Informationssicherheitsmanagement

Prof. Dr. Sachar Paulus, Fachhochschule Brandenburg

A. Informationen und ihr Wert für Unternehmen

1

In den Bilanzen tauchen sie nicht auf, und dennoch stellen sie inzwischen eine wesentliche Ressource fast jedes Unternehmens dar. Die Entwicklung von Wettbewerbsvorteilen gar ist ohne sie kaum noch denkbar: Informationen. Gerade börsennotierte Unternehmen, welche mehr an zukünftigen Möglichkeiten - und damit aufgrund von Informationen - gemessen werden als an den aktuellen Bilanzentwicklungen müssen auf die Informationen, die von ihrem Unternehmen stammen oder für ihr Unternehmen von hoher Bedeutung sind, acht geben.

1

Im Fokus dieses Kapitels steht dabei der Schutz von unternehmenseigenen Informationen. Die Ermittlung von Informationen zur vergleichenden Einschätzung der eigenen Lage im Verhältnis zur Konkurrenz („Competitive Intelligence“)[1] wie auch die Sicherstellung des eigenen Rufes durch Ausüben von Einfluss auf die öffentliche Meinung[2] werden in diesem Kapitel nicht angesprochen, wenngleich diese für eine ganzheitliche Sicherheitsstrategie für Informationen von hoher Bedeutung sind. Denn nicht nur die Informationen, die innerhalb einer Organisation vorhanden sind, müssen geschützt, sowie mögliche Auswirkungen von einer ungewollten Verwendung derer vorausgesehen werden. Dies gilt auch für Informationen über das Unternehmen außerhalb der Organisation – bei Konkurrenten, Kunden, Analysten und der Öffentlichkeit. Entsprechend sind über den reinen Schutz von unternehmensinternen Informationen auch Aktivitäten erforderlich, die Informationen ermitteln und zusammenstellen, bzw. die öffentliche Wahrnehmung des Unternehmens im eigenen Sinn beeinflussen.

2

Dieses Kapitel handelt von Informationssicherheit, also den organisatorischen, strukturellen und technischen Maßnahmen zur Sicherstellung eines möglichst risikofreien Umgangs mit Informationen im Rahmen der Unternehmenstätigkeiten.

3

Wer allerdings nun erwartet, eine vollständige Einführung in Informationssicherheitsmanagementsysteme zu bekommen, der muss allerdings enttäuscht werden, denn dies ist im Umfang dieses Kapitels leider nicht möglich. Zwar wird auf die Merkmale und Unterschiede der wichtigsten Normen eingegangen, aber eben nur im Rahmen eines Überblicks. Interessierten Lesern sei an dieser Stelle der Verweis auf zwei Standardwerke erlaubt, so etwa IT-Sicherheit mit System von Müller[3] oder Praxisbuch ISO/IEC 27001 von Brenner et. al[4].

I. Der Beitrag von Informationen zur Wertschöpfung

4

Michaeli, Rainer: Competitive Intelligence: Strategische Wettbewerbsvorteile erzielen durch systematische Konkurrenz-, Markt- und Technologieanalysen, Berlin Heidelberg 2006.

[2] *Gantner, Matthias*: Strategische Krisenkommunikation als Schlüssel zur Imagewahrung: Über die Relevanz proaktiver Kommunikation, Bonn 2010.

[3] *Müller, Klaus-Rainer*: IT-Sicherheit mit System, IT-Sicherheit mit System: Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement, 2011.

[4] *Brenner, Michael, Felde, Nils, Hommel, Wolfgang, Metzger, Stefan*: Praxisbuch ISO/IEC 27001: Management der Informationssicherheit und Vorbereitung auf die Zertifizierung, 2011.

Informationen sind heute im Kern jedes Unternehmens für den Erfolg entscheidend. Neue Marktzugangskonzepte, Vertriebsideen, Produktinnovationen werden „auf dem Papier“ entwickelt (wobei heute meist dafür elektronische Medien verwendet werden), in kleinem Rahmen getestet und schließlich ausgerollt. Dafür ist es notwendig, dass Informationen auch diejenigen erreichen, die sie nutzen, im Rahmen ihrer alltäglichen Arbeit. Eine offene, zielgerichtete Verteilung der Informationen zu allen möglichen sinnvollen Empfängern steigert den Wert einer Information, da dann daraus konkrete Handlungen und Entscheidungen abgeleitet werden können.

5

Aus Sicherheitssicht ist man aber hingegen schnell dabei, Informationen nur restriktiv zu verteilen, weil man gewohnt ist, dass Informationen grundsätzlich geheim oder vertraulich gehalten werden müssen. Dabei wird gerne übersehen, dass Informationen an sich keinen Wert darstellen, sondern erst im Kontext einer betriebswirtschaftlichen Aktivität Wert erlangen. Der Kontext ist sozusagen der Schlüssel für den einer Information zugeordneten Wert, und die Vertraulichkeit ist beileibe nicht die einzige Werthaltigkeit einer Information, in anderen Kontexten ist es z.B. die Integrität. In der Folge werden daher exemplarisch verschiedene Kontexte dargestellt, in denen Informationen ein gewisser Wert beigemessen wird.

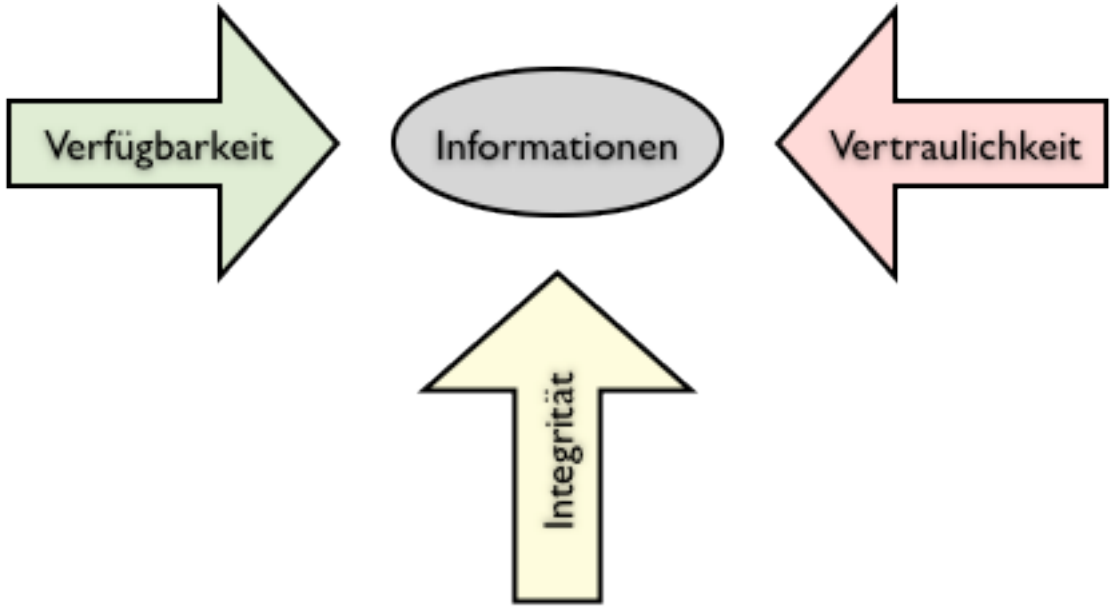


Abb. 1: Schutzziele von Informationen

1. Vertraulichkeit: Informationen als Wettbewerbsvorteil

6

Die gängigste Situation, bei der Sicherheitsverantwortliche die Sicherheit von Informationen sicherstellen sollen, ist die des Wissensvorsprungs. In der Regel gibt es eine kleine Gruppe von Menschen, die davon profitieren, dass sie etwas wissen, was andere nicht wissen. Dabei kann es sich um den Stand einer Ermittlung handeln, welche die mutmaßlichen Verbrecher nicht in Erfahrung bringen sollten, eine besondere Rabattaktion, welche Konsumenten für sich selbst nutzbar machen wollen, oder die Information über den genauern Ort von Goldfunden in der Goldgräberzeit.

7

Im Unternehmensumfeld gibt es zwei Aspekte, die hier eine bedeutsame Rolle spielen: zum einen Wettbewerbsvorteile durch besseres Know-How und Wissen gegenüber Konkurrenten und zum anderen die Vertraulichkeit von Informationen, die zur Vorbereitung von Entscheidungen von einer gewissen Tragweite dienen.

8

Zum Wettbewerbsvorsprung sind alle Informationen hilfreich, die dem Konkurrenten (mutmaßlich) nicht vorliegen, und die für eine Eroberung oder Abschottung eines Marktes dienlich sind. Hierzu zählen Kontakte zu möglichen Kunden, Informationen über anstehende Entscheidungen bei Kunden, aber auch die Information über bestimmte interne Abläufe wie Produktionsprozesse oder Rezepturen, z.B. bei Pharma-Unternehmen. Allzu oft wird aber die Bedeutung von internen Informationen überschätzt, so stellt landläufig der selbst entwickelte Programmcode für ein Softwareentwicklungsunternehmen eine sehr vertrauliche Information dar; in Wirklichkeit aber ist dies nur von geringer Relevanz weil man zum einen diese Information aus den fertigen Programmen erzeugen kann und zum anderen die Entwickler (hoffentlich) schon längst am nächsten Produkt arbeiten.

9

Dennoch sollte man hier mit höchster Vorsicht walten: Staaten, die gezielt Industriespionage betreiben (und dies mit Hilfe elektronsicher Mittel relativ leicht tun können), gibt es viele, und so ist es nicht so unwahrscheinlich, dass sich ein Staat gerade für Informationen über die Technologie in dem kleinen Unternehmen im Schwarzwald interessiert.[5]

10

Entscheidungsvorbereitungen sind hingegen in der Regel deutlich kritischer zu sehen. Je größer eine Organisation, desto vielfältiger sind die Motivationen der Mitarbeiter, und desto wahrscheinlicher ist es, dass eine vorab bekannt werdende, geplante Entscheidung zu Unruhe, oder gar zu Schaden führen kann. Die Problematik ist hierbei, dass die Gruppe der involvierten Personen sind üblicher Weise von Fall zu Fall ändert, und man daher mit einer Bewusstseinsbildung der „inneren“ Gruppen nur wenig erreichen wird. Zu dieser Gruppe gehören auch z.B. der Schutz von Informationen für Aufsichtsratssitzungen oder Vorstandssitzungen.

11

Einen Sonderfall stellt die rechtliche Anforderung zur Klassifikation von „Insidern“ dar. Insider sind Personen, welche möglicher Weise mit Informationen in Kontakt kommen, die eine „ad-hoc“ Meldung am Aktienmarkt erforderlich machen würden. Da diese Situation mit äußerster Sorgfalt und hoher Vertraulichkeit behandelt werden muss, sind die in diesem Umfeld behandelten Informationen entsprechend zu schützen.[6]

12

Aber auch wenn diese Situationen und Kontexte für die vertrauliche Behandlung von erheblicher Bedeutung sind, so darf man nicht vergessen, dass gerade die Verteilung und Verwendung von Informationen auch für das Unternehmen von Nutzen sind, und daher sollte mit dem „Vertraulichkeitsstempel“ sehr sparsam umgegangen werden, um die unternehmerische Dynamik in einer Organisation nicht zu stören.

2. Integrität: Schutz vor Manipulation

13

Ein zweites, wichtiges Feld, bei welchem Informationen geschützt werden müssen, sind die Fälle, bei denen es nicht auf der Vertraulichkeit der Informationen ankommt, sondern auf die Integrität. Die Erstellung der Quartalszahlen zum Beispiel für ein börsennotiertes Unternehmen erfordert zum einen die Zulieferung von korrekten Daten aus den Fachbereichen, Vertriebsorganisationen und Controlling-Prozessen, und auf der anderen Seite müssen diese Zahlen auch korrekt und ohne Fehler an die Öffentlichkeit kommuniziert werden. Auf der Korrektheit dieser Informationen beruht z.B. die aktuelle Börsenbewertung

[5] *Bundesamt für Verfassungsschutz*: Wirtschaftsschutz: Prävention durch Information.Ausgabe 4/2011.

[6] Rodrian, Heinrich: Insider-Regelungen. Insiderhandels-Richtlinien, Händler- und Beraterregeln und Verfahrensordnung, ???.

eines Unternehmens, eine - unbewusste oder absichtlich herbeigeführte - Veränderung dieser Informationen kann erheblichen Schaden anrichten.

14

Aber auch in der Produktion oder im Vertrieb ist es in vielen Fällen erforderlich, auf die Integrität von Informationen zu achten, damit keine Schäden entstehen. So könnte z.B. durch die Veränderung einer Rezeptur eines Lebensmittels erheblicher Schaden für den Hersteller bewirkt werden, mit Auswirkungen bis hin zur Erpressung. Die Integrität ist für viele Situationen eine erhebliche, wichtige zu schützende Eigenschaft von Unternehmensinformationen.

15

Der Fall Stuxnet hat vor einiger Zeit gezeigt, dass sogar die Integrität von Programmen und Steuerungssoftware für Industrieanlagen erheblich sicherheitskritisch sein kann. Durch die schleichende, nicht unmittelbar zu bemerkende Veränderung der Steuerungsinformationen wurden die Zentrifugen der atomaren Wiederaufbereitungsanlage Bushher nachhaltig beschädigt.[7]

16

Die Beispiele zeigen, dass der Integrität von Informationen, speziell bei einem möglichen Interesse für Manipulation durch Dritte, eine hohe Aufmerksamkeit zugewiesen werden muss, und dass sie in vielen Fällen vielleicht sogar höher bewertet werden muss als die Vertraulichkeit. Eine konkrete Aussage hierüber ist aber erst nach einer Risiko- oder Schutzbedarfsanalyse möglich (siehe Abschnitt 2).

3. Verfügbarkeit: Informationen sind da, wenn man sie braucht

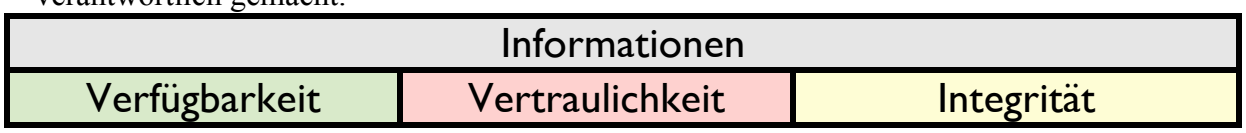
18

Neben der Vertraulichkeit und der Integrität von Informationen ist aber ein dritter Bereich nicht außer Acht zu lassen: die Verfügbarkeit. Nichts geht mehr bei einem Online-Händler, wenn die Web-Seite nicht erreichbar ist. Wenn Kontaktdaten nicht mehr per Handy vorhanden sind, dann ist man oft im wahrsten Sinne des Wortes verlassen. Viele erstellen sich daher für wirklich „wichtige“ Informationen eine Kopie in Papierform, um sie auch bei Systemausfällen oder Nicht-Erreichbarkeit zur Verfügung zu haben - oft im Gegensatz zum Prinzip der Vertraulichkeit. Je nach Geschäftszweck der betreffenden Organisation sind auch diese Aspekte zu berücksichtigen.

II. Typische Verantwortlichkeiten im Unternehmen

19

Die drei genannten Schutzziele für Informationen Verfügbarkeit, Vertraulichkeit und Integrität haben - sofern es kein Informationssicherheitsmanagementsystem (ISMS) im Unternehmen gibt - unterschiedliche „natürliche“ Stakeholder. So wird in der Regel der IT-Leiter für die Verfügbarkeit von Informationen verantwortlich gemacht, wird er doch meist an der Verfügbarkeit und Reaktionszeiten beim Ausfall von IT-Systemen gemessen. Aufgrund der Verantwortung für das Berichtswesen erklärt sich für die Integrität der Informationen, speziell derer, die für die Finanzberichte erforderlich sind, der Finanzchef zuständig. Und bei Verlust der Vertraulichkeit wird in der Regel der Sicherheitschef für mangelnde Sicherheit verantwortlich gemacht.



[7] *Symantec*: W32 Stuxnet Dossier: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf - Abgerufen am 19.12.2011.

Chief Information Officer	Chief Security Officer	Chief Financial Officer
Service Qualität	Know-How-Schutz	Compliance

Abb. 2: Typische Verantwortlichkeiten

20

Die unterschiedliche Wahrnehmung, mit der diese Personen auf das Thema Informationssicherheit schauen, macht die Koordination von geeigneten Maßnahmen nicht leichter. Gerade deswegen ist ein Management-System für Informationssicherheit, also ein Werkzeugkasten bestehend aus Richtlinien, organisatorischer Zuordnung, geeigneten Maßnahmen zum Schutz von Informationen und etablierten Berichtswegen unverzichtbar, um ein Minimum an Verlässlichkeit für den Schutz von wichtigen, kritischen, besonderen Informationen im Unternehmen sicher zu stellen. Ebenfalls unverzichtbar ist das Konzept des Informationseigners, also einer für jede wesentliche Information zuständigen Person im Unternehmen.

21

In der Folge konzentrieren wir uns bei den Bedrohungen und Maßnahmen auf Täter, die Informationstechnologie nutzen und ausnutzen, um an ihr Ziel zu kommen, seien es vertrauliche Informationen oder die Manipulation von wichtigen unternehmensinternen Daten. Es sei angemerkt, dass ein ISMS sehr wohl auch andere Tätergruppen kennt und auch z.B. physische Maßnahmen empfiehlt bzw. einfordert, denn jeder Angreifer sucht sich den leichtesten Weg, und mal führt er über die Informationstechnologie, und manchmal eben über klassischen Einbruch. Wir gehen aber davon aus, dass diese Aspekte bereits ausreichend in den anderen Kapiteln dieses Kompendiums behandelt wurden.

B. Risiko- und Schutzbedarfsanalyse

22

Eine korrekte Einschätzung der Situation ist ohne den Einsatz von systematischen Werkzeugen im Bereich der Informationssicherheit kaum noch möglich. Moderne Unternehmen setzen Informationstechnologie sehr umfassend ein, und überlassen oft schon den Mitarbeitern die Wahl des Endgeräts und damit auch die Sicherheit der Endpunkte des Unternehmensnetzwerks. Systematische Werkzeuge wie eine Risikoanalyse und die Schutzbedarfsanalyse ermöglichen einen besseren Überblick zu gewinnen, und damit die bestehenden Ressourcen und finanziellen Möglichkeiten auf die wichtigsten Handlungsfelder zu konzentrieren.

23

Einen hundertprozentigen Schutz gibt es nie, dies gilt auch in der Informationssicherheit. Entsprechend sind die Werkzeuge auch nicht darauf ausgerichtet, einen vollständigen Schutz zu erreichen, sondern „Mut zur Lücke“ an den geeigneten Stellen zuzulassen und sozusagen nachweisbar die riskantesten Bereiche abzusichern. Das ist im Bereich der Informationssicherheit nicht selbstverständlich, hin und wieder findet man immer noch IT-Sicherheitsverantwortliche, die versuchen, die 100%ige Sicherheit in bestimmten Feldern zu erreichen - oft auf Kosten der Vernachlässigung anderer, zum Teil wesentlich kritischerer Bereiche.

Bevor wir die Werkzeuge erläutern, sind allerdings noch einige Begriffe zu klären, die dabei Verwendung finden.

I. Begriffliches

In diesem Abschnitt werden für die Erläuterung der Werkzeuge Risikoanalyse und Schutzbedarfsanalyse wichtige Begriffe kurz eingeführt.

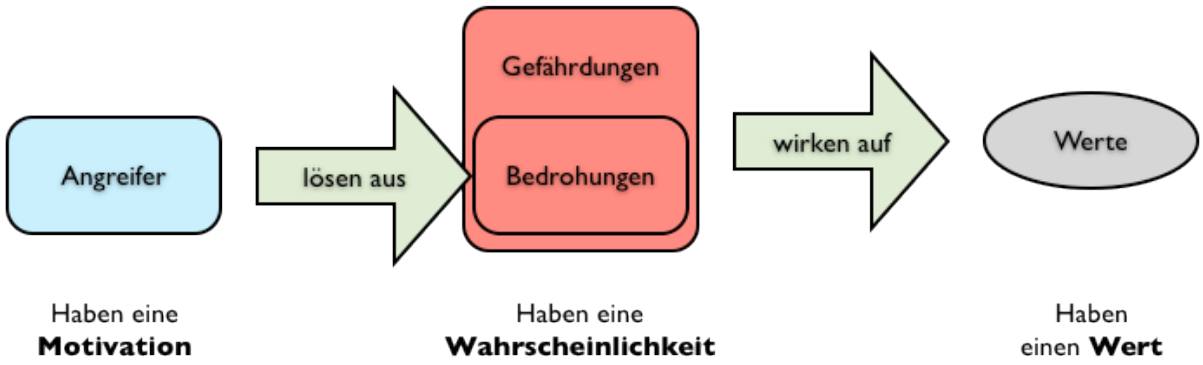


Abb. 3: Wichtige Begriffe.

1. Werte

24

Mit **Werten** sind üblicher Weise Güter gemeint, die als Aktiva auf der Bilanz des Unternehmens auftauchen. Nun sind Informationen jedweder Art nicht materiell, und finden daher üblicher Weise keinen Eingang in die Bilanz eines Unternehmens. Es gibt zwar den Begriff der „immateriellen Werte", diese sind aber üblicherweise beschränkt auf Software-Lizenzen einerseits und Abschreibungen von Unternehmensübernahmen („Goodwill") andererseits. Nicht materielle Werte wie das Image eines Unternehmens, das Know-How der Mitarbeiter oder auch eben Informationen werden bilanztechnisch (bisher) nicht erfasst.[8]

25

Dennoch ist es wichtig, sich mit diesem Begriff im Rahmen der Informationssicherheit auseinanderzusetzen. Informationen, wie in Abschnitt 1 beschrieben, haben selbst keinen Wert. Man kann vom Wert der **Verfügbarkeit, Vertraulichkeit** bzw. **Integrität** einer Information sprechen, wenn diese Eigenschaft in einem bestimmten Kontext gegeben sein muss. Zudem kann man die gleichen Eigenschaften auf IT-Systeme ausdehnen, die entsprechende Informationen halten. Informationen bezeichnen dabei die abstrakte Konstruktion, unter der man sich eine gegebene Information vorstellt, jede Erscheinungsform („Repräsentation"), wie z.B. ein Bild, eine Tabelle, ein sprachlich übermittelter Satz, wird in diesem Zusammenhang nicht Information sondern Datum genannt. Es sei an dieser Stelle schon vorausgeschickt, dass Informationen nie optimal geschützt werden können, wohl aber deren Repräsentationen, also die Daten.

26

Im Rahmen der Informationssicherheit sind also die zentralen zu betrachtenden Werte die Vertraulichkeit, die Verfügbarkeit und die Integrität von Informationen und IT-Systemen.

2. Gefährdungen und Bedrohungen

27

Werte sind Gefahren ausgesetzt und von Angriffen bedroht. In dieser Kurzform können die beiden Begriffe Gefährdung und Bedrohung in Beziehung gesetzt.

Dabei bezeichnet die **Gefährdung** eine potenzielle Gefahrenquelle, welche zu unterscheiden ist von der eigentlichen **Gefahr**, die die mögliche Schadwirkung einer Gefahrenquelle bezeichnet. Somit ist die Gefahr das mögliche Ergebnis, während die Gefährdung den Zustand bezeichnet. Die **Bedrohung** ist eine spezielle Form der Gefährdung, die von einem

[8] *Daum, Jürgen H.*: Intangible Assets oder die Kunst, Mehrwert zu schaffen, Galileo 2002.

aktiven Angreifer ausgeht. Dabei besteht - rechtlich - die Möglichkeit, dass der Angreifer durch Ausüben einer Aktivität eine Straftat begeht.[9]

28

In der IT wird oft der Begriff einer Bedrohung definiert durch eine Gefährdung, die von einer **Schwachstelle** ausgeht, dabei ist eine Schwachstelle eine Lücke des Sicherheitssystems. Durch diese Art der Definition wird aber ein Ringschluss erzeugt, denn bevor die zu schützenden Werte identifiziert sind, ist ja über das Sicherheitssystem noch nichts bekannt, und wäre es umgekehrt bekannt, so wäre a priori schon die Menge der Bedrohungen bestimmt. Daher empfehlen wir, dieser Definition nicht zu folgen, auch wenn sie in der einschlägigen Literatur (leider) allzu oft verwendet wird.[10]

29

Gefährdungen und Bedrohungen zu unterscheiden mag auf den ersten Blick spitzfindig erscheinen. Doch wenn man sich im weiteren Verlauf im Rahmen der Risikoanalyse mit den Schätzungen von Eintrittswahrscheinlichkeiten beschäftigt, spielt dieser Unterschied eine wesentliche Rolle.

30

Ein **Risiko** ist ein potenzieller erwarteter Schaden und ist gekennzeichnet durch die Eintrittswahrscheinlichkeit eines Schadensereignisses und die finanzielle Auswirkung des Schadens (Schadenshöhe). Wenn man Eintrittswahrscheinlichkeit mit Schadenshöhe multipliziert, dann bekommt man eine finanzielle Kenngröße für das Risiko (meist wird diese Zahl mit dem Risiko gleichgesetzt).[11]

3. Innentäter und Angreifer

31

In der Folge werden wir uns vorrangig mit Bedrohungen auseinander setzen, da diese für den Bereich der IT- und Informationssicherheit besonders bedeutsam sind. Bei den Bedrohungen gibt es eine wichtige Unterscheidung, nämlich ob die Bedrohung von „innen“ oder von „außen“ kommt.

32

Eine Bedrohung durch einen **Innentäter** ist dadurch gekennzeichnet, dass der Angriff durch eine Person erfolgt, der aufgrund ihrer Aufgaben in der Organisation eine gewisse Vertrauensstellung hat - in einem gegebenen Kontext - und damit schon Zugang zu den Informationen hat, die das Ziel des Angriffs darstellen. Dem Innentäter ist in dieser Form kein Erschleichen oder anderweitiges Erlangen von Berechtigungen (dies sind technische Merkmale, die in IT-Systemen entscheiden, ob eine Person Zugriff auf bestimmte Informationen bekommt) erforderlich. Hierbei handelt es sich also primär um das Ausnutzen einer Vertrauensstellung, und dies wird unter dem Gesichtspunkt „Compliance“ im Kapitel "Wirtschafts- und Mitarbeiterkriminalität/Compliance" genauer betrachtet. Dagegen ist ein System von wirkungsvollen internen Kontrollen erforderlich, welche nicht deckungsgleich sind mit Informationssicherheitsmaßnahmen.

33

Die typische Situation, die wir aber in diesem Kapitel genauer betrachten wollen, ist die des **Angreifers** von außen. Damit ist natürlich vorrangig der Hacker gemeint, der sich unbefugter Weise Zugang zu Informationstechnologie und Informationen verschafft, indem er Sicherheitslücken ausnutzt oder Sicherheitsmaßnahmen überwindet. In diesem Sinn ist aber auch der Mitarbeiter, der sich weitere Berechtigungen verschafft oder erschleicht, kein Innentäter, denn er beabsichtigt, Zugriff auf Informationen zu bekommen, zu denen er

[9] *ISO/IEC Guide 51*: Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen, 1999.
[10] *Königs, Hans-Peter*: IT-Risikomanagement mit System, Vieweg & Teubner, 2009.
[11] *Erben, Roland, Romeike, Frank*: Allein auf stürmischer See: Risikomanagement für Einsteiger, Wiley-VCH Weinheim 2006.

eigentlich keinen Zugang haben dürfte. IT- und Informationssicherheitsmaßnahmen müssen sich auch gegen diesen Typ Angreifer schützen, daher sind Konzepte wie „Need-to-know“ (jeder hat ausschließlich Zugriff auf Informationen, die er für seine Arbeit benötigt) und „least privilege“ (es ist immer die geringstmögliche Menge an Berechtigungen zu vergeben) zentral für ein funktionierendes IT-Sicherheitskonzept.

34

Aus einer Risikomanagement-Perspektive ist der Unterschied zwischen Innentäter und Angreifer unerheblich, für die Gestaltung der Abwahrmaßnahmen jedoch ist sie zentral. Denn jedes gut durchdachtes Informations- und IT-Sicherheitskonzept geht davon aus, dass die Mitarbeiter mit den ihnen übertragenen Verantwortlichkeiten vertrauensvoll umgehen.

II. Risikoanalyse

35

Eines der beiden wichtigen Werkzeuge, die für ein Informationssicherheitsmanagement erforderlich ist, ist die Risikoanalyse. Eine allgemeine Betrachtung des Risikomanagements findet sich im Kapitel "Unternehmenssicherheit als Bestandteil des unternehmerischen Risikomanagements". Jedoch gibt es einige Besonderheiten, die hier genauer beleuchtet werden sollen. Neben den Schätzungen von Eintrittswahrscheinlichkeit und Schadenshöhe eines möglichen Schadensereignisses ist insbesondere die Methodik der Risikoidentifikation zu beleuchten.

1. Risikoanalyse mit oder ohne bestehendem Sicherheitskonzept?

36

Denn bei Informationen, und allgemeiner bei Informationstechnologie, stellt die Identifikation aller möglichen Risiken eine sehr umfassende und oft erschlagende Aufgabe dar. Daher wird bei der Identifikation von Informationssicherheitsrisiken oft von einem Grund-Sicherheitsniveau bzw. einer bestehenden Sicherheitsarchitektur ausgegangen, wie z.B. einem Netzwerksicherheitskonzept oder sicheren Betriebssystemen. Es werden daher nicht alle denkbaren Risiken bei der Identifikation, etwa durch Brainstorming oder Szenarioanalyse, erfasst, sondern nur solche, die nicht primär durch die bestehende Sicherheitsarchitektur abgedeckt werden.

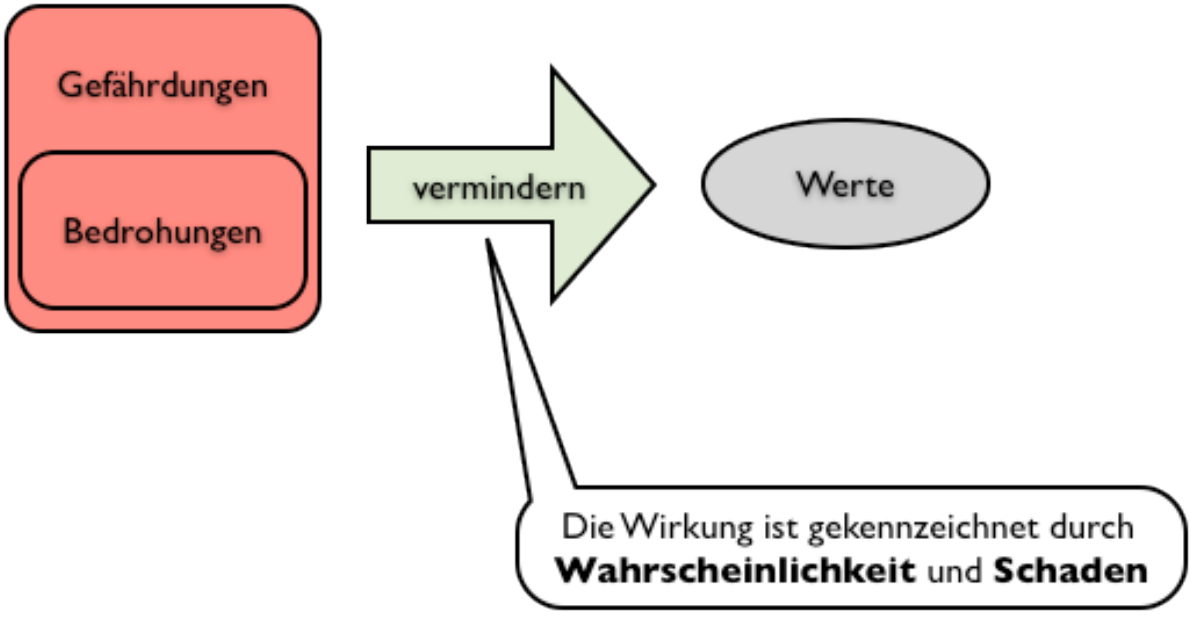


Abb. 4: Risikoanalyse ohne bestehendes Sicherheitskonzept.

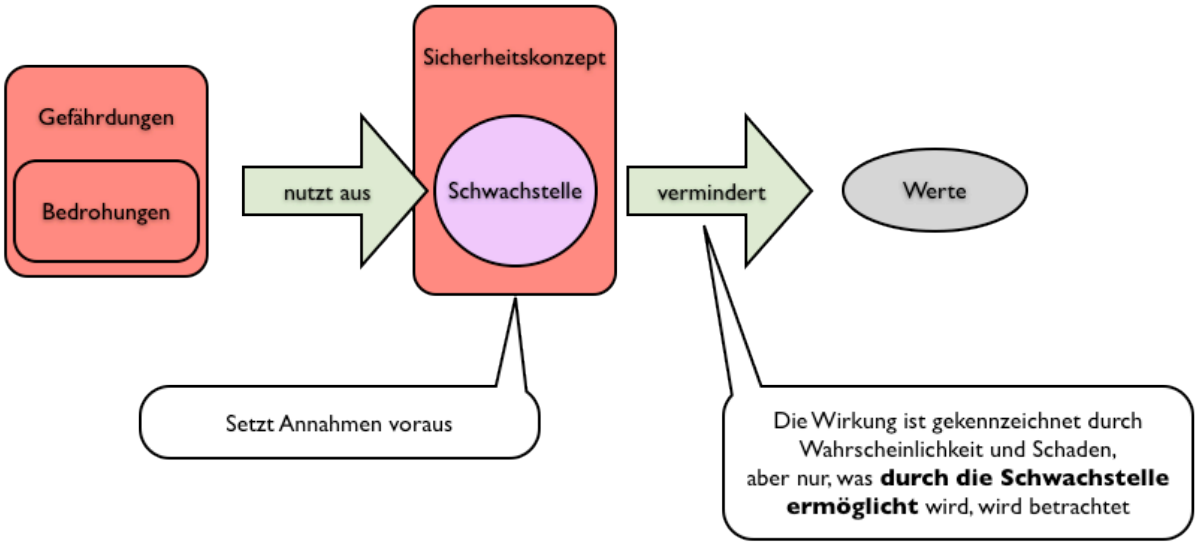


Abb. 5: Risikoanalyse mit bestehendem Sicherheitskonzept.

37

Dieser Ansatz ist nicht ohne Probleme. Zum einen muss man dann zwingender Weise den Begriff der Schwachstelle einführen, um Fehler in der Sicherheitsarchitektur im Modell zuzulassen (was natürlich tagtäglich passiert), und zum anderen ist die Annahme der Sicherheit durch eine gegebene Architektur trügerisch, und kann von wirklich erheblichen Risiken ablenken. Sofern möglich, wird daher empfohlen, dass unabhängig von der tatsächlich bestehenden Sicherheitsarchitektur eine allgemeine Betrachtung der IT-Sicherheitsrisiken vorgenommen wird, und anhand dessen eher bestehende Schutzmaßnahmen dagegen validiert werden.

38

Ein konkretes Beispiel: der Schutz von unternehmensinternen Daten auf mobilen Endgeräten stellt in den meisten Fällen ein erhebliches Problem dar. Wenn man nun von einer Sicherheitsarchitektur ausgeht, für welche unternehmensinterne Daten immer innerhalb der Unternehmensgrenzen liegen - außer es liegt ein Verstoß vor - dann muss das mobile Endgerät „immer“ Teil des Unternehmensnetzes sein. Das ist technisch heute zwar möglich, aber relativ teuer und sehr ineffizient. Dabei könnte man auch relativ abstrakt das Risiko des Abflusses von vertraulichen Daten über mobile Endgeräte auch anders fassen, ohne diese „Perimeter“-Sicherheitsarchitektur, und konsequenter Weise auch auf andere Schutzmechanismen kommen, z.B. den Einsatz von Information Rights Management (siehe weiter unten).

2. Ermittlung der Schadenshöhe

39

Die Ermittlung der Schadenshöhe ist eine besondere Herausforderung, wenn informationelle Schutzziele verletzt worden sind.

40

Ist die Verfügbarkeit von Information betroffen, so gestaltet sich der Schaden meist recht einfach: das Unternehmen bzw. Teile des Unternehmens können nicht arbeiten, wenn bestimmte Informationen nicht bereit stehen. Entsprechend kann man versuchen, einzuschätzen, welcher finanzielle Verlust für das Unternehmen entsteht, wenn die betroffenen Geschäftsprozesse für eine gegebene Zeit nicht „laufen“.

41

Ist die Vertraulichkeit von Information betroffen, so ist es schon etwas schwieriger, handelt es sich doch meistens um Wissensvorsprung den Konkurrenten gegenüber oder einer Vorbereitung von unternehmerischen Entscheidungen mit Tragweite. Hier bietet es sich an,

zu versuchen einzuschätzen, welche Investitionen erforderlich sind, um den ursprünglichen Zustand wieder herzustellen, also die Erarbeitung eines Wissensvorsprungs, die Option für bestimmte Umorganisationen etc. zu haben. Beim Verlust von Kundendaten ist in das Vertrauen der Kunden zu investieren, z.B. durch bessere Kundenbetreuung und Image-Kampagnen.

42

Ist die Integrität von Information betroffen, ist es noch schwieriger, korrekte Schätzungen für den betroffenen Schaden zu ermitteln. Sind durch einen Angreifer nachhaltig interne Steuerungsinformationen verändert worden, kann ein ganz erheblicher, dennoch schwer zu schätzender Schaden entstanden sein, weil man gerade nicht weiß, wie das Unternehmen sich entwickelt hätte, hätte es die Veränderung nicht gegeben. Doch genau das sollte versucht werden, abgeschätzt zu werden. Ist hingegen die Berichtslegung mit falschen Zahlen erfolgt, so ist dadurch ein Vertrauensverlust bei den Anlegern entstanden, der über vertrauensbildende Maßnahmen wettgemacht werden muss, hier kann man wiederum die dafür erforderlichen Investitionen für eine Schätzung des Schadens zu Grunde legen.

43

Generell ist von einfachen Einschätzungen eines Schadens in „niedrig, mittel, hoch“ abzuraten. Eine Vorgabe an die Beteiligten, nur einfache Einstufungen zu verwenden, führt erfahrungsgemäß dazu, dass man sich das Risiko nicht genau genug anschaut, um eine korrekte Einschätzung vornehmen zu können. Auch wenn die Schätzungen immer mit hohen Fehlerraten (prinzipbedingt) versehen sind, so sollte eine Einteilung in vereinfachende Schadensklassen erst nach einer detaillierten Schadensanalyse erfolgen.

3. Ermitlung der Wahrscheinlichkeit

44

Die Ermittlung der Wahrscheinlichkeit eines Informationssicherheitsrisikos ist ebenfalls durchaus nicht einfach, allerdings liegt das nicht an den verschiedenen Schadenstypen für Informationen. Vielmehr ist das in der Natur der Bedrohungen begründet. Die meisten Informationssicherheitsrisiken bestehen nicht durch unmotivierte, statistisch erfassbare, zufällige Gefährdungen wie etwa Stromausfälle, Unwetter oder ähnliches, sondern durch Bedrohungen durch aktive Angreifer, in der Menge meist durch organisierte Hacker, oft aber auch durch unloyale Mitarbeiter.

45

Wie schätzt man nun die Wahrscheinlichkeit für einen Angriff ein? Im Unterschied zu der Wahrscheinlichkeit von (nicht gerichteten) Gefährdungen, die „systemisch“ auftreten, und damit statistisch erfassbar sind - man kann aus statistischen Informationen der Vergangenheit Wahrscheinlichkeiten für die Zukunft ableiten, wie etwa bei Autounfällen oder Bränden - ist dies bei gerichteten Angriffen nicht möglich, da sie „nicht systemisch“ sind, sich also durch einen intelligente Akteur außerhalb des Systems auszeichnen, der sich gerade nicht vorhersehbar verhält.

46

Statt also zu versuchen, statistisch belastbare Zahlen zu ermitteln, wie oft ein Angriff auftritt, ist es daher deutlich gewinnbringender, zu überlegen, welche Faktoren für einen Angriff zusammen kommen müssen, und diese einzelnen Aspekte in Wahrscheinlichkeiten abzubilden. In diese Richtung hat die größte IT-Sicherheits-Gemeinde im Software-Bereich OWASP[12] ihre Risikoeinschätzung in den letzten Jahren angepasst. Hierzu zählen unter anderem:

[12] *OWASP*: https://www.owasp.org/index.php/OWASP_Risk_Management_Project. Abgerufen am 19.12.2011.

- Skill Level: ein bestimmter Angriff erfordert üblicher Weise eine bestimmte Qualifikation des Angreifers. Wie wahrscheinlich ist es, dass ein Angreifer die erforderlichen Skills hat oder sich erarbeiten kann?
- Motiv: wie interessant ist das Ziel für den Angreifer, welches Motiv verbirgt sich dahinter? Wie wahrscheinlich ist es, dass das Motiv interessant genug für einen Angriff ist?
- Aufwand: wie viel Aufwand muss der Angreifer treiben, um an das Ziel zu kommen? Wie wahrscheinlich ist es, dass er den Aufwand aufbringen kann (monetär, zeitlich, etc.)?

47

Diese Liste ist in keinster Weise erschöpfend, doch soll sie einen Ansatz vermitteln, wie man auch für gerichtete Angriffe und Bedrohungen die Eintrittswahrscheinlichkeit eines damit verbundenen Risikos schätzen kann.

III. Schutzbedarfsanalyse

48

Die Schutzbedarfsanalyse steht im Zentrum der Bedarfsaufnahme eines Informationssicherheitsmanagementsystems. Im Rahmen der Standards des Bundesamts für Sicherheit in der Informationstechnik wird die Schutzbedarfsanalyse Schutzbedarfsfeststellung genannt, da es sich dabei eher um eine Festlegung denn um eine höchst detaillierte Analyse handelt. Um im weiteren Verlauf den Prozess der Schutzmaßnahmen zu vereinfachen, werden verschiedene Schutzbedarfskategorien definiert, und für das jeweilige Unternehmen festgelegt. In der Folge werden dann die informationellen Werte der Organisation den Schutzbedarfskategorien zugeordnet.

49

Dieser Prozess der Analyse ist nur dann sinnvoll, wenn die damit durchgeführte Einteilung eine breite Unterstützung in der Organisation, und speziell bei der Führungsebene, hat. Denn mit der Einteilung sind natürlich auch Folgemaßnahmen und -Kosten verbunden, und letztlich ist die gemeinsame Feststellung des Schutzbedarfs die Basis, auf der Sicherheitsmaßnahmen argumentiert werden können. Eine breite Einbeziehung der verschiedenen Interessensgruppen führt zudem zu einer hohen Bewusstseinsbildung, und oft alleine dadurch schon zu einem veränderten Verhalten.

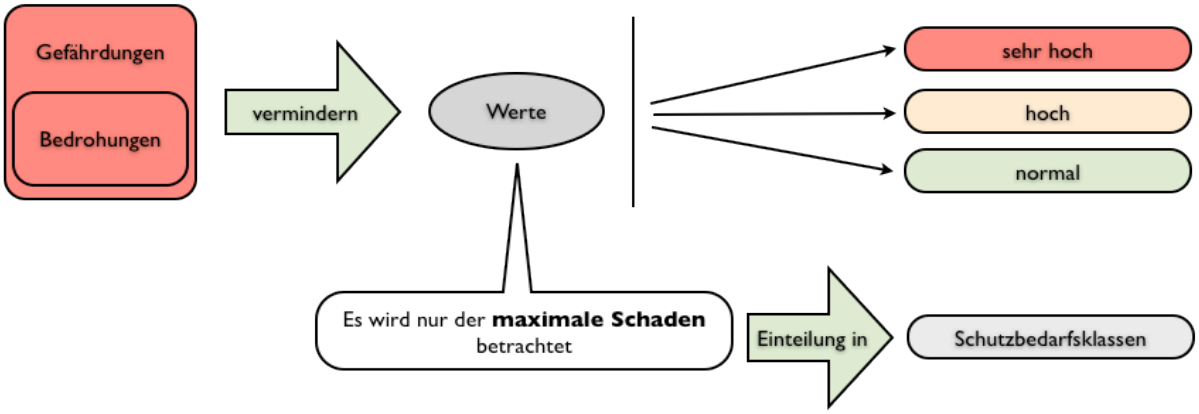


Abb. 6: Schutzbedarfsanalyse

1. Einteilung in Schutzbedarfskategorien

50

Üblicher Weise werden die folgenden Schutzbedarfskategorien verwendet:

- normal: mit einem auftretenden Angriff auf oder Verlust von informationellen Werten ist ein den Informationswerten angemessener, „normaler“ Schaden verbunden.

- hoch: mit einem auftretenden Angriff auf oder Verlust von informationellen Werten ist ein „hoher“ Schaden verbunden, der durch Auswirkungen auf andere Informationen und Prozesse der Organisation entsteht und nachhaltige negative Folgen für das Unternehmen hat.
- sehr hoch: mit einem auftretenden Angriff auf oder Verlust von informationellen Werten ist ein „sehr hoher“ Schaden verbunden, der durch Auswirkungen auf andere Informationen und Prozesse der Organisation entsteht und starke, eventuell existenzgefährdende, nachhaltige negative Folgen für das Unternehmen hat.

51

Diese Einteilung ist bewusst mit einem hohen Interpretationsspielraum verbunden, da diese eher allgemeinen Definitionen für jedes Unternehmen und jede Organisation anders zu interpretieren sind. Es hat sich bewährt, für die Festlegung der Kategorien zwei Aspekte zu betrachten: zum einen die maximale finanzielle Auswirkung, angegeben in Euro, und zum anderen die Auswirkung auf die Funktionsfähigkeit der Organisation in der Erfüllung ihrer Aufgaben, z.B. angegeben in maximalem Stillstand, z.B. in Stunden oder Tagen.

52

Besonders wichtig anzumerken ist, dass eine Einteilung in Schutzbedarfskategorien die Folgeschäden durch den Verlust von informationellen Werten mit betrachtet. Erst dann ist eine Schutzbedarfsanalyse sinnvoll und erst dann geht sie über den „normalen“ Werteverlust hinaus. Der Verlust der Vertraulichkeit von bestimmten Informationen kann eben deutlich über den Wert, der dieser Information in der Organisation üblicher Weise beigemessen wird, hinausgehen.

2. Ermittlung von Schutzbedarfskategorien

53

Sind die Schutzbedarfskategorien definiert, so sind die informationellen Werte zu identifizieren - sofern noch nicht geschehen - und in die Schutzbedarfskategorien einzuteilen. Zur Erinnerung: die informationellen Werte bestehen aus:

- der Verfügbarkeit einer Information,
- der Vertraulichkeit einer Information,
- und der Integrität einer Information.

54

Für jeden informationellen Wert, also drei Mal für jede betrachtete Information, müssen nun die möglichen Schäden eingeschätzt werden, analog zur Einschätzung der Schadenshöhe beim Risikomanagement. Dabei wird aber ganz bewusst die Wahrscheinlichkeit des Auftretens außen vor gelassen. Daher hat die Schutzbedarfsfeststellung auch eine völlig andere Zielsetzung als die Risikoanalyse: statt den tatsächlich wahrscheinlichsten Schaden zu betrachten, wird hier nur der mit einem Verlust des informationellen Wertes verbundene **maximale** Schaden betrachtet.

55

Für die Betrachtung der möglichen Schäden kommen die folgenden Aspekte in Betracht:

- Verstöße gegen Gesetze und Verträge,
- finanzielle Auswirkungen,
- Imageschäden,
- informationelle Selbstbestimmung.

56

IT-Systeme sind nach der in ihnen verarbeiteten Informationen einzuteilen. Dabei kann es aber zu einer Anpassung kommen, je nachdem ob es dadurch zu einem kumulativen Effekt kommen kann (also wenn sehr viele Informationen einer Schutzbedarfsklasse dort verarbeitet werden, kann der Schutzbedarf insgesamt größer werden) oder zu einem Verteilungseffekt

kommen kann (wenn die Informationen z.B. auch auf einem anderen System gehalten werden).

Kriterien	Risikoanalyse	Schutz
Anwendungsbereich	Alle Bereiche des Unternehmens	Sicherhe
Ziel	Ermittlung der größten Risiken	Ermittlur
Fokus	Betrachtung des Angreifers / der Gefährdung	Be schütz
Vorteil	Erlaubt betriebswirtschaftlich fundierte Priorisierung von Maßnahmen	Ermöglic die
Nachteil	Sehr breite Vergleichsbasis	Tende

Abb. 7: Vergleich Risikoanalyse - Schutzbedarfsanalyse

C. Organisatorische Maßnahmen

57

Neben den eigentlichen technischen Maßnahmen sind auch eine Reihe organisatorischer Maßnahmen sinnvoll, um die Informationssicherheit in einer Organisation sicher zu stellen. Vorrangig sinnvoll ist ein integriertes Managementsystem, welches die nachhaltige Beschäftigung mit den Schutzzielen, den Risiken und der Angemessenheit der Schutzmaßnahmen sicherstellt. Dazu zählen, neben einer Menge anderer organisatorischer Elemente, auch einige Aspekte, die aus Informationssicherheitssicht eine besondere Beachtung verdienen: die Informationssicherheitsrichtlinie, die Awareness-Maßnahmen für Informationssicherheit und das Konzept der Informationseigner.
Eine mögliche Ausrichtung an Standards ist beim Aufbau eines ISMS hilfreich, wir stellen die wichtigsten Aspekte der beiden in Deutschland dominierenden Standards vor: die ISO 2700X Familie und den IT-Grundschutz des BSI.

I. Informationssicherheitsmanagementsysteme (ISMS)

58

Ein Informationssicherheitsmanagementsystem (ISMS) dient dazu, Sicherheitsmaßnahmen nicht nur einmalig festzulegen und für immer daran festzuhalten, sondern nachhaltig die Auswahl der Maßnahmen dem sich entwickelnden Risiko- und Schutzbedarfsprofil kontinuierlich anzupassen. Ein ISMS muss also nicht nur die aktuelle Gefährdungssituation erfassen und Schutzmaßnahmen identifizieren, sondern auch den Veränderungsprozess steuern.

59

Die aktuellen ISMS werden nach dem Deming-Zyklus „Plan-Do-Check-Act“ strukturiert, und lassen sich in übergeordnete Security- und andere integrierten Managementsysteme relativ leicht integrieren.[13] Die wichtigsten Tätigkeitsfelder eines ISMS sind die folgenden:

- **Soll festlegen** (Plan): in einer ersten Phase müssen die Sicherheitsziele festgelegt werden. Diese speisen sich aus rechtlichen Anforderungen, die die Organisation erfüllen muss, vertraglichen Verpflichtungen Kunden und Partnern gegenüber, und einer

[13] *Benes, Georg, Groh, Peter*: Grundlagen des Qualitätsmanagement, Hanser, 2011.

Schutzbedarfsfeststellung für die informationellen Werte. Diese Entscheidungen werden in der Sicherheitsrichtlinie festgehalten.

- **Maßnahmen umsetzen** (Do): In der zweiten Phase werden erste Sicherheitsmaßnahmen eingeführt, unter anderem die Sicherheitsrichtlinien veröffentlicht und Awareness-Kampagnen gestartet, aber natürlich auch technische Lösungen eingesetzt.
- **Sicherheitsstatus ermitteln** (Check): In der dritten Phase wird die aktuelle Sicherheitssituation mit Hilfe der (Nicht-) Erfüllung von IT-Kontrollen ermittelt. Die IT-Kontrollen sind aus den Anforderungen in den Sicherheitsrichtlinien abzuleiten.
- **Maßnahmen anpassen** (Act): Aufgrund der aktuellen Sicherheitssituation sind die Sicherheitsmaßnahmen geeignet anzupassen.

60

Für die Auswahl der Maßnahmen in den Phasen Do und Act ist die Risikoanalyse heranzuziehen, um eine optimale Risiko-senkende Wirkung mit den gegebenen Investitionsmitteln erreichen zu können.

61

Abgesehen von den besonderen Schutzzielen und Schutzbedarfen sind aber Informationssicherheitsmanagementsysteme nicht wesentlich anders zu betrachten als „normale“ Securitymanagement-Systeme. Die Unterschiede wirken sich allerdings in einigen Bereichen besonders aus.

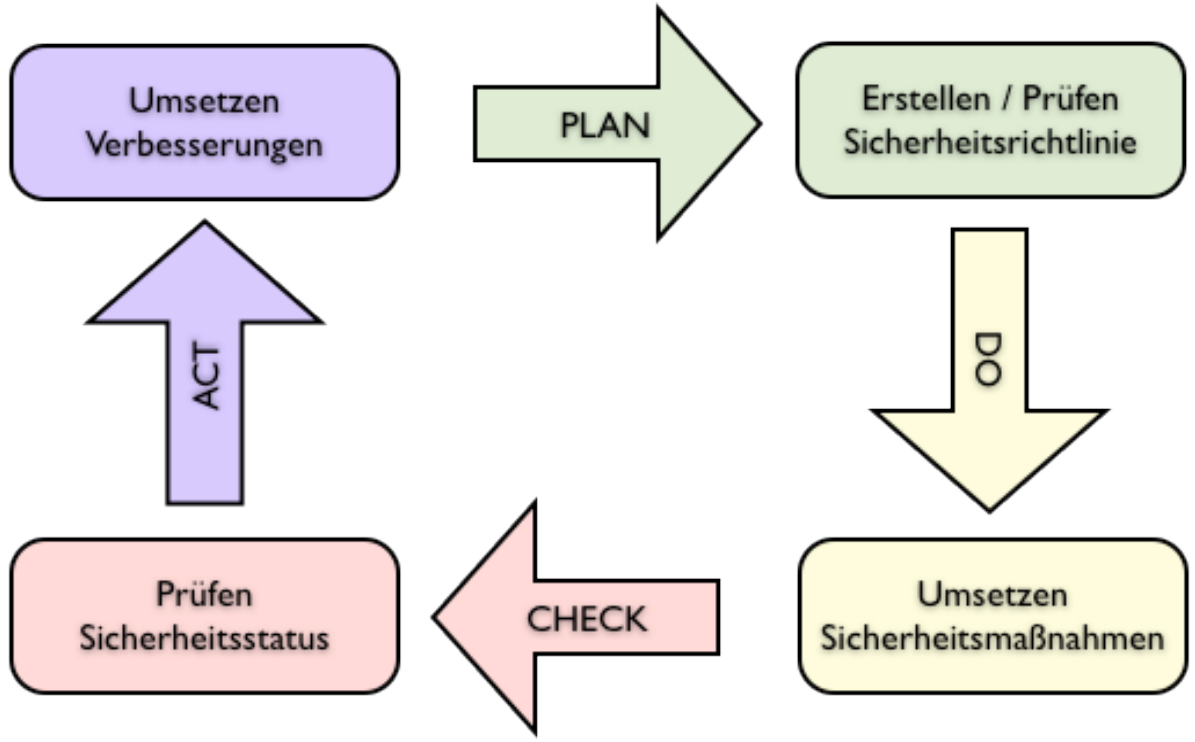


Abb. 8: Deming-Zyklus für Informationssicherheitsmanagement-Systeme.

1. Richtlinien

62

Die Informationssicherheitsrichtlinien sind in den meisten Aspekten identisch zu allgemeineren Sicherheitsrichtlinien. Die Elemente Schutzziele, Zweck, Methoden, Verantwortlichkeiten und Konsequenzen sind im Wesentlichen identisch. Was abweicht, ist die Breitenwirkung der verschiedenen detaillierten Richtlinien auf Arbeitsanweisungsebene.
Dadurch, dass inzwischen fast jeder Mitarbeiter eines Unternehmens mit technischer Informationsverarbeitung in Berührung kommt, sind viele verschiedene Vorgaben von sehr vielen Menschen im Hinblick auf die Informationssicherheit zu beachten. Dies hat zur Folge,

dass die Formulierungen einerseits sehr präzise, andererseits aber auch so allgemeinverständlich formuliert sein müssen, dass jeder durchschnittliche Mitarbeiter beim Durchlesen einer Richtlinie sofort erkennen kann, welche Handlungsoptionen für ihn bestehen. Beispiele sind hier nennenswert: Umgang mit mobilen Endgeräten, Umgang mit vertraulichen Informationen oder Verwendung von firmenfremder IT im Unternehmensnetzwerk sind nur einige Aspekte, die fast jeden Mitarbeiter inzwischen angehen.[14]

63

Eine besondere Situation bildet darüber hinaus der Datenschutz. Datenschutzanforderungen sind natürlich ebenfalls in Informationssicherheitsrichtlinien zu integrieren, und stellen einen großen Reibungspunkt bei der Erstellung der Richtlinien dar, da immer noch viele Unternehmenslenker dazu tendieren, den Datenschutz zugunsten einer scheinbaren besseren „inneren Sicherheit" aufzugeben (und wiederholen die Diskussionen, die auch auf staatlicher Ebene statt finden). Die Lösung besteht darin, Wege zu finden, die sowohl die Sicherheits- als auch die Datenschutzanforderungen erfüllen.[15]

2. Awareness

64

Ein weiteres großes Feld, welches für Informationssicherheitsmanagementsysteme speziell zu betrachten ist, ist der Themenbereich der „Security Awareness". Awareness-Maßnahmen dienen landläufig dazu, eine Informationssicherheitsrichtlinie bekannt zu machen, und für eine Einhaltung der Richtlinie(n) zu sorgen.

65

Das ist deshalb besonders wichtig, weil gerade bei Informationen viele Arbeitsschritte bei einem Mitarbeiter liegen, die nicht technisch „sichergestellt" werden können. Entsprechend gilt es, die Vorgaben, die in den Richtlinien schriftlich bindend erfasst wurden, auch bei den Mitarbeitern zur Umsetzung zu bringen.

66

Gute Awareness-Kampagnen, also solche, die besonders gut zu wirken scheinen, versuchen aber über die reine „Werbung" für eine Richtlinie und deren Einhaltung hinaus das Verhalten und die Optionen im Umgang mit Sicherheit in den Mittelpunkt zu stellen und somit den Mitarbeiter auf einer emotionalen Ebene zu erreichen und letztendlich die Loyalität mit dem Arbeitgeber zu erhöhen. Letztendlich geht es dabei um die Nutzung psychologischer Momente, um die emotionale Bindung von einzelnen Identifikationsmerkmalen auf den Arbeitgeber auszuweiten.[16]

67

Dies spielt insbesondere für den Schutz von Informationen eine sehr große Rolle, da Informationen, die von Mitarbeitern erzeugt, be- und verarbeitet werden, immer auch zu einem großen Teil als die „eigenen" Informationen angesehen werden. Wenn man es also schafft, die Identifikation auf die Organisation zu übertragen, werden die individuellen Entscheidungen, wie etwa eine Information versendet oder behandelt wird, auch bzw. eventuell sogar vorrangig am Wohl der Organisation ausgerichtet - statt am individuellen, eigenen Mehrwert.

68

Entsprechend ist es für ein Unternehmen, welches viel mit vertraulichen Informationen hantiert, sehr lohnenswert, sich über ein professionelles Awareness-Konzept Gedanken zu machen.

---

[14] *Bacik, Sandy*: Building an Effective Information Security Policy, Crc Pr Inc 2008.
[15] *Wytibul, Tim*: Handbuch Datenschutz im Unternehmen, Recht und Wirtschaft 2011.
[16] *Helisch, Michael, Pokoyski, Dietmar*: Security Awareness: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung, Vieweg & Teubner 2009.

3. Informationseigner

69

Ein weiteres wesentliches und für den Bereich der Informationssicherheit typisches Konzept ist das des Informationseigners. Dieses Konzept besagt, dass Informationen immer einen „Eigner“ (engl. „Owner“) haben, und dieser ist für den Schutz der informationellen Werte verantwortlich.

70

Der Informationseigner ist in der Regel der Ersteller einer Information, bzw. der für die Erstellung verantwortliche Abteilungsleiter. Ein Informationseigner sollte über alle Informationen bzw. Informationstypen, für welche er die Verantwortung hat, informiert sein. Im Idealfall kennt der Informationseigner sogar die Schutzmaßnahmen, die mit einzelnen Informationen verbunden sind, um deren Schutzbedarf erfüllen zu können.

71

Das Konzept ist sehr schwer in Organisationen einzuführen, es gibt eine Reihe von Hinderungsgründen. Die meisten sind darin begründet, dass die Mitarbeiter, selbst Führungskräfte, mit dieser Verantwortung nicht umgehen können oder wollen. Hier ist entsprechend Überzeugungsarbeit zu leisten. Ist das Konzept es Informationseigners aber einmal etabliert, ist für jede Informationsart die Verantwortlichkeit klar definiert, und Mitarbeiter gehen mit Informationen genau so verantwortungsvoll um wie mit physischen Ausstattungsgegenständen.

72

Im Zentrum der Verantwortung des Informationseigners liegt die Klassifikation von Informationen in verschiedene Vertraulichkeitsstufen, etwa: „offentlich“, „intern“ und „geheim“.Dokumente sollten mit der Klassifikation versehen sein, damit alle Mitarbeiter „höher“ klassifizierte vertrauliche Dokumente entsprechend den Vorgaben auch bearbeiten bzw. schützen können. Die IT-Abteilung hat dann dafür entsprechende technische Maßnahmen anzubieten, etwa Verschlüsselungsprogramme. Erst wenn diese technischen Möglichkeiten auch verfügbar sind, ist eine Klassifikation sinnvoll, sonst wird die Klassifikation nicht ernst genommen.

4. Einbettung in integrierte Management-Systeme

73

Informationssicherheitsmanagementsysteme lassen sich nahtlos in übergeordnete Management-Systeme einbinden, so z.B. Corporate Security Management Systeme, Qualitätsamanagementsysteme, oder Governance, Risk & Compiance Frameworks. Integration bedeutet hierbei, dass die Richtlinien-Rahmenwerke aneinander angepasst werden müssen, dass ggf. die Controls auf einander „gemappt“ werden müssen und dass die Reporting-Werkzeuge und Berichtslinien angeglichen werden müssen. Dann ist nicht nur eine Integration möglich (im Sinne einer einheitlichen Darstellung), dann ist auch damit die Option verbunden, Synergien zu heben.[17]

74

Es stellt sich jedoch oft die Frage, wie hierbei die Verantwortlichkeit aufgeteilt werden soll. In den meisten praktischen Fällen liegt die Verantwortung für die Einführung und den Betrieb eines ISMS innerhalb der IT-Organisation. Das ist leider für die Durchsetzung von Sicherheitszielen eher schädlich, da dann Sicherheitsziele und andere Managementziele oft aufeinander prallen. Die Integration in übergeordnete Management-Systeme bietet die Chance, in diesem Fall die Verordnung der Richtlinie aus Sicht der IT-Abteilung als „von

[17] *Bailly, Hans-Willi*: Integrierte Managementsysteme: Tipps und Empfehlungen zum Aufbau, Dokumentenbeispiele, TÜV Media 2011.

außen gegeben“ zu betrachten, und dieses als Anlass zu nehmen, mit möglichst effektiven und effizienten Maßnahmen die Vorgaben umzusetzen.

II. Relevante Normen und Standards

75

Zwei Normen haben sich im Bereich der Informationssicherheit in Deutschland durchgesetzt, zum einen ist das die ISO 27000 Familie oder Serie[18], zum anderen der IT-Grundschutz des BSI.[19]

1. Die ISO 27000 Familie

76

Geschichtlich beruht die ISO 27000 Familie auf zwei British Standards, dem BS-7799-1 aus 1995, welcher eine erste Reihe von IT-Kontrollen definiert, die für ein akzeptables Informationssicherheitsmanagementsystem vorhanden sein müssen, und dem BS-7799-2 aus 1998, welcher Anforderungen an ein Informationssicherheitsmanagementsystem für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung enthält. Die ISO Standardisierungsorganisation übernahm den Standard BS-7799-1 aus dem Jahr 1999 und veröffentlichte sie als ISO 17799 im Jahr 2000. Der BS-7799-2 wurde 2005 von der ISO übernommen und als ISO-27001 veröffentlicht. 1998 wurde der ISO 17799 überarbeitet und als ISO 27002 in die 2700X-Reihe integriert. Die beiden Normen ISO 27001 und 27002 liegen seit 2008 auch als DIN Norm vor.

77

Die ISO/IEC 27000-Familie enthält inzwischen folgende Dokumente:

- ISO/IEC 27000: Begriffe und Definitionen
- ISO/IEC 27001: Anforderungen an ein ISMS
- ISO/IEC 27002: IT-Kontrollen als Leitfaden und Prüfgegenstand
- ISO/IEC 27003: Leitfaden zur Umsetzung der ISO/IEC 27001 (Entwurf)
- ISO FCD 27004: Messung der Informationssicherheit (Entwurf)
- ISO FCD 27005: Risikomanagement für Informationssicherheit
- ISO/IEC 27006: Anforderungen an Audit- und Zertifizierungsorganisationen

Darüber hinaus sind eine Menge von fachspezifischen und technischen Normen in Planung.

78

Die bedeutsamsten Standards sind für den Alltag des Informationssicherheitsverantwortlichen die ISO 27001 (für Aufbau und Betrieb) und die ISO 27002 (für die Kontrolle und die Auditierung). Die ISO 27001 ist anwendbar für die folgenden Aktivitäten:

- Zur Formulierung von Anforderungen und Zielsetzungen zur Informationssicherheit
- Zum kosteneffizienten Management von Sicherheitsrisiken
- Zur Sicherstellung der Konformität mit Gesetzen und Regulatorien
- Als Prozessrahmen für die Implementierung und das Management von Maßnahmen zur Sicherstellung von spezifischen Zielen zur Informationssicherheit
- Zur Definition von neuen Informationssicherheits-Managementprozessen
- Zur Identifikation und Definition von bestehenden Informationssicherheits-Managementprozessen
- Zur Definition von Informationssicherheits-Managementtätigkeiten
- Zum Gebrauch durch interne und externe Auditoren zur Feststellung des Umsetzungsgrades von Richtlinien und Standards

79

[18] www.27000.org, abgerufen am 19.12.2011.
[19] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html, abgerufen am 19.12.2011.

Hingegen enthält die ISO 27002 11 Überwachungsbereiche mit 29 Kontrollzielen und 133 Sicherheitsmaßnahmen. Die Überwachungsbereiche sind die folgenden:

- Weisungen und Richtlinien zur Informationssicherheit
- Organisatorische Sicherheitsmaßnahmen und Managementprozess
- Verantwortung und Klassifizierung von Informationswerten
- Personelle Sicherheit
- Physische Sicherheit und öffentliche Versorgungsdienste
- Netzwerk- und Betriebssicherheit (Daten und Telefonie)
- Zugriffskontrolle
- Systementwicklung und Wartung
- Umgang mit Sicherheitsvorfällen
- Notfallvorsorgeplanung
- Einhaltung rechtlicher Vorgaben, der Sicherheitsrichtlinien und Überprüfungen durch Audits

80

Dabei ist wichtig, dass die jeweilige Ausgestaltung der Kontrollziele und Sicherheitsmaßnahmen der Organisation überlassen wird, es gibt also keine konkrete Vorgabe - und damit aber auch keine einfach umzusetzende Richtlinie. Zudem haben die Inhalte der ISO 27002 nur empfehlenden und keinesfalls normativen Charakter. Im Kern der Auswahl steht daher das Risikomanagement, welches durch Anwendung von geeigneten Maßnahmen angemessen reduziert werden muss.

2. IT-Grundschutz nach BSI

81

Unter IT-Grundschutz wird der Schutz von IT- und Informationsinfrastrukturen vor „normalen“ Bedrohungen verstanden. Dabei wird davon ausgegangen, dass für alle Unternehmen und Organisationen die Bedrohung ähnlich ist. Dies ist ein prinzipieller Unterschied zum Ansatz, der der ISO 27000 Serie zu Grunde liegt.

82

Das Bundesamt für Sicherheit in der Informationstechnik, primär verantwortlich für die IT-Sicherheit der Behörden, hat im Rahmen der Entwicklung ihrer IT-Grundschutzkataloge (früher: IT-Grundschutzhandbuch) vorausgesetzt, dass eine detaillierte Risikoanalyse für die meisten Behörden nicht durchführbar ist und hat statt dessen die (s. oben) bereits erläuterte Schutzbedarfsanalyse verwendet. Dabei wird für die meisten, in der Praxis verbreiteten IT-Komponenten von einem normalen Schutzbedarf ausgegangen, für diesen Fall enthalten die IT-Grundschutzkataloge entsprechende Anweisungen und Hinweise, mit welchen Mechanismen den Bedrohungen begegnet werden kann.

83

Das BSI hat dabei großen Wert darauf gelegt, dass die Anweisungen auch für informierte Laien umsetzbar sind. Seit Anfang 2000 sind die Grundschutzkataloge auch im Unternehmensumfeld im Einsatz, und erfreuen sich zunehmender Beliebtheit, speziell bei größeren KMU.

84

Die IT-Grundschutzkataloge enthalten unter anderem die folgenden Elemente:

- Bausteine: Übergreifende Aspekte - Infrastruktur - IT-Systeme - Netze - Anwendungen
- Gefährdungskataloge: Höhere Gewalt - Organisatorische Mängel - Menschliche Fehlhandlungen - Technisches Versagen - Vorsätzliche Handlungen
- Maßnahmenkataloge: Infrastruktur - Organisation - Personal - Hardware und Software - Kommunikation - Notfallvorsorge

85

Als Beispiel seien hier genannt: es gibt 146 Arten von Gefährungen im Bereich „vorsätzliche Handlungen“ und 345 Arten von Maßnahmen im Bereich „Hardware und Software“.
Erst für Schutzziele, die aufgrund der Schutzbedarfsfeststellung einen höheren als „normalen“ Schutzbedarf haben, ist eine Risikoanalyse durchzuführen. Das BSI hat hierzu einen eigenen Standard 100-3 entwickelt.

3. Zertifizierungen

86

Eine Zertifizierung des Informationssicherheitsmanagements ist nach beiden vorgestellten Standards möglich. Im Falle des IT-Grundschutzes gibt es eine Zertifizierung nach BSI-Standard 100-1, welche die Anforderungen des ISO 27001 auf die Vorgehensweise des IT-Grundschutzes (BSI-Standard 100-3) abbildet, und damit mit ein paar Kniffs ermöglicht, in Deutschland ein ISO-27001-Zertifikat „nach IT-Grundschutz“ erwerben zu können.

87

Der eigentliche Aufwand bei einer Zertifizierung besteht nicht darin, die Zertifizierung durchzuführen. Ist die Vorbereitung erfolgreich gewesen, ist diese Arbeit in wenigen Tagen getan. Zudem ist der Preis für das Zertifikat ebenso sehr gemäßigt, die Zertifizierung an sich bewegt sich daher für beide bei ca. 10.000 EUR. Aufwändig hingegen ist aber die Vorbereitung auf die Zertifizierung, um die erforderlichen Dokumente zu erstellen und die identifizierten (ISO) oder vorgeschlagenen (BSI) Maßnahmen auch umzusetzen. Da können die Kosten, je nach Umfeld, schnell explodieren.

88

Man kann sich aber in beiden Fällen aussuchen, welchen „Scope“, also welchen Anwendungsbereich das Zertifikat haben soll. Hier kann man sich z.B. auf eine Unternehmensabteilung (z.B. die interne IT), oder bestimmte Geschäftsprozesse (z.B. Kundendatenverwaltung) konzentrieren, und die Zertifizierung - und eben auch die Maßnahmen - auch nur für diesen Fall für die Zertifizierung betrachten. Hierdurch kann man die Kosten in der Regel deutlich senken.

89

Umgekehrt bedeutet dies aber auch, dass Sie als (potenzieller) Kunde einer Organisation, die eines der genannten Zertifikate stolz ihr eigen nennt, und damit für die Sicherheit der von ihr verarbeiteten Daten wirbt, genau prüfen sollten, was zertifiziert wurde, und ob dieses Zertifikat insofern nahe liegt, dass Ihre Daten dort auch tatsächlich sicher gehalten werden.

D. Technische Aspekte

90

Bei allen organisatorischen Maßnahmen und Modellen, die erforderlich sind, um Informationen einer Organisation angemessen schützen zu können, so ganz ohne technische Maßnahmen ist dies nun auch nicht möglich. In der Folge werden die wichtigsten Felder technischer Informationssicherheit kurz skizziert und beispielhaft Technologien beschrieben, die sich in den jeweiligen Bereichen bewährt haben. Die Informationen aus diesem Kapitel sind zum Teil der Fibel „IT-Sicherheit für den Mittelstand“ von Deutschland Sicher im Netz e.V.entnommen.[20]

I. Angriffstechniken

91

Bei den Angriffen auf Informationen werden fast immer auch technische Werkzeuge eingesetzt, um das Ziel zu erreichen. Dabei setzen die meisten technischen Angriffswerkzeuge

[20] https://www.sicher-im-netz.de/files/images/Fibel_IT_Sicherheit.pdf, abgerufen am 19.12.2011.

eine gewisse – oft ungewollte – Kooperation durch eine Zielperson ein, dies nennt man im Umfeld der Informationssicherheit „Social Engineering“.

1. Computer-Virus

92

Computer-Viren sind Programme oder Teile davon, die entweder von Experten mit zweifelhaften Zielen erstellt werden oder so genannten „Script-Kiddies“ mittels im Internet erhältlicher „Viren-Baukästen“ (so genannte „Virus Construction Kits“) erzeugt werden. Mögliche Schäden durch Computer-Viren sind ausgesprochen vielfältig; sie reichen von der einfachen Ausgabe störender Fenster, über Fehlfunktionen in Anwendungen bis hin zur Löschung vollständiger Datenbestände.

93

Die Verbreitungswege für Viren sind vielfältig: Im Gegensatz zu früheren Zeiten, in denen sich Viren über Disketten verbreiteten, dient heute die E-Mail als wichtigstes Übertragungsmedium. So genannte Makro-Viren verbreiten sich im Wesentlichen durch einfache Weitergabe oder gemeinsame Nutzung von Dokumenten in Netzwerken. Auch speziell präparierte Internetseiten sind ein beliebtes Mittel bei der Verbreitung von Viren.

2. Computer-Wurm

94

Würmer sind sehr populär und stellen eine spezielle Form der Viren dar. Auch hier erfolgt eine Infektion oft über E-Mails oder durch Ausnutzung von Schwachstellen in Anwendungen und Protokollen.

95

Würmer infizieren in aller Regel keinen fremden Programmcode oder Dokumente, sondern sind darauf ausgelegt, sich selbständig und schnell zu verbreiten. Manche Würmer verfügen sogar über Funktionen, die es ihnen erlauben, sich selbst per E-Mail zu verbreiten, ohne dass das installierte E-Mail-Programm genutzt werden muss. Heimtückisch ist auch die Eigenschaft, sich selbst an Adressen aus dem Adressbuch des installierten E-Mail-Programms weiter zu versenden. Dies beschleunigt die Verbreitung, da die Empfänger den Absender der Mail kennen. Es steigt die Wahrscheinlichkeit, dass ein Anhang geöffnet wird.

3. Trojanisches Pferd

96

Wie schon beim echten Trojanischen Pferd verbirgt auch die Computerversion (auch „Trojaner“ genannt) ein schädliches Programm im Bauch eines scheinbar nützlichen Programms. Dieses schädliche Programm installiert sich dann unbemerkt auf dem PC des Opfers.

97

Ziel von solchen Schädlingen ist zum Beispiel die Übermittlung von vertraulichen oder persönlichen Daten an seinen jeweiligen Versender oder die Öffnung des PCs zur Fernkontrolle durch den Hacker.

98

Der klassische Trojaner kann sich nicht selbst verbreiten, heute werden jedoch von Würmern und Viren häufig Trojaner nachinstalliert, die dann eine Kontrolle des PCs durch Dritte erlauben.

99

Eine von Kriminellen oft genutzte Variante des Trojaners sind die so genannten Bot-Netze. Bei einem Bot handelt sich um einen Trojaner, der sich bei seinem „Herrn“ meldet und Instruktionen erwartet. Viele (oft weit mehr als 10.000) mit Bots infizierte PCs bilden dann

ein Bot-Netzwerk. Oft werden derartige Bot-Netze von ihrem Herrn für kriminelle Machenschaften (verteilte Angriffe, Massen-Mailversand) verwendet oder sogar vermietet.

4. Bot-Netze

100

Bot-Netze stellen einen Zusammenschluss von gekaperten Rechnern dar, dabei läuft auf jedem gekaperten Rechner ein zweiter, virtueller Rechner, der ferngesteuert Aktionen für den Hacker ausführen kann. Bot-Netze sind in der Regel ausschließlich an der Rechenkapazität der gekaperten Systeme interessiert, und sind oft für den Anwender ger nicht zu bemerken.
Dennoch finden sich in der Regel auf diesen Rechnern ungesetzliche Anwendungen oder Dienstleistungen, etwa Spam-Versender oder kinderpornografische Webseiten. Aufgrund der möglichen rechtlichen Konsequenzen sind Bot-Netze speziell für Unternehmen nicht ungefährlich. Expertenschätzungen besagen, dass (Stand Herbst 2011) jeder 5. PC mit einem Bot infiziert ist.

5. Angriffe von Webseiten

101

Die meisten Angriffe werden allerdings inzwischen direkt von Webseiten aus ausgeführt, zum Teil sogar von eigentlich „sauberen“ Webseiten, etwa durch Einschleusen von Schadcode in Werbung. Dabei gibt es inzwischen Techniken, wo schon alleine das Aufrufen einer Webseite zur Installation eines Trojanischen Pferdes führen kann („Drive-by-Infection“). Mit Techniken wie Cross-Site-Scripting und Cross-Site-Request-Forgery werden ungewollte Inhalte geladen, oder wird auf Informationen von gleichzeitig geöffneten anderen Webseiten zugegriffen, z.B. Bankdaten.

6. Angriffe auf Webseiten

102

Um ihr Ziel zu erreichen, versuchen Hacker Webseiten unter ihre Kontrolle zu bringen. Dabei ist das öffentlich sichtbare „Defacement“, das nur dazu dient, nachzuweisen, dass man erfolgreich war, noch die harmloseste Variante. Webseiten werden in der Regel durch die Eingabemöglichkeiten angegriffen, dort wird gezielt nach Schwachstellen bei der Programmierung gesucht, und diese zielgerichtet ausgenutzt. Neben der Veränderung der Nutzdaten ist auch ein Ausspionieren von vertraulichen Informationen von hier aus oft kein Problem mehr.

7. Angriffe auf mobile Endgeräte

103

Mobile Endgeräte unterscheiden sich heute in Funktion und Leistungsfähigkeit kaum noch von den klassischen PCs. Entsprechend sind die Angriffe immer ähnlicher geworden. Das Injizieren von Handy-Viren, die kostenpflichtige Nummern anrufen, ist zwar immer noch möglich, wird aber kaum noch wahrgenommen.
Durch die Verwendung von Kameras und Ortungssystemen in jedem mobilen Endgerät stellt sich jedoch eine zusätzliche Gefahrenquelle ein: die Verwendung der Endgeräte des Benutzers als Spionagegerät des Angreifers. Sobald ein Trojaner auf einem mobilen Endgerät installiert ist, ist dies technisch problemlos möglich.

II. Schutzmaßnahmen

104

Der Schutz vor IT-basierten Angriffen auf Informationen wird am besten strukturiert nach den bestehenden Verantwortlichkeiten in der IT-Abteilung. Diese unterscheidet üblicher Weise zwischen Infrastruktur – dazu zählen Endgeräte und Netze –, Kommunikation – mit E-Mail,

Telefonie und Datenablagesystemen – sowie Anwendungen – klassische strukturierte Unternehmensanwendungen, aber auch Web-Seiten und Cloud-Dienste.

1. Schutz der Endgeräte

105

Unter „Endgeräten“ versteht man die Geräte, mit denen Personen arbeiten, um Informationen zu verarbeiten, also PCs, Macs, Notebooks, Netbooks, Smartphones, Pads etc. Sie werden „End“-Geräte genannt, da sie den Endpunkt der Kommunikation zu den meisten Informationsquellen darstellen, also Web-Seiten, Anwendungssystemen, E-Mail-Servern und so weiter. Die wichtigsten Maßnahmen sind – in absteigender Bedeutung – die folgenden:

- Das Betriebssystem des Endgeräts sollte immer auf aktuellem Stand sein.
  Die Sicherheit eines Betriebssystems steht und fällt mit seiner Aktualität. Der Grund hierfür ist, dass rund um die Uhr weltweit von Hackern an Programmen gearbeitet wird, die Schwachstellen in Betriebssystemen ausnutzen. Werden diese bekannt, wird vom Hersteller ein Update bereitgestellt, welches die Schwachstelle schließt (auch Patch genannt). Wird nun ein Betriebssystem nicht regelmäßig aktualisiert, wird es mit der Zeit immer anfälliger für Angriffe. Alle modernen Betriebssysteme bieten inzwischen die Automatisierung der Updates, dies sollte genutzt werden. Aber nicht nur Betriebssysteme müssen aktualisiert werden, inzwischen werden auch Anwendungen auf PCs und Servern über bekannte Schwachstellen direkt angegriffen. Entsprechend sollten auch die Anwendungen regelmäßig aktualisiert bzw. die Verfügbarkeit von Updates und Patches geprüft werden. Dies ist erforderlich, da die meisten Anwendungen bisher keine automatisierte Prüfung durchführen.
- Die Firewall des Betriebssystems sollte immer angeschaltet sein, um einen Schutz vor direkten Angriffen aus dem Internet zu gewährleisten.
  Jedes moderne Endgeräte-Betriebssystem (selbst von Smartphones und Handys) hat heutzutage eine Firewall. Diese schränkt die Erreichbarkeit der auf dem Endgerät betriebenen Anwendungen, die von „außen“ angesprochen werden könnten, ein. Dies ist neben dem Schließen von Sicherheitsproblemen die wichtigste Schutzmaßnahme. Manche Endgeräte erlauben erst gar nicht, die Firewall auszuschalten oder umzukonfigurieren. Dies ist zum Beispiel bei Smartpads oder Smartphones häufig der Fall. Im Sinne der Sicherheit ist dies ideal. Aufwändigere Betriebssysteme ermöglichen aber oft eine individuelle Anpassung der Firewall. Hiervon sollte normalerweise Abstand genommen werden. Häufig behaupten bestimmte Anwendungen (insbesondere im Bereich des Social Networking), dass sie besondere Anforderungen an die Konfiguration der Firewall haben, aber die Erfüllung dieser Anforderungen ist in den allermeisten Fällen auch ohne eine Veränderung der sicheren Einstellungen möglich.
- Die sichere Konfiguration des Web-Browsers ist für Sicherheit bei der Internetnutzung absolut erforderlich.
  Das Thema sichere Konfiguration des Browsers wird oft unterschätzt. Aktive Inhalte und Skriptsprachen, sowie neue Technologien für die Darstellung von Inhalten (wie zum Beispiel Adobe Flash), bergen auch Gefahren. Durch schadhafte Inhalte kann zum Beispiel der Zugriff auf lokale Programme und Daten ermöglicht werden. Ausspähen von persönlichen Daten und die Protokollierung des Surfverhaltens sind ebenso möglich wie die unbemerkte Umleitung auf Seiten mit schadhaften Inhalten. Bei Browsern, die die Verwendung von Plugins erlauben (etwa Mozilla Firefox), ist das Risiko besonders hoch, denn viele Plugins hebeln die eigentlich sichere Standard-Konfiguration der Browser wieder aus. Eine ähnliche Problematik liegt bei den Einstellmöglichkeiten des E-Mail-Anwendungen vor. Lässt man zum Beispiel beim Öffnen einer E-Mail eine HTML-Darstellung zu, so kann man sich die gleichen Viren und Würmer wie mit dem

Browser einfangen. Informationen zur sicheren Konfiguration von E-Mail-Anwendungen und Browsern finden sich auf den Webseiten der jeweiligen Hersteller.

- Der Viren-Scanner prüft E-Mails und aus dem Netz geladene Inhalte auf Schädlinge. Virenscanner helfen nicht nur gegen Viren, sondern inzwischen gegen jede Form von Malware, also bösartigen Software-Elementen. Sie können zum Beispiel automatisierte Angriffe mit Trojanern auf Betriebssystemschwachstellen erkennen, bevor der Hersteller des Betriebssystems ein Update geliefert hat. Sie schließen damit eine wichtige Bedrohungslücke.

106

Auch prüfen Virenscanner längst nicht mehr nur Dateien auf der Festplatte des Endgeräts (daher der Begriff „scannen“). Sie können inzwischen in E-Mails hineinschauen, Dateien, die aus dem Internet geladen werden, überprüfen und verdächtige Aktivitäten, die von Bots herrühren könnten, identifizieren.

107

Vertrauen Sie aber nicht den Virenscannern alleine, denn die Angriffe von Hackern werden immer intelligenter und die Virenscanner erkennen immer weniger der Angriffe.

2. Schutz der Computernetzwerke

108

Unter einem lokalen Netz (auch LAN = Local Area Network genannt) versteht man ein räumlich begrenztes Netzwerk, wie zum Beispiel PCs und Drucker in einem Gebäude oder einer Etage. Meistens bestehen lokale Netze aus zahlreichen Arbeitsplatzrechnern, einem oder mehreren Servern und zentralen Druckern, sowie Netzwerkkomponenten. Das Ziel eines lokalen Netzes ist die Zusammenarbeit der einzelnen Komponenten untereinander und somit das Teilen von Ressourcen, wie zum Beispiel Drucker und gemeinsame Dateiablagen.

109

Der Schutz eines lokalen Netzes erfolgt durch mehrere Komponenten: eine zentrale Firewall regelt als „Pförtner“ die Kommunikation zwischen dem lokalen Netz und dem Internet. Zentrale Content-Filter finden und unterdrücken in von Ihren Mitarbeitern angeforderten Web-Seiten Schädlinge oder unerwünschte Inhalte.

110

Systeme, die vom Internet aus erreicht werden können sollen, sollten in einer dedizierten Netzwerkzone stehen, damit sie, sofern sie erfolgreich angegriffen werden, keinen weiteren Schaden anrichten können. Hierzu wird eine so genannte „Demilitarisierte Zone“ (DMZ) aufgebaut.

111

Virtuelle Private Netze (VPN) erlauben die Kopplung von Standorten und Partnern über das Internet. Durch Authentifikation und Verschlüsselung ist die Sicherheit in einem VPN höher als bei dedizierten Leitungen oder Provider-Lösungen. Firewalls schränken für die Standortkommunikation, die Anbindung von Partnern oder Fernwartungszugänge die Kommunikation auf das notwendige Maß ein und verbessern so die Sicherheit Ihres lokalen Netzes.

112

Für die Anbindung von Heimarbeitsplätzen und mobilen Mitarbeitern kommt eine PC-basierte Softwarelösung zum Einsatz. Auch diese VPN-Technik ist unabhängig von der Art des Internet-Zugangs und kann somit für DSL, Dial-In, WLAN und UMTS benutzt werden. Bei der Anbindung von Heimarbeitsplätzen an das Netzwerk des Unternehmens muss auf eine sichere bzw. starke Authentifizierung geachtet werden. Eine Alternative zu der Einbindung des Endgeräts mit VPN sind „Virtual Desktops“, also virtuellen Maschinen, an die man sich über das Web anmelden kann (zum Beispiel Windows Terminal Services oder Citrix). Damit kann eine Sicherheitsprüfung des Endgeräts entfallen, und im Prinzip ist damit der Zugriff

von jedem Internet-fähigen Rechner aus möglich. Auf jeden Fall sollte auch hier eine starke Authentifizierung erfolgen.

113

Um Funknetze sicher nutzen zu können, kommen die gleichen Schutzverfahren wie bei mobilen Mitarbeitern und Heimarbeitsplätzen zum Einsatz. Baut man hingegen eine WLAN-Struktur selbst auf, so ist zusätzlich erhebliche Sorgfalt bei der Planung und Implementierung der Sicherungsmaßnahmen erforderlich.

114

Noch vor einigen Jahren war die Überwachung des Netzwerks ausschließlich für größere Unternehmen ein Thema. Inzwischen sind zum einen die Standard-Produkte wie Firewalls und VPN-Lösungen in diesem Punkt ausgereift, zum anderen gibt es auch Angebote für kleine und mittelständische Unternehmen, die handhabbar und bezahlbar sind. Bei der Überwachung des Netzwerks geht es darum, Anomalien zu entdecken und gegebenenfalls Angriffe zu identifizieren. Die zentrale, musterbasierte Erkennung von Hacking-Angriffen liefern sogenannte Intrusion-Detection-Systeme (IDS). Sie sind entweder Teil der Firewall oder bilden eigene Installationen. Bei IDS ist zu beachten, dass diese System oft - systembedingt - Fehlalarme auslösen können, sie erfordern also in der Praxis ein aufwändiges Feintuning. Die Zusammenführung der Informationen erfolgt mit einem sogenannten Security Information and Event Management (SIEM) Tool. Diese aggregieren Informationen aus verschiedensten Quellen (zum Beispiel auch die Aktualität der Betriebssysteme von Rechnern im Netz) und können neben einer Bedrohungsanalyse auch Analysen von vorliegenden Angriffen liefern.

3. Schutz von Informationen

115

Die meisten Informationen werden heute per E-Mail ausgetauscht. Entsprechend bietet es sich an, E-Mails auch zu schützen. Hierzu wird Verschlüsselung und Digitale Signatur als Mechanismus eingesetzt. Die Technologien hierfür sind inzwischen vollständig standardisiert und werden von allen gängigen E-Mail-Anwendungen unterstützt. Die Anerkennung der Schlüssel der Kommunikationspartner kann nach unterschiedlichen Prinzipien erfolgen, von stark zentralisiert (die IT-Abteilung entscheidet über das Vertrauen) bis vollständig liberal (der Mitarbeiter ist dafür selbst verantwortlich). Auch die Angebote für entsprechende kryptographische Schlüssel und Zertifikate sind massentauglich.

116

Vertrauliche Daten sollten auf einem Endgerät zusätzlich geschützt werden. Sie sollten auch dann noch sicher sein, wenn das Endgerät einem Dieb in die Hände fällt oder von einem Hacker übernommen werden kann. Entsprechenden Schutz bietet Verschlüsselung. Es gibt drei Varianten:

- Die Festplatte wird vollständig verschlüsselt. Dies bietet sich an, wenn man für das gesamte Unternehmen eine einheitliche, zentral administrierbare Lösung haben möchte. Dies geht nicht bei allen Endgeräten, ist aber für die meisten Standard-Notebooks verfügbar.
- Es wird eine Datei als „verschlüsseltes Dateisystem“ angelegt, welches wie eine zusätzliche Festplatte wirkt. Dies bietet sich für Freiberufler oder kleinere Unternehmen an, für die eine zentrale Administration zu teuer ist.
- Dateien werden einzeln verschlüsselt. Dies ist die flexibelste Lösung, aber auch die am wenigsten kontrollierbare.

117

Betriebssystemhersteller bieten inzwischen Funktionen für alle drei Varianten an. Oft ist der mitgelieferte Schutz für die meisten Bedürfnisse ausreichend, spezialisierte Lösungen unterscheiden sich durch die bessere Administrierbarkeit

118

XING, LinkedIn, Facebook oder Twitter haben Einzug in die Unternehmenskommunikation gehalten. Gerade kleine Anbieter haben durch den Einsatz dieser modernen Tools eine enorme Reichweite und können in Marketing und Kundenbindung große Erfolge aufweisen. Doch die Nutzung dieser Tools ist auch mit Vorsicht zu genießen: Sie erlauben es, vertrauliche Dokumente zu verteilen, und bieten selbst eine den Hackern wohlbekannte Angriffsplattform. Auf Facebook können Mitglieder sogar eigene Applikationen schreiben. Diese können natürlich, genau wie jede andere Web-Seite, gefährliche Inhalte verbergen. Darüber hinaus stellen Sie aber kein generelles Sicherheitsproblem dar.

119

Zunehmend wird das klassische Telefon mit analoger Übertragung durch digitale Varianten ersetzt. Selbst klassische Telefongespräche werden über die Weitverkehrsstrecken oft schon digitalisiert übertragen. Neue Telefonanlagen sind inzwischen komplett digitalisiert bis hin zum Telefon, für dessen Anschluss kein Telefon- oder ISDN-Kabel mehr notwendig ist, sondern ein Netzwerkkabel. Der Einsatz ist äußerst flexibel und erlaubt sehr einfach, auch physisch getrennt sitzende Kollegen virtuell in einer gemeinsamen Telefonanlage zusammen zu bringen. Damit sind aber auch Risiken verbunden. Da die IP-Telefonie in der Regel unverschlüsselte VoIP-Kommunikation verwendet, sind den klassischen Angriffen, wie man sie auch von E-Mail kennt, Tür und Tor geöffnet. VoIP-Angebote sollten daher nur mit Verschlüsselung verwendet werden.

4. Schutz von Anwendungen

120

Viele Unternehmen betreiben Software-Applikationen, die durchaus als geschäftskritisch zu bezeichnen sind, weil entweder ein Großteil des Umsatzes mit einer Applikation erwirtschaftet wird (zum Beispiel Versteigerungsplattformen und Online-Buchläden) oder die Applikation an sich als Produkt vertrieben wird (zum Beispiel Softwarehäuser). In beiden Fällen ist die Sicherheit der Applikationen für ihr Geschäft lebensnotwendig. Immer häufiger sind die daher die Anwendungen selbst das Ziel des Angriffs. Der Trend zum E-Business oder das erfolgreiche Erschließen neuer, transaktionsbasierter Geschäftsfelder kann hierbei ungeahnte Gefahren mit sich bringen. Denn nicht selten sind die dafür maßgeblichen Applikationen nur unzureichend vor individuellen Angriffen geschützt.

121

In vielen Fällen ist der Internetauftritt eines Unternehmens die elektronische Visitenkarte, die repräsentativen Zwecken dient oder Besucher mit Informationen versorgt. Somit ist der Auftritt im Web ein schützenswertes Gut. Ein ungeschützter Webauftritt kann schnell Ziel eines Angriffs werden. Imageschäden durch nicht verfügbare Webseiten oder manipulierte Inhalte können die Folge sein. Durch das Platzieren von illegalen Inhalten können neben rechtlichen Folgen auch zusätzliche Kosten durch erhöhten Datenverkehr entstehen.

122

Die folgenden Schutzmaßnahmen sollten angewendet werden:

- Wird der Webserver in den eigenen Räumlichkeiten betrieben, sollte er in der DMZ aufgestellt werden.
- Wird der Webserver bei einem Dienstleister betrieben (dies sollte der Standard sein), so sollten auch dort die Anforderungen an die Sicherheit des Systems erfüllt werden. Neben einer Besichtigung der physikalischen Schutzeinrichtungen vor Ort sollten die Maßnahmen zum Schutz der IT-Systeme auf Seiten des Dienstleisters schriftlich bestätigt werden.
- Wenn vom Endanwender des Webangebots vertrauliche oder persönliche Informationen an den Webserver übermittelt werden müssen (oder umgekehrt), sollten die Daten mittels SSL (Secure Socket Layer) verschlüsselt werden. SSL ist die gängige

Verschlüsselungstechnologie für Webinhalte. Je nach Vertraulichkeitsstufe ist das passende SSL-Zertifikat zu erwerben. Es gibt dort erhebliche Unterschiede.

- Professionelle Web-Seiten mit E-Commerce-Anwendungen verwenden heute sogenannte „Extended Validation"-Zertifikate. Diese veranlassen den Browser, zusätzliche vertrauensbildende Ansichten zu verwenden (etwa: Web-Adresse oder Web-Seiten-Betreiber in grün, besonders hervorgehoben).
- Der Webserver sollte - wie jeder andere Server auch – immer auf dem aktuellsten Stand sein und fortlaufend mit Sicherheitspatches versorgt werden.
- Zudem sollten regelmäßig Penetrationstests gegen die Webanwendung durchgeführt werden.

123

Bedingt durch die Interaktions- und Eingabemöglichkeiten für den Benutzer bieten E-Commerce-Angebote weit mehr Angriffsmöglichkeiten als statische oder rein informative Internetseiten. Angriffe auf E-Commerce-Anwendungen erfolgen in der Regel über das Ausnutzen von Schwachstellen bei der Eingabeüberprüfung. In der Praxis werden in Standardeingabefelder (zum Beispiel Benutzername) ganze Zeilen mit Programmcode eingegeben, die dann die Applikation veranlassen, etwa mehr Informationen preiszugeben als erlaubt. Dies kann passieren, wenn die Eingaben in Formularfeldern nur unzureichend überprüft werden.

124

Generell gibt es zwei Möglichkeiten, um eine Anwendung auf deren Sicherheit hin zu überprüfen. Man kann den gesamten Programmcode der Anwendung überprüfen oder mit einem Werkzeug automatisiert (mit Hilfe sogenannter Security- oder Application-Scanner) nach Sicherheitslücken suchen. Die Suche nach Sicherheitslücken kann selbstverständlich auch manuell erfolgen, bedeutet aber einen deutlich höheren Aufwand. Wichtig ist, dass beide Varianten durch erfahrene Spezialisten durchgeführt werden.

125

Erweist sich eine Anwendung nach einer Überprüfung als unsicher, bleiben Ihnen zwei Möglichkeiten, darauf zu reagieren. So sollten die entdeckten Schwachstellen auf jeden Fall durch eine Anpassung des Programmcodes behoben werden. Leider ist dies in manchen Fällen mit einem nicht vertretbaren Aufwand verbunden, bzw. dauert eine gewisse Zeit. In diesen Fällen empfiehlt es sich, die Applikation durch eine Spezial-Firewall zu schützen (so genannte Application Layer Gateways oder Applikationsfirewalls). Diese überprüfen zum Beispiel die Eingaben der Benutzer und blocken schadhafte Eingaben. Da diese aber nur bestimmte Angriffe abblocken können (ähnlich wie bei Antiviruslösungen), ist langfristig eine sichere Anwendung die einzig sinnvolle Lösung.

126

Outsourcing nimmt immer mehr zu, und gerade für kleine und mittelständische Unternehmen sind die Angebote für alle Anwendungen der IT in Web-basierter Form (Stichworte: Cloud Computing und Software as a Service) immer überzeugender. Da die Verwendung des Internet inzwischen für fast alle Branchen zum Alltag gehört, kann auch eine Versorgung für Anwendungen im Unternehmen durch Cloud-Angebote sinnvoll vorgenommen werden - wenn die entsprechenden Sicherheitsanforderungen erfüllt sind. Generell ist es aus Sicherheitssicht besser, professionelle Dienstleister in Anspruch zu nehmen, anstatt zu versuchen, die Sicherheit für eine bestimmte IT-Plattform selbst zu verantworten. Dafür sprechen die fokussiertere Ausbildung und das Geschäftsinteresse, die Services auch sicher anzubieten - sonst wandern die Kunden relativ schnell wieder ab. Dagegen spricht, dass Daten in der Cloud prinzipiell mehr Angriffen ausgesetzt sind, und dass meist auch andere Anwender (unter Umständen auch Konkurrenten) bei dem gleichen Dienstleister Kunde sind. Bei der Nutzung von Cloud-Diensten für kritische Unternehmensanwendungen sollte daher insbesondere der Anbieter auf die Einhaltung der eigenen Sicherheitsvorgeben verpflichtet

und die Anwendung regelmäßig – wie eigene Anwendungen auch – auf Sicherheit überprüft werden.

5. Schutz der Identitäten

Ein immer größer werdender Teil der Angriffe im Internet haben nicht mehr direkt die Informationen zum Ziel, sondern zielen auf die Identitätsdaten von berechtigen Personen. Damit können Angreifer nachhaltig Zugriff auf interessante Informationen bekommen. Zu Identitätsdiebstahl gehört nicht nur die Diebstahl von Kreditkartendaten, gerade das Abgreifen von Zugangsinformationen ist besonders einfach und zunehmend interessant.

127

In einem Unternehmen sollten daher die Identitätsdaten nicht dezentral bei jeder Anwendung verwaltet werden, sondern idealer Weise zentral administriert werden, um die Gefahr eines zu unsicheren Umgangs mit Identitätsdaten bei den einzelnen Anwendungen zu minimieren. Dies nennt man Identitätsmanagement. Identitätsmanagement-Lösungen sind inzwischen marktreif, die Protokolle zur Interaktion mit Anwendungssystemen sind standardisiert. Die größte Schwierigkeit bei der Einführung liegt darin, mit den Befindlichkeiten der betroffenen IT-Verantwortlichen umzugehen, denn viele IT-Systemverantwortliche begreifen die Identitätsdaten in den Systemen als „ihre“ User.

128

Ein zentrales Identitätsmanagement erlaubt auch die Zentralisierung, also die zentrale Administration der Passwörter. Es gibt einfache Regeln für gute Passwörter, diese sollten vom Identitätsmanagementsystem unterstützt werden:

- Zu einfache Passwörter vermeiden: Namen, Begriffe aus dem Duden, Kfz-Kennzeichen oder Geburtsdaten sind unsicher. Mindestens acht Zeichen mit verschiedenen Zeichensätzen sind erforderlich.
- Konstruieren eines leicht einzuprägenden Passworts, indem man sich einen einfachen Satz einprägt, wie zum Beispiel „Ich benutze immer ein sicheres Passwort am Computer“. Von diesem Satz werden die ersten Buchstaben jedes Wortes verwendet. Im Beispiel ergibt sich das Passwort „Ibi1sPaC“.
- Eine Alternative für ein gutes Passwort ist, zwei einfache Wörter, die gemeinsam keinen Sinn ergeben, hinter einander zu stellen. Dabei sollte das Passwort aber mindestens 12 Stellen haben. Beispiel „Elefantenrakete“.
- Ändern der sogenannten Standard-Passwörter: Voreingestellte Passwörter, zum Beispiel die des Herstellers bei Auslieferung von Computern, sollten sofort durch eigene Passwörter ersetzt werden.
- Passwörter sollten regelmäßig, aber nicht zu oft geändert werden - zum Beispiel alle 2 Jahre, aber sofort, wenn das Passwort unberechtigten Personen bekannt geworden ist. Wird das Passwort häufiger geändert, wird es oft aufgeschrieben oder nach einem einfachen Verfahren modifiziert, was es leichter zu erraten macht.

129

Zunehmend werden Endgeräte mit biometrischen Authentifizierungstechnologien, etwa einem Fingerprintsensor, ausgestattet. Biometrie ist ein zweischneidiges Schwert: Auf der einen Seite steht hoher Komfort und, bei Verwendung hochqualitativer Technologie, auch eine gute Erkennungsrate, aber andererseits werden Authentifizierungsdaten gesammelt, die man nicht wieder zurückziehen kann. Entsprechend ist die Akzeptanz oft nicht groß. Neben Fingerprint-Sensoren, für die es Standard-Lösungen für die Anmeldung zum Beispiel an Notebooks und Smartphones gibt, könnten auch noch die Spracherkennung und die „Tipp-Erkennung“ für einen Einsatz interessant sein. Komplexere Lösungen sind nur für den Einsatz von Hochsicherheitsbereichen geeignet.

130

Eine gute Alternative sind so genannte Zwei-Faktor-Authenfizierungsverfahren, wie z.B. Tokens, die Einmalpasswörter erzeugen. Diese bieten Komfort und gleichzeitig Sicherheit. Sie sollten für den Zugang zu Unternehmensressourcen von außen eingesetzt werden, sowie auch für Anwendungen mit höheren Sicherheitsanforderungen.

131

Chipkarten mit einem Kryptochip, so genannte Smart Cards, sind nun in einigen Unternehmen schon mehrere Jahre im Einsatz. Mit dem neuen elektronischen Personalausweis bietet sich die Chance, eine flächendeckende Lösung einzusetzen, wo das Identitätsmanagement durch den Staat geleistet wird.