ESARIS: sichere IT-Services industriell herstellen (2010 - 2018)

Eberhard von Faber

Ende 2019

Im Jahre 2010 arbeitete ich bei einem großen IT/TK-Dienstleister wieder als Berater (IT-Sicherheit). Die Firma war erfolgreich. Sie hatte große Kunden gewonnen und mit ihnen großvolumige Abschlüsse getätigt. Die Zukunft hatte auch technisch Einzug gehalten, denn das Cloud-Computing lief seit einigen Jahren, auch wenn es anfangs noch nicht so hieß. Das erforderte und begünstigte auch die Professionalisierung der Herstellung, die sich zunehmend ordnete und vereinfachte. – Allerdings mussten ein paar Sicherheitsexperten und Sicherheitsmanager im Oktober 2010 wieder einmal feststellen, dass es große Schwierigkeiten bei der Absicherung der IT-Services gab. Sie mussten sich auch eingestehen, nicht zu wissen, wie man es wirklich besser macht. Die illustre Runde gab aber nicht auf, sondern den Weg frei für strategisches und strukturiertes Denken. Basierend auf einigen ersten Gedanken habe ich in den folgenden Wochen und Monaten einige Modelle und Methoden entwickelt. Sie bilden noch heute den Kern jener „Architektur", die heute unter dem Namen *Enterprise Security Architecture for Reliable ICT Services*, kurz *ESARIS*, bekannt ist. Immer wieder gab es Fragestellungen und Herausforderungen für die neue Antworten und Lösungen entwickelt und implementiert wurden. So wuchs *ESARIS* von 2010 bis 2018 zu einer komplexen Sammlung von bewährten Verfahren für die Absicherung einer großtechnischen IT-Produktion heran. Bewährt deshalb, weil das Ganze ab 2014 bei einem IT-Dienstleister eingeführt wurde, der in den Anfangsjahren etwa 45.000 Mitarbeiter in etwa 20 Ländern beschäftigte.[1] *ESARIS* hat immer wieder auch eine wichtige Rolle dabei gespielt, große Kunden zu gewinnen, bedeutende Deals abzuschließen und laufende Verträge zu erneuern.

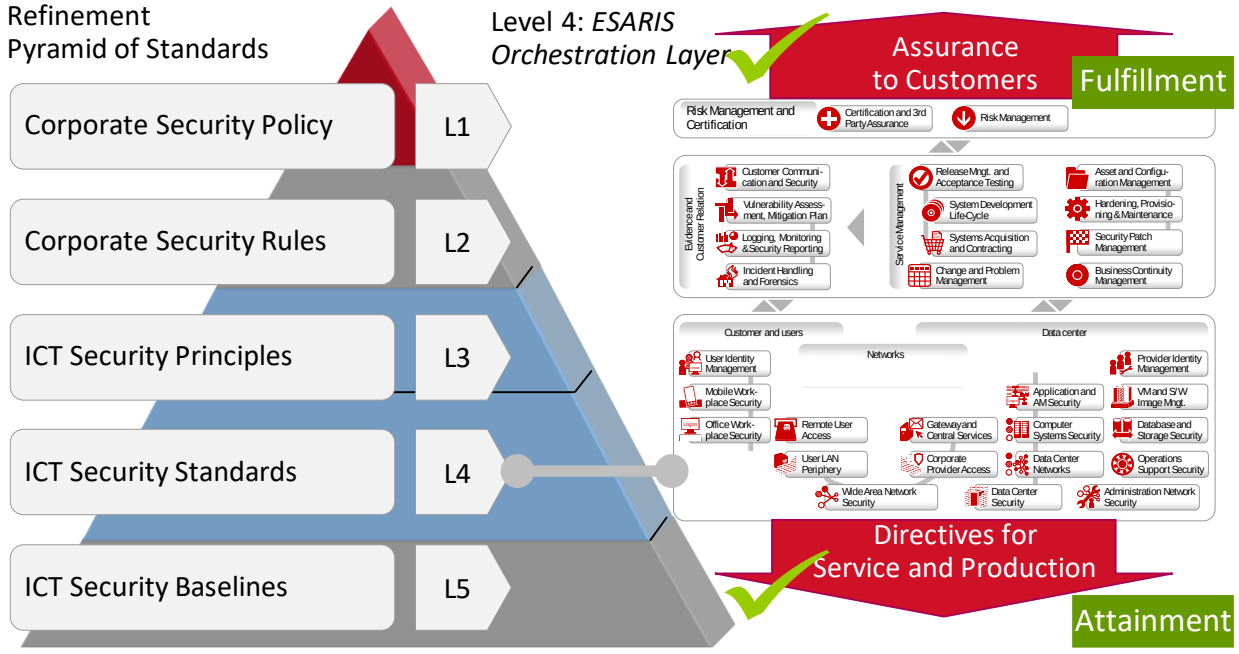


Abb. 1: Einige Architekturelemente von ESARIS

[1] Zum Zeitpunkt der Erstellung dieses Artikels weist die Firma 37.500 Mitarbeiter aus.

Was umfasst ESARIS?

Die *Enterprise Security Architecture for Reliable ICT Services (ESARIS)* ist eine Sammlung von Verfahren, Standards und Arbeitshilfen für die Absicherung von IT-Services. Risiken für den IT-Dienstleister und die Anwenderorganisation (seine Kunden) sollen minimiert werden. *ESARIS* berücksichtigt alle Aspekte, die die Sicherheit der IT-Services beeinflussen. Eine Hierarchie von Sicherheitsstandards verfeinert allgemeine Richtlinien schrittweise bis zu detaillierten, technischen Anweisungen.

ESARIS beschreibt nicht nur, „was" hinsichtlich der IT-Sicherheit getan bzw. erreicht werden muss. *ESARIS* liefert vielmehr konkrete Methoden, „wie" die IT-Sicherheit in der industriellen, markwirtschaftlichen Realität definiert, integriert, aufrechterhalten und weiterentwickelt werden kann. Die Komplexität dieser Realität stellt das entscheidende, zu meisternde Problem dar: Tausende von Maßnahmen der IT-Sicherheit an zehntausende Mitarbeiter kommunizieren, letztere befähigen diese umzusetzen, die Umsetzung überprüfen, zig Einheiten und Partnerunternehmen und Zulieferer und deren Produkte und Services hinsichtlich der IT-Sicherheit orchestrieren bzw. kontrollieren und das Ganze global in vielen Ländern umsetzen. Und nicht zuletzt ist dabei die Größe und Komplexität der „IT" und der industriellen Bereitstellung der IT-Services zu meistern.

ESARIS baut auf den existierenden Prozessen des IT-Services Managements (ITIL bzw. ISO/IEC 20000) und der Unternehmensorganisation auf. Eine großtechnische IT-Produktion ist komplex und durch einen hohen Grad an Arbeitsteilung und durch eine Verteilung von Aktivitäten über die gesamte Organisation hinweg gekennzeichnet. Dies setzt sich im Zuliefernetzwerk fort. *ESARIS* integriert das IT-Sicherheitsmanagement in dieses Umfeld.

Wie profitieren die Anwenderorganisationen/Kunden von ESARIS?

ESARIS hat die Standardisierung, Harmonisierung und Verbesserung der IT-Sicherheit und der dafür verwendeten Maßnahmen zum Ziel. Die Verwendung von standardisierten Elementen ist das entscheidende Mittel, um die Qualität und speziell das Maß an Sicherheit signifikant zu erhöhen. Die Servicequalität wird verbessert. Bereitstellung und Anpassung von IT-Services können beschleunigt werden. Gleichzeitig wird durch die Harmonisierung das Sicherheitsniveau angeglichen. Die Verwendung standardisierter Elemente aus der *ESARIS Library* ist die Grundlage für diese Verbesserungen.

ESARIS erleichtert und verbessert die Zusammenarbeit und die Abstimmung zwischen IT-Dienstleister und Anwenderorganisation erheblich. *ESARIS* unterstützt Kommunikation, Verhandlungen und Vertragsgestaltung. Beispielsweise definieren die sogenannten *ICT Security Standards* (Level 4) alle technischen und prozessoralen Sicherheitsmaßnahmen: Diese Sicherheitsmaßnahmen dienen einerseits als Vorgaben für die Absicherung der IT-Services durch den IT-Dienstleister („Attainment"). Andererseits dienen die gleichen Beschreibungen auch als Grundlage für Kommunikation, Verhandlungen und die Vertragsgestaltung („Fulfillment"). Damit ist sichergestellt, dass die versprochenen Maßnahmen tatsächlich implementiert sind.

ESARIS schafft die Transparenz, die Anwenderorganisationen für ihr Risikomanagement benötigen. Sie müssen wissen, ob ihre Sicherheitsanforderungen erfüllt sind. Dazu legt der IT-Dienstleister die mit *ESARIS* definierten grundlegenden Verfahren, Methoden und Modelle offen und stellt seinen Kunden die Beschreibung der Sicherheitsmaßnahmen zur Verfügung. Die implementierten Sicherheitsmaßnahmen und Informationen über ihre Wirksamkeit sind die Grundlage für das Management der IT-Risiken bzw. für die Bestimmung und Bewertung der IT-Risiken durch den Kunden.

ESARIS modularisiert Methoden und Maßnahmen und unterstützt dadurch deren Nutzung für verschiedene Kunden und Anwendungsbereiche einschließlich unterschiedlicher IT-Services. Trotz hohem Standardisierungsgrad können spezielle Kundenanforderungen erfüllt werden, indem einzelne Sicherheitsmaßnahmen optional implementiert werden. Insgesamt dient das Konzept der Modularisierung der industriellen IT-Produktion. Sie ermöglicht ein effektives Sicherheitsmanagement in einem großtechnischen, komplexen Umfeld mit einer Vielzahl von Kunden und einem reichhaltigen Portfolio an IT-Services. Die Modularisierung zieht sich bis in die strukturierte Dokumentation durch, was die effektive Erstellung, Aktualisierung und Pflege aller Methoden und Maßnahmen erst ermöglicht.

ESARIS integriert IT-*Sicherheits*management und IT-*Service*-Management. Diese Integration in die Standardprozesse des IT-Dienstleisters unterstützt die Arbeitsteilung und sorgt dafür, dass die Informationssicherheit wirklich und in allen Bereichen berücksichtigt wird. Alle Mitarbeiter und Bereiche müssen ihre Verantwortung in Bezug auf die Sicherheit der IT-Services wahrnehmen. Dadurch werden die bereitgestellten IT-Services und damit auch die Kunden noch besser geschützt.

ESARIS strukturiert und ordnet. *ESARIS* bietet einen umfassenden Ansatz und hilft nachweislich dabei, für Sicherheit in einer verzweigten IT-Produktion zu sorgen. *ESARIS* ist ein architektonischer Ansatz, der dabei hilft, die Komplexität zu beherrschen. Dadurch kann die Integration von Sicherheit gelingen und die Absicherung der IT-Services wird machbar – egal um welchen Kunden oder IT-Service es sich handelt.

Die Aufzählung zeigt, dass *ESARIS* nicht einfach ein weiterer IT-Sicherheitsstandard ist, der aufzählt an „was" alles zu denken und „was" alles zu berücksichtigen ist. *ESARIS* kümmert sich um das „wie" und hilft, die Dinge wirklich umzusetzen.

Was sind die Highlights?

ESARIS ist die Antwort auf die neuen Herausforderungen der Informationssicherheit in einer technologisch anspruchsvollen, industriellen IT-Produktion:

- ESARIS ist eine Sammlung aller Werkzeuge für die Absicherung von IT-Services.
- ESARIS standardisiert, harmonisiert und verbessert die Sicherheit.
- ESARIS unterstützt die Schnittstelle zwischen Anbieter (IT-Dienstleister) und Anwenderunternehmen (Kunden).
- ESARIS integriert IT-Sicherheitsmanagement (ISO 27001) und IT-Service-Management (ISO 20000).
- ESARIS schafft Transparenz über die erreichte Sicherheit.
- ESARIS strukturiert und ordnet.
- ESARIS verstehen nicht nur IT-Sicherheitsexperten.

Ein paar Details

Abb. 2 gibt die Struktur des *ESARIS*-Buches (zweite Auflage, siehe Literatur) wieder und einen Überblick über die wichtigsten *ESARIS*-Methoden. Diese sind in drei Teile (Parts) eingeteilt. Bei den Grundlagen (Part 1) sind insbesondere die erwähnte *ESARIS Security Taxonomy* und das Prinzip „Secured by definition" hervorzuheben. Die Taxonomy ist ein modulares Ordnungsschema, dass bei Verständnis, Kommunikation und Zusammenarbeit unterstützt und bezüglich der IT-Sicherheit Grundlage für Arbeitsteilung, Lieferkettenmanagement und Portfolio- und Service-Katalog-Management ist. Jeder Bereich in der *ESARIS Security Taxonomy* betrifft eine genau beschriebene Problemstellung; der zu jedem Bereich gehörende *ICT Security Standard (Level 4)* definiert die notwendigen Sicherheitsmaßnahmen. Die Taxonomy ist, kurz gesagt, ein Werkzeug, das es erlaubt, die Vollständigkeit zu prüfen, Abhängigkeiten zu verstehen und dafür zu sorgen, dass die Summe aller Maßnahmen zu einem integrierten, sicheren Ganzen führt, bei dem die Teile effektiv zusammenwirken.

Das Prinzip „Secured by definition" folgt, das wurde mir erst später klar, Grundsätzen aus dem Qualitätsmanagement und von Managementtheorien ganz allgemein. Dazu gehören Theorien wie das Scientific Management, die prozessorientierte Produktion, das Total Quality Management (TQM) sowie Business Process Reengineering und Kernkompetenzen. In der Essenz geht es um die erwähnte Integration von IT-*Sicherheits*management und dem IT-*Service*-Management.

Der Teil 2 in Abb. 2 zeigt vier Kernaktivitäten. Zunächst werden Methoden entwickelt für die Standardisierung. Sie verfolgt das Ziel hoher Qualität in Verbindung mit Effizienzsteigerungen (bzw. geringerem Aufwand oder Kosten). *ESARIS* nimmt die Herausforderung der Industrialisierung und den Druck im marktwirtschaftlichen Umfeld also ernst! Das *ESARIS Attainment Model* (oder *ESARIS Compliance Attainment Model*) beschäftigt sich mit allem, was mit der Integration oder Umsetzung von IT-Sicherheitsstandards zu tun hat. Am Ende sollen die IT-Services den Standards prüfbar entsprechen, und das Portfolio einschließlich der Service-Kataloge sollen entsprechende Sicherheitsspezifikation enthalten, die Grundlage für Vertrieb, Verhandlungen, Lösungsdesign und Vertragsabschluss sein können.

Beim *ESARIS Fulfillment Model* (oder *ESARIS Customer Fulfillment Model*) geht es darum, die Anforderungen der Anwenderorganisation und den geschlossenen Vertrag zu erfüllen. Das klingt sehr einfach, ist es aber nicht. Zunächst muss dies konzeptionell geprüft und nachgewiesen werden. Erst dann sollte der Vertrag fertiggestellt und die geplante Übernahme der IT-Services (einschließlich z.B. vorhandener Datenbestände) vorbereitet und schrittweise durchgeführt werden (Transition, Transformation). Dazu muss auch das (gemeinsame) Sicherheitsmanagement aufgesetzt werden im Sinne des *Joint Security Management (JSM)*. Dabei sind Prozesse und Verfahren zu implementieren, die im laufenden Betrieb zur Aufrechterhaltung der IT-Sicherheit und zur Behandlung z.B. von Sicherheitsvorfällen notwendig sind. Hier ist sowohl der IT-Dienstleister als auch die Anwenderorganisation gefragt. Im laufenden Betrieb nach Standards müssen betriebliche Nachweise bzgl. der Einhaltung der Vereinbarungen erzeugt, ausgetauscht und verwendet werden. Dies erfolgt insbesondere mit Hilfe von Security-Reports (Sicherheitsberichten), die die Anwender für ihr eigenes Risikomanagement und als Nachweise für Zertifizierungen, für Auditoren und Jahresabschlüsse sowie Kunden und andere Interessengruppen benötigen. Das JSM beschreibt weitere Bereiche notwendiger Zusammenarbeit.

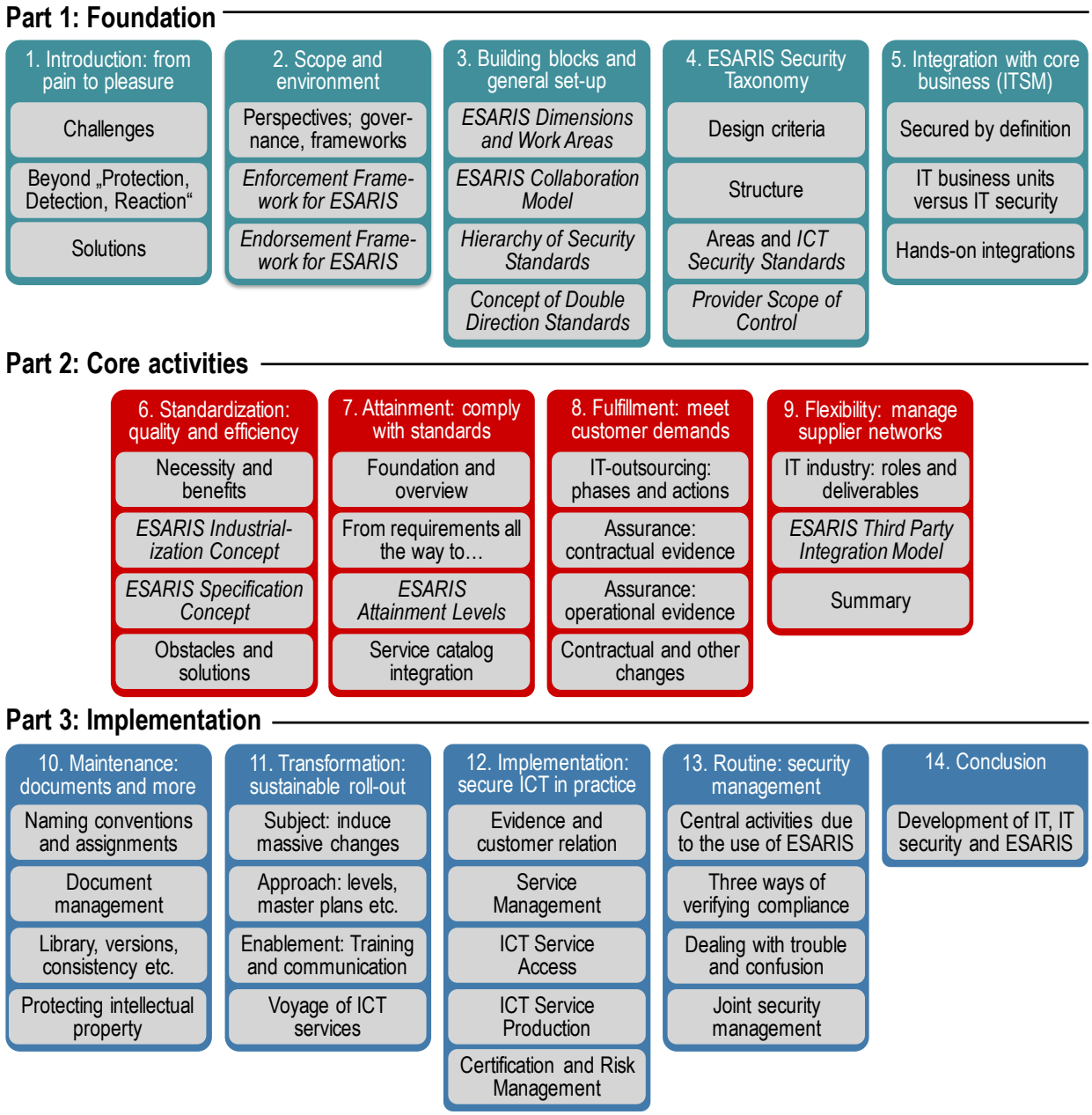


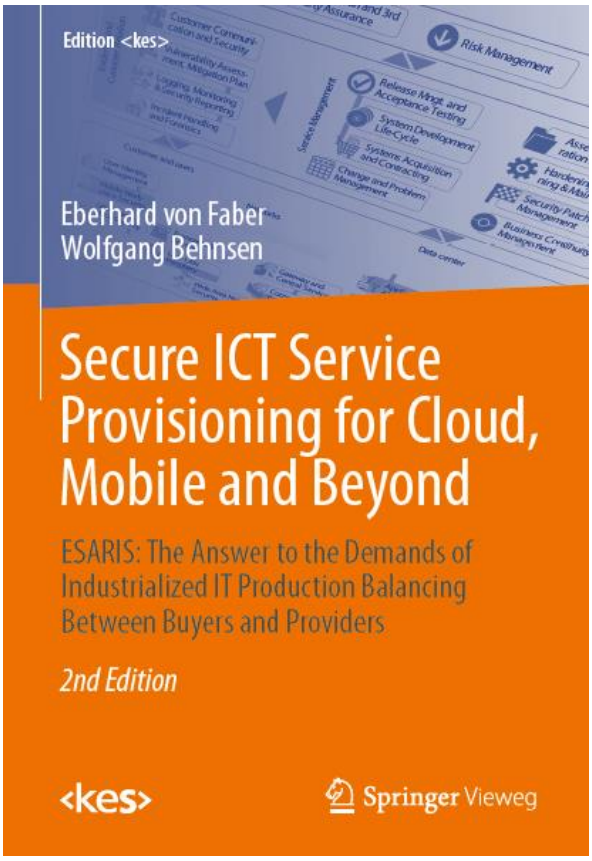
Abb. 2: Struktur des Buches bzw. Übersicht über wichtige ESARIS-Methoden

Das letzte Modell in Teil 2 (siehe Abb. 2) befasst sich mit dem Lieferkettenmanagement. Der IT-Dienstleister (Vertragspartner der Anwenderorganisation) stellt ja nicht alles selbst her, sondern nutzt Komponenten und Services anderer Hersteller und Dienstleister, um die IT-Services für seine Kunden bereitstellen zu können. Auch diese zugekauften Teile haben natürlich einen massiven Einfluss auf die insgesamt erreichte IT-Sicherheit. Deshalb gibt es ein *ESARIS Third Party Integration Model*, dass sich mit dem Einkauf und der sicheren Integration solcher Komponenten und Services Dritter beschäftigt.

Die Bereiche im Teil 3 (siehe Abb. 2) beschäftigen sich mit der Pflege des Systems, der Einführung von *ESARIS*, den zu implementierenden Standards und dem dazu notwendigen Sicherheitsmanagement.

Schlussbemerkung

ESARIS wurde für T-Systems entwickelt und dort systematisch eingeführt. Alle Grundlagen wurden herstellerunabhängig veröffentlicht (siehe Literatur unten). Der Verein *Zero Outage Industry Standard*, dem IT-Firmen wie Brocade, CISCO, EMC Dell, Hitachi Data Systems, IBM, Juniper, Maincubes, Suse, Swisscom, NetApp angehören, hat sich wesentliche Teil von *ESARIS* zu Eigen gemacht und als Standard veröffentlicht (https://www.zero-outage.com/security/). *ESARIS* ist umfassend und wird kontinuierlich weiterentwickelt. Das ESARIS-Buch (siehe Abbildung und Literatur) habe ich im Auftrag meines Arbeitgebers geschrieben; es ist jedoch vollständig hersteller- und firmenneutral abgefasst. Das neue *Joint Security Management (JSM)* funktioniert am besten auf Basis der Sicherheitsarchitektur *ESARIS*. Auch dazu gibt es ein Buch.



Der Umfang von *ESARIS* ist schwer abzuschätzen. Das Buch dazu (siehe Literatur) hat knapp 400 Seiten und ist damit schon weit umfangreicher als die meisten „Standards". *ESARIS* erklärt ja auch das „Wie". Trotzdem enthält das Buch nicht alle Details einer Umsetzung, die ja auch Firmenspezifika berücksichtigen muss. Der Anteil der Beschreibungen von Methoden lässt sich nur schwer von den „technischen" Standards der Ebenen 3 und 4 trennen (L3 und L4, siehe Abbildung). Die „Management"-Standards der Ebene 4 (L4) umfassen allein ca. 900 Seiten. Die „reinen" Beschreibungen der Methoden (übergreifend und Ebene 3) füllen wahrscheinlich etwa 1000 Seiten. Die prozessualen und technischen Standards der Ebene 5 sollten dagegen nicht dem „Managementsystem" *ESARIS* direkt zugerechnet werden, auch wenn sie Teil der „ESARIS"-Bibliothek des IT-Dienstleisters sind und die Vorgaben der Ebenen 3 und 4 verfeinern. *ESARIS* beschreibt ein ausgeklügeltes System, das es möglich macht, dass jeder und jeder Aufgabenbereich genau das findet, was konkret relevant und gebraucht wird.

Die wesentlichen Teile von *ESARIS* habe ich im Auftrag meines Arbeitgebers entwickelt. Er hat mir im Jahr 2010 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. An der Umsetzung und Einführung sind natürlich Unmengen anderer Mitarbeiter beteiligt gewesen. Ohne sie wäre *ESARIS* nie zu einem solchen Erfolg geworden. Nebenberuflich bin ich Professor für IT-Sicherheit und unterrichte seit 2008 im Masterstudiengang Security Management an der Technischen Hochschule Brandenburg.

Literatur

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

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