Klaus-Rainer Müller

IT-Sicherheit mit System

Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement – Sichere Anwendungen – Standards und Practices

6. Auflage

EBOOK INSIDE

Springer Vieweg

IT-Sicherheit mit System

Lizenz zum Wissen.

Sichern Sie sich umfassendes Technikwissen mit Sofortzugriff auf tausende Fachbücher und Fachzeitschriften aus den Bereichen: Automobiltechnik, Maschinenbau, Energie + Umwelt, E-Technik, Informatik + IT und Bauwesen.

Exklusiv für Leser von Springer-Fachbüchern: Testen Sie Springer für Professionals 30 Tage unverbindlich. Nutzen Sie dazu im Bestellverlauf Ihren persönlichen Aktionscode **C0005406** auf *www.springerprofessional.de/buchaktion/*

Jetzt 30 Tage testen!

Springer für Professionals.
Digitale Fachbibliothek. Themen-Scout. Knowledge-Manager.

- Zugriff auf tausende von Fachbüchern und Fachzeitschriften
- Selektion, Komprimierung und Verknüpfung relevanter Themen durch Fachredaktionen
- Tools zur persönlichen Wissensorganisation und Vernetzung

www.entschieden-intelligenter.de

Springer für Professionals

Springer

Klaus-Rainer Müller

IT-Sicherheit mit System

Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement – Sichere Anwendungen – Standards und Practices

6., erweiterte und überarbeitete Auflage

Springer Vieweg

Klaus-Rainer Müller
Groß-Zimmern, Deutschland

Das vorliegende Buch wurde aus fachlicher, nicht aus juristischer Sicht geschrieben und nach bestem Wissen und Gewissen sowie mit größter Sorgfalt erstellt und qualitätsgesichert. Weder Autor noch Verlag können jedoch die Verantwortung oder Haftung für Schäden übernehmen, die im Zusammenhang mit der Verwendung des vorliegenden Werkes und seiner Inhalte entstehen. Das Buch kann eine Beratung nicht ersetzen.
Bei zitierten oder ins Deutsche übersetzten Textpassagen, die aus Originaldokumenten stammen, gelten in Zweifelsfällen die Originaldokumente.
Die in diesem Buch angegebenen Quellen und Webseiten wurden zum Zeitpunkt ihrer Einsichtnahme nach bestem Wissen und Gewissen sowie mit größter Sorgfalt ausgewählt. Eine Haftung, Garantie oder Verantwortung für die in diesem Buch angegebenen Webseiten und Quellen sowie deren Inhalte kann in keinerlei Hinsicht übernommen werden. Für Webseiten, welche aufgrund einer solchen Angabe aufgerufen werden, wird keine Verantwortung übernommen. Dementsprechend distanziert sich der Autor ausdrücklich von ihnen.
Der Umfang dieses Buches ist – im Gegensatz zur behandelten Thematik – begrenzt. Demzufolge erhebt das Werk keinen Anspruch auf Vollständigkeit. Rechte Dritter wurden – soweit bekannt – nicht verletzt.
Für in diesem Werk genannte Markennamen, Warenbezeichnungen, Gebrauchsnamen, Handelsnamen etc. gelten, auch wenn sie falsch oder nicht als solche gekennzeichnet sind, die entsprechenden Schutzbestimmungen und -rechte in ihrer jeweils aktuellen Fassung.

ISBN 978-3-658-22064-8 ISBN 978-3-658-22065-5 (eBook)
https://doi.org/10.1007/978-3-658-22065-5

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

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

Vorwort

Welches Ziel verfolgt dieses Buch?

Sicherheit, Kontinuität und Risiken der Informationsverarbeitung müssen effizient und geschäftszentriert gemanagt werden, um die Existenz und Zukunft eines Unternehmens abzusichern. Die Bedeutung dieser Themen wächst rasant aufgrund des dynamisch steigenden Bedrohungspotenzials und zunehmender gesetzlicher Vorgaben wie dem IT-Sicherheitsgesetz für Betreiber kritischer Infrastrukturen, der EURichtlinie zum Sicherheitsniveau von Netz- und Informationssystemen, der EU-Datenschutz-Grundverordnung und der Neufassung des Bundesdatenschutzgesetzes sowie den buchführungsrelevanten Grundsätzen in Form der GoBD. Hinzu kommen branchenspezifische Gesetze und Regularien: Energieversorger müssen das EnWG beachten. Strom- und Gasnetzbetreiber müssen die Mindeststandards zur IT-Sicherheit erfüllen, die die Bundesnetzagentur im IT-Sicherheitskatalog niedergelegt hat, und sich bis zum 31. Januar 2018 gemäß DIN ISO/IEC 27001 unter Berücksichtigung der DIN ISO/IEC 27002 und DIN ISO/IEC TR 27019 zertifiziert haben lassen. Im Finanzsektor gelten Basel II und Basel III sowie das KWG, die MaRisk für Banken, die bankaufsichtlichen Anforderungen an die IT (BAIT), das KAGB und die KAMaRisk für Kapitalverwaltungsgesellschaften sowie WpHG und MaComp für Wertpapierdienstleistungsunternehmen. Für Zahlungen im Internet hat die BaFin Mindestanforderungen in Form der MaSI aufgestellt. Bei Versicherungsunternehmen ergeben sich Anforderungen aus Solvency II, dem VAG, in das auch Anforderungen aus Solvency II eingeflossen sind, sowie aus den MaGo und künftig aus den versicherungsaufsichtlichen Anforderungen an die IT (VAIT). In der chemischen bzw. pharmazeutischen Industrie sind das ChemG bzw. das AMG und die AMWHV sowie die verschiedenen Guten Praktiken zu beachten. Und auch die Normung entwickelt sich in den Bereichen Sicherheit, Datenschutz, Kontinuität und Risiko dynamisch weiter.

Unternehmen und unser Alltag sind durchdrungen von IT und werden es immer mehr. Begriffe wie digitale Transformation (DT, engl. DX), Digitalisierung, pervasive und ubiquitous computing, Internet of Things (IoT) sowie Industrie 4.0 und das Industrial Internet of Things (IIoT), aber auch Cloud Computing und Apps weisen darauf hin. So sind Geschäfts-, Produktions- und Fertigungsprozesse, Anlagen und Systeme ohne IT kaum mehr denkbar, geschweige denn wettbewerbsfähig. Dies macht Unternehmen jedoch zugleich verwund- und angreifbar. Ausfälle können zu hohen Schäden führen. Ohne entsprechenden Schutz des Unternehmens und seiner IT sowie ohne die erforderliche Sensibilität der Mitarbeiter und Dienstleister können Geschäfts- und Betriebsgeheimnisse oder Angebote Mitbewerbern in die Hände fallen, Produktions- und Fertigungsstraßen von Angreifern

ferngesteuert, beeinträchtigt oder lahmgelegt oder auch Online-Dienste blockiert werden.

Gleichzeitig machen sich Geheimdienste zur Spionage und Militärs für Angriffsszenarien das World Wide Web (WWW) zunutze. Cyberwars sind eine militärische Option und auch Terroristen können das WWW für Angriffe nutzen. Angriffsziele sind z. B. die vielfältigen Kritischen Infrastrukturen (KRITIS). Sie erstrecken sich von Versorgungsunternehmen für Elektrizität, Mineralöl, Gas und Wasser über Telekommunikations- und IT-Provider, Unternehmen aus den Branchen Finanzen, Transport und Verkehr bis hin zum Gesundheitswesen in Form der medizinischen Versorgung. Dass selbst bei gezielten Angriffen Kollateralschäden bewusst in Kauf genommen werden, zeigte der Angriff mit der Schadsoftware Stuxnet auf die Urananreicherungsanlagen im Iran. Dabei wurden hunderttausende andere Industrieanlagen infiziert. Der Studie „Im Dunkeln“ von McAfee aus dem Jahr 2011 zufolge gaben etwa 40 % der Befragten und 46 % der Stromerzeuger an, Stuxnet auf ihren Systemen gefunden zu haben.

Die weltweite Vernetzung zeigt sich auch in Lieferketten (supply chains). Unterbrechungen können schnell zum Stillstand der Produktion oder Fertigung und damit zu finanziellen und Reputationsschäden führen.

Deshalb ist das Sicherheits-, Kontinuitäts- und Risikomanagement – auch der IT – für Unternehmen von existenzieller Bedeutung. Auch die Anforderungen interner und externer Kunden steigen. Gesetzliche und aufsichtsbehördliche Vorgaben sowie Gute Praktiken stellen zudem oftmals direkt oder indirekt Anforderungen an die Sicherheit und Kontinuität der IT. Nationale und internationale Normen und Practices kennzeichnen den Stand der Technik und entwickeln sich zügig weiter wie u. a. die ISO-27000-Familie zur Informationssicherheit zeigt.

Wirtschaftliches, transparentes, durchgängiges und konsistentes Sicherheits-, Kontinuitäts- und Risikomanagement sind gefordert. Dafür sind Investitionen notwendig, deren Umfang von der Effizienz und Effektivität des Sicherheits-, Kontinuitäts- und Risikomanagements abhängt.

Doch trotz der hohen Bedeutung und der Haftungsrisiken weist die Sicherheits-, Kontinuitäts- und Risikosituation in Unternehmen häufig Defizite auf, z. B. hinsichtlich Zielen, Strategie, Struktur, Transparenz sowie anforderungsgerechter Umsetzung und Effizienz. Hinzu kommt eine separate oder gering vernetzte Betrachtung sowohl der Geschäftsprozesse als auch der IT, eine autarke Behandlung des Sicherheitsmanagements, des Kontinuitätsmanagements und des Risikomanagements sowie eine Fokussierung des Sicherheits-, Kontinuitäts- und Risikomanagements auf den IT-Betrieb. Die Integration der Sicherheit in den Lebenszyklus von Prozessen, Ressourcen, Organisation, Produkten und Dienstleistungen erfolgt oftmals nicht oder nur unzureichend. Der Schutz von Fertigungsstraßen und Produktionsanlagen, Prozessleitsystemen, Regelungs- und Steuerungssysteme sowie von Know-how wird oft vernachlässigt.

Vor diesem Hintergrund habe ich die dreidimensionale IT- bzw. Informationssicherheits(management)pyramide *Dr.-Ing. Müller* entwickelt. Sie ist top-down strukturiert und berücksichtigt die Prozesse, die Ressourcen, die Organisation, die Produkte und die Dienstleistungen sowie den Lebenszyklus der Informationsverarbeitungssysteme bzw. der IT bzw. IKT. ***Sie dient als durchgängiges, praxisorientiertes, systematisches und ingenieurmäßiges Vorgehensmodell für den Aufbau und die Weiterentwicklung des Sicherheits-, Kontinuitäts- und Risikomanagements***. In ihren mehrdimensionalen Rahmen können Sie die unterschiedlichsten Sicherheits-, Kontinuitäts- und Risikothematiken „einklinken". So lassen sich Defizite reduzieren oder beseitigen und die Effizienz durch Standardisierung steigern.

Zu den Abgrenzungs- und Alleinstellungsmerkmalen der Sicherheitspyramide gehören

- ihr dreidimensionales Vorgehensmodell, die dazu konsistente Darstellung und Bezeichnung,
- ihr hierarchisch durchgängiger Aufbau, der sich von der Sicherheits-, Kontinuitäts- und Risikopolitik über Anforderungen, die Transformationsschicht, Merkmale, Architektur, Richtlinien und Konzepte bis zu den Maßnahmen erstreckt,
- die Vernetzung des Unternehmens, seiner Management-, Geschäfts-, Support- und Begleitprozesse sowie der IT und anderer Ressourcen bis hin zur Organisation
- die Integration des hierarchischen Aufbaus mit den Themenfeldern Prozesse, Ressourcen, Organisation, Produkte und Dienstleistungen sowie dem Lebenszyklus,
- die integrative Behandlung des Sicherheits-, Kontinuitäts- und Risiko- sowie Compliance- und Datenschutzmanagements,
- der PDCA-orientierte Sicherheitsmanagementprozess,
- die Überwachung und Steuerung anhand des Sicherheitsregelkreises und der Balanced Pyramid Scorecard®.

Die Sicherheitspyramide stellt ein gesamtheitliches, systematisches und dadurch effizientes Vorgehensmodell dar, das sich an der unternehmensspezifisch geforderten Sicherheit ausrichtet. Sie integriert auf innovative Weise neben den Disziplinen Sicherheits-, Kontinuitäts- und Risiko- sowie Compliance- und Datenschutzmanagement Kernelemente und -methodiken, die, wenn auch in unterschiedlicher Ausprägung, Vollständigkeit, Detaillierung, Konkretisierung und Qualität sowie teilweise nach Erscheinen meiner Publikationen in bestehenden Standards und Practices vorkommen.

Die 1995 vorgestellte Sicherheitspyramide [1] lässt sich für die gesamte Palette von Sicherheitsthemen eines Unternehmens nutzen. In diesem Buch beschreibe ich ihre Version V unter dem Fokus der – von mir oftmals synonym verwendeten – Informations- bzw. IT- bzw. ITK-Sicherheit (IT + TK = ITK) bzw. – angelehnt an den englischsprachigen Begriff ICT (Information and Communication Technology)

– IKT-Sicherheit. Dementsprechend bezeichne ich sie als Informations- bzw. IT- bzw. ITK- bzw. IKT-Sicherheits- bzw. -Sicherheitsmanagementpyramide, oder kurz ISiPyr, ITK-/IKT-SiPyr (ISP), ISimPyr oder ISMP. Sie berücksichtigt das Sicherheits-, Kontinuitäts- und Risiko- sowie Compliance- und Datenschutzmanagement.

Das Buch bietet Ihnen durch die Struktur der Sicherheitspyramide das notwendige ***Handlungswissen***, um die IKT, ihre Prozesse, Ressourcen und Organisation entlang dem IKT-Lebenszyklus systematisch, anschaulich, effizient und ganzheitlich sowohl national als auch international auf die geforderte IKT-Sicherheit auszurichten. Neben den Erläuterungen illustrieren Abbildungen die Sachverhalte. Tipps sowie Beispiele, Checklisten, Gliederungen und Tabellen aus der Beratungspraxis beschleunigen den Einstieg. Informationen dienen der Einordnung des Gelesenen in den Arbeits- und Wirtschaftsalltag.

Wer sollte dieses Buch lesen?

Der Titel sagt es bereits – das Buch richtet sich an Leserinnen und Leser, die sich direkt oder indirekt mit der IT-Sicherheit bzw. dem Informationssicherheitsmanagement befassen, aber auch an jene, die für das Kontinuitäts-, das Risiko- oder das Compliance Management zuständig sind:

- ***Chief Information Security Officers (CISO) und IT-Sicherheitsbeauftragte***, die für die Sicherheit der Informations- und Kommunikationstechnologie (IKT) im Unternehmen bzw. von Teilen davon sowie für deren zielgerichteten strategischen Aufbau verantwortlich sind, sollten wissen, wie sich der Schutzbedarf und die Bedrohungslage entwickeln, wie das Informations- bzw. IKT-Sicherheitsmanagement in das Sicherheitsmanagement des Unternehmens integriert sein sollte, welche Zusammenhänge zwischen Sicherheits-, Kontinuitäts-, Risiko- und Compliancemanagement sowie der IKT, den Prozessen, den Ressourcen und der Organisation bestehen und wie sich das IKT-Sicherheitsmanagement ganzheitlich, systematisch, strategisch und praxisorientiert aufbauen und steuern lässt.
- ***Chief Information Officers (CIO) sowie IT-Verantwortliche***, die für die IKT sowie für deren Sicherheit verantwortlich sind, sollten wissen, mit welchem Vorgehensmodell das Sicherheitsmanagement aufgebaut, gesteuert und weiterentwickelt werden kann.
- ***Notfallmanager***, die für die Notfall-, Krisen- und Katastrophenvorsorge (NKK) des Unternehmens insgesamt oder nur für die IKT verantwortlich sind, sollten wissen, wie die NKK-Planung zielgerichtet aufgebaut und weiterentwickelt werden kann.
- ***Sicherheitsauditoren***, welche die IKT-Sicherheit im Unternehmen prüfen und Handlungsempfehlungen geben, sollten wissen, wie diese Prüfungen in das Si-

cherheitsmanagement eingebettet sind, wie sie durchgeführt werden können und wie die Zielkonstellation eines Sicherheitsmanagements aussehen sollte.

- ***Chief Risk Officer (CRO) und Risikomanager***, die für das Risikomanagement im Unternehmen verantwortlich sind, sollten wissen, wie sich dieses anhand der Sicherheits-, der Kontinuitäts- bzw. der Risiko(management)pyramide strukturieren lässt und welche Verbindungsstellen es zwischen dem Risiko- sowie dem Sicherheits- und Kontinuitätsmanagement gibt.
- ***Chief Compliance Officers (CCO)*** sollten die gesetzlichen und aufsichtsbehördlichen Anforderungen kennen, deren Einhaltung einfordern, verfolgen und steuern sowie die Anforderungen an das Sicherheits-, Kontinuitäts- und Risikomanagement kennen.
- ***Leiter Organisation oder Verwaltung sowie Bereichsleiter***, die für Geschäftsprozesse bzw. Organisationseinheiten verantwortlich sind und die Informationsverarbeitung zur Unterstützung ihrer Geschäftsprozesse nutzen, sollten wissen, wie sie ihre Sicherheitsanforderungen – einschließlich derer an die IKT – erheben und an den Geschäftsbereich IKT-Services weitergeben können.
- ***Vorstände und Geschäftsführer***, die für die Sicherheit, die Geschäftskontinuität und das Risikomanagement im Unternehmen verantwortlich sind, sollten die Entwicklung der Bedrohungslage, die gesetzlichen Rahmenbedingungen und ihre persönlichen Haftungsrisiken kennen und wissen, wie das Sicherheitsmanagement durch Sicherheitspolitik, Sicherheitspyramide und Sicherheitsregelkreis zielgerichtet und effizienzorientiert gesteuert werden kann. Auch ***Aufsichtsräte*** sollten ihre Haftungsrisiken kennen.

Wie können Sie dieses Buch nutzen?

Sie können das Buch komplett oder auch nur einzelne Kapitel lesen. Wer es insgesamt liest, kann sich einen Überblick über Trends bei Bedrohungen und Schutzbedarf sowie häufige Schwachstellen verschaffen. Gleichzeitig findet er eine systematische, durchgängige und ganzheitliche Vorgehensweise zum Aufbau eines geschäftszentrierten Sicherheits-, Kontinuitäts- und Risiko- sowie Compliance- und Datenschutzmanagements für die IKT anhand der dreidimensionalen Sicherheitspyramide$^{\text{Dr.-Ing. Müller}}$, ferner weitere von mir entwickelte Begrifflichkeiten und Methoden sowie Beispiele und Checklisten.

Alternativ können sich die Leserin oder der Leser ihrem Wissensbedarf entsprechend einzelnen Kapiteln zuwenden, beispielsweise dem Thema Sicherheits-, Kontinuitäts- und Risikopolitik, sicherheitsbezogene Anforderungen und Schutzbedarfsanalyse sowie Geschäftseinflussanalyse (Business Impact Analysis), Sicherheitsmerkmale, Sicherheitsarchitektur mit prinzipiellen Bedrohungen und Sicherheitsprinzipien sowie dem Sicherheitsschalenmodell und Sicherheitselementen für Prozesse, Ressourcen und Organisation, Richtlinien, Konzepte und Lebenszyklus,