1 Einführung

Grundlegende Voraussetzung für die erfolgreiche Realisierung der Geschäftsprozesse eines Unternehmens ist die Unternehmenssicherheit. Die Unternehmenssicherheit bezieht sich auf mehrere Bereiche, wie z. B. Arbeits- Prozess- oder IT-Sicherheit. In der folgenden Kurseinheit (KE) werden die IT-Sicherheit und das damit verbundene IT-Sicherheitsmanagement (ITSM) behandelt. Das ITSM hat in der heutigen digitalen Welt eine ausschlaggebende Bedeutung für die Aufrechterhaltung der Geschäftstätigkeit von Unternehmen. Diese Bedeutung ergibt sich aus der steigenden digitalen Abwicklung und Steuerung von Geschäftsprozessen und der draus resultierten hohen Abhängigkeit von einer funktionierenden und leistungsfähigen Informatik. Störungen in der betrieblichen Informatik können Störungen in den Geschäftsprozessen verursachen, die hohe finanzielle oder auch Reputationsschäden bei den betroffenen Unternehmen verursachen können.

Die Gewährleistung der IT-Sicherheit im Unternehmen wird zunehmend zu einer großen Herausforderung für dessen Management. Durch die fortschreitende Digitalisierung und Internet-basierte Vernetzung von Unternehmen und Menschen werden die Informationstechnik (IT) und ihre Nutzer zu wichtigen Risikofaktoren bzw. Angriffsstellen. Studien aus den letzten Jahren zeigen, dass die Anzahl an sogenannten Angriffen auf die Informatik gestiegen ist (vgl. BSI 2015, S. 12; PwC 2014, S. 24). Um sich erfolgreich vor solchen Angriffen zu schützen, benötigen Unternehmen ein ITSM. Es hat zum Ziel, ein angemessenes Niveau an IT-Sicherheit herzustellen, laufend zu überprüfen und sicherzustellen (vgl. BSI 2008a, S. 14).

1.1 Einordnung der Kurseinheit in den Lehrbrief Informationsmanagement

Das ITSM beschäftigt sich vorrangig mit der Entwicklung, Anpassung und Umsetzung von Sicherheitskonzepten im Bereich der Informatik sowie mit der Steuerung und Kontrolle der Entwicklungs- und Umsetzungsprozesse. Unter dem Begriff der Informatik werden, wie bereits in den vorherigen KE erläutert, sowohl die IT-Systeme als auch die Informatik-Ablauf- und -Aufbauorganisation zusammengefasst. Die IT-Systeme umfassen dabei die Hardware (z. B. Server, Speicher, PC, Laptops, Drucker, Faxgeräte), die Software (z. B. Betriebssysteme, Applikationen, Middleware) sowie die Kommunikationsinfrastruktur (z. B. Kommunikationsverbindungen, Router, Switches). Im Kontext der IT-Sicherheit sind aber auch die Nutzer der Informatik von großer Bedeutung, da sie zu den wichtigsten Gefahren für die IT-Sicherheit gehören.

Das ITSM hat alle diese relevanten Komponenten systematisch zu erfassen, ihre Bedeutung für die Erreichung der Unternehmens- und Informatikziele zu ermitteln, sie auf Schwachstellen zu analysieren und schließlich mithilfe geeigneter Maßnahmen zu schützen. Dadurch soll das ITSM das Management der Informatik unterstützen und gewährleisten, dass das Informationsmanagement seine Aufgaben erfüllen und seine Ziele erreichen kann. Somit ist das ITSM als ein Unterbe-

reich des Managements der Informatik und folglich auch des Informationsmanagements zu verstehen (vgl. Abbildung 1).

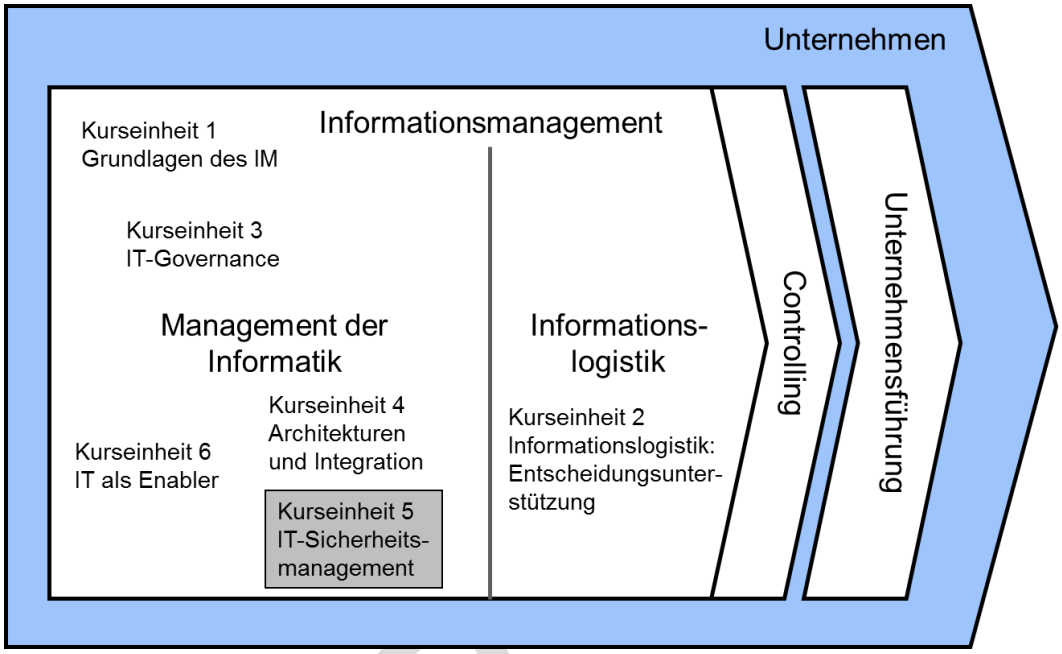

Abbildung 1: Einordnung der KE in den Lehrbrief Informationsmanagement

1.2 Inhalte und Lernziele der Kurseinheit

In der vorliegenden KE wird die Relevanz des ITSM für das Management der Informatik herausgestellt. Dazu werden zunächst wichtige Begriffe aus dem Themengebiet des ITSM eingeführt sowie die Ziele und Aufgaben des ITSM beschrieben. Aufbauend auf den Grundlagen wird im dritten Kapitel die Entwicklung und Steuerung einer IT-Sicherheitsstrategie diskutiert. Die IT-Sicherheitsstrategie wird in einem IT-Sicherheitskonzept konkretisiert. Kapitel 4 beschreibt, wie ein solches Konzept erarbeitet werden kann. Kapitel 5 beschäftigt sich zu Beginn mit dem Thema IT-Sicherheitsmaßnahmen und stellt Kategorien und Beispiele aus diesem Bereich vor. Als nächstes werden Gestaltungsoptionen für die IT-Sicherheitsorganisation sowie wichtige Rollen und Verantwortlichkeiten im ITSM aufgezeigt. Abschließend wird die Entwicklung und laufende Anpassung der IT-Sicherheitskultur als ein wichtiger Bestandteil eines erfolgreichen ITSM behandelt.

Die **Lernziele** dieser Kurseinheit lassen sich wie folgt zusammenfassen:

Kapitel 2: Grundlagen und Begriffe

Sie können die grundlegenden Begriffe aus dem Themengebiet des ITSM erklären. Sie verstehen, welche Zielsetzungen das ITSM in Unternehmen verfolgt und welche Aufgaben es zu erfüllen hat.

Kapitel 3: Entwicklung und Steuerung der IT-Sicherheitsstrategie

Sie kennen die Elemente der IT-Sicherheitsstrategie und können beschreiben, wozu das jeweilige Element dient. Weiterhin verstehen Sie die Ziele und Probleme der Steuerung der IT-Sicherheitsstrategie und kennen den Aufbau der IT

Security Balanced Scorecard.

Kapitel 4: Erarbeitung eines IT-Sicherheitskonzepts

Sie verstehen, was ein IT-Sicherheitskonzept ist und wissen, welche Ziele Unternehmen mit diesem verfolgen. Sie sind in der Lage, die Schritte zur Erarbeitung eines IT-Sicherheitskonzepts zu beschreiben sowie Beispiele für z. B. Schutzbedarfskategorien, Schadensszenarien und Bedrohungen für die IT-Sicherheit zu geben.

Kapitel 5: IT-Sicherheitsmaßnahmen, -organisation und -kultur

Sie kennen unterschiedliche Kategorien von IT-Sicherheitsmaßnahmen und sind in der Lage, Beispiele für IT-Sicherheitsmaßnahmen aus den jeweiligen Kategorien zu geben. Des Weiteren kennen Sie die drei Möglichkeiten für die organisationale Einbettung des ITSM im Unternehmen sowie einige wichtigen Rollen und Verantwortlichkeiten in diesem Bereich. Außerdem können Sie die Wichtigkeit einer IT-Sicherheitskultur begründen und die Phasen des Managementprozesses der IT-Sicherheitskultur beschreiben.

2 Grundlagen und Begriffe

Dieses Kapitel beschäftigt sich zuerst mit den grundlegenden Begriffen und Zielen im Bereich des ITSM. Anschließend werden die Aufgaben des ITSM vorgestellt.

2.1 Definitionen und Ziele im Rahmen des IT-Sicherheitsmanagements

Der Begriff Sicherheit hat unterschiedliche Facetten und wird kontextabhängig unterschiedlich definiert (vgl. Ritz 2015, S. 8; Krcmar 2015, S. 523 f.). Im organisationalen Kontext, in welchem ein Unternehmen als ein sozio-technisches System betrachtet wird, bezeichnet Sicherheit eine Systemeigenschaft (vgl. Ritz 2015, S. 5 ff.; Eckert 2013, S. 6) oder einen Systemzustand, bei welchem sämtliche schutzwürdigen Elemente des Systems vor Beeinträchtigungen geschützt sind (vgl. Heinrich und Stelzer 2011, S. 177 f.). Die IT-Sicherheit bezieht sich auf die IT eines Unternehmens und somit zunächst auf die Sicherheit der IT-Systeme. Da die IT-Systeme jedoch nicht isoliert existieren, sondern in einer zunehmend starken Interaktion mit den Stakeholdern des Unternehmens stehen, ist die Berücksichtigung der Nutzer im Rahmen der IT-Sicherheit unabdingbar (vgl. Eckert 2013, S. 3 f.).

In der Literatur werden, je nach Vertiefungsbereich, unterschiedliche Begriffe für die IT-Sicherheit verwendet. Diese Begriffe werden im Folgenden dargestellt und voneinander abgegrenzt.

- **Informationssicherheit** ist die Gewährleistung des notwendigen Zugangs zu den Informationen eines Unternehmens sowie des Schutzes dieser Informationen vor unautorisierter Offenlegung und Manipulation (vgl. ISACA 2015, S. 49). Der Begriff wird zunehmend als Synonym für IT-Sicherheit verwendet, hat aber einen breiten Geltungsbereich. Er bezieht sich auf alle Informationen eines Unternehmens und nicht nur auf diejenigen, die in IT-Systemen verarbeitet und gespeichert werden (vgl. Krcmar 2015, S. 524).

- Der Begriff **Datenschutz** wird in Deutschland durch die Gesetzgebung geprägt und betrifft den Schutz von Menschen. Er bezeichnet den rechtmäßigen Umgang (hierzu gehören die Erhebung, Verarbeitung und Nutzung (§1 Abs. 2 BDSG)) mit personenbezogenen Daten mit dem Ziel, den Einzelnen vor Beeinträchtigungen in seinem Persönlichkeitsrecht zu schützen (§ 1 Abs. 1 BDSG).

- Aus dem juristischen Datenschutz-Kontext ergibt sich die Bedeutung des Begriffs **Datensicherheit** i. e. S. Er beschreibt die Gewährung des Datenschutzes mittels geeigneter technischen und organisatorischen Maßnahmen (§ 9 BDSG). I. w. S. bezieht sich Datensicherheit auf Daten im Allgemeinen und bezeichnet den Schutz der Daten z. B. vor Verlust, Diebstahl und Fälschung durch geeignete Maßnahmen (vgl. Hansen et al. 2015, S. 372). Somit stellt die Datensicherheit die Grundlage für eine spätere Informati-

onssicherheit dar, da aus Daten – wie bereits in KE 1 erläutert wurde – Informationen generiert werden können.

Definition IT-Sicherheit

Aufbauend auf den vorgestellten Definitionen wird in dieser KE unter IT-Sicherheit der Zustand der Informatik, in welchem sämtliche schutzwürdigen Informatikelemente durch geeignete Maßnahmen vor Beeinträchtigungen geschützt sind, verstanden. Ziel dabei ist es, die Funktions- und Leistungsfähigkeit der Informatik sowie die Sicherheit der in den IT-Systemen befindlichen Daten bzw. Informationen sicherzustellen.

IT-Sicherheitsziele

Zur Konkretisierung der Ziele der IT-Sicherheit wird eine Reihe von Kriterien verwendet, welche Sicherheitsziele (vgl. Hansen et al. 2015, S. 373; Heinrich und Stelzer 2011, S. 179) oder auch Schutzziele (vgl. Eckert 2013, S. 7) genannt werden. Hierzu gehören vor Allem die Vertraulichkeit, Verfügbarkeit, Verbindlichkeit, Integrität, Authentizität und Anonymität. Im Folgenden werden diese Ziele zunächst erläutert und in Abschnitt 5.1 werden Maßnahmen zu ihrer Realisierung vorgestellt.

Das Sicherheitsziel der **Vertraulichkeit** bezieht sich auf Daten und Informationen. Sie stellt sicher, dass nur Berechtigte (diese können sowohl Menschen als auch Maschinen sein) auf schutzwürdige Daten oder Informationen zugreifen und diese lesen können (vgl. Krcmar 2015, S. 524; Hansen et al. 2015, S. 374). Die Vertraulichkeit ist vor allem im Rahmen der Gewährung des Datenschutzes und des Schutzes von Unternehmensgeheimnissen ein grundlegendes Ziel.

Das Sicherheitsziel der **Verfügbarkeit** bezieht sich sowohl auf Daten und Informationen, als auch auf Systeme und bezeichnet die Gewährleistung des uneingeschränkten Zugriffs auf und Nutzung von Daten oder Systemen durch Berechtigte (vgl. ISACA 2015, S. 10; Hansen et al. 2015, S. 377).

Unter der **Verbindlichkeit** oder auch **Nichtabstreitbarkeit** wird verstanden, dass ein Subjekt die Durchführung einer Aktion, wie z. B. das Absenden oder Erhalten einer Nachricht, nicht abstreiten kann (vgl. Hansen et al. 2015, S. 379).

Die **Integrität** bezieht sich auf Daten und Informationen und bezeichnet den Schutz dieser vor unautorisierter und unbemerkter Manipulation. Sie stellt die Echtheit und Verbindlichkeit von Daten und Informationen sicher (vgl. Eckert 2013, S. 9; ISACA 2015, S. 51).

Unter der **Authentizität** wird die Nachweisbarkeit der Echtheit oder der Identität von Objekten (z. B. Daten) oder Subjekten (z. B. Nutzer) anhand charakteristischer Eigenschaften verstanden (vgl. Eckert 2013, 12 f.; Hansen et al. 2015, S. 379). Sie ist eine Voraussetzung für die Gewährung des Zugangs von Berechtigten zu Systemen und somit auch für die Realisierung der Vertraulichkeit und Integrität (vgl. Eckert 2013, S. 465).

Die **Anonymität** ist ein Sicherheitsziel, dass im Datenschutz-Kontext besonders wichtig ist. Sie bezeichnet „das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder

nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können“ (§ 3 Abs. 6 BDSG).

Die vorgestellten Sicherheitsziele sind die Basis für die Bestimmung eines angemessenen Niveaus an IT-Sicherheit in Unternehmen. Je nach Branche, Unternehmensstrategie und Geschäftsprozess benötigen Unternehmen unterschiedliche Niveaus an IT-Sicherheit. Alle Unternehmen verarbeiten i. d. R. im Rahmen des Personalwesens personenbezogene Daten und müssen für diese Daten die Vertraulichkeit und die Integrität gewährleisten. Für Unternehmen aus dem Online-Handel ist die Sicherstellung der Verfügbarkeit ihrer Webseite eine Grundvoraussetzung für die Realisierung ihrer Geschäftsprozesse. Für einen lokalen Händler dagegen ist die Verfügbarkeit seiner Webseite, die er nur zur Darstellung seiner Angebote und Kontaktdaten nutzt, von nachrangiger Bedeutung. Die Verbindlichkeit ist insbesondere für Unternehmen relevant, die eine Großzahl ihrer Geschäfte elektronisch abwickeln (z. B. Online-Käufe, Online-Banking), da sie die Rechtsverbindlichkeit der durchgeführten Transaktionen gewährleistet (vgl. Eckert 2013, 12 f.; Hansen et al. 2015, S. 379). Die Anonymität ist bei der Realisierung von Online-Wahlen unbedingt zu gewährleisten (vgl. Heinrich und Stelzer 2011, S. 179).

Definition IT-Sicherheitsmanagement

Die Analyse relevanter Faktoren und Rahmenbedingungen sowie die Ermittlung der Bedeutung der verschiedenen IT-Sicherheitsziele für den Erfolg eines Unternehmens sind grundlegende Aufgaben des IT-Sicherheitsmanagements. Das IT-Sicherheitsmanagement hat dafür zu sorgen, dass ein angemessenes Niveau an IT-Sicherheit definiert, hergestellt und laufend überprüft und sichergestellt wird. Es vereint in sich zwei Bedeutungen:

Das ITSM bezeichnet zum einen die Gesamtheit aller Führungsaufgaben, die sich mit der IT-Sicherheit im Unternehmen befassen (vgl. Heinrich und Stelzer 2011, S. 173), und zum anderen die Organisationseinheit, die diese Aufgaben bearbeitet (vgl. Ritz 2015, S. 159). Für diese KE wird dem ITSM-Begriff die zuerst genannte Bedeutung zugrunde gelegt. Für die Organisationseinheit, die mit den ITSM-Aufgaben beauftragt ist, wird hier der Begriff IT-Sicherheitsorganisation verwendet.

Definition IT-Sicherheitsprogramm

Zur Erfüllung der Aufgaben des ITSM und Erreichung der IT-Sicherheitsziele werden geeignete Führungsstrukturen sowie eine Reihe von technischen, operativen und verfahrensorientierten Maßnahmen in einem Unternehmen geplant und implementiert. Die Gesamtheit all dieser Strukturen und Maßnahmen wird IT-Sicherheitsprogramm bezeichnet (vgl. ISACA 2015, S. 50).

2.2 Aufgaben des IT-Sicherheitsmanagements

Die Aufgaben des ITSM im Unternehmen sind vielfältig und betreffen mehrere Unternehmensebenen (vgl. Whitman und Mattord 2012, S. 174 ff.; BSI 2008a, S. 16 ff.) (vgl. Abbildung 2).

Strategische Ebene

Auf strategischer Ebene ist es Aufgabe des ITSM, eine unternehmensspezifische IT-Sicherheitsrichtlinie zu definieren sowie IT-Sicherheitsziele festzulegen. Darauf aufbauend ist ein grober Plan für die Erreichung der IT-Sicherheitsziele aufzustellen. Dadurch wird die IT-Sicherheitsstrategie formuliert. Die IT-Sicherheitsstrategie ist dann mithilfe geeigneter Instrumente zu steuern.

Taktische Ebene

Die IT-Sicherheitsstrategie wird in einem (oder auch mehreren) IT-Sicherheitskonzept(-en) konkretisiert. Die Erarbeitung eines IT-Sicherheitskonzepts ist der taktischen Ebene zuzuordnen und beinhaltet u. a. die Aufnahme der relevanten IT, die Analyse von Schutzbedarfen, Schwachstellen und Bedrohungen sowie die Festlegung von IT-Sicherheitsmaßnahmen.

Operative Ebene

Das IT-Sicherheitskonzept und der daraus resultierende Maßnahmenplan sind anschließend auf operativer Ebene zu realisieren. Hier werden technische IT-Sicherheitslösungen entwickelt bzw. angeschafft und implementiert, notwendige IT-Sicherheitsprozesse werden eingerichtet und laufend umgesetzt und Schulungs- und Sensibilisierungsprogramme für das Personal werden durchgeführt.

Das folgende Kapitel 3 wendet sich zunächst der Entwicklung und Steuerung der IT-Sicherheitsstrategie und bildet dadurch die Basis für die schließlich in Kapitel 4 und 5 erläuterten weiteren strategischen, taktischen und operativen Aufgaben des ITSM.

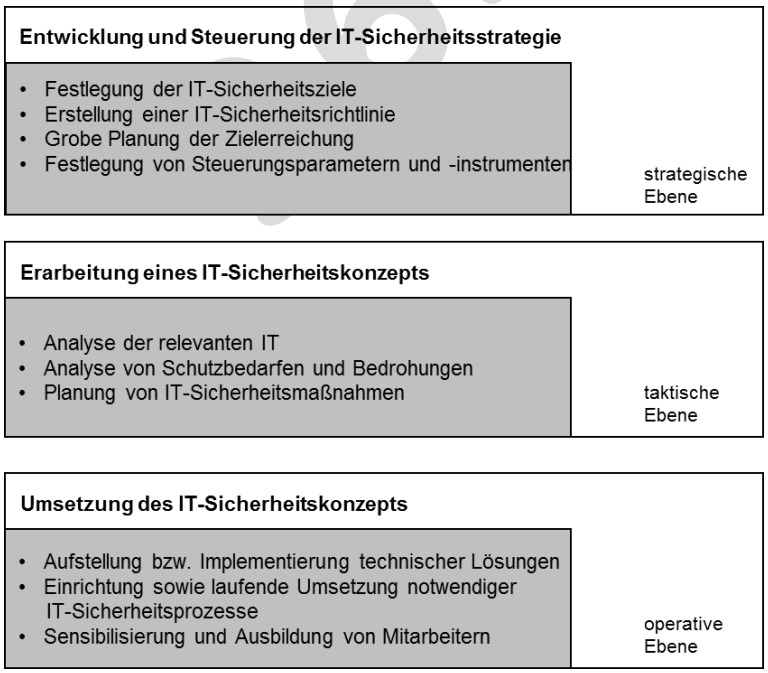

Abbildung 2: Aufgaben des IT-Sicherheitsmanagements
Quelle: In Anlehnung an BSI 2008a, 16 ff. und Eckert 2013, S. 195

3 Entwicklung und Steuerung der IT-Sicherheitsstrategie

Das vorliegende Kapitel beschäftigt sich mit zwei grundlegenden Aufgaben des strategischen ITSM. Im ersten Abschnitt wird die Entwicklung einer IT-Sicherheitsstrategie anhand ihrer Elemente vorgestellt und im zweiten Abschnitt wird die Steuerung der IT-Sicherheitsstrategie anhand eines konkreten Steuerungsinstruments – die IT Securiy Balanced Scorecard – verdeutlicht.

3.1 Die IT-Sicherheitsstrategie und ihre Elemente

Die erste wichtige Aufgabe im Rahmen des strategischen ITSM ist die Entwicklung der IT-Sicherheitsstrategie. Die IT-Sicherheitsstrategie dient der Schaffung „[...] eines umfassenden Rahmenwerks, das die Entwicklung, Institutionalisierung, Bewertung und Verbesserung des [IT-]Sicherheitsprogramms [eines Unternehmens] ermöglicht“ (Bowen et al. 2006, S. 6). Die Strategieentwicklung setzt eine Analyse und Auswertung des relevanten Umfelds voraus. Dieses Umfeld besteht sowohl aus externen als auch aus internen Faktoren. Zu den externen Faktoren gehören z. B. Geschäftspartner, Kunden, gesetzliche Regelungen, technische Entwicklungen. Geschäftspartner können bspw. den Aufbau eines Sicherheitsmanagementsystems nach dem Standard ISO/IEC 27001 verlangen. Der Gesetzgeber kann die Gewährleistung einer gewissen Verfügbarkeit und Vertraulichkeit von bestimmten Kategorien von Daten (z. B. personenbezogenen oder steuerrelevanten) fordern. Interne Faktoren sind u. a. die Geschäftsstrategie, die Unternehmenskultur sowie verfügbare finanzielle und personelle Ressourcen. Hierbei ist die Abstimmung der Geschäftsstrategie mit der IT-Sicherheitsstrategie eine der wichtigsten strategischen Aufgaben, um den Erfolg sowohl des IT-Sicherheitsmanagements als auch des Unternehmens insgesamt zu garantieren (vgl. Ma et al. 2009).

Elemente der IT-Sicherheitsstrategie

Aufgrund der unterschiedlichen Auffassungen des Strategiebegriffs[1] in der Literatur existiert für den IT-Sicherheitsstrategiebegriff[2] auch keine einheitliche Definition. Im Rahmen dieser KE wird dieser Begriff in Anlehnung an Beebe und Rao (2010) und Bowen et al. (2006, S. 7) als die Gesamtheit folgender Elemente verstanden:

- eine IT-Sicherheitsrichtlinie
- eindeutige IT-Sicherheitsziele, die den Unternehmenszielen entsprechen
- ein grober Plan, welcher beschreibt, wie die definierten Ziele zu erreichen sind
- Leistungsindikatoren bzw. Kennzahlen zur laufenden Steuerung und Kontrolle der Zielerreichung.

---

1 Für eine Auseinandersetzung mit dem Begriff Strategie vgl. KE 3, Abschnitt 3.1 des Lehrbriefs Informationsmanagement.

2 Eine umfassende Diskussion zum Begriff IT-Sicherheitsstrategie liefern Horne et al. 2015.

Mittelpunkt der Strategie sind die IT-Sicherheitsziele, welche unter Berücksichtigung der relevanten und bereits analysierten, externen und internen Faktoren unternehmensspezifisch zu definieren sind. Die Definition der Ziele basiert auf den in Abschnitt 2.1 erläuterten, grundlegenden IT-Sicherheitszielen und ihre Bedeutung für die Erreichung der übergeordneten Unternehmensziele. Wenn ein übergeordnetes Ziel eines Handelsunternehmens darin besteht, neue Kunden durch die Eröffnung eines Online-Shops zu gewinnen, wird die Gewährleistung einer ständigen (24/7/365) Verfügbarkeit des Online-Shops sowie aller weiteren Systeme, welche an den Shop angebunden sind, ein zentrales IT-Sicherheitsziel für das Unternehmen darstellen. Für die relevanten IT-Sicherheitsziele werden Soll-Werte festgelegt. Dabei handelt es sich i. d. R. um qualitative Werte, wie z. B. niedrig, mittel, hoch, sehr hoch (vgl. Bowen et al. 2006, S. 74 f.). Eine Ausnahme dabei ist die Verfügbarkeit, welche, wie das obere Beispiel zeigt, auch in quantitativen Größen ausgedrückt wird. Der Ausdruck 24/7/365 bedeutet, dass Daten oder Systeme 24 Stunden am Tag, 7 Tage die Woche, 365 Tage im Jahr verfügbar sein sollen.

IT-Sicherheitsrichtlinie

Der Begriff der IT-Sicherheitsrichtlinie ist ebenso umstritten wie der Begriff der IT-Sicherheitsstrategie. Er leitet sich aus dem englischen Begriff *IT security policy* ab und wird im deutschsprachigen Raum auch mit *IT-Sicherheitspolitik* (vgl. Eckert 2013, S. 34 f.) oder *IT-Sicherheitsleitlinie* (vgl. Heinrich und Stelzer 2011, S. 174) übersetzt. Nach der Definition von Heinrich und Stelzer (2011, S. 174) ist die IT-Sicherheitsrichtlinie das Dokument, das „[...] die wichtigsten Aussagen der Sicherheitsstrategie eines Unternehmens [beschreibt]“ und somit kein Bestandteil der Strategie selbst. Für diese KE wird eine andere Bedeutung gewählt: Die IT-Sicherheitsrichtlinie ist ein Dokument des Managements, das die Richtung und das Verhalten bezüglich der IT-Sicherheit für alle Stakeholder eines Unternehmens vorgibt und folgende Elemente festlegt (vgl. Aurigemma und Panko 2012; Alshaikh et al. 2015; Solms und Solms 2004; ISACA 2015, S. 71):

- die notwendigen Strukturen, Rollen, Verantwortlichkeiten und Prozeduren
- Prinzipien für den korrekten Umgang mit IT
- Konsequenzen bei inkorrektem Umgang mit IT
- sowie Mechanismen zur Steuerung und Kontrolle der Einhaltung der IT-Sicherheitsrichtlinie.

Die IT-Sicherheitsrichtlinie soll kurz sein und in einer eindeutigen, leicht verständlichen Sprache geschrieben werden, damit alle Stakeholder motiviert werden, sie zu lesen. Ihre Erstellung soll nach einem bestimmten Verfahren, welches ihre regelmäßige Überprüfung und Anpassung sicherstellt, erfolgen. Sie soll weiterhin durch geeignete Programmen, wie z. B. Workshops und Trainings, unternehmensweit vermittelt werden, um ein entsprechendes Bewusstsein für die Bedeutung der IT-Sicherheit für das Unternehmen zu schaffen (vgl. Alshaikh et al. 2015). Ein Beispiel für eine IT-Sicherheitsrichtlinie kann dem Anhang entnommen werden.

Die grobe strategische Planung für die Erreichung der IT-Sicherheitsziele führt zu einem Vorgehen für die Erarbeitung eines IT-Sicherheitskonzepts. Die Konzep-

terarbeitung erfolgt dann auf taktischer Ebene. Zur Unterstützung dieser Aufgabe existiert eine Reihe von nationalen und internationalen Standards und Empfehlungen, wie z. B. die internationale Norm ISO/IEC 27001 „Information security management“, das „Information Security Handbook“ des National Institute of Standards and Technology oder der „BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise“. Kapitel 4 setzt sich umfassend mit dieser Thematik auseinander.

Für die Definition geeigneter Kennzahlen zur Steuerung und Kontrolle der IT-Sicherheitsstrategie werden Instrumente benötigt, welche i. d. R. das Controlling liefert. Die Auswahl und Einsatz dieser Instrumente setzt eine Berücksichtigung der Besonderheiten der Steuerung der IT-Sicherheitsstrategie voraus. Der folgende Abschnitt beschreibt zunächst diese Besonderheiten und stellt anschließend ein mögliches Steuerungsinstrument vor.

3.2 Steuerung der IT-Sicherheitsstrategie

Ein weiterer, wichtiger Aufgabenbereich im Rahmen des strategischen ITSM ist die Steuerung der IT-Sicherheitsstrategie. Dieser Aufgabenbereich beschäftigt sich mit der Evaluierung von IT-Sicherheitsprozessen und -maßnahmen sowie ihren Ergebnissen. Ziel der Steuerung ist die Sicherstellung der Wirtschaftlichkeit von geplanten und implementierten Strukturen, Prozessen und Maßnahmen. Im Rahmen der Steuerung werden u. a. folgende Fragen angegangen (vgl. Herath et al. 2010):

- Welche Investitionen in die IT-Sicherheit sind sinnvoll bzw. gerechtfertigt?
- Sind die IT-Sicherheitsmaßnahmen erfolgreich, d. h. unterstützen sie die Unternehmensziele und -strategie?
- Arbeitet das ITSM effektiv und effizient?

Die Beantwortung dieser Fragen setzt die Entwicklung bzw. Ableitung von geeigneten Kennzahlen voraus, was i. d. R. schwierig ist, da sich der Nutzen eines erfolgreichen ITSM ähnlich wie der IT-Nutzen nur eingeschränkt in quantitativ-messbaren Parametern ausdrücken lässt. Aus diesem Grund werden in diesem Kontext Instrumente und Verfahren, welche auf einer Mischung aus traditionellen, quantitativen Metriken (z. B. Kosten für die Realisierung einer Maßnahme) und eher abstrakten, qualitativen Parametern (z. B. Kundenverlust aufgrund von Imageschäden infolge von Datenpannen) zurückgreifen, benötigt. Ein Beispiel für ein solches Instrument ist die Balanced Scorecard (BSC). Die Balanced Scorecard[3] ist ein Kennzahlensystem, welches von vielen Unternehmen für das Controlling insgesamt und für das IT-Controlling im spezifischen eingesetzt wird. Sie bietet ei-

[3] Die Idee und der Aufbau der klassischen Balanced Scorecard sowie ein Beispiel für eine angepasste IT Balanced Scorecard sind in KE 3 erläutert.

nen Rahmen, um verschiedene Kennzahlen, welche in einer Ursache-Wirkung-Relation mit strategischen Zielen stehen, abzuleiten (vgl. Herath et al. 2010; Huang et al. 2006). Die zuletzt genannten Autoren schlagen zwei Varianten einer BSC für das ITSM vor. Im Folgenden wird die IT Security BSC von Herath et al. (2010) vorgestellt.

ITSec BSC

Die IT security BSC (ITSec BSC) von Herath et al. (2010) besteht aus vier Perspektiven. In der Perspektive **Unternehmenswert** (business value) wird die Bedeutung der IT-Sicherheit für die Generierung von Mehrwert für das Unternehmen analysiert. Ein Mehrwert entsteht an erster Stelle durch die Eröffnung von neuen Möglichkeiten durch die IT, wie z. B. eine bequemere und schnellere Interaktion mit Lieferanten und Kunden, die Vereinfachung von Prozessen und Transaktionen oder die Erschließung neuer Vertriebskanäle. Diese Möglichkeiten können jedoch nur dann erfolgreich ausgeschöpft werden, wenn die Leistungsfähigkeit und die Funktionalität der IT sichergestellt sind. Außerdem kann durch die IT-Sicherheit Vertrauen bei den Stakeholdern geschaffen werden, was zu ihrer langfristigen Bindung an das Unternehmen beiträgt. Somit kann die IT-Sicherheit in der aktuellen, digitalen Zeit als ein Alleinstellungsmerkmal betrachtet werden, das den Unternehmenserfolg mitbestimmt. Wichtig ist aber, dass das ITSM wirtschaftlich ist, so dass hier die zentralen Fragestellungen sind:

- Wie wirtschaftlich sind die IT-Sicherheitsmaßnahmen?
- Ist der Nutzen von IT-Sicherheitsprozessen und -strukturen größer als die investierten finanziellen Mittel?

Die Perspektive **Stakeholder-Orientierung** befasst sich mit den unterschiedlichen Stakeholder-Gruppen, welche das ITSM berücksichtigen muss. Aus Kundenperspektive ist es z. B. wichtig, dass die organisationalen Prozesse und die angebotenen Dienste ausreichend abgesichert sind. Aus Mitarbeiterperspektive ist es wichtig, dass Rahmenbedingungen geschaffen werden, welche sie in die Lage versetzen, sicher Handeln zu können. Hierzu zählen z. B. die Bereitstellung von Ressourcen (Zeit und finanzielle Mittel), um sich mit der Thematik auseinander setzen zu können und die Implementierung von Kontrollmechanismen (z. B. Authentifizierung und Autorisierung). Die zentrale Fragestellung dieser Perspektive ist:

- Erfüllen wir die Anforderungen von Nutzern und Kunden?

Die internen Prozesse der IT beinhalten die Planung, Beschaffung, Einsatz, Betrieb und Wartung von IT-Produkten und Diensten, die Bearbeitung von Nutzeranfragen sowie die Nutzerschulung. Aus diesen Prozessen lassen sich drei Hauptkategorien ableiten, an denen sich die internen IT-Sicherheitsprozesse der Perspektive **Interne Prozesse** bewerten lassen. Diese sind: 1) Planung und Priorisierung von IT-Sicherheitsvorhaben; 2) Einsatz von IT-Sicherheitsprodukten und -diensten; 3) Betrieb und Wartung eingesetzter IT-Sicherheitsprodukte und -dienste. Die zentralen Fragestellungen hier sind:

- Wie verwundbar sind unsere Systeme?
- Sind die IT-Sicherheitsmaßnahmen adäquat geplant und umgesetzt, um Schwachstellen und Risiken entgegenzuwirken?

In der Perspektive **Zukunftsbereitschaft** wird zum einen die laufende Ausbildung von Nutzern und IT-Sicherheitspersonal, bezüglich diverser Bedrohungsarten und Möglichkeiten diesen entgegenzuwirken bzw. sich vor diesen zu schützen, behandelt. Zum anderen werden hier Ziele und Maßnahmen definiert, um die proaktive Analyse und Entwicklung von Gegenmaßnahmen für vorstellbare Bedrohungen „der nächsten Generation“ zu fördern. Die Leitfragen dieser Perspektive sind somit:

- Welche neuen IT-Sicherheitsmaßnahmen und -herausforderungen bzw. -bedrohungen entstehen?
- Können wir proaktive Maßnahmen entwickeln?

Für jede der vier Perspektiven setzt das ITSM konkrete Ziele fest. Die Ziele werden in geeignete Kennzahlen mit Soll-Werten übersetzt. Der Erfolg des ITSM wird regelmäßig anhand der Gegenüberstellung von erreichten (Ist-) und gewünschten (Soll-)Werten bestimmt. Werden Abweichungen von den Soll-Werten festgestellt, so können Vorkehrungen getroffen werden, um die Zielerreichung zu gewährleisten. Abbildung 3 veranschaulicht die Perspektiven und die entsprechenden Leitfragen der ITSec BSC und Tabelle 1 liefert mögliche Kennzahlen für die einzelnen Perspektiven.

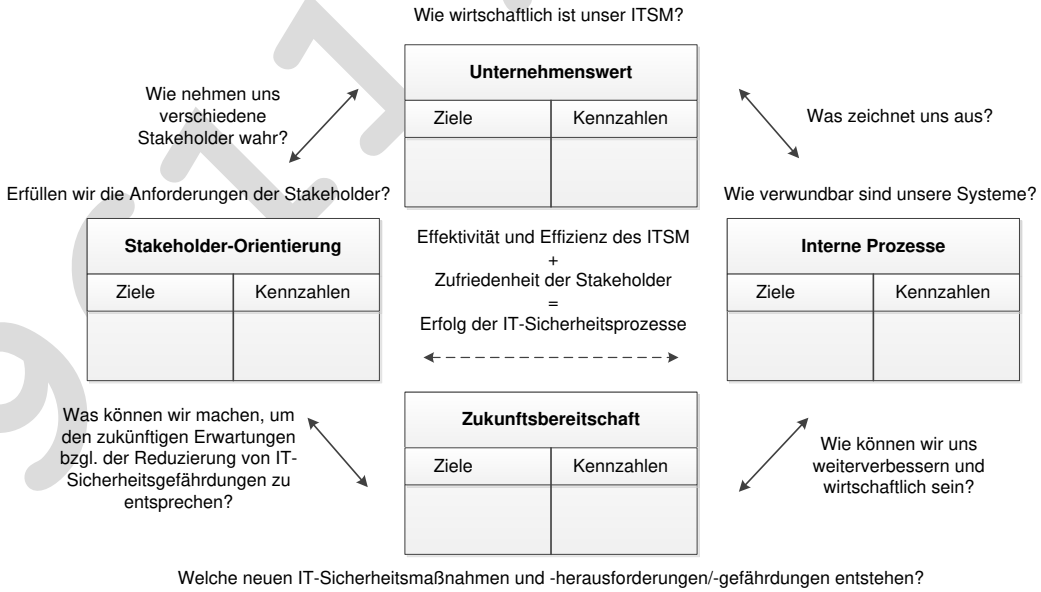

Abbildung 3: ITSec BSC
Quelle: Entnommen aus Herath et al. 2010, S. 77

Perspektive	Mögliche Kennzahlen
Unternehmenswert	• Prozentualer Anteil des Budgets für IT-Sicherheit am gesamten IT-Budget • Anzahl von schweren Vorfällen • Anzahl verlorener Kunden infolge von schweren Vorfällen • Summe der ausgefallenen Stunden kritischer Systeme • Finanzieller Schaden infolge von Ausfällen
Stakeholder-Orientierung	• Prozentsatz des IT-Budgets zur Sicherung der Kommunikation mit Kunden/Geschäftspartnern • Prozentsatz des IT-Budgets für die Bereitstellung einer sicheren externen Arbeitsumgebung (Home-Office) • Prozentsatz des IT-Budgets zur Sicherung von mobilen Geräten • Anzahl ungesicherter mobiler Geräte • Anzahl bearbeiteter, IT-sicherheitsrelevanter Anfragen (in einem vorgegebenen Zeitraum) • Prozentsatz des IT-Budgets für einen Datenschutzbeauftragten
Interne Prozesse	• Prozentsatz der für die internen IT-Sicherheitsprozesse bereitgestellten Ressourcen • Anzahl der bereitgestellten Produkte und Dienste • Anzahl identifizierter Bedrohungen • Anzahl Bedrohungen, welche in einem vorgegeben Zeitraum entgegengewirkt wurde • Prozentsatz der Systeme/Dienste, für welche ein bestimmtes Niveau an IT-Sicherheit vertraglich durch den Hersteller/Zulieferer zugesichert ist
Zukunftsbereitschaft	• Prozentsatz des IT-Budgets, bereitgestellt für laufende Ausbildung von Nutzern/IT-Sicherheitspersonal • Prozentsatz des IT-Sicherheitspersonals, welches eine Sicherheitsausbildung abgeschlossen hat • Prozentsatz des IT-Budgets, bereitgestellt für Tests (z. B. Penetrationstests) und Simulationen • Anzahl Vorfälle, ausgelöst durch Mitarbeiterfehler • Anzahl früh Identifizierter Softwarefehler, welche zukünftig ausgenutzt werden könnten

Tabelle 1: Mögliche Kennzahlen für die Perspektiven der ITSec BSC
Quelle: In Anlehnung an Chew et al. 2008, S. 15-18, A-2-A-24 und Herath et al. 2010

4 Erarbeitung eines IT-Sicherheitskonzepts

Definition IT-Sicherheitskonzept

Bestandteil der Entwicklung einer IT-Sicherheitsstrategie ist die Erstellung eines groben Plans, welcher beschreibt, wie die festgelegten IT-Sicherheitsziele erreicht werden sollen. Dieser Plan stellt ein Vorgehen dar, welches der Erarbeitung von IT-Sicherheitskonzepten dient. Ein IT-Sicherheitskonzept definiert die Hilfsmittel und Instrumente, welche die IT-Sicherheitszielerreichung unterstützen sollen und liefert begründete IT-Sicherheitsmaßnahmen (vgl. Heinrich und Stelzer 2011, S. 181). Wie bereits erwähnt, finden sich in der Literatur und Praxis unterschiedliche Empfehlungen und Standards für die Erstellung von IT-Sicherheitskonzepten. In diesem Kapitel wird ein Vorgehen in Anlehnung an die **IT-Grundschutz-Vorgehensweise** des Bundesamts für Sicherheit in der Informationstechnik (**BSI-Standard 100-2**) vorgestellt, da diese Vorgehensweise in Deutschland weit verbreitet und mit dem internationalen Standard ISO/IEC 27001 kompatibel ist.

Mit seinem Standard 100-2 bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Vorgehensweise für die Her- und Sicherstellung eines angemessenen IT-Sicherheitsniveaus an, welche effektiv und anwendungsbezogen ist. Ein wesentliches Ziel des Standards ist es, durch die Bereitstellung von modular aufgebauten Bausteinen und konkreten Umsetzungsvorschlägen, eine Methode zur Verfügung zu stellen, welche sich einfach an die spezifischen Gegebenheiten eines Unternehmens anpassen lässt. Somit soll der Aufwand für die Erstellung und Umsetzung von IT-Sicherheitskonzepten reduziert werden (vgl. BSI 2008a, S. 6, 36).

Die IT-Grundschutz-Vorgehenswese des BSI besteht insgesamt aus acht Schritten. Das in diesem Kapitel beschriebene und an die angesprochene Vorgehensweise angelehnte Vorgehen hat insgesamt fünf Schritte (vgl. Abbildung 4). Die Schritte Definition des Geltungsbereichs, Strukturanalyse, Schutzbedarfsanalyse und Maßnahmenplanung sind geeignet und ausreichend, um ein normales Niveau an IT-Sicherheit herstellen zu können. Der restliche Schritt kann als „ergänzend“ bezeichnet werden. Er wird für Objekte mit erhöhtem Schutzbedarf oder für solche, für welche keine passenden Bausteine bzw. IT-Sicherheitsmaßnahmen in den IT-Grundschutzkatalogen existieren, empfohlen (vgl. BSI 2008a, S. 70). Im Folgenden werden alle fünf Schritte detailliert erläutert.

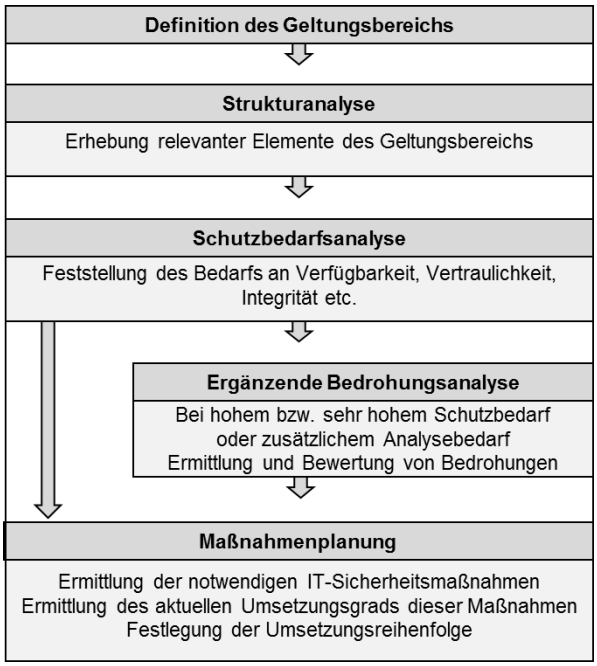

Abbildung 4: Vorgehensweise für die Erarbeitung eines IT-Sicherheitskonzepts
Quelle: In Anlehnung an vgl. BSI 2008a, S. 26 ff. und BSI 2011, S. 22 ff.

4.1 Definition des Geltungsbereichs

Die Erstellung und Umsetzung eines umfassenden IT-Sicherheitskonzepts für ein gesamtes Unternehmen ist eine anspruchsvolle Aufgabe, welche mit sehr hohem Aufwand verbunden ist. Aus diesem Grund empfiehlt das BSI, insbesondere wenn das Unternehmen bislang nur punktuell und unsystematisch IT-Sicherheitsmaßnahmen umgesetzt hat, zunächst ein Konzept für einen bestimmten Bereich des Unternehmens zu erstellen und zu implementieren. Anschließend soll das Konzept schrittweise auf die weiteren Unternehmemsbereiche übertragen werden. Der erste Schritt der vorgeschlagenen Vorgehensweise dient somit der Festlegung und klaren Abgrenzung des Bereichs, für welchen ein IT-Sicherheitskonzept zu erstellen und umzusetzen ist. Bei der Definition des Geltungsbereichs sollen technische und organisatorische Aspekte berücksichtigt werden. Hierzu gehören die Fachaufgaben und Geschäftsprozesse, für welche ein bestimmter Bereich (bzw. Abteilung) zuständig ist sowie die technischen Systeme, die diese Aufgaben und Prozesse unterstützen. Wird ein Teil der Fachaufgaben oder Geschäftsprozesse extern abgewickelt, so ist die Schnittstelle zum externen Bereich zu beschreiben. Der definierte Geltungsbereich wird vom BSI „Informationsverbund“ genannt. Er umfasst alle infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die der Informationsverarbeitung in dem betrachteten Bereich dienen (vgl. BSI 2008a, S. 37; 2011, S. 27). Beispiele für sinnvolle Bereiche für ein IT-Sicherheitskonzept sind die Produktion, die Forschungs- und Entwicklungsabteilung, der Vertrieb (insbesondere, wenn das Unternehmen im elektronischen Handel tätig ist).

4.2 Strukturanalyse

Die Strukturanalyse (vgl. BSI 2008a, S. 39 f.) dient im zweiten Schritt der Erfassung relevanter Elemente des Informationsverbunds sowie der Beziehungen zwischen ihnen. Um die Komplexität dieser und auch der nachfolgenden Schritte zu reduzieren sollen ähnliche Elemente zu Gruppen zusammengefasst werden. Ähnliche Elemente sind solche, die z. B. vom gleichen Typ sind (z. B. Datenbank (DB)-Server), ähnlich konfiguriert sind, gleiche Aufgaben oder Geschäftsprozesse unterstützen (z. B. Computer für die Personalverwaltung oder das Rechnungswesen). Die so gruppierten Elemente weisen i. d. R. den gleichen Sicherheitszustand und folglich auch den gleichen Schutzbedarf auf. Die Gruppe wird anschließend als ein Element behandelt. Die Strukturanalyse wird in folgende vier Teilschritte unterteilt:

1) **Erhebung von Informationen und Anwendungen**
   Zunächst werden die wichtigsten Informationen und Anwendungen des Informationsverbunds erfasst. Ausgangspunkte der Erhebungen sind die Fachaufgaben und die Geschäftsprozesse, welche den Informationsverbund ausmachen. Anhand dieser wird ermittelt, welche Informationen für die reibungslose Erfüllung der Fachaufgaben und Realisierung der Geschäftsprozesse benötigt werden und welche Anwendungen[4] die Aufgabenerfüllung und Prozessrealisierung unterstützen. Darüber hinaus wird die Wichtigkeit von Informationen anhand ihres Geheimhaltungsgrads und ihres besonderen Schutzes durch gesetzliche Vorschriften (z. B. das Bundesdatenschutzgesetzbuch (BDSG) für personenbezogene Daten oder die Abgabeordnung (AO) für steuerrelevante Daten) bestimmt (vgl. BSI 2011, S. 29). Für die strukturierte und übersichtliche Dokumentation dieser Informationen können Tabellen verwendet werden. Die Tabellen sollen mindestens die Bezeichnung der Anwendungen, die Art der mit den Anwendungen zu bearbeiteten Informationen, die durch die Anwendungen unterstützten Geschäftsprozesse, die Benutzer der Anwendungen sowie ihre Verantwortlichen beinhalten (vgl. Tabelle 2).

4 Das BSI verwendet eine von diesem Lehrbrief (vgl. KE 1 und 4) abweichende Definition für den Begriff Anwendung (vgl. BSI 2008a, S. 40), welche jedoch hier nicht zugrunde gelegt wird. Hier wird der Begriff Anwendung als Synonym von Applikation verwendet.

Nr.	Anwendung	Art der Informationen*	Verantwortlich	Benutzer	Geschäftsprozesse
A1	Personaldatenverarbeitung	p	Z1	Z1	GP0-1, GP0-2
A2	Beihilfeabwicklung	p	Z2	alle	GP0-2
A3	Reisekostenabrechnung	p, v, s	Z2	alle	GP0-1, GP0-3
A4	Benutzerauthentisierung	p, s	IT1	alle	GP0, GP5, GP6
A5	Systemmanagement	s	IT3	IT3	Alle
A6	Bürokommunikation	p, v, f, s	IT3	alle	Alle

*) p - personenbezogene Daten
v - verwaltungsspezifische Informationen, bspw. Organisationsstrukturen und Dienstanweisungen
f - fachliche Informationen, bspw. Korrespondenz mit den Kunden
s - systemspezifische/technische Informationen, bspw. Konfigurationsdateien von IT-Systemen

Tabelle 2: Dokumentation der Erhebung von Informationen und Anwendungen
Quelle: Entnommen aus BSI 2008a, S. 42

2) **Netzplanerhebung**

In diesem zweiten Schritt ist ein Netzplan für den betrachteten Informationsverbund zu erheben. Ist der Informationsverbund zu komplex und seine grafische Darstellung in einem Netzplan unübersichtlich, dann ist der Netzplan in mehrere Teilnetzpläne zu zerlegen. Ein Netzplan stellt alle informations- und kommunikationstechnischen Komponenten eines Bereichs und ihre Vernetzung graphisch dar. Netzpläne sind in einem Unternehmen i. d. R. vorhanden. Sie sollen elektronisch erstellt und regelmäßig aktualisiert werden. Die Netzplanerhebung kann mit Hilfe von Softwarewerkzeugen automatisiert werden. Allerdings arbeiten diese Werkzeuge nicht immer einwandfrei, sodass automatisch erstellte Netzpläne auf Korrektheit und Vollständigkeit überprüft werden sollen. Für die Zwecke der Strukturanalyse soll ein Netzplan mindestens folgende Elemente beinhalten:

- Geräte – z. B. Laptops, Arbeitsplatzcomputer, Server, Speicher, Drucker, Faxgeräte, Telekommunikationsanlagen
- Netzwerkkomponenten – z. B. Switches, Router, WLAN Access Points
- Verbindungen zwischen den Geräten
- Verbindungen des Informationsverbunds nach außen.

Ein Beispiel für einen Netzplan im Rahmen der Strukturanalyse liefert Abbildung 5.

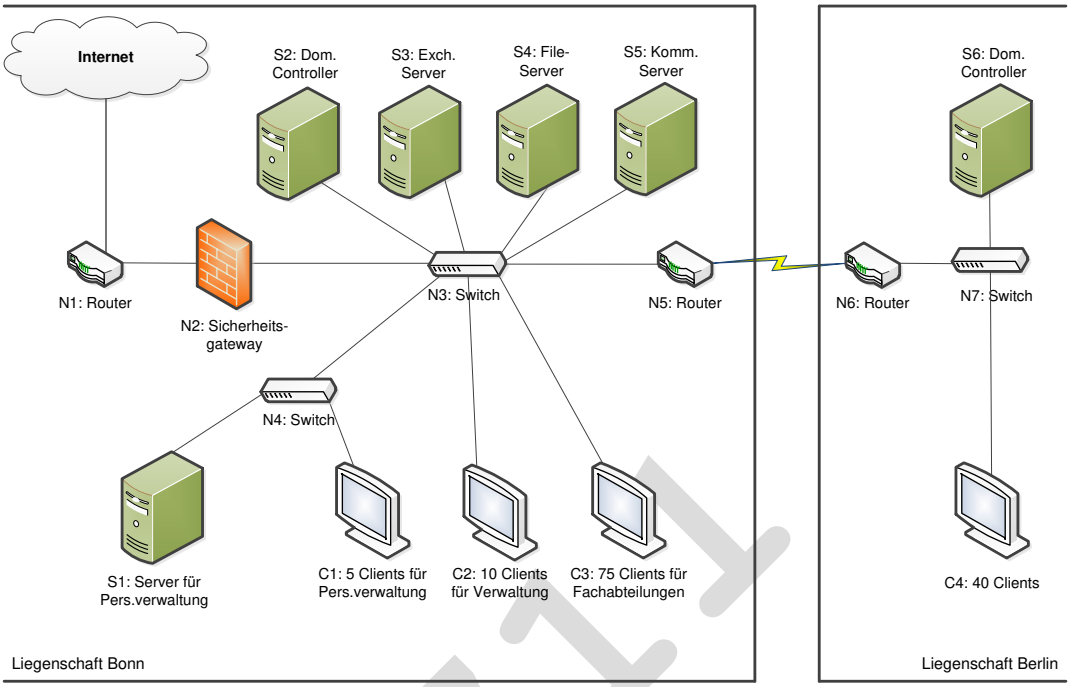

Abbildung 5: Beispiel eines Netzplans
Quelle: Entnommen aus BSI 2008a, S. 45

3) **Erhebung der Hardwaresysteme**[5]
In diesem Schritt werden alle vorhandenen und geplanten Geräte und Netzwerkkomponenten in tabellarischer Form aufgelistet. Dabei sollen sowohl vernetzte als auch nicht vernetzte Elemente erfasst werden. Die Erfassung soll folgende Informationen beinhalten:

- eindeutige Bezeichnung des Systems bzw. der Komponente
- Beschreibung inkl. Typ und Funktion
- Plattform
- Status
- Benutzer bzw. Administrator
- Aufstellungsort
- bei Gruppen: Anzahl der zusammengefassten Elemente.

Anschließend erfolgt eine Zuordnung der Systeme zu den im ersten Schritt erfassten Anwendungen. Dabei wird vermerkt, welche Anwendungen auf welchen Geräten installiert sind bzw. welche Komponenten für die Ausführung der Anwendungsfunktionen benötigt werden. Folgende zwei Tabellen stellen die Ergebnisse dieses Schrittes in Verbindung mit Abbildung 5 und Tabelle 2 beispielhaft dar.

5 Das BSI benutzt hierfür den Begriff „IT-Systeme“ (vgl. BSI 2008a, S. 45). Da aber in unserem Verständnis zu einem IT-System auch die Applikationen gehört, welche bereits im vorherigen Schritt erhoben wurden, wird hier zur besseren Abgrenzung der Begriff Hardwaresysteme verwendet.

Nr.	Beschreibung	Plattform	Anzahl	Aufstellungsort	Status	Benutzer
S1	Server für Personalverwaltung	Windows Server 2003	1	Bonn, R 1.01	in Betrieb	Personalreferat
S2	Domänen-Controller	Windows Server 2003	1	Bonn, R 3.10	in Betrieb	alle IT-Anwender
C1	Clients der Personal-datenverarbeitung	Windows Vista	5	Bonn, R 1.02 – R 1.06	in Betrieb	Personalreferat
C2	Clients in der Verwaltungsabteilung	Windows Vista	10	Bonn, R 1.07 – R 1.16	in Betrieb	Verwaltungs-abteilung
N1	Router zum Internetzugang	Router	1	Bonn, R 3.09	in Betrieb	alle IT-Anwender
N2	Firewall	Application Gateway auf Unix	1	Bonn, R 3.09	in Betrieb	alle IT-Anwender
N3	Switch	Switch	1	Bonn, R 3.09	in Betrieb	alle IT-Anwender
S - Server, C - Client, N - Netzkomponente						

Tabelle 3: Ergebnis der Erhebung von Hardwaresystemen
Quelle: Entnommen aus BSI 2008a, S. 46 f.

Nr.	Anwendung	Hardwaresysteme			
		S1	S2	S3	S6
A1	Personaldatenverarbeitung	X			
A2	Beihilfeabwicklung	X			
A3	Reisekostenabrechnung	X			
A4	Benutzerauthentisierung		X		X
A5	Systemmanagement		X		
A6	Bürokommunikation			X	

Tabelle 4: Zuordnung von Anwendungen zu Hardwaresystemen
Quelle: Entnommen aus BSI 2008a, S. 47

4) **Erfassung der Räume**

In dem letzten Schritt der Strukturanalyse werden alle Räume und Gebäude, in welchen die betrachteten Fachaufgaben und Geschäftsprozesse erledigt werden, erfasst. Dazu zählen ebenfalls private Liegenschaften, wenn Mitarbeiter die Möglichkeit haben, von zuhause aus zu arbeiten, sowie die Räumlichkeiten von Partnern, wenn diese für einen Teil der Geschäftsprozesse zuständig sind. Dabei sollen auch die Wegstrecken zwischen den Räumen und Gebäuden, die über Kommunikationsverbindungen laufen, aufgenommen werden. Darüber hinaus sind auch Räume, in welchen wichtige Informationen (z. B. auf Datenträgern oder auch in physischen Aktenordnern) aufbewahrt werden, zu erfassen. Für die Erfassung der Räume bietet sich ebenfalls die Verwendung von Tabellen an (vgl. Tabelle 5).

Raum			Hardwaresysteme/Datenträger
Bezeichnung	Art	Gebäude	
R U.02	Datenträgerarchiv	Bonn	Backup-Datenträger (Wochensicherung der Server S1 bis S5)
R B.02	Technikraum	Bonn	Telekommunikationsanlage
R 1.01	Serverraum	Bonn	S1, N4
R 1.02 - R 1.06	Büroräume	Bonn	C1
R E.03	Serverraum	Berlin	S6, N6, N7

Tabelle 5: Erfassung von Räumen
Quelle: Entnommen aus BSI 2008a, S. 48

Die Strukturanalyse liefert durch ihre Ergebnisse – den Netzplan (bzw. die Netzpläne) und die Tabellen – detaillierte und übersichtliche Informationen über die relevanten und wichtigsten Elemente des betrachteten Informationsverbunds. Auf Basis dieser Ergebnisse kann im nächsten Schritt ermittelt werden, welchen Schutzbedarf die einzelnen Elemente ausweisen.

4.3 Schutzbedarfsanalyse

Die Schutzbedarfsanalyse (vgl. BSI 2008a, S. 49 ff., 2011, S. 42 ff.), durch das BSI Schutzbedarfsfeststellung genannt, dient dazu, den Schutzbedarf für den Informationsverbund und seine Elemente zu ermitteln. Die begründete und nachvollziehbare Schutzbedarfsermittlung hat zum Ziel, darauf aufbauend, angemessene Sicherheitsmaßnahmen für die einzelnen Elemente des Informationsverbunds definieren zu können. Die Schutzbedarfsanalyse kann in folgende Teilschritte unterteil werden:

1) **Definition von Schutzbedarfskategorien**
   In einem ersten Schritt sollen Unternehmen eine für ihren Zweck und Kontext passende Anzahl an Schutzbedarfskategorien definieren. Das BSI schlägt folgende drei Schutzbedarfskategorien vor:
   - „**normal**: Die Schadensauswirkungen sind begrenzt und überschaubar.
   - **hoch**: Die Schadensauswirkungen können beträchtlich sein.
   - **sehr hoch**: Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen“ (BSI 2008a, S. 49).

2) **Definition von Schadensszenarien**
   Im zweiten Schritt sollen Unternehmen mögliche Szenarien, bei deren Eintreten Schäden für sie entstehen können, definieren. Dies kann mithilfe von „Was wäre wenn ...?“-Fragen erfolgen. Z. B. „Was wäre wenn Forschungs- und Entwicklungs- (FuE-)daten von uns an die Konkurrenz gelangen würden?“ Um die eindeutige Zuordnung der definierten Schadensszenarien zu entsprechenden Schutzbedarfskategorien zu ermöglichen, ist es darüber hinaus notwendig, Abgrenzungsbedingungen festzulegen. Die Abgrenzungsbedingungen sollen die Spezifika des Unternehmens berücksichtigen. So kann ein finanzieller Schaden in Höhe von 100.000 € für ein

Großunternehmen keine schwerwiegenden Folgen haben, während er für ein Kleinunternehmen sogar existenzbedrohend sein kann. Außerdem soll dieser Schritt in enger Zusammenarbeit mit den jeweiligen Fachabteilungen und IT-Nutzern erfolgen, da sie i. d. R. gut abschätzen können, welchen Einfluss unterschiedliche Systembeeinträchtigungen auf ihre Arbeit und auch auf das Unternehmen haben könnten. Die folgende Tabelle 6 stellt beispielhaft mögliche Schadensszenarien und ihre Zuordnung zu Schutzbedarfskategorien dar.

Schutzbedarfskategorien	Schadensszenarien
normal	Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen. Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen. Tolerable Beeinträchtigung der Aufgabenerfüllung, da die maximal tolerierbare Ausfallzeit größer als 24 Stunden ist. Finanzieller Schaden bis maximal 1 % vom Unternehmensumsatz.
hoch	Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen. Vertragsverletzungen mit hohen Konventionalstrafen. Negative Innen- oder Außenwirkung: Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten. Finanzieller Schaden zwischen 1 % und 10 % vom Unternehmensumsatz.
sehr hoch	Intolerable Beeinträchtigung der Aufgabenerfüllung (z. B. Ausfall des Produktionssystems), da die maximal tolerierbare Ausfallzeit kleiner als eine Stunde ist. Unerlaubte Weitergabe von FuE-Daten an die Konkurrenz, die zu existenzbedrohendem Schaden für die Institution führt. Finanzieller Schaden über 10 % vom Unternehmensumsatz.

Tabelle 6: Schutzbedarfskategorien und Schadensszenarien
Quelle: In Anlehnung an BSI 2008a, S. 50 f.

3) **Ermittlung der Schutzbedarfe**

Im letzten Schritt der Schutzbedarfsanalyse sollen die Schutzbedarfe der in der Strukturanalyse erfassten Elemente des Informationsverbunds mithilfe der definierten Schadensszenarien ermittelt werden. Der Schutzbedarf eines Elements wird auf der Basis des maximal möglichen Schadens bestimmt, welchen das Unternehmen erleiden kann, wenn bei diesem Element ein bzw. mehrere der in Abschnitt 2.1 erläuterten Sicherheitsziele (Vertraulichkeit, Verfügbarkeit, Verbindlichkeit, Integrität, Authentizität oder Anonymität) nicht eingehalten werden kann bzw. können.

Die Ermittlung der Schutzbedarfe aller Elemente soll systematisch erfolgen. Ausgangspunkt für die Ermittlung der Schutzbedarfe sind, wie bei der Strukturanalyse, die relevanten Fachaufgaben und die Geschäftsprozesse. Zunächst soll ermittelt werden, wie wichtig die jeweiligen Fachaufgaben und Geschäftsprozesse für das Unternehmen sind. Daraus ableitend soll der Stellenwert der Daten und Informationen, welche für diese Fachaufgaben und Geschäftsprozesse benötigt werden, bestimmt werden. In Abhängigkeit von ihrem Stellenwert können die unterschiedlichen Informationen den definierten Schutzbedarfskategorien zugeordnet werden. Die Schutzbedarfe der Informationen werden zum einen auf die Applikationen, welche sie verarbeiten, und zum anderen direkt auf Räume, wenn sie in diesen auf Datenträgern oder in Ordnern gelagert werden, übertragen. Aus dem

Schutzbedarf der Informationen und der Bedeutung der jeweiligen Fachaufgaben und Geschäftsprozesse sind die Schutzbedarfe der Anwendungen abzuleiten. Hierbei kann eine Zuordnung von Anwendungen zu den definierten Schutzbedarfskategorien anhand folgender Abhängigkeiten durchgeführt werden:

- „**normal**: Der Geschäftsprozess bzw. die Fachaufgabe kann mit tolerierbarem Mehraufwand mit anderen Mitteln (z. B. manuell) durchgeführt werden.
- **hoch**: Der Geschäftsprozess bzw. die Fachaufgabe kann nur mit deutlichem Mehraufwand mit anderen Mitteln durchgeführt werden.
- **sehr hoch**: Der Geschäftsprozess bzw. die Fachaufgabe kann ohne die Anwendung überhaupt nicht durchgeführt werden“ (BSI 2008a, S. 53).

Der Schutzbedarf der Hardwaresysteme ergibt sich dann aus den Schutzbedarfen der Anwendungen, für deren reibungslosen Betrieb sie zuständig sind. Entsprechend wird der Schutzbedarf der Räume aus den Hardwaresystemen und Infrastrukturkomponenten sowie aus den Informationen, welche sich in den Räumen befinden, abgeleitet.

Abschließend soll der Schutzbedarf der Kommunikationsverbindungen identifiziert werden. Hierbei wird bestimmt, welche Kommunikationsverbindungen als kritisch zu betrachten sind und warum. Begründungen für die Kritikalität können bspw. sein:

- es handelt sich dabei um eine Außenverbindung, d. h. diese führt in oder über Bereiche (z. B. das Internet), welche außerhalb der Kontrolle des Unternehmens sind
- es handelt sich um Kommunikationsverbindungen, über welche Informationen mit hohem oder sehr hohem Schutzbedarf übertragen werden
- es handelt sich um Kommunikationsverbindungen, über welche bestimmte Informationen nicht übertragen werden dürfen.

Diese Übertragung der Schutzbedarfe von einem Element (bzw. mehreren Elementen) auf andere wird auch „Vererbung“ des Schutzbedarfs genannt (vgl. BSI 2011, S. 47). Folgende Abbildung 6 stellt die Vererbungshierarchie im Rahmen der Schutzbedarfsanalyse graphisch dar.

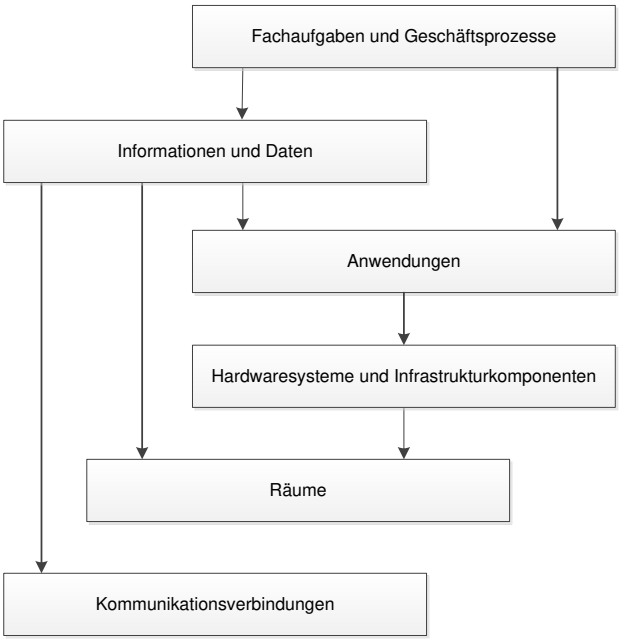

Abbildung 6: Vererbung des Schutzbedarfs

Bei der Vererbung des Schutzbedarfs sollen drei Prinzipien berücksichtigt werden:

- **Maximumprinzip**: Von einem Element wird der höchste Schutzbedarf der jeweiligen Elemente, welche ihren Schutzbedarf auf dieses Element übertragen, vererbt.
- **Kumulationsprinzip**: Weisen alle Elemente, welche ihren Schutzbedarf auf ein anderes übertragen, einen gleichen Schutzbedarf (z. B. normal) auf, so kann es sein, dass das vererbende Element einen höheren Schutzbedarf hat. Z. B. alle Anwendungen, welche auf einem Server installiert sind, haben einen normalen Schutzbedarf, da der Ausfall einer dieser Anwendung keinen wesentlichen Schaden für das Unternehmen verursachen kann. Beim Ausfall des Servers werden jedoch alle betroffenen Anwendungen ausfallen, was dann zu einem höherwiegenden Schaden führen kann, so dass der Schutzbedarf des Servers als hoch eingeschätzt wird.
- **Verteilungsprinzip**: Der vererbte Schutzbedarf eines Elements kann niedriger sein als die Schutzbedarfe der betroffenen Elemente. Z. B. eine Anwendung mit hohem Schutzbedarf wird auf zwei Servern installiert. Beim Ausfall des einen Servers kann der andere verwendet werden, so dass beide Server mit einem normalen Schutzbedarf eingeschätzt werden.

Die Ergebnisse der Schutzbedarfsanalyse sollen wiederum übersichtlich in Tabellenform dargestellt werden. Dabei sollen nicht nur die ermittelten Schutzbedarfe sondern auch Begründungen für die zugewiesenen Werte dokumentiert werden. Die Ermittlung und Darstellung der Schutzbedarfe soll für die relevanten IT-Sicherheitsziele jeweils separat erfolgen, da für ihre Einhaltung i. d. R. unter-

schiedliche Maßnahmen erforderlich sind. Beispiele für die Darstellung von Ergebnissen der Schutzbedarfsanalyse finden sich in Tabelle 7 und Tabelle 8.

Nr.	Bezeichnung	Art der Informationen	Schutzbedarf	Begründung
A1	Personaldatenverarbeitung	p	**Vertraulichkeit:** hoch **Integrität:** normal **Verfügbarkeit:** normal	Personaldaten sind besonders schutzbedürftige Daten, deren Missbrauch die Betroffenen erheblich beeinträchtigen kann. Fehler werden rasch erkannt und können entweder aus der Datensicherung eingespielt oder durch manuelle Eingabe korrigiert werden Ausfälle bis zu einer Woche können mit manuellen Verfahren überbrückt werden.
A2	Beihilfeabwicklung	p	**Vertraulichkeit:** hoch **Integrität:** normal **Verfügbarkeit:** normal	Wie A1
A4	Benutzerauthentisierung	p, s	**Vertraulichkeit:** normal **Integrität:** hoch **Verfügbarkeit:** hoch	Die Passwörter sind verschlüsselt gespeichert und damit praktisch nicht zugänglich. Der hohe Schutzbedarf ergibt sich daraus, dass sich alle Mitarbeiter hierüber identifizieren. Bei Ausfall sind keine Identifizierung und damit keine Ausführung von IT-Verfahren möglich. Ein Ausfall ist bis zu 24 Stunden tolerabel.

Tabelle 7: Schutzbedarf von Anwendungen
Quelle: Leicht verändert entnommen aus BSI 2008a, S. 53 und BSI 2011, S. 46

Nr.	Beschreibung	Schutzbedarf	Begründung
S1	Server für Personalverwaltung	**Vertraulichkeit:** hoch **Integrität:** normal **Verfügbarkeit:** normal	Maximumprinzip: A1, A2, A3
S2	Domänen-Controller	**Vertraulichkeit:** normal **Integrität:** hoch **Verfügbarkeit:** normal	Maximumprinzip: A4, A5 Verteilungsprinzip: Der Schutzbedarf von A4 ist mit "hoch" eingeschätzt. Diese Anwendung ist aber auf zwei Rechnersysteme verteilt. Eine Authentisierung über den zweiten Domänen-Controller S6 in Berlin ist für die Mitarbeiter des Bonner Standortes ebenfalls möglich. Der Schutzbedarf ist aus diesem Grund "normal".
R U.02	Datenträgerarchiv	**Vertraulichkeit:** hoch **Integrität:** normal **Verfügbarkeit:** normal	Maximumprinzip: Backup-Datenträger (Wochensicherung der Server S1 bis S5)
R 1.01	Serverraum	**Vertraulichkeit:** hoch **Integrität:** hoch **Verfügbarkeit:** normal	Maximumprinzip: S1, N4

Tabelle 8: Schutzbedarf von Hardwaresystemen und Räumen
Quelle: Leicht verändert entnommen aus BSI 2008a, S. 55 f.

Für die Elemente, bei welchen der Schutzbedarf als normal eingeschätzt wurde, kann nach der Schutzbedarfsanalyse die Maßnahmenplanung (vgl. Abschnitt 4.5) erfolgen. Für die restlichen Elemente ist vor der Maßnahmenplanung eine Bedrohungsanalyse durchzuführen.

4.4 Bedrohungsanalyse

Die Bedrohungsanalyse (vgl. Eckert 2013, S. 203; BSI 2008b, S. 4 ff.) dient der Ermittlung und Bewertung von Bedrohungen[6], welche auf die Elemente des Informationsverbunds einwirken können. Unter dem Begriff **Bedrohung** wird im Rahmen dieser KE jemand oder etwas (Ereignis), der bzw. das gezielt oder unabsichtlich eine Schwachstelle in einem System ausnutzt, um im System Schaden zu verursachen, verstanden. Eine **Schwachstelle** ist eine Stelle in einem System, die das System verwundbar macht (vgl. Eckert 2013, S. 16 f.). Der **Schaden** kann als negative Auswirkungen auf das System, welche die Erreichung festgelegter Ziele verhindern können, bezeichnet werden (vgl. Klipper 2015, S. 18 f.). Die Wahrscheinlichkeit, dass eine Bedrohung eine Schwachstelle ausnutzt, und der infolge der Ausnutzung potentiell entstandene Schaden werden **Risiko** genannt (vgl. Eckert 2013, S. 18). Aufgrund dieser begrifflichen Abhängigkeiten werden Bedrohungsanalysen im Rahmen des IT-Sicherheits- und Risikomanagements als Bestandteile einer übergeordneten Risikoanalyse aufgeführt. Auch das im Folgenden beschriebene Vorgehen wird vom BSI Risikoanalyse genannt. Allerdings handelt es sich hier um eine vereinfachte Methodik, welche mit möglichst geringem Aufwand angewandt werden kann.

Die Bedrohungsanalyse kann grob in folgende zwei Teilschritte unterteilt werden:

1) **Ermittlung von Bedrohungen**
   In diesem Schritt werden sämtliche Bedrohungen, die auf die betroffenen Elemente des Informationsverbundes (d. h. Elemente mit hohem und sehr hohem Schutzbedarf bezüglich mindestens eines der IT-Sicherheitsziele) einwirken, systematisch erhoben und tabellarisch dargestellt. In der Literatur existieren unterschiedliche Kategorisierungen von Bedrohungen, welche für ihre systematische Erhebung verwendet werden können. Das BSI schlägt z. B. die sechs Kategorien vor:
   - Elementare Gefährdungen
   - Höhere Gewalt
   - Organisatorische Mängel
   - Menschliche Fehlhandlungen
   - Technisches Versagen
   - Vorsätzliche Handlungen (vgl. BSI o. J. "Gefährdungskataloge").

6 Das BSI verwendet hierfür den Begriff „Gefährdung“ (vgl. BSI 2008b, S. 9 ff.).

Für jede dieser Kategorien beschreibt das BSI in seinen „Gefährdungskatalogen“ umfangreich mögliche Bedrohungen und Beispiele und stellt somit ein hilfreiches Instrument für die Durchführung dieses Schritts zur Verfügung. Das BSI unterscheidet jedoch aus Vereinfachungsgründen in seinen Ausführungen zwischen den Begriffen Bedrohung und Schwachstelle nicht. Ein Beispiel, das eine Unterscheidung zwischen den zuletzt genannten Begriffen vornimmt und sowohl Schwachstellen als auch Bedrohungen, welche diese Schwachstellen ausnutzen können, beispielhaft aufgezeigt, liefert Tabelle 9.

Kategorie	Schwachstellen	Bedrohungen
Organisation	Fehlende IT-Sicherheitsrichtlinie	Unerwünschtes Fehlverhalten
	Keine angemessene Zuweisung von IT-Sicherheitsverantwortlichkeiten	Verweigerung der Umsetzung von Maßnahmen
	Keine festgelegten disziplinarischen Folgen bei IT-Sicherheitsvorfällen	Datenmissbrauch
	Mangelnde Prozeduren für den Umgang mit sensiblen Daten	Unerwünschte Verbreitung sensibler Daten
	Fehlende formale Prozeduren für Nutzeran- und -abmeldung	Missbrauch der Zugriffsrechte
Personal	Unzureichende Nutzerschulung	Fehler bei der Nutzung
	Unzureichende IT-Sicherheitsausbildung	Inkorrekter Umgang mit z. B. Viren, Spam-Emails
	Inadäquate Personalrekrutierung	Absichtliches Fehlverhalten; Zerstörung von Geräten oder Daten
	Unzufriedene (ehemalige) Mitarbeiter	Gezielter Angriff auf die IT
	Externe Mitarbeiter (z. B. Handwerker, Reinigungskräfte)	Zerstörung von Geräten; Diebstahl von Medien/Dokumenten
Standort	Liegt in einem Gebiet mit Hochwassergefahr	Überschwemmung
	Liegt in einem Gebiet mit sehr hohen Temperaturen	Überhitzung
	Liegt in einem Gebiet mit instabiler Stromversorgung	Störungen in der Stromversorgung
	Liegt in einem Gebiet mit instabiler Internetverbindung	Ausfälle der Internetverbindung
	Fehlender, physischer Schutz des Gebäudes, der Türen oder Fenster	Zerstörung oder Diebstahl von Geräten
Netzwerk	Unsichere Netzwerkarchitektur	Spionage
	Inadäquate Netzwerkverwaltung	Entstehung vom sogen. „Flaschenhals“
	Ungesicherte Kommunikationsverbindungen	Abhören der Kommunikation
	Schlechte Verkabelung	Ausfall/Störung der Telekommunikationsanlage
	Ungesichertes drahtloses lokales Netzwerk	Unautorisierte Nutzung des Netzwerks
Hardware	Unzureichende Wartung/Fehlerhafte Installation eines Systems	Ausfall des Systems
	Mangel an wirksamer Konfigurationskontrolle	Funktionseinschränkung
	Anfälligkeit für Spannungsschwankungen	Ausfall der Stromversorgung
	Ungesicherte Speichermedien	Diebstahl der Medien
	Ungesicherte Kopierer	Diebstahl von Dokumenten
Software	Mangelnde oder unzureichende Softwaretests	Manipulation von Daten
	Bekannte Lücken in Software	Hackerangriffe durch Viren
	Fehlende Funktion für vollständige und sichere Datenlöschung	Auslesen inkorrekt gelöschter Daten
	Mangelnde Dokumentation	Fehler bei der Nutzung
	Komplizierte Benutzeroberfläche	Fehler bei der Nutzung

Tabelle 9: Beispiele für IT-sicherheitsrelevante Schwachstellen und Bedrohungen
Quelle: In Anlehnung an British Standards Institute 2008, S. 42 ff.

Das Ergebnis dieses Schritts ist eine tabellarische Darstellung der betrachteten Elemente mit den jeweils relevanten Bedrohungen. In der Darstellung sollen außerdem auch die Schutzbedarfe der Elemente aufgeführt werden, da dies die Analysen der nachfolgenden Schritte erleichtert. Tabelle 10 zeigt beispielhaft, wie die Bedrohungsübersicht eines Kommunikationsservers und eines Serverraums aussehen können.

	Kommunikationsserver S3		
Schutzbedarf	Vertraulichkeit: normal	Integrität: hoch	Verfügbarkeit: hoch
Bedrohung	Ausfall des Systems Fahrlässige Zerstörung des Geräts Ausfall der Stromversorgung Integritätsverlust schützenswerter Informationen		
	Serverraum R 1.01		
Schutzbedarf	Vertraulichkeit: normal	Integrität: hoch	Verfügbarkeit: hoch
Bedrohung	Feuer Wasser Unbefugter Zutritt Vandalismus		

Tabelle 10: Beispielhafte Bedrohungsübersicht für einen Kommunikationsserver und einen Serverraum

Quelle: Leicht verändert entnommen aus BSI 2008b, S. 10 f.

2) **Bewertung von Bedrohungen**

In diesem Schritt werden die im vorherigen Schritt ermittelten Bedrohungen bewertet. Dabei wird für jedes Element untersucht, ob geeignete Sicherheitsmaßnahmen bereits umgesetzt oder im Rahmen des entwickelten IT-Sicherheitskonzepts geplant sind, um den jeweiligen Bedrohungen entgegenzuwirken. Für die Bewertung können z. B. folgende Kriterien angewendet werden:

- **Vollständigkeit**: Hier wird auf die Frage, ob bereits eingesetzte oder geplante Sicherheitsmaßnahmen gegen alle Aspekte der untersuchten Bedrohung wirksam sind, eingegangen.
- **Stärke**: Hier wird auf die Frage, ob bereits eingesetzte oder geplante Sicherheitsmaßnahmen der untersuchten Bedrohung ausreichend stark entgegenwirken, eingegangen.
- **Zuverlässigkeit**: Hier wird auf die Frage, ob bereits eingesetzte oder geplante Sicherheitsmaßnahmen zu leicht umgegangen werden könnten, eingegangen.

Das BSI empfiehlt die Verwendung der Parameter aus der klassischen Risikobewertung – Eintrittswahrscheinlichkeit und potentieller Schaden – in diesem Kontext nicht, da es i. d. R. schwierig ist, zuverlässige Werte für sie zu bestimmen. Beide Parameter werden aber in den hier beschriebenen Bewertungskriterien implizit berücksichtigt.

Das Ergebnis der Bedrohungsanalyse ist eine Übersicht über die Bedrohungen pro Element, welchen durch bereits umgesetzte oder geplante Sicherheitsmaßnahmen

ausreichend bzw. nicht ausreichend entgegengewirkt werden kann. Die Gruppe der Bedrohungen, für welche noch keine ausreichenden Sicherheitsmaßnahmen umgesetzt oder geplant worden sind, wird im nächsten Schritt der Maßnahmenplanung weiter behandelt.

4.5 Maßnahmenplanung

Im letzten Schritt Erarbeitung eines IT-Sicherheitskonzepts erfolgt die Maßnahmenplanung. Hier werden zunächst die IT-Sicherheitsmaßnahmen, welche notwendig sind, um die Schutzbedarfe der Elemente des Informationsverbunds zu decken, erarbeitet. Für die Unterstützung dieses Schritts bietet das BSI ebenfalls umfangreiche Kataloge an (vgl. BSI 2008a, S. 60 ff.; BSI o. J. "Maßnahmenkataloge"). Kapitel 5 setzt sich mit den diversen IT-Sicherheitsmaßnahmen auseinander.

Für die Elemente mit hohem oder sehr hohem Schutzbedarf, für welche aus den angebotenen Katalogen keine geeigneten Maßnahmen abgeleitet werden können, ist zu entscheiden, wie mit den identifizierten Bedrohungen umgegangen werden soll. Hierbei ist grundsätzlich zwischen den folgenden vier Handlungsalternativen aus dem Risikomanagement zu unterscheiden (vgl. BSI 2008b, S. 17 f.; British Standards Institute 2008, S. 17 ff.):

- **Risikoreduktion**: Bei dieser Alternative wird durch die Entwicklung und Implementierung von Sicherheitsmaßnahmen versucht, die Eintrittswahrscheinlichkeit eines Sicherheitsvorfalls oder der daraus resultierende potentielle Schaden oder beides zu reduzieren.
- **Risikovermeidung**: Eine Bedrohung kann z. B. durch Umstrukturierung von Prozessen oder Strukturen vermieden werden. Diese Alternative ist dann auszuwählen, wenn z. B. die Entwicklung und Implementierung einer Sicherheitsmaßnahme zu teuer wäre oder eine Sicherheitsmaßnahme die Funktionalität oder Leistung des betroffenen Systems wesentlich einschränken würde.
- **Risikoübernahme** bzw. **Risikoakzeptanz**: Jedes Unternehmen soll Kriterien für die Akzeptanz von Risiken definieren. Solche Kriterien sind z. B.: Ein Sicherheitsvorfall kann lediglich mit einer sehr geringen Wahrscheinlichkeit eintreten und einen Schaden verursachen. Es sind aktuell keine effektiven Sicherheitsmaßnahmen bekannt, um der betrachteten Bedrohung entgegenzuwirken. Werden die Kriterien erfüllt, so ist diese Alternative zu wählen.
- **Risikotransfer**: Ein Risiko wird an eine andere Institution übertragen, wenn z. B. der Schaden rein finanziell ist (z. B. Abschluss von Versicherungen) oder andere Institutionen dieses effektiver und effizienter steuern können (z. B. Auslagerung des Infrastrukturmanagements an ein Systemhaus). Diese Alternative kann die Entstehung von neuen oder die Verände-

rung von identifizierten Bedrohungen als Folge haben und dadurch bereits festgelegte Handlungen beeinflussen.

Die Handlungsalternativen schließen sich gegenseitig nicht aus. Bei der Behandlung einer Bedrohung können mehrere Alternativen kombiniert werden, um bessere Ergebnisse zu erzielen.

Bei der Wahl der passenden Handlungsalternativen und Sicherheitsmaßnahmen ist auf unterschiedliche Kriterien zu achten, vor allem auf ihre Angemessenheit. Die **Angemessenheit** schließt in diesem Kontext ein (vgl. BSI 2008a, S. 65):

- **Wirksamkeit**: Die Maßnahmen decken die identifizierten Schutzbedarfe effektiv ab.
- **Eignung**: Die Maßnahmen führen nicht zu Beeinträchtigungen in den Unternehmensabläufen oder stehen nicht in gegenseitigem Konflikt zueinander.
- **Praktikabilität**: Die Maßnahmen sind praktisch umsetzbar, verständlich, wenig fehleranfällig.
- **Wirtschaftlichkeit**: Die Maßnahmen führen nach ihrer Umsetzung zu einem Nutzen für das Unternehmen, der größer ist als die für die Umsetzung benötigten Kosten.

Tabelle 11 stellt dar, wie Bedrohungen für einen Kommunikationsserver beispielhaft behandelt werden können.

	Kommunikationsserver S3
Schutzbedarf	Vertraulichkeit: normal Integrität: hoch Verfügbarkeit: hoch
Bedrohung	*Ausfall des Systems*
Behandlung	Ergänzende Sicherheitsmaßnahme: *Bereithalten eines vollständigen Ersatzsystems zur Kommunikation mit dem Auftraggeber* Es wird ein vollständiges Ersatzsystem zur Kommunikation mit dem Auftraggeber bereitgehalten. Dies umfasst alle technischen Komponenten einschließlich Kommunikationsverbindungen. Das Ersatzsystem wird in Raum E.3 gelagert. Es wird sichergestellt, dass das Ersatzsystem jederzeit die gleiche Konfiguration wie das Produktionssystem aufweist und innerhalb von 30 Minuten einsatzbereit ist. Die Kommunikation mit dem Auftraggeber erfolgt über eine Wählverbindung. Das gesamte Ersatzsystem einschließlich Wählverbindung wird mindestens einmal pro Quartal und bei jeder Konfigurationsänderung getestet.
Bedrohung	*Integritätsverlust schützenswerter Informationen*
Behandlung	Risikoübernahme: Das Risiko wird durch die in den Übertragungs- und IT-Systemen eingebauten Sicherheitsmechanismen zwar etwas reduziert, jedoch sind weiterhin Sicherheitsvorfälle denkbar, die zu verfälschten Bedarfsinformationen und somit zu hohen Kosten für das Unternehmen führen können. Dieses Restrisiko wird von der Geschäftsführung akzeptiert und verantwortet, da alle wirksamen Gegenmaßnahmen unwirtschaftlich sind.

Tabelle 11: Beispielhafte Behandlung von Bedrohungen
Quelle: Leicht verändert entnommen aus BSI 2008b, S. 19

Nach der Entwicklung der erforderlichen Sicherheitsmaßnahmen empfiehlt das BSI die Durchführung eines „Basis-Sicherheitschecks“. Dieser hat die Aufgabe, zu ermitteln, welche Sicherheitsmaßnahmen bereits umgesetzt sind und wo sich noch mögliche IT-Sicherheitslücken befinden (vgl. BSI 2008a, S. 65 f.).

Im Rahmen der Maßnahmenplanung ist weiterhin festzulegen, welche Sicherheitsmaßnahmen in welchem Zeitraum und welcher Reihenfolge umzusetzen sind. Das ist insofern wichtig, als für die Maßnahmenumsetzung i. d. R. nur begrenzte Ressourcen zur Verfügung stehen, was eine Priorisierung und Strukturierung der Maßnahmen voraussetzt. Die Planung der Umsetzungsreihenfolge beinhaltet (vgl. BSI 2008a, S. 77 f.):

- die Priorisierung einer Maßnahme bspw. anhand ihrer Wichtigkeit, Dringlichkeit, Wirkung
- die Identifikation möglicher Zusammenhänge zwischen Maßnahmen, welche zu einer zwingenden Umsetzungsreihenfolge führen
- die Festlegung von Aufgaben und Verantwortlichkeiten für die Umsetzung der einzelnen Maßnahmen sowie für die Kontrolle der Umsetzung.

Abschließend ist noch anzumerken, dass die Erarbeitung eines IT-Sicherheitskonzepts keine einmalige Aufgabe ist. Sie ist vielmehr als ein Prozess zu betrachten, den ein Unternehmen je nach Entwicklungen und Veränderungen in seiner strategischen Ausrichtung, in seiner Organisation oder auch im IT-Sicherheitsbereich regelmäßig durchzuführen hat. Das Ziel dabei ist, das IT-Sicherheitskonzept laufend an veränderte Rahmenbedingungen anzupassen.

5 IT-Sicherheitsmaßnahmen, -organisation und -kultur

Nachdem in den vorherigen Kapiteln die Entwicklung und Steuerung einer IT-Sicherheitsstrategie sowie die Erarbeitung eines IT-Sicherheitskonzepts behandelt wurden, wird in diesem Kapitel auf die Umsetzung der IT-Sicherheitsstrategie und -konzept eingegangen. Dabei werden zunächst grundlegende IT-Sicherheitsmaßnahmen vorgestellt, die heutzutage von den meisten Unternehmen umzusetzen sind. Als nächstes wird die IT-Sicherheitsorganisation betrachtet. Hierbei werden Möglichkeiten für die organisationale Einbettung des ITSM sowie einige wichtige Rollen und Verantwortlichkeiten in diesem Bereich erläutert. Der letzte Abschnitt dieses Kapitels befasst sich mit der IT-Sicherheitskultur, da sie eine besondere Bedeutung für die Erreichung der IT-Sicherheitsziele jedes Unternehmens hat.

5.1 Klassifikation und Beispiele für IT-Sicherheitsmaßnahmen

Die Norm ISO/IEC 27002 definiert den Begriff **Maßnahme** als „Mittel für das [ITSM], einschließlich Leitlinien, Verfahren, Richtlinien, Praktiken oder organisationseigene Strukturen, welche verwaltender, technischer, leitender oder gesetzlicher Natur sein können. Der Begriff „Maßnahme“ wird auch als Synonym für „Schutzmaßnahme“ und „Gegenmaßnahme“ verwendet.“ (ISO/IEC 27002:2005, S. 12). Hierzu wird aber auch der englische Begriff „Control“ (vgl. Klipper 2015, S. 15) oder in Anlehnung daran der Begriff „Kontrollmaßnahme“ (vgl. z. B. Eckert 2013, S. 28) benutzt. Aus dieser Definition wird deutlich, dass fast alle Aktivitäten im Rahmen des ITSM als IT-Sicherheitsmaßnahmen verstanden werden können. In diesem Abschnitt werden zunächst Möglichkeiten für die Klassifikation von IT-Sicherheitsmaßnahmen sowie Beispiele für die unterschiedlichen Maßnahmenkategorien gegeben. In den folgenden zwei Abschnitten wird dann vertieft auf organisatorische und den Mensch betreffende IT-Sicherheitsmaßnahmen eingegangen.

Klassifikation von IT-Sicherheitsmaßnahmen

In der Literatur finden sich unterschiedliche Klassifikationen für die IT-Sicherheitsmaßnahmen. Einige Beispiele dafür sind:

- BDSG § 9: „technische“ und „organisatorische“ Maßnahmen
- Schou und Hernandez (2015, S. 41): „Management“-, „operative“ und „technische“ Maßnahmen
- ISF (2007): Maßnahmen für die Bereiche „Sicherheitsmanagement“, „Kritische Geschäftsapplikationen“, „Computerinstallationen“, „Netzwerke“, „Systementwicklung“ und „Nutzerumgebung“
- BSI (o. J., "Maßnahmenkataloge"): Maßnahmen für die Bereiche „Infrastruktur“, „Organisation“, „Personal“, „Hard- und Software“, „Kommunikation“ und „Notfallvorsorge“.

Folgende Tabelle 12 liefert Beispiele für die zuletzt genannte Klassifikation des BSI. Ausführliche Erläuterungen zu den einzelnen Maßnahmen sowie weitere Beispiele finden sich bei der angegebenen Quelle.

Kategorie	Maßnahmen
Organisation	Festlegung von Verantwortlichkeiten und Regelungen Regelungen für Wartungs- und Reparaturarbeiten Vergabe von Zutritts- und Zugangsberechtigungen Rechtevergabe Regelung des Passwortgebrauchs Regelung für die Einrichtung von Benutzern / Benutzergruppen Regelung des Datenträgeraustausches Reaktion auf Verletzungen der Sicherheitsvorgaben Ermittlung und Dokumentation der Rechtsgrundlagen für Anwendungen Erstellung einer Cloud-Nutzungs-Strategie
Personal	Geregelte Einarbeitung/Einweisung neuer Mitarbeiter Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze und Vorschriften Vertretungsregelungen Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern Einweisung des Personals in den sicheren Umgang mit IT Nennen von Ansprechpartnern für Sicherheitsfragen Analyse sicherheitsrelevanter personeller Faktoren Analyse der Zielgruppen für Sensibilisierungs- und Schulungsprogramme Schulung der Administratoren von Cloud-Infrastrukturen Messung und Auswertung des Lernerfolgs
Infrastruktur	Erstellung eines Blitzschutzkonzepts und Installation einer Blitzschutzanlage Einhaltung von Brandschutzvorschriften und Installation einer Brandmeldeanlage Auswahl eines geeignetes Standorts Installation von Einbruchsschutz und Einbruchsmeldeanlage Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht Vermeidung von wasserführenden Leitungen Bereitstellung einer unterbrechungsfreie Stromversorgung Funktionstests der technischen Infrastruktur Dimensionierung und Nutzung von Schranksystemen Gesicherte Aufstellung aktiver Netzkomponenten
Hard- und Software	Einsatz von Viren-Schutzprogrammen Sperren und Löschen nicht benötigter Accounts und Terminals Test neuer Hard- und Software Software-Reinstallation bei Benutzerwechsel eines Laptops Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen Verhinderung der unautorisierten Nutzung von Rechnermikrofonen und Kameras Auswahl von Applikationen für Smartphones und Tablets Sichere Zugriffsmechanismen bei Fernadministration
Kommunikation	Entfernen oder Deaktivieren nicht benötigter Leitungen Auswahl einer geeigneten Netz-Topologie Dokumentation und Kennzeichnung der Verkabelung Regelmäßiger Sicherheitscheck des Netzes Kompatibilitätsprüfung des Sender- und Empfängersystems Sichere Nutzung von sozialen Netzwerken Sichere Anbindung von Smartphones und Tablets an das Netz der Organisation Sichere Konfiguration eines Netzes für virtuelle Infrastrukturen Einsatz von Stand-alone-Systemen zur Nutzung des Internets
Notfallvorsorge	Erstellung einer Übersicht über Verfügbarkeitsanforderungen Abschließen von Versicherungen Redundante Leitungsführung Sicherungskopie der eingesetzten Software Entwicklung eines Datensicherungskonzepts Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen Übungen zur Datenrekonstruktion Vorsorge vor Verlust und Diebstahl von Laptops, Smartphones, Tablets Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten

Tabelle 12: IT-Sicherheitsmaßnahmen
Quelle: Entnommen aus BSI o. J., "Maßnahmenkataloge"

Eine weitere Möglichkeit für die Klassifizierung der IT-Sicherheitsmaßnahmen bieten die in einem Unternehmen definierten IT-Sicherheitsziele. Im Folgenden werden daher beispielhafte Maßnahmen beschrieben, durch welche die in Abschnitt 2.1 dieser KE vorgestellten IT-Sicherheitsziele realisiert werden können.

- **Maßnahmen zur Gewährleistung der Vertraulichkeit**
  Grundlegende Maßnahmen in diesem Bereich sind die Festlegung von Berechtigungen und Kontrollen für den Zugriff auf Daten bzw. Informationen sowie die Einstufung der unterschiedlichen Daten in passende Vertraulichkeitskategorien (z. B. nicht vertraulich, vertraulich, hoch vertraulich). Eine weitere Maßnahme ist die Verschlüsselung. Hierbei kann einerseits eine Verschlüsselung der Daten selbst vorgenommen werden, um sicherzustellen, dass sie bspw. aus Datenbanken oder Datenträgern von Unbefugten nicht ausgelesen werden können. Andererseits können Techniken für die Verschlüsselung von Kommunikationsverbindungen angewendet werden, um den sicheren Datentransport zu gewährleisten (vgl. Eckert 2013, S. 10 ff.; Hansen et al. 2015, S. 384 ff.).
- **Maßnahmen zur Gewährleistung der Verfügbarkeit**
  Grundlegende Maßnahme in diesem Bereich ist die Bereitstellung bzw. Aufstellung von Redundanzen (vgl. Rath und Sponholz 2014, S. 237 f.). Insbesondere kritische Systeme, bei welchen kurzfristige Ausfälle nicht akzeptabel sind, sind redundant aufzustellen, so dass nach dem Ausfall des Hauptsystems (das System, das i. d. R. für die Durchführung bestimmter Prozesse bereitgestellt ist) ein Ersatzsystem seine Rolle übernehmen kann. Das gleiche gilt auch für wichtige Daten, welche mehrfach auf unterschiedliche Systeme und Medien zu speichern sind, so dass sie bspw. nach einer Beschädigung oder Löschung wiederhergestellt werden können. In diesem Zusammenhang wird auch von Datensicherung und -wiederherstellung (engl. Backup and Restoration) gesprochen (vgl. Schou und Hernandez 2015, S. 271 ff.). Eine weitere Maßnahme ist die Installation von sogenannten Intrusion Detection and Prevention Systemes, welche gezielte Angriffe auf die Verfügbarkeit von Systemen (Denial of Service-Attacken) aufdecken und verhindern (vgl. Schou und Hernandez 2015, S. 187, 209 f.).
- **Maßnahmen zur Gewährleistung der Verbindlichkeit**
  Die Verbindlichkeit kann vor allem durch die Anwendung von digitalen Signaturen sichergestellt werden. Digitale Signaturen können als „elektronisches Äquivalent zu handschriftlichen Unterschriften“ (Eckert 2013, S. 398) betrachtet werden und müssen Auskunft über den Unterzeichner geben, bestätigen, dass das signierte Dokument vom Unterzeichner genehmigt wurde und dass es inhaltlich richtig und vollständig ist. Außerdem demonstriert das Signieren eines Dokuments auf diese Art und Weise, dass es eine rechtliche Bedeutung hat (vgl. Eckert 2013, S. 13, 389 f.).

- **Maßnahmen zur Gewährleistung der Integrität**
  Grundlegende Maßnahmen in diesem Bereich sind, ähnlich wie im Bereich der Vertraulichkeit, die Festlegung und Vergabe geeigneter Schreib- und Leserechte auf Daten und Informationen, die Verschlüsselung der Daten, so dass eine Veränderung dieser nur nach der Entschlüsselung möglich ist. Für die Überprüfung der Integrität von Daten werden weiterhin kryptografische Verfahren eingesetzt, die „digitale Fingerabdrücke“ (Message Authentication Codes) berechnen und einer Datei hinzufügen (vgl. Eckert 2013, S. 9, 381 ff.). Darüber hinaus sind qualitätssichernde Maßnahmen, wie z. B. die Durchführung von Tests vor der Einführung neuer Hard- oder Software, umzusetzen, um sicherzustellen, dass keine Fehler in ihrer Erstellung oder Implementierung zu einer unerwünschten Manipulation von Daten führen können (vgl. Rath und Sponholz 2014, S. 238).

- **Maßnahmen zur Gewährleistung der Authentizität**
  Der Prozess zur Gewährleistung der Authentizität wird Authentifikation genannt. Die Authentifikation von Nutzern wird i. d. R. durch die Verwendung von Benutzerkennungsfunktionen, im Zusammenhang mit z. B. Benutzernamen und -kennwörtern, biometrischen Merkmalen (z. B. Fingerabdrücke), Identifikationskarten (z. B. Smartcards, Personalausweis) realisiert. Um die Wirksamkeit einzelner Verfahren zu erhöhen, werden bei manchen Systemen mehrere Verfahren kombiniert. So muss sich bspw. ein Kunde an einem Bankterminal mit seiner EC-Karte und einer PIN (persönliche Identifikationsnummer) ausweisen, um die Funktionen des Terminals nutzen zu können. Für die Überprüfung der Authentizität von Objekten, wie z. B. Webserver oder Access Points, werden kryptografische Verfahren eingesetzt, die den Ursprung oder den Urheber des Objekts nachweisen. Hierbei werden Authentifikationsprotokolle zwischen den Objekten abgewickelt (vgl. Eckert 2013, S. 8, 465 ff.).

- **Maßnahmen zur Gewährleistung der Anonymität**
  Der Prozess zur Gewährleistung der Anonymität wird Anonymisierung genannt. Er wird durch sogenannte Anonymisierungsdienste realisiert. Solche Dienste kombinieren Vermeidungstechniken, die z. B. Daten unterdrücken, mit Verschleierungstechniken, die z. B. Daten durch Standardmuster ersetzen, um den Personenbezug aus den Daten zu entfernen bzw. zu verstecken, bevor die Daten einem Dritten übermittelt werden. Diese Dienste werden insbesondere dafür verwendet, um die Erstellung von Nutzerprofilen aus Daten ihrer Bewegung, Kommunikation oder ihrer Zugriffen im Internet durch Dritte zu erschweren bzw. zu unterbinden (vgl. Eckert 2013, S. 13 f.).

5.2 IT-Sicherheitsorganisation

Die IT-Sicherheitsorganisation ist die Organisationseinheit des Unternehmens, welche für die IT-Sicherheit zuständig ist. In der IT-Sicherheitsorganisation werden Rollen, Aufgaben und Verantwortlichkeiten für alle im IT-Sicherheitsprozess involvierten Personen eindeutig definiert und zugewiesen. Der Aufbau der IT-Sicherheitsorganisation hängt von mehreren Faktoren, wie z. B. Unternehmensform, -größe, -branche, Geschäftsmodell, Stellenwert der IT, ab (vgl. Heinrich und Stelzer 2011, S. 181; Schou und Hernandez 2015, S. 83).

Strukturvarianten für die IT-Sicherheitsorganisation

Bei dem Aufbau der IT-Sicherheitsorganisation ist zwischen den folgenden drei Strukturvarianten zu wählen (vgl. Schou und Hernandez 2015, S. 84 f.):

- **zentralisierte Struktur**: Der IT-Sicherheitsmanagementprozess wird zentral, von einer Einheit geführt und verantwortet. Diese Struktur ist für kleinere Unternehmen mit begrenzten personellen und finanziellen Ressourcen geeignet.
- **verteilte Struktur**: Die Rollen, Verantwortlichkeiten und Kompetenzen im Rahmen des ITSM sind über die Geschäftseinheiten, operative Bereiche und geografische Standorte verteilt. Diese Struktur eignet sich besser für komplexe Unternehmen mit mehreren Standorten und internationalen Zweigstellen. Jede Funktionseinheit des Unternehmens ist für die Planung und Implementierung ihres eigenen IT-Sicherheitsprogramms zuständig. So können die lokalen Gesetze und Vorschriften von den unterschiedlichen Zweigstellen für das jeweilige Programm am besten berücksichtigt werden.
- **hybride Struktur**: Diese Struktur stellt eine Kombination zwischen der zentralisierten und der verteilten Struktur dar. Eine zentrale Einheit übernimmt dabei die Führungsaufgaben im Rahmen des ITSM, während die Ausführung der einzelnen IT-Sicherheitsaktivitäten verteilt erfolgt. Die zentrale Führung sorgt für Einheitlichkeit und die dezentrale Ausführung für einfache Durchsetzung der IT-Sicherheitsrichtlinien und -normen. Dieser Aufbau der IT-Sicherheitsorganisation zielt darauf ab, redundante Aufgaben und dadurch entstandenen Mehraufwand zu vermeiden, und wird zunehmend von den Unternehmen bevorzugt.

Rollen und Verantwortlichkeiten

Unabhängig von der gewählten Struktur existieren allgemeine Rollen und Verantwortlichkeiten, welche jedes Unternehmen im Rahmen seines ITSM eindeutig zu definieren und zuzuweisen hat. Die Definition der für ein Unternehmen relevanten Rollen und Verantwortlichkeiten ist bereits bei der Entwicklung der IT-Sicherheitsrichtlinie vorzunehmen (vgl. Abschnitt 3.1) und gehört somit zu den strategischen Aufgaben des ITSM. Die Rollen und Verantwortlichkeiten betreffen sowohl die Ebene der Unternehmensführung als auch einzelne Funktionseinheiten sowie die allgemeinen Nutzer. Einige der wichtigsten Rollen im Rahmen des ITSM sind (vgl. Schou und Hernandez 2015, S. 86 ff.):

- **Geschäftsführer** (Chief Executive Officer, CEO): Ihm obliegt die Gesamtverantwortung für die IT-Sicherheit im Unternehmen. Zu seinen Aufgaben in diesem Bereich gehört z. B. zu gewährleisten, dass die IT-Sicherheitsmanagementprozesse in den strategischen und operativen Unternehmensprozessen integriert sind und dass die anderen Verantwortlichen ihre IT-Sicherheitsmanagementaufgaben entsprechend erledigen. Der Geschäftsführer muss außerdem Sorge tragen, dass das Unternehmen über ausreichend ausgebildetes Personal verfügt, das den jeweiligen IT-Sicherheitsanforderungen sowie relevanten gesetzlichen Vorschriften und Normen entspricht. Weiterhin ist er für das Schaffen eines Bewusstseins für das Thema IT-Sicherheit im Unternehmen und die aktive Unterstützung der anderen Bereiche bei der Kontrolle und Verbesserung von IT-Sicherheitsprogrammen und -aktivitäten zuständig.
- **IT-Leiter** (Chief Information Officer, CIO): Er ist im ITSM-Bereich u. a. zuständig für die Entwicklung und Einhaltung von relevanten Richtlinien, Prozeduren und Kontrollen. Er beaufsichtigt das Personal, das wichtige IT-Sicherheitsaufgaben hat und stellt sicher, dass dieses über die notwendige Ausbildung verfügt. Weiterhin unterstützt er die Führungskräfte bei der Bewältigung ihrer Aufgaben im ITSM-Bereich und erstellt für sie mindestens einmal jährlich entsprechende Effektivitäts- bzw. Erfolgsberichte.
- **Informationssicherheitsverantwortlicher** (Chief Information Security Officer, CISO): Er ist insgesamt für die Gewährleistung der Informationssicherheit im Unternehmen zuständig und verfügt über die notwendige Qualifikation, Ausbildung und Erfahrung, um die ITSM-Funktionen zu verwalten. Er leitet die IT-Sicherheitsorganisation und hat die Aufgabe, das Unternehmen bei der Erhöhung seiner IT-Sicherheit zu unterstützen.
- **Verantwortlicher für die Informationssystemsicherheit** (Information System Security Officer, ISSO): Er ist für die Sicherheit der Informationssysteme während ihres gesamten Lebenszyklus zuständig. Er dient auch als Berater für alle Fragen rund um die Informationssystemsicherheit. Er steuert und überwacht die täglichen Sicherheitskontrollen in diesem Bereich.
- **Datenschutzbeauftragter** (Privacy Officer): Er ist für die Gewährleistung des datenschutzkonformen Umgangs mit personenbezogenen Daten von Seite der Unternehmensmitgliedern zuständig (vgl. Grünendahl et al. 2012, S. 29).
- **Auditor**: Er überprüft die Einhaltung von Richtlinien und Gesetzen. Er ist weiterhin für die Überwachung und Auswertung der Effektivität von internen Kontrollen und Sicherheitsmaßnahmen verantwortlich. Der Auditor darf nicht in die operativen IT-Sicherheitsprozesse involviert sein (vgl. Kersten und Klett 2015, S. 57 f.).

- **Nutzer**: Die IT-System- und Informationsnutzer spielen eine besondere Rolle für die Gewährleistung der IT-Sicherheit. Sie sind für die korrekte Nutzung der Systeme und Information verantwortlich. Weiterhin haben sie diese, den Unternehmensnormen und -regeln folgend, zu schützen. Um ihre Aufgaben und Verantwortlichkeiten jedoch wahrnehmen zu können, müssen sie zunächst entsprechend geschult werden.

Über die genannten Rollen hinaus sind auch **Technologie- und Dienstleistungszulieferer** für die Gewährleistung der IT-Sicherheit eines Unternehmens wesentlich, sodass deren Rollen, Aufgaben und Verantwortlichkeiten in diesem Bereich ebenfalls festzulegen sind. Diese Festlegung soll in Kooperation mit den Zulieferern erfolgen und in die Verträge aufgenommen werden.

Der reine Aufbau einer IT-Sicherheitsorganisation und die klare Definition und Zuweisung von IT-sicherheitsrelevanten Rollen, Aufgaben und Verantwortlichkeiten sind keine ausreichenden Maßnahmen, die garantieren können, dass diese von den jeweiligen Unternehmensmitgliedern auch wahrgenommen werden. Die Regeln und Kontrollen im Bereich der IT-Sicherheit werden oft als lästig oder unnötig empfunden und, als Folge dessen, ignoriert. Deswegen ist es hier besonders wichtig, eine Kultur, die zum notwendigen Bewusstsein für das Thema bei jedem einzelnen führt, zu entwickeln und im Unternehmen zu verankern. Mit dieser Aufgabe beschäftigt sich der folgende Abschnitt.

5.3 IT-Sicherheitskultur

Die fehlende Sensibilisierung von Mitarbeitern für das Thema IT-Sicherheit ist oft das größte Problem bei der Realisierung eines erfolgreichen ITSM. Ein Unternehmen kann, trotz einer gut funktionierenden und innovativen IT-Sicherheitstechnik und sinnvoll aufgebauter IT-Sicherheitsorganisation, Schwierigkeiten bei der Erfüllung seine IT-Sicherheitsziele haben, wenn seine Mitarbeiter Gefahren und Konsequenzen ihres Handelns nicht verstehen und absehen können. Aus diesem Grund gilt der Mensch seit Jahren als das „schwächste Glied“ in einem IT-Sicherheitssystem (vgl. z. B. Sasse et al. 2001). Dies wird durch mehrere Studien bestätigt. Beispielsweise ergab eine Umfrage des BSI aus dem Jahr 2015, an welcher sich 424 deutsche Institutionen beteiligten, dass die häufigste Ursache für den Erfolg von IT-Sicherheitsangriffen auf das Fehlverhalten von Mitarbeitern zurückzuführen ist (vgl. BSI 2015, S. 16). Ähnliche Ergebnisse liefern auch die Studie des Ponemon Institute, durchgeführt in den USA im Jahr 2014, (vgl. Ponemon 2015, S. 11) sowie die internationale Studie von PWC aus dem Jahr 2015 (vgl. PwC 2015, S. 24).

In diesem Abschnitt wird der Mensch in den Mittelpunkt der IT-Sicherheitsbetrachtung gestellt. Dabei wird herausgearbeitet, wie soziale, kulturelle und ethische Aspekte im Rahmen einer IT-Sicherheitskultur zu berücksichtigen sind (vgl. Schlienger 2007), um ein IT-sicherheitskonformes Verhalten bei den Unternehmensmitgliedern zu erreichen.

Die IT-Sicherheitskultur ist ein Bestandteil der Unternehmenskultur. Die **Unternehmenskultur** (häufig auch Organisationskultur genannt) wird als die Gesamtheit aller für das Unternehmen gültigen Wertvorstellungen, Grundsätze, Normen und Denkweisen, die das korrekte Verhalten der Mitglieder auf allen Unternehmensebenen prägen, verstanden (vgl. Schein 1984, S. 3). Folglich prägt die **IT-Sicherheitskultur** „[…] die Wahrnehmung, das Denken, Fühlen und Handeln [der Unternehmensmitglieder] in Bezug auf [IT-]Sicherheit" (Schlienger 2007, S. 487).

Einflussfaktoren auf die IT-Sicherheitskultur

Die Schaffung einer effektiven IT-Sicherheitskultur im Unternehmen wird von mehreren Faktoren beeinflusst. Zu diesen Faktoren gehören z. B. (vgl. Alnatheer 2015):

- **Unterstützung durch die oberste Führungsebene**: Dieser Faktor bezieht sich einerseits auf den Grad, bis zum welchen die oberste Führungsebene die Wichtigkeit des ITSM versteht und sich an den IT-Sicherheitsaktivitäten beteiligt, und andererseits auf ihr Engagement bei der Entwicklung und Etablierung der IT-Sicherheitskultur im Unternehmen. Dabei soll sie Programme und Aktivitäten zur Steigerung des IT-Sicherheitsbewusstseins fördern, sowie auf die Aktualität, Eignung und Einhaltung der IT-Sicherheitsrichtlinie bestehen.
- **Etablierung einer effektiven IT-Sicherheitsrichtlinie**: Die IT-Sicherheitsrichtlinie ist zentral für das gesamte IT-Sicherheitsprogramm jedes Unternehmens und eine Voraussetzung für die Entwicklung der IT-Sicherheitskultur. Denn sie liefert Definitionen für die Rollen und Verantwortlichkeiten aller Stakeholder sowie dafür, was ein IT-sicherheitskonformes Verhalten ist.
- **IT-Sicherheitsbewusstsein**: Der Begriff IT-Sicherheitsbewusstsein bezeichnet den Grad, bis zum welchem Unternehmensmitglieder die Bedeutung der IT-Sicherheit, das angeforderte Niveau an IT-Sicherheit sowie ihre individuellen, IT-sicherheitsrelevanten Verantwortlichkeiten im Unternehmen verstehen (vgl. ISF 2007, S. SM2.4). Mangelndes IT-Sicherheitsbewusstsein führt zu hohen IT-Sicherheitsrisiken, denen durch geeignete IT-Sicherheitsprogramme zu begegnen ist. Das IT-Sicherheitsbewusstsein wird somit als eine Vorstufe zur IT-Sicherheitskultur betrachtet.
- **IT-Sicherheitsschulung und -ausbildung**: Schulungen und Ausbildungen im Bereich der IT-Sicherheit gehören zu den IT-Sicherheitsmaßnahmen mit dem größten Nutzen. Sie schaffen bei den Nutzern das notwendige Wissen, um Bedrohungen für die IT-Sicherheit zu erkennen und IT-Sicherheitsmaßnahmen gegen diese zu ergreifen. IT-Sicherheitsschulungen und -ausbildungen sollen laufend durchgeführt werden, da sich die Rahmenbedingungen für die IT-Sicherheit stätig ändern.

- **Analyse und Bewertung von IT-Sicherheitsrisiken**: Die Analyse und Bewertung von Risiken helfen den Unternehmensmitgliedern, ein Verständnis für die möglichen Schäden infolge von IT-Sicherheitsvorfällen zu bekommen und bewirken dadurch Motivation für die Auseinandersetzung mit der Problematik und der Entwicklung einer IT-Sicherheitskultur.

Aufgrund der vielfältigen Einflussfaktoren auf die IT-Sicherheit insgesamt und auf die IT-Sicherheitskultur im Spezialfall muss die IT-Sicherheitskultur fortlaufend analysiert und an veränderte Rahmenbedingungen angepasst werden. Eine solche fortlaufende Analyse und Anpassung kann bspw. anhand des Deming-Zyklus vorgenommen werden (vgl. Abbildung 7).

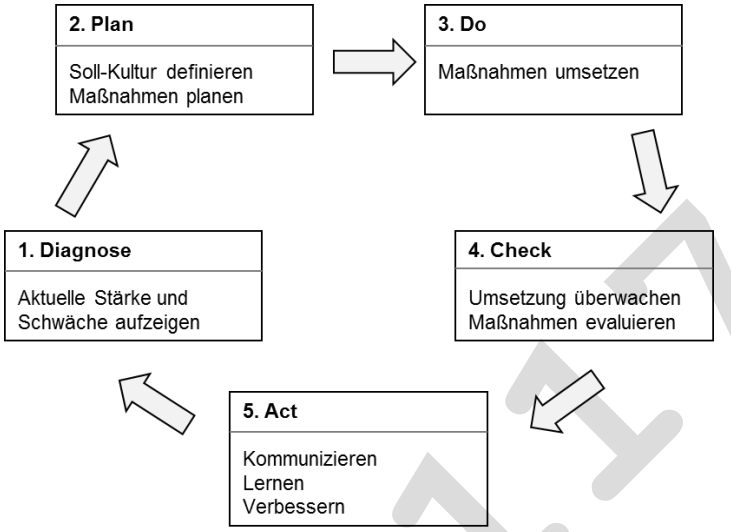

Abbildung 7: Managementprozess der IT-Sicherheitskultur
Quelle: In Anlehnung an Schlienger 2007

Managementprozess der IT-Sicherheitskultur

Der Deming-Zyklus wurde von Schlienger (2007) auf den Bereich der IT-Sicherheitskultur übertragen, um ihr Management als zyklischen Prozess abzubilden. Er beinhaltet folgende Schritte:

1) **Diagnose**: Im ersten Schritt stehen die Untersuchung der Ist-Situation und die Identifikation von Stärken und Schwächen der IT-Sicherheitskultur im Vordergrund. Für die Durchführung dieses Schritts soll eine Kombination aus mehreren Methoden, wie z. B. Analyse der IT-Sicherheitsrichtlinie, Befragungen und Interviews, Beobachtung und Messung von Verhaltensmustern, verwendet werden. Ziel ist es, Informationen über die offiziellen Werte und Verhaltensnormen sowie über das tatsächliche Wissen und gelebte Verhaltensweisen zu bekommen. Die Ergebnisse dieses Schritts ermöglichen die gezielte Anpassung bzw. Weiterentwicklung der IT-Sicherheitskultur in den nächsten Schritten.
2) **Plan**: Im zweiten Schritt wird zunächst eine Soll-IT-Sicherheitskultur definiert. Dabei wird entschieden, ob die bestehende IT-Sicherheitskultur belassen, leicht oder radikal verändert werden soll. Daran anschließend werden, wenn notwendig, Maßnahmen zur Veränderung der IT-Sicherheitskultur erarbeitet und priorisiert. Beispiele für Maßnahmen in

diesem Bereich sind Aufbau eines Dokumentensystems, Einbeziehung der oberen Führungsebene, Schulung und Ausbildung, Sensibilisierungskampagne.

3) **Do**: Im dritten Schritt erfolgt die Umsetzung der geplanten Maßnahmen im Rahmen von Projekten. Eine aktive Kommunikation und Bekanntmachung der Maßnahmen sowie eine durchgehende Unterstützung durch die obere Führungsebene sind in diesem Schritt äußerst wichtig.

4) **Check**: Im diesem Schritt wird die Umsetzung der Maßnahmen überwacht und die gewünschte Zielerreichung durch einen Vergleich der „alten“ und „neuen“ IT-Sicherheitskultur überprüft. Für die Kontrolle in diesem Schritt sind die gleichen Methoden wie bei der Diagnose einzusetzen. Ziel dieses Schritts ist es, die Effektivität der Maßnahmen und ihrer Umsetzung zu ermitteln.

5) **Act**: Der letzte Schritt des Managementprozesses dient einerseits der Kommunikation der erreichten Ziele sowie des Lernens aus den gemachten Erfahrungen. Andererseits soll er dazu beitragen, „[...] kurzfristig korrektive Maßnahmen zu ergreifen und die eingesetzten Methoden [...] zu verbessern“ (Schlienger 2007, S. 490).

Die Entwicklung und das Management der IT-Sicherheitskultur sind anspruchsvolle Aufgaben, welche angesichts der stetig steigenden Bedeutung sowie Komplexität der IT und der zentralen Rolle des menschlichen Faktors für die Erreichung der gewünschten IT-Sicherheitsziele im Rahmen des ITSM von allen Unternehmen unbedingt wahrzunehmen sind.

6 Zusammenfassung

Die IT gewinnt zunehmend an Bedeutung für die Zielerreichung von Unternehmen. Ihr störungsfreier Betrieb ist somit von hoher Priorität. Es wird jedoch immer schwieriger, ihn zu garantieren. Das liegt in der wachsenden Komplexität der IT-Systeme und -Lösungen sowie der Vernetzung von Unternehmen und Menschen. Hinzu kommt die Verbreitung von internetbasierten Diensten, wie z. B. das Cloud Computing oder die Nutzung (privater) mobiler Endgeräte, wie Smartphones und Tablets, für berufliche Zwecke, welche die Verwundbarkeit der IT weiter erhöhen. Aufgrund ihrer Wichtigkeit wird die IT immer häufiger gezielt als Angriffspunkt für z. B. Wirtschaftsspionage oder -sabotage ausgenutzt und die durch Angriffe angerichteten Schäden werden immer bedeutender. Aus diesen Gründen ist für Unternehmen die Auseinandersetzung mit dem Thema IT-Sicherheit unabdingbar.

Diese KE beschäftigte sich daher mit dem ITSM als unverzichtbarer Bestandteil des Informationsmanagements. Grundlegendes Ziel der Unternehmen in diesem Bereich ist es, ein geeignetes Niveau an IT-Sicherheit herzustellen, laufend zu überprüfen und aufrechtzuerhalten. Um dieses Ziel zu erreichen, ist es notwendig eine Vielzahl von strategischen, taktischen und operativen Aufgaben zu erfüllen, von denen hier einige grundlegende vorgestellt wurden.

In Kapitel 2 wurden zunächst die wichtigsten Begriffe und Ziele im Bereich des ITSM definiert sowie seine Aufgaben grob beschrieben. In Kapitel 3 wurden dann die IT-Sicherheitsstrategieentwicklung und -steuerung behandelt. Die IT-Sicherheitsstrategie beinhaltet u. a. die IT-Sicherheitsziele und -richtlinien und gibt dadurch die Richtung für die weitere Realisierung eines unternehmensspezifischen ITSM vor. Die IT-Sicherheitsstrategie ist an die Unternehmens- und Informatikstrategie anzulehnen, da ihre Umsetzung sonst zu Aktivitäten führen kann, die z. B. in Konflikt mit der Realisierung bestimmter Geschäftsprozesse oder zu Einschränkungen in der Funktionalität der IT führen kann. Die IT-Sicherheitsstrategie wird in einem IT-Sicherheitskonzept konkretisiert. Die Erarbeitung eines solchen Konzepts stellt die wichtigste taktische Aufgabe des ITSM dar und kann anhand von verschiedenen Verfahren, welche in nationalen und internationalen Normen und Standards enthalten sind, vorgenommen werden. Ein Verfahren, das an die Vorgehensweise des BSI angelehnt ist, wurde in Kapitel 4 vorgestellt. In diesem Zusammenhang wurden beispielhaft Schwachstellen und Bedrohungen für die IT-Sicherheit aufgezeigt. Die Erarbeitung eines IT-Sicherheitskonzepts ist keine einmalige Aufgabe. Sie ist vielmehr als ein laufender Prozess zu betrachten. Da das IT-Sicherheitskonzept die interne Unternehmenssituation, das spezifische Unternehmensumfeld sowie die aktuelle Situation und die Entwicklungen im Bereich der IT und der IT-Sicherheit, welche sich laufend verändern, berücksichtigt, ist eine stetige Anpassung des Konzepts erforderlich. In Kapitel 5 wurden verschiedene Möglichkeiten für die Klassifikation von IT-Sicherheitsmaßnahmen vorgestellt sowie einige Beispiele für IT-Sicherheitsmaßnahmen gegeben. Die IT-Sicherheitsmaßnahmen, welche von einem Unternehmen konkret umzusetzen sind, ergeben sich aus dem IT-

Sicherheitskonzept und unterliegen demzufolge ebenfalls einer laufenden Überprüfung und Anpassung. Anschließend wurde erläutert, wie eine IT-Sicherheitsorganisation in die Unternehmensorganisation eingebettet werden kann und einige der wichtigsten Rollen und Verantwortlichkeiten im Bereich des ITSM beschrieben. Zuletzt wurde die Bedeutung der IT-Sicherheitskultur erklärt und anhand eines Modells aufgezeigt, wie eine IT-Sicherheitskultur entwickelt und an Veränderungen laufend angepasst werden kann.

Übungsaufgaben

1. Was ist das Ziel des ITSM?
2. Nennen und erläutern Sie drei IT-Sicherheitsziele.
3. Welche sind die strategischen Aufgaben des ITSM?
4. Wozu dient ein IT-Sicherheitskonzept?
5. Nennen Sie die Ziele und die Schritte der Strukturanalyse im Kontext des ITSM.
6. Erklären Sie, was im Kontext des ITSM unter einer Schutzbedarfsanalyse zu verstehen ist.
7. Erläutern Sie den Zusammenhang zwischen den Begriffen Schwachstelle, Bedrohung und Risiko.
8. Geben Sie drei Beispiele für Schwachstellen der Kategorie Organisation.
9. Erläutern Sie die Rolle des Geschäftsführers im Rahmen des ITSM.
10. Nennen und beschreiben Sie drei Faktoren, von welchen die Schaffung einer effektiven IT-Sicherheitskultur im Unternehmen beeinflusst wird.
11. Nennen Sie Maßnahmen, mit denen das IT-Sicherheitsbewusstsein innerhalb eines Unternehmens verbessert werden kann.

Anhang

IT-Sicherheitsrichtlinie der Universität Göttingen
Quelle: Entnommen aus Georg-August-Universität Göttingen 2007

Präambel

Der Hochschulbetrieb erfordert in zunehmendem Maß die Integration von Verfahren und Abläufen, die sich auf die Möglichkeiten der Kommunikations- und Informationstechnik (IT) stützen. Funktionierende und sichere IT-Prozesse sind daher eine zentrale Grundlage für die Leistungsfähigkeit der Universität und ihrer Verwaltung auf den Gebieten der Forschung, Lehre, Krankenversorgung, der Dienstleistungen im öffentlichen Gesundheitswesen, der Aus-, Fort- und Weiterbildung sowie des Technologietransfers.

Unter diesen Bedingungen kommt der „Sicherheit in der Informationstechnik“ (IT-Sicherheit) eine grundsätzliche und strategische Bedeutung zu, die die Entwicklung und Umsetzung einer einheitlichen hochschulweiten Rahmenrichtlinie der IT-Sicherheit für die Hochschule erforderlich macht. Nicht zuletzt sind sichere IT-Prozesse eine Grundvoraussetzung für alle Datenschutzmaßnahmen, die vor allem bei der Verarbeitung personenbezogener Daten umzusetzen sind.

Dieses kann wegen der komplexen Materie, der sich schnell weiter entwickelnden technischen Möglichkeiten und der begrenzten finanziellen und personellen Möglichkeiten nur in einem kontinuierlichen IT-Sicherheitsprozess erfolgen. Die Entwicklung und Fortschreibung dieses IT-Sicherheitsprozesses muss sich einerseits an den Aufgaben und Rechten der Hochschule orientieren, andererseits ist sie nur über einen kontinuierlichen IT-Sicherheitsprozesses innerhalb geregelter Verantwortungsstrukturen zu erzielen.

Ziel der Organisationsrichtlinie zur IT-Sicherheit ist es nicht nur, die existierenden rechtlichen Auflagen zu erfüllen, sondern primär die in der Hochschule verarbeiteten, übertragenen und gespeicherten Daten und Anwendungen zu schützen sowie die Hochschule - soweit möglich - vor materiellen und immateriellen Schäden zu bewahren.

Ausdrücklich wird darauf hingewiesen, dass die erfolgreiche Umsetzung des IT-Sicherheitsprozesses die Unterstützung aller Mitarbeiterinnen und Mitarbeiter sowie aller Angehörigen der Universität und der Universitätsmedizin voraussetzt

1 Gegenstand der Richtlinie

Die Richtlinie legt die Zuständigkeiten, die Verantwortungsstrukturen, die Aufgabenzuordnung und die Zusammenarbeit der Beteiligten im hochschulweiten IT-Sicherheitsprozess sowie dessen Finanzierung fest.

2 Geltungsbereich

Diese Richtlinie gilt für alle Einrichtungen der Universität und der Universitätsmedizin, für deren gesamte IT-Infrastruktur einschließlich der betriebenen IT-Systeme sowie die Gesamtheit der Benutzer.

3 IT-Sicherheitskonzept

(1) Das IT-Sicherheitskonzept der Universität basiert auf

- dieser Richtlinie zur IT-Sicherheit,
- der in den Amtlichen Mitteilungen veröffentlichten IT-Sicherheitsrahmenrichtlinie der Universität einschließlich der Universitätsmedizin,
- der Nutzungsregelung für die IT-Infrastruktur der Universitätsmedizin und
- Einzelregelungen, auf die in der IT-Sicherheitsrahmenrichtlinie verwiesen wird.

(2) Das Sicherheitskonzept orientiert sich am Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik (BSI).

4 Organisationsstruktur des IT-Sicherheitsprozesses

(1) Die Verantwortung für die IT-Sicherheit und den IT-Sicherheitsprozess liegt beim Präsidium für die Universität und beim Vorstand für die Universitätsmedizin.

(2) Die Koordinierung des IT-Sicherheitsprozesses obliegt der Arbeitsgruppe „IT-Strategie“ des Präsidiums der Universität und des Vorstands der Universitätsmedizin in ihrer Funktion als Chief Information Office (CIO) der Universität und der Universitätsmedizin.

In der Arbeitsgruppe „IT-Strategie“ sind vertreten:

- das Präsidiumsmitglied für IT,
- das Präsidiumsmitglied für Bibliothekswesen,
- das Mitglied des Vorstands für Wirtschaftsführung und Administration und
- weitere vom Präsidium und Vorstand benannte Mitglieder.

(3) Die Arbeitsgruppe „IT-Strategie“ setzt die Arbeitsgruppe „IT-Sicherheit“ ein.

Die Arbeitsgruppe „IT-Sicherheit“ wird gebildet aus

- je einem Vertreter der Rechenzentren (GWDG und G3-7) sowie einem Vertreter der NSUB Göttingen,
- den Datenschutzbeauftragten der Universität und der Universitätsmedizin und
- weiteren von der Arbeitsgruppe „IT-Strategie“ benannten Mitgliedern.

(4) Die Leiter der Einrichtungen sind für die Umsetzung von IT-Sicherheit in ihren Einrichtungen verantwortlich. Den Leitern der Einrichtungen wird empfohlen, der Arbeitsgruppe „IT-Sicherheit“ IT-Beauftragte für ihre Einrichtungen zu benennen und diese mit der Umsetzung des IT-Sicherheitsprozesses innerhalb der Einrichtung zu beauftragen. Werden keine IT-Beauftragten benannt, so ist die Funktion des IT-Beauftragten vom Leiter der Einrichtung wahrzunehmen.

(5) Mehrere Einrichtungen können einen gemeinsamen IT-Beauftragten benennen. Die Funktion des IT-Beauftragten kann dabei auch auf der übergeordneten Organisationsebene angesiedelt werden.

5 Aufgaben der Beteiligten

(1) Die Arbeitsgruppe „IT-Strategie“ koordiniert den IT-Sicherheitsprozess.

(2) Die Arbeitsgruppen „IT-Strategie“ und „IT-Sicherheit“ beraten das Präsidium der Universität und den Vorstand der Universitätsmedizin in Fragen der IT-Sicherheit.

(3) Die Arbeitsgruppe „IT-Sicherheit“ erarbeitet und überarbeitet Vorlagen für die hochschulinternen technischen Standards, Richtlinien und Notfallpläne zur IT-Sicherheit, die durch das Präsidium der Universität und den Vorstand der Universitätsmedizin in Kraft gesetzt werden, und unterstützt die Arbeitsgruppe „IT-Strategie“ bei der Umsetzung und Überwachung des IT-Sicherheitsprozesses. Die Arbeitsgruppe „IT-Sicherheit“ koordiniert die Schulung und Weiterbildung der IT-Beauftragten und unterstützt diese bei der Richtlinienumsetzung. Die Arbeitsgruppe „IT-Sicherheit“ erstellt in Abstimmung mit der Arbeitsgruppe „IT-Strategie“ jährlich einen IT-Sicherheitsbericht für das Präsidium der Universität und den Vorstand der Universitätsmedizin.

(4) Die IT-Beauftragten überwachen kontinuierlich die Umsetzung des IT-Sicherheitsprozesses in ihren jeweiligen Verantwortungsbereichen. Dafür müssen sie von der Leitung der jeweiligen Einrichtung mit entsprechenden Kompetenzen ausgestattet werden. Sie informieren regelmäßig sowohl die Leitung ihrer Einrichtung als auch die Arbeitsgruppe „IT-Sicherheit“ über den Stand der Umsetzung. Sie melden sicherheitsrelevante Vorfälle unverzüglich der Arbeitsgruppe „IT-Sicherheit“ und der Leitung der Einrichtung. Sie sind verpflichtet sich auf dem Gebiet der IT-Sicherheit weiterzubilden und ihr Wissen auf dem aktuellen Stand zu halten. Sie werden hierbei von der Leitung der jeweiligen Einrichtung unterstützt.

(5) Alle Angehörigen und Mitarbeiter der Hochschule sind verpflichtet, sicherheitsrelevante Vorfälle unverzüglich dem zuständigen IT-Beauftragten zu melden.

(6) Die Rechenzentren sind für die system-, netz- und betriebstechnischen Aspekte der IT-Sicherheit verantwortlich. Sie arbeiten eng mit den Arbeitsgruppen „IT-Strategie“ und „IT-Sicherheit“ zusammen.

6 Gefahrenintervention

(1) Um eine Gefahr für die IT-Sicherheit abzuwehren, treffen die Rechenzentren (GWDG bzw. G3-7) die erforderlichen Maßnahmen; diese können auch die Sperrung von Netzanschlüssen und Benutzerkonten (auch ohne vorherige Benachrichtigung der Betroffenen) beinhalten. Der zuständige IT-Beauftragte sowie die Arbeitsgruppe „IT-Sicherheit“ sind unverzüglich zu informieren. Die Aufhebung der Gefahrenabwehrmaßnahmen durch die Rechenzentren erfolgt nach der Durchführung hinreichender IT-Sicherheitsmaßnahmen in Abstimmung mit der Arbeitsgruppe „IT-Sicherheit“; der zuständige IT-Beauftragte ist zu informieren.

(2) Wenn es zur Abwehr einer akuten Gefahr für die IT-Sicherheit erforderlich ist, treffen die IT-Beauftragten die erforderlichen Maßnahmen; dies kann auch die Stilllegung von IT-Systemen in ihrem Verantwortungsbereich bedeuten. Die Ar-

beitsgruppe „IT-Sicherheit“ und die Leitung der Einrichtung sind unverzüglich zu informieren. Die Aufhebung der Gefahrenabwehrmaßnahmen durch die IT-Beauftragten erfolgt nach Durchführung hinreichender IT-Sicherheitsmaßnahmen in Abstimmung mit der Arbeitsgruppe „IT-Sicherheit“.

7 Finanzierung

Die personellen und finanziellen Ressourcen aller zentralen und dezentralen IT Sicherheitsmaßnahmen sind aus den Budgetmitteln der IT Dienstleister, Zentralverwaltung, zentralen Einrichtungen und Fakultäten zu finanzieren. Hierunter fallen auch zentral und dezentral angebotene Schulungsmaßnahmen für IT Beauftragte und Benutzer.

8 Inkrafttreten

Diese Richtlinie wird vom Präsidium der Universität und vom Vorstand der Universitätsmedizin verabschiedet. Sie tritt am Tag nach ihrer Bekanntmachung in den Amtlichen Mitteilungen der Universität in Kraft.

Lösungen zu den Übungsaufgaben

1. Was ist das Ziel des ITSM?

Ziel des ITSM ist es, ein angemessenes Niveau an IT-Sicherheit herzustellen, laufend zu überprüfen und sicherzustellen. Dabei wird das angemessene IT-Sicherheitsniveau anhand der IT-Sicherheitsziele ermitteln. Deswegen wird als Ziel des ITSM auch die Erreichung der gesetzten bzw. gewünschten IT-Sicherheitsziele genannt.

2. Nennen und erläutern Sie drei IT-Sicherheitsziele.

1) Das Sicherheitsziel der Vertraulichkeit bezieht sich auf Daten und Informationen. Sie stellt sicher, dass nur Berechtigte (diese können sowohl Menschen als auch Maschinen sein) auf schutzwürdige Daten oder Informationen zugreifen und diese lesen können. Die Vertraulichkeit ist vor allem im Rahmen der Gewährung des Datenschutzes und des Schutzes von Unternehmensgeheimnissen ein grundlegendes Ziel.
2) Das Sicherheitsziel der Verfügbarkeit bezieht sich sowohl auf Daten und Informationen, als auch auf Systeme und bezeichnet die Gewährleistung des uneingeschränkten Zugriffs auf und Nutzung von Daten oder Systemen durch Berechtigte.
3) Die Integrität bezieht sich auf Daten und Informationen und bezeichnet den Schutz dieser vor unautorisierter und unbemerkter Manipulation. Sie stellt die Echtheit und Verbindlichkeit von Daten und Informationen sicher.

3. Welche sind die strategischen Aufgaben des ITSM?

Die strategischen Aufgaben des ITSM sind die Entwicklung und Steuerung der IT-Sicherheitsstrategie. Die Entwicklung der IT-Sicherheitsstrategie beinhaltet die Formulierung einer unternehmensspezifischen IT-Sicherheitsrichtlinie, die Erarbeitung von IT-Sicherheitszielen in Anlehnung an die Gesamtunternehmensziele, die Festlegung eines groben Plans für die Erreichung der IT-Sicherheitsziele sowie die Definition von Kennzahlen zur Steuerung der Zielerreichung.

4. Wozu dient ein IT-Sicherheitskonzept?

Ein IT-Sicherheitskonzept dient dazu, die festgelegte IT-Sicherheitsstrategie zu konkretisieren. Es beinhaltet die Beschreibung geplanter Vorgehensweisen, um die gewünschten IT-Sicherheitsziele zu erreichen.

5. Nennen Sie die Ziele und die Schritte der Strukturanalyse im Kontext des ITSM.

Ziel der Strukturanalyse ist es, relevante Elemente des Informationsverbunds sowie die Beziehungen zwischen ihnen zu erfassen.

Die Schritte der Strukturanalyse sind:
1) Erhebung von Informationen und Anwendungen
2) Netzplanerhebung

3) Erhebung der Hardwaresysteme
4) Erfassung der Räume

6. Erklären Sie, was im Kontext des ITSM unter einer Schutzbedarfsanalyse zu verstehen ist.

Im Kontext des ITSM ist die Schutzbedarfsanalyse ein Schritt zur Entwicklung eines IT-Sicherheitskonzepts. Sie dient dazu, den Schutzbedarf der Elemente eines Informationsverbunds zu ermitteln. Der Informationsverbund ist der Unternehmensbereich (kann auch das gesamte Unternehmen sein), für welchen ein IT-Sicherheitskonzept entwickelt wird. Auf der Basis der Ergebnisse der Schutzbedarfsanalyse ist es möglich, angemessene IT-Sicherheitsmaßnahmen für die einzelnen Elemente des Informationsverbunds zu definieren.

7. Erläutern Sie den Zusammenhang zwischen den Begriffen Schwachstelle, Bedrohung und Risiko.

Eine Bedrohung ist jemand oder etwas (Ereignis), der bzw. das gezielt oder unabsichtlich eine Schwachstelle in einem System ausnutzt, um im System Schaden zu verursachen. Die Wahrscheinlichkeit, dass eine Bedrohung eine Schwachstelle ausnutzt, und der infolge der Ausnutzung potentiell entstandene Schaden werden Risiko genannt.

8. Geben Sie drei Beispiele für Schwachstellen der Kategorie Organisation.

1) Fehlende IT-Sicherheitsrichtlinie
2) Keine angemessene Zuweisung von IT-Sicherheitsverantwortlichkeiten
3) Keine festgelegten disziplinarischen Folgen bei IT-Sicherheitsvorfällen

9. Erläutern Sie die Rolle des Geschäftsführers im Rahmen des ITSM.

Ihm obliegt die Gesamtverantwortung für die IT-Sicherheit im Unternehmen. Zu seinen Aufgaben in diesem Bereich gehört z. B. zu gewährleisten, dass die IT-Sicherheitsmanagementprozesse in den strategischen und operativen Unternehmensprozessen integriert sind und dass die anderen Verantwortlichen ihre IT-Sicherheitsmanagementaufgaben entsprechend erledigen. Der Geschäftsführer muss außerdem Sorge tragen, dass das Unternehmen über ausreichend ausgebildetes Personal verfügt, das den jeweiligen IT-Sicherheitsanforderungen sowie relevanten gesetzlichen Vorschriften und Normen entspricht. Weiterhin ist er für das Schaffen eines Bewusstseins für das Thema IT-Sicherheit im Unternehmen und die aktive Unterstützung der anderen Bereiche bei der Kontrolle und Verbesserung von IT-Sicherheitsprogrammen und -aktivitäten zuständig.

10. Nennen und beschreiben Sie drei Faktoren, von welchen die Schaffung einer effektiven IT-Sicherheitskultur im Unternehmen beeinflusst wird.

1) Unterstützung durch die oberste Führungsebene: Dieser Faktor bezieht sich einerseits auf den Grad, bis zum welchen die oberste Führungsebene die

Wichtigkeit des ITSM versteht und sich an den IT-Sicherheitsaktivitäten beteiligt, und andererseits auf ihr Engagement bei der Entwicklung und Etablierung der IT-Sicherheitskultur im Unternehmen. Dabei soll sie Programme und Aktivitäten zur Steigerung des IT-Sicherheitsbewusstseins fördern, sowie auf die Aktualität, Eignung und Einhaltung der IT-Sicherheitsrichtlinie bestehen.

2) Etablierung einer effektiven IT-Sicherheitsrichtlinie: Die IT-Sicherheitsrichtlinie ist zentral für das gesamte IT-Sicherheitsprogramm jedes Unternehmens und eine Voraussetzung für die Entwicklung der IT-Sicherheitskultur. Denn sie liefert Definitionen für die Rollen und Verantwortlichkeiten aller Stakeholder sowie dafür, was ein IT-sicherheitskonformes Verhalten ist.

3) IT-Sicherheitsbewusstsein: Der Begriff IT-Sicherheitsbewusstsein bezeichnet den Grad, bis zum welchem Unternehmensmitglieder die Bedeutung der IT-Sicherheit, das angeforderte Niveau an IT-Sicherheit sowie ihre individuellen, IT-sicherheitsrelevanten Verantwortlichkeiten im Unternehmen verstehen. Mangelndes IT-Sicherheitsbewusstsein führt zu hohen IT-Sicherheitsrisiken, denen durch geeignete IT-Sicherheitsprogramme zu begegnen ist. Das IT-Sicherheitsbewusstsein wird somit als eine Vorstufe zur IT-Sicherheitskultur betrachtet.

11. Nennen Sie Maßnahmen, mit denen das IT-Sicherheitsbewusstsein innerhalb eines Unternehmens verbessert werden kann.

- Durchführung von Sicherheitsschulungen für Mitarbeiter
- Durchführung verstärkter Sicherheitskontrollen
- Prämierung von sicherheitsbewusstem Verhalten
- Kopplung von Stellenbesetzungen an eine bestimmte Sicherheitsqualifikation
- Einsatz von (Computer-)Spielen zum Thema IT-Sicherheit
- Verwendung und Verteilung von humoristischen Mitteln (z. B. Witze, Karikaturen) zum Thema IT-Sicherheit