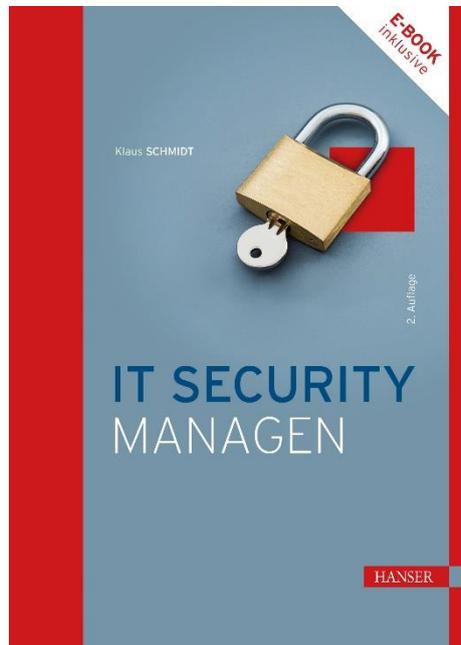


HANSER



Leseprobe

zu

IT Security managen

von Klaus Schmidt

Print-ISBN: 978-3-446-47759-9
E-Book-ISBN: 978-3-446-47822-0
E-Pub-ISBN: 978-3-446-48168-8

Weitere Informationen und Bestellungen unter
<https://www.hanser-kundencenter.de/fachbuch/artikel/9783446477599>

sowie im Buchhandel

© Carl Hanser Verlag, München

Inhalt

Vorwort	XIII
Der Autor	XIV
1 Stellenwert der Informationssicherheit	1
1.1 Das Wesen einer Information	2
1.2 Informationstechnik als Informationsinfrastruktur	4
1.3 Sicherheit als Erfolgsfaktor	5
1.4 Sicherheitsfunktionen im Unternehmen	7
1.5 Risikomanagement vs. IT-Sicherheit	7
2 Risiko und Sicherheit	9
2.1 Risiko	9
2.1.1 Begriffsbedeutung	10
2.1.2 Risiko und Gefahr	11
2.1.3 Deutungen des Risikobegriffs	12
2.1.4 Erkenntnisse über Risiken	13
2.2 Sicherheit	15
2.2.1 Sicherheitskriterien	15
2.2.2 Sicherheitsgrad	19
2.2.3 Sicherheitsstufen	20
2.2.4 Verhältnis zwischen Sicherheitsgrad und Aufwand	21

3	Entstehung und Auswirkungen von Risiken	23
3.1	Schwachstelle	23
3.2	Angriffspfad	24
3.3	Auslöser	25
3.4	Bedrohung	26
3.5	Sicherheitsrelevantes Ereignis	27
3.6	Risikoszenario	28
3.7	Auswirkungen	29
3.8	Beispiele für Schadensszenarien	31
4	Sicherheitsorganisation	35
4.1	Sicherheitsbereiche im Unternehmen	35
4.1.1	Physische Sicherheit	36
4.1.2	Arbeitssicherheit	37
4.1.3	Technische Sicherheit	37
4.1.4	Produktionssicherheit	38
4.1.5	Produktsicherheit	38
4.1.6	Informationssicherheit	39
4.1.7	Umweltschutz	39
4.1.8	Datenschutz	39
4.1.9	Revision	40
4.1.10	Finanzielle Sicherheit	40
4.1.11	Patentschutz	40
4.2	Rollen in der IT-Sicherheit	41
4.2.1	IRM/ITRM	41
4.2.2	ISM/ITSM	41
4.2.3	ISB	42
4.2.4	ITSB	42
4.2.5	DSB	42
4.2.6	ITM	43
4.2.7	IT-Revision	43
4.2.8	IT-Sicherheitsgremium	43
4.2.9	IT-Benutzersupport	44
4.3	Organisationsmodelle	44
4.3.1	Beispiel 1	45

4.3.2	Beispiel 2	46
4.3.3	Beispiel 3	47
4.3.4	Beispiel 4	48
4.3.5	Beispiel 5	49
4.4	Gestaltung einer Sicherheitsorganisation	50
5	IT Security Policy	53
5.1	Historie	54
5.2	Bedeutungen und Ausprägungen	55
5.2.1	IT Security Policy als Sammlung technischer Sicherheitsmaßnahmen	56
5.2.2	IT Security Policy als Liste generischer IT-Sicherheitsanforderungen	56
5.2.3	IT Security Policy mit Meta-Anforderungen	57
5.2.4	IT Security Policy als Grundsatzdokument	57
5.3	Bestandteile einer IT Security Policy	58
5.3.1	Gültigkeitsbereich bzw. Reichweite	58
5.3.2	Inkraftsetzung	59
5.3.3	Behandlung von Verstößen	60
5.3.4	Verständlichkeit und Eindeutigkeit	60
5.4	Koordinierung und Strukturierung	61
5.4.1	Policy-Hierarchie	61
5.4.2	Zentrale Koordinierung	69
5.4.3	Objektorientierte und verkettete Policies	70
5.5	Information Security Controls	71
5.5.1	Formulierung von Controls	72
5.5.2	Control Objective	78
5.5.3	Zielrichtung der Control-Aktivität	79
5.6	Policy Management	82
6	Sicherheit definieren und vorgeben	85
6.1	Ziele	87
6.2	IT-Sicherheitsstrategien	91
6.2.1	Strategie der chinesischen Mauer	91
6.2.2	Strategie der prozessbasierten Sicherheit	92
6.2.3	Sicherheit von innen nach außen	92

6.2.4	Sicherheit durch Eigentümerschaft	93
6.2.5	Auswahl der Strategie	93
6.3	IT-Sicherheitspolitik	94
6.4	Business-Impact-Analyse	96
6.5	Abhängigkeitsmatrix	100
6.6	Schutzbedarfsanalyse	100
6.6.1	Technikorientierte Schutzbedarfsanalyse	101
6.6.2	Informationsorientierte Schutzbedarfsanalyse	102
6.7	IT-Sicherheitsstandards	103
6.7.1	BSI-Grundschutz	104
6.7.2	ISO 27001 und 27002	109
6.8	Vier-Phasen-Managementkreislauf	112
6.9	Der Information Security Circle	113
6.10	Zusammenspiel zwischen Statik und Dynamik	117
6.11	IT-/OT-Sicherheit	118
6.11.1	Erweiterter Sicherheitsbegriff	119
6.11.2	OT Security Norm IEC 62443	120
6.11.3	Übergreifendes IT/OT-Sicherheitsmanagement	123
7	Risiken erkennen und bewerten	125
7.1	Definition und Abgrenzung des Analyseobjekts	126
7.2	Ist-Aufnahme	126
7.2.1	Sichten von Dokumentationen	127
7.2.2	Führen von Interviews zur Ist-Aufnahme	128
7.2.3	Erheben des Ist-Zustands mit Fragebögen	134
7.3	Schwachstellenanalyse	136
7.4	Bedrohungsanalyse	138
7.4.1	Analyse der Bedrohungsfaktoren	138
7.4.2	Überprüfung vordefinierter potenzieller Bedrohungen	141
7.5	Risikoszenarien	142
7.6	Risikobewertung mit der Risikoformel	142
7.6.1	Eintrittswahrscheinlichkeit	143
7.6.2	Schadenshöhe	146
7.6.3	Probleme der Risikoformel	148
7.7	Darstellung der Risikosituation	149

7.8	Der Risikokorridor	151
7.9	Bewerten der Risikosituation und Risikopriorisierung	153
7.10	Risikobehandlung	154
7.11	Angemessene Schutzkonzepte	156
7.12	FMEA	158
7.13	Projektbegleitende Risikoanalyse	160
8	Reporting	163
8.1	Strukturmodell für das IT-Sicherheitsmanagement	163
8.1.1	Architekturschichten	165
8.1.2	Dimensionen	167
8.1.3	Betrachtungsebenen	168
8.1.4	Lebenszyklusphasen	170
8.1.5	Tiefe und Schärfe	172
8.2	Risk Reporting mit der Balanced Scorecard	173
8.2.1	Die betriebswirtschaftliche Balanced Scorecard	174
8.2.2	Anwendung der BSC im Sicherheitsmanagement	176
8.3	Security Capability Maturity Model	178
8.3.1	Das Capability Maturity Model (CMM)	178
8.3.2	Das Security Capability Maturity Model	180
8.4	Reporting mit dem Netzdiagramm	182
8.5	Security Landscape	182
9	Business Continuity	185
9.1	Ausgangssituation	187
9.2	Klassische Datensicherung	189
9.3	Datenspiegelung	192
9.4	RAID	194
9.5	Storage-Technologien	201
9.6	Replikation	203
9.7	Failover	207
9.8	Redundanz	208
9.9	Outsourcing	211
9.10	Fallback	212

10	Notfallmanagement	215
10.1	Notfallvorsorge	216
10.2	Notfallplanung	217
10.3	Erkennen des Notfalls	221
10.4	Notfallhandbuch	224
10.5	Notfallorganisation	226
10.6	Notfallverlauf	230
10.6.1	Sofortmaßnahmen	231
10.6.2	Notfallbeherrschung	234
10.6.3	Eskalation	236
10.6.4	Notbetrieb	238
10.6.5	Notfall-Recovery	239
10.6.6	Notfallende und Nachbereitung	241
11	Der Mensch in der Informationssicherheit	243
11.1	Politisches Wirken im IT-Sicherheitsmanagement	244
11.1.1	Formale Macht	244
11.1.2	Unternehmensebenen	246
11.1.3	Informelle Macht	248
11.1.4	Standing	249
11.1.5	Die Konsequenzen	251
11.1.6	Netzwerke schaffen	251
11.2	Change Management	254
11.2.1	Offener Widerstand	254
11.2.2	Verdeckter Widerstand	255
11.2.3	Verhinderungsgründe	256
11.2.4	Verschiedene Reaktionsmuster	257
11.2.5	Ablauf der Veränderung	259
11.2.6	Handlungsstrategien	260
11.3	Information Security Awareness	263
11.3.1	Gründe und Argumente für fehlende Awareness	263
11.3.2	Einsichten zum Leben der IT-Sicherheit	265
11.3.3	Die Awareness verbessern	266
11.4	User Security Standard	268

12	Incident Handling und IT-Forensik	271
12.1	Computerkriminalität	271
12.2	Erkennung von sicherheitsrelevanten Ereignissen	273
12.2.1	Ablauf eines möglichen Angriffs	273
12.2.2	Erkennung über Abweichungen	276
12.2.3	Weiterleiten des sicherheitsrelevanten Ereignisses	277
12.3	Beweissicherung	277
12.3.1	Den unveränderten Originalzustand sicherstellen	277
12.3.2	Probleme mit Zeitangaben	279
12.4	Forensische Untersuchung	280
12.5	Bewertung von sicherheitsrelevanten Ereignissen	281
12.6	Umgang mit der verursachenden Person	282
12.6.1	Interne Personen	282
12.6.2	Externe Personen	283
12.7	Eskalation von sicherheitsrelevanten Ereignissen	283
12.7.1	Eskalation an das Notfallmanagement	283
12.7.2	Einbeziehung von externen Ermittlungskräften	284
12.7.3	Einbindung sonstiger externer Kräfte	284
13	IT-Sicherheit und externe Partner	285
13.1	Externe Partner	286
13.2	Informationssicherheitsrisiken	286
13.3	Sicherheitsanforderungen für externe Partner	289
13.4	Security Service Level Agreements	293
13.5	Vertraulichkeitserklärungen	294
13.6	Datenschutz im Outsourcing	297
14	Rechtliche Einflüsse	299
14.1	IT-Sicherheitsgesetz	300
14.2	Datenschutz	302
14.2.1	Anwendbarkeit des Datenschutzes	303
14.2.2	EU Datenschutz-Grundverordnung (DSGVO)	305
14.2.3	Bundesdatenschutzgesetz (neu)	306
14.2.4	Der/die betriebliche Datenschutzbeauftragte	308
14.3	EU Cybersecurity Act	309

14.4	KonTraG	310
14.4.1	Stellung des Vorstands	311
14.4.2	Maßnahmen nach KonTraG	312
14.4.3	Geforderte Eigenschaften des Früherkennungssystems	313
14.4.4	Prüfungen nach KonTraG	314
14.5	COSO-Framework	315
14.6	UK Corporate Governance Code	318
14.7	Sarbanes-Oxley Act (SOX)	319
14.8	EU-Richtlinie 2006/43/EG („EuroSOX“)	322
14.9	Arbeitsrechtliche Haftung	323
14.10	Sonstige Haftungsregelungen	326
14.11	ITK-Gesetze	327
14.11.1	Informations- und Kommunikationsdienstegesetz (IuKDG)	328
14.11.2	Telemediengesetz (TMG) und Digitale-Dienste-Gesetz (DDG)	328
14.11.3	Signaturgesetz	330
14.11.4	Telekommunikationsgesetz (TKG)	330
14.11.5	Datenschutzgesetzgebung im ITK-Bereich	331
14.12	GoBS und GoBD	332
	Literatur	335
	Index	339

Vorwort

Die Zeiten sind längst vergangen, in denen Unternehmen von der Notwendigkeit der Informationssicherheit überzeugt werden mussten. Spektakuläre Sicherheitsvorfälle wie Nutzerdatendiebstähle im großen Stil oder empfindliche Betriebsunterbrechungen durch IT-Angriffe haben in den Unternehmen ein Bewusstsein für die Verletzlichkeit der Informationsverarbeitung und damit letztendlich auch der Geschäftstätigkeit geschaffen.

Die Erfahrung zeigt, dass die auf Informationen und die Informationstechnik bezogenen Bedrohungen vielfältig sind. Neben den Angriffen von außen, verübt von Hackern, Cyberkriminellen oder gar Geheimdiensten, sind es vor allem die Angriffe von innen, die, ausgestattet mit einem umfangreichen Wissen über das Unternehmen, durch Ausspähung und Diebstahl von unternehmenswichtigen Daten oder Sabotage dem Unternehmen schaden können. Solche Schadensfälle werden aufgrund der Image-schädigung in der Regel nicht publik gemacht.

Aber auch ohne Vorsatz existieren Informationsrisiken, zum Beispiel durch menschliche Schwächen wie Naivität oder Fehlbedienungen oder durch Elementargefahren wie Brände, Überflutungen oder Blitzschlag.

Die Unternehmen haben die Notwendigkeit und Wichtigkeit der IT-Sicherheit erkannt und mitunter umfangreiche IT-Sicherheitslösungen im Einsatz. Doch mit technischen Maßnahmen allein ist es nicht getan. Für die Planung, die Koordinierung, den Einsatz und die Kontrolle solcher Lösungen und für das weite Feld der organisatorischen Maßnahmen ist das Sicherheitsmanagement von großer Bedeutung.

Das vorliegende Buch soll Personen, die in das Thema Informationssicherheit einsteigen, das notwendige Wissen vermitteln, um im Management dieses Themas erfolgreich zu sein. Aber auch „alte Hasen“ und Personen aus anderen Sicherheitsbereichen werden nützliche Dinge in diesem Buch finden. Bewusst konzentriert sich das Buch auf die organisatorischen und methodischen Aspekte der IT-Sicherheit und

nicht auf die technische Behandlung des Themas. Hierfür wird die Perspektive der für das IT-Sicherheitsmanagement verantwortlichen Person eingenommen. Alle Geschlechter sind dabei gleichberechtigt angesprochen, auch wenn zur Erhaltung der Lesbarkeit an einigen Stellen (z. B. bei Rollenbezeichnungen) das generische Maskulin verwendet wurde.

Ich wünsche allen, die dieses Buch lesen, viele Denkanstöße bei der Lektüre und hoffe, dass Sie von dem Inhalt in Ihrem Verantwortungsbereich profitieren.

Vielen Personen ist zu danken, dass dieses Buch in dieser Form entstehen konnte. Der Zertifikatslehrgang „Information Security Manager“ der Akademie der Technologie gab ursprünglich den Anstoß für das Buch, daher sei hier Herr Klaus Häbel als damaliger Veranstalter erwähnt. Die vielen fachlichen Diskussionen mit Geschäftspartnern und Freunden waren konstruktiv und hilfreich – allen dafür ein herzliches Dankeschön. Mein Dank geht auch an das Lektorat vom Carl Hanser Verlag.

Ein besonderer Dank gilt meiner Frau Susanne Slater-Schmidt, die viel Geduld bewiesen und mich immer unterstützt hat. Ihr widme ich dieses Buch.

Klaus Schmidt

Flensburg, im Sommer 2023

Der Autor



Klaus Schmidt begann seine berufliche Laufbahn als Informationselektroniker in einer Entwicklungsabteilung der Siemens AG. Es folgten ein Hochschulstudium der Angewandten Informatik und Mathematik und der Einstieg in das IT-Consulting mit dem Schwerpunkt der Beratung deutscher Großunternehmen in den Themen IT-Infrastruktur und IT-Sicherheitsmanagement.

Seit 2001 unterstützt er mit seiner Marke Innomenta Unternehmen hinsichtlich des Managements der Informations- und IT-Sicherheit. Er erlangte die Zertifizierung zum Information Security Manager (CISM, ISACA), war Ausbilder für verantwortliche Personen im IT-Sicherheitsmanagement, Referent auf Sicherheitskonferenzen, regelmäßiger Seminarleiter bei Veranstaltungen des Management Circle und publiziert in diesem Themengebiet.

Sie erreichen den Autor per E-Mail unter klaus.schmidt@innomenta.de.

8

Reporting

Eine wichtige Aufgabe im IT-Sicherheitsmanagement besteht darin, andere Sicherheitsbereiche und die Leitungsebene über die gegenwärtige Situation der IT-Sicherheit zu informieren und darüber zu berichten. Für diese Aufgabe wird hier der englische Begriff Reporting verwendet.

Vor allem das Management ist Adressat für das Reporting, denn das Management (Vorstand, Geschäftsleitung) ist gesamtverantwortlich für die Informationssicherheit. Dieser Verantwortung kann es nur nachkommen, wenn es vom IT-Sicherheitsmanagement adäquat informiert wird.

Aufgabe ist, die Sicherheitssituation transparent zu machen und sie zusammen mit dem vorhandenen Handlungsbedarf zu kommunizieren.

8.1 Strukturmodell für das IT-Sicherheitsmanagement

Um die Sicherheitssituation verständlich reporten zu können und vor allem, um sie besser steuern zu können, muss zunächst die Komplexität des jeweiligen Betrachtungsgegenstands überschaubar gemacht werden (siehe Bild 8.1). Dazu wird die Realität des Betrachtungsgegenstands in einzelne Bereiche eingeteilt. Ohne diesen Schritt würde man vor einer Fülle von Objekten und Sicherheitsaspekten stehen, die nur schwer greifbar wären.

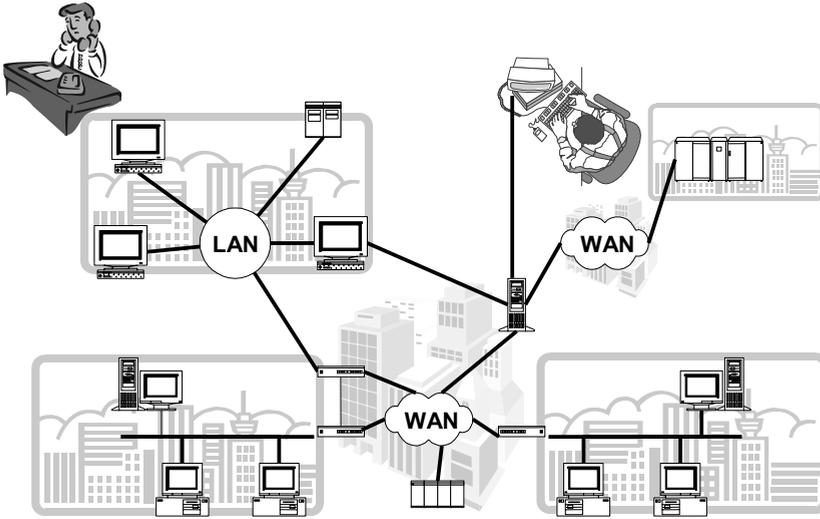


Bild 8.1 Komplexität der Realität

Die Sicherheit der Gesamtsituation setzt sich aus der Sicherheit dieser Bereiche und ihrem Zusammenspiel zusammen. Für die Strukturierung dieser Bereiche gibt es keinen verbindlichen Standard, man hat also freie Hand. Als zweckmäßig hat sich allerdings erwiesen, gleichartige Objekte zusammenzufassen und die Bereiche logisch aufzubauen (Bild 8.2).

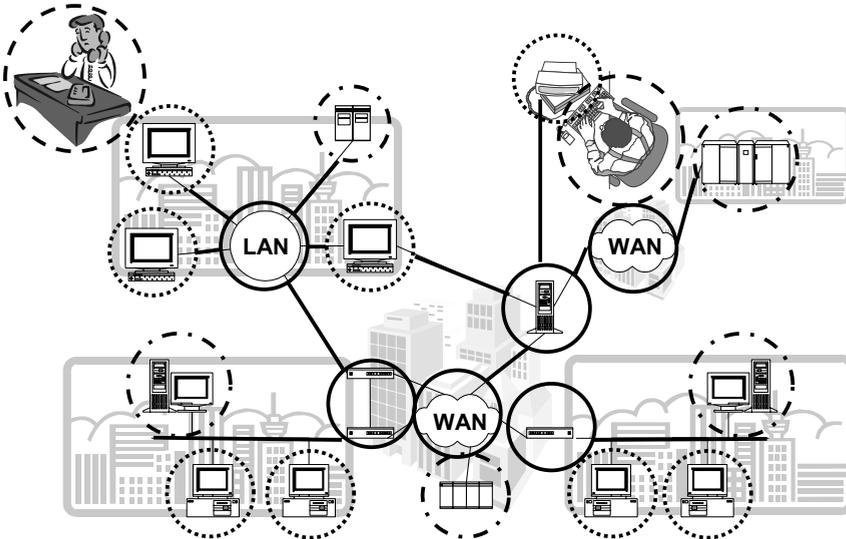


Bild 8.2 Klassifizierung von Objekten

In Bild 8.2 wurden als Bereiche Personen (gestrichelter Kreis), Backend-Systeme (Strichpunkt-Kreis), Frontend-Systeme (gepunkteter Kreis) und Netzwerkkomponenten (durchgängige Linien und Kreise) definiert.

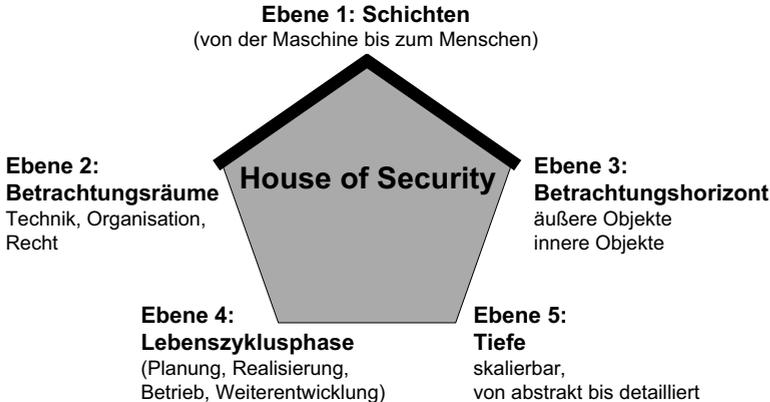


Bild 8.3 House of Security

Für die Strukturierung der Realität hat der Autor 1996 ein eigenes Strukturierungsmodell entwickelt und veröffentlicht. Da man sich die einzelnen Betrachtungsebenen als Eckpunkte der Silhouette eines Hauses vorstellen kann (Bild 8.3), hat sich intern der Name „House of Security“ gebildet, der auch hier verwendet werden soll. Das Modell hat sich in vielen Beratungsprojekten bewährt, die Logik der Schichten und auch direkt einige der Schichten wurden in die IT-Grundschutz-Methodik des Bundesamtes für Sicherheit in der Informationstechnik übernommen.

8.1.1 Architekturschichten

Die Betrachtungsebene, die als Erstes hier dargestellt werden soll, ist die Ebene der Architekturschichten. Der Betrachtungsgegenstand wird hier als Architektur begriffen, die sich in sieben Schichten einteilen lässt. Die Schichten bauen dabei logisch aufeinander auf, wie das nachfolgende Bild 8.4 zeigt:

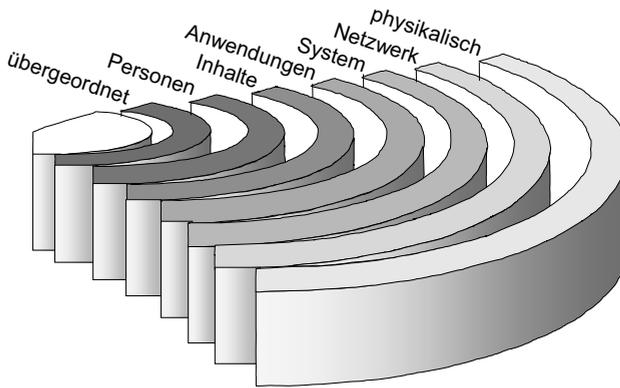


Bild 8.4 Schichten des HoS-Strukturmodells (Ebene 1)

Im House of Security existieren sieben Schichten¹⁾:

1. **Physikalisch (Schicht PHY).** Die physikalische Ebene enthält alle physischen Objekte, Komponenten oder Aspekte. Hier finden sich die baulichen Objekte wie Gelände, Gebäude, Etagen oder Räume. Auch Einrichtungen wie Klimaanlage, Brandschutzvorrichtungen o. Ä. gehören in die physikalische Schicht.
2. **Netzwerk (Schicht NET).** Alle Komponenten, die im Netzwerkbereich vorhanden und mit dem Netzwerk verbunden sind, finden sich in der Netzwerkschicht. Dies sind z. B. Netzwerkmedien, Switches, Router oder Hubs.
3. **System (Schicht SYS).** Die Systemschicht betrifft IT-Systeme wie Server oder Clients, aber auch systembezogene Komponenten wie Betriebssysteme und andere Systemsoftware.
4. **Anwendungen (Schicht ANW).** In diese Schicht wird Software eingeordnet. Auch Protokolle und Dienste zählen dazu. Anwendungssoftware, Skripte, Hilfsprogramme – alles Beispiele von Softwarekomponenten, die in die Anwendungsschicht eingeordnet werden.
5. **Inhalte/Daten (Schicht INH oder DAT).** Daten und Informationen gehören in diese Schicht. Das können Nutzdaten (z. B. Text- oder Grafikdateien) oder Systemdaten (z. B. Konfigurations- oder Protokollierungsdaten) sein. In welchem Format sie vorliegen, wie sie gespeichert sind und ob die Daten manuell erstellt oder automatisiert erzeugt werden, ist für die Einordnung unerheblich.
6. **Personen (Schicht PERS).** Hier finden sich alle sicherheitsbezogenen Aspekte, die sich auf Personen beziehen, z. B. das Thema Awareness.

¹⁾ Als betrachtetes Objekt (mehr dazu in Abschnitt 8.1.1) wird hier die IT-Architektur eines Unternehmens zugrunde gelegt.

7. **Übergeordnet/Prozesse (Schicht ÜBER oder PRZ).** Alle einer Schicht übergeordneten Aspekte, also Aspekte, die sich auf mehrere oder alle Schichten beziehen, finden in der Schicht ÜBER ihren Platz. Ein Beispiel wäre ein Sicherheitskonzept, das sich auf eine komplette Sicherheitslösung als Ganzes bezieht.

Diese Schicht nimmt auch die Organisation (z. B. das Sicherheitsmanagement selbst) und Prozesse auf, z. B. Sicherheitsaspekte von IT-Betriebsprozessen.

Die Schichten folgen einer inneren Logik. Bauliche Objekte wie Gebäude und Räume werden mit Netzwerken verbunden, an die Rechnersysteme angeschlossen sind. Die IT-Systeme tragen Anwendungen bzw. Applikationen (z. B. Datenbanken), welche wiederum Daten enthalten und/oder verarbeiten. Die Systeme, Anwendungen und Daten schließlich werden von Personen über definierte IT-Prozesse verwaltet.

In allen Schichten existieren IT-Sicherheitsanforderungen. Grundlage dafür ist die IT Security Policy (siehe Kapitel 5).

8.1.2 Dimensionen

Die Einteilung in einzelne Bereiche reicht alleine nicht aus, um die Sicherheitssituation transparent und steuerbar zu machen. Denn auch in den Bereichen bzw. Schichten gibt es noch eine Vielzahl von möglichen Sichten auf die Realität. Beispiele dafür sind die Perspektiven der Balanced Scorecard (z. B. finanzielle, prozessuale oder Entwicklungsperspektive) oder auch die rechtliche, menschlich/psychologische oder politische Sicht.

Daher muss die Realität in einer Schicht weiter unterteilt werden. Eine Möglichkeit aus dem Modell des House of Security zeigt Bild 8.5:

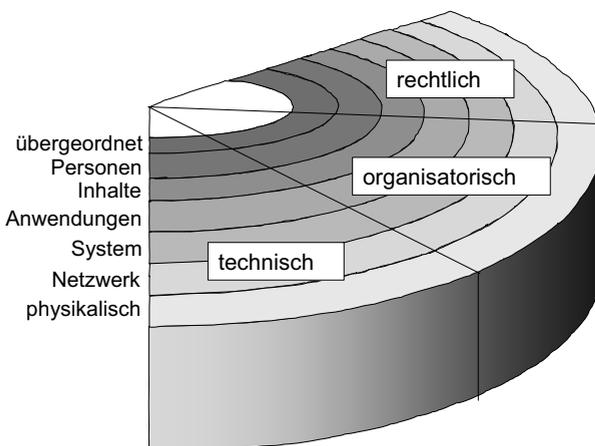


Bild 8.5 Dimensionen in den Schichten des House-of-Security-Modells

Es werden drei Dimensionen berücksichtigt:

- Technik (alle technischen Sicherheitsaspekte)
- Organisation (alle organisatorischen und menschlichen/psychologischen Sicherheitsaspekte²⁾)
- Recht (alle rechtlichen Sicherheitsaspekte)

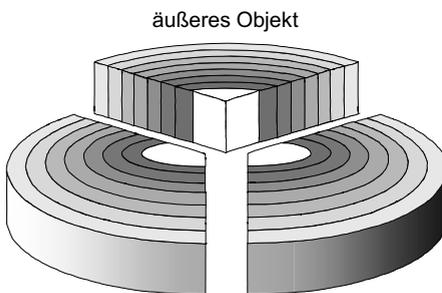
Weitere Dimensionen können je nach Bedarf definiert werden.

8.1.3 Betrachtungsebenen

Zu Beginn dieses Kapitels wurde erwähnt, dass es beim Reporting darum geht, die Sicherheitssituation des Unternehmens transparent zu machen. Die Sicherheitssituation des Unternehmens kann jedoch nicht direkt ermittelt werden, denn „das Unternehmen“ als einzelnes Objekt gibt es in der Realität nicht. Ein Unternehmen kann man weder sehen noch mit ihm telefonieren. Ein Unternehmen setzt sich aus vielen einzelnen Elementen zusammen: Standorten, Gebäuden, Personen, Maschinen, Verträge, Patente, Geschäftsbeziehungen usw.

Die Sicherheitssituation des Unternehmens setzt sich daher aus den Sicherheitssituationen der einzelnen Elemente der Realität zusammen. Das Ziel der Schichten war es, diese Elemente sinnvoll zu gruppieren. Dabei war die Betrachtungsebene die gesamte Realität (bezogen auf das Unternehmen also das gesamte Unternehmen).

Wenn die Sicherheitssituation aber nur bei den einzelnen Elementen zu ermitteln ist, muss es eine Möglichkeit geben, den Fokus auf ein einzelnes Element zu beschränken.



betrachtetes Objekt

inneres Objekt

Bild 8.6 Betrachtungsebenen

Dies geschieht, indem drei Betrachtungsebenen eingeführt werden. Das Element im Mittelpunkt wird als „betrachtetes Objekt“ bezeichnet. Es gibt eine Ebene oberhalb des betrachteten Objekts, in dem äußere Objekte existieren (bei einem Server ist ein äußeres Objekt z. B. der Raum, in dem er steht), und eine Ebene unterhalb des be-

² Auf die menschlich/psychologischen Aspekte wird in Kapitel 11 näher eingegangen.

trachteten Objekts, die innere Objekte enthält (bei einem Server z. B. eine auf dem Server installierte Software). Die Teilung in diese drei Ebenen wird in Bild 8.6 gezeigt. Dort ist auch zu sehen, dass jede Ebene alle sieben Schichten behält. Dies bedeutet: Für die Sicherheitssituation eines einzelnen Elements (z. B. einen einzelnen Server) müssen alle sieben Schichten betrachtet werden.

Beispiel Server: Liegt der Fokus auf dem ganzen Unternehmen, dann ist ein Server ein inneres Objekt in der Schicht SYS. Liegt der Fokus auf dem Server, so könnten in den sieben Schichten folgende Objekte vorhanden sein:

- **PHY:**
Äußere Objekte: Serverraum, Gebäude, Klimatisierung, Energieversorgung
Innere Objekte: Server-Hardware wie Gehäuse, Netzteil, Laufwerke
- **NET:**
Äußere Objekte: Netzwerkmedium, Switch, andere Komponenten des Netzwerks
Innere Objekte: Netzwerkinterface
- **SYS:**
Äußere Objekte: Domänenanbindung
Innere Objekte: Alle Komponenten der Betriebssystem-Software
- **ANW:**
Äußere Objekte: Replikationsverbindungen mit anderen Servern
Innere Objekte: Jede Anwendungssoftware und alle Dienste auf dem Server
- **INH:**
Äußere Objekte: Daten auf externen Datenträgern
Innere Objekte: Alle Daten, die auf internen Laufwerken des Servers liegen
- **PERS:**
Äußere Objekte: Administrationspersonal für den Server oder Wartungspersonal
Innere Objekte: Keine
- **ÜBER:**
Äußere Objekte: Server Policies
Innere Objekte: Serverspezifische Service Level Agreements

Die Betrachtungsebenen sorgen für Skalierbarkeit. Die Sicherheitssituation des Unternehmens kann bis auf einzelne Elemente skaliert werden, indem der Fokus verlagert wird. Diesen Zusammenhang zeigt Bild 8.7.

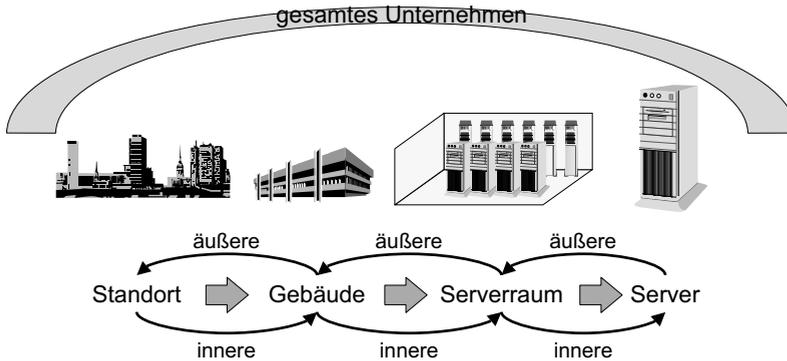


Bild 8.7 Skalierung der Sicherheitsbetrachtung

Für einen Serverraum ist das Gebäude das äußere Objekt, ein Server ist ein inneres Objekt. Liegt der Fokus auf dem Serverraum, so finden sich in der Schicht PERS Objekte wie Reinigungspersonal oder das Facility Management. Liegt der Fokus auf dem Server, sind in der gleichen Schicht andere Objekte zu finden wie z. B. das Personal für die Administration des Servers. Wichtig ist deshalb, zunächst die Betrachtungsebenen festzulegen und dann die Sicherheitssituation in der jeweiligen Betrachtungsebene aufzunehmen.

8.1.4 Lebenszyklusphasen

Jedes Objekt in der IT-Architektur durchläuft einen individuellen Lebenszyklus wie auch die IT-Architektur selbst. Eine ausreichende IT-Sicherheit sollte in allen Phasen dieses Lebenszyklusses sichergestellt sein. Das IT-Sicherheitsmanagement kann dabei in den einzelnen Phasen variieren. Es existieren verschiedene Lebenszyklusmodelle. Das Modell im House of Security ist relativ allgemeingültig und umfasst sechs Lebenszyklusphasen, die hier wieder anhand des Objekts eines Servers erläutert werden:

- **Planung.** In dieser ersten Phase wird der Einsatz des Servers konzipiert. Der Server selbst ist noch nicht vorhanden. Der Bedarf für den Server wird dokumentiert, Kostenbetrachtungen angestellt, das Einsatzszenario und die Ausprägungen spezifiziert (Netzwerkeinbindung, Dienste, Lastverhalten usw.) und ein Pflichtenheft für die Erfüllung der Anforderungen erstellt.
- **Entwicklung/Beschaffung.** Diese Phase besitzt zwei Ausprägungen: Entweder es wird ein Produkt konform zum Pflichtenheft entwickelt oder es werden fertig entwickelte COTS-Produkte verwendet, die lediglich ausgewählt und beschafft werden müssen.
- **Implementierung.** In der Implementierungsphase wird das fertig entwickelte bzw. beschaffte Objekt in einen betriebsfertigen Zustand gebracht. Das beginnt mit

der Qualitätskontrolle bei Anlieferung und geht über Inventarisierung, Aufstellung, Anschluss, Installation und Konfiguration, Integration in die IT-Architektur, Tests, Inbetriebnahme, Probetrieb bis hin zur Abnahme durch den vorgesehenen Betreiber.

- **Betrieb.** Mit der Abnahme beginnt die Betriebsphase, in der der Server gemäß des existierenden Betriebskonzepts im Regelbetrieb eingesetzt wird. Der Server wird überwacht, notwendige Wartungsmaßnahmen werden vorgenommen, Datensicherungen durchgeführt, Patches eingespielt usw.

Ebenfalls zur Betriebsphase gehört der Stör- und Notbetrieb. Hier werden Störungen, Sicherheitsvorfälle, Funktionsausfälle und Notfälle behandelt bzw. behoben.

- **Änderung/Weiterentwicklung.** In dieser Phase wird der Server geändert, angepasst, erweitert und weiterentwickelt. Gründe dafür können sich verändernde Anforderungen, Veränderungen in der IT-Architektur oder in der Nutzung der vom Server angebotenen Dienste sein. Aus technischen, organisatorischen oder vertraglichen Gründen kann sich auch ein Migrationsbedarf ergeben, bei dem der komplette Server getauscht wird. Strenggenommen gehören diese Maßnahmen noch zur Betriebsphase, denn der Server wird weiter eingesetzt, die Maßnahmen gehen aber über den täglichen Routinebetrieb hinaus, weshalb hier eine eigene Phase definiert ist.
- **Außerbetriebnahme/Entsorgung.** Diese letzte Phase tritt ein, wenn der Server veraltet ist und ersetzt werden muss oder der Server nicht mehr benötigt wird. Sie beginnt mit der Roll-off-Planung und geht über die De-Integration (Herausnahme aus der IT-Architektur) und die Abschaltung bis hin zum letzten Schritt, der Entsorgung der Server-Hardware.

In der Darstellung des Bottom-up-Vorgehens wurde bereits erwähnt, dass sich das Vorgehen in einzelnen Lebenszyklusphasen unterscheiden kann. So kann eine technische Risikoanalyse in der Planungsphase nicht stattfinden, da die konkreten technischen Ausprägungen der Objekte zu diesem Zeitpunkt noch nicht feststehen. Es ist daher wichtig zu wissen, welche Lebenszyklusphase gerade im Fokus steht.

In Bild 8.8 wurde das Modell des House of Security um die Lebenszyklusphasen erweitert. In der grafischen Darstellung wird die zweidimensionale Scheibe nun zur dreidimensionalen Säule.

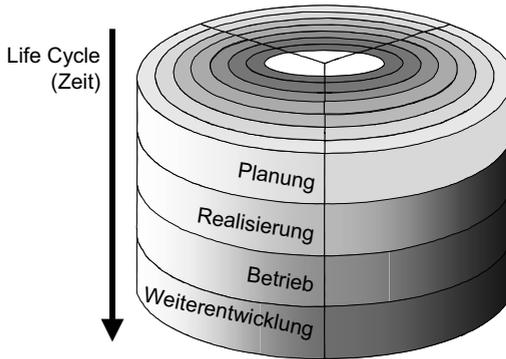


Bild 8.8 Lebenszyklusphasen (Ebene 4)

Mit den bisher aufgeführten Mitteln kann die Sicherheitssituation nicht nur punktgenau dargestellt, sondern auch gesteuert werden, denn die Situation lässt sich nach den einzelnen Komponenten des House of Security auswerten. Für jeden Fokus (Abschnitt 8.1.3) ergibt sich eine solche Säule, wie Bild 8.9 zeigt.

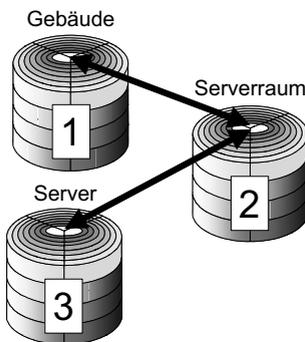


Bild 8.9 Das House of Security mit verschiedenen Betrachtungsebenen

Alle Schichten, Dimensionen, Lebenszyklusphasen und Betrachtungsebenen kontinuierlich im Auge zu behalten, ist auf manuellem Wege aufwendig und schwierig. Daher empfiehlt es sich, zur Unterstützung entsprechende Software zum IT-Sicherheitsmanagement einzusetzen.

8.1.5 Tiefe und Schärfe

Der letzte Eckpunkt des „Hauses“ im House of Security widmet sich der Ausprägung der Sicherheit. Es ist leicht nachvollziehbar, dass nicht alle Objekte den gleichen Schutzbedarf aufweisen. Ein Serverraum, der existenziell wichtige IT-Systeme beherbergt, muss sehr viel stärker geschützt werden als ein Serverraum, in dem nur relativ unwichtige Server stehen.

Diese Tatsache wird mit dem Eckpunkt „Tiefe und Schärfe“ berücksichtigt. Er greift die Frage „Wie viele und wie scharfe Sicherheitsanforderungen sind an das Objekt zu stellen?“ auf, die auch in der Top-down Security relevant ist. Dort stellt sie sich für die Anforderungen in der Security Policy. Welcher Schutzbedarf für die Objekte besteht, wird in der Schutzbedarfsanalyse (Abschnitt 6.7) ermittelt, dabei kann eine Business Impact Analyse (Abschnitt 6.5) sehr hilfreich sein.

Für das Reporting der Sicherheitssituation liefert dieser Eckpunkt die Information, die einen Soll-Ist-Vergleich zulässt. Die Soll-Information wird in Form von Anforderungen aus der IT Security Policy über das Top-down-Vorgehen in diesen Eckpunkt des House of Security eingebracht. Die Anforderungen werden dabei ebenfalls über das Modell des House of Security strukturiert, d. h. beispielsweise in Schichten eingeteilt.

8.2 Risk Reporting mit der Balanced Scorecard

Bei der Entscheidung, wie die Ergebnisse des IT-Sicherheitsmanagements zu berichten sind, sollte die Denkwelt der Personen bedacht werden, an die berichtet wird. In vielen Unternehmen zeigen sich immer noch zwei weitgehend isolierte Denkwelten: die Denkwelt der Technik und die Denkwelt des Managements. Beide Welten verfügen über eine grundverschiedene Philosophie und unterschiedliche Anforderungen.

Im Management muss man viele parallele Dinge im Auge behalten und benötigt daher kurze, prägnante Informationen. Die Informationen müssen schnell Auskunft darüber geben, wie die Situation einzuschätzen ist, ob und wie dringend Handlungsbedarf besteht und welche Handlungsmöglichkeiten bestehen.

Eine der dafür genutzten Methodiken, die in der Betriebswirtschaft für das strategische Management entwickelt wurde, ist die Balanced Scorecard (BSC). Sie eignet sich bei entsprechender Anpassung auch für das Risk Reporting an das Management. Der Vorteil liegt darin, dass ein solches Reporting im Management schnell verstanden wird, weil es in die Denkwelt des Managements passt.

Die Balanced Scorecard kann darüber hinaus auch als Steuerungsinstrument für das gesamte IT-Risiko- und IT-Sicherheitsmanagement verwendet werden. Weil die Verantwortung für die Informationssicherheit und insbesondere für die IT-Sicherheit aber immer noch überwiegend in den Händen von technisch geprägten Personen liegt und die Verwendung der Balanced Scorecard dort nicht verbreitet ist, soll sie in diesem Abschnitt vorgestellt werden.

8.2.1 Die betriebswirtschaftliche Balanced Scorecard

Anfang der 90er Jahre des letzten Jahrhunderts entwickelte Robert S. Kaplan an der Harvard Business School die Managementtechnik der Balanced Scorecard, um die stark finanzlastigen amerikanischen Managementsysteme um eine Liste von nicht-finanziellen Kennzahlen zu erweitern. Es zeigte sich, dass ein Zielsystem (Scorecard) mit einigen wenigen Größen (Perspektiven) für die Unternehmenssteuerung ausreicht, wenn sie die relevanten Geschäftsinhalte wie Kunden oder Geschäftsprozesse ausgewogen (balanced) berücksichtigt.

Die originäre Balanced Scorecard geht von vier grundsätzlichen Dimensionen aus, so wie sie in Bild 8.10 dargestellt sind.

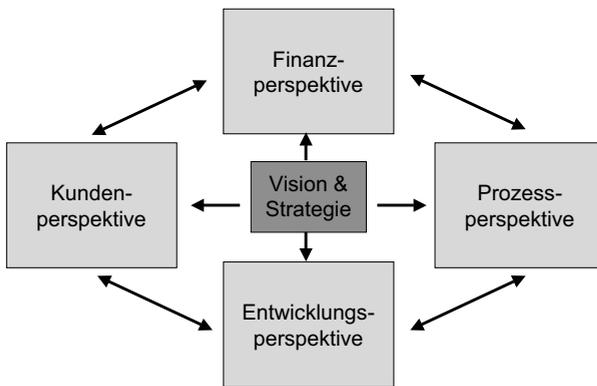


Bild 8.10 Die Perspektiven der Balanced Scorecard

Sie war als Kennzahlensystem gedacht und daher ursprünglich ein Instrument, das im Bottom-up-Bereich angesiedelt war. Die Kennzahlen wurden in vier Perspektiven gruppiert:

- Finanzperspektive (finanzielle Kennzahlen wie Umsatz, Gewinn usw.)
- Kundenperspektive (Kundenzufriedenheit, Servicequalität, Produktqualität)
- Prozessperspektive (Durchlaufzeiten, Transparenz, Stabilität)
- Entwicklungsperspektive (Innovationskraft, Flexibilität, Optimierung)

Die Balanced Scorecard als Liste von Kennzahlen wurde bald modifiziert. Nun standen die strategischen Ziele im Vordergrund, deren Grundlage die Unternehmensvision bildet. Damit wurde die Balanced Scorecard zu einem Top-down-Instrument, um Unternehmensstrategien umzusetzen.

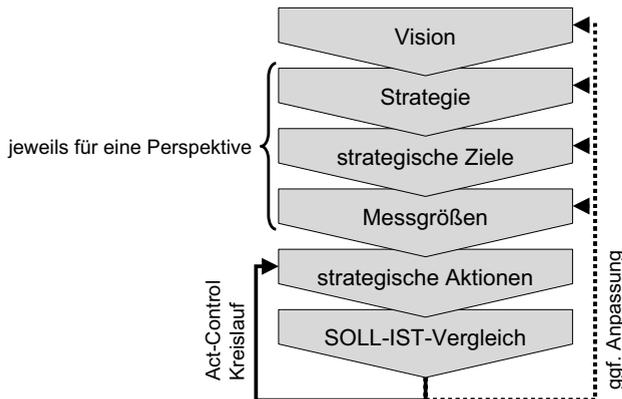


Bild 8.11 Von der Vision zur Strategieumsetzung

Die Umsetzung der Unternehmensstrategie erfolgt in mehreren Schritten (siehe dazu auch Bild 8.11):

1. Erarbeiten einer Vision (Wo wollen wir als Unternehmen in entfernter Zukunft stehen?)
2. Aufstellen der Strategie (Welchen Weg müssen wir einschlagen?)
3. Ableiten strategischer Ziele (Welche Etappen definieren wir auf diesem Weg?)
4. Definieren von Messgrößen (Wie merken wir, wo wir in Bezug auf die Ziele stehen?)
5. Strategische Aktionen (Was tun wir, um die strategischen Ziele zu erreichen?)
6. Soll-Ist-Vergleich (Wie nahe sind wir an der Zielerfüllung?)

Die strategischen Ziele, Messgrößen, Aktionen und Soll-Werte werden den vier Perspektiven zugeordnet, sodass sich ein vollständiges Zielsystem aufbaut, bei dem alle Perspektiven ausgewogen (balanced) behandelt werden sollen. Die Angaben in den Perspektiven wandelten sich nun von Kennzahlen hin zu strategischen Zielen:

- **Finanzperspektive.** Welche Ziele leiten sich aus den finanziellen Erwartungen der Kapitalgeber ab?
Beispiel: „Am Ende des nächsten Geschäftsjahres ist das Umsatzvolumen um 15 % gewachsen.“
- **Kundenperspektive.** Welche Ziele ergeben sich aus der Kundenstruktur und den Anforderungen der Kundenseite, um die finanziellen Ziele zu erreichen?
Beispiel: „Der Anteil der Großkunden beträgt im nächsten Quartal mindestens 20 %.“

- **Prozessperspektive.** Welche Ziele müssen hinsichtlich der Prozesse gesteckt werden, um die Kundenerwartungen erfüllen zu können und trotzdem finanzielle Ziele wie Kostenminimierung zu erreichen?

Beispiel: „Bis zum Monatsende sind unsere Mitarbeitenden in der Lage, Angebote innerhalb von zwei Werktagen abzugeben.“

- **Entwicklungsperspektive.** Welche Ziele müssen hinsichtlich der Weiterentwicklung, Innovation und Entwicklung von Potenzialen erreicht werden, um auch in Zukunft erfolgreich zu sein?

Beispiel: „Die Fremdsprachenkompetenz muss im Hinblick auf unsere Internationalisierung verbessert werden. Bis zum Ende des Geschäftsjahres haben alle Mitarbeitenden einen Fremdsprachenkurs besucht.“

Am Rande sei bemerkt, dass in letzter Zeit die Diskussion um eine weitere Perspektive aufkommt, mit der die Aspekte Nachhaltigkeit, ethische Verantwortung, soziale Solidarität und Bewahrung der Lebensgrundlagen abgebildet werden sollen.

8.2.2 Anwendung der BSC im Sicherheitsmanagement

Auch im IT-Sicherheitsmanagement existieren strategische Ziele und Soll-Definitionen. Damit lässt sich die Balanced Scorecard auch im Reporting des IT-Sicherheitsmanagements einsetzen. Sie wird dann, je nach Ausgestaltung, zur Security Scorecard oder Risk Scorecard (Bild 8.12).

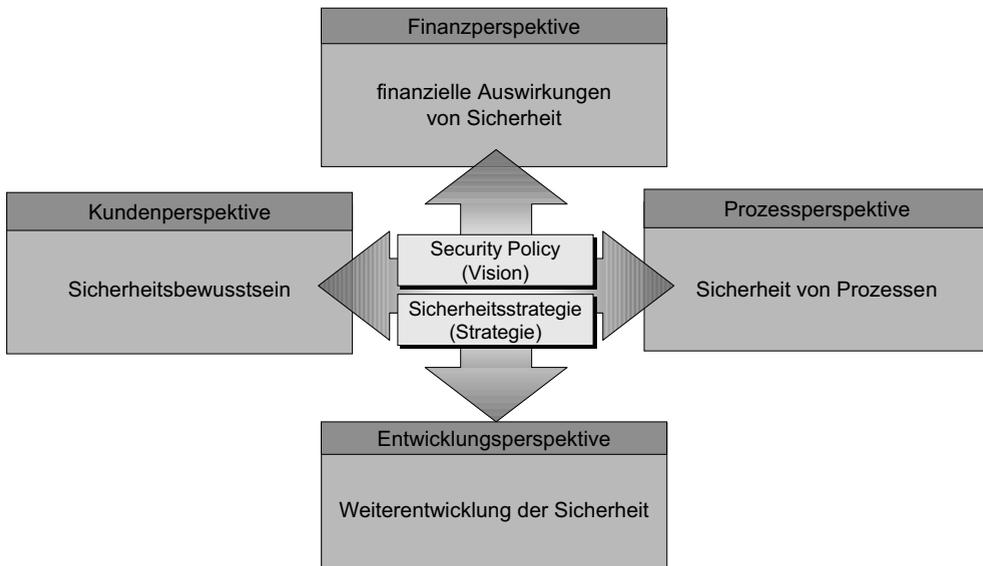


Bild 8.12 Security Scorecard

Die Vision des IT-Sicherheitsmanagements ist das optimal sichere Unternehmen in Bezug auf die IT-Sicherheit. Die Vision lässt sich mithilfe der Sicherheitskriterien (Kapitel 2) und der Strukturierung gemäß des House of Security in strategische Ziele herunterbrechen. Mit der gleichen Strukturierung kann die erreichte Situation berichtet werden. Dazu können in der Security Scorecard die gleichen Perspektiven wie in der betriebswirtschaftlichen Balanced Scorecard verwendet werden:

- **Finanzperspektive.** Welche Kostenminimierungsziele leiten sich für die Informationssicherheit aus den Erwartungen von übergeordneten, budgetverantwortlichen Stellen ab? Welche Ziele bestehen hinsichtlich der Vermeidung von finanziellen Verlusten? Welche Ziele werden hinsichtlich des Return on Investment (ROI) an IT-Sicherheitslösungen gestellt? Welchen Beitrag liefert die Informationssicherheit zur Realisierung der finanziellen Ziele?

Beispiel Ziele: „Innerhalb von zwei Jahren werden mit der flächendeckenden PKI-Integration viele der derzeitigen und proprietären Security-Insellösungen abgelöst und die Gesamtkosten für die IT-Sicherheitslösungen um mindestens 5 % reduziert. Innerhalb von zwei Jahren muss sich eine Investition in IT-Sicherheit amortisieren (Return on Security Invest).“

Beispiel Reporting: „Im vergangenen Jahr konnten durch die neuen BCM-Maßnahmen bei drei Betriebsausfällen rund 30 000 € finanzieller Verlust verhindert werden.“

- **Kundenperspektive.** Die IT-Sicherheit kann als Dienstleistung für das Unternehmen begriffen werden, die Unternehmensbereiche und auch die Mitarbeitenden wären damit „Kunden“ der IT-Sicherheit, die Produkte, Lösungen oder Dienste der IT-Sicherheit nutzen oder ganz allgemein ein IT-Sicherheitsinteresse besitzen.

Welche Ziele existieren für die IT Security Awareness der Mitarbeitenden? Welche Ziele ergeben sich aus dem Sicherheitsinteresse der „Kunden“?

Beispiel Ziele: „Bis zum Quartalsende werden wir ein Online-Portal für die Meldung von Sicherheitsvorfällen aufbauen.“

Beispiel Reporting: „Bislang haben 68 % der Mitarbeitenden an der diesjährigen Kampagne im Bereich IT Security Awareness teilgenommen.“

- **Prozessperspektive.** Welche Ziele werden hinsichtlich der Sicherheit von Geschäftsprozessen und IT-Prozessen gesteckt (Außenperspektive)? Welche Ziele werden für die IT-Sicherheitsmanagementprozesse verfolgt?

Beispiel Ziele: „Die IT in den geschäftstragenden Prozessen muss eine Verfügbarkeit von 99,999 % aufweisen.“

Beispiel Reporting: „Mit der Erstellung und Anwendung des IT-Security-Bedrohungskatalogs konnte der Zeitbedarf für die Erstellung von Risikoanalysen um ca. 20 % verringert werden.“

- **Entwicklungsperspektive.** Welche Ziele werden für die Weiterentwicklung des IT-Sicherheitsmanagements und der IT-Sicherheitsituation geplant? Welche Zielsetzung ergibt sich für den Reifegrad der Informationssicherheit?

Beispiel Ziele: „Bis zum Jahresende wird die Anzahl der erfüllten Security-Policy-Anforderungen um 25 % erhöht.“

Beispiel Reporting: „Der IT-Sicherheitsmanagementprozess wird in seiner neuen Form auch der KRITIS-Verordnung gerecht.“

Die detaillierte Gestaltung der Security bzw. Risk Scorecard ist nicht einheitlich festgelegt, hier gibt es demnach viel Spielraum für eigene Ideen. Beispielsweise könnte man das House of Security in die Scorecard integrieren.

8.3 Security Capability Maturity Model

In Kapitel 6 wurden innerhalb der Top-down Security mithilfe der Security Policy Sicherheitsanforderungen definiert. In der Praxis kommen dabei leicht Hunderte von Anforderungen zusammen.

Mit der Verwendung der Systematik des Capability Maturity Models in Verbindung mit dem Erfüllungsgrad der Anforderungen wird es möglich, den Reifegrad des Unternehmens in Bezug auf die Informationssicherheit zu ermitteln. Sie bietet sich auch deshalb an, weil es im Bereich der Informationssicherheit leichter fällt, eine „Optimalsituation“ zu formulieren – es ist schließlich bekannt, mit welchen Kriterien sich die Sicherheit definieren lässt (siehe Kapitel 2).

Damit steht ein Bewertungsrahmen mit unternehmensweitem Fokus zur Verfügung, der die Situation der Informationssicherheit im Unternehmen bewertbar macht.

8.3.1 Das Capability Maturity Model (CMM)

An der Carnegie Mellon University in Pittsburgh gibt es ein Institut, das sich mit Aspekten der Softwareentwicklung beschäftigt. Dieses Institut untersteht dem US-Verteidigungsministerium. Im Jahre 1986 begann man dort mit der Entwicklung eines Modells, mit dem sich die Reife von Softwareentwicklungsprozessen bewerten lässt. Dieses Modell wurde 1991 als Capability Maturity Model (CMM) in der Version 1.0 herausgegeben und in den Folgejahren weiterentwickelt. CMM wurde 2002 vom Nachfolgemodell Capability Maturity Model Integration (kurz CMMI) abgelöst.

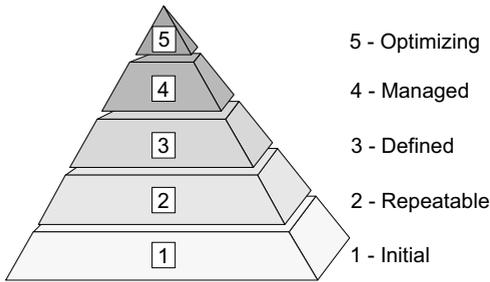


Bild 8.13 Capability Maturity Model

Das Modell selbst verfügt über fünf Reifegrade (Stufen), die die Qualität des Softwareentwicklungsprozesses widerspiegeln. Sie bauen aufeinander auf, sodass mit dem Modell auch Verbesserungen geplant werden können.

- **Initial (Stufe 1).** Die Softwareentwicklung ist chaotisch, es ist nicht vorhersehbar, wann die in Entwicklung befindliche Software fertig wird, welche Qualität sie aufweisen wird und was die Entwicklung kostet – denn alles wird weder geplant noch überwacht.
- **Repeatable (Stufe 2).** Die Abläufe der Softwareentwicklung gleichen sich von Projekt zu Projekt, das Wissen dafür ist aber oft nur in den Köpfen der Personen, die die Software entwickeln. Erfahrungen aus vergangenen Softwareentwicklungsprojekten werden für neue Projekte verwendet, dadurch kann die Entwicklungszeit grob eingeschätzt werden. Die Qualität ist schwer vorhersehbar, weil keine Qualitätskontrollen vorgesehen sind.

Im neuen CMMI-Modell wird diese Stufe mit „Managed“ bezeichnet.

- **Defined (Stufe 3).** Ein Standard-Softwareprozess mit Abläufen und Verantwortlichkeiten ist definiert, dokumentiert und wird gelebt. Die Entwicklungszeiten und -kosten können so einigermaßen beurteilt werden. Aufgrund fehlender Rückkopplung lässt sich die Qualität jedoch nicht garantieren. Die Software ist so gut, wie die entwickelnden Personen es sich vorstellen.
- **Managed (Stufe 4).** Die Softwareentwicklung richtet sich an quantitativen und qualitativen Zielen aus und nicht mehr an den Fähigkeiten der entwickelnden Personen. Fortschrittmessungen machen Zeiten und Kosten genauer planbar und auch die Qualität ist nun kontrollierbar. Im neuen CMMI-Modell wird diese Stufe mit „Quantitatively Managed“ bezeichnet.
- **Optimizing (Stufe 5).** Der Entwicklungsprozess wird regelmäßig auf Verbesserungspotenziale hin untersucht und weiterentwickelt. Das Unternehmen wird zur lernenden Organisation, Schwächen und Fehler werden gesucht, beseitigt und neue Fehler vorbeugend verhindert.

Die hier sehr knapp gehaltene Beschreibung der Stufen dient nur zum Verständnis. In der Praxis können die Maßnahmen, insbesondere für die Stufen 3 und 4, sehr um-

fangreich sein. Mit den Stufen lässt sich leicht nachvollziehen, was man benötigt, um von einer Stufe zur nächsten zu gelangen, und kann damit den Entwicklungsprozess Schritt für Schritt verbessern.

8.3.2 Das Security Capability Maturity Model

Ziel des CMM ist es, die Qualität des Softwareentwicklungsprozesses zu verbessern. Im Bereich der IT-Sicherheit ergibt sich die gleiche Aufgabe, nur dass es sich nicht um den Softwareentwicklungsprozess, sondern um den IT-Sicherheitsmanagementprozess handelt.

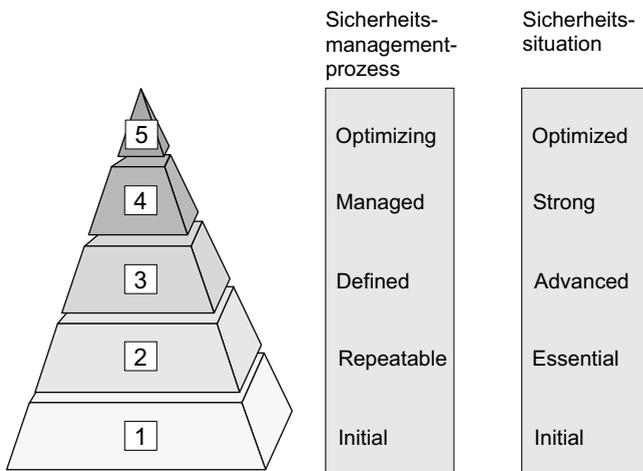


Bild 8.14 Security Capability Maturity Model

Das CMM lässt sich entsprechend anpassen und wird zum Security Capability Maturity Model (SCMM)³, das Auskunft über die Reife des Sicherheitsmanagements gibt. Die Stufen können hierbei 1:1 übernommen werden:

- **Initial (Stufe 1).** Diese Stufe beschreibt den Zustand eines Unternehmens, das sich im Bereich des Managements der Informationssicherheit „um nichts kümmert“. Das Vorgehen ist chaotisch, Entscheidungen werden ad hoc auf einer intuitiven Basis getroffen. Erfolge in der Informationssicherheit beruhen allein auf dem persönlichen Engagement einzelner Mitarbeitenden.
- **Repeatable (Stufe 2).** Es gibt Vorgehensmodelle für einzelne Aufgaben im Sicherheitsmanagement (z. B. für die Durchführung von Audits), die jedoch nicht unbedingt dokumentiert sein müssen. Erfahrungswerte werden weiterverwendet.

³ Bei dem Begriff Security Capability Maturity Model handelt es sich um eine Wortschöpfung, die aus der Anpassung des CMM resultiert, und nicht um einen standardisierten Begriff.

- **Defined (Stufe 3).** Ein IS-Managementprozess und die Bausteine der Informationssicherheit (z. B. ein Notfallmanagement) sind definiert, dokumentiert (und damit unabhängig von einzelnen Personen) und werden im Unternehmen auch gelebt. Es sind Verantwortlichkeiten für die Informationssicherheit benannt.
- **Managed (Stufe 4).** In der vierten Stufe werden quantitative und qualitative Ziele für die Informationssicherheit formuliert, die Zielerreichung wird mittels geeigneter Kennzahlen gemessen und überwacht. Es existiert ein ISMS mit entsprechenden Kreisläufen (Security Circle, Kapitel 6). Durch Rückkopplungen ist die Wirksamkeit der Informationssicherheit kontrollierbar.
- **Optimizing (Stufe 5).** Es existiert ein kontinuierlicher Verbesserungsprozess, mit dessen Hilfe das ISMS weiterentwickelt und optimiert wird.

Die CMM-Stufen können auch zur Beurteilung der Sicherheitssituation bzw. der Höhe des Sicherheitsgrades genutzt werden. Sie werden dazu teilweise anders bezeichnet:

- **Initial (Stufe 1).** Sicherheit ist in dieser Stufe Zufall bzw. ergibt sich durch die so wieso vorhandenen Eigenschaften, es ist keine geplante Sicherheit vorhanden. Organisierte Sicherheitslösungen sind weder im Einsatz noch geplant.
- **Essential (Stufe 2).** Nur die nötigsten Sicherheitsvorkehrungen sind getroffen. Entweder sind dies Vorkehrungen, die selbstverständlich erscheinen (z. B. die Türen zu sensiblen Räumen sind verschlossen), oder die Notwendigkeit ist aufgrund wiederkehrender Sicherheitsvorfälle offensichtlich.
- **Advanced (Stufe 3).** In wichtigen Bereichen werden Sicherheitsmaßnahmen entsprechend dem Sicherheitsbedarf vorgesehen. Sicherheitsanforderungen sind formuliert, der Erfüllungsgrad kann bis zu 60 % erreichen, liegt jedoch meist unter 40 %.
- **Strong (Stufe 4).** Die Informationssicherheit wird flächendeckend in Angriff genommen. In allen Bereichen sind Sicherheitsmaßnahmen entsprechend dem Sicherheitsbedarf vorgesehen. Der Erfüllungsgrad der systematisch formulierten Sicherheitsanforderungen liegt zwischen 60 % und 90 %.
- **Optimized (Stufe 5).** Die optimale Sicherheit ist erreicht. In allen Bereichen wurden entsprechend dem Sicherheitsbedarf und den Vorgaben der Security Policy Sicherheitsmaßnahmen umgesetzt. Die dafür definierten Anforderungen sind zu 90 bis nahezu 100 % erfüllt. Der Schutz berücksichtigt die verschiedenen Dimensionen (Technik, Organisation, Recht), Lebenszyklusphasen usw. Für die Informationssicherheit existiert ein Managementprozess, der mindestens in Stufe 4 des SCMM einzuordnen ist.

Mit dem Erreichen der Stufe 5 ist die Arbeit nicht etwa abgeschlossen. Die Sicherheitssituation verändert sich durch neue Technologien, Architekturänderungen, Nutzungsänderungen und vieles mehr ständig, sodass es großer Anstrengungen bedarf, den hohen Reifegrad zu halten.

8.4 Reporting mit dem Netzdiagramm

Das Security Capability Maturity Model kann mit dem House of Security so kombiniert werden, dass nicht nur für das gesamte Unternehmen der Reifegrad ermittelt wird, sondern auch für einzelne Schichten. Die Ausprägungen in den einzelnen Schichten können dann mithilfe eines Netz- bzw. Spinnennetzdiagramms grafisch dargestellt werden. Dies zeigt Bild 8.15.

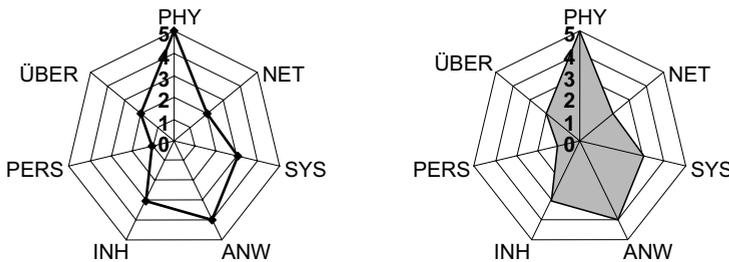


Bild 8.15 Reporting mit dem Spinnennetzdiagramm

In einem solchen Reporting ist schon rein optisch sehr schnell erkennbar, in welchen Bereichen die Informationssicherheit stark ausgeprägt ist und wo sich Schwächen zeigen. Die Bewertung erfolgt analog zu den Stufen des SCMM.

8.5 Security Landscape

Den Gedanken aus dem vorigen Abschnitt kann man fortführen, indem man den Reifegrad nicht nur für jede Schicht ermittelt, sondern auch die Dimensionen (z. B. Technik, Organisation, Recht) mit aufnimmt. Dies ergibt eine gute Übersicht über die Sicherheitssituation, für die die Bezeichnung „Security Landscape“ gewählt wurde, weil sie einer Landschaft mit Hügeln und Tälern gleicht.

Aus der Security Landscape lässt sich erkennen, wie homogen der Schutz des jeweiligen Betrachtungsgegenstands ausgestaltet ist. Sie kann damit Investitionsentscheidungen unterstützen und helfen, Fehlinvestitionen zu vermeiden. In der Landscape in Bild 8.16 konzentriert sich die Sicherheit auf den technischen Schutz der Anwendungen bzw. Applikationen. Andere Bereiche hinken weit hinterher, weshalb es vermutlich sinnvoller ist, in andere Bereiche zu investieren und nicht alles auf eine Karte zu setzen.

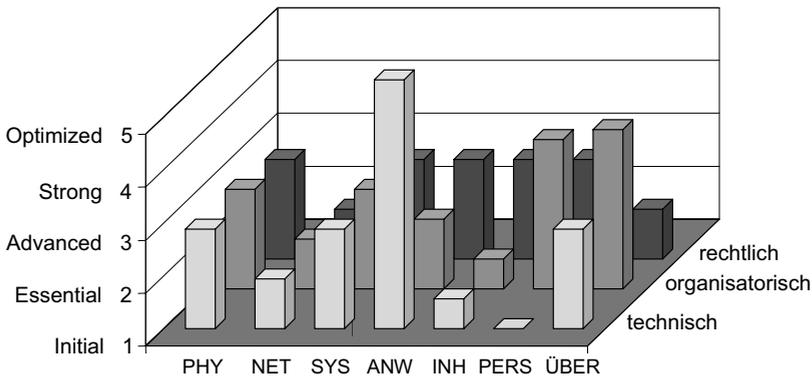


Bild 8.16 Security Landscape

Für die Y-Achse kann anstelle der Reifegradstufen auch der Sicherheitsgrad eingetragen werden. In diesem Fall lässt sich aus der Landscape das in den Schichten erreichte Sicherheitsniveau ablesen.

Wie beim House of Security kommt es auch hier auf den Betrachtungshorizont an. Die Security Landscape kann für das gesamte Unternehmen, aber auch für innere Elemente erstellt werden. So könnte es eine Landscape für einen Standort, einen Raum oder einen Server geben. Der Vorteil ist wie beim House of Security die Skalierbarkeit. Für jedes Element ist die Sicherheitssituation mit einem Blick erkennbar.

Zurückgreifend auf das in Bild 8.16 dargestellte Beispiel könnte nach Kenntnisnahme der Security Landscape die Frage auftauchen: „Warum ist die Sicherheitssituation der technischen und organisatorischen Dimension der Schicht INH so schlecht?“ In diesem Fall ist es sinnvoll, den Betrachtungshorizont auf die Schicht INH zu verlagern und zu hinterfragen, welche Umstände zu dieser Ausprägung in der Security Landscape geführt haben.

Index

A

Abhängigkeitsmatrix 100
akute Bedrohung 26, 27
Anforderungskatalog 65
Angriffsmuster 273
Angriffspfad 24 ff., 31, 34
Arbeitssicherheit 37
Architekturschichten 165
Asset 85
Ausfalltoleranz 195
Ausführungshaftung 327
Auslöser 25 ff., 31
Auswirkungen 23, 26 ff.
Authentizität 18 f.

B

Backdoor 275
Balanced Scorecard 167, 173
– betriebswirtschaftliche 174
BCM 186, 220
BCP 186, 220
BDSG 304
Bedrohung 26 ff.
Bedrohungsanalyse 125, 138
Bedrohungsfaktoren 138
Bedrohungskatalog 141
Betrachtungsebenen 165, 168

Beweissicherung 277
BIA 97
Bottom-up-Vorgehen 85 f., 112, 125, 158
BSC 173
BSI *siehe* Bundesamt für Sicherheit in der Informationstechnik
BSI-Standards 104, 107
Bundesamt für Sicherheit in der Informationstechnik 55, 61, 87, 104, 300
Bundesdatenschutzgesetz 306
Business Contingency Planning 186
Business Continuity 185
Business Continuity Management 186, 220, 234
Business Continuity Planning 186, 220
Business-Impact-Analyse 96
Business Resumption Planning 239

C

Capability Maturity Model 178
Capability Maturity Model Integration 178
Change Management 254
Chief Information Officer 123
Chief Information Security Officer 2, 123
Chief Operation Officer 123
Chinese Wall Strategie 91
CIO 123

CISO 2, 123
 Clustering 211
 CMM 178
 CMMI 178
 COBIT 321
 Cold standby 210
 Combined Code 318
 Committee of Sponsoring Organizations
 of the Treadway Commission 315
 Computerkriminalität 271
 – Ausspähung 272, 275
 – Computerbetrug 272
 – Computersabotage 273
 – Denial of Service 273
 Conduits 121
 Control 71, 86, 104, 110
 Control Objective 71, 78
 Control Objectives for Information
 Technologies 321
 COO 123
 Corporate Governance 310, 318
 Corporate Information Security Policy
 53, 69
 COSO 315
 COSO-Framework 315
 CSMS 122
 Cybersecurity 109, 111

D

DAS 201
 Data protection by default 305
 Data protection by design 305
 Datenschutz 39, 302, 331
 – Anwendbarkeit 303
 Datenschutzbeauftragte 42, 308
 Datenschutz-Grundverordnung 305 f.
 Datensicherung 189
 Datenspiegelung 192
 DCGK 313
 DCS 124
 DDG 328
 Deutscher Corporate Governance Kodex
 313

Digitale-Dienste-Gesetz 328
 digitale Signatur 17, 19
 Digital Services Act 329
 Dimensionen 167
 Direct Attached Storage 201
 Domain of trust 92
 DSB 42
 DSGVO 304 f.

E

Eintrittswahrscheinlichkeit 11, 143
 Elementargefahren 14
 ENISA 309
 ENISA Threat Landscape 309
 ePrivacy-Richtlinie 332
 Eskalation 236
 EU Cybersecurity Act 309
 EU-Richtlinie 2006/43/EG 322
 European Network and Information
 Security Agency 309
 EuroSOX 322
 Externe Partner 286
 – Haftung 291
 – Integritätsrisiken 288
 – Know-how-Risiken 287
 – Schutzrechtsrisiken 288
 – Sicherheitsanforderungen 289, 293
 – Verfügbarkeitsrisiken 287
 – Verschwiegenheitspflicht 295
 – Vertraulichkeitsrisiken 288

F

Failover 207
 Failure Mode and Effects Analysis 158
 Fallback 212
 Finanzielle Sicherheit 40
 FMEA 158
 Folgewirkungen 31
 Formale Macht 244
 Foundational requirements 121, 122
 Fragebögen 134
 Funktionsanalyse 159

G

GAU 222
 Gefahr 10 f., 19 f.
 Geliehene Macht 248
 Generischer Sicherheitsstandard 65
 GoBD 332 f.
 GoBS 332
 Grenzkrisiko 20
 Größter anzunehmender Unfall 222
 Grundschatz-Bausteine 107
 GSS 65

H

Haftung
 – arbeitsrechtlich 323
 – deliktisch 325
 – vertragsrechtlich 323
 Hauptwirkungen 30
 Heartbeat 211
 Honey Pot 275
 Hot standby 210
 Hot Swapping 194
 House of Security 165

I

IACS 120, 122
 IEC 62443 120, 123
 Incident Handling 271
 Industrielle Automatisierungs- und Steuerungssysteme 120
 Information 1 ff.
 – Komponenten 2
 – Merkmale 2
 – Wahrheitsgehalt 3
 Information Risk Managements 41
 Information Security Awareness 263
 Information Security Circle 113
 Information Security Controls 71
 Information Security Management 41
 Information Security Policy 53, 62

Informationssicherheit 1 ff., 6 ff., 35, 39, 243, 249, 263, 266, 268
 Informationssicherheitsbeauftragter 42
 Informationssicherheitsleitlinie 62
 Informationstechnik 4
 Informations- und Kommunikationsdienstegesetz 328
 Informelle Macht 248
 Integrität 17, 19
 International Society for Automation 120
 Interview 128
 Interviewleitfaden 131
 IRM 41
 ISA 120
 ISB 42
 ISM 41
 ISMS 105 f., 109
 ISO 27001 109
 ISO 27001/27002 104
 ISO 27002 110
 ISP 62
 Ist-Aufnahme 125 f., 158
 IT 2, 4 f., 7 f.
 IT-Bedrohungsanalyse 86
 IT-Benutzersupport 44
 IT-Forensik 18, 271
 IT-Grundschatz 104
 IT-Grundschatz-Kompendium 103 f.
 IT-Management 43
 IT-Outsourcing-Partner 286
 IT-Revision 18, 40, 43
 IT-Risikoanalyse 87
 ITRM 41
 ITSB 42
 IT Security Control 71
 IT Security Policy 53 f., 57
 IT-Sicherheit 2, 5, 8
 IT-Sicherheitsbeauftragter 42
 IT-Sicherheitsgesetz 300
 IT-Sicherheitsgremium 43
 IT-Sicherheitsmanagement 9, 16
 IT-Sicherheitsmanager/in 2, 88, 94, 96
 IT-Sicherheitsmaßnahmen 86

IT-Sicherheitsniveaus 86
 IT-Sicherheitspolitik 53, 94
 IT-Sicherheitsstandards 86, 103
 IT-Sicherheitsstrategien 91
 ITSM 2, 4, 88
 IuKDG 328

K

Kernprozesse 97
 Konformität 18
 KonTraG 310, 326
 Krise 223
 Krisenstab 226
 KritisV 302
 KRITIS-Verordnung 302

L

Lebenszyklusphasen 170

M

Master/Slave-Replikation 203
 MDStV 328
 Medienstaatsvertrag 328
 Multi-Master-Replikation 204

N

Nachvollziehbarkeit 18
 NAS 201
 Nebenwirkungen 30
 Network Attached Storage 201
 Network Time Protokoll 205
 NIS-Richtlinie 309
 Notbetrieb 220, 231, 238
 Notfall 215, 221, 223
 – akuter 230
 Notfallbeherrschung 234
 Notfallbewältigung 216, 218 f., 225 f.
 – Dokumentation 229
 Notfallende 241
 Notfallentscheidung 228

Notfallhandbuch 220, 224
 Notfallkonzept 218 f., 224, 229
 Notfallmanagement 215, 223, 230
 Notfallorganisation 219, 226, 229
 Notfallplanung 217, 233, 236
 Notfallprävention 216
 Notfall-Recovery 239
 Notfallübung 219, 241
 Notfallvorsorge 216
 NTP 205

O

Objective 78
 Operational Technology 106, 118
 Organisationsmodelle 44
 OT 106, 118
 Outsourcing 211
 – Datenschutz 297

P

Panikeffekt 14
 Paritätsverfahren 197
 – Parity Bit 198
 Patentschutz 40
 PDCA 112
 Persönliches Netzwerk 252
 Physische Sicherheit 36
 PKI 330
 Plan-Do-Check-Act-Kreislauf 112
 Policies
 – objektorientierte 70
 – verkettete 70
 Policy-Hierarchie 61
 Policy Management 82
 POM 69
 Potenzielle Bedrohung 26
 Primärrisiken 30
 Product-based Operating Manuals 69
 Produktionssicherheit 38
 Produktsicherheit 38
 Produktspezifischer Sicherheitsstandard 69

Prozessbasierte Sicherheit 92
 PSS 69
 Public Key Infrastructure 330

R

RAID 194
 Ransomware 271
 Reaktionsmuster 257
 Recovery 231, 234, 238 f.
 – Zeitdauer 240
 Redundant Array of Independent
 Disks
 – Aufteilung 195
 – Ausfalltoleranz 195
 – Stripeseit 197
 – Striping 195
 Redundanz 208
 Replikation 203
 Reporting 163
 Restrisiko 155
 Revision 40
 Risiko 9, 11
 Risikoakzeptanz 13 f.
 Risikoanalyse 125, 217
 – projektbegleitende 160
 Risikoaspekte 10
 Risikobehandlung 125, 154
 Risikoberechnung 13
 Risikobewertung 125, 142
 Risikoeinschätzung 14
 Risikoformel 11, 125, 142
 – Probleme 148
 Risikokorridor 151
 Risikomanagement 8
 Risikomatrix 149
 Risikopriorisierung 153
 Risikoprofil 150
 Risikosituation 14, 149
 Risikoszenarien 125, 142
 Risikoszenario 28 f.
 Risikoverdrängung 14
 Risikowahrnehmung 13 f.
 Risk Reporting 173

Risk Scorecard 176
 Round Robin 196

S

Safety 119
 SAN 202
 Sarbanes-Oxley Act 319
 SarbOx 319
 SAS 201
 SCADA 124
 Schadensereignis 11, 25, 27
 Schadenshöhe 146
 Schadenskategorien 102, 147
 Schadensklassen 102
 Schadensszenarien 31
 Schutzbedarf 21
 Schutzbedarfsanalyse 99 f., 102
 – informationsorientiert 102
 – technikorientiert 101
 Schutzbedarfsfeststellung 108
 Schutzklassen 20
 Schutzkonzepte 156
 Schutzziel 20
 Schwachstelle 23 ff., 31 ff.
 Schwachstellenanalyse 24, 125, 136
 Security 109, 120, 123
 Security by Ownership 93
 Security Capability Maturity Model 178,
 180
 Security Landscape 182
 Security Level 121 f.
 Security Policy 54, 57, 86, 121
 Security-Policy-Modell 62
 Security Scorecard 176
 Security Service Level Agreements 293
 Sekundärrisiken 30
 Server Attached Storage 201
 Sicherheit 9, 15
 – funktionale 119
 – protektive 120
 Sicherheitsanforderungen 86, 103
 Sicherheitsbereiche 7, 35
 Sicherheitsgrad 7, 19, 21

Sicherheitsklassen 20
 Sicherheitskriterien 15
 Sicherheitsorganisation 35, 117
 – Gestaltung 50
 sicherheitsrelevantes Ereignis 27, 28 f.,
 32 f.
 Sicherheitssituation 9
 Sicherheitsstufen 20
 Sicherheitsvorgabe 20
 SIEM 301
 SigG 328, 330
 Signaturgesetz 328, 330
 SMART-Ansatz 89
 SOA 319
 SOC 301
 Social Engineering 24
 Sofortmaßnahmen 231
 SOX 315, 319
 SSLA 293
 Standing 249
 Storage Area Network 202
 Störfall 221
 Strukturanalyse 108
 Supportprozesse 97

T

TDDSG 328, 331
 TDG 328
 TDSV 332
 Technische Sicherheit 37
 Teledienstedatenschutzgesetz 328, 331
 Teledienstegesetz 328
 Telekommunikations-Datenschutz-
 verordnung 332
 Telekommunikationsgesetz 300, 328,
 330
 Telekommunikations-Telemedien-Daten-
 schutzgesetz 332
 Telemediengesetz 300, 328, 331
 TKG 328, 330
 TMG 328
 Top-down-Vorgehen 85, 112
 TTDSG 332

U

Übernahmehaftung 326
 UK Corporate Governance Code 318
 Umsetzungsplan zum Schutz kritischer
 Infrastrukturen 300
 Umweltschutz 39
 UP KRITIS 300
 User Security Standard 268, 281

V

VDG 330
 Veränderungsmotivation 262
 Veränderungsprozess 259
 Verbindlichkeit 19
 Verfügbarkeit 16
 Verhinderungsstrategie 256
 verliehene Macht 244
 Vertrauensdienstegesetz 330
 Vertraulichkeit 17 f.
 Vertraulichkeitserklärung 294
 Verwundbarkeit 24

W

Watchdog 211
 Widerstand
 – offen 254
 – Umgang 261
 – verdeckt 255
 Wiederherstellung 231, 238 ff.
 Wirkungskette 28, 31
 Wirkungsstränge 29 f.
 Wissensmanagement 4

Z

Zertifizierung 18
 Zielformulierung 89
 Zielhierarchie 88
 Zielkategorien 89
 Zielplanung 88