Joint Security Management (JSM): organisationsübergreifend handeln (2017-2018)

Eberhard von Faber

Oktober 2019

Als wichtiger Ideengeber in der Firma und als nebenberuflicher Professor für IT-Sicherheit erhebe ich für mich selbst den Anspruch, wissenschaftlich tätig zu sein und die Ergebnisse meiner Überlegungen der Öffentlichkeit vorzustellen, damit sie aufgegriffen und diskutiert werden können. Nachdem ich ab 2010 mit *ESARIS* eine Sicherheitsarchitektur für IT-Dienstleister bzw. eine großtechnische IT-Produktion entwickelt und eingeführt hatte, begann ich Ende 2016, einen neuen Gedanken umzusetzen. Während *ESARIS* eine Blaupause für IT-Dienstleister war, wollte ich nun die Anwenderunternehmen stärker in den Blick nehmen. Anwenderunternehmen (Unternehmen und Institutionen, die IT nutzen) produzieren die für die Digitalisierung ihrer Geschäftsprozesse benötigten IT-Services immer seltener mit eigenem Personal und Mitteln. Vielmehr nutzen sie die Angebote spezialisierter IT-Dienstleister. Früher hieß das „IT-Outsourcing“, heute spricht man vereinfachend häufig einfach von „Auslagerung“ in „die Cloud“. Damit dabei die IT-Sicherheit adäquat berücksichtigt wird, die Risiken also beherrschbar bleiben, müssen Anwender und Dienstleister einiges tun und vor allem kooperativ zusammenarbeiten. Aber wie? Und was sollen sie tun? Aus einigen Beispielen aus meiner beruflichen Erfahrungswelt formte ich schließlich ein neues Modell, das *Joint Security Management (JSM)*. Abb. 1 zeigt mich bei einem Vortrag zum Thema Anfang 2018. Zu dieser Zeit ist mein Buch darüber im Druck, das im April erscheint.

Abb. 1: Bei einem Vortrag im Januar 2019 (Bild aus einem Fernsehbeitrag)

Obwohl die Notwendigkeit punktueller Zusammenarbeit zwischen Anwender und Anbieter prinzipiell bekannt ist, fehlte es bisher an einem systematischen Ansatz. Das JSM gibt Anwendern wie Dienstleistern die notwendige Orientierung und Anleitung. Viele Unternehmen schrecken davor zurück, ihre Daten und Anwendungen in „die Cloud“ zu geben, weil Unsicherheit bezüglich der IT-Sicherheit besteht. Mit JSM kann dies systematisch angegangen werden. Die Anleitung führt durch die wichtigsten Themen.

Situation und Kurzfassung

Kein Unternehmen kann heute noch komplexe IT-Services marktgerecht aus eigener Kraft bereitstellen. Anwenderunternehmen bedienen sich spezialisierter IT-Dienstleister und letztere greifen auf Komponenten und Dienste aus einem weit gefächerten Zuliefernetzwerk zurück. Dies ist Folge einer zunehmenden Industrialisierung der IT-Produktion, die durch eine starke Arbeitsteilung gekennzeichnet ist. Damit dabei die Sicherheit nicht auf der Strecke bleibt, wird ein unternehmensübergreifendes Sicherheitsmanagement benötigt. Es gibt Standards und Literatur, die Aufbau und Funktion eines Informations-Sicherheits-Management-Systems (ISMS) beschreiben. Allerdings sind diese ISMS auf ein Unternehmen bezogen und verlassen die Unternehmensgrenze praktisch nicht. Das leuchtet erst einmal auch ein, denn man kann nur das regeln, was man auch unter Kontrolle hat. Allerdings hat sich die IT und die Verantwortung dafür längst stark ausgedehnt und den engen Rahmen eines Unternehmens verlassen. Das Internet und seine zentralen Anwendungen geben ein beredtes Zeugnis dafür ab. Im Umfeld der Geschäfts- und Großkunden ist die Komplexität des „Liefernetzwerks“ oder der Wertschöpfungskette meist besonders groß.

Das *Joint Security Management* ist ein auf der Sicherheitsarchitektur *ESARIS* basierender Ansatz, bei dem die Interaktion zwischen rechtlich verschiedenen Organisationen von vornherein im Mittelpunkt steht.[1] 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. JSM beschreibt nicht einfach das bekannte Sicherheitsmanagement unter Hinzufügung zweier Rollen.[2] Das *Joint Security Management* baut das Sicherheitsmanagement vielmehr neu auf entlang des Skeletts der industriellen, marktwirtschaftlichen Prozesse und der für moderne IT charakteristischen Wertschöpfungsketten.

Ableitung der Struktur des JSM

Ausgangspunkt ist die in Abb. 2 veranschaulichte Situation. Links ist die Anwenderorganisation und rechts ist der IT-Dienstleister. Die blauen Pfeile stellen die Erwartungen bzw. Lieferleistungen der jeweiligen Seite dar.

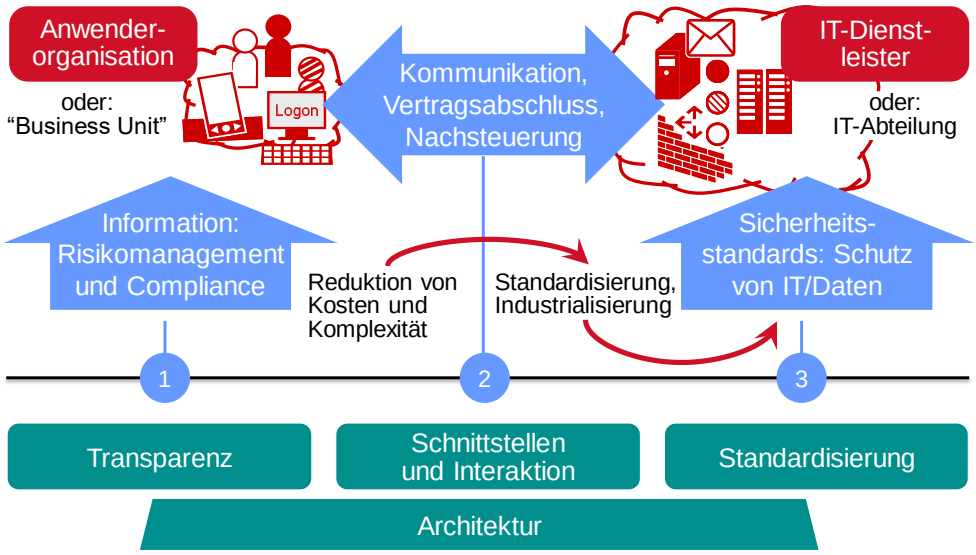


Abb. 2: Situation mit Anforderungen und Lösungen und Ableitung des Steuerungsmodells

---

1 Das *JSM* funktioniert auf Basis von *ESARIS* am besten (siehe Literatur am Ende des Artikels). *ESARIS* muss aber nicht unbedingt und nicht vollständig umgesetzt sein. Davon unabhängig gibt es Parallelen: *JSM* setzt das *ESARIS Customer Fulfillment Model* (kurz: *ESARIS Fulfillment Model)* um und nutzt das Prozessverständnis von *ESARIS* und einige Modularisierungsmodelle (wie *ESARIS Security Taxonomy* und *Provider Scope of Control*).

2 Das ist etwa in ISO/IEC 27017 eher der Fall.

Das in Abb. 2 dargestellte *ESARIS*-Steuerungsmodell bildet eine Grundlage für das *Joint Security Management (JSM)*, indem es die Interessen von Anwenderorganisation und IT-Dienstleister zusammenführt und dabei vier Aspekte hervorhebt. In Abb. 3 ist es in der oberen Hälfte in verkürzter Form dargestellt (grün und rot).

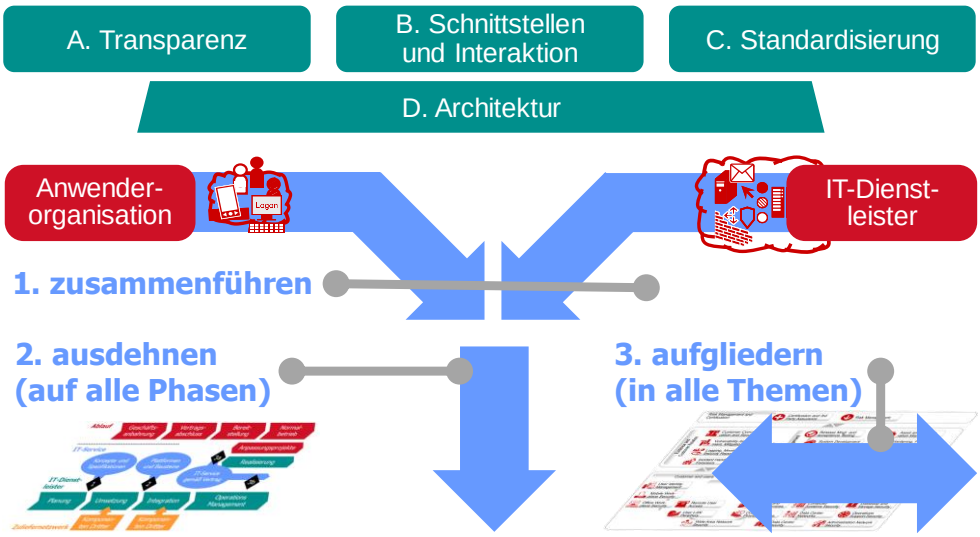


Abb. 3: Vom Steuerungsmodell zum Joint Security Management

Ausgehend von diesen vier Grundbausteinen bzw. Themenkomplexen werden drei „Operationen" vorgenommen, die in Abb. 3 blau dargestellt sind. 1) Das „Zusammenführen" betrifft das Vorhaben, ein gemeinsamen, organisationsübergreifenden Sicherheitsmanagements zu schaffen, wie es gleich in der nächsten Abbildung dargestellt und dann ausgearbeitet wird. Die Details folgen aus den beiden anderen Operationen: 2) „Ausdehnen": Das gemeinsame Sicherheitsmanagements muss über die einzelnen Phasen der Zusammenarbeit im Sinne eines Lebenszyklus betrachtet werden. Insbesondere unterscheiden sich Schnittstellen (beteiligte Rollen und Aufgaben) je nachdem, ob man sich z.B. in der Phase der Geschäftsanbahnung oder im laufenden IT-Betrieb befindet, deutlich. 3) In jeder Phase müssen jeweils die relevanten Themen betrachtet werden. Das ist mit „Aufgliederung" gemeint.

Ergebnis: Das JSM in der Übersicht

Als Ergebnis entsteht das *Joint Security Management (JSM)*, das in Abb. 4 zusammengefasst ist. Links stehen die Aufgaben der Anwenderorganisation, rechts die des IT-Dienstleisters. Während beide Parteien anfangs noch unabhängig voneinander agieren, verschmelzen ihre Aktivitäten mit Beginn der Zusammenarbeit. Die Zeitachse der Geschäftsbeziehung verläuft von oben nach unten. Das gibt dem Verlauf eine „Y"-Form. Die obere Hälfte umfasst die Vorbereitungsphase, die untere die Betriebsphase. Die neun farbigen Schilder stehen für neun Aufgabenbereiche. Ein in der Mitte stehendes Schild signalisiert „enge Verflechtung und Zusammenarbeit" – ganz im Sinne des *Joint Security Managements*. Die Bullet-Punkte sind Teilaufgaben, die jeweils genau definiert und ausgeführt sind. Dabei wird die Verflechtung (Zusammenarbeit) hervorgehoben.

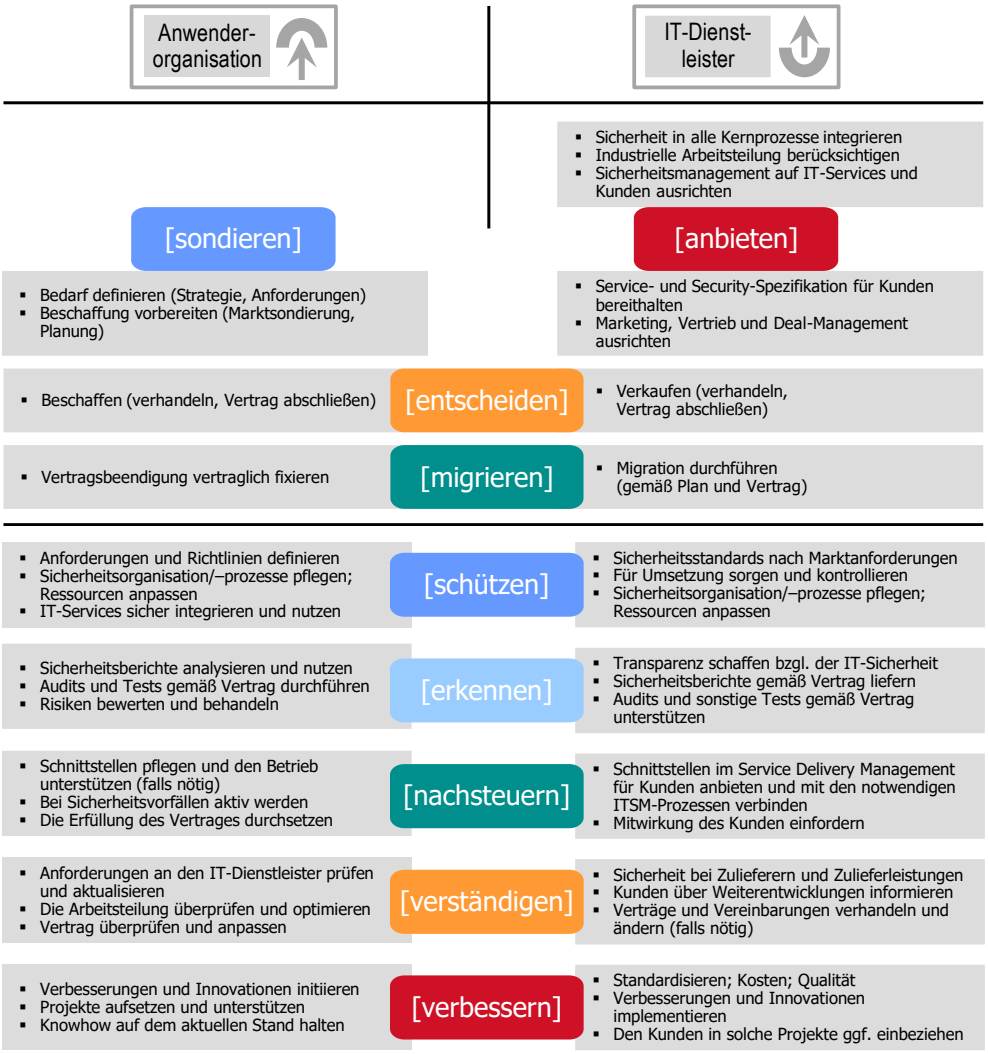


Abb. 4: Zusammenfassung der Aufgaben im Joint Security Management

Es folgt eine sehr kurze Übersicht über alle neun Aufgabenbereiche.

[anbieten]: die Hausaufgaben der IT-Dienstleister

Bevor der Kunde in das Blickfeld des IT-Dienstleisters kommt, muss der IT-Dienstleister das Sicherheitsmanagement auf das Kerngeschäft seiner industrialisierten IT-Produktion ausrichten. Das Prinzip „secured by definition“ entstammt *ESARIS*. Die eigentliche und zentrale Aufgabe im Kontext des *Joint Security Managements (JSM)* besteht jedoch darin, das Sicherheitsmanagement auf die Kunden auszurichten. Dazu ist viel mehr nötig, als man anzunehmen geneigt ist.

[sondieren]: Markt analysieren und Angebote bewerten

In der Phase der Geschäftsanbahnung geht es für die Anwenderorganisation vor allem darum, die eigenen Anforderungen zu kennen und zu dokumentieren. Komplexe Geschäfte werden häufig über sogenannte Ausschreibungen vergeben, bei weniger komplexen Geschäften kann sich die Anwenderorganisation auf die Bewertung der Angebote der IT-Dienstleister konzentrieren. In allen Fällen muss überlegt werden, was getan werden soll, wenn Erwartungen oder Anforderungen nicht erfüllt werden können.

[entscheiden] einigen und Vertrag abschließen

Dies ist der erste vollständig gemeinsame Aufgabenbereich. Eine Entscheidung basiert auf einem umfangreichen Vergleich zwischen den Anforderungen und den wirklich implementierten Sicherheitsmaßnahmen. In einem komplexeren Vertrag (deal) ist dies nur mit einem systematischen Ansatz praktikabel umsetzbar, denn komplexere Kundenlösungen werden aus diversen, im Servicekatalog beschriebenen Bausteinen zusammengestellt. Beide Seiten müssen zudem bis zum Ende der

Vorbereitungsphase bestimmte Rollen besetzen, um im Sinne des *Joint Security Managements* zusammenzuarbeiten.

[migrieren]: Übergabe und Anpassungen

Die Migrationsphase, in der der IT-Dienstleister das Geschäft übernimmt, kann sehr unterschiedlich ablaufen. Wie jeder Umzug muss er sorgfältig vorbereitet werden, gerade was die IT-Sicherheit anbelangt. In der Phase der Bereitstellung erfolgen nach der Migration verschiedene Modernisierungen (Anpassungen). Beim Übergang aus diesen Projekten in den normalen Betriebsmodus muss insbesondere der Übergang der Verantwortung (für die IT-Sicherheit) sorgfältig geplant und durchgeführt werden.

[schützen]: Unterbau und Überbau entwickeln

Dies ist das erste Arbeitsgebiet der Betriebsphase. Der IT-Dienstleister realisiert Sicherheit als Standard gemäß den Standards, die er während der Betriebsphase aktualisiert und an neue Anforderungen anpasst. Die Anwenderorganisation ist Teil des Marktes, bestimmt also die Anforderungen mit. Es ist keine einfache Aufgabe zu entscheiden, welche Sicherheitsmaßnahmen bzw. Sicherheitslösungen an welcher Stelle integriert werden müssen. Aus diesem Grund wird ein Vorgehensmodell beschrieben, das für beide Partner von Bedeutung ist. Den eigentlichen Unterbau und Überbau in diesem Aufgabenbereich bilden Rollen bzw. Expertenprofile für das *Joint Security Management*, die beide Seiten schaffen und besetzen müssen.

[erkennen]: Transparenz schaffen und nutzen

Es ist die Aufgabe des IT-Dienstleisters, die für beide Partner benötigten Informationen zur IT-Sicherheit bereitzustellen. Die Anwenderorganisation kontrolliert und sieht sich in der Rolle des Überwachenden, wobei sie gegebenenfalls selbst Informationen erfasst (z.B. bei Audits), Sicherheitsberichte und dergleichen auswertet und natürlich für entsprechende Rückmeldungen an die Adresse des IT-Dienstleisters sorgen muss. Während in der Vorbereitungsphase mehr die konzeptionellen Nachweise im Vordergrund stehen, sind es im Normalbetrieb die betrieblichen Nachweise. *ESARIS* unterscheidet zwischen „contractual evidence“ (Vorbereitungsphase) und „operational evidence“ (Betrieb). Letztere bzw. die betrieblichen Nachweise sind für die Anwenderorganisation essentiell und bilden die Grundlage dafür, Anpassungen und Verbesserungen zu planen.

[nachsteuern]: Interaktion ermöglichen und unterstützen

IT und IT-Sicherheit bleiben nicht stehen. Obwohl die Durchführung der Änderungen dem IT-Dienstleister obliegt, ist bei vielen Änderungen die Mitwirkung der Anwenderorganisation angezeigt. Größere Änderungen werden häufig von der Anwenderorganisation angestoßen. Damit beide Partner interagieren können, ist es nicht ausreichend, Rollen zu definieren und Personen zu benennen. Sie müssen in die prozessualen Abläufe integriert werden. Das genaue Verständnis der Aufgaben und Schnittstellen ist die Grundlage dafür.

[verständigen]: Vereinbarungen treffen und pflegen

Im weitesten Sinne geht es hier um das Beziehungs- und Vertragsmanagement als einem Bestandteil des Geschäfts der Anwenderorganisation und des IT-Dienstleisters, in dem die IT-Sicherheit ihren Platz einnehmen und verteidigen muss. Als der Verkäufer ist es der IT-Dienstleister, der die Vereinbarungen primär zu treffen hat. Es gibt sehr viele und sehr verschiedene Anlässe, warum eine erneute Verständigung auch in der Betriebsphase notwendig wird. Erstaunlich vieles, was einer Verständigung bedarf, geht dabei von der Anwenderorganisation aus, weshalb oft sie es ist, die Verträge aktualisieren will und kontinuierlich für deren Überprüfung sorgen sollte.

[verbessern]: Effektivität und Effizienz steigern

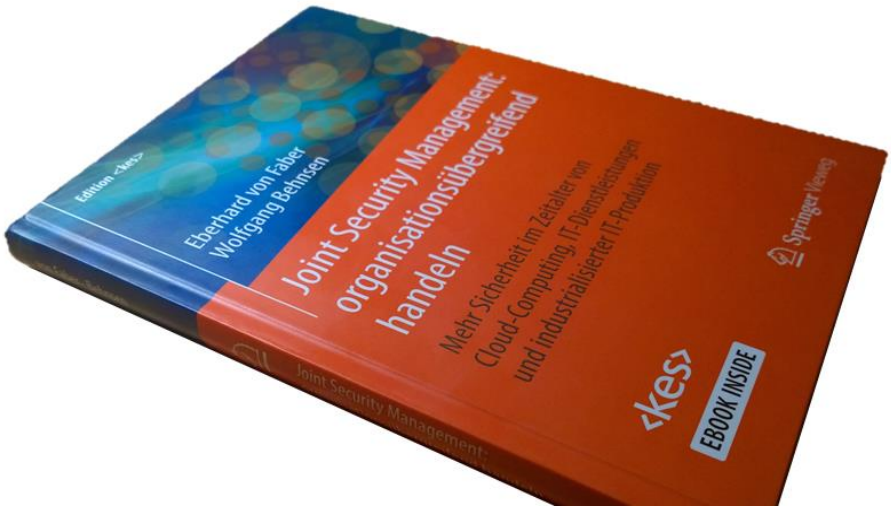
Eines der wichtigsten Ziele bei der Verbesserung von IT-Services bzw. deren Sicherheit besteht darin, die Effektivität und die Effizienz zu erhöhen. Oft ist es so, dass die entsprechenden Entwicklungs- und Realisierungs-projekte über den bestehenden Vertrag hinausgehen und zusätzlich durchgeführt werden oder zu Änderungen des bestehenden Vertrags führen. Während Verbesserungen in Richtung Effizienz in der Regel vom IT-Dienstleister initiiert werden, um wettbewerbsfähig zu bleiben, werden Projekte zur Erhöhung der Effektivität oft auch von der Anwenderorganisation angestoßen.

Jeder Aufgabenbereich wird aufgefächert in Einzelaufgaben (Bullet-Punkte in Abb. 4), die auch beschreiben, wie die Partner miteinander zusammenarbeiten und konkret interagieren. Dazu sind jeweils Schnittstellen nötig, die ebenso wie Expertenprofile bzw. Rollen definiert und implementiert werden müssen. Das *Joint Security Management (JSM)* geht weit über andere Ansätze für das Sicherheitsmanagement bzw. ein ISMS hinaus, setzt diese jedoch voraus.

Anwenderorganisationen und IT-Dienstleister sollten sich an der „Y"-Form des JSM orientieren und sich frühzeitig auf die Bearbeitung der einzelnen, den Aufgabenbereichen zugeordneten Aufgaben vorbereiten. Dabei ist zu beachten, dass diverse Aufgaben in späteren Phasen neben eigenen Vorbereitungen auch vertragliche Festlegungen benötigen. Jede der Aufgaben umfasst Aktivitäten, zu besetzende Rollen sowie die Interaktion zwischen Anwender und Anbieter im Sinne einer Schnittstellenbeschreibung. Die „Aktivitäten" ergeben sich aus der erwähnten Aufgliederung, wobei die zu betrachtenden Themen durch die *ESARIS Security Taxonomy* beschrieben sind. Sie umfassen die üblichen, in zahlreichen Sicherheitsstandards beschriebenen Disziplinen der IT-Sicherheit. Hinzukommen aber Erweiterungen der IT-Service-Management-Prozesse, da diese gemäß *ESARIS* die Umsetzung und Pflege der anderen, überwiegend technischen IT-Sicherheitsmaßnahmen sicherstellen müssen.

Schlussbemerkung

Das *Joint Security Management (JSM)* ist nicht im Auftrag meines Arbeitgebers entstanden, sondern auf eigene Veranlassung und in meiner Freizeit. Ich habe Freude daran, Dinge zu entwickeln und richtig gut zu machen. Viele Jahre und in verschiedenen Zusammenhängen habe ich als Berater auf dem Gebiet der IT-Sicherheit gearbeitet. Ich bin Professor für IT-Sicherheit und unterrichte seit 2008 im Masterstudiengang Security Management an der Technischen Hochschule Brandenburg. Dies ist eine nebenberufliche oder ehrenamtliche Tätigkeit, in der ich meine Fähigkeiten weiterentwickelt habe, Zusammenhänge anschaulich darzustellen und auf den Kern zu bringen. Im Jahr 2010 hat mir mein Arbeitgeber (ein großer IT-Dienstleister) die Aufgabe übertragen, die Absicherung aller IT/TK-Services zu verbessern und völlig neu zu organisieren. Ich entwickelte Dutzende neuer Methoden (die unter dem Namen *ESARIS* firmieren), führte existierende Sicherheitsstandards zusammen und verbesserte Transparenz, Effektivität und Effizienz.



Literatur

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, ISBN 978-3-658-20833-2, 244 Seiten, 60 farbige Abbildungen

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, ISBN 978-3-658-16481-2, 383 Seiten, 159 farbige Abbildungen, zweite aktualisierte und erweiterte Auflage