Heinrich Kersten | Gerhard Klett

Der IT Security Manager

Edition <kes>

herausgegeben von Peter Hohl

Mit der allgegenwärtigen Computertechnik 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.

Herausgeber der Reihe ist Peter Hohl. Er ist darüber hinaus Herausgeber der <kes>– Die Zeitschrift für Informations-Sicherheit (s.a. www.kes.info), die seit 1985 im Secu-Media Verlag erscheint. Die <kes> 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.

IT-Sicherheit – Make or Buy
Von Marco Kleiner, Lucas Müller und Mario Köhler

Mehr IT-Sicherheit durch Pen-Tests
Von Enno Rey, Michael Thumann und Dominick Baier

ITIL Security Management realisieren
Von Jochen Brunnstein

IT-Sicherheit kompakt und verständlich
Von Bernhard C. Witt

IT-Risiko-Management mit System
Von Hans-Peter Königs

Praxis des IT-Rechts
Von Horst Speichert

IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz
Von Heinrich Kersten, Jürgen Reuter und Klaus-Werner Schröder

Datenschutz kompakt und verständlich
Von Bernhard C. Witt

Profikurs Sicherheit von Web-Servern
Von Volker Hockmann und Heinz-Dieter Knöll

Heinrich Kersten | Gerhard Klett

Der IT Security Manager

Expertenwissen für jeden IT Security Manager –
Von namhaften Autoren praxisnah vermittelt

2., aktualisierte und erweiterte Auflage

Mit 21 Abbildungen

herausgegeben von Heinrich Kersten und
Klaus-Dieter Wolfenstetter

PRAXIS

VIEWEG+
TEUBNER

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

Das in diesem Werk enthaltene Programm-Material ist mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Der Autor übernimmt infolgedessen keine Verantwortung und wird keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieses Programm-Materials oder Teilen davon entsteht.

Höchste inhaltliche und technische Qualität unserer Produkte ist unser Ziel. Bei der Produktion und Auslieferung unserer Bücher wollen wir die Umwelt schonen: Dieses Buch ist auf säurefreiem und chlorfrei gebleichtem Papier gedruckt. Die Einschweißfolie besteht aus Polyäthylen und damit aus organischen Grundstoffen, die weder bei der Herstellung noch bei der Verbrennung Schadstoffe freisetzen.

1. Auflage 2005
2., aktualisierte und erweiterte Auflage 2008

Alle Rechte vorbehalten
© Vieweg+Teubner Verlag | GWV Fachverlage GmbH, Wiesbaden 2008

Lektorat: Sybille Thelen | Andrea Broßler

Der Vieweg+Teubner Verlag ist ein Unternehmen von Springer Science+Business Media.
www.viewegteubner.de

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Umschlaggestaltung: KünkelLopka Medienentwicklung, Heidelberg
Druck und buchbinderische Verarbeitung: MercedesDruck, Berlin
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.
Printed in Germany

ISBN 978-3-8348-0429-7

Vorwort

Vorwort zur 2. Auflage

Nachdem die Erstauflage des Buches im Herbst 2007 vergriffen war, stellte sich die Frage nach einem unveränderten Nachdruck oder der Herausgabe einer überarbeiteten Fassung.

Verlag und Autoren haben sich für Letzteres entschieden: Eine Überarbeitung und Ergänzung erschien unter anderem deshalb sinnvoll, weil mit dem Erscheinen der ISO 27001 – auch in deutscher Sprache – viele Unternehmen eine neue Herausforderung sehen, andererseits einige wichtige technische Themen wie Internet-Sicherheit, Risikoanalyse und IT Compliance bei der Erstauflage nur beschränkt berücksichtigt wurden.

Zwischenzeitlich eingegangene Kritiken und Vorschläge der Leser sind ebenfalls in die Überarbeitung eingeflossen: hierfür herzlichen Dank.

Dem Verlag, seinem Programmleiter Herrn Günter Schulz und dem Lektorat danken die Autoren für die Unterstützung bei der zweiten Auflage dieses Buches.

Im Februar 2008, Dr. Gerhard Klett, Dr. Heinrich Kersten

Vorwort zur 1. Auflage

Das vorliegende Buch richtet sich an Leser, die sich in das interessante Gebiet der Informationssicherheit einarbeiten möchten.

Dieses Gebiet ist z. T. unter anderen Überschriften wie IT-Sicherheit (IT Security), Datensicherheit, Informationsschutz bekannt und berührt auch Themen wie den Datenschutz, das Qualitätsmanagement, die Ordnungsmäßigkeit der Datenverarbeitung.

Sicherheit der Information und Sicherheit bei der Verarbeitung von Daten sind heute keine Ziele mehr, für die man Werbung betreiben müsste. Jeder hat mehr oder weniger eigene Erfahrungen mit diesen Themen gemacht – sei es als Geschädigter oder als Verantwortlicher. Deshalb wollen wir uns hier ersparen, Horror-Szenarien zu beschreiben – man kennt sie hinlänglich aus entsprechenden Publikationen.

Im Vordergrund stehen heute mehr die Fragen,

– wie man die gewünschte Sicherheit erreichen kann,

– wie man gegenüber Partnern, Kunden, Aufsichtsbehörden und Banken die eigene Sicherheit nachweisen kann,

– ob es einen *Return on Security Investment* (ROSI) gibt und wie man ihn ggf. erreicht.

Im Grunde muss sich heute jede Institution, die schützenswerte Informationen besitzt und Daten sicher verarbeiten will, mit diesem Thema beschäftigen: Es ist zu einem wichtigen Faktor der Unternehmensvorsorge geworden. Dabei hat sich die Erkenntnis durchgesetzt, dass sich Sicherheit nicht allein aufgrund technischer Vorkehrungen einstellt, sondern dass man Sicherheit „managen" muss, woraus sich beinahe zwangsläufig ergibt, dass „Sicherheit" kein Zustand ist, sondern eine kontinuierliche Aufgabe darstellt.

Dies hat dazu geführt, dass in vielen Institutionen ein Sicherheitsmanagement eingerichtet worden ist, das sich in Gestalt eines *IT-Sicherheitsbeauftragten* oder eines entsprechenden Gremiums der Sicherheitsthematik annehmen soll – aber wie?

Das Thema der Informationssicherheit ist ein sehr komplexes – sowohl vom Umfang als auch vom methodischen Zugang her. Wichtige Aspekte betreffen die rechtliche Sicherheit, Fragen der organisatorischen und personellen Sicherheit, die Infrastruktursicherheit, die Sicherheit der IT-Systeme und Netze, die Sicherheit von Geschäftsprozessen.

Es existieren unzählige Vorschläge, sogar umfangreiche Kataloge für Sicherheitsmaßnahmen: Die Bewertung solcher Maßnahmen im Hinblick auf die Eignung und Sicherheit in einem speziellen Einsatzszenario stellt eine nicht zu unterschätzende Herausforderung dar.

Sicherheitskonzept

Eine wichtige Funktion kommt dabei dem so genannten *Sicherheitskonzept* zu, das alle Analysen und Entscheidungen, die die IT-Sicherheit betreffen, enthalten soll. Um dieses meist umfangreiche Dokument rankt sich in der Praxis ein ganzes Bündel von begleitenden Dokumenten – sehr zum Leidwesen der Beteiligten, da „Paperware" einerseits meist Schwerstarbeit ist und andererseits allein noch gar nichts bringt.

Von der methodischen Seite ist das Schreiben von aussagekräftigen Sicherheitskonzepten in diesem Gebiet ein Kardinalproblem: Individuelle Risiken, die Wirksamkeit von Gegenmaßnahmen und das verbleibende Restrisiko können meist nicht berechnet, sondern bestenfalls aus der Erfahrung „geschätzt" werden.

Wer in dieses Gebiet neu einsteigt, kann schnell den Überblick verlieren und wird auch nach vielen Jahren Berufserfahrung immer wieder Neues entdecken. Dennoch gilt es gerade zu Beginn, sich auf das Wesentliche zu konzentrieren.

Sicherheitsmaßnahmen gibt es in großer Zahl und unterschiedlicher Ausprägung. Ihre detaillierte Behandlung würde den Rahmen dieses Buches sprengen. Es musste deshalb eine Auswahl getroffen werden: Als Orientierung dienten mehrtägige Einführungsseminare in die Aufgaben des IT Security Managers, die die Autoren in den vergangen Jahren zahlreich durchgeführt haben (und noch durchführen). Das Feedback der Teilnehmer hat dabei vielfältige Anregungen zur Überarbeitung von Methodik und Didaktik gegeben.

Zielgruppe

Das vorliegende Buch ist speziell auf die Belange von Einsteigern zugeschnitten; es kann aber auch dem erfahrenen Praktiker einige neue Aspekte und Sichtweisen näher bringen – wenn er auch zwangsläufig manche Themen vermissen wird.

An vielen Stellen in diesem Buch ist von „Unternehmen“ die Rede; alle Ausführungen gelten selbstverständlich auch für andere Formen von Institutionen wie Behörden, Verbände, Vereine, usw.

An einigen Stellen in diesem Buch geben wir bei neuen Begriffen die einschlägige englische Übersetzung an, um das Lesen von weiterführender Literatur in englischer Sprache zu erleichtern.

Danksagung

Für viele anregende Diskussionen möchten die Autoren vor allem Herrn Christoph Fischer (BFK edv-consulting GmbH), Herrn Manfred Hübner (WestLB AG), Herrn Dr. Gerald Spiegel (SerCon GmbH) und Herrn Klaus-Dieter Wolfenstetter (Deutsche Telekom AG, Laboratories) danken.

Dem Vieweg-Verlag und seinem Programmleiter Herrn Dr. Reinald Klockenbusch möchten die Autoren für die professionelle Unterstützung bei der Herstellung dieses Buches und vor allem für die große Geduld danken, da eigentlich alles viel schneller gehen sollte…

Im August 2005, Dr. Gerhard Klett, Dr. Heinrich Kersten

Inhaltsverzeichnis

1 Zur Motivation 1

2 Sicherheitsmanagement – Konzeptionelles 5
2.1 Sicherheit als Management-Prozess 5
2.2 Das PDCA-Modell 6
2.3 Unverzichtbar: Sensibilisierung, Schulung, Training 15
2.4 Management der Dokumentation 19

3 Grundstrukturen der IT-Sicherheit 23
3.1 Organisation und Personal 24
3.2 Information und Daten 29
3.3 Datenträger und Datenverarbeitung 31
3.4 IT-Systeme und Einsatzumgebung 32
3.5 Infrastruktur 34
3.6 Software-Anwendungen 36
3.7 IT-Verbund 38
3.8 Geschäftsprozesse 39

4 Sicherheitsziele auf allen Ebenen 43
4.1 Informationen und Daten 43
4.2 IT-Systeme und IV-Systeme 53
4.3 Geschäftsprozesse 56

5 Analysen 59
5.1 Betrachtungsmodell der ISO 27001 59
5.2 Analyse nach IT-Grundschutz 61
5.3 Risikoanalyse nach ISO 13335-3 67
5.4 Ein Ansatz auf der Basis der ISO 15408 79
5.5 Ergänzendes zur Schwachstellenanalyse 89
5.6 Umgang mit dem Restrisiko 92

6 Die Sicherheitsleitlinie ... 93
6.1 Inhalte der Sicherheitsleitlinie ... 93
6.2 Management der Sicherheitsleitlinie ... 96

7 Grundsätzliches zu Sicherheitsmaßnahmen ... 99
7.1 Maßnahmenklassen ... 99
7.2 Validierung von Maßnahmen ... 101

8 Das Sicherheitskonzept ... 105
8.1 Grundsätzliches ... 105
8.2 Gliederung des Sicherheitskonzeptes ... 107
8.3 Vorspann ... 108
8.4 Gegenstand des Sicherheitskonzeptes ... 108
8.5 Ergebnis der Anforderungsanalyse ... 109
8.6 Objekteigenschaften ... 110
8.7 Subjekteigenschaften ... 113
8.8 Bedrohungsanalyse ... 113
8.9 Maßnahmenauswahl ... 116
8.10 Schwachstellenanalyse ... 118
8.11 Validierung der Maßnahmen ... 119
8.12 Restrisiko und seine Behandlung ... 120
8.13 „Sicherheitskonzept“ nach ISO 27001 ... 120

9 Rechtliche Sicherheit ... 125
9.1 Befolgen von Gesetzen ... 126
9.2 Vermeidung von Strafprozessen ... 129
9.3 Outsourcing ... 130
9.4 Verschiedenes ... 132

10 Personelle Sicherheit ... 135
10.1 Arbeitsverträge ... 135
10.2 Vertrauliche Personaldaten ... 139
10.3 Verantwortung der Mitarbeiter für die Informationssicherheit ... 141

10.4 Personalmanagement ... 144
10.5 Ausscheiden von Mitarbeitern ... 144

11 Technische Sicherheitsmaßnahmen ... 147
11.1 Wahrung der Vertraulichkeit ... 147
11.2 Identifizierung und Authentisierung ... 147
11.3 Zugriffskontrolle ... 152
11.4 Wiederaufbereitung ... 156
11.5 Verschlüsselung ... 157
11.6 Wahrung der Integrität ... 167
11.7 Elektronische Signatur ... 170
11.8 Verfügbarkeit von Daten ... 179
11.9 System-Verfügbarkeit ... 182
11.10 Übertragungssicherung ... 188
11.11 Beweissicherung und Auswertung ... 189

12 Sicherheit im Internet ... 193
12.1 Gefährdungen ... 194
12.2 Schutzmaßnahmen: Regelwerke für Internet und E-Mail ... 196
12.3 Technische Schutzmaßnahmen: Internet-Firewalls ... 197
12.4 Zusammenfassung ... 200

13 Infrastruktursicherheit ... 203
13.1 Geltungsbereiche und Schutzziele ... 203
13.2 Gebäude, Fenster, Türen ... 204
13.3 Verkabelung ... 205
13.4 Drahtlose Netzwerke ... 206
13.5 Weitere Infrastrukturprobleme und -maßnahmen ... 210
13.6 Richtlinien zur Zutrittskontrolle ... 213
13.7 Verfahren der Zutrittskontrolle ... 214

14 Sicherheitsmanagement – die tägliche Praxis ... 219
14.1 Aufrechterhaltung der Sicherheit ... 219
14.2 Management von Sicherheitsvorfällen ... 220
14.3 Berichtswesen ... 223

15 IT Compliance ... 225
15.1 Unternehmensstrategie ... 225
15.2 Compliance als essentieller Bestandteil der IT-Strategie ... 226
15.3 Compliance und Risikomanagement ... 228

16 Zum Schluss... ... 231

Abbildungsverzeichnis ... 235
Tabellenverzeichnis ... 236
Verwendete Abkürzungen ... 237
Quellenhinweise ... 243
Sachwortverzeichnis ... 245

1 Zur Motivation

Insgesamt ist es eine nicht zu unterschätzende Herausforderung, gute IT-Sicherheitskonzepte zu schreiben und die IT-Sicherheit qualifiziert zu managen. Man kann sich diese Aufgabe aber auch unnötig schwer machen: Betrachten wir einige Erfahrungen aus der Praxis von Sicherheitsberatern:

- Unklare Verantwortlichkeiten bezüglich der IT-Sicherheit sowie eine schwammige Abgrenzung zu anderen Aufgaben im Unternehmen erschweren ein zielführendes Sicherheitsmanagement, machen es teilweise sogar unmöglich.
- Operiert man mit unklaren Begriffen, so versteht jeder Beteiligte etwas anderes, es gibt langwierige, ineffektive Diskussionen unter den Betroffenen, die Analysen werden unterschiedlich interpretiert, das Ergebnis ist in alle Richtungen auslegbar und damit nichtssagend.
- Verwendet man für den Sicherheitsprozess Vorgehensmodelle, die hoch-wissenschaftlich angelegt oder im Gegenteil zu banal gestrickt sind, ist das Ergebnis praxisfern, nutzlos und bestenfalls für die „Schublade“ geeignet.
- Das leidige Thema „Dokumentation“: Man kann bei der Vielzahl von Dokumenten, Listen und Informationen in der Praxis leicht den Überblick verlieren, wenn man hier ohne eine gute Struktur und Planung einsteigt.
- Macht das Sicherheitsmanagement nur Vorgaben, ohne die Einhaltung derselben zu kontrollieren, hat man eine klassische Management-Aufgabe nicht erfüllt und damit grob fahrlässig gehandelt.

Es kann deshalb nur dringend empfohlen werden,

- eine klare Aufgabenbeschreibung für das IT-Sicherheitsmanagement zu erstellen und die Schnittstellen zu anderen Verantwortlichkeiten festzulegen,
- ein einheitliches Begriffsverständnis zwischen den Beteiligten herzustellen und dieses schriftlich festzuhalten, etwa in Form eines Glossars, das allen weiteren Dokumenten vorangestellt wird,

– erprobte, möglichst standardisierte Vorgehensmodelle heranzuziehen und nutzbringend anzuwenden,

– im Sicherheitsprozess regelmäßige Überprüfungen der Vorgaben und ihrer Einhaltung vorzusehen.

Eine wichtige Entscheidung gleich zu Beginn betrifft die Frage, ob man mit der Sicherheitsdiskussion im Unternehmen auf der Ebene von

– IT-Systemen und Netzen,

– IT-Anwendungen oder gar

– „ganz oben" bei den Geschäftsprozessen

einsteigen möchte. Grundsätzlich sind die IT und die Unternehmensnetze „Werkzeuge", die die Geschäftstätigkeit des Unternehmens unterstützen – das eigentliche Problem ist damit die Sicherheit der Geschäftsprozesse. Bei deren Diskussion kommt man natürlich automatisch auch zur klassischen IT-Sicherheit von Daten, Systemen, Netzwerken und Anwendungen, aber dies allein ist nicht ausreichend: Ein „ganzheitlicher" Ansatz betrachtet auch die Anteile an Geschäftsprozessen, die ohne IT erledigt werden und je nach Lage einen signifikanten Beitrag zur Sicherheit und zur Unsicherheit liefern können.

Inzwischen gibt es einige Jahrzehnte an Erfahrung auf dem Gebiet der IT-Sicherheit und der Informationssicherheit, so dass es nicht verwundert, wenn Sicherheitsmanagement und Sicherheitsmaßnahmen Gegenstand von Standards und vergleichbaren Vorgaben geworden sind.

Bei den Sicherheitsverantwortlichen in den Unternehmen findet man zwei unterschiedliche Gruppen vor: Während die eine im Schwerpunkt sehr Maßnahmen-orientiert denkt, sieht die andere mehr den Sicherheitsprozess und sein Management im Vordergrund.

Dies ist eigentlich gar kein Gegensatz – die „Wahrheit" ist: Man braucht beides. Ein Prozess lässt sich natürlich international viel leichter standardisieren als etwa ein Maßnahmenkatalog, dessen Inhalt schnell „veraltet" ist und der bei der Vielzahl von Anwendungen der IT immer nur Ausschnitte abdecken kann.

ISO 27001

Es verwundert deshalb nicht, dass ausgehend von dem British Standard (BS) 7799 der internationale Standard ISO 27001 entstanden ist, der die IT-Sicherheit im Kern als einen Management-Prozess sieht. Für alle zu behandelnden Sicherheitsthemen werden zwar (im Anhang des Standards) Maßnahmenziele und An-

forderungen angegeben – die Auswahl von geeigneten Einzelmaßnahmen bleibt jedoch dem Anwender überlassen.

Ein Vergleich zeigt, dass eine Reihe von Management-Elementen nicht nur im ISO 27001, sondern auch in anderen Management-Standards wie dem Qualitätsmanagement (ISO 900x) und dem Umweltschutz-Management (EN 1400x) auftreten. Dieser gemeinsame Querschnitt aller bekannten Management-Standards beinhaltet das so genannte PDCA-Modell. Andere Verfahrenselemente wie z. B. das Änderungsmanagement (Change Management) und die Dokumentenlenkung sind typische QM-Verfahren und werden für die Sicherheit analog angewendet. Hieraus ergibt sich auch die Möglichkeit, gemeinsame Management-Strukturen für diese Themen im Unternehmen aufzubauen und somit einen ersten Beitrag zum Return on Security Investment zu liefern.

Grundschutzhandbuch

Parallel dazu hatte sich mit dem vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebenen Grundschutzhandbuch in Deutschland ein Quasi-Standard entwickelt, dessen Kern letztlich die Maßnahmen-orientierte Sichtweise ist. Dieses umfangreiche und regelmäßig aktualisierte Werk stellt im Grunde einen kommentierten Maßnahmenkatalog dar, dessen Anwendbarkeit nach Aussage des BSI auf den „normalen“ Schutzbedarf beschränkt ist.

Nachdem lange Zeit – vor allem in Deutschland – eine Kontroverse zwischen beiden Sichtweisen der IT-Sicherheit bestand, hat man inzwischen eine Kehrtwendung vollzogen: Die Management-Elemente der IT-Sicherheit sind aus dem IT-Grundschutzhandbuch herausgelöst und in Form von BSI-Standards veröffentlicht worden. Dabei wurde auf Konformität zu den entsprechenden Elementen der ISO 27001 geachtet.

Gefährdungs- und Maßnahmenkataloge sind nunmehr eigenständig; letztere sind insbesondere dazu geeignet, eine Reihe von Vorgaben aus dem Anhang A des Standards mit Einzelmaßnahmen zu versehen (nur für den „normalen“ Schutzbedarf“).

Als weiterer BSI-Standard ist eine Vorgehensweise für eine „Risikoanalyse“ veröffentlicht worden, die für die Schutzbedarfe „hoch“ und „sehr hoch“ anwendbar ist und auf der Grundschutzmethode aufbaut.

Wir wollen die genannten Werke hier nicht in anderer Formulierung wiedergeben, sondern eher eine generische Sichtweise der IT-Sicherheit und ihres Managements bringen, die von Einsteigern wie auch erfahrenen IT-Sicherheitsbeauftragten leicht in

die Praxis umgesetzt werden kann. Will man ggf. später die Konformität zum Standard ISO 27001 (mit oder ohne Grundschutz) oder zu anderen Standards herstellen, wird dies mit geringem Zusatzaufwand erreichbar sein. In diesem Zusammenhang sei auf /KRS2008/ verwiesen.

2 Sicherheitsmanagement – Konzeptionelles

2.1 Sicherheit als Management-Prozess

Einige wichtige Erfahrungen wollen wir diesem Kapitel voranstellen:

– Eine absolute Sicherheit[1] gibt es in der Realität nicht.

Man ist von diesem Idealzustand immer ein gutes Stück entfernt. Das sollte auch so bleiben, weil andernfalls die Kosten für die Sicherheit nicht mehr tragbar wären. Wir sprechen deshalb von einem gewünschten bzw. erreichten Sicherheitsniveau, d. h. Sicherheit ist eine Frage von „mehr“ oder „weniger“.

– Ein erreichtes Sicherheitsniveau bleibt nicht auf Dauer bestehen.

Dies hat seinen Grund darin, dass immer wieder bisher nicht bekannte Sicherheitslücken bzw. Schwachstellen in der Technik entdeckt werden und neue Angriffstechniken entstehen – aber auch neue Sicherheitsvorkehrungen entwickelt werden. Sicherheit ist also zeitabhängig: Was heute als sicher gilt, kann unter Umständen in Kürze als unsicher angesehen werden.

– Ein erreichtes Sicherheitsniveau gilt nur für ein genau abgegrenztes Szenario.

Anwendungsbereich

Wenn man Sicherheit konzipiert, geht man so vor, dass zunächst der Gegenstand festgelegt wird, auf den sich das Konzept beziehen soll, d. h. die zu betrachtenden Systeme, Netze, Geschäftsprozesse werden angegeben.

Vor allem in Standards verwendet man anstelle von „Szenario“ auch gerne den Begriff „Anwendungsbereich“ oder das englische Wort „Scope“.

Änderungen des Anwendungsbereiches sind in der Praxis an der Tagesordnung: Häufige Änderungen an den Geschäftsprozessen eines Unternehmens, seiner IT und den betriebenen Anwendun-

---

1 In diesem Abschnitt verwenden wir „Sicherheit“ stellvertretend für IT-Sicherheit, Informationssicherheit, etc. Eine genauere Festlegung solcher Begriffe erfolgt in einem späteren Kapitel.

gen machen es aber den Sicherheitsverantwortlichen nicht leicht: Ändert man den Anwendungsbereich – und sei es nur marginal – kann dies jede denkbare Auswirkung auf die Sicherheit haben: Sie kann sich erhöhen, gleich bleiben, aber auch verringern.

– Sicherheit und Sicherheitsmanagement funktionieren nur in einem sensibilisierten Umfeld.

Das beste Sicherheitskonzept und die teuersten Maßnahmen kommen nicht richtig zum Zug, wenn es bei den Mitarbeitern und der Leitungsebene an Problembewusstsein und Problemwissen („Awareness") fehlt.

Prozess

Aus den zuvor dargestellten Überlegungen erkennt man, dass Sicherheit im wahrsten Sinne eine „Variable" ist und ein permanentes Bemühen erfordert. Sicherheit ist also kein erreichbarer Zustand, sondern ein Prozess. Ziel des Prozesses ist es, ein gewünschtes Sicherheitsniveau erstmalig zu erreichen, dieses aufrechtzuerhalten und die Sicherheit insgesamt weiterzuentwickeln bzw. zu verbessern.

Damit haben wir auch die Aufgabe des Sicherheitsmanagements umrissen.

Verbesserungspotenzial

Das Verbessern der Sicherheit *kann*

– die Veränderung des Anwendungsbereichs betreffen: Man „sichert" beispielsweise zunächst nur bestimmte Organisationseinheiten des Unternehmens und nimmt dann sukzessive weitere hinzu, bis man die gewünschte „Ausbaustufe" erreicht hat,

– eine Anpassung des Sicherheitsniveaus an eine reale Gefährdungslage zum Ziel haben: Man beginnt mit einem bestimmten Sicherheitsniveau und passt dieses von Zeit zu Zeit an die aktuelle Gefährdungslage an; dabei kann es um ein Erhöhen oder Verringern des Sicherheitsniveaus gehen,

– die Erhöhung der Sensibilität für die Sicherheit im Unternehmen zum Ziel haben,

– den Prozess des Sicherheitsmanagements als solches betreffen.

2.2 Das PDCA-Modell

Wir brauchen nun eine Art „Vorgehensmodell", um das Verbesserungspotenzial sukzessive ausschöpfen zu können. Genau dies leistet das so genannte *PDCA-Modell*. Die Buchstaben stehen für

die englischen Wörter **P**lan, **D**o, **C**heck, **A**ct. Dahinter verbirgt sich ein Management-Modell, mit dem man

- die Erreichung von Zielen – hier das gewünschte Sicherheitsniveau – zunächst plant bzw. konzipiert (*plan*),
- die Planung bzw. Konzeption realisiert (*do*),
- über eine gewisse Zeit Erfahrungen mit der Realisierung macht, d. h. überprüft, ob die Konzepte sich in der Praxis bewähren bzw. wo es Probleme gibt (*check*),
- aus den gewonnen Erkenntnissen und anderen zwischenzeitlich gestellten neuen Anforderungen notwendige Veränderungen ableitet (*act*).

Diese 4 Phasen des PDCA-Zyklus sind als Regelkreis zu verstehen, d. h. nach der Phase *act* steigt man wieder in die Phase *plan* ein, um die als notwendig erkannten Änderungen zu planen, danach in die Phase *do*, usw.

Bei der Phase *act* werden neben den Erkenntnissen der Phase *check* auch andere zwischenzeitlich gestellte neue Anforderungen berücksichtigt. Hiermit reagiert man auf die Erfahrung, dass im laufenden Prozess oft der Anwendungsbereich oder das Sicherheitsniveau angepasst werden soll oder auch nur neue Sicherheitserkenntnisse zu berücksichtigen sind.

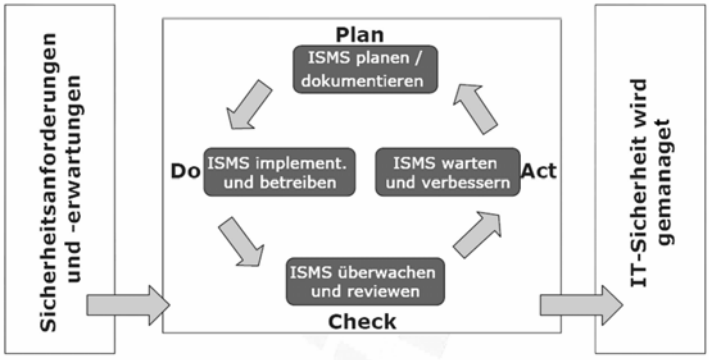

Abbildung 1: PDCA-Zyklus in der IT-Sicherheit

ISMS

Man erkennt sofort, dass dieses Modell im Grunde für das Management jedes Themas geeignet ist. Es findet deshalb in zunehmendem Maße in allen Management-Standards Anwendung[2]. Die Abbildung 1 konkretisiert das PDCA-Modell für das „Informationssicherheits-Management-System" (ISMS).

Wie und wo soll nun das PDCA-Modell angewendet werden?

Betrachten wir die ideale Situation, dass von der Unternehmensleitung das Thema IT-Sicherheit aufgegriffen, ein Sicherheitsmanagement eingerichtet und diesem die interne Verantwortung für die Sicherheit übertragen wird. Auf beiden Ebenen – der Leitung und dem Sicherheitsmanagement – ist nun das PDCA-Modell zu realisieren:

Leitungsebene

Bei der Leitung besteht *plan* darin, eine Zielvorgabe für die Sicherheit zu geben; dies solle schriftlich geschehen, und zwar mit der so genannten „Sicherheitsleitlinie". Die Phase *do* besteht darin, das Sicherheitsmanagement einzurichten und damit zu beauftragen, die Sicherheitsleitlinie umzusetzen. In der Phase *check* prüft die Leitung aufgrund der Berichte des Sicherheitsmanagements und ggf. eigener Erkenntnisse, ob die Zielvorgabe umgesetzt worden ist und ob es Probleme in der Anwendung gegeben hat. Aus dem Ergebnis werden Schlüsse über notwendige Anpassungen der Sicherheitsleitlinie getroffen (*act*).

Management-Bewertung

Praktisch geschieht dies alles dadurch, dass die Leitung den PDCA-Zyklus in regelmäßigen Sitzungen abarbeitet und über die Ergebnisse entsprechende Aufzeichnungen macht. Themen dieser Sitzungen sind die Berichte des Sicherheitsmanagements, eigene Erkenntnisse über die Sicherheit des Unternehmens oder von Dritten, ebenso wesentliche Änderungen der Gesetzeslage oder neue geänderte Sicherheitsanforderungen aus aktuellen Kundenverträgen.

Der zentrale Besprechungspunkt ist dabei regelmäßig die *Bewertung* der Sicherheitslage des Unternehmens und die *Bewertung* der Wirksamkeit des Sicherheitsmanagements sein, weshalb

---

2 z. B. beim Quality Management (ISO 900x), Umweltschutz-Management (EN ISO 1400x), Sicherheitsmanagement (ISO 27001); es findet aber auch implizit Anwendung beim Management von sicherheitskritischen Organisationseinheiten; ein Beispiel hierfür sind Vorgaben in einer Schweizer Richtlinie zum Sicherheitsmanagement beim Betrieb von Trust Centern oder den entsprechenden Vorgaben des Standards ETSI 101.456.

im Standard ISO 27001 auch von einer *Management-Bewertung* die Rede ist.

Im Ergebnis dieser Sitzungen kann eine Entlastung des Sicherheitsmanagements erfolgen oder diesem eine geänderte Sicherheitsleitlinie zugeleitet werden mit der Vorgabe, die Änderungen umzusetzen.

Sicherheitsmanagement

Auf der Ebene des Sicherheitsmanagements wird ebenfalls nach PDCA gearbeitet: Mit der Zielvorgabe der Sicherheitsleitlinie als Input wird die gewünschte Sicherheit konzipiert (*plan*), d. h. es entsteht ein „Sicherheitskonzept", oder es werden Anpassungen an einem existierenden Sicherheitskonzept vorgenommen.

Die Umsetzung dieses Konzeptes geschieht in der Phase *do*. Alle Erfahrungen aus der Praxis und aus regelmäßigen Überprüfungen werden aufgezeichnet (*check*). In der Phase *act* werden die gesammelten Aufzeichnungen – in Verbindung mit sonstigen Erkenntnissen – ausgewertet und Handlungsvorschläge zur Verbesserung der Sicherheit abgeleitet. Das Ergebnis der Phase *check* wird der Leitung mitgeteilt. Stimmt diese dem Ergebnis zu, plant das Sicherheitsmanagement die Umsetzung der Verbesserungsvorschläge und steigt damit wieder in die Phase *plan* ein…

Auch beim Sicherheitsmanagement sollte man sich konsequent am PDCA-Modell orientieren, folglich regelmäßig Sitzungen mit den Beteiligten anberaumen, um sukzessive die 4 Phasen abzuarbeiten. Gegenstand der Besprechungen sind u. a. neue Sicherheitserkenntnisse und eventuelle Sicherheitsvorkommnisse, die analysiert und bewertet werden müssen. Die Ergebnisse solcher Besprechungen sind natürlich aufzeichnen!

In welchem Abstand sind solche Besprechungen durchzuführen? Sie könnten z. B. quartalsweise durchgeführt werden mit dem Ziel, den vollen PDCA-Zyklus einmal pro Jahr bearbeitet zu haben. Je nach Erfordernissen kann man diese Abstände auch verlängern oder verkürzen. In den Standards finden sich hierzu keine bindenden Vorgaben. Ungeachtet dessen können z. B. gravierende Sicherheitsvorfälle Anlass bieten, solche Besprechungen anzuberaumen.

Man erkennt, dass durch Einhaltung dieses Vorgehensmodells das Verbesserungspotenzial sukzessive ausgeschöpft und somit die Sicherheit Schritt für Schritt verbessert werden kann.

Konkretisierung

Das PDCA-Modell wollen wir nun eine Ebene tiefer konkretisieren, indem wir die relevanten Tätigkeiten für die Leitung und das

Sicherheitsmanagement zusammenstellen. Beginnen wir mit der Leitungsebene:

Tabelle 1: PDCA für die Leitungsebene

Phase	Erst-Aktivitäten	Folge-Aktivitäten
Plan		
Plan1	Sensibilisierung (wenn nötig)	
Plan2	Informationen beschaffen	
Plan3	Sicherheitsleitlinie als Zielvorgabe erstellen (lassen)	Sicherheitsleitlinie ggf. anpassen / überarbeiten (lassen)
Plan4	Sicherheitsleitlinie formell in Kraft setzen	Ggf. geänderte Sicherheitsleitlinie formell in Kraft setzen
Do		
Do1	Sicherheitsmanagement einrichten	ggf. Sicherheitsorganisation anpassen
Do2	Ressourcen bereitstellen	Ressourcen ggf. anpassen
Do3	Auftrag an das Sicherheitsmanagement: Sicherheitsleitlinie umsetzen, regelmäßig Berichte für die Leitungsebene erstellen	
Check		
Check1	Berichte des Sicherheitsmanagements prüfen	
Check2	sonstige Erkenntnisse einbringen	
Act		
Act1	Informationen analysieren	
Act2	Verbesserungspotenzial feststellen	
Act3	Vorschläge des Sicherheitsmanagements prüfen / genehmigen bzw. ablehnen	

Einige Anmerkungen zu den einzelnen Punkten:

Plan1/2 Als Teil der Phase *plan* haben wir zwei neue Aktivitäten einbezogen:

– die Sensibilisierung der Leitungsebene für die Informationssicherheit,
– die Beschaffung weiterer Informationen, um die folgenden Schritte qualifiziert angehen zu können.

Dies erscheint notwendig, weil oft nur ein rudimentäres Verständnis für das Thema und seine Strukturen gegeben ist. Weitere Informationen hierzu finden Sie im Abschnitt „2.3 Unverzichtbar: Sensibilisierung, Schulung, Training".

Plan3 Die Sicherheitsleitlinie ist das zentrale Vorgaben-Dokument der Leitungsebene für die Informationssicherheit im Unternehmen. Es stellt einerseits den wichtigen Input für das vom Sicherheitsmanagement zu erstellende Sicherheitskonzept dar, andererseits ist es auch eine Zielvorgabe für alle Mitarbeiter des Unternehmens. Weitere Informationen finden Sie im Kapitel „6. Die Sicherheitsleitlinie".

Plan4 Die Sicherheitsleitlinie ist erstmalig und ebenso nach Änderung per Unterschrift in Kraft zu setzen. Sie muss anschließend den Mitarbeitern des Unternehmens bekannt gegeben werden.

Check2 In dieser Teilphase geht es um sonstige Erkenntnisse der Leitungsebene – z. B. aus eigenen Beobachtungen und Sicherheitsvorfällen oder Mitteilungen Dritter.

Kommen wir nun zu den PDCA-Aktivitäten des Sicherheitsmanagements:

Tabelle 2: PDCA für das Sicherheitsmanagement

Phase	Erst-Aktivitäten	Folge-Aktivitäten
Plan		
Plan1	eigene Sensibilisierung (wenn nötig)	
Plan2	Informationen beschaffen, ggf. eigene Schulung	
Plan3	Sicherheitsleitlinie und sonstige Vorgaben der Leitungsebene identifizieren	die geänderte Sicherheitsleitlinie und sonstige Vorgaben der Leitungsebene identifizieren

Phase	Erst-Aktivitäten	Folge-Aktivitäten
Plan4	Sicherheitskonzept und Begleitdokumente erstellen (lassen)	Sicherheitskonzept und Begleitdokumente ggf. anpassen und überarbeiten (lassen)
Plan5	Abstimmung und Genehmigung des Sicherheitskonzeptes und der Begleitdokumente	Abstimmung und Genehmigung nur der Änderungen bzw. Neuerungen
Do		
Do1	Sicherheitskonzept (resp. Änderungen) durch zuständige Fachabteilungen umsetzen lassen	
Do2	Umsetzung überwachen	
Do3	Maßnahmen aus den Bereichen Sensibilisierung, Schulung, Training aufsetzen.	
Do4	Sicherheitskonzept in Kraft setzen	
Do5	Sicherheitsvorfälle managen	
Check		
Check1	Praxis überprüfen	
Check2	Sicherheitsvorfälle auswerten	
Check3	sonstige Erkenntnisse einbringen	
Act		
Act1	Schlussfolgerungen ziehen	
Act2	Verbesserungspotenzial feststellen, Berichte an die Leitung	

Plan 3

Eher selten kommt der Fall vor, dass die Leitungsebene die Sicherheitsleitlinie selbst erstellt, vielmehr erhält das Sicherheitsmanagement den Auftrag, einen Entwurf zu erstellen. Wesentlich ist aber, dass die Leitung die Sicherheitsleitlinie in Kraft setzt. Erst dann sollte sie als Input für das Sicherheitsmanagement gelten.

Plan4

Das Sicherheitskonzept ist das zentrale Dokument für das Sicherheitsmanagement. Es sollte vollständig, in sich konsistent und nachvollziehbar sein. Weitere Informationen zum Sicherheitskon-

zept finden Sie im Kapitel „8. Das Sicherheitskonzept“. Hinweise zu den Begleitdokumenten und zum Aufbau der Sicherheitsdokumentation finden Sie im Abschnitt „2.4 Management der Dokumentation“.

Plan5 Dieser Punkt *Plan5* muss bei der Planung der Schritte berücksichtigt werden, weil er erfahrungsgemäß immer einen hohen zeitlichen Verzug mit sich bringt.

Do1/Do2 Nach der Genehmigung des Sicherheitskonzeptes müssen die dort aufgeführten Maßnahmen sukzessive umgesetzt werden. Dabei ist es *nicht* die Aufgabe des Sicherheitsmanagements, die Umsetzung ganz oder in Teilen selbst vorzunehmen. Vielmehr ist dies die Aufgabe der zuständigen Fachabteilungen, etwa der Personalabteilung für personelle Maßnahmen, der IT-Abteilung für IT-bezogene Maßnahmen, usw.

Das Sicherheitsmanagement überwacht diese Umsetzungen in dem Sinne, dass eine genaue Übereinstimmung zwischen Sicherheitskonzept und Praxis erzielt wird. Um dies zu erreichen ist es sinnvoll, die ausführenden Fachabteilungen mit einem Formular auszustatten, mit dem für jede Maßnahme

- entweder die korrekte Umsetzung bestätigt wird,
- oder ggf. aufgetretene Probleme mit entsprechenden Lösungsvorschlägen an das Sicherheitsmanagement berichtet werden.

Do3 Hier geht es um Maßnahmen für die *Mitarbeiter* als Zielgruppe: Es muss eine ausreichende Sensibilität für die Informationssicherheit vorhanden sein und aufrechterhalten werden. Schulungsmaßnahmen betreffen die vorgesehenen Sicherheitsmaßnahmen und deren Nutzung bzw. Einsatz. Training bezieht sich auf die Tätigkeiten sicherheitskritischer Rollen. Nähere Informationen finden Sie im Abschnitt „2.3 Unverzichtbar: Sensibilisierung, Schulung, Training“.

Do5 Beim Management von Sicherheitsvorfällen geht es um die drei Aktivitäten *Erkennen*, *Melden* und *Bearbeiten* von Sicherheitsvorfällen.

- Das Erkennen geschieht auf der Ebene von Mitarbeitern oder auch Externen, ggf. auch durch automatische Systeme (Alarmfunktionen, Intrusion Detection).
- Sobald ein vermeintlicher oder tatsächlicher Sicherheitsvorfall erkannt worden ist, muss eine Meldung erfolgen. Dazu muss der Meldeweg dokumentiert sein.

– Läuft eine Meldung beim Sicherheitsmanagement auf, so besteht dessen Aufgabe darin, eine Klassifizierung des Vorfalls vorzunehmen und dann entsprechend dem Ergebnis angemessen zu reagieren. Nähere Informationen zu diesem Thema finden Sie im Abschnitt „14.2 Management von Sicherheitsvorfällen".

Check1 Die Einhaltung des Sicherheitskonzeptes in der Praxis zu garantieren ist eine der Kernaufgaben des Sicherheitsmanagements. Dies verlangt eine entsprechende Überprüfungstätigkeit. Dazu zählen Aktivitäten wie

– Informationsgespräche mit Mitarbeitern führen,
– Vorgaben stichprobenartig auf Einhaltung prüfen,
– technische Untersuchungen (z. B. Penetrationstests) durchführen (lassen),
– Konfigurationen und Einstellungen technischer Systeme überprüfen,
– Checklisten kontrollieren,
– Log-Protokolle prüfen (lassen),
– interne und externe Audits veranlassen.

Dabei sollte es die Regel sein, von allen Aktivitäten dieser Art Aufzeichnungen zu machen. Andernfalls hat das Sicherheitsmanagement kein Material für die Phase *act* und keine objektiven Nachweise für seine Tätigkeiten.

Check2 Eine wichtige Quelle von Informationen sind Sicherheitsvorfälle: Auch wenn ihr Eintreten meist mit einem Schaden verbunden ist, sind sie für das Sicherheitsmanagement geradezu der Paradefall, an dem man erkennen kann, wie es um die reale Sicherheit des Unternehmens und die Praxisnähe seiner Verfahren bestellt ist.

Scherzhaft wird oft gesagt: „Wenn es diesen Vorfall nicht gegeben hätte, hätten wir ihn geradezu herbeiführen müssen…". Sicherheitsvorfälle sind einerseits wichtig, um daraus lernen zu können, andererseits „beflügeln" sie oft Entscheidungen, die vorher nicht zu bekommen waren.

Check3 Jeder IT-Sicherheitsbeauftragte erhält wichtige Informationen durch das Studium von Artikel in Fachzeitschriften bzw. aus dem Internet. Unter Umständen hat man CERT-Dienste abonniert und wird mit „heißen" Meldungen versorgt (s. Abschnitt „5.5 Ergänzendes zur Schwachstellenanalyse"). Solche Informationen sind

dahingehend zu prüfen, ob sie für das eigene Unternehmen relevant sind.

Act1/2

Bei diesen Punkten geht es darum, die Gesamtheit zwischenzeitlich aufgelaufener Informationen auszuwerten, um ggf. Korrektur- und Vorbeugemaßnahmen abzuleiten. Dabei müssen stets mögliche Rückwirkungen auf die Sicherheitsdokumente geprüft werden. Änderungen an der Dokumentation sind zu planen, und zwar in der nächsten Runde mit der Phase *plan*.

Schlussendlich sei angemerkt, dass die Anwendung von PDCA nicht auf die Leitung und das Sicherheitsmanagement beschränkt sein muss. Man kann hierin eine Vorgehensweise für jede am Sicherheitsprozess beteiligte Rolle sehen…

Information Security Forum

Wir haben die Vorgehensweise nach PDCA in einem Organisationsmodell vorgestellt, in dem die *Fachebene* (IT-Sicherheitsmanagement) der *Entscheidungsebene* (Unternehmensleitung) berichtet. In komplexen Unternehmensstrukturen kann es sinnvoll sein, zwischen dem Sicherheitsmanagement und der Leitung ein Entscheidungsgremium einzurichten, in dem die Leitung *und* die Fachebene vertreten sind, um eine Beschlussfähigkeit herzustellen. In den Standards BS 7799 und ISO 17799 wird ein solches Gremium als *Information Security Forum* (ISF) bezeichnet.

2.3 Unverzichtbar: Sensibilisierung, Schulung, Training

Beschäftigen wir uns zunächst mit den Begriffen:

- „Sensibilisieren“ heißt, auf ein für das Unternehmen wichtiges Problem aufmerksam machen.
- „Schulen“ meint, Lösungen für das Problem vermitteln.
- „Training“ hat den Sinn, Lösungen in der Praxis zu üben.

Wir behandeln diese drei Ebenen in den folgenden Abschnitten.

Sensibilisierung

Wer Sicherheit in seinem Unternehmen vorantreiben möchte, macht oft die Erfahrung, dass die Leitungsebene vom Thema IT-Sicherheit nicht gerade begeistert ist. Das geringe Interesse tendiert sogar gegen Null oder provoziert negative Emotionen, wenn man zur Behandlung des Themas Kompetenzen und Ressourcen einfordert. Selbst wenn man die gewünschten Ressourcen nach intensivem Bemühen bekommt, wird man sich immer wieder der Situation ausgesetzt sehen, dass „oben“ kein Verständnis für die Aufgabe der IT-Sicherheit herrscht und man