1 Einführung in die IT-Sicherheit

1.1 IT-Sicherheit und wie man sie erreicht

Die produktive Auseinandersetzung mit einem Thema, insbesondere wenn man Ratgeber oder Literatur dafür hinzuzieht, setzt immer ein gemeinsames Verständnis für die benutzten Begriffe voraus. Im vorliegenden Buch dreht sich alles um das Thema »IT-Sicherheit« und deshalb möchte ich voranschicken, was sich dahinter, meinem Verständnis nach, verbirgt. Im folgenden Kapitel werden zudem weitere Begriffe erläutert.

Zunächst muss deutlich gemacht werden, dass, wie in vielen anderen Fachgebieten auch, Themen aus verschiedenen Perspektiven und aus verschiedenen Motivationen heraus betrachtet werden können. So kann eine Person aus der Abteilung Firewall-Administration eine andere Definition des Begriffs »IT-Sicherheit« finden als ein Support-Mitarbeiter. Das ist zunächst kein Problem, da beide Gruppen ihre Aufgabe getrennt voneinander bearbeiten. Treffen sie aber in einem Projekt aufeinander, in dem es um den Aufbau von IT-Sicherheit geht, dann kann es schnell zu Missverständnissen kommen. So ist einzusehen, dass eine Aufgabe, wie die Konfiguration und Überwachung von Firewalls, Teil der IT-Sicherheit ist, genauso wie das Aufstellen und Betreiben von Computern. Wie diese jeweils zu gewichten sind und wie sie zusammenhängen, steht wiederum auf einem anderen Blatt. Insbesondere die Frage nach der Priorität führt zu Diskussionen, wenn es darum geht, Entscheidungen zu treffen und Geld zu investieren. In diesen fachlichen Auseinandersetzungen ist es die Aufgabe des Verantwortlichen für die IT-Sicherheit, formale Kriterien mit in die Diskussion zu tragen, auf deren Basis die richtigen Entscheidungen getroffen werden können.

Es ist hilfreich, noch mal einen Schritt zurückzutreten und den Begriff »IT-Sicherheit« möglichst unvoreingenommen zu betrachten. Um zu einer einheitlichen Definition zu kommen, ist der gemeinsame Nenner zu finden. Der einfachste gemeinsame Nenner ist die Definition, dass IT-Sicherheit immer die Abwesenheit von IT-Unsicherheit ist. Unsicherheit wird in diesem Zusammenhang mit dem Begriff »Gefahren« übersetzt. Die Abwesenheit von Gefahren ist demnach gleichzusetzen mit Sicherheit. Angenommen, man

übersetzt das Wort Gefahren mit einem Wort aus dem IT-Risikomanagement, und zwar dem Begriff »Bedrohung«, dann ist man noch ein bisschen näher am Wesen der IT-Sicherheit. Bedrohungen wiederum sind nur dann vorhanden, wenn es sowohl eine Schwachstelle gibt als auch eine Möglichkeit, diese auszunutzen. So ist ein Rechner unter Windows 8.1 auf Betriebssystem-Ebene nur dann einer Bedrohung ausgesetzt, wenn sowohl eine technische Schwachstelle, wie z. B. ein Programmfehler, existiert als auch ein Exploit, der diesen Fehler ausnutzen kann. Hat ein Hacker sowohl die Möglichkeit, zum Zielrechner vorzudringen, als auch den Exploit zur Verfügung, dann entsteht eine Bedrohung für diesen Rechner.

IT-Sicherheit ist also dann gegeben, wenn einem Angreifer entweder die Schwachstelle entzogen wird, z. B. durch Patchen des Rechners, oder aber die Möglichkeit zum Angriff über das Netzwerk, z. B. durch die Implementierung einer Firewall, entzogen wird.

Beide vorher genannten Gruppen arbeiten damit an verschiedenen Stellen am gleichen Ziel mit, und zwar parallel zueinander und gleichberechtigt. Um zu beantworten, was denn nun wichtiger ist, die Firewall oder das Patchen des PC, ist eine Rechnung aufzustellen, die die Faktoren »Bedrohung«, »Eintrittswahrscheinlichkeit der Gefährdung« und die dann entstehenden Kosten mit einbezieht. Ein solcherart errechnetes Risiko dient dann dazu, von subjektiven Meinungen zu objektiven Einschätzungen zu gelangen.

Hinweis

Die Abwesenheit von IT-Unsicherheit ist dann gegeben, wenn keine Schwachstellen oder keine Möglichkeiten, diese auszunutzen, vorliegen. Die IT-Sicherheit hat sich damit genau darum zu kümmern: Sie merzt Schwachstellen aus oder macht das Ausnutzen derselben schwierig oder gar unmöglich.

Um dies möglichst lückenlos zu bewerkstelligen, arbeitet die IT-Sicherheit wie ein Uhrwerk, in dem zahllose kleine Zahnrädchen im Gleichtakt ticken. Fällt ein Zahnrädchen aus, so kann das Gesamtsystem bereits kompromittiert werden. Damit dies nicht unbemerkt passiert, gibt es IT-Sicherheitsprozesse und Regelwerke. Die Prozesse legen Vorgehensweisen fest und sollen damit verhindern, dass das Uhrwerk aus dem Takt gerät, wenn eine Stelle von der korrekten Vorgehensweise abweicht.

Ein Beispiel wäre die Aufstellung eines Windows-8.1-Rechners ohne Sicherheits-Patches. Die Aufgabe der IT-Sicherheitsprozesse wäre es in diesem Fall, ein solches Vorgehen von vornherein als regelwidrig zu entlarven und, wenn möglich, komplett zu unterbinden. Das Regelwerk legt dazu die Rahmenbedingungen fest und dient im Nachhinein als Vorlage für eine Überprüfung der IT-Systeme im Rahmen eines Audits.

Ein weiterer Gedanke wäre, auch wenn es sich zunächst wie eine zu kurz gedachte Methodik anhört: Sicherheit ist durchaus auch dann gegeben, wenn das Asset, das schützenswert ist, vom potenziellen Angreifer nicht gesehen werden kann. Im Englischen spricht man dann von der fehlenden »visibility«. Das macht keinen Sinn, wenn man Daten vor dem Mitarbeiter schützen möchte, der das Unternehmen verlassen wird und gerne die Daten mitnehmen würde. Aber schon, wenn es darum geht, IT-Systeme zu benennen, zeigt sich der Nutzen. Warum soll man den Server mit den kritischen Daten denn »Berlin-SRV-Prod-Daten« nennen? Viel zu viele Informationen werden alleine schon mit der Bezeichnung an den potenziellen Angreifer weitergegeben. So ist dessen Standort vermutlich in Berlin zu verorten, produktive Daten sind darauf gespeichert und es handelt sich bei dem System um einen Server. Praktisch für den Administrator, kontraproduktiv hinsichtlich der IT-Sicherheit.

Aus den bislang gewonnenen Erkenntnissen kann man nun schlussfolgern, dass ein Unternehmen Sicherheit für die zu schützenden Assets entweder dadurch erreicht, dass es die Bedrohungen für das jeweilige Asset beseitigt oder aber das Asset von den Bedrohungen trennt. Ein Server, der in einem Raum mit einer Tür ohne Verriegelung untergebracht ist, kann also entweder durch das Einsetzen einer vernünftigen Schließanlage gesichert werden oder aber dadurch, dass man ihn in einem entsprechenden Computerraum mit sinnvollem Zugangsschutz verlegt. Diese Maßnahme schützt den Server dann gegen genau diese eine Bedrohung. Eine weitere, mögliche Bedrohung, nämlich dass jemand über das Netzwerk unbefugten Zugang erhält, bleibt dabei zunächst außen vor. Anhand dieser Beispiele ist schnell zu erkennen, dass die Schaffung von IT-Sicherheit in den meisten Fällen nur durch die Umsetzung einer ganzen Reihe von Maßnahmen, die verschiedene Perspektiven abdecken, zu erreichen ist.

Hinweis

Die Kunst der IT-Sicherheit besteht darin, die Gefährdungen, denen die IT-Systeme und Daten ausgesetzt sind, möglichst aus den verschiedensten Perspektiven zu betrachten und dann diejenigen Maßnahmen auszuwählen, die unter Berücksichtigung von Kosten und Nutzen den meisten Erfolg im Zusammenspiel versprechen. Dieser Gedanke muss in allen Phasen des Projekts und später auch im Betrieb der IT-Sicherheit im Vordergrund stehen.

Ein paar Worte noch zum eben erwähnten »Zusammenspiel von Maßnahmen«. Nicht jede Maßnahme, die für sich selbst gesehen das Risiko für ein Asset verringern kann, muss auch im Gesamtkontext gesehen eine gute Wahl darstellen. So ist es durchaus denkbar, dass gerade durch die Implementierung einer eigentlich sinnvoll erscheinenden Maßnahme neue Verwundbarkeiten erst entstehen. So gibt es ein Beispiel aus der Vergangenheit, bei dem die Installation eines Antivirenprogramms zwar zunächst dabei geholfen hat, Viren auf Client-Computern zu entdecken und zu löschen, aber auf der anderen Seite hatte die Applikation selbst wiederum Schwachstellen, die ausgenutzt werden konnten, den Zielrechner, mit lokalen Administrationsrechten ausgestattet, zu übernehmen. Es wurden dann zwar bald Updates bereitgestellt, diese wurden aber nicht automatisch installiert, sondern mussten von Hand eingespielt werden. Eine Implementierung eines solchen Programms ohne flankierende Maßnahmen, die sich um das Patchen der Anwendung selbst kümmern, führte damit zu einem erhöhten Risiko.

1.2 Wichtige Begriffe

Wie viele andere Fachbereiche auch hat die IT-Sicherheit eine ganze Reihe an Begriffen geprägt, die sich in den letzten Jahren zunehmend durchgesetzt haben. Die meisten davon werden von englischen Worten abgeleitet, manchmal existieren sie auch nur in dieser Sprache, sie wurden neu geprägt oder ganz und gar neu erfunden. Aus diesen Gründen kann es durchaus dazu kommen, dass ganze Vorgaben und Ziele aufgrund einer missverständlichen Wortwahl unverständlich bleiben oder in einer kontroversen Diskussion zerpflückt werden. Das ist der eine Grund, warum ich an dieser Stelle mein Verständnis der wichtigsten Begriffe erläutern möchte.

Hinweis

Die eben kurz angerissene Unschärfe mancher Begriffe zeigt schon auf, dass es für ein Unternehmen durchaus Sinn macht, speziell hierfür ein Dokument anzulegen, in dem zumindest diejenigen (Fach-)Begriffe erläutert werden, die in den eigenen Richtlinien, Präsentationen oder in der täglichen Kommunikation verwendet werden.

Der andere Grund ist schlicht der, dass nicht jeder, der vor die Aufgabe gestellt wird, ein Projekt dieser Art zu leiten oder zu begleiten, automatisch auch ein Experte für IT-Sicherheit sein muss. Der Weg dorthin ist lang und steinig und das Nahebringen der wichtigsten Fachbegriffe kann man auch als kleinen Einführungskurs betrachten, mit der Aufgabe, ein paar Abkürzungen einzubauen.

1.2.1 Normenreihe ISO 2700x und Dokumente des BSI

Es ist immer sinnvoll, etwas als Grundlage zu nutzen, das bereits, am besten international, als gutes Vorgehensmodell akzeptiert wird. In der IT-Sicherheit stellt sich diese Grundlage unter anderem als eine Reihe von ISO-Standards dar, die auch bereits in die DIN-Normenreihe übernommen wurden. Diese Standards bilden alle wesentlichen Aspekte der IT-Sicherheit ab und bestehen zum Teil bereits seit vielen Jahren im Markt. Das heißt, ihre Bestandteile bilden nicht nur ein rein akademisches Grundwissen ab, sondern sind bereits in der täglichen Praxis erprobt.

Hinweis

Auch wenn die Normen wichtig sind, ist deren Kenntnis keine Grundvoraussetzung, das IT-Sicherheitsprojekt zu einem erfolgreichen Ergebnis zu führen.

Für das IT-Sicherheitsprojekt sind die Normen ISO 27001 und 27002 am interessantesten. Die Norm ISO 27005, die sich um das Thema Risikomanagement kümmert, bildet einen weiteren Pfeiler, der in einigen wichtigen Prozessen eine Rolle spielt, und die ISO 27035 beschreibt die Funktion und den Aufbau eines sogenannten CERT – dazu mehr in späteren Abschnitten.

Neben den eben genannten Normen hat auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) einige sehr wichtige Dokumente veröffentlicht, die auf die Herausforderungen Bezug nehmen, denen wir uns im Projekt gegenübersehen werden. In den entsprechenden Abschnitten verweise ich dann jeweils auf die wichtigsten Quellen und gebe dem Leser dann die Möglichkeit, sein Wissen zu vertiefen. Die Kenntnisse, die man aus diesen Leitfäden herauslesen kann, sind wichtig, um Regelungen und Vorgaben in unternehmerischen Alltag einzuführen und zu betreiben.

1.2.2 Information-Security-Management-System

Die ISO 27001, auf die immer wieder referenziert wird, wenn es um IT-Sicherheit geht, trägt den Begriff »Information-Security-Management-System«, abgekürzt ISMS, bereits prominent im Titel. Des Weiteren wird es im Rahmen der Norm folgendermaßen definiert:

> *Teil des gesamten Managementsystems, der auf der Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung der Informationssicherheit abdeckt.*

Auch wenn es sich etwas kryptisch anhört, bietet diese Definition doch einige gute Anhaltspunkte. Zum einen geht es hier nicht um etwas völlig Neues. Es kann als Teil eines in einem Unternehmen bereits gelebten Managementsystems, wie es z. B. ein Qualitätsmanagement-System vorgibt, implementiert werden und damit auf vorhandenen Prozessen aufsetzen. Der Gedanke der stetigen Verbesserung im Rahmen eines Zyklus wird bereits in solchen Systemen aktiv angewandt.

Ein ISMS bezieht sich nicht auf ein bestimmtes Unternehmensfeld oder eine definierte Unternehmensgröße. Daraus kann man ableiten, dass sich nicht ein Unternehmen verbiegen muss, um einem ISMS gerecht zu werden, sondern ganz im Gegenteil, ein ISMS muss so adaptierbar sein, dass es auf die Unternehmenswirklichkeit angepasst werden kann. Natürlich unter der Prämisse, dass der Sinn, ein höheres Sicherheitsniveau zu erreichen, nicht verfehlt wird.

Des Weiteren ist der Risikomanagement-Ansatz zu nennen. Dieser wird uns auch im IT-Sicherheitsprojekt immer begleiten, auch wenn er hier nicht die Detailschärfe erreichen wird, wie es in den Normen eigentlich verlangt wird.

Dies liegt vor allem daran, dass das Ziel eines umfassenden und tragfähigen Sicherheitskonzepts zwar nicht ohne Einbezug eines IT-Risikomanagements erreichbar ist, das Ziel aber, wirklich alles danach auszurichten, würde den Umfang dieses Projekts zu stark erweitern und wäre demnach kontraproduktiv. Aus diesem Grund wird auch immer wieder von der »Basissicherheit« und einer »angestrebten Sicherheit« die Rede sein. Beides liegt auf dem gleichen Weg, wenn auch die »angestrebte Sicherheit« einiges mehr an Aufwand erfordert. Davon aber später mehr.

Ansonsten gilt das, was Bruce Schneier, der Experte für umfassende IT-Sicherheit schlechthin, bereits vor einigen Jahren treffend formuliert hat: IT-Sicherheit ist keine bestimmte Software oder eine einzelne gezielte Maßnahme, sondern ein Prozess, der sich immer weiter verbessert. Daraus abgeleitet ist ein angestrebtes Niveau an IT-Sicherheit nicht dadurch zu erreichen, dass nur ausgewählte Sicherheitsthemen, wie das Patchmanagement oder die Firewall-Betreuung, ausgebaut werden, es ist immer darauf zu achten, dass alle Felder der IT-Sicherheit Beachtung finden und in ein übergreifendes Kontrollsystem eingebunden werden. Diese Betrachtung fasst die Definition eines ISMS, denke ich, am besten zusammen.

1.2.3 IT-Sicherheitsorganisation

In Bezug auf ein Unternehmen oder eine Behörde umfasst die IT-Sicherheitsorganisation alle Stellen, die sich mit dem Schutz der Vertraulichkeit, Verfügbarkeit und Integrität von Daten, und im weiteren Sinne von Informationen, auseinandersetzen. Zu klären sind die Schnittstellen zwischen Organisationseinheiten wie z. B. dem Werkschutz, der das Rechenzentrum, als Teil eines Gebäudes, schützt, und dem IT-Sicherheitsmanager, der parallel dazu auch für den physischen Schutz des Rechenzentrums verantwortlich sein kann.

Sind in einem Unternehmen für die operative IT-Sicherheit und das IT-Sicherheitsmanagement unterschiedliche, kaum organisatorisch miteinander verbundene Organisationseinheiten zuständig, so kann sich der Gesamtkomplex »IT-Sicherheitsorganisation« dennoch über alle diese Stellen erstrecken. In diesem Fall ist es entscheidend, entsprechende übergreifende Prozesse und Kommunikationsbeziehungen aufzusetzen.

Es ist unerheblich, ob ein Unternehmen eine umfangreiche IT-Sicherheitsorganisation mit vielen Mitarbeitern unterhält oder ob eine einzelne Person diese Aufgabe wahrnimmt, die Vernetzung zu anderen Einheiten wie die IT-

Abteilung, zur Personalabteilung, zum Werkschutz, zum Betriebsrat und zum Datenschutzbeauftragten ist von kritischer Wichtigkeit, um die Effizienz über eine sinnvolle Durchdringung zu steigern.

1.2.4 Unternehmenswerte

Das Wort »Werte« leitet sich von dem englischen Begriff »assets« ab, der in der Norm ISO 27001 entscheidend geprägt wird. Dort steht, dass unter »Werten« alles zu verstehen ist, was für ein Unternehmen von Wert ist. Zunächst einmal hört sich dies wie eine Binsenweisheit an. Auf den zweiten Blick wird aber auch deutlich, dass wir von viel mehr reden als nur Daten auf Servern. Kritische Informationen können auf verschiedensten Wegen und auf verschiedenen Medien im Unternehmen kursieren. Dazu kommt, dass Daten nicht im luftleeren Raum existieren können und damit ist auch immer die Infrastruktur mit einzubeziehen. Zu guter Letzt ist zu bedenken, dass der Verlust von Informationen auch weitreichende Folgen für Werte haben kann, die man zunächst nicht auf dem Schirm hat. Dies hat vor Kurzem ein großes Unternehmen erfahren müssen, als Kreditkartendaten der Kunden »verloren gegangen« sind. Auf einen Schlag kann in einem solchen Fall die Reputation unwiderruflich beschädigt werden. Die IT-Sicherheitsorganisation wiederum hat die Aufgabe, direkt oder auch indirekt, diese Werte zu schützen. Sinnvollerweise sind dabei vor allem folgende Werte zu betrachten:

- Informationen in Form von **Daten:** Darunter fallen alle Arten von Daten. Diese können sich unter vielen anderen Ausprägungen auf Datenservern, Datenbanken, auf Netzwerkkomponenten oder auch auf Wechseldatenträgern befinden.
- Informationen in Form von **Dokumenten:** Hierunter fallen alle Informationen, die z. B. in Verträgen, Gesprächsnotizen, Besprechungsprotokollen, Handbüchern, E-Mails, auf Flipcharts oder in Aktenordnern abgelegt sind.
- **Physische Werte:** Darunter fällt die Hardware des Unternehmens – also alle Arten an Rechnern, Servern, Netzwerkkomponenten, die Verkabelung, aber auch Datenträger wie DVDs oder Backup-Medien wie Bandkassetten.
- **Software:** Neben Anwendungsprogrammen sind hier vor allem Applikationen zur Softwareentwicklung und die Betriebssysteme von Computern oder Netzwerkkomponenten gemeint.

- **Dienstleistungen:** Das Rechenzentrum ist ein typisches Beispiel für eine Infrastruktur, für die Dienstleistungen erbracht werden. Innerhalb des Rechenzentrums arbeiten interne und externe Stellen, um z. B. die unterbrechungsfreie Stromversorgung, die Installationen zur Bekämpfung von Feuer oder Wasser, den Aufbau von Serverschränken oder auch eines doppelten Bodens zu initiieren oder zu betreiben.
- **Mitarbeiter:** Mitarbeiter haben Qualifikationen und Fähigkeiten, die im Grunde einen großen Teil des Know-hows des Unternehmens darstellen.
- **Immaterielle Werte** wie der Ruf eines Unternehmens, der unter einem Sicherheitsvorfall leiden könnte.

Manche dieser Werte werden gedanklich automatisch mit der IT-Sicherheit verknüpft, da es sich um klassische Werte handelt, die etwas mit elektronischen Daten oder Computerhardware zu tun haben. Andere Werte wiederum, wie z. B. die Kostenkalkulation auf einem Flipchart, werden zwar als schützenswert wahrgenommen, aber eher in der Verantwortung des Einzelnen gesehen. Aus Sicht der ISO-27002-Norm ist es unerheblich, in welcher Form Informationen bewahrt oder dargestellt werden, und dementsprechend behandeln wir auch die Werte des Unternehmens im IT-Sicherheitsprojekt.

1.2.5 Dateneigentümer und Risikoeigentümer

Der Dateneigentümer (*data owner*) ist für einen bestimmten Teil der Unternehmensdaten verantwortlich. Darunter fallen vor allem die durch ihn selbst erstellten und verwalteten Daten. Damit folgt man dem Gedanken, dass derjenige, der Daten erfasst oder erzeugt, auch am besten darüber entscheiden kann, welchen Schutzbedarf diese Daten haben und, davon abgeleitet, wie diese Daten sicher gehalten werden sollten. Damit ist der Dateneigentümer der erste Ansprechpartner, wenn es darum geht, den Schutzbedarf von Daten zu bestimmen, Risiken zu bewerten oder Maßnahmen zur Risikoverringerung abzuschätzen.

Im Rahmen der IT-Sicherheit führte eine solche Vorgehensweise aber auch dazu, dass es mit steigender Komplexität und einer steigenden Masse an Daten immer schwieriger wird, den Dateneigentümer zu bestimmen. Oftmals war der Dateneigentümer, aus seiner Rolle im Unternehmen heraus, nicht in der fachlichen Position, die damit verbundenen Aufgaben wahrzunehmen. Das sind zwei der Gründe, warum mit der überarbeiteten Version

der ISO 27001:2013 der Risikoeigentümer (*risk owner*) eingeführt wurde. Damit wird die Verantwortung für Daten wieder mehr in die Richtung der Führungskräfte gelenkt.

1.2.6 Asset-Management

Im Zusammenhang mit den Unternehmenswerten ist auch oft von einem »Asset-Management« die Rede. Wieder ein Begriff, bei dem es fast keinen Sinn macht, ihn ins Deutsche zu übersetzen. Das Asset-Management besteht aus einem systematischen Prozess, der die Aufgabe hat, Assets, also Unternehmenswerte, zu erfassen und zu verwalten. Der Prozess reicht in Form eines sogenannten »Lebenszyklus« dabei von der Anschaffung, über die Inbetriebnahme, die Wartung, den Vorgang der Erweiterung bis hin zur Entsorgung oder dem Verkauf. Es ist offensichtlich, dass dieser Prozess nicht auf alle, in Abschnitt 1.2.4 genannten, Werte angewendet werden kann.

Hinweis

In den meisten Unternehmen existiert bereits ein Datenpool, der viele Arten an Werten auflistet. Dies ist der Fall, da viele dieser Informationen, unter anderen was die Hardware und Software angeht, auch von anderen Bereichen, wie z. B. der Buchhaltung zu Abschreibungszwecken oder der IT zur Planung, benötigt werden. Es kann durchaus Sinn machen, diese Datenbank für die eigenen Zwecke mit zu benutzen. Um damit sinnvoll arbeiten zu können müssen oft weitere Arten an Werten, wie z. B. Daten, hinzugefügt werden und dann noch den entsprechenden Systemen zugeordnet werden. Es geht also oft nicht um die Neuentwicklung des Rades, sondern darum, herauszufinden, wo die benötigten Informationen im Unternehmen zu finden sind und wie sie genutzt werden können, um im Rahmen eines Information-Security-Management-Systems als Datenbasis zu dienen.

Aus den eben beschriebenen Bestandteilen eines solchen Prozesses lassen sich entsprechende, erforderliche Eigenschaften ableiten, die ein Asset-Management-System erfüllen sollte. Aus Sicht der IT-Sicherheit sind die nachfolgenden Eigenschaften relevant und sollten in jedem Fall erfasst werden:

- Jeder Unternehmenswert hat einen Eigentümer (*data owner*) . Dieser heißt auch Dateneigentümer oder Informationseigentümer.
- Unternehmenswerte müssen zunächst identifiziert, also als solche erkannt werden, bevor sie sinnvoll geschützt werden können. Dazu kommt, dass jeder Unternehmenswert entsprechend gekennzeichnet bzw. dokumentiert sein sollte.
- Jeder Unternehmenswert hat einen bestimmten monetären Wert. Da dieser in den allermeisten Fällen nicht auf den Euro bekannt ist, kann eine vereinfachte Einteilung Sinn machen. So könnte eine Einschätzung des Werts zwischen 1 Euro und 5.000 Euro als »niedrig« angelegt werden und so weiter. Diese Thematik wird im Zusammenhang mit der Klassifizierungsrichtlinie vertieft. Es ist wichtig, dass man immer im Hinterkopf behält, dass der Aufwand, den man zum Schutz eines Unternehmenswertes aufbringen sollte, vom jeweiligen (z. B. monetären) Wert bzw. der Einstufung zwischen »niedrig« und »sehr hoch« abhängt.
- Wie mit einem Unternehmenswert umgegangen werden soll, wird in den entsprechenden Richtlinien festgelegt.

Im Rahmen der IT-Sicherheit ist nicht nur der jeweilige Wert als Teil des Asset-Managements als solcher wichtig, sondern auch eine Reihe seiner Attribute. So hat der Wert »Server A« Attribute wie eine Netzwerkadresse und einen Standort. Genauso aber auch Eigenschaften wie einen Patchstand oder eine Version des darauf installierten Virenscanners. Gerade diese Eigenschaften sind für die IT-Sicherheit wichtig und stellen einen wichtigen Eckpfeiler der Aufgabe, Transparenz zu schaffen, dar.

1.2.7 Schutzbedarf, Schutzziele, Schutzstufen und die Klassifizierung

In der IT-Sicherheit dreht sich alles darum, Unternehmenswerte zu schützen. Gegen was genau und in welchem Ausmaß etwas zu schützen ist, beschreibt der **Schutzbedarf**. Im Zuge der Schutzbedarfsfeststellung wird dabei der Grad des erforderlichen Schutzes definiert. So kann dabei z. B. herauskommen, dass der Unternehmenswert »CAD-Zeichnung Prototyp« sehr stark gegen das Einsehen durch nicht autorisierte Personen geschützt werden muss. Der Schutzbedarf hinsichtlich dieses **Schutzziels** wäre daraus abgeleitet z. B. »sehr hoch«.

Die Schutzziele beschreiben diejenigen Ziele, die definieren, hinsichtlich was ein Wert zu schützen ist. Zu den bekanntesten Schutzzielen gehören die folgenden drei:

- **Vertraulichkeit** (*confidentiality*): Die Vertraulichkeit des Unternehmenswerts, z. B. einer Information, wird geschützt. Anders ausgedrückt: Informationen werden nur dafür autorisierten Subjekten, wie Personen, Prozessen oder Applikationen, zugänglich gemacht.
- **Integrität** (*integrity*): Unternehmenswerte, wie Informationen, werden vor nicht autorisierten Änderungen geschützt. Das spielt z. B. dann eine große Rolle, wenn diese Informationen in einer Datenbank abgelegt sind und es ausdrücklich gewünscht ist, dass nur befugte Personen oder Prozesse Änderungen an diesen Daten, wie z. B. dem Monatsgehalt der Mitarbeiter, vornehmen können.
- **Verfügbarkeit** (*availability*): Unternehmenswerte, wie Server oder auch Daten, stehen dafür autorisierten Benutzern oder auch IT-Systemen zur Verfügung. Dabei handelt es sich um ein eher technisches Schutzziel, das im Gegenzug leichter überprüfbar und definierbar ist, wie z. B. in Service Level Agreements (SLAs).

Die genannten drei Schutzziele sind die sogenannten »klassischen Schutzziele«. Im Englischen hat sich die Abkürzung »CIA« eingebürgert, ein Begriff, der sich aus den ersten Buchstaben der Worte *confidentiality, integrity* und *availability* zusammensetzt. Neben diesen Schutzzielen ist eine beliebige Anzahl weiterer Schutzziele denkbar, an denen ein Unternehmen die Strategie zum Schutz der Unternehmenswerte ausrichten kann.

Es ist nicht ganz leicht, den Schutzbedarf mathematisch exakt zu definieren. Aus diesem Grund bedient man sich häufig einer gewissen Unschärferegelung und unterteilt den Schutzbedarf in gröbere **Schutzstufen**. So würde es sich anbieten, den oben genannten Unternehmenswert »CAD-Zeichnung Prototyp« in eine von, sagen wir, drei Stufen einzuordnen. Diese Stufen könnten von »Niedrig« über »Mittel« bis »Hoch« reichen. Jede dieser Stufen muss dabei hinreichend definiert werden, um dem Dateneigentümer und allen, die eine solche Einschätzung vornehmen müssen, die Möglichkeit zu bieten, dieses System anzuwenden. So könnte die mittlere Schutzstufe so definiert sein: Bei Verlust der Vertraulichkeit würde ein größerer Schaden, maximal 100.000 Euro auftre-

ten. Damit verbindet man die Schutzstufe mit einer Schadensumme zur besseren Handhabung. Im Abschnitt, der sich um die Erstellung der Klassifizierungsrichtlinie dreht, wird dieser Vorgang noch detaillierter erläutert.

In der **Klassifizierungsrichtlinie** finden die Schutzbedarfe, die Schutzstufen und deren Beschreibung wieder zusammen. Sie definiert, wie ein Unternehmenswert zu klassifizieren ist, und stellt damit eine wichtige Grundlage für das Risikomanagement dar, denn ein hoher Schutzbedarf ist einem großen monetären Verlust bei Eintritt des Risikos gleichzusetzen und daraus folgt eine hohe Risikoeinstufung.

1.2.8 Risiko, Risikoberechnung, Risikobehandlung und Maßnahmen

Mit der Berechnung des Risikos für eine mögliche Verletzung eines Schutzziels visualisiert man die Höhe einer Gefährdung und macht sie dadurch erst handhabbar. Anders ausgedrückt: Der Eintritt eines Risikos verhindert die Erreichung eines Schutzziels und mithilfe der Risikoberechnung wird das Risiko des Eintretens quantifiziert. So kann man z. B. berechnen, wie hoch das Risiko ist, dass das Schutzziel Vertraulichkeit bezüglich einer CAD-Zeichnung nicht erreicht wird. Für diese Berechnung benötigt man die Werte von drei Variablen, wobei ich hier von einer recht einfachen von vielen möglichen Arten der Risikoberechnung ausgehe.

Die erforderlichen Variablen sind:

- **Eintrittswahrscheinlichkeit:** Mit welcher Wahrscheinlichkeit wird das Risiko tatsächlich eintreten?
- **Möglicher Verlust:** Welcher monetäre Verlust würde eintreten, falls das Risiko eintritt?
- **Maßnahmen, die das Risiko mindern** und die bereits umgesetzt wurden.

Die Berechnung lautet nun:

> *Risiko = (Eintrittswahrscheinlichkeit x Möglicher Verlust) – Mindernde Maßnahmen*

Ist es bereits im letzten Jahr zweimal vorgekommen, dass CAD-Zeichnungen gestohlen wurden, und lag der Schaden jeweils bei 10.000 €, dann wäre das

Risiko, vorausgesetzt es macht Sinn, diese Daten fortzuschreiben, und ohne den Einbezug von mindernden Maßnahmen:

$$2 \times 10.000\ € = 20.000\ €$$

Wurde in der Zwischenzeit aber als **Maßnahme** ein Sicherheitssystem eingeführt, das zu 50% einen solchen Diebstahl verhindern soll, dann würde sich das Risiko auf 10.000 € halbieren.

Das offensichtliche Problem bei solchen Berechnungen liegt in den vielen Annahmen, die zu treffen sind und die jeweils Schätzungen darstellen, die wiederum auf Erfahrungen aus der Vergangenheit beruhen. Dennoch ist es unabdingbar, in der IT-Sicherheit in Kategorien von Risiken und Maßnahmen zu denken.

Ist ein Risiko berechnet oder auch nur bekannt, dass es existiert und eine gewisse Schwere hat, dann existieren grundsätzlich vier verschiedene Möglichkeiten, damit umzugehen. Den Vorgang dazu nennt man die »**Risikobehandlung**«. Die Festlegung, wie mit Risiken umzugehen ist, ist eine typische Managementaufgabe.

Die vier gängigen Arten, mit einem bekannten Risiko umzugehen, sind:

- **Das Risiko kann eliminiert werden.** Ein riskanter Prozess wird ersetzt oder ein Betriebssystem, das nicht mehr mit Sicherheitsupdates versorgt werden kann, wird ersetzt.
- **Das Risiko wird akzeptiert und damit getragen.** Ein Risiko ist immer auch gleichzeitig eine Chance. So kann es unter Umständen unter dem Strich viel Geld sparen, ein Risiko zu akzeptieren und es hinzunehmen, statt es mit hohem Geldaufwand zu reduzieren oder zu eliminieren.
- **Ein Risiko kann aus dem eigenen Verantwortungsbereich heraus verlagert werden.** Dazu können z. B. entsprechende Versicherungen abgeschlossen werden, mit denen man sich z. B. gegen Angriffe von Hackern durch sogenannte »Cyber-Crime-Versicherungen« versichern kann.
- **In den häufigsten Fällen wird man ein aufgedecktes Risiko reduzieren wollen.** Durch eine oder mehrere entsprechende Maßnahmen wird die Eintrittswahrscheinlichkeit vermindert oder es werden entsprechende Maßnahmen umgesetzt, um den möglichen Schaden im Falle des Eintritts des Risikos zu reduzieren.

Maßnahmen werden in den verschiedenen Standards nach Kategorien gegliedert, um sie besser handhaben zu können. So werden die Maßnahmen aus Anhang A der ISO 27001 nach Maßnahmenzielen gegliedert und ihnen zugeordnet. Deren Sortierung erfolgt wiederum auf Ebene von Funktionsbereichen oder Themen. So gibt es Maßnahmen z. B. aus dem Bereich der Personalabteilung, der physischen Umgebung, der Zugangs- und Zugriffskontrolle oder auch der allgemeinen Sicherstellung des Geschäftsbetriebs.

Ein anderer Ansatz ist die Gliederung von Maßnahmen nach rein technischen Gesichtspunkten. Dies wird immer dann Sinn machen, wenn Maßnahmen tatsächlich in erster Linie dazu dienen, Gefahren für die Unternehmenswerte aufzuspüren, z. B. im Rahmen von Penetrationstests, und technisch zu lösen. In solchen Fällen lassen sich Maßnahmen z. B. Themenbereichen wie der Authentifizierung, Autorisierung, der Netzwerktrennung, der Verschlüsselung oder der Absicherung von Gerätschaften zuordnen. Im täglichen Betrieb der IT-Sicherheit ist dann zu beobachten, dass beide Ansätze, individuell von Unternehmen zu Unternehmen auf unterschiedliche Weise, miteinander verschmelzen.

1.2.9 Angriffspfad, Schwachstellen und Bedrohungen

Grundsätzlich gilt, dass ein System nur dann einer **Bedrohung** ausgesetzt ist, wenn es eine **Schwachstelle** hat und eine Möglichkeit existiert, diese auszunutzen. Schadcode, der dazu geeignet ist, eine vorhandene Schwachstelle für einen Angriff zu nutzen, nennt sich »Exploit«. So kann selbst ein Sicherheitsloch in einer Betriebssystemsoftware akzeptiert werden, falls es kein denkbares Mittel gibt (*exploit*), diese Schwachstelle auszunutzen. Dies kann z. B. dann der Fall sein, wenn sich das entsprechende System in einem Rechenzentrum befindet und nicht mit dem Netzwerk verbunden ist. Ein Angreifer müsste also zunächst in das Rechenzentrum eindringen, um das System anzugreifen. Der **Angriffspfad** ist damit, falls man annimmt, der Angreifer kann nur von außen kommen, und das Rechenzentrum entsprechend geschützt wurde, an dieser Stelle nicht durchgängig vorhanden.

1.2.10 Richtlinien

Ein zentrales Thema des IT-Sicherheitsprojekts ist die Erstellung von Richtlinien. Wichtig ist dabei, dass die Erstellung einer Richtlinie implizit auch deren Umsetzung bzw. Durchsetzung beinhaltet. Wenn also eine Richtlinie

erstellt wird, dann geht man davon aus, dass die Vorgaben, die darin formuliert werden, auch tatsächlich umgesetzt werden. Eine Richtlinie als Dokument muss deshalb alle Informationen beinhalten, die erforderlich sind, um die darin enthaltenen Vorgaben auch umsetzen zu können.

Der Begriff »Richtlinie« wird der Einfachheit halber mit den Ausdrücken »Vorgabe«, »Regelung« oder aus dem Englischen »Policy« gleichgesetzt. Alle diese Begriffe haben gemeinsam, dass damit ein Dokument beschrieben wird, das **verbindliche** (*mandatory*) Vorgaben über ein bestimmtes Thema macht. Wie eine Richtlinie ausgestaltet werden kann und welche Komponenten sie beinhalten sollte, wird in Abschnitt 4.1.4 detailliert beschrieben.

Eine Unterscheidung zwischen Richtlinie und Verordnung, wie sie z. B. im europäischen Recht üblich ist, wird im Bereich der Informationstechnik (IT) üblicherweise nicht gemacht. Wie man daran gut erkennen kann, ist letztendlich vor allem wichtig, sich auf eine unternehmensweite, einheitliche Sprachregelung zu verständigen.

1.2.11 IT-Sicherheitskonzept

Das IT-Sicherheitskonzept ist die Beschreibung der Gesamtheit aller Maßnahmen im Bereich der IT-Sicherheit und deren Zielvorgaben. Damit ist es mehr als nur die Summe aller operativen Vorgänge in der IT-Sicherheit. Das IT-Sicherheitsprojekt versucht, die regulativen Bestandteile eines IT-Sicherheitskonzepts zu beschreiben und deren operative Umsetzung zu begleiten. Das IT-Sicherheitskonzept ist also mehr als nur ein Dokument oder ein Prozess.

Im Rahmen des Projekts werden einige grundlegende Komponenten des Konzepts bearbeitet. Dies reicht vom

- Projektauftrag, inklusive dem Geltungsbereich,
- über die IT-Sicherheitsorganisation,
- die Schutzbedarfsanalyse im Rahmen der Business-Impact-Analyse,
- die Richtlinien, der Überprüfung derselben,
- vom Audit abgeleitete Maßnahmen,
- das IT-Risikomanagement
- bis hin zu den IT-Sicherheitsprozessen.

Alle diese Komponenten und noch mehr sind Teil eines umfassenden IT-Sicherheitskonzepts.

Die IT-Sicherheit hat eine klare Aufgabe im Unternehmen. Diese Aufgabe leitet sich wiederum von den Zielen des Unternehmens und den Zielen der IT ab. Aus diesem Grund können sich die Ziele der IT-Sicherheit von Unternehmen zu Unternehmen erheblich voneinander unterscheiden. So wird ein Unternehmen aus dem Einzelhandel andere Schwerpunkte in der IT und in der IT-Sicherheit legen als ein Unternehmen, das Produkte herstellt. Kurz: Die Ziele der IT-Sicherheit und damit das IT-Sicherheitskonzept ist stark mit dem Geschäftszweck und damit der Unternehmensstrategie verbunden.

1.3 Das Hamsterrad

Sisyphos, ein Held der griechischen Mythologie, wird gezwungen, einen Felsblock einen Hang hinaufzurollen. Ganz knapp, bevor er es hinbekommt, entgleitet ihm der Stein aber und rollt den Hang wieder hinab. Also beginnt seine Arbeit von Neuem. Er eilt den Hang hinab, nimmt den Stein erneut auf und rollt ihn wieder nach oben – bis er ihm wieder entgleitet. Da er dies nun schon seit sehr langer Zeit tut, ist kaum zu erwarten, dass der Stein einmal oben zu liegen kommt.

Was hat nun die IT-Sicherheit mit Sisyphos zu tun? Die Gemeinsamkeiten sind vielfältiger, als man zunächst annimmt. Das wird deutlich, wenn man es ein wenig abgewandelt ausdrückt: Der Prozess, dem Sisyphos folgt, schreibt ihm vor, den Stein nach oben zu rollen. Ihn oben zu platzieren, käme einem 100%igen Erfolg gleich, den er aber nie erreichen wird, genauso wie es niemals 100%ige IT-Sicherheit geben kann.

Mit etwas Weitsicht wird er aus dem Vorgang des Hinaufrollens und der Analyse des Scheiterns Folgerungen ziehen, die dem nächsten Versuch zugutekommen. Mit anderen Worten, er folgt einem kontinuierlichen Verbesserungsprozess mit dem Ziel, einem perfekten Ergebnis möglichst nahe zu kommen. Da Sisyphos es schon sehr lange probiert, und das ohne Unterlass, ist davon auszugehen, dass sein Ergebnis schon heute sehr gut ausfällt. Dass er alles den existierenden Regeln und Vorgaben entsprechend tut und alle Rahmenbedingungen einhält, davon gehe ich, trotz der mageren Kenntnislage, einfach mal aus.

IT-Sicherheit ist per definitionem ein Zustand, den es anzustreben gilt. Erreichen wird man ihn niemals in Perfektion. Diesen Zusammenhang zu verstehen ist wesentlich, um den Erfolg oder Misserfolg eines Projekts im Nachhinein messen zu können. Denn es gilt, dass es nicht nur wichtig ist, IT-Sicherheit einzuführen, sondern noch viel wichtiger ist es, dies aus den richtigen Gründen mit den richtigen Erwartungen zu tun. Der Unterschied zwischen fast perfekter Sicherheit und perfekter Sicherheit, die es nie geben wird, kann ein Sicherheitsvorfall sein, der einen großen Schaden anrichtet. Damit geht es letztendlich um Wahrscheinlichkeiten und das Ziel, besser zu werden, ohne jemals wirklich fertig zu sein.

1.4 Die allzu menschlichen Fallstricke

Wie viele andere Felder im Unternehmen hat die IT-Sicherheit mit einer Reihe von, zumeist menschlichen, Unwägbarkeiten zu kämpfen. Diese zu kennen ist der erste Schritt, um sie im Rahmen eines IT-Sicherheitsprojektes zu adressieren und, im besten Fall, zum eigenen Vorteil einzusetzen.

Das erste Problem ist eines, das jeder Mensch hat, wenn auch in unterschiedlicher Ausprägung. Es geht um die Art und Weise, in der man Entscheidungen trifft. Viele Entscheidungen, da ist man sich einig, werden aus dem **Bauch heraus getroffen**. Damit basieren sie auf der eigenen Erfahrung, der eigenen Kompetenz und der Größe des eigenen Selbstbewusstseins. Das muss nicht schlecht sein und, wie es eine Redensart schon sagt, wenn man auf seinen Bauch hört, dann liegt man schon sehr häufig richtig. Das mag sogar stimmen, das Problem ist nur, dass jeder Bauch anders tickt und damit auch anders entscheidet. Das ist in vielen Bereichen des täglichen Lebens kein Problem. Wenn es aber um Entscheidungen im Bereich der IT-Sicherheit geht, dann ist dies ein Unding!

Entscheidungen müssen **formal korrekt** und jederzeit **nachvollziehbar** sein. Dies kann erreicht werden, wenn Entscheidungen formalen Kriterien, wie z. B. einem vorgelagerten Risikomanagement, unterliegen. Aus diesem Grund liegt der maßgebliche Fokus der wichtigsten Normen genau auf dem Thema der Einführung der Bestandteile eines Information-Security-Management-Systems (ISMS). Nur ein solches Regelungsinstrument ist in der Lage, weitgehend automatisiert formal korrekte Entscheidungen zu erzwingen.

Die nächste Herausforderung betrifft wieder den eigenen Bauch. Es geht um die **selektive Wahrnehmung**, die aufgrund vergangener Erfahrungen geprägt ist. Kommt ein IT-Sicherheitsmanager aus dem Bereich der Serveradministration, so liegt es nahe, dass er bei Fragen, die diesen Bereich betreffen, mit einer ganz anderen Verve Entscheidungen trifft als bei Fragen, die aus dem Bereich Softwareentwicklung kommen – ein Bereich, den er vielleicht nicht im Detail kennt. Die Sicherheit, die er auf ihm bekanntem Terrain verspürt, kann von Vorteil, aber auch von Nachteil sein. Der Nachteil kommt immer dann zum Tragen, wenn er Fehlentscheidungen trifft, einfach aus Erfahrungen heraus, die zwar objektiv gesehen falsch sind, ihm aber aufgrund des täglichen Umgangs vertraut und sicher erscheinen.

Apropos tägliche Erfahrungen: An dieser Stelle setzt ein weiterer Automatismus ein. Nennen wir ihn den »das hat auch schon in der Vergangenheit immer gut funktioniert«-Mechanismus. Den als vertraut empfundenen **Status quo zu überhöhen** und Neuem als übertrieben positiv entgegenzustellen, ist menschlich. Bewährtes zu ändern, anzupassen oder zu ersetzen, fällt schwerer, als etwas vollkommen Neues einzuführen. Da wird dann gerne das Bewährte bewahrt. Dieser Zustand wird weiter verschärft, wenn eine bestimmte Vorgehensweise bereits als erfolgreich und komplett umgesetzt nach oben kommuniziert wurde. In diesem Fall wird man nicht nur den direkt Verantwortlichen überzeugen müssen, sondern zudem Personen aus den Hierarchien darüber. Diesem Mechanismus muss mit Werkzeugen entgegengetreten werden, die Bewertungen, z. B. in Form von Entscheidungsmatrizen, auf einen möglichst objektiven Entscheidungspfad setzen.

Unzählige IT-Sicherheitsprojekte sind aus den falschen Gründen gescheitert: den **Kosten**. Das liegt zum einen darin begründet, dass Kosten generell schwer einzuschätzen sind, und zum anderen darin, dass dies in noch größerem Maße für Kosten im IT-Sicherheitsumfeld gilt. So werden Aufwände häufig nur punktuell betrachtet, ohne die Kosten für anhängige Systeme ausreichend genau zu hinterfragen. Die Einführung eines neuen Internetzugangs für eine neue Fabrik zieht, das wissen die Verantwortlichen, die Installation und den Betrieb einer Firewall nach sich. Dazu kommt dann noch ein Internetproxy, um den Benutzern den Zugang zum Internet zu erleichtern und um zusätzliche Sicherheit zu schaffen. Auf dem Proxy wird selbstverständlich auch eine Antivirensoftware benötigt mit laufenden Kosten für die Virensignaturen. Das Netzwerk zwischen dem internen Core-Router und dem Internet muss dazu noch von einem Intrusion Detection System (IDS) überwacht

werden. Das macht es nicht alleine und damit wird entsprechendes Personal benötigt. Die Meldungen, die dieses System macht, müssen bewertet und im Falle eines Ereignisses an wiederum weitere Personen geschickt werden, die entscheiden, ob eine Maßnahme, wie das Abschalten des Zugangs, erforderlich ist. In diesem Fall müssen Maßnahmen für eine Backup-Leitung zum Internet getroffen werden. Und so weiter und so fort. Sehr häufig zieht eine Sicherheitsmaßnahme einen Rattenschwanz an weiteren Maßnahmen nach sich. Es ist gefährlich, diesen Prozess nicht vollständig zu durchdenken oder an einer beliebigen Stelle abzubrechen und als »nicht projektrelevant« zu markieren. Im weiteren Verlauf, eventuell erst nach Monaten, werden die Folgekosten sichtbar werden und die dann unweigerlich folgenden negativen Erfahrungen werden sich dann wiederum auf Entscheidungen hinsichtlich späterer Projekte auswirken.

Eng mit Kosten ist auch das eingesetzte Verfahren zum **Risikomanagement** verbunden. Hier geht es darum, Risiken einzuschätzen und die korrekten Maßnahmen zu treffen, um identifizierte Risiken zu reduzieren. Dieser Ansatz funktioniert häufig nicht flächendeckend. Menschen tendieren dazu, diejenigen Risiken, die sie als beherrschbar einstufen, vorrangig zu betrachten. Das führt dann zu Situationen, in denen Unternehmen viel Geld und Zeit in das Management des WLAN-Zugangs stecken, während der Zugang zum Internet wenig Beachtung findet. Das gleiche Phänomen ist zu beobachten, wenn es um das Einspielen von Sicherheits-Updates geht. Man fokussiert sich automatisch auf diejenigen Produkte, bei denen das Update einfach und am besten zudem automatisiert möglich ist. Andere Software-Produkte, die ein Herunterfahren des IT-Systems erfordern oder die einfach komplex sind, werden ausgeblendet. Man verliert den Blick auf die Gesamtsituation und fühlt sich dennoch sicher, man tut ja schließlich auch etwas dafür.

Die nächste hier aufgeführte Herausforderung ist die des **fehlgeleiteten Fokus**. Völlige Sicherheit ist nicht erreichbar. Das ist ein Fakt, der jedem einleuchten muss. Daraus folgt, dass es darum geht, so viel wie möglich an IT-Sicherheit zu erreichen. Und dies ist nicht durch, häufig kostenintensive, gezielte Maßnahmen möglich, sondern nur durch die Erhöhung des Gesamtsicherheitsniveaus. Anders ausgedrückt: Wenn ein CEO von einem Berater bzw. Verkäufer davon überzeugt wird, für sein Rechenzentrum eine Personenvereinzelungsanlage zu beschaffen, die bei jedem Zutritt die jeweilige Person und ihr Gepäck wiegt, um es mit dem Gewicht beim Verlassen zu vergleichen, dann ist dies unleugbar ein Schritt hin zu mehr Sicherheit. Ob es

aber der richtige Schritt ist, lässt sich nur im Gesamtzusammenhang abschätzen. Denn vor dem Kauf einer solchen Anlage stehen der Brandschutz, die unterbrechungsfreie Stromversorgung, geregelte und sichere Prozesse für Besucher und das Reinigungspersonal, Maßnahmen zur Sicherung der IT-Systeme inklusive des Netzwerks, die Unterbringung der Originaldaten in von den Sicherungsbändern getrennten Brandabschnitten und viele andere Maßnahmen, die zunächst umgesetzt werden können, da sie unter Umständen eine höhere Priorität besitzen, im Vordergrund. Ist dies alles bereits vorhanden, dann handelt es sich um eine Erweiterung der Sicherheit. Ist ein einzelner der genannten Punkte noch nicht vollständig umgesetzt, dann liegt die Vermutung nahe, dass ein Akt des fehlgeleiteten Aktionismus stattfindet und damit der Blick auf die näher liegenden Aufgaben verschleiert wird.

Der letzte Punkt betrifft die Art der Entscheidungsfindung aus Teams heraus. Dabei soll keine Überhöhung »diktatorischer Entscheidungen« gegenüber den Entscheidungen, die aus einem **Team-Konsens** heraus getroffen werden, stattfinden. Dennoch möchte ich zumindest am Rande die Herausforderungen erwähnen, denen sich ein Entscheider in der IT-Sicherheit gegenübersieht, und der Schwierigkeit, sich auch einmal dem Konsens in größeren Runden zu entziehen, um eine formal korrekte Entscheidung zu treffen. Jede größere Entscheidung wird immer unterschiedliche Interessen berühren, und wenn diese Entscheidungen in Teamsitzungen getroffen werden, dann ist es nicht leicht, sich gegen den Strom zu stemmen. Manchmal ist dies aber erforderlich und das sollte sowohl dem Vorgesetzten als auch dem IT-Sicherheitsmanager selbst immer bewusst sein.

1.5 Motivation, die IT-Sicherheit zu erhöhen

1.5.1 Externe Vorgaben

Sehr häufig ist es ein äußerer Zwang, der Unternehmen dazu bewegt, sich verstärkt für die Aufgabenstellungen der IT-Sicherheit zu engagieren. Dabei ist es zweitrangig, ob es sich um immer neue Enthüllungen, die in der Tagesschau über den Schirm flimmern, handelt, die aufzeigen, wie gefährlich es heutzutage ist, Daten auszutauschen oder überhaupt zu kommunizieren, oder ob es sich um klar definierte Anforderungen der Kunden oder, wie im Falle des Datenschutzgesetzes, des Gesetzgebers handelt. Auch Unternehmen, die sich bislang aus Kostengründen gescheut haben, das Thema IT-

Sicherheit intensiv und ganzheitlich zu betrachten, beginnen immer mehr, es auch formal in Form von Regelungen und einer eigenen Organisationseinheit zu etablieren. Das kann in sehr kleinem Rahmen beginnen, um dann über die Zeit ausgedehnt zu werden.

Am Beginn werden dementsprechend die klassischen Themen, die auch im privaten Umfeld relevant sind, angegangen. Dazu zählen die üblichen Vorkehrungen, wie Virenscanner zu installieren, Firewalls oder ein Patchmanagement einzurichten. Geht es aber in Richtung eines ISMS und damit einer Vernetzung dieser einzelnen Puzzlestücke, dann ist Planung und ein konzertiertes Vorgehen nicht nur sinnvoll, sondern notwendig. Wegweisend für die jeweilige Vorgehensweise sind dann wiederum die Ziele, die man sich steckt, und diese, und hier schließt sich der Kreis, werden maßgeblich durch externe Vorgaben definiert.

Es existiert kein Gesetz, das die Etablierung einer Organisationseinheit »Datensicherheit« im Unternehmen fordert. Bezüglich des Datenschutzes verhält es sich anders. Hier ist ein Datenschutzbeauftragter einzusetzen und mit definierten Vollmachten auszustatten. Warum werden diese beiden so stark voneinander abhängigen Themen so unterschiedlich behandelt? Der Grund liegt unter anderem darin begründet, dass der Datenschutz vorrangig die Belange der Arbeitnehmer schützt und die Datensicherheit die des Unternehmers. Der Gesetzgeber stärkt mit dem Datenschutzbeauftragten die Rechte der Arbeitnehmer und die Durchsetzung der Regelungen des Bundesdatenschutzgesetzes.

Bei einem Unternehmer geht man davon aus, dass Vorschriften zum ordnungsgemäßen Betreiben eines Unternehmens, wie z. B. im GmbH-Gesetz gefordert, ausreichend sein müssten, dass der Unternehmer seine Aufgabe wahrnimmt und durch Maßnahmen auch umsetzt. Schließlich ist der Unternehmer nicht nur verantwortlich dafür, sondern im höchsten Maße auch daran interessiert, dass der Geschäftsbetrieb durch den Diebstahl, die verbrecherische Veränderung oder die Nicht-Verfügbarkeit seines Know-hows, sprich von seinen Daten und denen der Kunden und Lieferanten, nicht gefährdet wird. Aus dieser Gemengelage heraus ist auch zu verstehen, warum es die ureigenste Aufgabe und auch das Bedürfnis der Unternehmensleitung sein muss, die Aufgabe der Datensicherheit durch ein geeignetes IT-Sicherheitsmanagement wahrzunehmen. Dass dies nicht immer der Realität entspricht, ist Fakt und die Ursachen dafür sind mannigfaltig.

1.5.2 Verpflichtung zur Datensicherheit

Unternehmerische Entscheidungen beruhen auf dem ständigen Abwägen verschiedener Faktoren. Die Grundlage wird dabei in den meisten Fällen die Abwägung zwischen Kosten und einem Risiko bzw. einer Chance bilden. Es gibt keine Grundregel und kein Gesetz, das einem Unternehmer vorschreibt, wie er mit einem Risiko umgehen muss. Aber abwägen, das zumindest muss er tun, um die erforderliche unternehmerische Sorgfalt walten zu lassen. Um wiederum abwägen zu können, benötigt der Entscheider Informationen. Dazu gehören Faktoren wie die genauen Kosten, die eine Maßnahme erzeugen würde, aber genauso auch eine möglichst genaue Einschätzung, was passieren würde, wenn er Aufgaben, wie den Schutz des Unternehmens-Knowhows, nicht in ausreichendem Maße wahrnehmen würde. An diesem Punkt zögern viele Unternehmer und berufen sich auf nicht erhältliche, kaufmännisch belastbare Daten, wie z. B. die Kosten für den möglichen Eintritt eines Sicherheitsereignisses. Eine weitere Reaktion, die zu beobachten ist, ist die schlichte Ausblendung des Risikos, da andere, handfeste Probleme zu jedem Zeitpunkt priorisiert im Fokus stehen. Auch wenn diese Reaktionen auf den ersten Blick nachvollziehbar erscheinen, so sind sie dennoch falsch oder zumindest gefährlich.

Hinweis

In einem Gespräch mit einem IT-Leiter eines Klinikums hat es sich so dargestellt, dass in Folge langjähriger Tradition eine ganze Reihe von Prozessen mit dem Umgang von Patientendaten auf Papier befasst ist. Von der Verwaltung der Ordner über die Ausgabe und die Eingabe sind alle Prozessschritte genau definiert und bei der Belegschaft in Fleisch und Blut übergegangen. Dies hat sich auch einige Monate nach der parallelen Einführung einer IT-gestützten Patientenverwaltung nicht geändert. Die Daten auf Papier werden sorgfältig verwahrt und sind strengen Zugriffsregeln unterworfen. Auf die Daten in der Datenbank können dagegen neben dem Standard-Systemuser, dessen Passwort im Übrigen nie geändert wurde, nahezu alle Mitarbeiter zugreifen.

Die gleichen Daten, in zwei verschiedenen Systemen, die aus dem Blickwinkel der Datensicherheit völlig unterschiedlich betrachtet werden. Wer glaubt, dass dies ein Einzelfall ist, der irrt.

Der Grund dafür liegt eigentlich auf der Hand: In jeder modernen Firma ist ein Datensicherheitsproblem denkbar, das den Fortbestand der Firma gefährden kann. Der Verlust aller Finanzdaten im äußersten Fall ist ein markantes Beispiel. Wenn es also grundsätzlich in jeder Firma wichtig ist, bestimmte Daten vor Verlust oder Manipulation zu schützen, dann ist auch ein bestimmtes Maß an Aufwand im Bereich Datensicherheit zwingend erforderlich. Dies sagt aber natürlich nichts über den Umfang eines solchen Projekts aus. Und damit gilt wieder die Regel, dass man als Unternehmer genau den notwendigen Teil umsetzt, der nach einer Abwägung von Kosten und Risiken sinnvoll ist.

An diesem Punkt setzt das vorliegende Projekt auf. Das Ziel ist es nicht, alles zu tun, was möglich ist. Das Ziel ist auch nicht, das zu tun, was Berater als notwendig erachten. Der Weg, den das Projekt geht, sieht eher so aus, dass es an Ihr Unternehmen angepasst diejenigen Maßnahmen umsetzen soll, die Sie zu Beginn des Projekts als erforderlich definiert haben. Das dabei verwendete Modell fängt grundsätzlich bei den wichtigsten Daten und IT-Systemen an, setzt eine grundlegende Basissicherheit um und arbeitet sich dann von innen nach außen hin zu immer mehr Sicherheit. Es ist Ihr Risiko und damit auch Ihre Entscheidung, wie weit Sie jeweils gehen wollen. Das Projekt liefert dazu die Methodik und eine Beschreibung der wichtigsten Maßnahmen.

Unabhängig davon, wie die einzelnen Maßnahmen zu einem Mehr an Datensicherheit aussehen sollen. Unabhängig davon, wie stark sich das Unternehmen engagieren und finanziell einbringen möchte, und auch unabhängig davon, ob es eine dedizierte Organisationseinheit geben soll, die sich des Themas annimmt, ist es unbedingt erforderlich, dass sich die Unternehmensleitung über die folgenden Fakten klar wird:

- Der Schutz der eigenen Daten, der Daten der Mitarbeiter, der Daten der Kunden und der Daten von Lieferanten und aller mit dem Unternehmen verbundenen Unternehmen und Personen ist wichtig.
- Die Unternehmensleitung ist für den Schutz dieser Daten verantwortlich.
- Der Schutz dieser Daten geschieht einzig und allein zum Nutzen des Unternehmens.

Eines der Ergebnisse aus vielen Projekten und Studien zu diesem Thema ist, und dabei handelt es sich um einen der wirklich grundlegenden Punkte, dass nur ein konsequenter **Top-down-Ansatz** im Bereich der Datensicherheit wirklich Erfolg verspricht.

1.5.3 Haftung auf verschiedenen Ebenen

Haftung beginnt, wie so vieles, zunächst mit einer Regelung. Das Unternehmen, der Gesetzgeber oder eine andere Instanz stellt eine Regel auf, überprüft deren Durchführung und belegt denjenigen, der dagegen verstößt, mit einer Strafe. Genau diese Konstellation wird mit dem wolkigen Begriff »Compliance« beschrieben. Dabei kann es sich z. B. um einen Kunden handeln, der die Regel aufstellt, dass seine Daten, die er Ihrem Unternehmen zur Verfügung stellt, nicht weitergegeben werden dürfen. Vor allem nicht an die Konkurrenz, aber auch an sonst niemanden. Diese Regel packt er in einen Vertrag und definiert dort auch gleich, was im Falle eines Verstoßes passiert. Das kann eine Kündigung des Geschäftsverhältnisses sein oder aber eine Strafe, die zu bezahlen wäre. Dieser Vertrag wird vonseiten des Unternehmens von einer Person unterschrieben, die in den meisten Fällen mit dem Zusatz »per procura« unterschreibt. Diese Person handelt also im Namen des Unternehmens. Passiert nun etwas mit diesen Daten, sagen wir ein IT-Administrator verschickt sie versehentlich per E-Mail an einen Bekannten, der zufällig für die Konkurrenz des Kunden arbeitet, so wird sich der Kunde an das Unternehmen wenden und die Strafe vollstrecken wollen.

Während einer Einigung, ob gütlich oder durch Richterspruch, stehen sich zunächst einmal zwei Unternehmen gegenüber. In einer zweiten Runde wird es aber auch intern darum gehen, wer die Schuld trägt und in einem weiterführenden Prozess haften könnte. Genau an dieser Stelle geraten nun irgendwann auch der IT-Leiter und, in letzter Konsequenz, der IT-Administrator in den Fokus. Im Gegensatz zu Arbeitnehmern aus IT-fremden Arbeitsgebieten können sich diese beiden Personen nicht herausreden und sagen, dass sie nicht wussten, was sie taten. Und somit ist es tatsächlich möglich, dass beide oder einer von beiden tatsächlich in irgendeiner Form für den Schaden haften muss. Wie diese Haftung von der Höhe her aussieht, hängt dann wiederum davon ab, ob Vorsatz oder Fahrlässigkeit im Spiel war, und von anderen Punkten wie zum Beispiel, ob es geeignete Regelungen gibt, an die sich der IT-Administrator hätte halten müssen.

Es ist nicht möglich, einen solchen Vorgang grundsätzlich vollständig zu verhindern. Es ist aber sehr wohl möglich, die Wahrscheinlichkeit für sein Eintreten zu verringern. Dies fängt bei den generellen Zugriffregeln an und endet bei der Möglichkeit, sie unverschlüsselt an Dritte per Mail zu versenden. An den verschiedensten Punkten kann man ansetzen, um durch geeig-

nete Maßnahmen das Risiko möglichst gering zu halten, dass ein solcher, versehentlicher, Verstoß geschieht. Die Maßnahmen, die im Laufe des Projekts umgesetzt werden, dienen damit nicht nur dazu, die Datensicherheit zu erhöhen, sondern auch dazu, Sicherheit für Arbeitnehmer zu schaffen, indem klare Regeln und klare Prozesse definiert werden, die den Freiraum für Fehler so weit wie möglich eingrenzen.

Unternehmen, die Güter herstellen und verkaufen, häufen Wissen in Form von Daten an und sind auf das gesammelte Know-how angewiesen. Unternehmen, die Daten Dritter verarbeiten, wie z. B. Hostingunternehmen oder Webmailer, arbeiten direkt mit Daten, die ihnen nicht gehören, für die sie aber die Verantwortung tragen. In beiden Fällen spielt die IT und jeder einzelne Arbeitnehmer eine maßgebliche Rolle und ist verpflichtet, sorgfältig mit den ihnen anvertrauten Informationen umzugehen. Selbst wenn diese Informationen ausschließlich dem Unternehmen selbst gehören, verpflichtet das GmbH-Gesetz zum ordnungsgemäßen Umgang, da ein Verlust ein unternehmerisches Risiko für das Unternehmen darstellen könnte. Diese Verantwortung überträgt sich von der Unternehmensleitung herunter bis zu den Administratoren und auch auf alle anderen Mitarbeiter, die tagtäglich direkten Kontakt zu den IT-Systemen haben, auf denen diese kritischen Daten abgelegt und verarbeitet werden.

1.6 Reduzierung des Risikos

1.6.1 Angriffe durch eigene Mitarbeiter

Mitarbeiter und dazu zählt man häufig auch Externe, die im Namen des Unternehmens ihnen aufgetragene Arbeit verrichten, verursachen aus Fahrlässigkeit oder aufgrund von gezieltem Diebstahl oder Sabotage mehr als 70 % des gesamten Schadens, der in den Bereich der Datensicherheit fällt. Diese Zahl wird immer wieder genannt, und auch wenn es fraglich ist, dass sie wirklich statistisch untermauert ist, zeigt sie doch einen wichtigen Punkt auf. Es wird nämlich schnell ersichtlich, dass Aufwand, der in Maßnahmen, die zum Schutz vor dieser Kategorie an Angreifern gesteckt wird, am effektivsten ist. Zu den direkten Maßnahmen, die sich darauf fokussieren, zählen alle Punkte, die sich mit Zugriffsrechten beschäftigen, alle Maßnahmen, die zur Protokollierung von Zugriffen dienen, und Aktionen wie Awareness-Maßnahmen. Auch Unternehmen, die dazu tendieren, ihren Mitarbeitern

und Administratoren grundsätzlich zu vertrauen, sollten darüber nachdenken, ob ihre Kunden hinsichtlich dieser Sichtweise den gleichen Maßstab anlegen.

Die Abgrenzung von Kundendaten gegeneinander, die Verhinderung von kritischen Rollen in Buchungssystemen und das Verbot des Einsatzes von Wechseldatenträgern sind weitere Beispiele für Maßnahmen im Bereich der Basissicherheit und demnach allgemein als erforderlich anerkannt.

1.6.2 Angriffe von außen

Beginnend in den Jahren 2013 und 2014 sind immer neue Fakten über die staatlichen Spionagetätigkeiten, insbesondere in den USA, an die breite Öffentlichkeit gelangt. Dabei handelt es sich durchgehend um Punkte, die zwar schon lange vermutet wurden, deren Umfang aber selbst Fachleute erstaunt. Des Längeren zeigt schon der jährliche Verfassungsschutzbericht auf, dass viele Staaten wirtschaftliche Spionage gezielt verfolgen. Davon auszugehen, dass nur Länder wie Russland oder China, beides Staaten, die in diesen Berichten explizit aufgeführt werden, ganz vorne mit dabei sind, wäre weltfremd. In der Zwischenzeit ist selbst der Bundesnachrichtendienst (BND) in den Verdacht geraten für die amerikanischen Dienste die Kommunikation von inländischen Wirtschaftsunternehmen abzuhören.

Natürlich werden Daten im großen Stil direkt aus den nationalen und transatlantischen Kabeln heraus gespeichert und zum Teil auch ausgewertet. Alles, was technisch möglich und wirtschaftlich vertretbar ist, wird auch umgesetzt. Neu ist nur, dass jetzt der Punkt erreicht zu sein scheint, an dem es tatsächlich möglich ist, beinahe alle Daten über einen längeren Zeitpunkt abzuspeichern und durch Software komplett auswerten zu lassen. Damit fällt das letzte Argument, das bislang immer hieß: »Alles können die auch nicht sehen und so interessant ist meine Firma auch wieder nicht«. Heute muss man davon ausgehen, dass alle Daten gesichert werden und man vielleicht erst später, bei Bedarf, gezielt darauf zurückgreifen wird.

Es ist davon auszugehen, dass selbst, wenn die Welle der Empörung wieder abflachen wird, die Zeit der Unschuld nun endgültig vorüber ist und dieses Thema die breite Öffentlichkeit erreicht hat. Zukünftig werden Verantwortliche, die jetzt noch den Kopf in den Sand stecken, im Falle eines Falles kaum noch Argumentationsstoff haben, um sich zu rechtfertigen. Es nicht besser gewusst zu haben, zieht nicht mehr als Ausrede.

Auf der anderen Seite stehen die sogenannten »Hacker«, die eigentlich »Cracker« heißen, die mit einiger krimineller Energie versuchen, in Firmennetzwerke einzudringen und, zum Teil im Auftrag, zum Teil aus Eigenantrieb, versuchen, Daten zu entwenden oder aber gezielt Schaden anzurichten.

Der Unterschied zwischen der Kategorie »Hacker« und »staatliche Stelle« ist vor allem an einer Sache festzumachen: den technischen Möglichkeiten. Für einen erfolgreichen Angriff auf ein gut gesichertes Netzwerk von außen ist es erforderlich, über möglichst viele Detailinformationen zu verfügen. Dies erreicht ein Staat durch eine Komplettüberwachung von Telefonen, Netzwerkkommunikation, Diebstahl von Unterlagen und Gerätschaften bis hin zum Einbruch auf dem Campus. Gegen einen massiven Zugriff auf breiter Front ist es dementsprechend schwer, wirklich wirksame Gegenmaßnahmen zu implementieren. Aus diesem Grund ist selbst auf dem erweiterten Level kein vollständiger oder auch nur befriedigender Schutz möglich. Das gilt aber nicht gegen Angriffe durch weniger gut ausgerüstete Hacker oder gar ambitionierte Laien (Script-Kiddies), die nur über wenige dieser Möglichkeiten verfügen. Hier ist es durchaus möglich, wirksame Schutzwälle aufzubauen, die durch diese Art an Angreifern kaum überwunden werden können.