1 Aufgaben und Ziele der Informationssicherheit

Einleitung

Viele Trends von der Einbindung von Kunden und Partnern in die eigenen Prozesse über mobile Anwendungen bis hin zu Industrie 4.0 verstärken die Integration unternehmensinterner Abläufe in die Informationstechnik. Damit wächst auch die Abhängigkeit der Geschäftsprozesse vom Funktionieren der Technik und der Verfügbarkeit korrekter Datenbestände. Die in der Literaturliste am Ende dieses Kapitels aufgeführten Studien zeigen, dass die Probleme der Informationssicherheit und die durch Angreifer verursachten Schäden kontinuierlich zunehmen.

Bei den Angriffen ist eine deutliche Kommerzialisierung feststellbar. Ging es bis vor einigen Jahren noch um »Ruhm« und »Ehre« der sogenannten Hacker[1], so spielen inzwischen finanzielle Motive die Hauptrolle. Mit Kryptotrojanern und MiningBots kann man viel Geld verdienen. Die Vermietung von Bots bis hin zur Erpressung von Onlineanbietern mit der Androhung verteilter Denial-of-Service-Angriffe sind keine Seltenheit. Zudem wird Wirtschaftsspionage gezielt über IT-Systeme und Anwendungen betrieben. Das unerlaubte Kopieren oder Versenden von Daten mit Geschäftsgeheimnissen oder die Auftragsentwicklung eines Trojaners, um einen Wettbewerber gezielt ausspähen zu können, sind durch reale Fälle belegt. Neben diesen primär wirtschaftlich motivierten Angriffen nehmen auch politisch motivierte Attacken in Form von »Cyber War« und »Cyber-Terrorismus« zu.

Um der hohen Abhängigkeit von Informationstechnik, den modernen und vielfältigen Angriffsformen und den rechtlichen Vorgaben Rechnung zu tragen, muss das Thema Informationssicherheit im Unternehmen mit einer klaren Strategie geordnet angegangen und umgesetzt werden. Dies soll durch ein Informationssicherheits-Managementsystem (ISMS) erreicht werden. Ohne ein ISMS bestehen große Risiken für die Werte und die Produktionsabläufe des jeweiligen Unternehmens.

Der erste Abschnitt dieses Kapitels gibt einen kurzen Überblick über die wichtigsten Aspekte eines ISMS. Anschließend werden im zweiten Abschnitt die grundlegenden Sicherheitsziele dargestellt, die häufig als Ausgangspunkt zur Auswahl von Sicherheitsmaßnahmen herangezogen werden. Diese Einleitung stellt damit zugleich den inhaltlichen Rahmen der T.I.S.P.-Kurse und der Prüfung für das T.I.S.P.-Zertifikat auf und soll den Einstieg ins Thema erleichtern.

1 Nach dem Selbstverständnis der Szene ist der Begriff Hacker nicht negativ besetzt. Ein Hacker ist eine Person mit hohem Begeisterungsgrad für technische Zusammenhänge, der auch nach Lücken in IT-Systemen sucht und darüber informiert. Sein Ziel ist es, durch Hinweise auf Schwachstellen aufzuklären, vor Gefahren zu warnen und gegebenenfalls auch zu einer Verbesserung der Technik beizutragen. Der Begriff wird heute aber häufig als Synonym für einen Angreifer verwendet.

1.1 Aufgaben und Anforderungen eines ISMS

Ein Informationssicherheits-Managementsystem (englisch: Information Security Management System) soll geordnete Prozesse zum Umgang mit den Problemstellungen der Informationssicherheit bereitstellen. Ein ISMS benötigt:

- eine Informationssicherheits-Organisation, mit Rollen und Ressourcen sowie Regelungen zur Verantwortung,
- definierte Prozesse, in denen Risiken erfasst und bewertet werden (Risikomanagement mit Analyse von Gefährdungen und Angreifermodellen) sowie ein Sicherheitskonzept, in dem dokumentiert wird, welche Maßnahmen ergriffen werden sollen, um ein angestrebtes Sicherheitsniveau zu erreichen,
- Maßnahmen, mit denen die Einhaltung der Sicherheitsvorgaben überprüft werden.

Eine Übersicht zu den Elementen eines ISMS geben die folgenden Abschnitte, weitere Details zum Aufbau und Betrieb eines ISMS sind in Kapitel 5 und unter dem Blickwinkel des IT-Grundschutzes in Kapitel 6 dargestellt.

1.1.1 Risikomanagement

Die Möglichkeit eines Schadens wird als Risiko bezeichnet, wobei die Höhe des Risikos von der Wahrscheinlichkeit des Eintritts und der Schadenshöhe bestimmt wird. Risiken sollen für ein Unternehmen nur in dem Umfang bestehen, der als tragbar bewertet wird. Um zu wissen, welche Risiken für ein Unternehmen bestehen, muss identifiziert und bewertet werden,

- welche Gefährdungen zu Störfällen führen können,
- welche Sicherheitsmaßnahmen die Wahrscheinlichkeit von Störfällen vermindern oder den Schaden begrenzen sollen und
- welche Restrisiken verbleiben und vom Unternehmen getragen werden müssen.

Genau dies ist die Aufgabe des Risikomanagements: Die unternehmensspezifische Bewertungsmethodik[2] für die Faktoren von Risiken und für »tragbare« Risiken zu entwickeln sowie den Analyseprozess umzusetzen und laufend zu überwachen. Im Mittelpunkt dazu steht die Bestandsaufnahme der Unternehmenswerte, die Zusammenstellung der Gefährdungen, durch die Schäden der Unternehmenswerte auftreten können und die Bewertung der gewonnenen Ergebnisse.

Als Grundlage für das Risikomanagement mit Bezug zu Informationen und IT-Systemen sind insbesondere die folgenden Fragestellungen zu klären:

2 Hierfür wird in der Regel eine qualitative Bewertung, z. B. mit den Stufen niedrig, mittel und hoch, ausreichen. Die mathematische »Berechnung« eines Risikowertes ist dagegen in den meisten Fällen problematisch. Zum Beispiel tragen einfache Formeln, wie die Multiplikation von Wahrscheinlichkeit und Schadenshöhe, der existenziellen Bedeutung hoher Schäden für ein Unternehmen nur unzureichend Rechnung. Für eine aussagekräftige Berechnung liegen in der Praxis auch kaum die notwendigen validen Ausgangswerte vor.

- Welche Werte hat das Unternehmen oder die Institution? Mit welchen Geschäftsprozessen wird Umsatz und Rendite erwirtschaftet? Welches sind die wichtigsten Geschäftsprozesse?
- Welche IT-Ressourcen sind zur Unterstützung dieser Geschäftsprozesse erforderlich? Welche Systeme und Anwendungen werden benötigt? Welche Möglichkeiten bestehen, die Prozesse mit eingeschränkter oder ohne IT-Unterstützung weiter zu führen?
- Welche Schwachstellen sind in den Architekturen, Systemen und Anwendungen vorhanden, die zu Störungen führen können? Welchen weiteren Gefährdungen sind die Prozesse ausgesetzt? Wie können diese erfasst und systematisiert werden?
- Welche Schäden können auftreten, wenn die verschiedenen Gefährdungen eintreten? Wie wirken sich Störungen beispielsweise auf Produktion, Vertrieb, Umsatz, Kundenbindung oder öffentliches Ansehen der Organisation aus?

Im Rahmen der Bewertung der Risiken wird entschieden, welche Risiken durch Gegenmaßnahmen vermindert werden sollen und welche tragbar sind. Gegebenenfalls können Risiken auch externalisiert werden, beispielsweise durch vertragliche Regelungen mit Lieferanten oder durch Versicherungsverträge.

Veränderungen im Unternehmen, die Umgestaltung von Geschäftsprozessen und die Entwicklungsdynamik der Informationstechnik führen dazu, dass sich die Risiken und die Wirksamkeit der Sicherheitsmaßnahmen im Laufe der Zeit verändern. Die Risikoanalyse für ein Unternehmen kann deshalb nicht eine einmalige Bestandsaufnahme sein, sondern muss als regelmäßig wiederkehrender Prozess organisiert werden. Ein definierter Risikomanagementprozess soll erreichen, dass Risiken möglichst frühzeitig identifiziert und im Verlauf der Zeit beobachtet werden. Je früher Risiken festgestellt und bewertet werden können, desto eher kann von den Entscheidungsträgern festgelegt werden, wie mit ihnen umgegangen werden soll.

1.1.2 Gefährdungen erkennen und bewerten

Der zentrale Faktor für die Wahrscheinlichkeit von Störfällen im Bereich der Informationsverarbeitung sind Gefährdungen. Beschäftigt man sich mit der Frage, in welcher Form informationsverarbeitende Prozesse gefährdet sind, können vielerlei Möglichkeiten identifiziert werden, durch die die technischen Prozesse gestört, Daten verändert oder vernichtet sowie Informationen unbefugt eingesehen werden können.

Zu den **unbeabsichtigten Ursachen** von Schäden gehören insbesondere Feuer, Wassereinbruch oder Hardwaredefekte (z. B. Festplattenausfälle). Auch die Fehlbedienung durch Benutzer oder Administratoren können dieser Kategorie zugeordnet werden. Für **Gefährdungen aus Angriffsszenarien** müssen die Möglichkeiten absichtlicher Manipulationen und Störungen betrachtet werden, hierbei können sowohl Außentäter als auch Innentäter eine Rolle spielen. Für die Bewertung von Risiken sind daher Angreifermodelle auszuwählen, die für die Organisation relevant erscheinen. Die Angreifer können ihre Ressourcen einsetzen, um Angriffsszenarien zu realisieren, beispielsweise das Eindringen in IT-Systeme, das Abhören von Kommunikationsverbindungen oder gezielte Angriffe gegen einen Prozess. Details zu Angriffsmethoden sind unter anderem in Kapitel 4 dargestellt.

Auch Schwachstellen in der Software dienen Angreifern als Ansatzpunkte. Bei diesen Schwachstellen handelt es sich oft um konzeptionelle Fehler, wie fest implementierte Kennwörter, schwache Kryptografie oder die unzulängliche Prüfung von Benutzereingaben.

Schwachstellen aufgrund von Fehlern in der Software werden vom Hersteller des Produkts verursacht und können vom Betreiber kaum vermieden werden. Umso wichtiger ist es, für die Systeme und Anwendungen durch ein geordnetes Patch-Management zeitnah für einen möglichst aktuellen Stand der eingesetzten Produkte zu sorgen.[3] Eine wesentliche Weichenstellung wird aber schon mit der Auswahl der Softwareprodukte vorgenommen. Um spätere Gefährdungen zu vermindern, müssen die qualitativen Anforderungen an die Software definiert sowie ausreichende Ressourcen für die Umsetzung und Prüfung von Sicherheitsanforderungen bereitgestellt werden.

Das IT-Grundschutz-Kompendium des BSI (Bundesamt für Sicherheit in der Informationstechnik) enthält eine gut strukturierte Sammlung von elementaren Gefährdungen. Sie bieten somit einen sehr guten Ausgangspunkt zur Erfassung und Beurteilung von Gefährdungen und Risiken für die eigene IT-Landschaft. Als ein Teil dieser Fragestellungen müssen Angreifermodelle betrachtet werden.

1.1.3 Angreifermodelle betrachten

Sicherheitsmaßnahmen sollen einerseits kostengünstig und andererseits wirksam sein. Ein Zuwenig an Maßnahmen gegen Angriffe könnte leerlaufen, die Investitionen würden nur eingeschränkt wirken. Würden dagegen Maßnahmen gegen unrealistisch Angriffe realisiert, sind unnötige Kosten zu erwarten. Um Sicherheitsmaßnahmen sinnvoll auswählen und kombinieren zu können, muss geprüft werden, welche Angreifer und Angreifermodelle in den Angriffsszenarien zu berücksichtigen sind.

Viele Fälle aus der Praxis zeigen, dass Störungen und Informationsabfluss nicht von »außen«, sondern absichtlich oder fahrlässig durch die Mitarbeiter verursacht wurden. Einige Länder geben offen zu, dass die eigenen Geheimdienste für die jeweilige Industrie auch Spionage betreiben und dazu entweder versuchen, Mitarbeiter des Zielunternehmens anzuwerben, eigene Mitarbeiter einzuschleusen oder über externe Wege an die gewünschten Informationen zu gelangen. Neben dem mehr oder weniger anonymen Angreifer aus dem Internet sollten deshalb gezielte Ausforschung, Interessen der Mitbewerber oder eigene Mitarbeiter bei den Betrachtungen berücksichtigt werden.

Die Überlegungen zu Angreifermodellen münden unter anderem in Annahmen zu den Ressourcen, die einem potenziellen Angreifer zur Verfügung stehen. Werden diesen die Werte des Unternehmens gegenübergestellt, kann entschieden werden, ob z. B. nur gegen einen Gelegenheitstäter aus dem Internet, gegenüber verärgerten Mitarbeitern oder möglichst auch vor einer Institution mit professionellen Angriffsmöglichkeiten Schutz geboten werden soll. Diese Entscheidungen gehen in die Identifikation von Angriffsszenarien und damit die Risikoanalyse ein.

3 Aktuelle Meldungen zu Schwachstellen und Software-Patches kann man den einschlägigen Newstickern und Mailinglisten entnehmen, Beispiele siehe Literaturverzeichnis am Ende dieses Kapitels.

1.1.4 Hauptursachen für Sicherheitsprobleme identifizieren

Die Hauptursachen für Sicherheitsprobleme werden in der Regel in den »Hackern« oder »unachtsamen Mitarbeitern« gesehen. Die Verantwortlichen für die Informationsverarbeitung müssen sich aber vor Augen führen, dass die wirklichen Ursachen oft tiefer liegen.

Voraussetzungen für erfolgreiche Angriffe sind oft Schwachstellen in der Software. Auch viele unbeabsichtigte Fehler könnten durch »gute« Software vermieden werden. Fehler in den Programmen entstehen oder werden übersehen, weil Software häufig unter sehr hohem Zeitdruck entwickelt wird. Das Einhalten des Release-Termins wird hoch priorisiert, Maßnahmen zur Qualitätssicherung dagegen zurückgestellt. Solche Produkte erscheinen gelegentlich als »Bananen-Software«: Die Software reift beim Kunden. Die Qualitätssicherung wird erst durch den Anwender durchgeführt. Die Lernkurve beinhaltet dann potenziell viele Störfälle durch Fehler wie auch Angriffe. Unzureichende Qualitätssicherungs- und Abnahmeprozesse sind deshalb eine der Hauptursachen für Sicherheitsprobleme.

Eine weitere Ursache für Sicherheitsprobleme wird oft in der Komplexität der jeweiligen IT-Landschaft gesehen. Dazu tragen die Abhängigkeit der zahlreichen IT-Komponenten untereinander, die sich ständig ändernde Technologie oder auch die Kompliziertheit von einzelnen Softwarelösungen bei. Auch wenn diese Aspekte eine Rolle für Sicherheitsprobleme spielen, tragen zu Störfällen mit komplexen Ursachen und Manipulationsmöglichkeiten eher die unzureichende Kapselung von Teilsystemen und die daraus entstehenden unerwarteten Wechselwirkungen bei. Schnelle, unbedachte Einführungsprozesse, die solche und andere Randbedingungen für die Informationssicherheit nicht berücksichtigen, tragen dann zu Sicherheitsproblemen und Unternehmensrisiken bei.

Schließlich fehlt es oft auch bei Produkten mit hohem Qualitätsstandard an den notwendigen personellen Ressourcen, um sie mit den gebotenen Sicherheitsmechanismen einzusetzen. Viele sinnvolle Sicherheitsfunktionen werden in der Praxis wegen Zeitdruck, aus Unkenntnis oder aus Bequemlichkeit nicht genutzt. Der Mangel an Ressourcen, und damit sind vor allem Zeit und qualifizierte Mitarbeiter gemeint, ist eine weitere wesentliche Ursache für Sicherheitsprobleme. Um dieser Ursache zu begegnen, muss den Sicherheitszielen von der Unternehmensleitung ein hoher Stellenwert eingeräumt werden. Mitarbeiter müssen dazu qualifiziert werden und die zeitlichen Spielräume bekommen, um Sicherheitsmaßnahmen im Alltag umzusetzen.

Um effektiv auf Sicherheitsprobleme reagieren und Schwachstellen möglichst von vorneherein vermeiden zu können, muss die Organisation ein Sicherheitskonzept erstellen und umsetzen.

1.1.5 Sicherheitskonzept erstellen

Es erscheint sinnvoll, auf Sicherheitsprobleme wirksam zu reagieren. Daher muss festgelegt werden, welche nicht tragbaren Risiken wie zu vermindern sind. Im Sicherheitskonzept werden deshalb den in der Risikoanalyse erkannten Sicherheitsproblemen systematisch die Maßnahmen zu ihrer Verringerung oder Vermeidung gegenübergestellt. Eine bewährte Praxis ist es, Maßnahmen gegen Bedrohungen anhand von vier generischen Sicherheitszielen der Informationssicherheit abzuleiten. Die Maßnahmen umfassen alle Bereiche, wie technische, bauliche, organisatorische, personelle, informationstechnische

Maßnahmen oder auch Maßnahmen der Qualifikation und Motivation von Mitarbeitern (Awareness). Im Sicherheitskonzept müssen die Verantwortlichkeiten und das Vorgehen für die Umsetzung der Maßnahmen geregelt sein. Dadurch soll gewährleistet werden, dass die finanziellen und personellen Ressourcen für die Umsetzung zur Verfügung stehen.[4]

Das Sicherheitskonzept soll ebenso alle Phasen im Lebenszyklus von Geschäftsprozessen oder IT-Produkten berücksichtigen. Wie oben dargestellt, ist das richtige Prozessdesign oder die Auswahl geeigneter Softwareprodukte für das erreichbare Sicherheitsniveau genauso wichtig, wie die Maßnahmen während der Einführung und des Betriebs. Aber auch das »Lebensende« von Datenbeständen muss einbezogen werden, in dem die Verantwortlichen ein sicheres Löschen und eine adäquate Entsorgung von Datenträgern gewährleisten.[5]

Die Auswahl und Gestaltung der Maßnahmen im Sicherheitskonzept wird von mehreren Faktoren beeinflusst. Im Vordergrund steht regelmäßig die Bewertung der Eignung und des Nutzens von Maßnahmen unter Berücksichtigung der monetären Kosten wie auch der betrieblichen Aufwände und des Beitrags zur Verbesserung des Sicherheitsniveaus. Häufig muss auch zwischen Zielkonflikten balanciert werden. So kann die durchgängige Verschlüsselung von Daten in bestimmten Störfallszenarien zu einem Datenverlust führen, wenn nicht mehr auf den notwendigen Schlüssel zurückgegriffen werden kann. Zielkonflikte zwischen Sicherheitsmaßnahmen auf der einen Seite und der Eignung für die Nutzer auf der anderen Seite treten immer dann auf, wenn zusätzliche Eingaben erwartet werden, weitere Voraussetzungen erfüllt sein müssen (z. B. »Chipkarte muss stecken«), Laufzeitverzögerungen nicht akzeptiert werden oder ein erforderliches Know-how benutzerseitig nicht gegeben ist. Die Auswahl von Maßnahmen muss deshalb in die Sicherheitskultur des Unternehmens passen und auch die Anforderungen an eine gute Ergonomie berücksichtigen.

Das Sicherheitskonzept muss in Form eines oder mehrerer Dokumente schriftlich vorliegen. Nur so kann diese komplexe Aufgabenstellung bewältigt und Entscheidungen nachvollzogen werden. Ein dokumentiertes Sicherheitskonzept ist zudem eine zwingende Voraussetzung, um beispielsweise durch Audits überprüfen zu können, ob die Sicherheitsmaßnahmen umgesetzt sind.

Für den Aufbau eines Sicherheitskonzepts gibt es keine formale Vorgabe oder Vorgehensweise. Eine Orientierung an etablierten Standards wie beispielsweise dem IT-Grundschutz (siehe Kapitel 6) wird empfohlen. In der Regel bietet es sich an, das Gesamtkonzept auf mehrere Dokumente aufzuteilen. Dazu sollte vorab eine Dokumentationsstruktur festgelegt werden, so dass die Informationen nicht redundant dargestellt werden und mit möglichst geringem Aufwand gepflegt werden können.

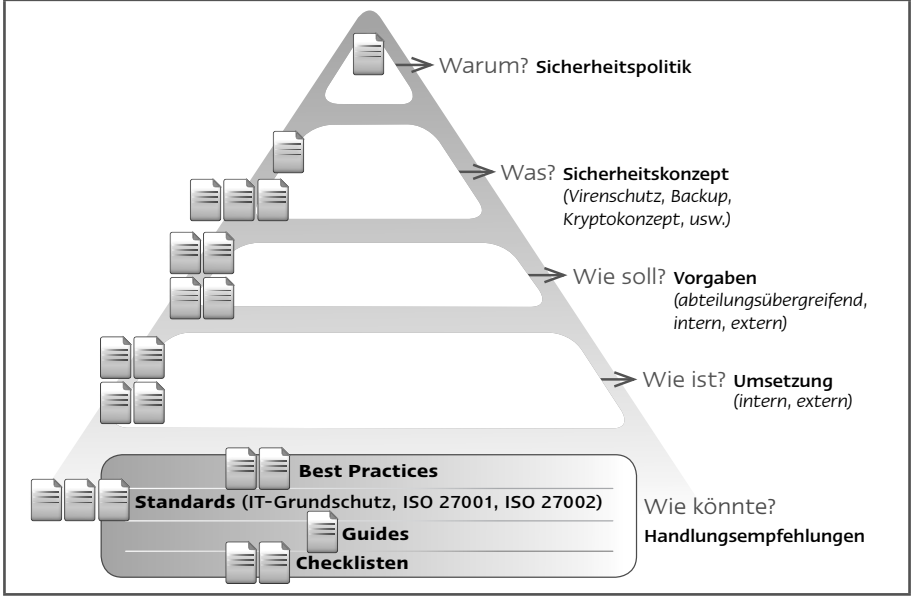
Ein hierarchischer Ansatz bietet den Vorteil, dass allgemeine Teile »vor die Klammer« gezogen werden können. Auf den unteren Ebenen können die Dokumente dann auf Zielgruppen ausgerichtet werden, z. B. nach Verantwortlichkeiten oder für Umsetzungsbereiche, sowie konkrete technische Vorgaben für einzelne Systeme oder Systemgruppen.

4 Siehe dazu auch Kapitel 7

5 Siehe dazu auch Kapitel 19

Für die Durchsetzung der Sicherheitsmaßnahmen ist es entscheidend, dass das ISMS und das Sicherheitskonzept von der Unternehmensleitung in einer Sicherheitsleitlinie verankert wird. Nur wenn so deutlich wird, dass die Geschäftsführung Informationssicherheit als ein wichtiges Unternehmensziel sieht und die Ressourcen dafür bereitstellt, haben die Verantwortlichen für Informationssicherheit den notwendigen Rückhalt.

Abbildung 1.1: Beispiel für eine Dokumentenstruktur im ISMS



Die Geschäftsprozesse, die Risikobewertung wie auch die eingesetzten Techniksysteme unterliegen regelmäßigen Veränderungen. Deshalb muss auch das Sicherheitskonzept regelmäßig überprüft und an die Veränderungen angepasst werden.

1.1.6 Sicherheitsmaßnahmen überprüfen

In Organisationen besteht aus unterschiedlichen Gründen häufig eine mehr oder weniger große Abweichung zwischen den Vorgaben für Prozesse und Systeme und der Betriebspraxis. Dies gilt leider auch für die Sicherheitsmaßnahmen und -prozesse. Um zu gewährleisten, dass die Sicherheitsmaßnahmen umgesetzt werden, ist es deshalb notwendig, zu überprüfen, wie sie realisiert sind. Eine sinnvolle Prüfung ist nur möglich, wenn es eine definierte Soll-Vorgabe gibt. Idealerweise wird das Sicherheitskonzept mit den nachgeordneten Dokumenten so gestaltet, dass diese Soll-Vorgabe und damit die Prüfbedingungen einfach abgeleitet werden können.

Die Analyse von Sicherheitsvorfällen ist eine zweite wichtige Quelle für die Überprüfung des Sicherheitskonzepts. Sie kann Erkenntnisse zum Incident-Prozess und zur Wirksamkeit von technischen Maßnahmen sowie organisatorischen Prozessen liefern. Durch geplante interne oder externe Audits kann zusätzlich festgestellt werden, ob Lücken im Sicherheitskonzept oder der Umsetzung bestehen. Sie bilden somit eine gute Grund-

lage die Realisierung des Konzepts und die Wirksamkeit der Maßnahmen zu überprüfen (siehe auch [Gora07]).

Die Prozesse des Informationssicherheitsmanagements müssen gewährleisten, dass die Ergebnisse der Überprüfungen in die nächste Risikobewertung einfließt. Auch die Maßnahmen des Sicherheitskonzepts sind hinsichtlich der Wirksamkeit und der Kosten-/Nutzen-Aspekte neu zu bewerten, soweit die Erkenntnisse dafür relevant sind. Falls notwendig, muss im Sicherheitskonzept bei der Auswahl von Maßnahmen und der Gestaltung von Prozessen entsprechend nachgesteuert werden.

1.2 Generische Sicherheitsziele

Die Auswahl von Maßnahmen und die Gestaltung des Sicherheitskonzepts werden an den Sicherheitszielen der Organisation ausgerichtet. Als Grundlage für die spezifischen Sicherheitsziele ist es sinnvoll, die vier generischen Sicherheitsziele der Informationssicherheit heranzuziehen. Sie haben sich seit den 90er-Jahren etabliert und zielen darauf, die folgenden Eigenschaften von Daten zu gewährleisten:

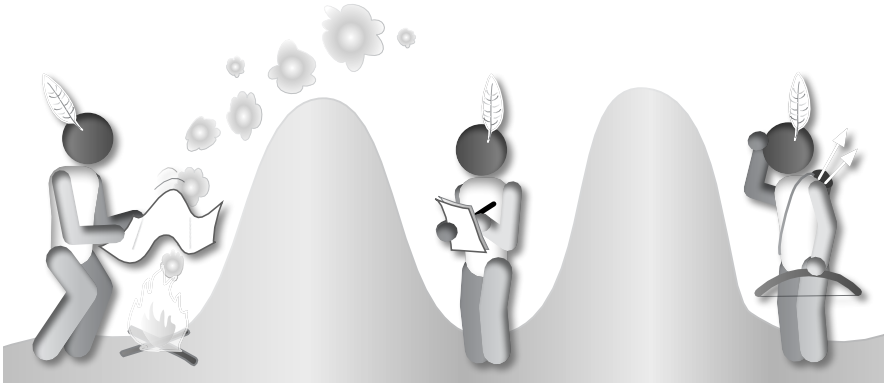
- **V**ertraulichkeit
- **I**ntegrität
- **V**erfügbarkeit
- **A**uthentizität

Diese vier Sicherheitsziele werden auch oft als VIVA-Kriterien bezeichnet und sind in Form dieser Abkürzung gut zu merken. Im Folgenden werden diese vier generischen Sicherheitsziele kurz vorgestellt.[6]

6 Auf weitere Sicherheitsziele wird im Index unter dem Stichwort »Sicherheitsziele« verwiesen.

1.2.1 Vertraulichkeit

Abbildung 1.2: Verlust der Vertraulichkeit



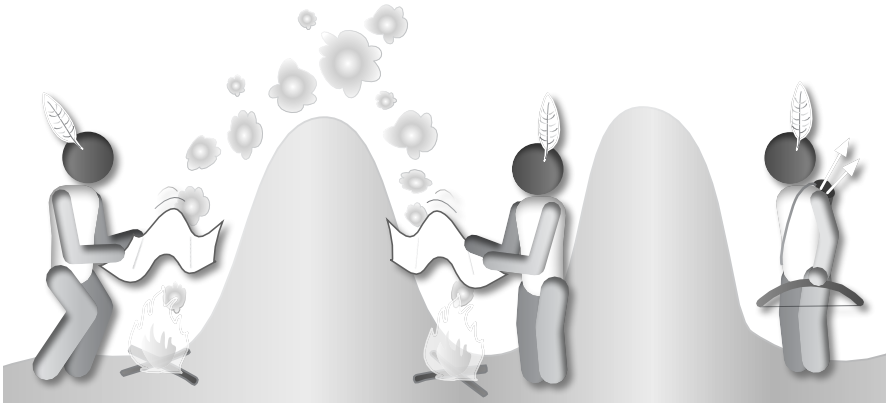
Grafikvorlage: Secunet AG, Foliensatz 2007

Für das Ziel Vertraulichkeit muss der Schutz von Informationen vor der Kenntnisnahme durch unbefugte Personen gewährleistet werden. Um die Vertraulichkeit zu erreichen, können beispielsweise für den Zugriff auf Datenbestände in Anwendungen oder für die Zugriffssicherung von Dateien geeignete Berechtigungen vergeben werden. Eine Verschlüsselung kann bei der Übertragung von Daten wie auch zur Absicherung von Beständen auf Speichermedien eingesetzt werden. Auch physische Maßnahmen, wie eine Zutrittssicherung oder die Verwendung von Tresoren können erforderlich sein, um die Vertraulichkeit von Daten zu erreichen. Die Abbildung 1.2 zeigt ein historisches Beispiel für eine Gefährdung der Vertraulichkeit.

1.2.2 Integrität

Ein weiteres Sicherheitsziel ist der Schutz der Integrität von Daten bei der Speicherung oder Übertragung. Dazu sollte verhindert werden, dass Daten unbefugt verändert werden oder zumindest muss erkannt werden, dass Veränderungen vorgenommen wurden. Beispiele für schützenswerte Bestände sind Finanztransaktionen, die Rezeptur für ein Medikament oder eine von einem Server heruntergeladene Software, die so wie vom Hersteller freigegeben installiert werden soll.

Abbildung 1.3: Verlust der Integrität von Daten



Grafikvorlage: Secunet AG, Foliensatz 2007

Um unberechtigte Veränderungen an Daten zu verhindern. sind unbefugte Benutzer vom Zugriff auszuschließen. Die Maßnahmen der Zugriffskontrolle und physische Sicherheitsmaßnahmen können den Zugang und damit die Möglichkeit zu Manipulationen erschweren. Mit einer anderen Gruppe von Maßnahmen können Veränderungen an Daten nachträglich erkannt werden. Dafür eignen sich mathematische Prüfsummen, wie Message Authentication Codes (MAC) oder digitale Signaturen. Auch eine nicht mehr entschlüsselbare Datei kann ein Indiz für eine Veränderung sein. In der Abbildung 1.3 könnte der Empfänger die Veränderung nur dann feststellen, wenn der Angreifer ungeschickt ist und die Nachricht deshalb sinnlos wird.

1.2.3 Verfügbarkeit

Geschäftsprozesse und andere Vorgänge sind für ihren reibungslosen Ablauf darauf angewiesen, dass Daten, Software und Hardware geeignet verfügbar sind. Zu den geforderten Zeiten soll für autorisierte Benutzer der Zugriff auf Programme und Daten möglich sein. Je »wertvoller« der Geschäftsprozess ist und je mehr Anwender auf eine IT-Unterstützung angewiesen sind, desto höher sind in der Regel die Verfügbarkeitsanforderungen.

Abbildung 1.4: Verlust der Verfügbarkeit

Grafikvorlage: Secunet AG, Foliensatz 2007

Der Ausschluss unbefugter Benutzer vom Zugriff kommt auch hier wieder zum Tragen, weil dadurch für Unbefugte die Angriffe gegen die Verfügbarkeit erschwert werden. Daneben kann durch das Vorhalten redundanter Komponenten die Verfügbarkeit erhöht werden. Zu den einfachsten Maßnahmen gehören Backups und Ersatzrechner. In Abhängigkeit vom Schutzbedarf können aber auch redundante Systeme, von RAID-Platten über Server-Cluster mit Lastverteilung bis hin zu Reserverechenzentren im Hot-Standby-Betrieb, eingesetzt werden. Reaktionsmöglichkeiten bei Denial-of-Service-Angriffen aus dem Internet können durch gezielte Maßnahmen des Monitorings, Filtermechanismen für Web-Anfragen und angepasste Lastverteilung verbessert werden. Wichtige Aspekte zur Verbesserung der Verfügbarkeit sind auch die Qualitätssicherung von Software sowohl hinsichtlich Fehlervermeidung als auch bezüglich Lasttests.

Eine Verfügbarkeit von 100 %, also 24 Stunden am Tag, 7 Tage die Woche und 365 Tage im Jahr ist praktisch kaum zu erreichen, da Wartungsfenster, Migrationserfordernisse und ungeplante Systemausfälle zumindest zu kurzzeitigen Ausfällen führen können. In der Praxis hat es sich daher bewährt, Verfügbarkeitskategorien zu definieren und Prozentwerte wie 99 % oder 99,9 % von den erforderlichen Betriebszeiten anzugeben.

1.2.4 Authentizität

Für das Sicherheitsziel Authentizität und der damit zusammenhängenden Nicht-Abstreitbarkeit von Daten müssen die Daten einem Absender eindeutig zugeordnet werden können. Der Absender kann eine Person oder auch ein System oder eine Anwendung sein. Das Sicherheitsziel ist erfüllt, wenn ein Dritter überprüfen kann, ob die Daten wirklich vom angenommenen Absender stammen. Auch für dieses Sicherheitsziel soll ein Beispiel skizzieren, wie die Authentizität verfälscht werden kann.

Je nach Anwendungskontext kann die Anforderung an den Nachweis unterschiedlich weit gehen. In einfachen Szenarien kann schon ein unternehmensinterner Nachweis ausreichen. Die Prüfmöglichkeit könnte dann beispielsweise für einen digitalen Workflow

erreicht werden, wenn durch ein mit engen Zugriffsrechten geschütztes Log-Protokoll nur der Vorgesetze oder der Datenschutzbeauftragte nachvollziehen kann, wer für die einzelnen Arbeits- und Genehmigungsschritte verantwortlich ist. Umfassende Szenarien fordern dagegen sogar die Möglichkeit zum Nachweis vor Gericht mit hohem Beweiswert. Eine Sicherheitsmaßnahme, die dieses Ziel unterstützt, ist die elektronische Signatur: Damit kann beispielsweise auch der Absender einer E-Mail eindeutig bestimmt werden.

Abbildung 1.5: Störung der Authentizität einer Nachricht

Grafikvorlage: Secunet AG, Foliensatz 2007

1.2.5 Sicherheitsziele und Sicherheitskonzept

Verschiedene Störungsursachen können sich auf die Sicherheitsziele auf unterschiedliche Weise auswirken. Beispielsweise kann die Verfälschung von Daten (Integrität) oder das Scheitern einer Signaturprüfung (Authentizität) eine Prozessstörung und damit eine Verfügbarkeitseinschränkung zur Folge haben. Auch können Sicherheitsmaßnahmen zugunsten mehrerer Sicherheitsziele wirken. Für die Maßnahmen der Zutritts- und Zugriffsbeschränkung, durch die Unbefugte ausgeschlossen werden sollen, wurde dies oben angedeutet. Auch können Zielkonflikte bei der Auswahl von Maßnahmen auftreten. So führt die Verschlüsselung von Daten in den meisten Fällen dazu, dass ein zusätzliches Störfall-Szenario für die Verfügbarkeit, nämlich der Schlüsselverlust, beherrscht werden muss. Schließlich müssen auch andere Anforderungsbereiche berücksichtigt werden. Die Vorgaben des Datenschutzrechts schränken beispielsweise die Möglichkeiten der Überwachung von Benutzern ein. Wenn Aspekte der Ergonomie nicht berücksichtigt werden, scheitern Sicherheitsmaßnahmen in der Praxis oft daran, dass die Benutzer sie nicht ausführen wollen oder nicht über die Zeit oder die Fähigkeiten verfügen, sie einsetzen zu können.

Für die Erarbeitung eines Sicherheitskonzepts ist es daher wichtig, nach den verschiedenen Sicherheitszielen zu unterscheiden. Denn es hängt von den jeweiligen Unternehmensanforderungen, der Ausgestaltung der Geschäftsprozesse und dem IT-Einsatz ab, wie der Schutzbedarf spezifischer Komponenten einzustufen ist. Je nachdem wie stark die Sicherung von Verfügbarkeit, Vertraulichkeit, Integrität oder Authentizität gefordert

ist, müssen im Sicherheitskonzept Maßnahmen unterschiedlich gewichtet und kombiniert werden. So könnte es für ein Unternehmen eher akzeptabel sein, die Produktion eines Medikaments auszusetzen, als eine Charge mit falscher Rezeptur zu vertreiben. Bei einer Farbproduktion ist dagegen Liefertreue möglicherweise das entscheidende Kriterium, während geringfügige Abweichungen im Farbton von den Kunden toleriert werden. Die Gewichtung der Sicherheitsziele ist daher zentral für das Sicherheitskonzept. Darüber hinaus können auch weitere Faktoren Einfluss auf die Gestaltung des Sicherheitskonzepts haben, damit es erfolgreich in der Praxis umgesetzt wird. So müssen die Maßnahmen derart ausgewählt werden, dass sie von den Verantwortlichen auch umgesetzt oder beachtet werden können, also beispielsweise die Zuständigkeiten und Ressourcenlage berücksichtigen. Ein weicherer Faktor ist die Unternehmenskultur, die beispielsweise stärker auf Kontrolle, auf klare Anweisungen oder die Motivation und Eigenverantwortung der Mitarbeiter ausgerichtet sein kann. Auch solche Kriterien sollten bei der Auswahl von Alternativen berücksichtigt werden.

In der folgenden Tabelle sind noch einmal zusammenfassend die vier Sicherheitsziele, ausgewählte Beispiele für IT-basierte Angriffe und Sicherheitsmaßnahmen aufgeführt.

Tabelle 1.1: Sicherheitsziele, Angriffsbeispiele und Beispiele für Sicherheitsmaßnahmen

Sicherheitsziel (englische Bezeichnung)	Angriffsbeispiel	Beispielsmaßnahmen
Vertraulichkeit (confidentiality)	Abhören des Übertragungsmediums	Verschlüsselung, Zugangskontrolle, Berechtigungskonzepte
Integrität (integrity)	Einspielen falscher Datenpakete	Verwendung von Prüfsummen, Definierte Installationsprozesse
Verfügbarkeit (availability)	Denial-of-Service-Angriffe	Einsatz von Filtermechanismen, Hohe Leistungsreserven Hardware, Redundante Auslegung
Authentizität (authenticity)	Fälschung der Datenherkunft (Person, E-Mail, IP-Adresse)	Digitale Signatur, Organisatorische Prozesse

Ein gutes Sicherheitskonzept stellt das Gewicht der Sicherheitsziele für die verschiedenen Unternehmens- und Technikbereiche dar und begründet unter Berücksichtigung von Zielkonflikten, Restrisiken und anderen Faktoren, eine ausgewogene Auswahl von Sicherheitsmaßnahmen. Die weiteren Kapitel dieses Buches vertiefen hierzu relevante Aspekte wie technische Lösungen und konzeptionelle Fragen, z. B. von rechtlichen Fragestellungen über Standards der Informationssicherheit bis hin zu Business Continuity.

Zusammenfassung

In diesem Kapitel wurde die Notwendigkeit eines kontrollierten und gesteuerten Umgangs mit dem Thema Informationssicherheit durch ein Informationssicherheits-Managementsystem sowie die wesentlichen Sicherheitsziele der Informationssicherheit dargestellt. Welche Maßnahmen und Methoden geeignet sind, die Sicherheitsziele und ein angemessenen Maß an Informationssicherheit zu erreichen, wird in den folgenden Kapiteln detailliert ausgeführt.

Literatur

[Gora07] *Gora, S.:* Security Audits, Secorvo White Paper, 2007; *http://www.secorvo.de/publikationen/secorvo-wp14.pdf* (Stand: 15.12.2009)

[BSI17] *Bundesamt für Sicherheit in der Informationstechnik (BSI):* BSI-Lagebericht IT-Sicherheit 2017 *https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html* (Stand: 15.06.2018)

[HEISE] *heise online:* Heise Newsticker; *http://www.heisec.de*

[MELAN] *Melde- und Analysestelle Informationssicherung MELANI der Schweiz:* Melani-Berichte; *http://www.melani.admin.ch/*