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!

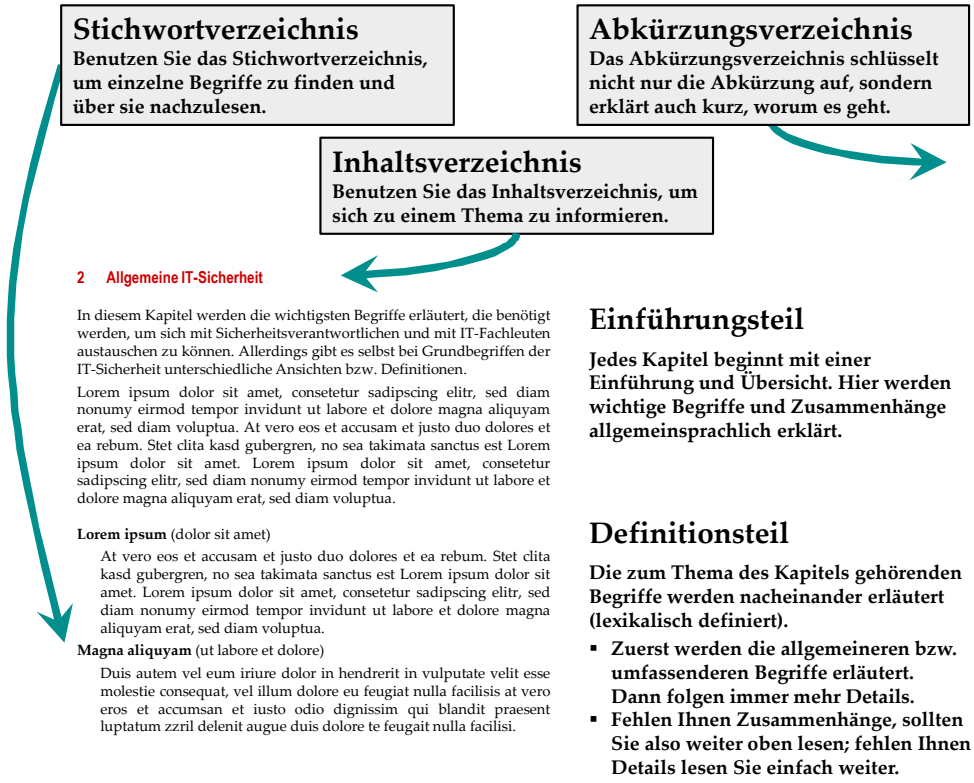
Alle 64 Abbildungen und eventuell weiteres Zusatzmaterial finden Sie in elektronischer Form über https://link.springer.com/ auf der Seite der eBook-Version.

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.

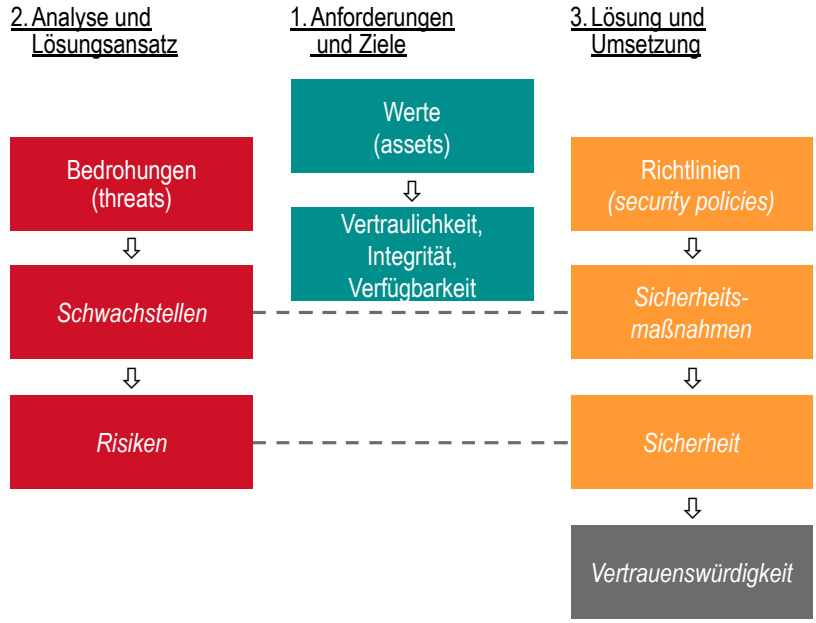


Abb. 1: Grundbegriffe – erste Annäherung und drei Themen

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.

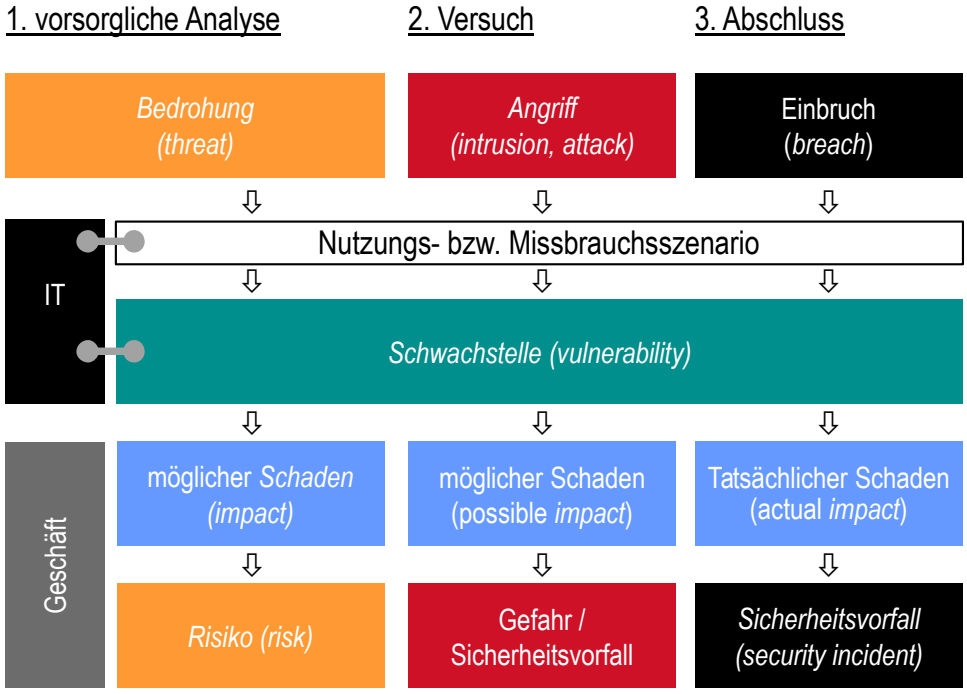


Abb. 2: Risikobewertung (Vorsorge) und zwei Abläufe bei der Nutzung der IT (*kursive Begriffe* sind gängig, andere nicht)[5]

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.

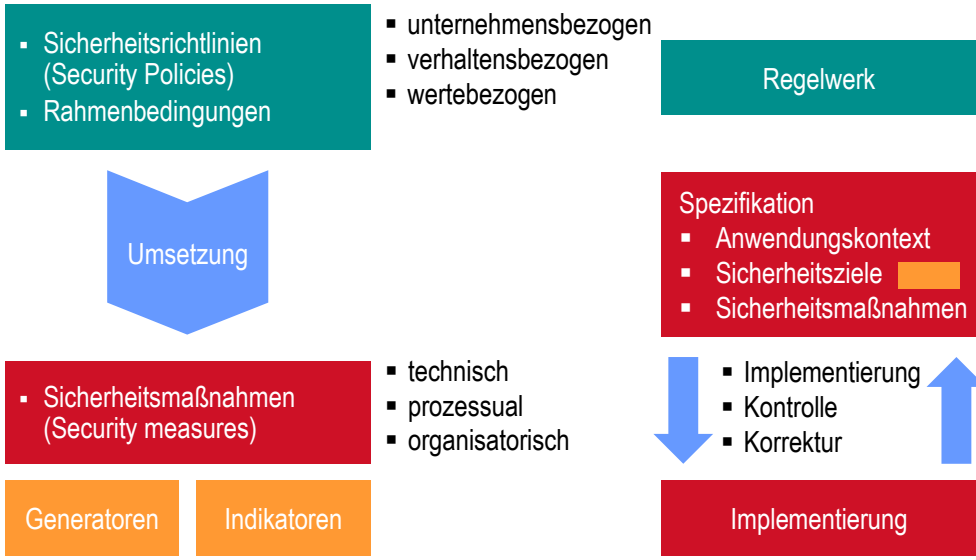


Abb. 3: Regelwerke und Sicherheitsmaßnahmen[13]

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