Edition <kes>

Eberhard von Faber
Wolfgang Behnsen

Joint Security Management: organisationsübergreifend handeln

Mehr Sicherheit im Zeitalter von Cloud-Computing, IT-Dienstleistungen und industrialisierter IT-Produktion

<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.
Die Autoren der Zeitschrift und der Buchreihe Edition <kes> helfen den Anwendern in Basic- und Expert-Seminaren bei einer praxisnahen Umsetzung der Informations-Sicherheit: www.itsecuritycircles.de

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

Eberhard von Faber · Wolfgang Behnsen

Joint Security Management: organisationsübergreifend handeln

Mehr Sicherheit im Zeitalter von Cloud-Computing, IT-Dienstleistungen und industrialisierter IT-Produktion

Springer Vieweg

Eberhard von Faber
Bornheim, Deutschland

Wolfgang Behnsen
Erlangen, Deutschland

ISSN 2522-0551 ISSN 2522-056X (electronic)
Edition <kes>
ISBN 978-3-658-20833-2 ISBN 978-3-658-20834-9 (eBook)
https://doi.org/10.1007/978-3-658-20834-9

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

Springer Vieweg

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

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

Gemeinsames Geleitwort

von einem Anwender und einem Anbieter

Der weltweit stattfindende gesellschaftliche Wandel wird sehr stark durch das gesammelte Wissen, die Erfahrung, die Produktion und den Konsum von Gütern und Dienstleistungen geprägt. Viele Prozesse, insbesondere in der industriellen Produktion, werden komplexer und immer stärker durch die Digitalisierung beeinflusst. Fast kein Marktteilnehmer kann heute alles alleine machen. Das ist oft weder technisch machbar noch ökonomisch sinnvoll. Die IT-Welt mit ihren diversen Produkten und Dienstleistungen ist hier keine Ausnahme. Spezialisierung und Arbeitsteilung erfordern jedoch Kooperation und Kommunikation. Es entstehen verstärkt Abhängigkeiten (z.B. in Liefernetzwerken) und Kommunikationsrelationen. IT-Dienstleister treffen auf IT-Anwender/IT-Anwenderorganisationen und beide Parteien sind aufeinander angewiesen. Beide müssen gekonnt interagieren, um die eigenen Geschäftsziele in einem „win-win"-Kontext zu erreichen. Das heißt, sie müssen gemeinsam und verbunden handeln. Die rhetorische Klammer oder das Bindeglied heißt „Joint".

Das vorliegende Buch von Eberhard von Faber und Wolfgang Behnsen (beide exzellente IT-Experten und Praktiker mit langjähriger Erfahrung) widmet sich diesem „Joint"-Thema und richtet den Fokus auf das IT-Sicherheitsmanagement und die Absicherung von IT-Services in einer Welt voller Geber und Nehmer. Der Komplexität der Geber-Nehmer-Wechselbeziehung wird mit dem Ruf nach mehr Struktur und Transparenz im Hinblick auf die IT-Sicherheit begegnet (das wird inzwischen auch verstärkt durch gesetzgeberische Initiativen untermauert). Im Buch liegt das Epizentrum des Interesses und der Darstellung nicht auf der Seite des IT-Dienstleisters oder der Anwenderorganisation, sondern genau in der Mitte, dort, wo beide Parteien aufeinandertreffen (Schnittstellen, Interaktionen). Diese Perspektive macht das Buch innovativ und interessant. Sie zeigt, dass nicht singuläre Sichtweisen (mein Unternehmen, meine Geschäftsziele, meine Interessen), sondern duales/gemeinsames Handeln zu einer neuen Qualität der IT-Sicherheit führen kann.

Das Buch glänzt durch klare Struktur (drei Teile: Fundamente, Ausgestaltung, Bonus), logischen Aufbau, sorgfältige Sprache und viele Abbildungen, die den Inhalt einzelner Abschnitte komprimiert darstellen oder ergänzen. Die, die Schnelligkeit mögen, können sich an die Themenbreite und Materialfülle über die Text-Blöcke „Einführung und Zusammenfassung" herantasten. Das Buch enthält viele grundlegende Einsichten, neue Methoden und nützliche Tipps. Den Spagat zwischen beiden Sprachwelten Deutsch-Englisch (dieser Dualismus lässt sich in der IT-Literatur kaum vermeiden) haben die Autoren auch elegant gelöst. Dort, wo es

Sinn macht, werden beide Begriffe zusammenhängend erwähnt, z.B. „Unternehmensrichtlinien (corporate policies)“. Die Bonus-Kapitel (Informationssicherheit messen, wichtige Begriffe der IT-Sicherheit) und der Anhang (mit Literaturverzeichnis und einem hilfreichen Index) runden das Buch ab. Das Buch eignet sich sowohl für Disziplin-Einsteiger als auch für gestandene Profis (IT-Sicherheitsverantwortliche, IT-Manager, IT-Service-Manager) und hat einen starken praxisbezogenen Charakter. Man kann wirklich viel daraus lernen, vorausgesetzt man liest das ganze Buch mit erforderlicher Sorgfalt und ohne Zeitdruck. Der Aufwand lohnt sich, da das Gesamtbild über das komplexe Gefüge der industriellen IT-Sicherheit klarer wird. Es wäre erfreulich, wenn dieses Buch nicht nur gelesen werde würde, sondern auch seinen Weg in die faszinierende Welt der modernen, praktischen IT-Sicherheit sowohl bei IT-Dienstleistern als auch bei IT-Anwenderorganisationen finden würde. Gemeinsam werden wir sicherer und stärker!

München bzw. Freiburg im Breisgau, im Januar 2018

Dr. Andrzej Debski

Chief Information Security Officer (CISO), Linde AG

Heike Bayerl

Vice President Global Security Compliance & Quality Management, T-Systems, IT Division

Vorwort der Autoren

Der große Erfolg unseres Buches „Secure ICT Service Provisioning for Cloud, Mobile and Beyond“ hat uns sehr gefreut und ermutigt. Darin legen wir Grundlagen für die Absicherung von IT-Services in einer *großtechnischen, industrialisierten IT-Produktion*, in der Sicherheit so ganz anders organisiert werden muss, als man sich das lehrbuchhaft manchmal vorstellen mag.

Das vorliegende Buch bleibt den Motiven „servicebezogen“ und „bezogen auf die marktwirtschaftliche Realität“ treu und verlagert den Schwerpunkt weiter in Richtung Anwenderorganisation. Anlass für dieses Buch waren drei Beobachtungen:
1. IT-Sicherheit macht man *mit IT* (und nicht ohne Bezug zur IT). Vielen Sicherheitsverantwortlichen scheint es an Einblicken in IT und die IT-Industrie zu fehlen.
2. IT-Sicherheit macht man *nicht alleine* (und nicht nur im eigenen Unternehmen). Das Sicherheitsmanagement kreist noch zu sehr im gewohnten Erfahrungsbereich.
3. IT-Sicherheit braucht *mehr Struktur*, um die Komplexität beherrschen zu können.

Freuen Sie sich auf neue Methoden, grundlegende Einsichten und praktische Tipps. Wir bieten Seminare für Ihre Experten auch in Ihren Räumlichkeiten. Schreiben Sie uns unter ESARIS@t-online.de!

Eberhard von Faber, Wolfgang Behnsen

Über dieses Buch

Sicher in „die Cloud“? Geschäftsprozesse digitalisieren und komplexere Anwendungen von Fremddienstleistern betreiben lassen? Skaleneffekte und das Know-how externer Spezialisten nutzen, um Kosten zu senken und IT-Services mit höherer Qualität zu erhalten? Für viele Unternehmen in fast allen Branchen ist das eine richtige Strategie, denn „Digitalisierung“ und „Outsourcing“ bringen Vorteile. Diese Vorteile wirken aber nur dann (nachhaltig), wenn die IT-Services *sicher* sind, also die digitalen Geschäftsprozesse der Anwenderorganisation nicht unzulässig gefährden.

Sicherheit entsteht jedoch 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. Die Kette ist so stark wie ihr schwächstes Glied. Deshalb muss der Sicherheitsmanagementprozess übergreifend sein. Viele Anwender und Dienstleister sind damit jedoch überfordert! Kataloge von Anforderungen und Berge von Maßnahmen helfen ihnen nicht. Das Konzept *Joint Security Management (JSM)* schafft Abhilfe und gibt Anwendern wie Dienstleistern die notwendige Orientierung und Anleitung. *JSM wurde firmenunabhängig entwickelt.* Was Sie erwartet, ist in Abb. 1 zusammengefasst.

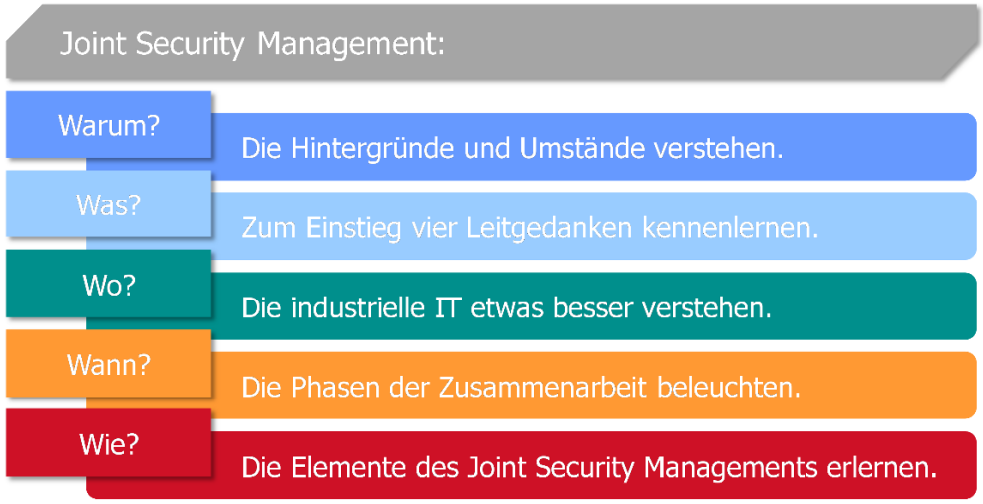

Abb. 1: Übersicht über *JSM* und dieses Buch

Neugierig? Interessiert? *JSM* ist etwas Neues, das IT- und IT-Sicherheitsmanagern zur Lektüre und Anwendung empfohlen wird. Die „Ära der Digitalisierung“ bietet Möglichkeiten! Sie können aber nur dann genutzt werden, wenn inhärente Risiken erkannt und adäquat behandelt werden. Organisationsübergreifend!

Inhaltsverzeichnis

Teil 1: Fundamente des Joint Security Managements (JSM)

1 Einführung und Überblick

Einführung und Zusammenfassung: Organisationsübergreifend handeln? Was kann das schon bedeuten! Müssen wir nicht irgendwie immer organisationsübergreifend handeln bei diesem übergreifenden Thema IT-Sicherheit? Alter Wein in neuen Schläuchen? Das *Joint Security Management (JSM)* ist das erste wirklich organisationsübergreifende Sicherheitsmanagementsystem, das Anwenderorganisationen und IT-Dienstleister zusammenbringt und bei dem die Interaktion zwischen rechtlich verschiedenen Organisationen von vornherein im Mittelpunkt steht. Dahinter steckt die Einsicht, dass die heutige IT-Industrie sehr arbeitsteilig organisiert ist und dass mehrere Firmen und Institutionen ihren Beitrag leisten müssen, damit die IT-Services adäquat abgesichert sind. Das *Joint Security Management* baut das Sicherheitsmanagement neu auf entlang des Skeletts der industriellen, marktwirtschaftlichen Prozesse und der für moderne IT charakteristischen Wertschöpfungsketten.

1.1 Vorderseite: JSM, ein neues Zusammenarbeitsmodell

Einführung und Zusammenfassung: Dieses Kapitel gibt eine kurze Einführung, in der skizziert wird, was sich hinter dem Begriff *Joint Security Management (JSM)* verbirgt und warum eine solche neue Form des Sicherheitsmanagements heute benötigt wird. Es werden Beispiele für betriebliche und industrielle Realitäten genannt, die vom traditionellen Sicherheitsmanagement gar nicht oder nur unzureichend berücksichtigt werden. Ihre explizite Beachtung ist die Grundlage des *Joint Security Managements*. Zuletzt werden Elemente für das *Joint Security Management* genannt. Sie beschreiben, wie die beteiligten Organisationen und Firmen zusammenarbeiten und interagieren müssen, damit sichergestellt werden kann, dass die IT-Services den Sicherheitsanforderungen genügen und Risiken beherrschbar bleiben.

Notwendigkeit eines *Joint Security Managements*

Kein Unternehmen kann heute noch komplexe IT-Services marktgerecht aus eigener Kraft bereitstellen. Anwenderorganisationen bedienen sich spezialisierter IT-Dienstleister und letztere greifen auf Komponenten und Dienste aus einem weit gefächerten Zuliefernetzwerk zurück. Damit dabei die Sicherheit nicht auf der Strecke bleibt, wird ein unternehmensübergreifendes Sicherheitsmanagement benötigt. Dieses Buch zeigt, wie Anwenderorganisation und Lieferanten in einem solchen *Joint Security Management* zusammenarbeiten um sicherzustellen, dass die mit der Nutzung von IT verbundenen Geschäftsrisiken beherrschbar bleiben.

IT wird zunehmend industriell produziert. Sie wird damit nicht nur größer und komplexer; ihre Produktionsweise ist auch durch eine hochgradige Spezialisierung

E. von Faber und W. Behnsen, *Joint Security Management: organisationsübergreifend handeln*, Edition <kes>, https://doi.org/10.1007/978-3-658-20834-9_1

und Arbeitsteilung gekennzeichnet. Sichtbare Kennzeichen dieser Entwicklung sind die fortschreitende Nutzung von fremden IT-Services und Begriffe wie Cloud-Computing. Doch was bedeuten die Trennung zwischen Anwenderorganisation und Produzent und die tiefgreifende Arbeitsteilung in der Bereitstellung für die IT-Sicherheit? Wie hat ein gemeinsames, organisationsübergreifendes Sicherheitsmanagement auszusehen? Wie funktioniert es? Welche Bausteine machen ein solches Steuerungsmodell aus? Wie arbeiten die Sicherheitsorganisationen der Anwenderseite und die des Dienstleisters konkret zusammen? Welche Aufgaben nimmt welche Seite in welchen Phasen der Zusammenarbeit wahr? Wie soll die Interaktion erfolgen, damit Lücken und Reibungspunkte vermieden werden, und wie korrespondiert dies mit den Anforderungen an die Absicherung komplexer IT-Services?

Das Buch zeigt, wie ein ganzheitliches, marktgerechtes Sicherheitsmanagement in der neuen Welt industrialisierter IT-Services möglich ist und konkret umgesetzt werden kann. Das Buch beschreibt nicht nur, was zu tun ist, sondern auch wie. Besondere Berücksichtigung finden dabei die allzu oft vernachlässigten, durch IT und das Geschäft bestimmten Abläufe, Organisationsformen und Beziehungen. Denn IT-Sicherheitsmanagement kann keine Parallelwelt sein, sondern muss sich, will sie erfolgreich sein, in die betriebliche und industrielle Realität integrieren.

Betriebliche und industrielle Realität als Basis für das *Joint Security Management*

Doch woraus besteht, kurz zusammengefasst, diese betriebliche und industrielle Realität, die es zu berücksichtigen gilt?

1. Prozesse, Abläufe und Aktivitäten während der Entwicklung und Implementierung (IT-Service-Management, ITSM Teil 1)

   Es ist allgemein bekannt, dass die IT-Sicherheit möglichst frühzeitig, während der Entwicklung und Implementierung berücksichtigt werden muss. Für die Entwicklung von Software gibt es dazu viel Literatur. Doch leider ist die sichere Entwicklung und Implementierung komplexer IT-Systeme wie z.B. für die Cloud weniger gut spezifiziert. Doch die Release- und Deployment-Management-Prozesse und das Service-Catalog-Management liefern eine Basis.

2. Prozesse, Abläufe und Aktivitäten während der Bereitstellung, zur Aufrechterhaltung und Verbesserung (IT-Service-Management, ITSM Teil 2)

   Die Prozesse zur Bereitstellung, Aufrechterhaltung und Verbesserung von IT-Services sind in ISO/IEC 20000 oder ITIL[1] beschrieben. Sie gelten als Standard

[1] ITIL: IT Infrastructure Library, eine Sammlung von vordefinierten Prozessen, Aktivitäten und Rollen entlang des Lebenszyklus von IT-Services, wobei die Betriebsphase besonders beachtet wird. Die Aktivitäten werden auch unter dem Begriff IT-Service-Management (ITSM) zusammengefasst. Sie sind auch beschrieben in: ISO/IEC 20000 –

und werden von allen größeren IT-Dienstleistern angewendet. Allerdings geben die Standards nur grundsätzliche Hinweise und führen nicht aus, wie sie umgesetzt werden sollen. IT-Sicherheit wird weitgehend ignoriert.

3. Technologie, Produkte, Lösungen – und Komplexität

Natürlich zählen die Struktur der IT und ihre Gliederung in Komponenten, Subsysteme und IT-Services einschließlich aller Beziehungen zwischen ihnen zu den Grundlagen, die es zu verstehen und zu berücksichtigen gilt. Hierbei ein vollständiges und konsistentes Bild zu erhalten, ist nicht einfach. Die Konzentration auf Server, Netze und Endgeräte greift in einer modernen IT zu kurz. Vielmehr wird eine Architektur bzw. ein übergreifendes Ordnungsschema benötigt, das dabei hilft, die Komplexität der IT-Komponenten einerseits und die der Prozesse, Abläufe und Aktivitäten im IT-Service-Management (ITSM) andererseits zu beherrschen und diese in einem industriellen Umfeld flexibel zu handhaben.

4. Struktur und Logik der Lieferkette mit Herstellern und Lieferanten und deren Geschäftsmodellen

Technologien, Produkte und Lösungen werden von einer Vielzahl von Herstellern und Lieferanten bereitgestellt. Das Gleiche gilt für Aktivitäten im IT-Service-Management. Oft werden Produkte und Lösungen als „managed service“ bereitgestellt. Da die Kette so stark ist wie ihr schwächstes Glied, muss die Lieferkette mit all ihren möglichen Bestandteilen verstanden werden. Nur dann kann man darangehen, für adäquate Sicherheit zu sorgen.

5. Phasen der Beziehung zwischen Anwenderorganisation (Kunde) und IT-Dienstleister (Lieferant)

Große Anwenderorganisationen (z.B. international tätige Konzerne) benötigen eine komplexe IT, um ihre vielfältigen Geschäftsprozesse zu unterstützen. Der Vorgang der Beschaffung (IT-Dienstleister übernimmt IT-Services) ist aufgrund der Komplexität der IT-Services und des Vertragsvolumens mehrstufig und kein einfacher Kaufvorgang. Die Verträge umfassen häufig viele Hundert Seiten. Der Unterzeichnung des Vertrages folgt die Migration der IT-Services (Daten, häufig auch IT-Komponenten), ggf. deren Anpassung und Modernisierung sowie der Betrieb. Auch die Betriebsphase ist von zahlreichen Eingriffen gekennzeichnet.

6. Interessenlage der Beteiligten und Aufbau von Verträgen

Anwenderorganisationen und IT-Dienstleister sind Marktteilnehmer. Erstere wollen ihre branchenspezifischen Geschäftsprozesse mit hochwertigen IT-

Information technology – Service management – Part 1: Service management system requirements, Part 2: Guidance on the application of service management systems; 2012 [5]

Services zu geringen Kosten unterstützen. Die IT-Dienstleister müssen dem gerecht werden, aber dabei gleichzeitig eine Vielzahl von unterschiedlichen Anforderungen verschiedenster Kunden erfüllen. Insgesamt sind Zielkonflikte unvermeidlich. Die notwendigen Festlegungen zur IT-Sicherheit müssen sich in die Normen und die Praxis des Vertragswesens einfügen und sich im Einklang mit den marktwirtschaftlichen Gegebenheiten befinden.

Elemente des *Joint Security Managements*

Auf dieser Basis müssen nun Lösungen entwickelt werden, die genau beschreiben, wie die Beteiligten zusammenarbeiten und interagieren müssen, damit sichergestellt werden kann, dass die IT-Services den Sicherheitsanforderungen genügen (Risiken sind beherrschbar). Was wird gebraucht?

A. Ein Steuerungsmodell, das die Beziehung zwischen Anwenderorganisation und IT-Dienstleister grundsätzlich ordnet,

B. Eine Logik der technologischen Vervollständigung der IT-Services durch Integration von Leistungen von Anwenderorganisation und Dienstleistern,

C. Eine Logik der verfahrenstechnischen Vervollständigung der IT-Services durch Integration von Leistungen von Anwenderorganisation und Dienstleistern,

D. Das Verständnis der Strategien bei der Beschaffung einerseits und der Angebotsgestaltung andererseits vor dem Hintergrund industrialisierter IT,

E. Ein Referenzmodell für den Ablauf der Geschäftsbeziehung zwischen Anwenderorganisation und Dienstleistern verschränkt mit dem Lebenszyklus von IT-Services im Cloud-Zeitalter,

F. Ein einfaches Modell für das *Joint Security Management*, das

   (a) alle Aufgaben übersichtlich in Bereiche ordnet,

   (b) die Aufgaben der Anwenderorganisation und die des IT-Dienstleisters einander zuordnet,

   (c) diese Aufgaben der beiden Partner miteinander verzahnt,

   so dass

   (d) jede Partei genau weiß, was zu tun ist, und

   (e) der Mehrwert der Zusammenarbeit klar und deutlich wird.

Hinweise

Joint Security Management bedeutet, organisationsübergreifend zu handeln. Von welchen „Organisationen" reden wir? In diesem Buch legen wir ein einfaches Modell zugrunde, das aus zwei bzw. drei Parteien besteht.

- Wir sprechen stets von **Anwenderorganisation** (die immer links in den Abbildungen angeordnet ist), wenn wir eine Firma, Behörde oder eine Geschäftseinheit meinen, *die IT-Services nutzt, ohne sie selbst zu produzieren*. Es kann sich

also um einen Automobilkonzern, eine Stadtverwaltung, eine Nichtregierungsorganisation oder anderes handeln.

- Wir sprechen stets von **IT-Dienstleister** (der immer rechts in Abbildungen auftaucht), wenn wir die IT-Firma oder Organisation meinen, *die die IT-Services für die Anwenderorganisation bereitstellt und deren Vertragspartner ist*. Implizit setzen wir dabei voraus, dass der IT-Dienstleister die IT-Systeme auch selbst bereitstellt und betreibt, die IT-Services also selbst produziert.[2] In den meisten Fällen werden wir zudem annehmen, dass der IT-Dienstleister seine IT-Services auf dem freien Markt anbietet. In vielen Fällen kann es sich aber auch um eine sehr große interne IT-Abteilung handeln, die ihre Dienste diversen Geschäftseinheiten z.B. innerhalb eines Konzerns anbietet.
- Wir sprechen von **Zulieferern**, wenn wir andere IT-Firmen oder Organisationen meinen, *die keine direkte Vertragsbeziehung mit der Anwenderorganisation unterhalten*, sondern einen Beitrag dazu leisten, dass der IT-Dienstleister seinen Vertrag erfüllen kann. D.h., sie liefern IT-Komponenten oder IT-Systeme oder übernehmen Aktivitäten im IT-Service-Management während der Bereitstellung, zur Aufrechterhaltung oder zur Verbesserung der IT-Services.

Der von uns meist angenommene Normalfall betrifft eine Firma, Behörde oder Organisation, die IT-Services bei einer IT-Firma einkauft. Doch was verstehen wir unter IT-Services?

- Mit **IT-Service** bezeichnen wir den Liefergegenstand eines Lieferanten (IT-Dienstleister oder Zulieferer). Wir unterscheiden in vielen Fällen nicht, ob es sich um eine IT-Komponente, ein IT-System, um eine komplette IT-Dienstleistung oder um einzelne Aktivitäten im IT-Service-Management (während der Entwicklung und Implementierung, der Bereitstellung, zur Aufrechterhaltung oder zur Verbesserung der IT-Services) handelt. Falls eine solche Differenzierung erforderlich ist, weisen wir darauf hin.
- In den allermeisten Fällen bezieht sich der Begriff **IT-Service** auf alles, was die Anwenderorganisation nutzt. Der Leser möge sich dabei immer vorstellen, dass der IT-Service bzw. die IT-Services von *einem* IT-Dienstleister bereitgestellt werden. Sollte es für das Verständnis wichtig sein, dass *mehr als ein* IT-Dienstleister beteiligt ist, werden wir darauf hinweisen.

In diesem Buch verweisen wir durchgängig auf die **IT-Sicherheit**, denn darum geht es ja beim *Joint Security Management*. Wir verstehen diesen Begriff so, dass er den Schutz von IT-Systemen und den Schutz von Informationen umfasst, die in IT-Systemen verarbeitet werden. Der Begriff Schutz bezieht sich dabei primär auf die Sicherheitsziele der Erhaltung von **Vertraulichkeit**, **Integrität** und **Verfügbarkeit**.

---

[2] Falls der Vertragspartner der Anwenderorganisation z.B. nur ein Wiederverkäufer ist, werden wir explizit darauf hinweisen.

Spätestens jedoch mit dem Internet-der-Dinge (IoT) und der fortschreitenden Digitalisierung aller möglichen Geschäftsprozesse kommen die Aspekte **Safety** (Funktionssicherheit und Unbedenklichkeit) bzw. **Reliability** (Zuverlässigkeit) hinzu. Das macht IT-Sicherheit schwieriger, weil wir nicht unmittelbar wissen, welche Folgen ein unzureichender Schutz haben kann.

Wir haben uns bemüht, dieses Buch sehr strukturiert aufzubauen. Schließlich haben wir in unserem zuvor erschienenen Buch eine Sicherheits*architektur (ESARIS)* vorgestellt.

- Jedem Kapitel (und Unterkapitel) ist ein Abschnitt **„Einführung und Zusammenfassung“** vorangestellt. Der Leser sollte jedoch nicht erwarten, dass in den wenigen Sätzen alle wichtigen Sachverhalte angesprochen werden.
- Wir machen ausführlich davon Gebrauch, unsere Ausführungen durch **Schaubilder** zu untermauern. Dies sollte für Architekten selbstverständlich sein. Doch später mehr dazu. Auch hier gilt: Die Schaubilder untermauern den Text lediglich.
- Alle **Referenzen** sind als Fußnoten aufgeführt, so dass das lästige Blättern entfällt. Dieses Buch enthält ein sehr ausführliches **Glossar**, das viele wichtige Begriffe erläutert. Es ist nach Themen gegliedert und kann daher auch abschnittsweise gelesen werden. Ebenfalls möchten wir auf das liebevoll gepflegte **Stichwortregister (Index)** ganz am Ende des Buches hinweisen. Es hilft, wenn der Leser etwas sucht und das Inhaltsverzeichnis an seine Grenzen stößt.

Schon mit unserem ersten Buch haben wir uns um Standards bemüht. Auch dazu später mehr. IT-Sicherheit ist eine relativ junge Disziplin. Vielleicht liegt es daran, dass Standards rar sind, die der Komplexität der heutigen, industriellen IT-Produktion gerecht werden und sich der marktwirtschaftlichen Realität in der IT-Industrie stellen. Andere Branchen wie die Bauwirtschaft sind da schon weiter: Stürzen in Zentraleuropa Häuser zusammen, weil sie nicht fachgerecht geplant und gebaut wurden? Nein! Es gibt nämlich Standards, Bauvorschriften und sogar Genehmigungs- bzw. Zulassungsverfahren. Haben wir dergleichen auch für die Absicherung der IT? Stürzen IT-Systeme regelmäßig ab oder werden zweckentfremdet „genutzt“, weil sie nicht fachgerecht abgesichert wurden? Ja! – Dieses Buch soll einen Beitrag dafür leisten, dass sich das ändert.

1.2 Hintergründe: Arbeitsteilung und Vertrauenswürdigkeit

Einführung und Zusammenfassung: Für die meisten Sicherheitsprobleme gibt es technische und/oder organisatorische Lösungen. Allerdings machen die heutige Größe und Komplexität der IT ihre Implementierung zu einer echten Herausforderung. Doch die eigentliche Herausforderung für das Sicherheitsmanagement ergibt sich aus der zunehmenden Arbeitsteilung. Sie war uns Anlass für die Entwicklung von *ESARIS* und gibt auch den Anstoß für das *Joint Security*

Management. Wenn Anwender überlegen, ob sie einem IT-Service „trauen“ und ihn verwenden wollen, sammeln sie Informationen darüber, wie es mit der IT-Sicherheit bestellt ist. Dabei kalkulieren sie sehr gezielt das Maß an Wissen, dass keine nicht-akzeptierten Risiken bestehen. Je mehr sie wissen, desto höher ist die Vertrauenswürdigkeit (assurance), was jedoch mit einem höheren Aufwand für das Sicherheitsmanagement verbunden ist. Beim Nachdenken über ein *Joint Security Management (JSM)* muss man daher den Begriff der Vertrauenswürdigkeit im Auge behalten.

Größe, Komplexität, Arbeitsteilung

IT-Sicherheitsexperten haben in den letzten Jahrzehnten viele bewährte Verfahren (best practices) für die Absicherung von IT beschrieben. Die als „Orange Book“ bekannten TCSEC (Trusted Computer System Evaluation Criteria) des US-amerikanischen Verteidigungsministeriums aus dem Jahre 1983 markiert dabei wohl einen wichtigen Meilenstein aus den Anfängen der IT-Sicherheit. Später wurde die anfangs durch staatliche Organisationen dominierte Arbeit vor allem durch IT-Sicherheitsexperten großer Beratungshäuser und durch Standardisierungsgremien fortgesetzt. Heute dominieren oft Zusammenschlüsse bzw. Arbeitsgemeinschaften von Unternehmen und Herstellern die Definition von „Guidelines“. Bei der Lektüre sollte man immer daran denken, dass viele Dokumente und manche Strategie dem Kalkül eines Unternehmens folgt und dessen wirtschaftlichen Zielen dient. Man sollte zweitens nicht vergessen, dass viele Maßnahmen der IT-Sicherheit von IT-Experten bzw. den IT-Firmen entwickelt wurden. Oft haben die IT-*Sicherheits*-experten daran nur einen kleinen Anteil.

Uns stellt sich die aktuelle Situation von „Wissenschaft und Technik“ so dar: Für die meisten Sicherheitsprobleme gibt es technische und/oder organisatorische Lösungen. Oft bedarf es der Kombination beider. Natürlich sind die zunehmenden Bedrohungen ein Thema, da die Angriffe massiver werden und oft raffinierter ausgeführt werden. Dies führt dazu, dass Organisationen sich stärker um die Detektion (Aufklärung der Bedrohungssituation und Erkennen von Angriffen) und um die Reaktion (Vorbereitung für eine aktive Abwehr und eine Wiederherstellung des Betriebs) kümmern müssen. Die reine Protektion (Installation von Schutzmaßnahmen) reicht schon lange nicht mehr aus. Auch für die Detektion und die Reaktion gibt es methodische Ansätze sowie Produkte und Lösungen. Doch darum geht es nicht allein. Wir sehen diese beiden Herausforderungen:

- Größe und Komplexität (z.B. 50.000 Server anstelle von 50),
- Arbeitsteilung (z.B. komplexe Wertschöpfungsketten bzw. Wertschöpfungsnetze, in denen „IT“ entsteht und zur Verfügung gestellt wird).

Wir glauben, dass diese beiden Punkte einen ganz wesentlichen Unterschied machen, dass sie die Art und Weise, wie Sicherheitsmanagement zu erfolgen hat, wesentlich beeinflussen und dass diese Themen in Bezug auf die IT-Sicherheit bisher unzureichend bearbeitet wurden.

Was ist damit gemeint? Wir beginnen mit dem ersten Punkt: Größe und Komplexität. Der Betrieb und die aktive Verwaltung und Pflege von 50 Computern kann eine herausfordernde Tätigkeit sein. Aber ein kleines Team sollte dafür ausreichen, wenn die Bedingungen stimmen. Die Menschen in diesem Team kennen einander, und sie können direkt miteinander kommunizieren und sich abstimmen. Wird eine Herausforderung oder ein Problem erkannt, so wird dies geeignet kommuniziert und die Lösung einer oder mehreren Personen übertragen. Wurde die Lösung implementiert, wird dafür gesorgt, dass dies bekannt ist. Gibt es Schwierigkeiten, können sich die Personen direkt an ihnen bekannte Kollegen/Kolleginnen wenden, die entsprechend unterstützen. Soweit, so gut. Beim Betrieb von 5.000 Servern sieht es sicher schon etwas anders aus. Spätestens dann, wenn es aber z.B. um 50.000 Server geht, erkennt man, dass man eine andere Art der Arbeitsorganisation benötigt. Das gilt erst recht dann, wenn die vielen Server verschiedene IT-Services für viele Kunden bereitstellen und geografisch weit verteilt sind. Die Unterschiede sind wirklich gravierend. Während für 50 Server noch nicht einmal ein „richtiges" Rechenzentrum benötigt wird, erfordert die Installation von 50.000 Servern etwa eine Fläche von 9.000 m² nur für die IT *ohne* Stromversorgung und Klimatisierung. Zum Vergleich: Ein großes Fußballfeld hat ungefähr 7.100 m². Und in einer modernen IT kann jeder dieser physischen Server mehrere logische Server („virtuelle Maschinen") beheimaten. Natürlich sind die Server nur ein Teil der IT. Die Komplexität ist viel größer. Die 50.000 Server müssen vernetzt und mit der Außenwelt sowie mit zentralen Speichersystemen verbunden werden. Nicht nur die Netzwerke hierfür, auch die Speichersysteme (storage systems) sind kompliziert auch hinsichtlich ihrer adäquaten Absicherung. Wir werden dies in Kap. 3 ein wenig vertiefen.

Stellen Sie sich eine Arbeitsanleitung für die Absicherung dieser IT vor! Es gibt nicht „die eine Anleitung für die IT-Sicherheit". Wir sind damit beim zweiten Thema: der Arbeitsteilung. Es gibt auch nicht „das eine Team". Alles ist anders, als bei den 50 Servern. Die Dinge sind viel zu kompliziert und vielschichtig, als dass sie von einzelnen Experten vollständig durchdrungen, verstanden und beherrscht werden könnten. Das Knowhow ist verteilt in vielen Köpfen. Personen, Teams und ganze Abteilungen sind hochgradig spezialisiert. Doch wie bringt man sie zusammen? Wie sorgt man dafür, dass Teams, die das Gleiche in unterschiedlichen Regionen oder für unterschiedliche IT-Systeme tun, nach den gleichen Standards handeln, um das gleiche Sicherheitsniveau zu garantieren? Wie sollen sie kommunizieren, damit die besten Ideen aus den verteilten Quellen allen zugutekommen und von allen als gemeinsamer Standard akzeptiert und umgesetzt werden? Wie koordiniert man die Arbeit von Teams, die ganz unterschiedliche Dinge tun, dergestalt, dass die von ihnen implementierten Sicherheitsmaßnahmen sich gegenseitig verstärken und am Ende ein sicheres Ganzes entsteht? Wie stellt man sicher, dass die letztendlich erreichte Sicherheit den für die Organisation definierten Zielen und Richtlinien entspricht? In unserem zuletzt erschienenen Buch haben wir

dafür Lösungen vorgestellt, die wir in einer Architektur namens *ESARIS* zusammengefasst haben.[3] Wir werden auf einen Teil davon in Kap. 4 eingehen.

Die IT-Sicherheit wird immer noch zu sehr als die Aufgabe eines Unternehmens oder einer Organisation gesehen. Doch die industrielle Realität hat dem längst die Grundlage entzogen.

Die Arbeitsteilung erfolgt zunehmend zwischen Unternehmen, die Produkte und Dienstleistungen über den freien Markt austauschen. Damit werden die meisten Entscheidungen hinsichtlich der IT-Sicherheit nicht mehr innerhalb einer Organisation getroffen. Dies führt dazu, dass das Sicherheitsmanagement nicht mehr ausschließlich innerhalb einer Organisation stattfinden kann. Es wird daher ein zunehmend *organisationsübergreifendes* Sicherheitsmanagement benötigt. Wir nennen unseren Ansatz dafür *Joint Security Management (JSM)*.

Sicherheit? Vertrauenswürdigkeit!

Sicherheit ist ein abstrakter Begriff. Die beste Definition ist: Sicherheit ist die Abwesenheit nicht-akzeptierter Risiken. Diese Definition setzt aber voraus, dass alle Risiken bekannt sind und auch analysiert wurden. Der Vorteil dieser Definition besteht darin, dass sie deutlich macht, dass es sich bei der IT-Sicherheit nicht um eine absolute Größe handelt, sondern dass eine Entscheidung basierend auf Einschätzungen zu erfolgen hat. Wenn Anwender überlegen, ob sie einem IT-Service „trauen“ und ihn verwenden wollen, werden sie also Informationen darüber sammeln, wie es mit dessen IT-Sicherheit bestellt ist.

Ein naheliegender Ansatz könnte darin bestehen, möglichst viele Informationen zu sammeln, um eine möglichst gute und fundierte Entscheidung treffen zu können. Doch Entscheidungen und Einschätzungen können sich nicht auf vollständige Informationen stützen. Warum? Vollständige Informationen zu bekommen, ist schon im eigenen Unternehmen sehr schwierig. Die Ausführungen zu „Größe und Komplexität“ sollten dies verdeutlicht haben. In einer industriellen Wertschöpfungskette mit mehreren Firmen ist es sogar ganz unmöglich und auch unökonomisch, vollständige Informationen zu beschaffen oder zu bearbeiten. Die bisherigen Ausführungen zur Arbeitsteilung konnten dies sicher nicht vollständig zeigen, aber man kann sich vorstellen, dass es bedeutend schwieriger wird, wenn die Informationen in einem ganzen Industriezweig verteilt sind.

Aber schwierig heißt nicht unmöglich. Doch wir sehen es so:

- Anwender benötigen zwar Informationen, um entscheiden zu können, ob sie einen IT-Service als „sicher“ ansehen und daher nutzen wollen. Es ist aber gar

---

[3] 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 [51]

nicht wünschenswert, zu viele Informationen zur IT-Sicherheit zu haben und zu verarbeiten. Es werden nur „die richtigen Informationen" benötigt.

- Die notwendigen Entscheidungen treffen Anwender nicht aufgrund von Einzelinformationen bzgl. der IT-Sicherheit, sondern aufgrund dessen, was mit „Vertrauenswürdigkeit" bezeichnet wird. Der Begriff Vertrauenswürdigkeit (assurance) muss stärker in den Mittelpunkt der Betrachtungen gerückt werden, wenn es um „Sicherheitsmanagement" geht.

Was bedeutet dies? Warum sollen Anwender *nicht* möglichst viel wissen wollen, wenn es um ihre Entscheidung geht, ob sie einen IT-Service nutzen wollen, weil sie ihn für „sicher" halten? Die Antwort ist einfach, auch wenn viele Sicherheitsexperten sie manchmal ungern hören wollen: Die Beschaffung und Bewertung einer solchen großen Informationsmenge würde schlicht der Arbeitsteilung und der Industrialisierung widersprechen. Der Vorteil der Industrialisierung mit Arbeitsteilung und Spezialisierung besteht ja gerade darin, dass eine produzierende Partei die Verantwortung übernimmt (der IT-Dienstleister) und die andere konsumierende Partei (die Anwenderorganisation) der Nutznießer ist und sich um die vielen Themen und Details eben *nicht* kümmern muss.

IT-Sicherheitsexperten müssen ökonomisch denken. Ihr Denken und Handeln muss den durch die Anwenderorganisation (ihren „Arbeitgeber") gesetzten Prioritäten folgen und nicht umgekehrt.

Die zweite Einsicht besteht, wie bereits angedeutet, darin, dass Menschen wie folgt vorgehen: Wenn sie einen Zug besteigen, sich in ein Flugzeug setzen oder ein Zahlungsverkehrssystem nutzen, bewerten sie nicht wirklich die Sicherheit. Sie schätzen ein, ob ihnen das System *vertrauenswürdig* genug ist. Dies hat viel mit dem zu tun, was wir Reputation nennen und auf Einschätzungen und Erfahrungen anderer zurückgeht. Bevor wir ein Beispiel ausführen, kurz ein Bonmot, dass uns zum Kern führt: „In diesem Restaurant ist es so voll, da geht keiner mehr hin." Spätestens beim zweiten Lesen wird einem klar, dass hier etwas nicht stimmen kann. Und doch ist es so, dass die Annahme oder das Gerücht, es wäre zu voll, dazu führen kann, dass das Restaurant leer bleibt. Zu einem Beispiel: Einer der Autoren hat mit einem Kollegen Ende der 1990er Jahre im Auftrag einer großen deutschen Bank die Sicherheit von Ecash untersucht. Ecash ist ein Bezahlsystem mit digitalen Münzen im Internet, das Anonymität mit Sicherheit verbindet. Es wurde von David Chaum erfunden und basiert u.a. auf der genialen Erfindung der „blinden Signatur". Bei der Untersuchung zeigte sich, dass die technische Realisierung recht kompliziert und fehleranfällig ist. Immer wieder haben wir Implementierungsfehler gefunden, die dann beseitigt werden mussten. Am Ende war das Vertrauen der Bank soweit gesunken, dass das System nicht eingeführt wurde. Die Anzahl und Schwere von Sicherheitslücken spielt dann keine Rolle mehr. Die Entscheidung basierte nicht primär auf einer Bewertung der IT-Sicherheit, sondern auf der Einschätzung der Vertrauenswürdigkeit.

Anwender verwenden Produkte und Dienstleistungen Dritter eben nicht, weil die IT-Sicherheit ein bestimmtes Niveau erreicht hat, sondern weil sie überzeugt sind, dass keine nicht-akzeptierten oder nicht-akzeptablen Risiken bestehen. Diese Überzeugung gründet auf *unvollständiger* Information, und der Begriff Vertrauenswürdigkeit bietet den Spielraum dafür, das Maß an Information bzw. Wissen entsprechend den Bedürfnissen des Anwenders zu steuern. Vertrauenswürdigkeit ist das Maß an Wissen, dass keine nicht-akzeptierten bzw. nicht-akzeptablen Risiken bestehen, das Produkt oder der IT-Service also als sicher gelten kann. Entscheidungen von Anwendern gründen auf dieser relativen, individuell einstellbaren Skala.

Keine Chipkarte, kein Terminal, kein elektronisches Pin-Pad wird ohne eine Sicherheitsüberprüfung (Evaluierung) eingesetzt. Die Bauartzulassung auf Basis eines positiven Sicherheitsgutachtens ist die Voraussetzung dafür, dass Banken und Netzbetreiber diese Komponenten in Zahlungsverkehrssystemen mit Kredit- und EC-Karten einsetzen dürfen. Die Evaluierungen basieren auf Sicherheitsvorgaben. Diese definieren funktionale Anforderungen (z.B. PIN-Authentisierung nötig). Vor allem beinhalten sie aber sogenannte Vertrauenswürdigkeitsanforderungen, die den Umfang und die Tiefe der Sicherheitsüberprüfungen festlegen. Beispiele für solche Vertrauenswürdigkeitsanforderungen sind in Abb. 2 dargestellt. Sie sind auf jede Sicherheitsfunktion bzw. funktionale Anforderung anzuwenden bzw. beziehen sich auf diese.

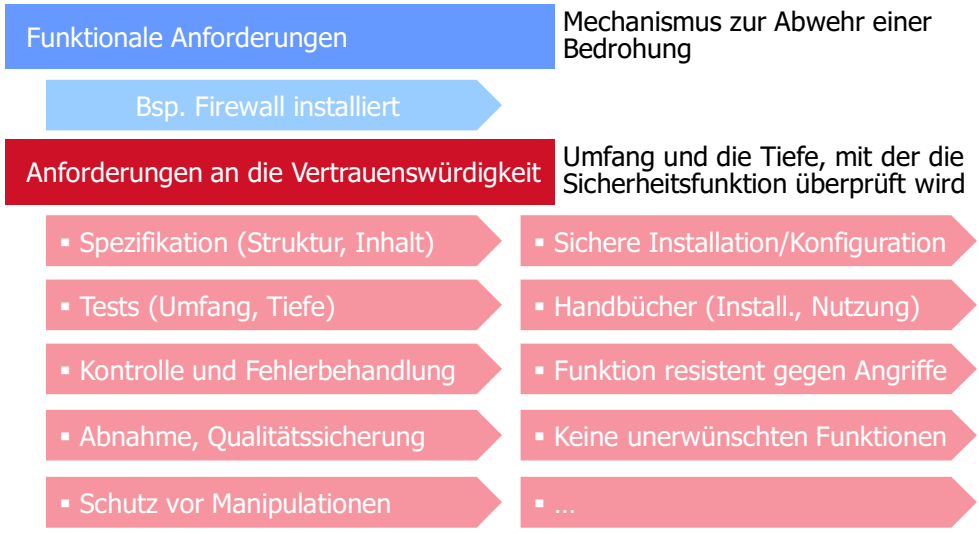

Abb. 2: IT-Sicherheit und die Rolle der Vertrauenswürdigkeit

Im Falle von Zahlungsverkehrssystemen sind die Vertrauenswürdigkeitsanforderungen aufgrund des hohen Risikos (es geht um viel Geld) eher umfangreich. Das Gleiche gilt für Evaluierungen z.B. von Hypervisoren, die eine zentrale Rolle in Cloud-Infrastrukturen spielen. In den für solche Produkte verwendeten Kriterien

für Sicherheitsuntersuchungen[4] werden sogenannte Evaluation-Assurance-Levels (EAL) definiert. Sie ermöglichen eine Abstufung der erreichten Vertrauenswürdigkeit durch Anpassung des Umfangs und der Tiefe der herangezogenen und geprüften Informationen. Je nach Risiko bzw. Risikotoleranz werden weniger oder mehr Informationen bereitgestellt bzw. Überprüfungen und Tests durchgeführt. In der folgenden Liste, welche die Abb. 2 etwas näher erläutert, kann man sich an jeder Stelle fragen, ob diese Dinge zu prüfen oder zu wissen notwendig sind, bevor eine Entscheidung getroffen werden kann, ob das Produkt oder der IT-Service akzeptiert und genutzt werden soll.

- Funktionale Anforderungen (an die IT-Sicherheit):
  - Daten werden verschlüsselt,
  - …[5]
- Anforderungen an die Vertrauenswürdigkeit:
  - Funktion wirkt/funktioniert (wurde getestet),
  - Funktion wurde sachgemäß entwickelt und implementiert,
  - Funktion wurde nachvollziehbar entwickelt und implementiert; die Entwicklungsdokumentation erfolgt hierarchisch, schrittweise verfeinernd,
  - Fehler bei der Entwicklung und Implementierung werden z.B. durch ein Konfigurationsmanagementsystem sowie Abnahme- und Qualitätssicherungsverfahren vermieden,
  - unautorisierte Einwirkung bzw. Manipulation wird wirksam verhindert und zwar während der Entwicklung, Herstellung und Installation,
  - Produkt wurde nicht durch eine Fälschung ersetzt oder während der Auslieferung manipuliert,
  - Funktion bzw. Produkt wurde sicher installiert und konfiguriert,
  - Nutzer (insbesondere Administratoren) verfügen über Handbücher, die alle notwendigen Informationen für die sichere Installation, Nutzung und Pflege der Funktion oder des Produktes geben,
  - Funktion kann nicht umgangen oder mit realistischem Aufwand überwunden werden,
  - es sind keine Funktionen implementiert, mit denen die Sicherheitsfunktionen umgangen oder manipuliert werden können.

Erst durch die Prüfung der Vertrauenswürdigkeitsanforderungen wird klar, ob die Sicherheits*funktionen* überhaupt ausreichend zur Erfüllung der IT-Sicherheitsanforderungen beitragen.

---

[4] Common Criteria: ISO/IEC 15408 – Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components; 2008 [4]

[5] Auch die funktionalen Anforderungen hat man versucht zu „standardisieren“: ISO/IEC 15408 – Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components; July 2008 [3]