mitp

Thomas W. Harich

2. Auflage

IT-Sicherheitsmanagement

Praxiswissen für IT Security Manager

Thomas W. Harich

IT-Sicherheitsmanagement

Praxiswissen für IT Security Manager

2. 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 978-3-95845-274-9
2. Auflage 2018

www.mitp.de
E-Mail: mitp-verlag@sigloch.de
Telefon: +49 7953 / 7189 - 079
Telefax: +49 7953 / 7189 - 082

Lektorat: Sabine Janatschek
Korrektorat: Petra Heubach-Erdmann
Covergestaltung: Christian Kalkert, www.kalkert.de
Bildnachweis Cover: fotolia.com/Vladitto
Satz: III-satz, Husby, www.drei-satz.de

Inhaltsverzeichnis

Einleitung

Vorwort zur zweiten 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.

Anlass für die zweite Auflage dieses Buches sind neben dem technischen Fortschritt, der unaufhaltsam ist, die umfassenden Änderungen in den ISO-Normen, der nun europaweit vereinheitlichte Datenschutz und eine Reihe

von neuen Themen, die ich in den entsprechenden Kapiteln aufgenommen habe. Dementsprechend halten Sie ein stark überarbeitetes Buch in Händen.

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.

Einführung

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.

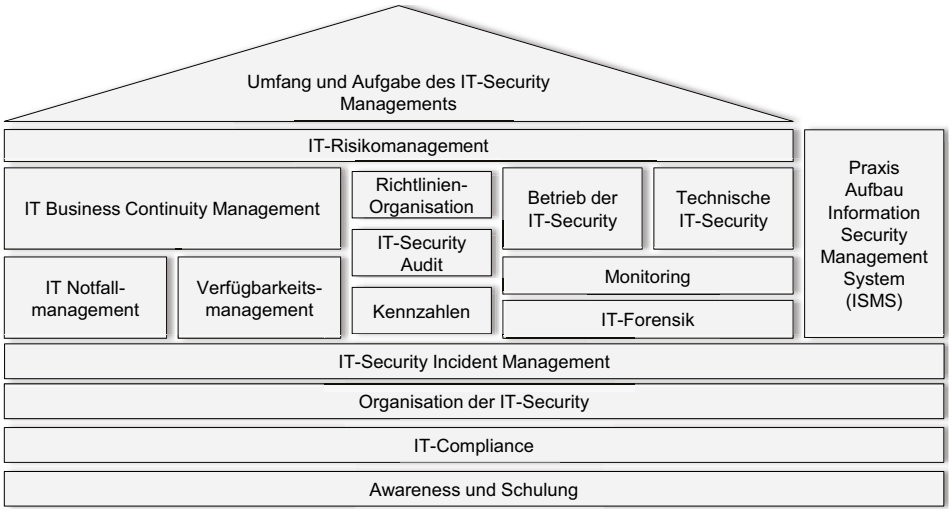
Andere, und damit sind wir wieder bei den vielen Wegen angekommen, die zum Ziel führen, sind Neueinsteiger oder Quereinsteiger. Vielleicht kommen sie aus der IT-Abteilung und haben zuvor Server administriert oder Softwareprojekte geleitet. In manchen Fällen waren sie davor aber auch im Controlling oder 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 nun in der Situation, das Know-how des Unternehmens zu schützen, indem er die Bedrohungen erkennt, abschätzt und diesen dann geeignete Sicherheitskonzepte 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.

1.3 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. Maßnahmen wiederum kann man nicht direkt auf Informationen beziehen. Setzt man Verschlüsselung ein, dann werden die Daten verschlüsselt. Installiert man einen Virenscanner, 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 aber 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 immer noch hoch, aber nicht mehr so 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 vor allem von den Kosten ab, die bei ihrem Verlust entstehen würden.

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 durchzie-

hen 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 Länder wie die USA in dieser Hinsicht einen Schritt weiter sind als europäische Unternehmen. Der Grund hierfür liegt vor allem in der sich schnell weiterentwickelnden Gesetzgebung im amerikanischen Raum. So haben die Skandale um die Firmen Enron und WorldCom hohe Wellen geschlagen, die letztendlich 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 Produkten. 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 auch 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 Zweifelsfall 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 veröffentlich 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.

Seit einiger Zeit erfasst das Computer Security Institute (CSI) Daten rund um die IT-Security und erstellt ausführliche Analysen, welche die Gefährdungslage detailliert darstellen. Unter *http://www.gocsi.com* sind die entsprechenden Dokumente erhältlich.

Aus nachvollziehbaren Gründen ist keine Fremdanalyse 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, 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 2007 umgedreht. Seit 2015 macht das Schreckgespenst »CEO Fraud« die Runde und mehrere namhafte Unternehmen wurden seitdem dazu gebracht, große Summen aufgrund gefälschter E-Mails an Diebe zu überweisen. Ab

2017 kam zu diesem Problem noch eine recht neue Disziplin hinzu, die sogenannte Erpressersoftware (*ransomware*), die einigen technischen Schaden angerichtet hat. Gerade diese Art an Angriff bietet ein recht gutes Auskommen bei sehr geringem Risiko und deshalb finden Angriffe dieser Art auf zum Teil hochprofessionellem Wege statt.

Auf diesen Strauß an Angriffsarten mit einzelnen Maßnahmen zu antworten, ist der falsche Weg – auch wenn dies durchaus noch der Fall ist. Das Bewusstsein für die aktuell größte Gefahr wird immer noch aus Studien, aus Berichten in Film, Funk und Fernsehen und der Werbung der Sicherheitsindustrie abgeleitet. Was man dabei schnell vergisst, ist: Studien werden über längere Zeiträume verfasst, und selbst wenn sich ein Trend herausbildet, wäre die Reaktionszeit zu hoch, um jedes Mal gezielt auf Verschiebungen der eingesetzten Angriffsmittel zu reagieren. Was aber in jedem Fall abgelesen werden kann, sind die Hauptangriffswege und damit die Hauptgefahren. Dementsprechend können auch die Prozesse der IT-Security ausgerichtet werden. Ableiten kann man daraus für jeden Verantwortlichen für IT-Security, dass nur ein umfassendes IT-Security-Management, das alle Bedrohungen einkalkuliert, ein transparentes und verlässliches Sicherheitsniveau gewährleisten kann.

1.5.3 Die eigene Wahrnehmung

Wie sicher fühlt man sich im Unternehmen? Wie schätzt man die Bedrohungslage realistisch ein? Ist wirklich jemand oder etwas hinter dem Know-how des Unternehmens her und versucht, an dieses heranzukommen? Diese Fragen stellen sich zahllose Unternehmen und haben dabei eines gemeinsam: Objektive Antworten auf diese Fragen kann es nur in Einzelfällen geben, und deshalb beantworten Unternehmen diese Fragen aufgrund einer subjektiven Wahrnehmung. Damit wird auch gleich eine Antwort auf das Phänomen gegeben, warum jeder medial ausgeschlachtete, große Fall von Schadsoftware oder Datendiebstahl bei weithin bekannten Unternehmen branchenübergreifenden Aktionismus auslöst. Kurze Zeit später, die Medien sind bereits weitergezogen, verlaufen viele dieser Aktionen im Sande, werden aus Kostengründen eingestellt oder nur unter Sparflamme weiterverfolgt.

Um ein annähernd genaues Bild von der Realität zu bekommen, ist es also erforderlich, möglichst viele Fakten zu kennen und zu bewerten. Die Analysen des Verfassungsschutzes, Statistiken von unabhängigen Gesellschaften

kombiniert mit den Ergebnissen von Protokollen der eigenen Firewall und eigenen IDS-Systemen ergeben eine Momentaufnahme, die als Grundlage für die Sicherheitsstrategie dienen kann. Damit werden Informationen, die einen Durchschnitt abbilden, mit Informationen kombiniert, die tatsächliche, individuell aufgetretene Ereignisse beschreiben.

An diesem Punkt setzen Awareness-Maßnahmen an. In einem Top-down-Vorgehen werden die einzelnen Entscheidungsebenen laufend und möglichst mit faktenbasiertem Material über die Gefährdungslage informiert. Damit wird eine Grundlage geschaffen, vom reflexartigen Reagieren hin zum proaktiven Handeln zu gelangen. Den dann erreichten Zustand und die definierte weitere Vorgehensweise sowie die zugrunde liegenden Ziele kann man dann als IT-Security-Strategie umschreiben.

1.6 Begrifflichkeiten

Der Begriff »IT-Sicherheitsmanagement« beinhaltet bereits in seinem Namen eine Einschränkung: Es geht ganz offensichtlich um eine Aufgabe innerhalb der IT, besser ausgedrückt, um eine Aufgabe innerhalb der Abteilung, die sich mit der Informationstechnologie beschäftigt. Wenn man nun aber den Prozess der Wertschöpfung eines Unternehmens betrachtet, dann fällt schnell auf, dass sich, um ein Produkt herzustellen, viele zu schützende Unternehmenswerte überhaupt nicht im Einflussgebiet der IT bewegen. Dazu kann der Prototyp gehören, dessen Form von Hand hergestellt wird, oder die Kalkulation, die von einem Controller auf ein Flip-Chart aufgeschrieben und im Besprechungszimmer vergessen wird. Wenn man die Schutzmaßnahmen betrachtet, die erforderlich sind, um Informationen oder auch den Prototyp von eben zu schützen, dann wird dies noch deutlicher. Die ISO 27002 führt diesbezüglich eine ganze Reihe an Maßnahmen auf, wie den Gebäudeschutz inklusive des Zauns um den Entwicklungsstandort. So gesehen deckt die IT-Security einen großen Teil der in den einschlägigen Standards beschriebenen Themenfelder ab, aber eben nicht alle. Folgt man dieser Logik, dann kann die IT-Security als Untermenge der Informationssicherheit gesehen werden. Die Informationssicherheit wiederum kann um sicherheitsrelevante Themen wie den Reiseschutz oder den Werkschutz ergänzt werden. Was letztendlich welchem Oberbegriff zugeschlagen wird, ist individuell in jedem Unternehmen zu regeln. Wichtig ist nur, dass die Trennung klar kommuniziert ist, um Rei-

bungspunkte zu vermeiden. Aus diesem Grund werden diese Aufgaben in großen Unternehmen meistens gebündelt und einem Gesamtverantwortlichen unterstellt. Seitdem die EU-Datenschutz-Grundverordnung im Mai 2018 in Kraft getreten ist, steht an der Spitze einer solchen Organisation immer häufiger der Datenschutzbeauftragte.

Im Rahmen dieses Buches sprechen wir durchgehend von der IT-Security, dem Manager IT-Security und dem IT-Security-Management, weil es sich vorwiegend auf die Aufgaben innerhalb der Informationstechnologie bezieht. Wenn angrenzende oder nicht klar abgegrenzte Themengebiete angesprochen werden, z.B. wenn der Schutz von Rechenzentren zur Sprache kommt, die man gut und gerne dem physischen Schutz und damit z.B. dem Facility-Manager zuordnen kann, dann wird auf diesen Sachverhalt hingewiesen.

In der Diskussion rund um den Themenbereich »IT-Security« taucht eine Reihe von weiteren Begriffen auf, die zum Teil synonym verwendet werden. Dazu gehören zum einen der Begriff »Datenschutz« und zum anderen die Begriffe »Informationsschutz«, »Informationssicherheit«, »Datensicherheit« oder »IT-Sicherheit«. Der Datenschutz, auf Englisch »data privacy«, bezieht sich dabei auf personenbezogene Informationen, deren Speicherung und Verarbeitung in der EU-Datenschutz-Grundverordnung und den länderspezifischen Gesetzen geregelt werden.

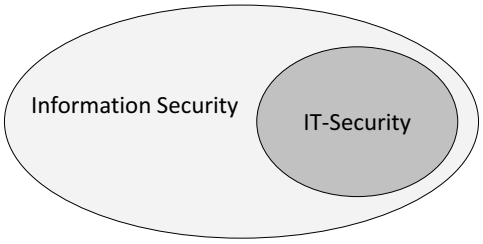


Abbildung 1.1: Schnittmenge Information-Security und IT-Security

Die Begriffe »Informationsschutz«, »Informationssicherheit«, »Datensicherheit« und »IT-Sicherheit« werden im Englischen oft unter dem Oberbegriff »data security« oder allgemeiner »information security« zusammengefasst und beschreiben den allgemeinen Schutz von Informationen. Dabei ist es zunächst unerheblich, ob diese Informationen in Form von elektronisch verarbeitbaren Daten oder in Form von Papierdokumenten vorliegen.

Hinweis

Im vorliegenden Buch wird der Begriff »IT-Security« als Oberbegriff des Informationsschutzes in Abgrenzung zum Datenschutz verwendet. Im Fokus liegt dabei vorwiegend der Schutz von Daten, Applikationen und IT-Systemen. Alternativ wird von »Informationsschutz« oder auch »Informationssicherheit« die Rede sein. Alle diese Begriffe werden als Synonyme betrachtet.

Das IT-Security-Management hat den Schutz von Know-how im weitesten Sinne zum Ziel. Daraus ist abzuleiten, dass die Sicht rein auf elektronische Daten zu kurz greift, auch wenn dies die Bezeichnung »IT-Security« so suggeriert. Prozesse, Richtlinien und schlicht das Verhalten im Umgang mit Informationen muss so ausgelegt sein, dass der Träger der Information dabei möglichst variabel sein kann. Greift eine Richtlinie in den Prozess des Ausdruckens von Kalkulationstabellen ein, so sind technische Maßnahmen sinnvoll, die es erlauben, sicherzustellen, dass der Ausdruck erst dann geschieht, wenn der berechtigte Mitarbeiter vor dem Drucker steht. Daneben muss es aber auch Richtlinien geben, die festlegen, wie mit den ausgedruckten Tabellen umgegangen werden muss. Zu diesen Vorschriften gehört eine Clean-Desk-Richtlinie genauso wie eine definierte Kennzeichnungspflicht und Regeln bezüglich der Weitergabe dieser Dokumente.

1.7 Selbstverständnis der IT-Security-Organisation

Verantwortlich für das Know-how des Unternehmens in jeder Form ist die Unternehmensleitung. Der Manager IT-Security arbeitet innerhalb des Kompetenzrahmens, der ihm zugewiesen wird, und setzt die Vorgaben und Ziele der Unternehmensleitung zum Informationsschutz um. Sinnvollerweise sind diese Ziele weit gefasst und geben dem Manager IT-Security die Möglichkeit, eigenverantwortlich und umfassend zu agieren. Da anerkanntermaßen kein 100%iger Schutz möglich ist, wird es immer um eine Annäherung an einen definierten Idealzustand gehen. Dieser Idealzustand bewegt sich zwischen einem optimalen Sicherheitszustand und dem, was mit vertretbarem Aufwand und Kosten möglich ist. Dieser Idealzustand ist das sogenannte »angestrebte Sicherheitsniveau«. Die Annäherung erfolgt in allen Teilberei-