Edition <kes>

Eberhard von Faber

IT-Service-Security in Begriffen und Zusammenhängen

Managementmethoden und Rezepte für Anwender und IT-Dienstleister

<kes>

MOREMEDIA

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.

Eberhard von Faber

IT-Service-Security in Begriffen und Zusammenhängen

Managementmethoden und Rezepte für Anwender und IT-Dienstleister

Springer Vieweg

Eberhard von Faber
Bornheim, Deutschland

ISSN 2522-0551 ISSN 2522-056X (electronic)
Edition <kes>
ISBN 978-3-658-41932-5 ISBN 978-3-658-41933-2 (eBook)
https://doi.org/10.1007/978-3-658-41933-2

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

Planung/Lektorat: 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

Vorbemerkungen

Für die IT- bzw. Cybersecurity von IT-Dienstleistungen (IT-Services) zu sorgen, kann ein komplexes Unterfangen sein. Das erreichte Maß an IT-Sicherheit adäquat einzuschätzen nicht minder. Je größer die IT-Produktion und je vielfältiger die IT-Services (das Portfolio), desto unübersichtlicher werden diese Aufgaben.

Dieses Buch bringt Ordnung in das Dickicht von Prozessen, Aktivitäten und Informationen, indem neue Begriffe eingeführt und definiert werden sowie existierende geschärft und in den Zusammenhang gesetzt werden.

Die Aufteilung der komplexen Materie in einzelne Begriffe ermöglicht es dem Leser, sich jeweils auf eine Fragestellung konzentrieren zu können.

Zusammenhänge werden durch die Abfolge und Hierarchie der Begriffe offenbar sowie durch Verweise und Zwischentexte. Der Gesamtzusammenhang erschließt sich bereits bei den allgemeineren Begriffen am Anfang. Das Verständnis wird weiter vertieft, je mehr Details nachfolgende Beschreibungen liefern.

Abbildungen bzw. Schaubilder unterstützen die Orientierung.

In diesem Buch geht es allein um das Management der IT-Sicherheit, genauer um das Sicherheitsmanagement von IT-Services! Das Management hat primär die Aufgabe, die notwendigen Voraussetzungen dafür zu schaffen, dass definierte Ziele erreicht werden. Dazu werden zum Beispiel Themen gegliedert, Abläufe spezifiziert und Aufgabenbereiche definiert. Genau dies ist das Ziel und der Inhalt dieses Buches. Das Buch richtet sich an Anwender (Anwenderorganisationen) und an IT-Dienstleister (Firmen und IT-Abteilungen) und ist hilfreich für Hersteller, die beide Parteien zufriedenstellen müssen.

Dieses Buch liefert eine neue und stark verbesserte Version der Sicherheitsarchitektur ESARIS (Enterprise Architecture for Reliable ICT Services).

→ Fragen Sie sich, was so kompliziert an „IT-Service-Security“ ist und warum es ein Buch braucht, um zu erklären, wie man sie „managed“? Auf der nächsten Seite finden Sie ein einfaches Beispiel für vier Arten von Übereinstimmung (Compliance). Alle vier sind wichtig sowohl für den Anwender als auch für den IT-Dienstleister. Allein dies erhöht die Komplexität. Das Beispiel zeigt aber auch wie man sie mit etwas Systematik meistern kann.

→ Fehlt etwas? Sind Sie anderer Meinung? Schreiben Sie mir eine E-Mail an ESARIS@t-online.de!

Alle 30 Abbildungen und eventuell weiteres Zusatzmaterial finden Sie in elektronischer Form über https://link.springer.com/ auf der Seite der eBook-Version.

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

Warum „IT-Service-Security" komplexer ist, als manche denken… Ein Beispiel.

Übereinstimmung (Compliance) ist ein Trend, ein Muss oder einfach nur etwas sehr Grundlegendes. Denn Ziele, Vorgaben, Standards und dergleichen sind sinnlos, wenn man nicht auch prüft, ob sie erreicht bzw. eingehalten werden, man also eine Übereinstimmung feststellen konnte. Und ohne Ziele, Vorgaben, Standards und dergleichen ist alles beliebig und daher nutzlos.

Abb. 1 veranschaulicht, welche Übereinstimmungen zu prüfen und sicherzustellen sind, damit ein IT-Service (rechts oben in Rot) den vertraglichen Zusicherungen (in Gelb links) entspricht. Es gibt vier Arten oder Formationen von Soll-Ist-Paaren, für die die Compliance zu prüfen ist. Dies erwartet der Anwender (Kunde) und der IT-Dienstleister muss sie herstellen und prüfen.

Wir besprechen alle vier Fälle nacheinander in der an dieser Stelle gebotenen Kürze. (Weiter unten im Buch werden die verwendeten Begriffe und Zusammenhänge genauer erläutert.)

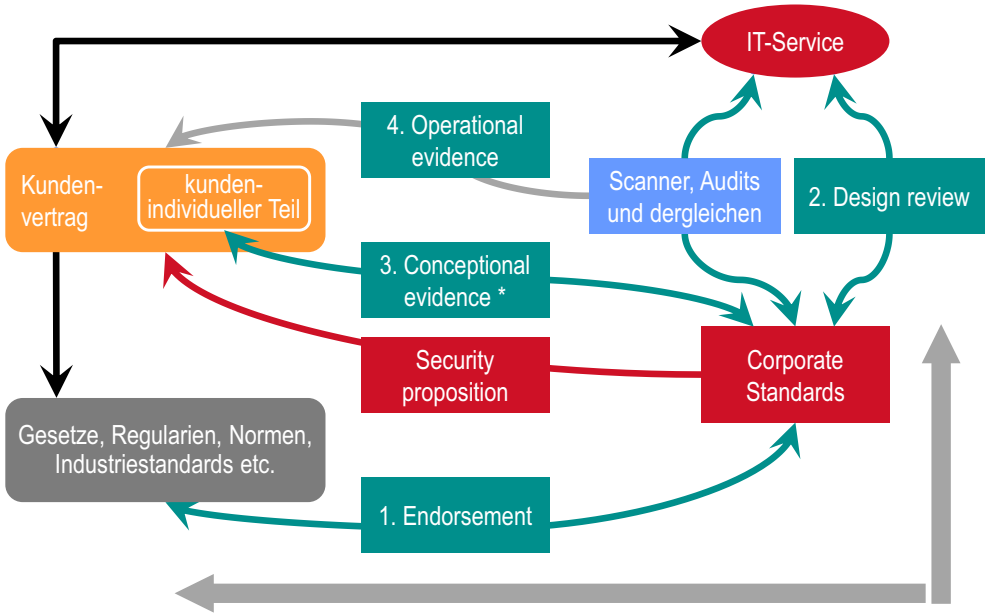

Abb. 1: Vier Arten der Feststellung der Übereinstimmung (Compliance) eines IT-Service

1. Endorsement (siehe Abb. 1): Anwenderorganisationen müssen selbst Gesetze, Regularien, Normen und dergleichen erfüllen und einige dieser Anforderungen können die IT betreffen, die sie nicht selbst herstellen, sondern von einem IT-Dienstleister beziehen. Seinen eigenen Standards folgend (Corporate Standards, siehe

Abb. 1) sorgt der IT-Dienstleister für die Absicherung der IT-Services. Er wird daher im Vorfeld prüfen, ob seine eigenen Standards ausreichen, um die Kundenanforderungen zu erfüllen, die sich aus bestimmten Gesetze, Regularien, Normen und dergleichen für ihn ergeben.

Die Anwenderorganisationen (Kunden) erhalten Informationen zur IT-Sicherheit der IT-Services (siehe Security proposition in Abb. 1), die auf den Standards des IT-Dienstleisters basieren.

2. Design reviews (siehe Abb. 1): Der IT-Dienstleister entwickelt und implementiert seine IT-Services. Seine eigenen Standards sind die Grundlage dafür und bestimmen, wie sie abgesichert werden. Im Rahmen der Qualitätssicherung muss er überprüfen, ob und in wieweit die anzuwendenden Standards bei der Entwicklung und Implementierung wirklich umgesetzt wurden. Dies ist der zweite Compliance-Bereich.

3. Conceptional evidence (siehe Abb. 1): Gerade größere Anwenderorganisationen haben häufig eigene Vorstellungen und Anforderungen an die IT-Service-Security. Dies kann sehr unterschiedliche Gründe haben. Aber IT ist selten völlig identisch und „one size fits it all“ gilt auch in der IT-Sicherheit nicht immer. In diesen Fällen muss geprüft werden, ob die kundenindividuellen Anforderungen erfüllt werden können. Diese dritte Form von Übereinstimmung ist nur relevant im Falle kundenindividueller Verträge bzw. Vertragsklauseln.

4. Operational evidence (siehe Abb. 1): Ist bis hierher alles OK., kann der Vertrag unterzeichnet werden, und der IT-Dienstleister kann den IT-Service bereitstellen. Allerdings wird die IT laufend geändert, die Bedrohungssituation verändert sich gegebenenfalls ebenfalls und die IT-Sicherheitsmaßnahmen müssen laufend daraufhin überprüft werden, ob sie ausreichend wirksam sind. Sowohl der IT-Dienstleister selbst als auch die Anwenderorganisation benötigen und erwarten daher entsprechende Überprüfungen und Berichte über deren Ergebnisse meist in Form von Security Reports. Diese Compliance-Überprüfungen werden meist sehr stark automatisiert.

Die vier Fälle wurden hier nur oberflächlich skizziert. Sie sollen zeigen, dass es diverse Quellen (für Vorgaben) und mehrere Arten der Überprüfung (der Compliance) gibt. Allein dies ist einer der Gründe für mehr Komplexität bei der Absicherung geschäftsmäßig angebotener IT-Services und deren Nutzung.

Das Beispiel soll aber auch verdeutlichen, wie dieses Buch mit Hilfe von Systematik und mit Begrifflichkeiten Ordnung schafft, Zusammenhänge erhellt und konkret dabei unterstützt, IT-Service-Security erfolgreich und mit Augenmaß umzusetzen.

Eberhard von Faber

Inhaltsverzeichnis

Abbildungen und Tabellen

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einführung

1.1 Über dieses Buch

Der Autor arbeitet seit vielen Jahren im Bereich Absicherung von IT-Dienstleistungen (IT-Services) und hat schon viel darüber geschrieben. Das erste Buch über IT-Service-Security zeigt im Nachhinein, dass sich die Gesamtarchitektur und ihre Konzepte im Jahr 2012 noch etwas im Entwicklungs- bzw. Experimentierstadium befanden. Das zweite Buch von 2017 versuchte, das Ganze sehr logisch und planmäßig aufzubauen, worunter manchmal die Lesbarkeit litt. Das dritte Buch von 2018 merzte den Mangel aus, dass sich die beiden ersten fast ausschließlich an IT-Dienstleister richteten, auch wenn dieser zur Kundenorientierung geradezu gedrängt wurde.

Das vorliegende Buch richtet sich sowohl an IT-Dienstleister (einschließlich IT-Abteilungen) als auch an Anwenderorganisationen (einschließlich Geschäftseinheiten), insofern die IT-Dienstleistungen (IT-Services) einen gewissen Umfang und eine größere Komplexität aufweisen. Wir befinden uns im B2B-Bereich (Geschäfte zwischen größeren Firmen, Behörden und dergleichen bzw. bei adäquater Größe zwischen ihren Gliederungen). Das Buch baut auf mehr als einem Jahrzehnt praktischer Erfahrung auf und baut die Sicherheitsarchitektur ESARIS (Enterprise Architecture for Reliable ICT Services) und ihre Konzepte leicht lesbar vom Allgemeinen zum Konkreten auf.

Der Autor hat sich außerdem entschieden, das Konzept seines erfreulich erfolgreichen „thematisch sortierten Lexikons“ (über IT und IT-Sicherheit) von 2021 zu nutzen. Es handelt sich aber um kein Lexikon im herkömmlichen Sinne.

- Der Kern der Informationen zu einem Thema wird anhand von Begriffsdefinitionen gegeben. Diese sind hierarchisch sortiert. Nachfolgende erweitern und verfeinern bereits erläuterte Begriffe und Zusammenhänge.
- 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.
- Die einzelnen Begriffserklärungen sind lexikonartig, also relativ kurz und präzise. Dies kommt Lesern entgegen, die es gewohnt sind, Informationsschnipsel zu verarbeiten, die sie dann schrittweise zusammenfügen.

Ergänzende Information Die elektronische Version dieses Kapitels enthält Zusatzmaterial, auf das über folgenden Link zugegriffen werden kann https://doi.org/10.1007/978-3-658-41933-2_1.

E. von Faber, *IT-Service-Security in Begriffen und Zusammenhängen*,
Edition <kes>, https://doi.org/10.1007/978-3-658-41933-2_1