Thomas W. Harich

IT-Sicherheits-management

Das umfassende Praxis-Handbuch

IT-Security und technischer Datenschutz nach ISO/IEC 27001 und IT-Grundschutz

4. Auflage

mitp

Inhaltsverzeichnis

Einleitung

Anmerkung zur vierten Auflage

Auch wenn die grundlegenden Pfeiler des IT-Sicherheitsmanagements immer noch dieselben sind wie in der ersten und den darauffolgenden Auflagen, so hat sich innerhalb der verschiedenen Themenbereiche dennoch vieles getan. Aus diesem Grund habe ich die vierte Auflage genutzt alle Kapitel gründlich zu überarbeiten, zu erweitern, veraltete Vorgehensweisen zu entfernen und neue hinzuzufügen. Damit trage ich auch den neuesten europäischen Regularien Rechnung, die eine neue Perspektive in das Thema einbringen. Es ist schlicht etwas anderes, ob ein Unternehmen Sicherheit nur aus der Innensicht heraus voranbringt oder ob durch Gesetze eine gesamtwirtschaftliche Sichtweise hinzugefügt wird. So ist das erklärte Ziel aus Sicht der europäischen Nationalstaaten und letztendlich aus europäischer Sicht, die Sicherheitsrisiken über alle relevanten Branchen im Blick zu haben und zu jeder Zeit eine Art Übersicht über die Gefährdungslage im Zugriff zu haben. Natürlich ist man davon noch Jahre entfernt, aber die ersten Schritte wurden mit dem IT-Sicherheitsgesetz begonnen und werden nun mit NIS2 (Network and Information Security Directive 2) fortgesetzt. Wenn man über den europäischen Tellerrand hinausblickt, stellt man fest, dass Länder wie Indien oder China dem europäischen Raum schon ein paar Jahre voraus sind.

Fortschritte macht zudem das organisierte Verbrechen. Die Zeitspanne, die zwischen der ersten Phising-Mail und der erfolgreichen Verschlüsselung von Daten liegt, sinkt weiter von mehreren Tagen auf wenige Stunden. Der steigende Automatisierungsgrad der verschiedenen Phasen eines Angriffs legt nahe, dass diese Zeitspanne weiter sinken wird. Dementsprechend schnell müssen die Verteidiger einen Angriff entdecken und zielgerichtet darauf reagieren. Damit verschiebt sich generell der Fokus weiter weg von den präventiven Maßnahmen wie dem klassischen Antivirenprogramm hin zum Management von Sicherheitsereignissen und deren Behandlung.

Diesen neuen Schwerpunkten trage ich Rechnung, indem ich die entsprechenden Kapitel erweitert habe.

Mein Dank gilt auch dieses Mal all denjenigen, die sich mit Lob oder konstruktiver Kritik eingebracht haben. Dazu gehören neben den Hochschulen auch Vertreter von Unternehmen, die als praktische Anwender und Umsetzer ganz genau sehen, wo es Raum für Verbesserungen gibt, und dies auch an mich weitergegeben haben.

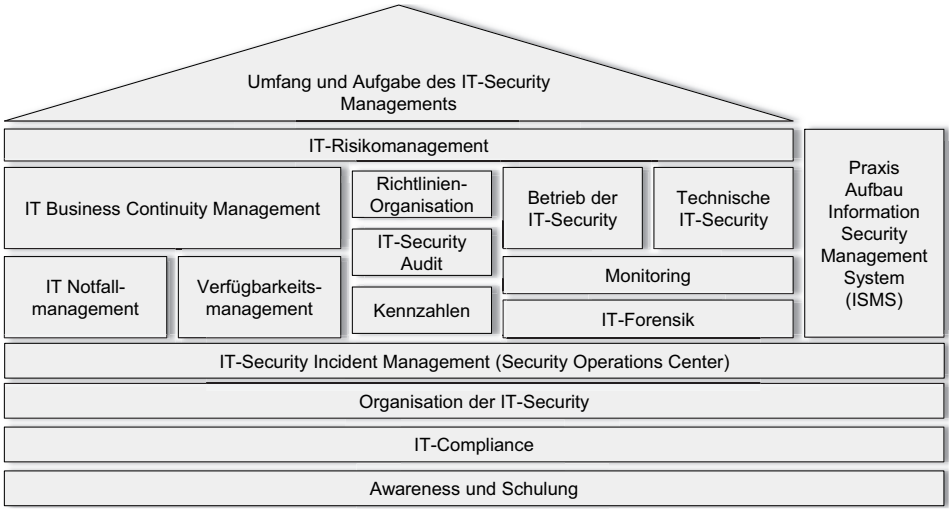
Über die Zielgruppe

Noch immer ist die Bandbreite an Ausbildungen, die ein typischer IT-Security-Manager vorweisen kann, überraschend groß. Das liegt vermutlich daran, dass die Aufgabe vor allem ein gut ausgeprägtes analytisches Denken voraussetzt, das auf einem breiten technischen Verständnis für IT-Zusammenhänge aufsetzt. Da der technische Background, genauso wie die Kompetenz hinsichtlich Compliance-Themen, auch nachträglich, durch Weiterbildungen, ausgebaut werden kann, ist es durchaus möglich, sich auch als Quereinsteiger für einen solchen Job zu qualifizieren. Das ist aber nur die halbe Wahrheit. Im Zuge der vielen neuen Studiengänge im Bereich der Informationssicherheit wird die Konkurrenz mit passenden Bachelor- und Masterabschlüssen weiter zunehmen. Wenn man einen solchen Abschluss nicht nachweisen kann, dann empfiehlt es sich in jedem Fall, passende Zertifizierungen zu erwerben.

Weiterhin gilt, dass die Aufgabe zukunftssicher ist und an Vielschichtigkeit eher zunimmt als abnimmt. Gerade die Komplexität 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 wie-

der 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 eine einzukaufende 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 stellen sich die Fragen, 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 Kapitelausblick

Im ersten Kapitel 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, die Sicherheit der Lieferkette, neue europäische Cyber-Gesetze wie NIS2, Heimarbeitsplätze, Cloud-Services und viele andere Themen beherrschen die Schlagzeilen in den Medien genauso wie die Diskussionen in den Fachkreisen. 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

die verschiedenen Sicherheitsfelder miteinander verwoben sind. Klassische Aufgaben der Prävention, wie der Schutz vor Schadsoftware oder das Patchen, müssen mit der aktiven Erkennung von Angriffen zusammenspielen, um effizient zu sein. Altes Wissen, das aus den Frühzeiten der Personal Computer stammt, trifft auf völlig neue Angriffsmuster. In dieser Gemengelage ist es die Aufgabe des Managers IT-Security, den Überblick zu bewahren und auf die wesentlichen 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 überwiegend 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 vergleichsweise junge EU-Datenschutz-Grundverordnung und eine Mehrheit aktueller Gesetze der Prozesse der deutlich »älteren« ISO 27001-Norm bedient.

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 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,

geht es im Grunde darum, alle Systeme inklusive der Daten technisch zu schützen, um die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen zu bewahren.

Jede Form von Informationen, wie immer sie auch ausgestaltet sein mögen und deren Verlust einen Schaden für das Unternehmen bedeuten würde, 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 regelmäßig nicht mehr so hoch wie zu Beginn. Dieser sinkt weiter, wenn die Produktion und die Auslieferung beginnen.

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.

Informationen sind unterschiedlich wichtig, eine Tatsache, die sich in der Bewertung auf Basis der Klassifizierungsrichtlinie widerspiegelt. Diese dient dazu, Unternehmenswerte nach Schutzbedarf einzustufen. Im Rahmen der Verfügbarmachung von Informationen spielt es zudem 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 organisatorischen 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 treten. Diese Sichtweise ist einem laufenden Wandel unterzogen und es ist zu erkennen, dass sich dies in vielen Ländern bereits 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 »Network and Information Security Directive« (NIS2) wird der Geltungsbereich auf noch deutlich mehr Unternehmen ausgeweitet, was einen neuen Schub mit sich bringen wird. Europäische Verordnungen

wie der Cyber Resilience Act (CRA) wiederum verschieben den Fokus von der Infrastruktur auf Produkte selbst, die einen Sicherheitsstandard einhalten müssen, und machen damit neue Felder auf, die in ein umfassendes Sicherheitskonzept mit eingebunden werden müssen.

Länder wie die USA sind den Europäern um einige Jahre voraus. 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. Ein Blick auf die verschiedenen repräsentativen Umfragen zeigt weiterhin ein sehr inhomogenes Bild. Auch wenn die gesetzlichen und normativen Vorgaben dieselben sind, bedeutet das nicht, dass der Stand des IT-Sicherheitsmanagements auch überall auf dem gleichen Niveau ist. Die Unterschiede zwischen den Unternehmen sind gewaltig. Das liegt an verschiedenen Faktoren wie der Sicht der Unternehmensleitung, der Größe der Budgets für IT-Sicherheit oder auch dem »gefühlten« Schutzbedarf der eigenen Daten. Dazu kommt, dass ein Softwareunternehmen von Natur aus eher in IT-Dimensionen denkt als eine Bäckerei. 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**, deren kritische Geschäftsprozesse von datenverarbeitenden Systemen, im weitesten Sinne, abhängig sind.
- **IT-Security ist wichtig für alle Unternehmen**, die personenbezogene Daten verarbeiten oder speichern.

Wenn man die Dinge von dieser Warte aus sieht, gibt es keine Unterschiede mehr zwischen Bäckereien, Softwareherstellern 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 zu übertragen.

1.5.1 Sicht des Verfassungsschutzes

Die Landesämter für Verfassungsschutz, die sich gezielt mit dem Thema Wirtschaftsspionage beschäftigen, touren seit Jahren 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 großen Unternehmen, vielmehr rücken die Mittelständler in den Fokus. Unternehmen mit wenigen Tausend Mitarbeitern, die auf einem Sektor technologisch führend 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.

Ein noch höheres Risiko besteht laut Verfassungsschutz darin, Opfer eines Ransomware-Angriffs zu werden – also eines Angriffes mit dem Ziel, das Unternehmen oder die öffentliche Einrichtung um ein Lösegeld zu erpressen. Das Opfer wird in diesem Fall nicht mehr aufgrund dessen ausgesucht, ob es lohnenswerte Geheimnisse hat, sondern schlicht nach der finanziellen Leistungsfähigkeit und danach, wie einfach es ist, es zu hacken.

1.5.2 Öffentliche Wahrnehmung

Wenn es erforderlich wird, zumeist abstrakte Gefährdungen mit Daten und Fakten zu hinterlegen, 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 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 Angriffe, bei denen Datendiebstahl im Vordergrund steht, die niemand bemerkt. Das hängt damit zusammen, dass die entsprechenden Prozesse zur Erkennung und Verarbeitung von Sicherheitsereignissen in vielen Unternehmen entweder überhaupt nicht existieren oder noch sehr rudimentär entwickelt sind.

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.

Studien zeigen: Waren in den 90er Jahren Angriffe mit Makro- und Bootsektor-Viren ein Thema weniger eingeweihter Experten, so hat sich das geändert, als Schadsoftware ein Problem wurde, das auch den Heimanwender betreffen konnte. Mit dem Auftreten des sogenannten CEO-Fraud-Angriffes, bei dem vorgegaukelt wurde, dass ein Vertreter der Unternehmensleitung die Überweisung von Geldern anordnet, ging es auf einmal um große Summen. In den Fokus des organisierten Verbrechens geriet das Thema spätestens dann, als mit Ransomware-Angriffen Millionenbeträge zu erbeuten waren. Alle diese Angriffe sind auch heute noch aktuell und werden laufend ausgebaut.

Was sich zeigt, ist, dass es nicht genügt, auf diesen Strauß an Angriffsarten mit Einzelmaßnahmen zu antworten. 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 und alle damit verbundenen Angriffsvektoren 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 jemand 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 Berichten des Security Operations Center (SOC) Teams oder generell der IT-Security bieten dafür eine Grundlage.

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« (IT Security Management) 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, 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 Flipchart aufgeschrieben und im Besprechungszimmer vergessen wird. Wenn man die Schutzmaßnahmen betrachtet, die erforderlich sind, um Informationen oder auch den Prototyp von eben zu schützen, 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 welchem Oberbegriff zugeschlagen wird, ist individuell in jedem Unternehmen zu regeln. Wichtig ist nur, dass die Trennung klar kommuniziert ist, um Reibungspunkte zu vermeiden. Aus diesem Grund werden diese Aufgaben in großen Unternehmen meistens gebündelt und einem Gesamtverantwortlichen unterstellt.

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.

Hinweis

Der Begriff IT-Security wird zunehmend durch den Ausdruck »Cybersecurity« ersetzt. Dabei ist zu beachten, dass der Zuständigkeitsbereich der IT-Security den Bereich der Cybersecurity beinhaltet. Die Cybersecurity beschäftigt sich spezifisch mit Bedrohungen aus dem Internet, die von menschlichen Akteuren gezielt oder ungezielt ausgehen. Die IT-Security kümmert sich darüber hinaus auch um viele weitere Themen wie den Prototypenschutz, die sicher Datenvernichtung oder den Zutrittsschutz.

In der Diskussion rund um den Themenbereich »IT-Security« taucht eine Reihe von weiteren Begriffen auf, die zum Teil synonym verwendet werden.

Dazu gehört zum einen der Begriff »Datenschutz« und zum anderen die Begriffe »Informationsschutz«, »Informationssicherheit«, »Datensicherheit«, »Cybersecurity« (siehe Hinweis oben) 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.

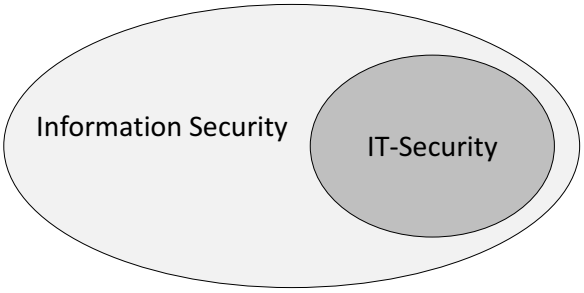


Abbildung 1.1: Schnittmenge Information-Security und IT-Security

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 Prinzipien der IT-Security

Die allermeisten Handlungen, die im Rahmen der IT-Security auf Basis von Vorgaben, die aus Normen, Regelungen, Verträgen oder auch dem gesunden Menschenverstand abgeleitet wurden, ausgeführt werden, lassen sich auf eine Reihe von grundlegenden Regeln zurückführen, die man oft auch als »Prinzipien der IT-Security« bezeichnet. Diese Prinzipien werden im Rahmen des vorliegenden Buches an verschiedenen Stellen immer wieder auftauchen. Sie zu kennen, ist sehr hilfreich, um das »Warum« zu verstehen, wenn innerhalb eines Themenbereichs eine Vorgehensweise beschrieben wird.

Regel	Beschreibung
Daten-Informationseigentümer	Der Ersteller von Informationen (*data owner*) ist sowohl für deren Sicherheitseinstufung (Klassifizierung) als auch für die ordnungsgemäße Weitergabe der Informationen verantwortlich.
Risikoeigentümer	Unter Risikoeigentümer (*risk owner*) ist ein Vertreter der Leitung gemeint, der dem Dateneigentümer im Normalfall vorgesetzt ist. Der Risikoeigentümer soll besser als der Dateneigentümer in der Lage sein, den Schutzbedarf der Information einzuschätzen und die erforderlichen Maßnahmen abzuleiten.
Wirtschaftlichkeit	Jede Maßnahme wird auf Wirtschaftlichkeit geprüft, indem ihre Kosten den möglichen Kosten bei Eintritt eines Schadens gegenübergestellt werden. Damit soll vermieden werden, dass mehr Mittel für die Vermeidung eines möglichen Sicherheitsproblems aufgewendet werden, als das Sicherheitsproblem bei Eintritt verursachen würde.
Funktionstrennung (*segregation of duties* oder auch *separation of duties*)	Verschiedene kritische Schritte eines Prozesses sollen nicht durch dieselbe Person oder Organisationseinheit wahrgenommen werden. Dies soll sicherstellen, dass nicht eine einzelne Person ihre Rechte missbrauchen kann, um einen gesamten Prozess zu manipulieren.

Regel	Beschreibung
Vieraugenprinzip (*two-man rule*)	Sensible Arbeitsschritte sollen nicht durch eine Person umgesetzt werden. So kann z.B. das Passwort für ein kritisches IT-System auf zwei Personen aufgeteilt werden, und der Zugriff auf das System wird in der Folge immer die Anwesenheit beider Personen voraussetzen.
Rechte nach Bedarf (*need-to-know*)	Jeder Mitarbeiter sollte nur die Zugriffsrechte bekommen, die er für die Durchführung seiner Arbeit benötigt. So haben nur definierte Personen Zugang zu sensiblen Bereichen wie dem Rechenzentrum. Auch der Zugriff auf Daten im Allgemeinen wird nach diesem Prinzip festgelegt.
Weitere Einschränkung von Zugriff und Zugang zu sehr sensiblen Daten und Räumlichkeiten	Auch Personen mit hoher Sicherheitseinstufung bekommen kritische Zugriffsrechte auf bestimmte Daten oder Systeme immer nur zu dem Zeitpunkt und für die Dauer, zu der sie diesen Zugriff benötigen. In dieser Ausprägung handelt es sich um eine Verschärfung der allgemeinen Need-to-know-Regel.
Standardisierung	Das Funktionieren eines IT-Security-Managements setzt die Existenz von Transparenz voraus. Ordnung und Standardisierung von Bezeichnungen, Prozessen oder Installationen sind eine wichtige Voraussetzung, um darauf wiederum standardisierte Sicherheitsprozesse aufsetzen zu können.
Poka Yoke	Menschliche, unabsichtliche Fehler führen zu sicherheitsrelevanten Problemen, wie Ausfällen von IT-Systemen oder Fehleingaben. Diese Fehler sind nicht zu 100 % ausschließbar. Die Vorgehensweise nach Poka Yoke (aus dem Japanischen: Poka = Vermeidung, Yoke = unbeabsichtigter Fehler) versucht, durch technische und organisatorische Vorkehrungen die Fehlerrate zu minimieren. Das können Überprüfungsalgorithmen bei der Dateneingabe in Softwaresysteme sein oder ein besseres Eingabe-Interface, das benutzerfreundlicher gestaltet wird.

Regel	Beschreibung
Datensparsamkeit	Die Datensparsamkeit ist ein Begriff aus dem Datenschutzrecht. Diese Regel besagt, dass es immer vorzuziehen ist, möglichst wenige Daten einer Gefährdung auszusetzen. Besteht die Aufgabe z.B. darin, die Datenübermittlung kritischer Informationen sicher zu gestalten, so ist der erste Schritt der, dafür Sorge zu tragen, dass nur die absolut erforderlichen Informationen übertragen werden.
Privacy by Default	Privacy by Default legt fest, dass in einem Softwareprodukt, auf einem Betriebssystem oder in einer Firmware schon bei der ersten Inbetriebnahme alle Sicherheitseinstellungen so eingestellt sein müssen, dass der Schutz von personenbezogenen Daten maximiert wird.
Privacy by Design	Privacy by Design bezieht sich auf den Entwicklungsprozess einer Software, eines Betriebssystems oder einer Firmware und legt fest, dass Sicherheitskriterien zum Schutz von Know-how und personenbezogenen Daten in den verschiedenen Entwicklungsschritten mit einfließen müssen.
Eigenverantwortlichkeit jedes Mitarbeiters	Den Bildschirm zu sperren, wenn ein Mitarbeiter in die Pause geht, oder sensible Informationen nicht auf dem Arbeitsplatz liegen zu lassen, gehören genauso zu den Verantwortlichkeiten eines Mitarbeiters wie der verantwortungsbewusste Umgang mit Daten und Gerätschaften.

Wie die meisten Regeln haben sich auch diese im Laufe der Zeit herausgebildet und wurden schlussendlich als notwendig anerkannt. Um allgemeingültig anwendbar zu sein, müssen sie schon per se auf einer höheren Abstraktionsebene angesiedelt sein. Trotzdem fällt es leicht, sich für jedes Prinzip einen Anwendungsfall vorzustellen.

1.8 Umfang des IT-Security-Managements

Das IT-Security-Management ist eine umfangreiche Disziplin, die alle Ebenen und Teilbereiche der IT-Security beinhaltet. Es umfasst zahlreiche technische und organisatorische Aspekte, die bei vielen Gelegenheiten ineinander über-

greifen. In Abbildung 1.2 werden viele dieser Aspekte genannt. Eine vollständige Übersicht aller Arbeitsgebiete wird sich allerdings erst im Laufe der Ausgestaltung der Arbeit eines jeden einzelnen Managers IT-Security herauskristallisieren.

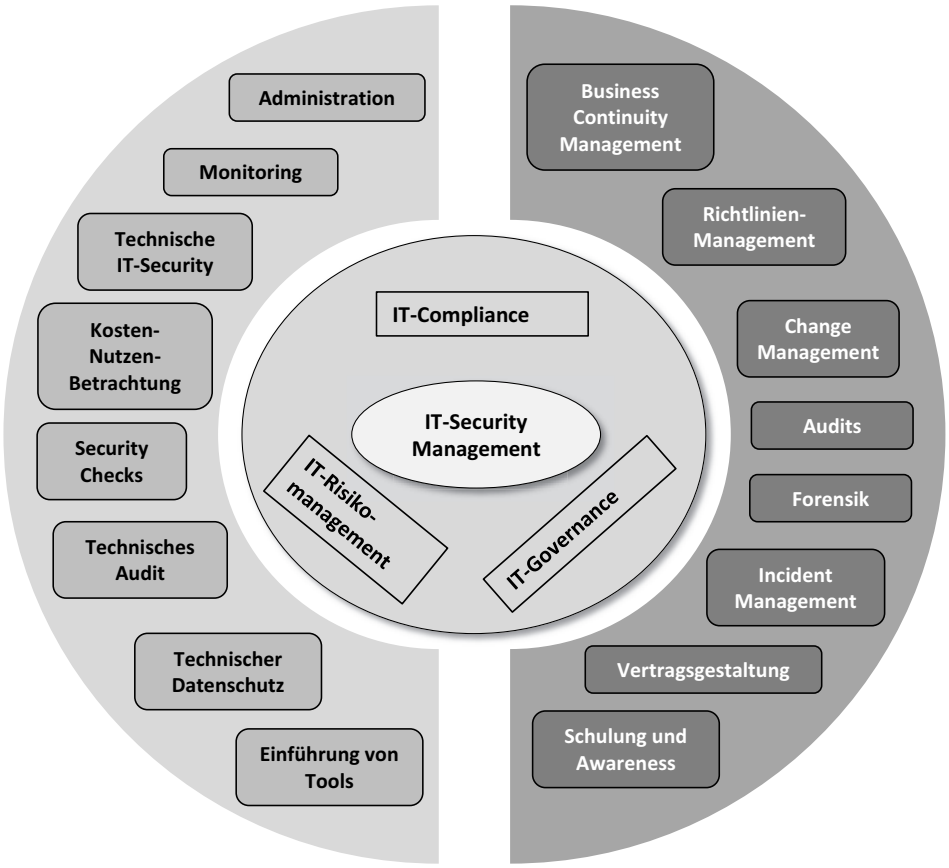


Abbildung 1.2: Aufgabenspektrum des Managers IT-Security

Die Pfeiler des IT-Security-Managements sind die Kernkomponenten IT-Compliance, IT-Risikomanagement und IT-Governance. Sie unterteilen die IT-Security in die drei maßgeblichen Sektoren. Im folgenden Abschnitt wird darauf detaillierter eingegangen. Das Spektrum an Aufgaben, denen sich ein Manager IT-Security stellen muss, ist sehr umfangreich, hat viele Schnittstellen und ist zudem in ständiger Veränderung begriffen. Jede Änderung von

Technologien erzeugt automatisch neue Aspekte, die daraufhin in verschiedenen Teilbereichen ihren Niederschlag finden. Auf strategischer Ebene beantworten die Pfeiler der IT-Security die Fragen: »Warum machen wir IT-Security?«, »Wer ist mit IT-Security-Themen befasst?« und »Wie setzen wir IT-Security um?« Wenn diese Fragen beantwortet sind, wird sich das weitere Tagesgeschäft in den Teilbereichen abspielen, die im äußeren Kreis in Abbildung 1.2 gezeigt werden.

Jeder Teilbereich hat Schnittstellen zu anderen Teilbereichen und es ist wichtig, die Zusammenhänge zu kennen. So macht die Erstellung von Richtlinien ohne die Überprüfung im Rahmen von Audits keinen Sinn, die Erstellung von Notfallplänen ohne vorhergehendes Risikomanagement ist uneffektiv, ein Monitoring ohne Mechanismen, auf Ereignisse zu reagieren, ist zwecklos oder die Implementierung von Maßnahmen ohne Feststellung, auf welche Bedrohungen sie eine Antwort finden sollen, ist ziellos. Das stellt die Verantwortlichen vor die Herausforderung, dass es nicht genügt, nur einen Teilbereich zu beherrschen, sondern dass auch die Wechselwirkungen bekannt sein müssen, um im Zweifelsfall die richtige Vorgehensweise wählen zu können.

1.8.1 Pfeiler der IT-Security

Der Aufgabenbereich der IT-Security ist groß, unübersichtlich und wird häufig von verschiedenen Managementstufen aus auch unterschiedlich gesehen. Ein Geschäftsführer will sicher schlafen können, ohne Angst haben zu müssen, dass wichtiges Know-how des Unternehmens bei der Konkurrenz landet. Der Datenschutzbeauftragte benötigt den Manager IT-Security, um technisch-organisatorischen Maßnahmen adäquat umzusetzen. Erst dadurch kann er seinen im Bundesdatenschutzgesetz-Neu formulierten Aufgaben gerecht werden. Für den IT-Leiter ist der Manager IT-Security die Person, die zum einen juristischen und technischen Ärger fernhält, auf der anderen Seite aber auch alle sicherheitsrelevanten Maßnahmen anstößt und lenkt. Für den Budgetverantwortlichen stehen die Kosten im Vordergrund, die auch dann auflaufen, wenn nichts Greifbares geschieht, die Aufgabe also wirksam verrichtet wird. Diese zahlreichen Anforderungen stehen einer häufig schwammigen Arbeitsplatzbeschreibung entgegen, und dabei den Überblick zu behalten, ist oft nicht leicht. Aus diesem Grund gibt es das IT-Security-Management, das die tragenden Säulen der IT-Security benennt und mit Leben füllt.

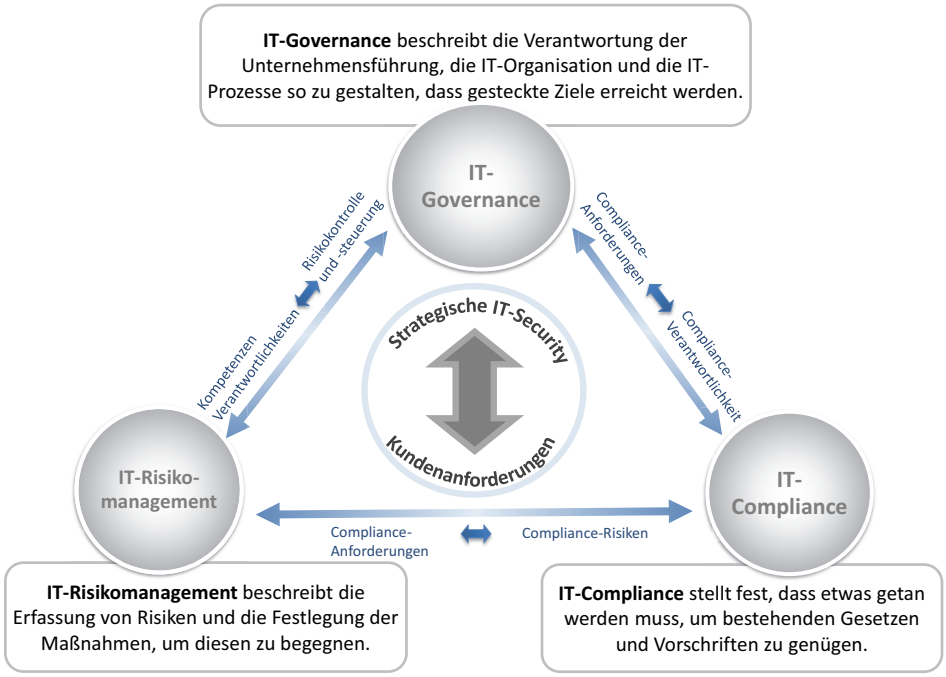


Abbildung 1.3: Spannungsfeld der IT-Security

Drei grundsätzliche Teilbereiche setzt das IT-Security-Management auf strategischer Ebene den eben aufgeführten Schwierigkeiten entgegen:

- das IT-Risikomanagement,
- die IT-Compliance
- und die IT-Governance.

Alle drei Sektoren werden vom Manager IT-Security bearbeitet, sofern sich die Prozesse und Inhalte mit dem Schutz von Informationen beschäftigen. Die Reihenfolge wurde bewusst so gewählt, und es ist gewollt, dass die drei Begriffe als gleichberechtigte Komponenten eines Vorgehensmodells verstanden werden.

Der Manager IT-Security wird sich immer mit diesen drei Sektoren beschäftigen müssen, sofern es keine Organisationseinheiten gibt, die das eine oder andere Feld bereits bearbeiten und auch die Belange der IT-Security mit betrachten. Die jeweilige Gewichtung wird individuell entschieden werden müssen und hängt von vielen Faktoren ab. Zum einen kommt es vor, dass der Manager IT-Security ein bereits existierendes Vorgehensmodell nur modifi-

zieren muss, und zum anderen werden Aufgaben, die z.B. die Verteilung von Aufgaben und Kompetenzen betreffen, außerhalb der IT-Security getroffen und spielen damit direkt in das Feld der IT-Governance hinein. Existiert ein funktionierendes IT-Risikomanagement, angesiedelt z.B. innerhalb des IT-Controllings, dann wird es sinnvoll sein, die dort gelebten Vorgehensmodelle anzupassen oder zu übernehmen. Das Gleiche gilt für das Themengebiet IT-Compliance: Werden die Vorgaben und Regelungen aus Vorschriften oder Gesetzen, die für IT gelten, bereits von einer Rechtsabteilung untersucht, dann wird dies nicht mehr gesondert im Rahmen des Arbeitsplatzes IT-Security erforderlich sein. Die Erfahrung zeigt allerdings, dass dies in den wenigsten Fällen zutrifft.

In die richtige Reihenfolge gebracht beantworten die drei strategischen Sektoren die wichtigsten Fragen der IT-Security. Natürlich wäre es zu kurz gedacht, wenn man die IT-Security darauf beschränken würde. Das liegt schon daran, dass ein Manager IT-Security abhängig davon, in welchem Unternehmensbereich er organisatorisch tätig ist, häufig auch Bereiche bearbeitet, die aus diesem Schema herausragen. Dazu gehören Felder wie das IT-Controlling oder gar die Aufgabe, den Datenschutzbeauftragten zu unterstützen, die immer häufiger mit in das Aufgabenfeld des Managers IT-Security eingebracht werden und weitergehende Qualifizierungen erfordern.

IT-Compliance

Die IT-Compliance beantwortet die Frage: **»Was muss getan werden?«**

Im Rahmen der IT-Compliance wird definiert, was und warum eine Aufgabenstellung in der IT-Security angepackt werden muss. Dies wird durch eine Vielzahl von Gesetzen, internen Regelungen und die Hauptaufgabe des Schutzes des internen Know-hows flankiert.

Im Kapitel »IT-Compliance« werden einige, von außen herangetragene Anforderungen exemplarisch aufgeführt, aber sie bilden dennoch nur einen Teil der existierenden Richtlinien ab. Das Spannungsfeld, in dem sich ein Unternehmen befindet, ist äußerst vielschichtig und durch eine große Anzahl an verzahnten Abhängigkeiten geprägt. Jeder Vertrag mit einem Kunden, jede Änderung der Allgemeinen Geschäftsbedingungen und regelmäßige Gesetzesänderungen führen zu einem Geflecht, in dem es für den Manager IT-Security immer schwieriger wird, die jeweils für die Datensicherheit relevanten Vorgaben zu extrahieren.

Wichtig

Im Grunde lässt sich von den einzelnen Anforderungen ein Arbeitsplatzprofil für den Manager IT-Security ableiten. Was nur wieder auf die Grundaussage hinausläuft: Aus dem Bereich der IT-Compliance lässt sich ableiten, was zu tun ist. Da aber vor allem die gesetzlichen Vorgaben schwammig und damit interpretationsfähig sind, ist dieser Anhaltspunkt weniger hilfreich, als zunächst vermutet werden könnte. Aus diesem Grund schaut ein Manager IT-Security neben dem reinen Gesetzestext vor allem auch auf die entsprechenden Gerichtsurteile.

»Compliance« ist eine relativ neue Bezeichnung für ein sehr altes Thema. Schon zu Beginn der Zeiten, als die Großrechner die Rechenzentren in den Unternehmen bevölkerten, war das Thema »Umsetzung von Gesetzen« wie z.B. der Steuergesetzgebung ein Thema. Jahr für Jahr wurden die entsprechenden Lochkarten angepasst und die neuesten Steuerberechnungen elektronisch umgesetzt. Die Personalabteilung war schon in den 1980er Jahren (und in manchen Unternehmen schon Jahre davor) häufiger Gast in den IT-Abteilungen, um die jährlichen Veränderungen Compliance-gerecht umzusetzen. Vor den Computern, zu Zeiten der nichtdigitalen Buchhaltung, war es ebenso. Compliance und im IT-Umfeld die IT-Compliance sind ein Thema, das es gibt, seit die ersten Gesetze und Vorschriften auf Prozesse Einfluss nahmen, die durch die Datenverarbeitung unterstützt wurden.

Der Tenor der IT-Compliance-Themen der letzten Jahre hat sich verändert. Sie zielen immer mehr direkt auf den Schutz digitaler Daten ab. Im Zuge dieser Modernisierung werden Gesetze ersetzt oder überarbeitet. Diejenigen, die Vorschriften und Gesetze erstellen und in Kraft setzen, arbeiten parallel dazu auch an Methoden, die Umsetzung in den Unternehmen wie auch bei Privatpersonen zu überprüfen. Regelungen ohne Audit führen zu einem Laisser-faire-Verhalten, das sich der Staat nicht leisten will und kann. Die neue Flut an Regelungen und die immer tiefer gehende Überprüfung führten in den letzten Jahren zu einem gesteigerten Bewusstsein aufseiten der Unternehmen für die Wichtigkeit dieses Themas und halfen mit, die Renaissance des Begriffes »Compliance« zu forcieren.

Das kann einer der Gründe sein, warum viele Kommentatoren diesen Sektor als Oberbegriff für das gesamte Thema IT-Security sehen. Gleichgültig, wie man auch zu dieser Aussage steht, eine entscheidende Triebfeder ist sie allemal.

Index

C

D

I

K

S

Z