentum; bei geistigem Eigentum besteht oft die Möglichkeit der Patentierung

IPS *Intrusion Prevention System*; identifiziert Versuche, in ein Netzwerk oder ein Computersystem einzubrechen, generiert einen Alarm und greift aktiv ein, um den Einbruch zu verhindern

IPSEC Internet Protocol Security; Protokoll für ein *Virtual Private Network (VPN)*, bei dem das gesamte Netzwerk im anderen LAN bzw. im Endgerät sichtbar wird

IRAM2 Information Risk Assessment Methodology 2; Methodik und Tool des ISF (Information Security Forum) zur Bewertung und Behandlung von Informationsrisiken

ISF Information Security Forum; eine unabhängige, gemeinnützige Organisation, deren Mitglieder Methoden, Prozesse und Lösungen für die Informationssicherheit und das Risikomanagement entwickeln

ISMS Information Security Management System; Informationssicherheitsmanagementsystem; Managementsystem für die Informationssicherheit, das die Organisation, Vorgehensweisen und Regeln umfasst; ISO/IEC 27001 definiert ein ISMS; siehe *Informationssicherheits-Managementsystem*

ISACA Information Systems Audit and Control Association; ISACA (es wird fast ausschließlich die Abkürzung benutzt) ist ein weltweiter

	Berufsverband, der zu den Themen IT-Prüfungswesen, IT-Revision, IT-Sicherheitsmanagement und IT-Governance arbeitet
ISO	International Standards Organization; internationale Normungsorganisation
ISP	*Internet Service Provider*; Firmen, die Anwender mit dem Internet verbinden
IT	Information Technology
ITIL®	Information Technology Infrastructure Library®; Sammlung von bewährten Verfahren (best practices) für das *IT-Service-Management*, *ITSM*. ITIL bzw. ISO/IEC 20000 gilt de facto als Standard für die Organisation einer IT-Produktion; seit 2013 ist ITIL eine Marke von Axelos
ITSEC	Information Technology Security Evaluation Criteria; europäische Kriterien für die Bewertung und Zertifizierung der IT-Sicherheit vor allem von Produkten; durch die Common Criteria for Information Technology Security Evaluation ersetzt

>>J<<

JRE	Java-Runtime-Environment (JRE); *Middleware* für Computersysteme; stellt *Anwendungen* diverse Funktionen zur Verfügung, die das *Betriebssystem* nicht bietet

>>K<<

KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KPI	Key Performance Indicator; Leistungsparameter zur Messung des Erfolgs eines Unternehmens (einer Organisation); anhand von KPIs können Vergleiche angestellt und Entwicklungen beobachtet werden; KPIs sind Indikatoren, die Handlungsbedarf anzeigen
KRI	Key Risk Indicator; von Gartner eingeführtes Konzept von Indikatoren, die frühzeitig anzeigen, dass Geschäftsabläufe oder entsprechende Leistungsparameter (business performance) gefährdet sind; wird nicht entsprechend gehandelt, so ist mit negativen Auswirkungen zu rechnen, die sich in schlechteren Werten eines oder mehrerer Key Performance Indicators (KPIs) zeigen werden
KVP	Kontinuierlicher Verbesserungsprozess

>>L<<

LAN — Local Area Network; lokales, d.h. räumlich relativ begrenzt ausgedehntes Computernetzwerk; ein LAN erstreckt sich zum Beispiel auf ein Grundstück, einen Gebäudekomplex, ein Gebäude oder Rechenzentrum oder einen Raum

LTE — LTE-Advanced: Long Term Evolution; Mobilfunknetze der vierten Generation (4G)

LoI — Letter of Intent (siehe auch unter *LoI, Letter of Intent*); Unverbindliche Absichtserklärung zweier Parteien.

>>M<<

M2M — Machine-to-Machine; automatische, IT-gestützte Kommunikation zwischen zwei (Computer-) Systemen

MAC — *Message Authentication Code*; kryptografische Prüfsumme

MIME — Multipurpose Internet Mail Extension; Standard, der es ermöglicht, nicht nur Text, sondern auch Bilder und andere Medien in E-Mails zu versenden; besser bekannt ist S/MIME, die Variante mit Sicherheitsfunktionen (siehe auch dort)

MIPS — Millionen Instruktionen pro Sekunde; Einheit zur Messung der Rechengeschwindigkeit (Performance) von Prozessoren (CPUs)

MoU — Memorandum of Understanding (siehe auch unter *MoU, Memorandum of Understanding*); offizielle Absichtserklärung zweier oder mehrerer Parteien.

MPLS — Multiprotocol Label Switching; Standard für die Übertragung von Daten verschiedener Anwender und verschiedener Anwendungen (Konferenzen, Ton, Daten usw.) über ein physisches Netz; →*Multiprotocol Label Switching (MPLS)*

MTBF — **Mean Time Between Failures**; durchschnittlich erwartete Zeit, bis ein System in einen Fehlerzustand läuft und wiederhergestellt werden muss

MTTF — **Mean Time To Failure**; durchschnittlich erwartete Zeit, bis ein System in einen Fehlerzustand läuft und nicht wiederhergestellt werden kann

MTTR — **Mean Time to Repair**; durchschnittliche Reparaturzeit; durchschnittlich erwartete Zeit, bis ein System wiederhergestellt werden kann;

Mean Time to Recovery / Restore; synonym, wird aber oft eher für IT-Systeme oder IT-Services verwendet;

beide Begriffe beziehen sich auf durchschnittliche Werte, die keine Garantie abgeben und daher von der **Maximum Time to Recovery** zu unterscheiden sind; die **Mean Downtime** enthält nicht nur die

	Reparaturzeit, sondern auch eventuelle Verzögerungen bis die Reparatur / Wiederherstellung beginnen kann
MVP	Minimum Viable Product; Ausdruck für ein Produkt mit Minimalausstattung, das den grundlegenden Bedarf deckt

>>N<<

NAS	*Network Attached Storage*; Speicher, der an ein lokales Netz (LAN) angeschlossen ist; eventuell wird, wie bei anderen Komponenten/Services in Netzen üblich, auch der Fernzugriff aus anderen Netzen ermöglicht
NAT	Network Address Translation; Übersetzung von Netzwerkadressen; die Umsetzung ist meist nötig, um nur lokal gültige („private“) IP-Adressen in solche umzuwandeln, die im Internet gültig sind und erkannt werden; dies wird durch ein Gateway (wie einen DSL-Router) geleistet, der auch das interne Netz nach außen abschirmt
NFC	Near Field Communication; Standard für die kontaktlose Übertragung von Daten in einem räumlich stark begrenzten Nahbereich
NFS	Network File System; Kommunikationsprotokoll, das ermöglicht, auf entfernte Dateien so zuzugreifen, als wären sie lokal gespeichert
NIST	National Institute of Standards and Technology; Bundesbehörde der USA, die, vergleichbar dem BSI in Deutschland, Handreichungen zur IT-Sicherheit herausgibt und sich an der Standardisierung und Überprüfung von Verfahren der Kryptografie beteiligt; andere Aufgaben des NIST werden in Deutschland von der Physikalisch-Technischen Bundesanstalt (PTB) in Braunschweig wahrgenommen; bekannte Veröffentlichungen des NIST zur IT-Sicherheit sind die FIPS-Standards und die Reihe SP-800

>>O<<

OPEX	Operational Expenses (siehe auch unter *OPEX*); laufende Betriebsausgaben; Gegensatz: *CAPEX* (Capital Expenses), Kapitalausgaben, Einmalkosten bzw. Investitionen
OLA	*Operational Level Agreements*; Verträge, die der IT-Dienstleister intern mit Einheiten schließt, die IT-Services bereitstellen
OS	Operating System; *Betriebssystem*
OSI	Open Systems Interconnection; Arbeitsgruppe der ISO (International Standards Organization), die offene Standards erarbeitet; am bekanntesten ist das OSI-Schichtenmodell oder *OSI-Referenzmodell*, das die Datenübertragung zwischen Instanzen über Netzwerke in sieben Schichten einteilt

OTA Over the Air; meist im Zusammenhang mit der Installation von Software bzw. der Konfiguration von Endgeräten über kabellose Netzwerke verwendeter Begriff; zum Beispiel nutzen Mobilfunkbetreiber solche Funktionen

OTP One Time Password; Einmalpasswort; siehe auch *Einmalpasswortverfahren*; Methode zur Dynamisierung von Passworten. Sie schützt davor, dass Passwörter abgehört und missbräuchlich eingesetzt werden, nachdem der rechtmäßige Nutzer sie verwendet hat.

>>P<<

PaaS *Platform as a Service*; Service-Modell beim Cloud-Computing, bei dem der IT-Dienstleister so gut wie alle Komponenten des IT-Stacks bereitstellt, jedoch nicht die Anwendungssoftware (Applikation)

PCI Peripheral Component Interconnect; Hardware-Schnittstelle bzw. Bussystem für die Verbindung des Prozessors (CPU) mit Peripheriegeräten wie Festplatten

PCMCIA Personal Computer Memory Card International Association; internationale Vereinigung, die die physischen und logischen Schnittstellen von etwa kreditkartengroßen Einsteck- bzw. Erweiterungskarten für Computer spezifiziert, die als PCMCIA-Karten bzw. heute als PC-Cards bekannt sind; schon die ersten Standards unterstützten nicht nur Speicherkarten, sondern auch die Umsetzung von Peripheriefunktionen wie Modems oder SCSI zum Anschluss externer Festplatten- und CD-ROM-Laufwerken an Notebooks; bereits Anfang der 1990er Jahre gab es aber auch Sicherheitssysteme in Form solcher Karten wie zum Beispiel die CryptCard

PDA Personal Digital Assistent; Bezeichnung für mobile Kleinstcomputer, die inzwischen etwas außer Mode bekommen ist

PDF Portable Document Format; plattformunabhängiges Format für die Kodierung von Dokumenten, das von vielen Softwareprodukten unterstützt wird; ursprünglich von der Firma Adobe entwickelt; PDF ist eine vektorbasierte Seitenbeschreibungssprache, die die skalierbare und präzise Darstellung unterstützt und für eine stets originalgetreue und gleiche Darstellung auf Bildschirmen und beim Drucken sorgt; PDF ist von der ISO (International Standards Organization) in ISO 32000 und in ISO 19005 in der Form PDF/A für die Langzeitarchivierung genormt

PHP Skriptsprache, die genutzt wird, um auf Servern im Internet dynamische Webseiten zu erzeugen, die dann an das Endgerät bzw. den Browser übermittelt werden

PII Personally Identifiable Information; personenbezogene Daten/Informationen

PIM Personal Information Manager; Software für die Verwaltung von Terminen, Kontaktinformationen und Aufgaben; die genannten Daten werden oft auch als PIM-Daten bezeichnet

PIN Persönliche Identifikationsnummer; Geheimzahl bzw. *Authentisierungsmerkmal* zur *Authentisierung*

PKI *Public Key Infrastructure*; System für das *Schlüsselmanagement* bei asymmetrischen Verschlüsselungsverfahren, PKI nutzt *Zertifikate*

PLC Programmable Logic Controller; speicherprogrammierbare Steuerung; Gerät zur Steuerung einer Maschine oder Anlage, das programmierbar ist im Gegensatz zu früheren fest, verdrahteten Schaltungen

PoC Proof of Concept; Bestätigung der Machbarkeit oder Umsetzbarkeit bzw. der Richtigkeit der Konzeption

POP Point of Presence; Orte, an denen ein Netzdienstleister Zugänge zu einem Weitverkehrsnetz (zum Beispiel dem Internet) und damit Anschlussmöglichkeiten bietet

PPP Public Private Partnership; Kooperation zwischen öffentlicher Hand und Unternehmen in der Privatwirtschaft, die meist mit der Übertragung staatlicher Aufgaben und oft mit Teilprivatisierungen verbunden ist

>>Q<<

QoS Quality of Service; Garantie von Leistungsparametern meist bei Netzwerken, auch Dienstgüte genannt

>>R<<

RADIUS Remote Authentication Dial-In User Services; Authentisierungssystem (siehe auch unter *RADIUS*), das ursprünglich entwickelt wurde, um Nutzer mit Netzen wie GSM, ISDN und DSL zu verbinden; wird jedoch auch im Unternehmensbereich eingesetzt, zum Beispiel um den Zugang zu verschiedensten LDAP-Servern zu ermöglichen

RAID Redundant Array of Independent Discs; System aus mehreren physischen Festplattenlaufwerken (HDD oder SSD), das eine hohe Ausfallsicherheit durch Redundanz sowie Fehlererkennungs- und Fehlerkorrekturmechanismen bietet

RAM Random Access Memory; frei adressierbarer, flüchtiger Halbleiterspeicher, der auch als Hauptspeicher in Computern zum Einsatz kommt; es gibt Speicher, die ihren Inhalt statisch speichern (solange sie mit

	Strom versorgt werden) und dynamische Speicher, deren Inhalt zyklisch wiederaufgefrischt werden muss, um nicht verloren zu gehen
RAS	Remote Access Service; Fernzugriff; ermöglicht den Zugriff von einem Arbeitsplatzrechner ins Unternehmensnetz; typischerweise erfolgt der Zugriff heute weniger über einen zentralen RAS-Server, sondern aus dem Internet über ein VPN oder über ein WLAN vor Ort
RDBMS	Relationales Datenbankmanagementsystem; System zur Ablage strukturierter Daten (*Datenbank*), bei dem die einzelnen Daten durch Beziehungen verbunden sind; fast alle Datenbanken sind relationale Datenbanken; Abfragen und Manipulation von Inhalten werden mit Befehlen vorgenommen, deren Syntax durch SQL definiert ist
RegTP	Regulierungsbehörde für Post und Telekommunikation; heute Bundesnetzagentur (BNetzA) der Bundesrepublik Deutschland
RFID	Radio Frequency Identification; kontaktlose Abfrage von Informationen; dabei liest ein Lesegerät einen Transponder (RFID-Tag) aus, der über die Luftschnittstelle mit Energie (Strom) versorgt wird
RfC	*Request for Change*; Änderungsanforderung in der IT
RFC	Request for Comment; meist technische Dokumente, die anfangs noch zur Kommentierung auffordern, später zu Standards werden und die Bezeichnung RFC jedoch beibehalten
RfI	*Request for Information*; Aufforderung an Anbieter, Informationen bereitzustellen, anhand derer der Kreis der Anbieter auf diejenigen eingeschränkt wird, die eine Aufforderung erhalten, ein Angebot abzugeben (RfP)
RfP	*Request for Proposal*; Ausschreibung bzw. Aufforderung, ein Angebot abzugeben
ROI	Return on Investment; Gewinn pro investiertem (ausgegebenem) Kapital bzw. aufgewendeten Ressourcen (in Geldwert); misst die Wirtschaftlichkeit eines Vorhabens
ROM	Read Only Memory; nicht-flüchtiger Festwertspeicher; der eigentliche ROM wird beim Herstellungsprozess gefüllt (programmiert); als PROM ist er einmalig elektrisch programmierbar (schreibbar); EPROMs können wiederholt elektrisch programmiert werden, nachdem ihr Inhalt mittels UV-Licht gelöscht wurde; EEPROMs oder E²PROM können elektrisch geschrieben und gelöscht werden; Flashspeicher sind EEPROMs, bei denen nicht einzelne Speicherbytes, sondern nur ganze Zeilen zugleich geschrieben werden können
RPC	Remote Procedure Call; Netzwerkprotokoll, das es erlaubt, Funktionen (Software-Prozeduren) auf einem entfernten Rechner auszuführen
RSA	asymmetrisches Verschlüsselungsverfahren benannt nach seinen Erfindern Rivest, Shamir und Adleman

>>S<<

SAN	*Storage Area Network*; zentrales System zur persistenten Speicherung von Daten, das aus sehr vielen Festplatten besteht und von vielen Serversystemen über ein Hochgeschwindigkeitsnetzwerk angesprochen werden kann
SCADA	Supervisory Control and Data Acquisition; System der sogenannten Operational Technology (OT), das zur Steuerung und Überwachung von Industrieanlagen dient
SCM	Supply Chain Management; Lieferkettenmanagement bzw. Anwendungssoftware für diesen Zweck
SDL	*Security Development Lifecycle*; von Microsoft entwickeltes Konzept für die Entwicklung sicherer Software
SDM	Service Delivery Manager, oder Service Delivery Management; Personen bzw. Organisation bei einem IT-Dienstleister; vertritt den Kunden intern gegenüber der IT-Produktion, stellt die Einhaltung des Vertrages mit dem Kunden sicher und ist Ansprechpartner für den Kunden
SDN	*Software-defined Networking (SDN)*; Architektur zur Optimierung von Netzwerken, bei der über die ursprünglichen Netzwerke (data layer/plane) eine zusätzliche Steuerungsebene (control layer/plane) in Form einer Software-Abstraktionsschicht gelegt wird
SDP	Software-Defined Perimeter; siehe unter *Zero Trust Network Access (ZTNA)*
SPA	*Simple Power Analysis (DPA)*; Angriff, bei dem der Stromverbrauch analysiert wird, um Informationen über den geheimen Schlüssel zu erhalten
SWG	*Secure Web Gateway*; Gateway-Lösung eines *Content-Filters*, der in der Regel auch einen Virus/Malware-Schutz enthält
SLA	*Service Level Agreement*; Leistungsversprechen in Bezug auf die Bereitstellung eines IT-Service
SLM	*Service Level Management*; IT-Service-Management-Prozess in ISO/IEC 20000 und ITIL®
S/MIME	Secure Multipurpose Internet Mail Extension; Standard, der es ermöglicht, nicht nur Text, sondern auch Bilder und andere Medien in E-Mails zu versenden und diese zu signieren und/oder zu verschlüsseln
SOA	Service-Oriented Architecture; IT und speziell Applikationen werden an den Geschäftsprozessen ausgerichtet und in Form einzelner Services modularisiert, was die Flexibilität erhöht und es gestattet, auf veränderliche Geschäftsanforderungen reagieren zu können

SOAP Simple Object Access Language; Protokoll zur Übertragung von Nachrichten im XML-Format

SOGP Standard of Good Practice for Information Security; Sicherheitsstandard des ISF (Information Security Forum); befasst sich mit der Informationssicherheit aus einer geschäftlichen Perspektive und bietet praktische und verlässliche Anleitungen für die Bewertung und Verbesserung der Informationssicherheit einer Organisation

SQL Structured Query Language; Sprache zum Bearbeiten und Abfragen von Daten in relationalen *Datenbanken* (RDB, RDBMS)

SSD Solid-State Drive; Festkörperspeicher; Speicherlaufwerk aus Flashspeicherchips; sie ersetzen die Festplatten, bei denen die Daten auf schnell rotierenden starren Scheiben gespeichert sind (Hard Disk Drive, HDD); logisch werden beide Speicherlaufwerke gleich angesprochen und genutzt

SSDL Secure Software Development Lifecycle; manchmal auch als Secure SDLC abgekürzt; dabei handelt es sich meist um Erweiterungen hinsichtlich der Security (S) eines Software-Development-Lifecycle-Modells (SDL)

SSH Secure Shell; Protokoll bzw. Funktion, mit deren Hilfe man sich über ein potentiell unsicheres Netzwerk auf einem entfernten Rechner anmelden und dort Konsolenfunktionen (Kommandos) ausführen kann

SSL Secure Sockets Layer; Vorgänger von TLS; Protokoll zur Herstellung einer verschlüsselten Verbindung

>>T<<

TAN Transaktionsnummer; ein Einmalpasswort (PIN) für das Online-Banking; siehe auch *TANs*

TCO *Total Cost of Ownership*; Gesamtkostenansatz; es werden neben den Anschaffungskosten insbesondere auch Kosten für den Betrieb und den Erhalt berücksichtigt

TCP/IP Zusammenfassung der Protokolle TCP (Transmission Control Protocol) und IP (Internet Protocol); IP ist ein Standard zur Datenübertragung in Form einzelner Pakete; TCP übernimmt die Zusammensetzung in der richtigen Reihenfolge und die Quittierung des Empfangs

TCSEC Trusted Computer System Evaluation Criteria; auch als Orange-Book bekannt; US-amerikanische Kriterien für die Bewertung und Zertifizierung der IT-Sicherheit vor allem von Produkten; durch die Common Criteria for Information Technology Security Evaluation ersetzt

TK Telekommunikation

TLS Transport Layer Security; Protokoll zur Herstellung einer sicheren, verschlüsselten Verbindung; Nachfolger von SSL

TOGAF The Open Group Architecture Framework; TOGAF (es wird fast ausschließlich die Abkürzung benutzt) bietet einen umfassenden Ansatz für den Entwurf, die Planung, die Implementierung und die Verwaltung einer Informationsarchitektur für Unternehmen

TOM technische und organisatorische Maßnahmen (TOM); siehe *Datenschutz (privacy)*

TPM Trusted Platform Module; *Hardware-Sicherheitsmodul (HSM)*, das in Computer verschiedenster Bauform eingebaut wird und auf dem Computer kryptografische Operationen sowie sicheren Speicher zur Verfügung stellt

TQM Total Quality Management; sehr unterschiedlich interpretierter Ansatz für ein umfassendes Qualitätsmanagement; etwa: Qualität muss erzeugt und nicht nur kontrolliert werden; sie ist Ergebnis aktiven Handelns eines jeden Mitarbeiters; das Management muss einen Rahmen definieren, der Qualität ermöglicht.

>>U<<

UC Unified Communication; Integration von Kommunikationssystemen und Kommunikationsanwendungen

UEFI Unified Extensible Firmware Interface; Firmware für moderne Computersysteme, siehe →*UEFI*

UMTS Universal Mobile Telecommunication System; Mobilfunknetze der dritten Generation (3G)

UPS Uninterruptable Power Supply; unterbrechungsfreie Stromversorgung (USV)

URL Uniform Resource Locator; Kombination aus Übertragungsart und Speicherort, die es ermöglicht, alle Dokumente im Internet auffinden zu können

USV unterbrechungsfreie Stromversorgung; englisch: Uninterruptable Power Supply (UPS)

UTM *Unified Threat Management*; Produkte, die typischerweise Lösungen aus den drei Bereichen Netzwerksicherheit, sicherer Internet-Zugang und Datensicherheit integrieren

>>V<<

VBA Visual Basic for Applications; Skriptsprache von Microsoft für die Steuerung und Nutzung von Anwendungen

VLAN Virtual Local Area Network; ein physisches Netz (LAN) wird in logische Teilnetze (VLANs) aufgeteilt, die jeweils nur von einem Anwender (Mandanten) verwendet werden; sieh auch: *VLAN*

VoIP Voice over IP; Übertragung von Sprache über ein IP-Netz

VPN *Virtual Private Network*; schafft eine gesicherte Verbindung zwischen zwei IT-Komponenten in einem unsicheren Netz

VM Virtual Machine; *Virtuelle Maschine (VM)*; Arbeitslast (workload) für einen virtualisierten Server; enthält neben der Anwendung und der zugehörigen Middleware auch ein Betriebssystem

>>W<<

WAN *Wide Area Network*; Netzwerk, das geografisch größere Distanzen überwindet

WLAN Wireless Local Area Network; Funknetz (drahtlos)

WWW World Wide Web; auf Basis des Internets System von Webseiten, die mittels Hyperlinks miteinander verbunden sind

WYSIWYG What you see is what you get; schon bei der Eingabe wird dem Anwender auf dem Bildschirm der Inhalt in seiner endgültigen Form präsentiert, wie er zum Beispiel auch beim Ausdrucken oder beim erneuten Öffnen in der Anwendung erscheint

>>X<<

XML Extensible Markup Language; Metasprache oder Format zur Darstellung und Übertragung von strukturierten Daten; ermöglicht den Austausch von Daten zwischen verschiedenen Anwendungen, da ein einfaches Textformat für die Daten selbst, deren Beschreibung sowie die Beziehungen unter ihnen verwendet wird

>>Y<<

>>Z<<

ZTNA *Zero Trust Network Access*; eine Lösung, die die Verteidigungslinie vom Netzwerkzugang bis vor die Anwendungen verlegt

Literatur

Besonders ein solches Buch, das sich zur Aufgabe macht, Definitionen von Fachbegriffen zu geben, kann nicht geschrieben werden, ohne dass der Autor vielfältige Literatur gelesen hätte – in der langen Zeit der Tätigkeit auf diesem Gebiet, bei der Erstellung von Lehrunterlagen für Studierende und beim Schreiben dieses Buches. Die Definitionen sollen ja den Stand der Technik korrekt wiedergeben und konsensfähig sein. Das bedeutet auch, dass Begriffe und Zusammenhänge auch in anderen Veröffentlichungen so oder ähnlich vorkommen können – ja müssen.

[1] Karen Scarfone and Victoria Thompson: System and Network Security Acronyms and Abbreviations; National Institute of Standards and Technology (NIST), NIST Interagency Report 7581, September 2009

[2] National Institute of Standards and Technology (NIST): Glossary; https://csrc.nist.gov/glossary

10 Stichwortverzeichnis (Index)

Tipp für eBook-Leser:

> Suchen Sie nach „=“-**Buchstabe** (zum Beispiel „**=B**“ oder „**=H**“), um zu dem entsprechenden Buchstaben bzw. der Rubrik zu gelangen. Diese Lösung funktioniert von jeder Stelle im eBook aus und ist wahrscheinlich schneller und für die meisten Leser einfacher, als zwischen 26 Lesezeichen zu navigieren (die daher im eBook nicht angelegt wurden).
>
> (Um zum und im Abkürzungsverzeichnis (Kapitel 9) zu navigieren, suchen Sie bitte nach „**>B**“ oder „**>H**“ usw.)

Wichtiger Hinweis für eBook-Leser:

> Die Seitenzahlen in diesem Stichwortverzeichnis entsprechen der Seitenzählung wie sie in der Kopfzeile stehen. Dies ist zum Beispiel Seite 263. Allerdings wurden hierbei die ersten 12 Seiten bis zum Inhaltsverzeichnis nicht mitgezählt. Wenn ihr Reader jetzt also Seite 275 anzeigt, müssen Sie von allen Angaben im Register immer 12 abziehen.
>
> Diese altertümliche Zählweise stammt aus den Zeiten vor dem DTP[163], als der Front Matter mit Inhaltsverzeichnis ganz zum Schluss gesetzt werden musste, um korrekte Seitenzahlen zu erhalten. Der Verlag hält an dieser Form der Formatierung fest.

Das Buch enthält etwa 700 Begriffe, deren Bedeutung mit einem eigenen Eintrag oder Untereintrag ausführlich erläutert wird. Sind sowohl die deutsche Bezeichnung als auch der englische Begriff in Gebrauch, so zählen diese allerdings doppelt. Das gleiche gilt, wenn eine Abkürzung gleichberechtigt zum Fachterminus verwendet wird bzw. diesen als solchen ersetzt hat. Beide Dopplungen machen aber nur einen kleinen Teil der Gesamtheit aus.

Diese Hauptbegriffe haben eine **fettgedruckte** Seitenzahl im nachfolgenden Verzeichnis. Allerdings hat das Textverarbeitungssystem diverse dieser Formatierungen unterschlagen, die eventuell nicht alle manuell nachgepflegt wurden.

Wird auf einen solchen Begriff an anderer Stelle (wo er nicht erklärt wird) verwiesen, so ist die Seitenzahl in normaler Schrift (also nicht fett) angegeben.

---

[163] DTP: Desktop Publishing; computergestütztes Setzen

E. von Faber, *IT und IT-Sicherheit in Begriffen und Zusammenhängen*,
Edition <kes>, https://doi.org/10.1007/978-3-658-33431-4

Zusätzlich zu diesen etwa 700 Begriffen erschließen sich viele Begriffe durch den Zusammenhang, in dem sie verwendet werden. In Fällen, in denen ein Begriff im gegebenen Kontext als wesentlich erschien, ist er ebenfalls in das Stichwortregister aufgenommen worden. Das betrifft etwa 100 weitere Begriffe.

==B==

==C==

==D==

==E==

==F==

==G==

==H==

==I==

==J==

==K==

==L==

==M==

==N==

==O==

==P==

==Q==

==R==

==S==

==T==

==U==

==V==

==W==

==X==

==Z==