



Thomas W.
Harich

3. Auflage



IT-Sicherheitsmanagement

Das umfassende Praxis-Handbuch

für IT-Security und technischen Datenschutz nach ISO 27001

- **Aufgaben des IT-Security-Managers**
- **Informationssicherheit ausarbeiten**
- **IT-Sicherheitskonzepte einrichten**
- **Information Security Management System aufbauen**

Hinweis des Verlages zum Urheberrecht und Digitalen Rechtemanagement (DRM)

Liebe Leserinnen und Leser,

dieses E-Book, einschließlich aller seiner Teile, ist urheberrechtlich geschützt. Mit dem Kauf räumen wir Ihnen das Recht ein, die Inhalte im Rahmen des geltenden Urheberrechts zu nutzen. Jede Verwertung außerhalb dieser Grenzen ist ohne unsere Zustimmung unzulässig und strafbar. Das gilt besonders für Vervielfältigungen, Übersetzungen sowie Einspeicherung und Verarbeitung in elektronischen Systemen.

Je nachdem wo Sie Ihr E-Book gekauft haben, kann dieser Shop das E-Book vor Missbrauch durch ein digitales Rechtemanagement schützen. Häufig erfolgt dies in Form eines nicht sichtbaren digitalen Wasserzeichens, das dann individuell pro Nutzer signiert ist. Angaben zu diesem DRM finden Sie auf den Seiten der jeweiligen Anbieter.

Beim Kauf des E-Books in unserem Verlagsshop ist Ihr E-Book DRM-frei.

Viele Grüße und viel Spaß beim Lesen,

Ihr mitp-Verlagsteam



Neuerscheinungen, Praxistipps, Gratiskapitel,
Einblicke in den Verlagsalltag –
gibt es alles bei uns auf Instagram und Facebook



[instagram.com/mitp_verlag](https://www.instagram.com/mitp_verlag)



[facebook.com/mitp.verlag](https://www.facebook.com/mitp.verlag)

Thomas W. Harich

IT-Sicherheitsmanagement

Das umfassende Praxis-Handbuch

für IT-Security und technischen Datenschutz nach ISO 27001

3. Auflage

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.

ISBN 978-3-7475-0147-4

3. Auflage 2021

www.mitp.de

E-Mail: mitp-verlag@sigloch.de

Telefon: +49 7953 / 7189 - 079

Telefax: +49 7953 / 7189 - 082

© 2021 mitp Verlags GmbH & Co. KG, Frechen

Dieses Werk, einschließlich aller seiner Teile, ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Dies 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.

Lektorat: Katja Vöpel

Korrekturat: Petra Heubach-Erdmann

Covergestaltung: Christian Kalkert, Sandrina Dralle

Coverbild: [nightstranger1/stock.adobe.com](https://www.adobe.com/stock/nightstranger1)

Satz: III-satz, Husby, www.drei-satz.de



Inhaltsverzeichnis

	Einleitung	15
1	Umfang und Aufgabe des IT-Security-Managements	21
1.1	Kapitelzusammenfassung	21
1.2	Einführung	21
1.3	Informationen und Daten	22
1.4	IT-Security-Management ist wichtig	24
1.5	Wie gefährdet sind die Unternehmensdaten	26
1.5.1	Sicht des Verfassungsschutzes	27
1.5.2	Öffentliche Wahrnehmung	27
1.5.3	Die eigene Wahrnehmung	29
1.6	Begrifflichkeiten	30
1.7	Selbstverständnis der IT-Security-Organisation	32
1.8	Grundregeln	35
1.9	Umfang des IT-Security-Managements	38
1.9.1	Pfeiler der IT-Security	39
1.9.2	Aufgaben des IT-Security-Managements	44
1.10	IT-Security zwischen Nutzen und Kosten	47
2	Organisation der IT-Security	49
2.1	Kapitelzusammenfassung	49
2.2	Einführung	49
2.3	Rollen innerhalb des IT-Security-Managements	50
2.3.1	Manager IT-Security	50
2.3.2	Unternehmensleitung	56
2.3.3	Weitere Rollen	56

2.4	Verankerung im Unternehmen	58
2.4.1	IT-Security im Organigramm	58
2.4.2	IT-Security und der Datenschutz	65
2.4.3	Zusammenspiel mit anderen Sicherheitsbereichen	66
3	IT-Compliance	71
3.1	Kapitelzusammenfassung	71
3.2	Einführung	73
3.3	Standards	78
3.3.1	ISO-2700x-Reihe	79
3.3.2	Standards des Bundesamts für Sicherheit in der Informationstechnik	85
3.3.3	Gegenüberstellung ISO 2700x und BSI-Grundschutz	89
3.3.4	ITIL	92
3.3.5	Weitere Standards	93
3.4	Gesetze	94
3.4.1	EU-Datenschutz-Grundverordnung	95
3.4.2	IT-Sicherheitsgesetz	99
3.4.3	Weitere Gesetze	99
3.4.4	Branchenstandards am Beispiel TISAX	101
3.4.5	ISO 27001 und TISAX	104
3.4.6	Vorbereitende Maßnahmen	106
3.4.7	Fragenkatalog	109
4	Organisation von Richtlinien	127
4.1	Kapitelzusammenfassung	127
4.2	Einführung	128
4.3	Strukturierung von Richtlinien	129
4.4	Beschreibung und Kategorisierung	130
4.5	Pflege und Lenkung von Richtlinien	131
4.6	Richtlinien und Audits	133

4.7	Verschiedene Richtlinien	135
4.7.1	Sicherheitsrichtlinie	136
4.7.2	Klassifizierungsrichtlinie	141
4.7.3	ISMS-Handbuch	144
4.7.4	Richtlinie zum IT-Risikomanagement	146
4.7.5	IT-Sicherheitsrichtlinie	148
4.7.6	IT-Systemrichtlinien	152
4.8	Von der Theorie in die Praxis	153
5	Betrieb der IT-Security	155
5.1	Kapitelzusammenfassung	155
5.2	Einführung	155
5.3	IT-Security und der IT-Betrieb	157
5.4	Betriebliche Grundsätze	158
5.4.1	Ableitung aus gesetzlichen Vorschriften	158
5.4.2	Vertragswesen	159
5.4.3	Administrative Tätigkeiten	159
5.4.4	Trennung von Funktionen	160
5.4.5	Prinzip der geringsten Rechte	161
5.5	IT-Security-Prozesse	162
5.5.1	Zugangs- und Zugriffskontrolle	162
5.5.2	Sicherheit von Software	169
5.5.3	Sichere Softwareentwicklung	174
5.5.4	Identitätsmanagement	176
5.5.5	Genehmigungsprozesse	181
5.5.6	Standardisierung	182
5.5.7	Unterstützung des IT-Betriebs	183
6	IT Business Continuity Management	185
6.1	Kapitelzusammenfassung	185
6.2	Einführung	186
6.3	Abgrenzung der Begriffe	190

6.4	IT-Notfallmanagement und Verfügbarkeitsmanagement	192
6.5	Gesetzliche Rahmenbedingungen des IT Business Continuity Managements	193
6.6	Business-Impact-Analyse	193
6.6.1	Erfassung und Priorisierung der Geschäftsprozesse	194
6.6.2	Business-Impact-Analyse in der Praxis	200
6.7	Weitere Einflussfaktoren	201
7	IT-Notfallmanagement	203
7.1	Kapitelzusammenfassung	203
7.2	Einführung	203
7.3	IT-Notfallmanagement	204
7.4	Richtlinie zum IT-Notfallmanagement	205
7.5	Ableitung von Notfallstrategien	206
7.6	IT-Notfallkonzepte erstellen	207
7.6.1	Schweregrade	209
7.6.2	Notfallvorsorge	211
7.7	Notfallorganisation	217
7.7.1	Organisationsstruktur	217
7.7.2	Kompetenzen und Zuständigkeiten	218
7.7.3	Notfallhandbuch	219
7.8	Notfallbewältigung	221
7.9	Notfallübungen	225
7.10	Überprüfung des IT-Notfallmanagements	226
7.11	Monitoring im Rahmen des IT Business Continuity Managements	227
7.12	Checklisten IT-Notfallmanagement	228
7.12.1	Checkliste Business-Impact-Analyse	228
7.12.2	Checkliste Notfallorganisation	229
7.12.3	Checkliste Notfallpläne und Wiederanlaufpläne	230
7.12.4	Checkliste Rechenzentrum	230

8	Verfügbarkeitsmanagement	233
8.1	Kapitelzusammenfassung	233
8.2	Einführung	233
8.3	Richtlinie zum Verfügbarkeitsmanagement	234
8.4	Verfügbarkeit	235
8.4.1	Klassifizierung von Verfügbarkeit	236
8.4.2	Vorgehensweise	238
8.4.3	Berechnung der Verfügbarkeit	239
8.5	Ausfallsicherheit	240
8.6	Ausprägungen von Redundanz	241
8.6.1	Strukturelle Redundanz	242
8.6.2	Funktionelle Redundanz oder unterstützende Redundanz	243
8.6.3	Informationsredundanz	243
8.7	Redundante Hard- und Software	243
8.8	Virtualisierung	245
8.9	Bauliche Maßnahmen zur Steigerung der Verfügbarkeit	246
9	Technische IT-Security	249
9.1	Kapitelzusammenfassung	249
9.2	Einführung	250
9.3	Technisch-Organisatorische Maßnahmen	252
9.3.1	Zugangskontrolle	254
9.3.2	Zugriffskontrolle	259
9.3.3	Übertragungskontrolle und Transportkontrolle	261
9.3.4	Eingabekontrolle	265
9.3.5	Verfügbarkeitskontrolle, Wiederherstellbarkeit und Zuverlässigkeit	266
9.3.6	Datenintegrität	267
9.4	Verschlüsselung	268
9.4.1	Begriffsbestimmungen	269
9.4.2	Symmetrische Verschlüsselungssysteme	270
9.4.3	Asymmetrische Verschlüsselungsverfahren	271

9.5	Cloud Computing	272
9.5.1	Dienstleistungen in der Cloud	276
9.5.2	Risikofaktoren	278
9.5.3	Datenschutzrechtliche Aspekte	285
9.5.4	Vertragliche Vereinbarungen	287
9.5.5	Sinnvolle Freigabeprozesse	288
9.6	Betrieb von Firewalls	290
9.6.1	Paketfilter und Application-Gateways	292
9.6.2	Firewall-Regelwerk	295
9.6.3	Internet-Proxyserver	297
9.7	Internetzugang und Nutzung von E-Mail	298
9.7.1	Risikofaktor E-Mail	299
9.7.2	Verschlüsselung von E-Mails	300
9.7.3	Risikofaktor Internetbrowser	301
9.8	Penetrationstests	302
9.9	Digitale Signatur	304
9.10	Intrusion-Detection-Systeme	306
9.11	Wireless LAN	308
10	IT-Risikomanagement	311
10.1	Kapitelzusammenfassung	311
10.2	Einführung	312
10.3	IT-Risikomanagement im Unternehmenskontext	312
10.4	Akzeptanz des IT-Risikomanagements	314
10.5	Operatives IT-Risikomanagement	315
10.5.1	Vorgehensweise	318
10.5.2	IT-Risikomanagementprozess	320
10.5.3	Übergeordnete Risikobetrachtung	322
10.5.4	Schwachstellen	325
10.5.5	Bedrohungen	328
10.5.6	Zusammenspiel von Bedrohungen, Schwachstellen und Maßnahmen	330
10.5.7	Verhältnismäßigkeit	332

10.6	Schutzbedarfsfeststellung	333
10.6.1	Schutzziele	333
10.6.2	Schutzstufen	336
10.6.3	Prinzipien	337
10.6.4	Feststellung des Schutzbedarfs	338
10.6.5	Veränderung des Schutzbedarfs	343
10.6.6	Widersprüchliche Schutzziele	344
10.6.7	Schadensklassen	344
10.6.8	Abbildung des Datenflusses	345
10.6.9	Entscheidungsfindung auf Basis des Schutzbedarfs	346
10.7	IT-Risikomanagement Prozess	348
10.7.1	Risiken identifizieren	348
10.7.2	Risikoermittlung	353
10.7.3	Risikobewertung	356
10.8	Quantitative Darstellung von Risiken	359
10.8.1	Grundlagen der Risikoberechnung	360
10.8.2	Risikoberechnung im Beispiel	362
10.8.3	Risikomatrix	364
10.8.4	Risikokatalog	366
10.9	Risikobehandlung	368
10.9.1	Risiko akzeptieren	370
10.9.2	Risiko reduzieren	371
10.9.3	Risiko vermeiden	372
10.9.4	Risiko auf Dritte verlagern	372
10.10	Maßnahmen definieren	373
10.10.1	Maßnahmentypen	374
10.10.2	Individuelle Maßnahmenkataloge	375
11	Sicherheitsmonitoring	377
11.1	Kapitelzusammenfassung	377
11.2	Einführung	378
11.3	Ebenen des Monitorings	380

11.4	System-Monitoring	382
11.4.1	Sicherheitsaspekte	383
11.4.2	Auswahl zu überwachender Systeme	383
11.4.3	Implementierung im Netzwerk	384
11.5	Protokoll-Monitoring	385
11.5.1	Unterstützung von Audits	386
11.5.2	Überwachung administrativer Tätigkeiten	387
11.5.3	Schwachstellenmanagement	388
12	IT-Security-Audit	391
12.1	Kapitelzusammenfassung	391
12.2	Einführung	392
12.3	Audits im Kontext des IT-Security-Managements	392
12.4	Audits im Unternehmenskontext	396
12.5	Audits nach Kategorien	397
12.6	Vor-Ort kontra Selbstauskunft	399
12.7	Anforderungen an den Auditor	400
12.8	Ein Audit Schritt für Schritt	402
12.8.1	Vorbereitung	403
12.8.2	Durchführung	404
12.8.3	Nachbereitung	408
12.8.4	Abschlussbericht	408
13	Management von Sicherheitsereignissen und IT-Forensik	413
13.1	Kapitelzusammenfassung	413
13.2	Einführung	414
13.3	Angriffe auf Ihre Daten	415
13.3.1	Durch eigene Mitarbeiter	416
13.3.2	Durch Außenstehende	418
13.3.3	Angriffe und Angriffsvektoren	418
13.3.4	Angriffsarten	419
13.4	Management von Sicherheitsereignissen	424

13.5	IT-Forensik	426
13.5.1	Arten der IT-Forensik-Analyse	431
13.5.2	Einrichtung von Honeypots	432
13.6	Elemente der forensischen Untersuchung	433
13.6.1	Zielsetzung	434
13.6.2	Anforderungen an die Analyse	435
13.6.3	Forensische Methoden	436
13.6.4	Forensische Untersuchung	437
14	Kennzahlen	443
14.1	Kapitelzusammenfassung	443
14.2	Einführung	444
14.3	Die Aufgabe von Kennzahlen	444
14.4	Quantifizierbare Kennzahlen	447
14.5	Steuerung mithilfe von Kennzahlen	449
14.6	Qualität von Kennzahlen	451
14.6.1	Gute Kennzahlen	451
14.6.2	Schlechte Kennzahlen	452
14.6.3	Vergleichbarkeit von Kennzahlen	452
14.7	Verschiedene Kennzahlen aus der IT-Security	453
14.8	Kennzahlen im laufenden Verbesserungsprozess	458
14.9	Laufende Auswertung von Kennzahlen	460
14.10	Annualized Loss Expectancy	460
14.11	IT-Security Balanced Scorecard	463
14.11.1	Einführung der IT-Security Balanced Scorecard	465
14.11.2	Maßnahmenziele für den Bereich IT-Security	469
15	Praxis: Aufbau eines ISMS	473
15.1	Kapitelzusammenfassung	473
15.2	Einführung	474
15.3	ISMS in Kürze	474

15.4	Herangehensweise	477
15.5	Schritt für Schritt zum ISMS	478
15.5.1	Plan-Do-Check-Act	482
15.5.2	Vorarbeiten	483
15.5.3	Plan: Gestaltung des ISMS	488
15.5.4	Do: Umsetzung der Arbeitspakete	503
15.5.5	Check: Überprüfung des ISMS	505
15.5.6	Act: Umsetzung von erkannten Defiziten	506
15.5.7	Dokumentation	506
15.6	Softwaregestützter Aufbau eines ISMS	511
15.6.1	Auswahl einer ISMS-Lösung	512
15.6.2	Darstellung der Risiken und der Unternehmenswerte	514
15.6.3	Darstellung von Prozessen	517
15.6.4	IT-Risikomanagement	518
15.6.5	Richtlinienmanagement	520
15.6.6	Arbeitsabläufe abbilden	521
15.6.7	Berichte erstellen	522
15.7	Zertifizierung nach ISO 27001	523
15.7.1	Ansprechpartner	525
15.7.2	Prinzipien	526
16	Awareness und Schulung	529
16.1	Kapitelzusammenfassung	529
16.2	Verbesserungsprozess	530
16.3	Voraussetzungen für eine Sicherheitskultur	531
16.4	Erfassung der Sicherheitskultur	533
16.5	Top-down-Ansatz	534
16.6	Awareness-Projekte	535
	Index	539

Einleitung

Anmerkung zur dritten Auflage

Die grundlegenden Bestandteile eines IT-Sicherheitsmanagements ändern sich nicht in ähnlich kurzen Zeiträumen, wie sich die technische Seite der IT und der IT-Security ändert. Die Schwerpunkte, die fachliche Ausgestaltung und die Prozesse bleiben davon aber nicht unbeeindruckt. Werden Daten vermehrt in Public Clouds verarbeitet, auf Mobiltelefonen gespeichert, über Chat-Apps geteilt oder im Rahmen von Industrie 4.0 in einer Größenordnung erhoben, die bislang kaum denkbar war, dann müssen sich die entsprechenden Maßnahmen der IT-Security an diese Veränderungen anpassen. Der Gesetzgeber hat parallel dazu die Aufgabe, Regelungen zu erlassen, um frühzeitig die Rahmenbedingungen festzulegen und dabei zu helfen, dem Missbrauch entgegenzuwirken. In diesem Zusammenhang werden weltweit neue Gesetze erlassen und entsprechende Kontrollgremien eingesetzt. Völlig unterschiedlich gelagerte Beispiele dafür sind die EU-Datenschutz-Grundverordnung (EU-DSGVO), das IT-Sicherheitsgesetz oder das China Cybersecurity Law. Alle diese Regelungen haben immense Auswirkungen darauf, wie Unternehmen Daten erfassen, verarbeiten, speichern oder austauschen dürfen. In der Fülle und der Bandbreite der neuen Regelungen liegt aber immer auch die immanente Gefahr, etwas falsch zu machen, weil man eben den falschen Weg gewählt hat, mit diesen Anforderungen umzugehen. Der Weg aus dieser Problematik ist es, einem Lösungsansatz zu folgen, der zum einen international bekannt und anerkannt ist und zum anderen auf einem stringenten Prozess-Modell basiert, das so angelegt ist, dass alle oben genannten Punkte abgedeckt werden können. Dieser Weg ist die Einführung eines IT-Sicherheitsmanagements auf Basis der ISO-27000-Normen-Familie unter Beachtung der datenschutzrechtlichen Bestimmungen der EU-DSGVO.

Auch wenn sich seit der 2. Auflage einiges auf dem Sektor der Informationssicherheit getan hat, so hat sich dennoch gezeigt, dass die Leitplanken, die durch die beherrschenden Normen der ISO-2700x-Reihe gelegt wurden, Bestand hatten und auch weiterhin Bestand haben werden. So richten sich an

den Prozessmodellen dieser Normen in der Zwischenzeit nationale Gesetze genauso aus wie auch die Anforderungen von Unternehmen und dem öffentlichen Sektor. Diese Standardisierung und das damit einhergehende Ziehen am gleichen Seil ist auch bitter nötig. Die Zahl der täglich gemessenen gezielten Cyber-Angriffe steigt unaufhörlich weiter, während parallel deren Qualität im Durchschnitt immer weiter zunimmt.

Mit der Covid-19-Krise ändern sich die Angriffsvektoren und passen sich neuen Arbeitsprozessen an. Insbesondere Unternehmen, die kein umfassendes Sicherheitskonzept etabliert haben, bekommen dies zu spüren. Mitarbeiter arbeiten im weitgehend ungesicherten häuslichen Umfeld, Budgets werden eingefroren und personell ausgedünnte IT-Abteilungen werden der Masse an Makro- und Ransomware-Angriffen nicht mehr Herr. Jede Fehlkonfiguration an einem Server oder einer Sicherheitssoftware kann in einem solchen Umfeld schnell den Cyber-Supergau bedeuten. Für Unternehmen, die gleichzeitig in einem angespannten wirtschaftlichen Umfeld agieren, kann dies schnell auch das Aus bedeuten.

Niemals zuvor ist die Verflechtung von Lieferketten so offensichtlich zutage getreten wie nach den Lockdowns verschiedener Länder oder Regionen. Dies gilt auch für Datenflüsse zwischen Lieferanten und Herstellern und damit verwundert es nicht, dass die großen Branchenverbände längst damit begonnen haben, nicht nur diejenigen Daten sicher zu verarbeiten, die sie im eigenen Zugriff haben, sondern auch Lieferanten anzuhalten, Sicherheitsstandards einzuhalten. Aus diesem Grund habe ich ein Kapitel zu dem viel beachteten Branchenstandard der deutschen Automobilindustrie, der unter der Abkürzung »TISAX« bekannt ist, im Kapitel »Compliance« hinzugefügt. Sehr ähnliche Standards entstehen in vielen Branchen und letzten Endes werden sie sich aufgrund der gleichen Wurzeln auch nicht wesentlich voneinander unterscheiden.

Neben dem eben erwähnten neu hinzugefügten Sicherheitsfeld wurden in der vorliegenden Auflage viele Kapitel aktualisiert.

Ich möchte all denjenigen danken, die mir Input bezüglich neuer Gesichtspunkte gegeben haben. Dies schließt sowohl die wohlmeinende Kritik an einzelnen Punkten durch Leser als auch das Feedback meiner Studierenden und der Professoren an der Hochschule oder von Kollegen im Unternehmen mit ein. Auch wenn man sich selbst als Generalisten im IT-Sicherheitsbereich

sieht, ist man nicht ganz vom Tunneldenken befreit und übersieht doch das eine oder andere Mal neue Aspekte und neue Denkansätze – obwohl sie doch so offensichtlich vor einem liegen.

Über die Zielgruppe

Nicht alle Wege, aber zumindest sehr viele, führen nach Rom, und wohl ebenso viele Wege führen zum Job des IT-Security-Managers. Einige Kandidaten haben schon ein paar Jahre Berufserfahrung in ähnlichen Bereichen gesammelt, haben bereits einschlägige Erfahrungen gemacht oder kommen direkt aus dem Studium, in dem sie das Thema, zumindest theoretisch, schon behandelt haben.

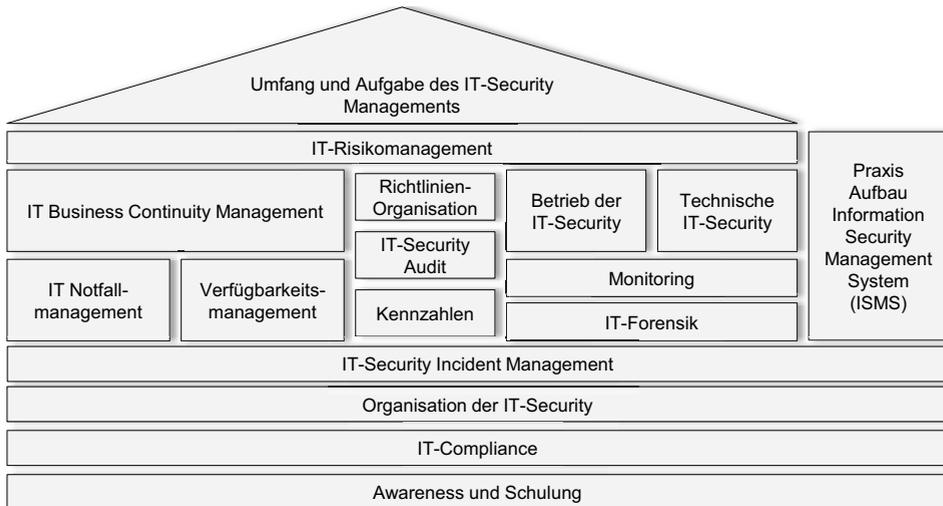
Andere, und damit sind wir wieder bei den vielen Wegen angekommen, die zum Ziel führen, sind Neueinsteiger oder Quereinsteiger. Vielleicht kommen sie aus der IT-Abteilung und haben zuvor Server administriert oder Softwareprojekte geleitet. In manchen Fällen waren sie davor aber auch im Controlling oder in der Unternehmensplanung tätig und haben sich mit Qualitätsaudits oder Risikomanagement beschäftigt. Diese Kollegen stehen dann häufig vor der Herausforderung, dass sie, selbst wenn sie angekommen sind (nicht in Rom selbstverständlich, sondern am Arbeitsplatz des IT-Security-Managers), die schiere Menge an Einzelthemen dann fast erschlägt.

Beiden Gruppen kann man aufrichtig versichern, dass es kaum eine Aufgabe gibt, die vielschichtiger und vielseitiger gestaltbar ist, als diese. Gerade der Umfang schafft die Chance, dem Arbeitsplatz den eigenen Stempel aufzudrücken, und wenn man die Grundlagen einmal verstanden hat, fällt es schwer, sich eine spannendere Aufgabe vorzustellen. Das Gebiet der IT-Security ist nicht so alt, als dass es bereits fest ausgetretene Pfade gäbe. Vielmehr gehen die Meinungen, was denn ein IT-Security-Manager zu tun hat, weit auseinander. Damit muss sich die IT-Security-Organisation dem Unternehmen flexibel anpassen. Stetige Veränderungen, hinzukommende Verknüpfungen mit anderen Abteilungen und die laufende Kommunikation mit denen, die Daten verarbeiten, und denen, die sie verwalten, bringen einerseits Abwechslung und andererseits den Druck, laufend hinzuzulernen.

Für alle, die frisch einsteigen, schon Erfahrungen haben oder gar aus einem ganz anderen Fachgebiet heraus quereinsteigen und nun auf einfache, aber

doch umfassende Art in die Thematik IT-Security eingeführt werden wollen, ist das vorliegende Buch gedacht.

Aufbau des Buches



Für eine strukturierte Vorgehensweise beim Durcharbeiten des Buches ist es sinnvoll, mit dem ersten Kapitel »Umfang und Aufgabe des IT-Security-Managements« zu beginnen. Im Grunde umreißt es das Aufgabengebiet und bringt die verschiedenen Themen in einen Zusammenhang. Ein guter Einstieg, um danach zielgerichtet diejenigen Kapitel zu betrachten, die einem selbst am interessantesten erscheinen. Aus diesem Grund sind alle Kapitel so verfasst, dass ein direkter Einstieg erleichtert wird.

Ansonsten gilt: Für ein durchgängiges Verständnis und als eine Art roter Faden ist es empfehlenswert, sich erst um Fundament und Dach zu kümmern, bevor die verschiedenen Säulen abgearbeitet werden.

Jedes Kapitel beschreibt einen zusammenhängenden Themenbereich der IT-Security. Der Aufbau bleibt dabei immer ähnlich. Obligatorische Theorie wechselt sich ab mit Tipps aus der Praxis für die Praxis, ein paar Beispielen und dazu Aufzählungen und Checklisten als Hilfestellung. Die einzelnen Themen umfassen dabei das notwendige Wissen, um den Arbeitsplatz IT-Security ausfüllen zu können, und häufig noch etwas mehr.

Die Aufgaben eines IT-Security-Managers sind vielfältig und abwechslungsreich, bauen aber immer wieder aufeinander auf. Es gibt Themen wie das IT-Risikomanagement, die in den verschiedensten Fragestellungen immer wieder auftauchen. So ist das Wissen notwendig, wie eine Risikobewertung durchgeführt wird, wenn es darum geht, Prioritäten in der Notfallvorsorge zu treffen, aber genauso auch im alltäglichen Betrieb, wenn es um die Berechtigungsvergabe oder die Entscheidung für und wider einer einzukaufenden Software geht. Aus diesem Grund wird dieses Aufgabenfeld als Teil der Dachkonstruktion in der Abbildung abgebildet.

Die weiteren Elemente des Hauses stellen die anderen Kapitel des Buches dar. Manche Themen bilden das Fundament für den gesamten Komplex, wieder andere bilden zusammen mit einem oder zwei Bereichen eine Einheit. So sind die Kapitel zum IT-Notfallmanagement und zum Verfügbarkeitsmanagement zwei Teile des übergeordneten Themas IT Business Continuity Management.

Die Wahl, die IT-Security-Organisation, die IT-Compliance, das IT-Security Incident Management und die Bildung von Awareness als Fundament zu nutzen, fiel aufgrund der Tatsache, dass es nicht möglich ist, sie immer und immer wieder mitzubetrachten. Gleichgültig, welche Maßnahme implementiert oder welche Richtlinie durchgesetzt werden soll, immer stellt sich die Frage, wie diese zu kommunizieren und zu schulen ist, wie die inneren und äußeren Anforderungen aussehen und wie die IT-Security-Organisation aufgebaut sein muss, um dies auch bewältigen zu können.

Ein Kapitel sticht etwas hervor. Das reine Praxiskapitel über die Einführung eines Information Security Management Systems (ISMS) steht etwas abseits am rechten Rand des Hauses. Diese Zuordnung soll vergegenwärtigen, dass alle im Buch behandelten Themen in irgendeiner Art und Weise Teil des ISMS sind. Die Zusammenführung und die Annäherung an die Praxis werden an dieser Stelle vertieft angegangen.

1 Umfang und Aufgabe des IT-Security-Managements

1.1 Kapitelzusammenfassung

Im Rahmen des ersten Kapitels werden die einzelnen Themengebiete des IT-Security-Managements in einen Gesamtzusammenhang eingebettet. Es wird erläutert, warum man Informationen schützen muss und wie diese Aufgabe durch die IT-Security-Organisation wahrgenommen wird.

Die Top-5-Fragen zum aktuellen Kapitel:

- Sind die Aufgabengebiete definiert, die dem IT-Security-Management zugeordnet werden?
- Sind die organisatorischen Einheiten, die sich um die Betreuung von sicherheitsrelevanten Systemen kümmern, darüber informiert und dahin gehend instruiert, dass sie sich im Einflussbereich des IT-Security-Managements befinden?
- Wurden Schutzziele zusammen mit der Unternehmensleitung definiert?
- Werden die Grundregeln (Prinzipien) im Umgang mit Informationen kommuniziert und in der Praxis umgesetzt?
- Werden die Grundpfeiler der IT-Security, das IT-Risikomanagement, die IT-Compliance und die IT-Governance auch in Verbindung mit dem IT-Security-Management gebracht und damit auch als Aufgabe des Managers IT-Security gesehen?

1.2 Einführung

Ransomware, Industrie 4.0, die EU-Datenschutz-Grundverordnung, Mobility, Heimarbeitsplätze, Public-Cloud-Services und viele andere Themen haben in letzter Zeit die Schlagzeilen beherrscht. Angesichts der Wucht dieser Themen und den häufig noch fehlenden, umfassenden Sicherheitsarchitekturen, die man benötigt, um diese zu beherrschen, geht immer häufiger das Gefühl

dafür verloren, wie diese Sicherheits-Felder miteinander verwoben sind, und vor allem auch, wie diese mit den klassischen Sicherheitsanforderungen wie dem Assetmanagement oder auch einem Antivirenkonzept verknüpft werden müssen. Altes Wissen trifft dabei auf völlig neue Bedrohungen. In dieser Gemengelage ist es die Aufgabe des Managers IT-Security, den Überblick zu bewahren und auf die wichtigen Bedrohungen mit den erforderlichen Maßnahmen in angemessener Weise zu reagieren. Im Sprachgebrauch dieses Buches unterscheidet er sich damit von einem IT-Security-Experten, der Fachmann für ein dediziertes Feld der IT-Security ist und sich vorwiegend auch nur innerhalb dieses Arbeitsgebiets bewegt.

Der Manager IT-Security sieht sich in der Situation, das Know-how des Unternehmens zu schützen, indem er Bedrohungen erkennt, abschätzt und diesen dann geeignete Sicherheitskonzepte und Maßnahmen entgegensetzt. Zu diesem Zweck bedient er sich Werkzeugen, die in diesem Buch dargestellt werden. Diese Werkzeuge haben sich über die Jahre bewährt und in der Zwischenzeit auch international durchgesetzt. Aus diesem Grund ist es nicht überraschend, dass sich eine recht junge EU-Datenschutz-Grundverordnung der gleichen Prozesse bedient wie eine »ältere« ISO-27001-Norm.

1

1.3 Informationen und Daten

Der Schutz von Informationen, also dem Know-how des Unternehmens, ist die Aufgabe des IT-Security-Managements. Nur was sind Informationen und worin unterscheiden sie sich von Daten? Daten sind eine technische Darstellung von Informationen. Anders ausgedrückt: Informationen sind Daten, die einen Sinn ergeben. Auf niedrigster Ebene bestehen sie aus den physikalischen Zuständen »hohe Spannung« oder »niedrige Spannung« oder übersetzt null oder eins. Somit sind Daten zunächst einmal Bits und Bytes, deren Interpretation wiederum Informationen ergeben. Sicherheitsmaßnahmen wiederum kann man nicht direkt auf Informationen beziehen. Setzt man Verschlüsselung ein, dann werden die Daten verschlüsselt. Installiert man einen Virens scanner, dann schützt man das Betriebssystem und indirekt wieder die Daten. Ganz anders, wenn man dies aus der Perspektive des Risikomanagements betrachtet, dann stehen die Informationen im Mittelpunkt und deren Wert für das Unternehmen. Wenn wir also von Informationsschutz sprechen, dann geht es im Grunde darum, alle Systeme inklusive der Daten technisch zu

schützen, um die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen zu bewahren.

Die Gewinnung von Informationen aus einem Pool von Daten geschieht durch eine Fragestellung. So sind Daten mit der Ausprägung »4 Eier, 450 g Mehl, 400 ml Milch, Vanillezucker, 210 g Zucker und eine Prise Salz« nur im Zusammenhang mit der Frage »Was benötige ich, um vernünftige Pfannkuchen machen zu können?« als Information anzusehen. Ohne Fragestellung sind es nur beliebige, nicht zusammenhängende Daten. Daraus kann man ersehen, dass Daten zunächst einmal keinen Kontextbezug haben. Das wertvolle Gut, das es zu schützen gilt, ist also mehr als nur eine Menge von Bits und Bytes auf Festplatten.

Jede Form von Informationen, wie immer sie auch ausgestaltet sein mögen und deren Verlust einen Schaden für das Unternehmen bedeutete, gehört zu den Unternehmenswerten, die im Fokus des Managers IT-Security liegen.

Wichtig

Auch wenn sich das IT-Security-Management auf Daten und Daten verarbeitende Systeme konzentriert, stehen noch eine ganze Reihe weiterer Unternehmenswerte im Fokus der IT-Security. Dazu zählen auch abstrakte Werte wie der Ruf des Unternehmens oder das Wissen in den Köpfen der Mitarbeiter.

Informationen können in vielfältiger Form vorliegen. Die Erfahrungen von Mitarbeitern gehören genauso zu den schützenswerten Informationen wie Informationen, die auf Datenträgern vorliegen und durch IT-Systeme verarbeitet werden. Im Gegensatz zu Ersteren können Informationen, die auf Datenträgern wie Festplatten oder auf Papier vorliegen, generell geschützt werden. Deshalb konzentrieren sich viele Maßnahmen der IT-Security auf diese Art der Informationen.

Informationen haben einen Lebenszyklus und einen je nach Alter unterschiedlichen Schutzbedarf. So sind Informationen über eine technische Neuentwicklung zunächst einmal sehr sensibel, da der Schaden bei Verlust in diesem Stadium am höchsten wäre. Wird die Neuentwicklung zur Serienreife gebracht, so ist der Schutzbedarf vielleicht immer noch hoch, aber nicht mehr

so hoch wie zu Anfang. Dies ändert sich dann weiter, wenn die Produktion und Auslieferung beginnt. Ab diesem Zeitpunkt kann auch ein Konkurrent leicht auf das Produkt zugreifen und erforderliche Informationen extrahieren. Der Schutzbedarf ist in dieser Phase damit deutlich niedriger als zu Beginn.

Wichtig

Der Wert einer Information hängt von seiner generellen Bedeutung für das Unternehmen, seiner Qualität, seinem Alter und letztendlich von den Kosten ab, die bei ihrem Verlust oder der Nichtverfügbarkeit entstehen würden.

1

Informationen sind unterschiedlich wichtig, eine Tatsache, die sich in der Bewertung auf Basis der Klassifizierungsrichtlinie widerspiegeln muss. Diese dient dazu, Unternehmenswerte nach Schutzbedarf einzustufen. Im Rahmen der Verfügbarmachung von Informationen spielt es noch eine Rolle, inwieweit unwichtige Informationen herausgefiltert werden können. Dazu zählen Informationen, die für den Betrieb des Unternehmens keinerlei Rolle spielen und deren Vermischung mit relevanten Informationen Zeit und Ressourcen kosten. Zu diesen unwichtigen Informationen kann man z.B. Spam-E-Mails zählen.

Die Klassifizierung von Informationen ist ein wichtiges Instrument für den Manager IT-Security, weil sie aufzeigt, worauf er sich konzentrieren muss und worauf nicht. Außerdem bildet sie die Grundlage für das IT-Risikomanagement. Der Prozess der Einstufung von Unternehmenswerten wird unter aktiver Mithilfe des Erstellers der Information durchgeführt und hat weitreichende Auswirkung auf die Speicherung, die Verarbeitung, den Zugang und das Backup der Information.

1.4 IT-Security-Management ist wichtig

In Unternehmen, in denen ein organisatorischer Bereich IT-Dienstleistungen erbringt, ohne direkt Teil der Wertschöpfungskette zu sein, wird es schwerer fallen, IT-Security zu leben, als in einem Unternehmen, dessen Selbstzweck aus IT-Dienstleistungen besteht. Unternehmen, deren IT-Leitung in der Unternehmensspitze repräsentiert wird, haben wiederum einen administrativen Vorteil gegenüber Unternehmen, in denen dies nicht der Fall

ist. Diese Zusammenhänge lassen sich immer wieder finden und durchziehen alle Unternehmen. Damit im Zusammenhang steht die Tatsache, dass IT-Security immer noch stark als IT-Thema gesehen wird und häufig nicht die Unternehmensleitung, das Controlling oder der Vorstand als Treiber und Förderer in Erscheinung tritt. Diese Sichtweise ist einem laufenden Wandel unterzogen und es ist zu erkennen, dass sich dies in vielen Ländern immer schneller ändert. So hat das in Deutschland seit Juli 2015 gültige Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, das IT-Sicherheitsgesetz (IT-SiG), dazu geführt, dass Unternehmen, die kritische Infrastrukturen betreiben, mit hohem Aufwand Sicherheitsmanagementsysteme implementiert haben. Mit der Version 2.0 dieses Gesetzes wird der Geltungsbereich auf noch deutlich mehr Unternehmen ausgeweitet, was wiederum einen neuen Schub mit sich bringen wird. Auf europäischer Ebene sind weitere Richtlinien in der Ausarbeitung, die diesen Schwung noch verstärken werden.

In Ländern wie den USA hat man bereits früher damit begonnen. Der Grund hierfür liegt auch in der sich schnell weiterentwickelnden Gesetzgebung. So haben die Skandale um die Firmen Enron und WorldCom hohe Wellen geschlagen, die bereits 2002 im Sarbanes-Oxley Act mündeten. Dieses Gesetz soll die Verlässlichkeit von Finanzdaten amerikanischer Firmen sicherstellen, und dafür greift es tief in die Nachvollziehbarkeit administrativer Handlungen im Umgang mit Daten ein. Eine ganze Reihe an Prozessen und Vorgehensmodellen müssen umgesetzt werden, um dies zu erreichen, und die meisten davon zielen in die gleiche Richtung wie ein umfassendes IT-Security-Management.

Das führt zu dem zugegebenermaßen nicht repräsentativen Bild, dass ein Softwareunternehmen, das mit dem Verkauf von Applikationen seinen Umsatz erzielt, von vornherein eher darauf bedacht sein wird, dass die Innovationen, die im Produkt stecken, vertraulich bleiben, als ein Unternehmen der Chemiebranche mit mindestens ebenso sensiblen Daten. Das zeigt die Erfahrung der letzten Jahre und das viele Feedback auf entsprechende Umfragen.

Worin liegt aber nun der Unterschied zwischen Unternehmen A, das, sagen wir mal, Dünger verkauft, und Unternehmen B, das sein Geld mit innovativer Grafiksoftware verdient? Zum einen liegt es vermutlich daran, dass in Unternehmen B Menschen beschäftigt sind, die innerhalb des großen Feldes der IT arbeiten. Programmierer und Administratoren, die sich ständig austauschen und die schon von Berufs wegen eine starke Affinität zu dieser Thematik haben. In Unternehmen B arbeiten vor allem Ingenieure an den neuen Pro-

dukten. Sie tun dies zwar, indem sie Computer für die Modellierung benutzen, aber im Grunde ist die IT eine Abteilung, die nur dafür zu sorgen hat, dass diese Arbeit reibungslos vonstattengeht. Sie sollte sich also, möglichst unsichtbar, im Hintergrund halten.

Hebt man den Blick an und konzentriert sich auf die strategische Ebene, dann verschwinden die Unterschiede sehr schnell, und es wird ersichtlich, dass die Aufgabe des IT-Security-Managements aus genau den gleichen Gründen wichtig für beide Unternehmen ist.

Folgende Grundsätze sollen verdeutlichen, warum das IT-Security-Management eine unternehmerische Kernaufgabe darstellt – unabhängig von Geschäftszweck und auch unabhängig von der Unternehmensgröße:

- **IT-Security ist wichtig für alle Unternehmen**, die Know-how besitzen, das sie zu einem wichtigen Player auf dem Markt macht.
- **IT-Security ist wichtig für alle Unternehmen**, die Konkurrenten auf dem Markt haben.
- **IT-Security ist wichtig für alle Unternehmen**, die Technologien einsetzen, die verwundbar gegenüber Angriffen sein könnten.
- **IT-Security ist wichtig für alle Unternehmen**, die personenbezogene Daten speichern und verarbeiten.

Wenn man die Dinge von dieser Warte aus sieht, dann gibt es keine Unterschiede mehr zwischen Düngerherstellern, Softwareproduzenten oder öffentlichen Einrichtungen. Die Implementierung eines IT-Security-Managements ist für alle Unternehmen aller Geschäftsfelder entscheidend, um auf dem freien Markt bestehen zu können.

Die Unterschiede liegen dann nur noch in der Handhabung und Bewertung der verschiedenen Sicherheitsprozesse begründet. Also darin, wie man Risiken bewertet und davon abgeleitet, welches Budget man investiert, um Maßnahmen zur Risikoreduzierung zu installieren.

1.5 Wie gefährdet sind die Unternehmensdaten

Staatliche und private Stellen versuchen, die globale Gefährdungslage regelmäßig zu erfassen und geeignet darzustellen. Aus dieser Darstellung lassen sich Trends ablesen, die der Unternehmensleitung ein unabhängiges Bild

ermöglichen, bevor sie daran geht, die dort gesammelten Informationen auf das eigene Unternehmen abzubilden.

1.5.1 Sicht des Verfassungsschutzes

Die Landesämter für Verfassungsschutz, die sich gezielt mit dem Thema Wirtschaftsspionage beschäftigen, touren seit einigen Jahren ohne Unterlass durch die Unternehmen und geben eine Einschätzung, was ihrer Erfahrung nach im Bereich des professionellen Datendiebstahls vor sich geht. Und die Zahlen, die sie dabei präsentieren, haben es in der Tat in sich. Es geht nicht nur um konkrete Beispiele, die bemüht werden, sondern darum, dass die Menge aufgedeckter staatlicher Spionageaktionen exponentiell steigt und dass sich ihrer Ansicht nach viele Staaten angesichts des weltweiten Konkurrenzkampfs im Wirtschaftssektor nicht mehr anders zu helfen wissen, als die Informationen zu stehlen, die sie benötigen. Im Gegensatz zu früher trifft es dabei nicht mehr nur die ganz großen Unternehmen, vielmehr rücken die Mittelständler in den Fokus. Unternehmen mit wenigen Tausend Mitarbeitern, die auf einem Sektor technologisch weit vorne mit dabei sind, werden zum Zielobjekt. Zur Zielerreichung wird laut Verfassungsschutz die ganze Bandbreite an Angriffsmöglichkeiten genutzt. Das reicht von Angriffen über das Internet über eigens für einen Angriff entwickelte Trojaner bis hin zum lokal durchgeführten Spionageangriff durch studentische Hilfskräfte oder Diplomanden.

Ein Zitat von der Webseite des baden-württembergischen Verfassungsschutzes drückt es so aus: »Der Verfassungsschutz sieht in den internetgebundenen Angriffen auf Netzwerke und Computersysteme von Firmen und Regierungsstellen die aktuell gefährlichste Bedrohung im Bereich Wirtschaftsspionage.« Hilfestellungen gibt das Amt auch: Es verweist auf die Schriften des Bundesamts für Sicherheit in der Informationstechnik (BSI), und dort wiederum wird das IT-Security-Management als der Prozess beschrieben, der eingeführt werden muss, um die Sicherheit des eigenen Know-hows und damit den Fortbestand des Unternehmens zu sichern.

1.5.2 Öffentliche Wahrnehmung

Wenn es erforderlich wird, zumeist abstrakte Gefährdungen mit Daten und Fakten zu hinterlegen, dann werden die eher generellen Verdachtsmomente und die wenigen konkreten Beispiele des Verfassungsschutzes im Zweifels-

fall nicht ausreichen, um die nötigen Mittel bewilligt zu bekommen, die erforderlich sind, ein modernes IT-Security-Management aufzubauen. Für diesen Zweck sind einige Quellen im Internet hilfreich, die sich seit Jahren bemühen, Vorfälle zu sammeln und statistisch darzustellen. Das Problem dabei ist grundsätzlich, dass niemand gerne darüber spricht, wenn er zum Mittelpunkt eines erfolgreichen Angriffs geworden ist. Angst um die eigene Reputation oder die Sorge, verklagt zu werden, falls auch anvertraute Daten gestohlen wurden, tun ihr Übriges.

Der Schaden einer Veröffentlichung wird somit häufig höher eingeschätzt als der Nutzen einer Anzeige. Das liegt auch daran, dass der Prozentteil an aufgeklärten Vorfällen verschwindend gering ist. Während große, publikumswirksame Vorfälle auch von staatlichen Stellen verfolgt werden, bleibt es kleinen Unternehmen häufig selbst überlassen, Nachforschungen anzustellen. Auch heute noch sind die allermeisten Polizeidienststellen nicht in einem Maß ausgerüstet, das sie in die Lage versetzen würde, selbst erfolgreich tätig werden zu können.

Ein zweiter wichtiger Grund, warum viele Vorfälle niemals veröffentlicht werden, ist der, dass sie schlicht und einfach nicht entdeckt werden. Schätzungen gehen bis an die 90 % aller Vorfälle, die niemand bemerkt. Das hängt damit zusammen, dass Systeme zur Entdeckung von Sicherheitsvorfällen, sogenannte Intrusion-Detection-Systeme (IDS), nur in wenigen Unternehmen eingesetzt werden und aufgrund ihrer Komplexität selbst dort nur selten durchgängig brauchbare Ergebnisse liefern. Dazu kommt, dass ein solches System nur einen Baustein auf dem Weg zur Einführung eines IT-Security-Managementprozesses darstellt. Ohne entsprechende Prozesse, in die ein IDS eingebunden werden kann, ist die erfolgreiche Nutzung fast nicht möglich.

Aus nachvollziehbaren Gründen sind die Analysen der verschiedenen Institutionen nicht geeignet, wenn es darum geht, von den vorliegenden Aussagen konkrete Informationen abzuleiten, die auf das eigene Unternehmen eins zu eins abgebildet werden können. Das ist aber auch nicht immer erforderlich. Zumeist reichen die dort zusammengetragenen Informationen aus, um eine Entwicklung abzulesen und daraus eigene Schlüsse abzuleiten, was die Priorisierung von Themen angeht.

Aus Studien seit 2010/2011 ist der Verlauf sichtbar, den die Bedrohung Schadsoftware im Vergleich mit der Bedrohung Phishing seit 2005 nimmt. War 2005 das Auftreten von Schadsoftware das größte Problem, so hat sich dies