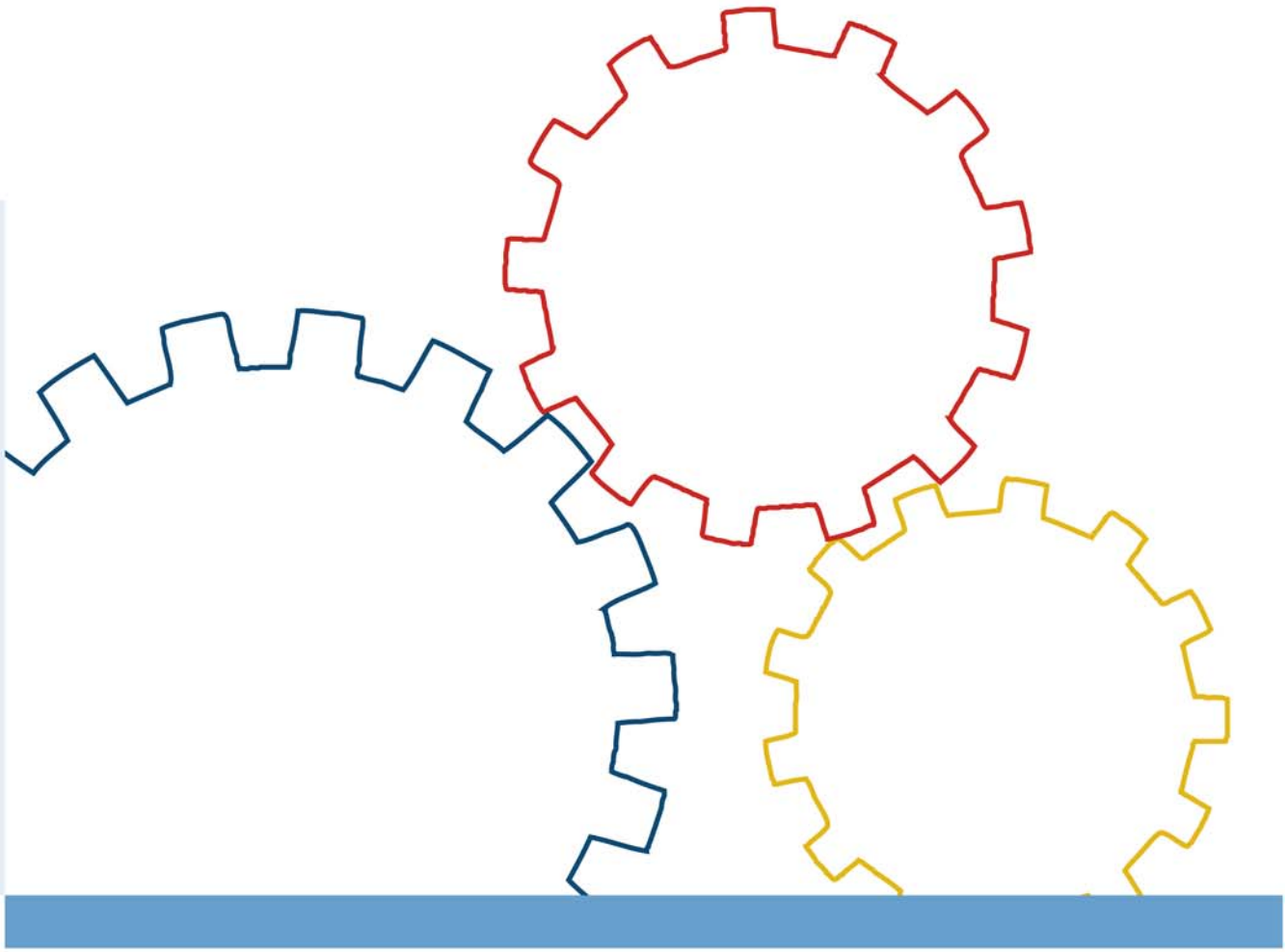
Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Standard 100-2

IT-Grundschutz-Vorgehensweise



www.bsi.bund.de/gshb

Version 2.0

Inhaltsverzeichnis

1 Einleitung

1.1 Versionshistorie

Stand	Version	Änderungen
Dezember 2005	1.0	
Mai 2008	2.0	• Stärkere Betonung der Informationssicherheit statt IT-Sicherheit, daher auch verschiedene Begriffe angepasst • Ergänzung von Datenschutz-Aspekten • Anpassungen an Fortschreibung der ISO-Standards • Verbesserte Gliederung • Bei der Strukturanalyse wurde die Reihenfolge der Erfassung geändert. • Klare Trennung der Aufgaben im Sicherheitsprozess in vorbereitende Aufgaben in Kapitel 3 und Umsetzung in Kapiteln 4 bis 6

1.2 Zielsetzung

Das BSI hat mit der Vorgehensweise nach IT-Grundschutz eine Methodik für ein effektives Management der Informationssicherheit entwickelt, die einfach auf die Gegebenheiten einer konkreten Institution angepasst werden kann.

Die in den nächsten Kapiteln beschriebene Methodik baut auf den BSI-Standard 100-1 "Managementsysteme für die Informationssicherheit (ISMS)" (siehe [BSI1]) auf und erläutert die dort vorgestellte Vorgehensweise des IT-Grundschutzes. Ein Managementsystem für die Informationssicherheit (ISMS) ist das geplante und organisierte Vorgehen, um ein angemessenes Sicherheitsniveau für die Informationssicherheit zu erzielen und aufrechtzuerhalten. Zu diesem Zweck wird für jede einzelne Phase, die im BSI-Standard 100-1 beschrieben wird, die vom IT-Grundschutz vorgeschlagene Umsetzung explizit dargestellt.

Der IT-Grundschutz repräsentiert einen Standard für die Etablierung und Aufrechterhaltung eines angemessenen Schutzes aller Informationen einer Institution. Diese vom BSI seit 1994 eingeführte und weiterentwickelte Methode bietet sowohl eine Vorgehensweise für den Aufbau eines Managementsystems für Informationssicherheit als auch eine umfassende Basis für die Risikobewertung, die Überprüfung des vorhandenen Sicherheitsniveaus und die Implementierung der angemessenen Informationssicherheit.

Eines der wichtigsten Ziele des IT-Grundschutzes ist es, den Aufwand im Informationssicherheitsprozess zu reduzieren, indem bekannte Vorgehensweisen zur Verbesserung der Informationssicherheit gebündelt und zur Wiederverwendung angeboten werden. So enthalten die IT-Grundschutz-Kataloge Standard-Gefährdungen und -Sicherheitsmaßnahmen für typische Geschäftsprozesse und IT-Systeme, die nach Bedarf in der eigenen Institution eingesetzt werden können. Durch die geeignete Anwendung der vom IT-Grundschutz empfohlenen organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen wird ein Sicherheitsniveau für die betrachteten Geschäftsprozesse erreicht, das für den normalen Schutzbedarf angemessen und ausreichend ist, um geschäftsrelevante Informationen zu schützen. Darüber hinaus bilden die Maßnahmen der IT-Grundschutz-Kataloge nicht nur eine Basis für hochschutzbedürftige IT-Systeme und Anwendungen, sondern liefern an vielen Stellen bereits höherwertige Sicherheit.

1.3 Adressatenkreis

Dieses Dokument richtet sich primär an Sicherheitsverantwortliche, -beauftragte, -experten, -berater und alle Interessierte, die mit dem Management von Informationssicherheit betraut sind. Es bietet aber auch eine sinnvolle Grundlage für IT-Verantwortliche, Führungskräfte und Projektmanager, die dafür Sorge tragen, dass Sicherheitsaspekte in ihrer Institution bzw. in ihren Projekten ausreichend berücksichtigt werden.

Die Vorgehensweise des IT-Grundschutzes richtet sich an Institutionen aller Größen und Arten, die eine kosteneffektive und zielführende Methode zum Aufbau und zur Umsetzung der für sie angemessenen Informationssicherheit benötigen. Der Begriff „Institution“ wird in diesem Zusammenhang für Unternehmen, Behörden und sonstige öffentliche oder private Organisationen verwendet. IT-Grundschutz kann hierbei sowohl von kleinen als auch großen Institutionen eingesetzt werden. Dabei sollte aber beachtet werden, dass alle Empfehlungen unter dem Kontext der jeweiligen Institution betrachtet und angemessen umgesetzt werden sollten.

1.4 Anwendungsweise

Im BSI-Standard 100-1 "Managementsysteme für Informationssicherheit" wird beschrieben, mit welchen Methoden Informationssicherheit in einer Institution generell initiiert und gesteuert werden kann. Die Vorgehensweise nach IT-Grundschutz bietet nun konkrete Hilfestellungen, wie ein Managementsystem für die Informationssicherheit Schritt für Schritt eingeführt werden kann. Es wird dabei auf die einzelnen Phasen dieses Prozesses eingegangen und es werden vorbildliche Lösungen aus der Praxis, so genannte "Best Practice"-Ansätze, zur Bewältigung der Aufgaben vorgestellt.

Diese Vorgehensweise bietet ein umfangreiches Gerüst für ein ISMS und muss nur auf die individuellen Rahmenbedingungen einer Institution entsprechend angepasst werden, damit ein geeignetes Managementsystem für die Informationssicherheit aufgebaut werden kann. Für die erfolgreiche Etablierung eines kontinuierlichen und effektiven Prozesses für Informationssicherheit müssen eine ganze Reihe von Aktionen durchgeführt werden. Hierfür bieten die IT-Grundschutz-Vorgehensweise und die IT-Grundschutz-Kataloge Hinweise zur Methodik und praktische Umsetzungshilfen.

Des Weiteren bietet die IT-Grundschutz-Vorgehensweise einen Standard, nach dem eine Institution die Qualität des eigenen ISMS mit Hilfe eines Zertifikates publik machen kann, sowie ein Kriterium, um sich über den Reifegrad der ISMS anderer Institutionen informieren zu können.

Eine Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz kann auch als Sicherheitsanforderung für mögliche Kooperationspartner verwendet werden, um das erforderliche Niveau an Informationssicherheit bei dem Partner zu definieren. Auch wenn als Grundlage für das ISMS eine andere Methodik angewendet wird, ist es trotzdem möglich, von der IT-Grundschutz-Vorgehensweise zu profitieren. So bietet der IT-Grundschutz auch Lösungsansätze für verschiedene, die Informationssicherheit betreffende Aufgabenstellungen, beispielsweise für die Erstellung von Konzepten oder die Durchführung von Revisionen und Zertifizierungen im Bereich Informationssicherheit. Abhängig von der vorliegenden Aufgabenstellung sind dabei unterschiedliche Anwendungsweisen des IT-Grundschutzes zweckmäßig, indem beispielsweise einzelne Aspekte davon genutzt werden. Je nach Anwendungsbereich bilden bereits einzelne Bausteine, die Gefährdungs- und Maßnahmen-Kataloge und weitere Hilfsmittel, die der IT-Grundschutz zur Verfügung stellt, hilfreiche Grundlagen für die Arbeit des Sicherheitsmanagements.

Kapitel 2 gibt eine Übersicht der wichtigen Schritte für die Einführung eines ISMS und der Vorgehensweise für die Erstellung einer Sicherheitskonzeption.

In Kapitel 3 wird beschrieben, wie die grundlegende Phase der Initiierung des Informationssicherheitsprozesses aussehen kann und welche Organisationsstrukturen dafür sinnvoll sind. Es wird außerdem ein systematischer Weg aufgezeigt, wie ein funktionierendes Sicherheitsmanagement eingerichtet und im laufenden Betrieb weiterentwickelt werden kann.

Kapitel 4 beschreibt die IT-Grundschutz-Vorgehensweise zur Erstellung einer Sicherheitskonzeption. Dabei wird aufgezeigt, wie zunächst die Grundinformationen über einen Informationsverbund erhoben werden und diese durch Gruppenbildung reduziert werden können. Anschließend muss ausgehend von den Geschäftsprozessen der Schutzbedarf für Anwendungen, IT-Systeme, Kommunikationsverbindungen und Räume festgestellt werden. Aus den Empfehlungen der IT-Grundschutz-Kataloge müssen ferner die für den jeweiligen Informationsverbund passenden Bausteine und Maßnahmen ausgewählt, also die Modellierung nach IT-Grundschutz durchgeführt werden. Vor der Realisierung von Sicherheitsmaßnahmen müssen vorhandene und zusätzliche Sicherheitsmaßnahmen, die beispielsweise durch die ergänzende Sicherheitsanalyse und die daran angeschlossene Risikoanalyse auf der Basis von IT-Grundschutz gemäß BSI-Standard 100-3 (siehe [BSI3]) erkannt und definiert wurden, in die IT-Grundschutz-Vorgehensweise integriert werden.

Wie die Umsetzung der erkannten und konsolidierten Sicherheitsmaßnahmen durchgeführt werden sollte, wird anschließend in Kapitel 5 beschrieben.

Die wesentliche Aufgabe eines ISMS ist es, die Aufrechterhaltung der Informationssicherheit zu gewährleisten. Dieses Thema wird im Kapitel 6 angegangen und ergänzend dazu wird die Möglichkeit dargestellt, das erreichte Sicherheitsniveau in Form einer Zertifizierung publik zu machen.

Die IT-Grundschutz-Vorgehensweise, aber vor allem die IT-Grundschutz-Kataloge werden regelmäßig erweitert und an aktuelle Entwicklungen angepasst. Durch den ständigen Erfahrungsaustausch mit Anwendern des IT-Grundschutzes ist eine bedarfsgerechte Weiterentwicklung möglich. Diese Bemühungen zielen letztlich darauf, aktuelle Empfehlungen zu typischen Sicherheitsproblemen aufzeigen zu können.

1.5 Literaturverzeichnis

[BSI1] Managementsysteme für Informationssicherheit (ISMS), BSI-Standard 100-1, Version 1.5, Mai 2008, www.bsi.bund.de

[BSI2] IT-Grundschutz-Vorgehensweise, BSI-Standard 100-2, Version 2.0, Mai 2008, www.bsi.bund.de

[BSI3] Risikoanalyse auf der Basis von IT-Grundschutz, BSI-Standard 100-3, Version 2.5, Mai 2008, www.bsi.bund.de

[GSK] IT-Grundschutz-Kataloge - Standard-Sicherheitsmaßnahmen, BSI, jährlich neu, http://www.bsi.bund.de/gshb

[SHB] IT-Sicherheitshandbuch - Handbuch für die sichere Anwendung der Informationstechnik, BSI, Version 1.0 - März 1992, Bundesdruckerei

[OECD] Organisation for Economic Co-operation and Development (OECD), Guidelines for the Security of Information Systems and Networks, 2002, www.oecd.org/sti/security-privacy

[ZERT] Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz - Prüfschema für ISO 27001-Audits, BSI, Version 1.2, März 2008, www.bsi.bund.de/gshb/zert

[ZERT2] Zertifizierungsschema für Auditteamleiter für ISO 27001-Audits auf der Basis von IT-Grundschutz, BSI, März 2008, www.bsi.bund.de/gshb/zert

[27000] ISO/IEC 27000 (3rd CD, 2008) "ISMS – Overview and vocabulary", ISO/IEC JTC1/SC27

[27001] ISO/IEC 27001:2005 "Information technology - Security techniques - Information security management systems requirements specification", ISO/IEC JTC1/SC27

[27002] ISO/IEC 27002:2005 "Information technology - Code of practice for information security management", ISO/IEC JTC1/SC27

[27005] ISO/IEC 27005 (2nd FCD, 2008) "Information security risk management", ISO/IEC JTC1/SC27

2 Informationssicherheitsmanagement mit IT-Grundschutz

Informationen sind ein wesentlicher Wert für Unternehmen und Behörden und müssen daher angemessen geschützt werden. Die meisten Informationen werden heutzutage zumindest teilweise mit Informationstechnik (IT) erstellt, gespeichert, transportiert oder weiterverarbeitet. Moderne Geschäftsprozesse sind heute in Wirtschaft und Verwaltung ohne IT-Unterstützung längst nicht mehr vorstellbar. Eine zuverlässig funktionierende Informationsverarbeitung ist für die Aufrechterhaltung des Betriebes unerlässlich. Unzureichend geschützte Informationen stellen einen häufig unterschätzten Risikofaktor dar, der für manche Institution existenzbedrohend sein kann. Dabei ist ein vernünftiger Informationsschutz ebenso wie eine Grundsicherung der IT schon mit verhältnismäßig geringen Mitteln zu erreichen.

Um zu einem bedarfsgerechten Sicherheitsniveau für alle Geschäftsprozesse, Informationen und auch der IT-Systeme einer Institution zu kommen, ist allerdings mehr als das bloße Anschaffen von Antivirensoftware, Firewalls oder Datensicherungssystemen notwendig. Ein ganzheitliches Konzept ist wichtig. Dazu gehört vor allem ein funktionierendes und in die Institution integriertes Sicherheitsmanagement. Informationssicherheitsmanagement (oder kurz IS-Management) ist jener Teil des allgemeinen Risikomanagements, der die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, Anwendungen und IT-Systemen gewährleisten soll. Dabei handelt es sich um einen kontinuierlichen Prozess, dessen Strategien und Konzepte ständig auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf fortzuschreiben sind.

Informationssicherheit ist nicht nur eine Frage der Technik, sondern hängt in erheblichem Maße von den organisatorischen und personellen Rahmenbedingungen ab. Die Vorgehensweise nach IT-Grundschutz und die IT-Grundschutz-Kataloge des BSI tragen dem seit langem Rechnung, indem sie sowohl technische als auch nicht-technische Standard-Sicherheitsmaßnahmen für typische Geschäftsbereiche, Anwendungen und IT-Systeme empfehlen. Im Vordergrund stehen dabei praxisnahe und handlungsorientierte Hinweise mit dem Ziel, die Einstiegshürde in den Sicherheitsprozess so niedrig wie möglich zu halten und hochkomplexe Vorgehensweisen zu vermeiden.

In der IT-Grundschutz-Vorgehensweise wird dargestellt, wie ein effizientes Managementsystem für die Informationssicherheit aufgebaut werden kann und wie die IT-Grundschutz-Kataloge im Rahmen dieser Aufgabe verwendet werden können. Die Vorgehensweise nach IT-Grundschutz in Kombination mit den IT-Grundschutz-Katalogen bietet eine systematische Methodik zur Erarbeitung von Sicherheitskonzepten und praxiserprobten Standard-Sicherheitsmaßnahmen, die bereits in zahlreichen Behörden und Unternehmen erfolgreich eingesetzt werden.

Die schon seit 1994 veröffentlichten, mittlerweile ca. 4000 Seiten starken IT-Grundschutz-Kataloge beschreiben detailliert mögliche Gefahren und Schutzvorkehrungen. Die IT-Grundschutz-Kataloge werden ständig weiterentwickelt und bedarfsgerecht um aktuelle Fachthemen ergänzt. Alle Informationen rund um IT-Grundschutz sind kostenfrei über die Webseiten des BSI abrufbar. Um die internationale Zusammenarbeit von Behörden und Unternehmen zu unterstützen, werden alle Dokumente rund um IT-Grundschutz auch in englischer Sprache und in elektronischer Form zur Verfügung gestellt.

Immer mehr Geschäftsprozesse werden über die Informations- und Kommunikationstechnik miteinander verknüpft. Dies geht einher mit einer steigenden Komplexität der technischen Systeme und mit einer wachsenden Abhängigkeit vom korrekten Funktionieren der Technik. Daher ist ein geplantes und organisiertes Vorgehen aller Beteiligten notwendig, um ein angemessenes und ausreichendes Sicherheitsniveau durchzusetzen und aufrechtzuerhalten. Eine Verankerung dieses Prozesses in allen Geschäftsbereichen kann nur gewährleistet werden, wenn dieser zur Aufgabe der obersten Managementebene wird. Die oberste Managementebene ist verantwortlich für das zielgerichtete und ordnungsgemäße Funktionieren einer Organisation und damit auch für die Gewährleistung der Informationssicherheit nach innen und außen. Daher muss diese den Sicherheitsprozess initiieren, steuern und kontrollieren. Dazu gehören strategische Leitaussagen zur Informationssicherheit, konzeptionelle Vorgaben und auch organisatorische Rahmenbedingungen, um Informationssicherheit innerhalb aller Geschäftsprozesse erreichen zu können.

Die Verantwortung für Informationssicherheit verbleibt in jedem Fall bei der obersten Managementebene, die Aufgabe "Informationssicherheit" wird allerdings typischerweise an einen Beauftragten für Informationssicherheit delegiert. In den IT-Grundschutz-Dokumenten wird diese Rolle häufig als IT-Sicherheitsbeauftragter bezeichnet, auch wenn deren Aufgaben über pure IT-Sicherheit hinausgehen.

Wenn diese Randbedingungen in einer konkreten Situation nicht gegeben sind, so sollte zunächst versucht werden, die Umsetzung der fehlenden Sicherheitsmaßnahmen auf Arbeitsebene durchzuführen. In jedem Fall sollte aber darauf hingewirkt werden, die Leitungsebene für die Belange der Informationssicherheit zu sensibilisieren, so dass sie zukünftig ihrer Verantwortung Rechnung trägt. Der vielfach zu beobachtende sich selbst auf Arbeitsebene initiierende Informationssicherheitsprozess führt zwar zu einer punktuellen Verbesserung der Sicherheitssituation, garantiert jedoch kein dauerhaftes Fortentwickeln des Informationssicherheitsniveaus.

Die Vorgehensweise nach IT-Grundschutz beschreibt einen Weg, wie ein IS-Management in einer Institution aufgebaut und integriert werden kann. Wenn eine Institution ein effektives und in die Geschäftsprozesse integriertes IS-Management hat, kann davon ausgegangen werden, dass dieses sowohl in der Lage ist, das angestrebte Sicherheitsniveau zu erreichen und wo notwendig zu verbessern, aber auch neue Herausforderungen zu meistern.

Ein fundiertes und gut funktionierendes Sicherheitsmanagement ist die unerlässliche Basis für die zuverlässige und kontinuierliche Umsetzung von Sicherheitsmaßnahmen in einer Institution. Daher findet sich neben der ausführlichen Behandlung in diesem Dokument in den IT-Grundschutz-Katalogen ein Baustein *Sicherheitsmanagement*. Dies dient sowohl dazu, eine einheitliche Methodik bei der Anwendung des IT-Grundschutzes zu erreichen, als auch dazu, das Sicherheitsmanagement seiner Bedeutung angemessen in die Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz einbeziehen zu können.

Ergänzend zu der Vorgehensweise nach IT-Grundschutz werden in den IT-Grundschutz-Katalogen Implementierungshilfen für den Sicherheitsprozess in Form von praxiserprobten Standard-Sicherheitsmaßnahmen zur Verfügung gestellt. IT-Grundschutz verfolgt dabei einen ganzheitlichen Ansatz. Durch die geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen wird ein Sicherheitsniveau erreicht, das für den normalen Schutzbedarf angemessen und ausreichend ist, um geschäftsrelevante Informationen zu schützen. Darüber hinaus bilden diese Maßnahmen nicht nur eine Basis für hochschutzbedürftige IT-Systeme und Anwendungen, sondern liefern an vielen Stellen bereits höherwertige Sicherheit.

In den IT-Grundschutz-Katalogen wird beschrieben, wie auf der Basis von Standard-Sicherheitsmaßnahmen Sicherheitskonzepte erstellt und geprüft werden können. Für typische Prozesse, Anwendungen und Komponenten in der Informationstechnik finden sich außerdem geeignete Bündel ("Bausteine") von Standard-Sicherheitsmaßnahmen. Diese Bausteine sind entsprechend ihrem jeweiligen Fokus in folgende fünf Schichten aufgeteilt:

- Schicht 1 umfasst sämtliche übergreifenden Aspekte der Informationssicherheit. Beispiele sind die Bausteine Personal, Datensicherungskonzept und Outsourcing.
- Schicht 2 befasst sich mit den baulich-technischen Gegebenheiten. Beispiele sind die Bausteine Gebäude, Serverraum und häuslicher Arbeitsplatz.
- Schicht 3 betrifft die einzelnen IT-Systeme. Beispiele sind die Bausteine Allgemeiner Client, Allgemeiner Server, TK-Anlage, Laptop und Mobiltelefon.
- Schicht 4 betrachtet die Vernetzungsaspekte der IT-Systeme. Beispiele sind die Bausteine Heterogene Netze, WLAN, VoIP sowie Netz- und Systemmanagement.
- Schicht 5 schließlich beschäftigt sich mit den eigentlichen Anwendungen. Beispiele sind die Bausteine E-Mail, Webserver und Datenbanken.

Jeder Baustein enthält eine kurze Beschreibung der Thematik, eine Liste mit Verweisen auf die jeweils relevanten Gefährdungen und eine Liste mit Verweisen auf die jeweils relevanten Standard-Sicherheitsmaßnahmen. Die Gefährdungen und Maßnahmen sind wiederum getrennt voneinander in

entsprechende Gefährdungs- und Maßnahmenkataloge gegliedert. Hierbei unterteilen sich die Gefährdungen in Kataloge zu Höherer Gewalt, Organisatorische Mängel, Menschliche Fehlhandlungen, Technisches Versagen und Vorsätzliche Handlungen. Die Maßnahmen gruppieren sich in die Kataloge Infrastruktur, Organisation, Personal, Hardware und Software, Kommunikation und Notfallvorsorge.

2.1 Thematische Abgrenzung

Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung. Der Begriff "Informationssicherheit" statt IT-Sicherheit ist daher umfassender und wird zunehmend verwendet. IT-Grundschutz verfolgt seit langem einen ganzheitlichen Ansatz, mit dem auch geschäftsrelevante Informationen und Geschäftsprozesse geschützt werden, die nicht oder nur teilweise mit IT unterstützt werden. Da aber in der Literatur noch überwiegend der Begriff "IT-Sicherheit" zu finden ist, wird er auch in dieser sowie in anderen Publikationen des IT-Grundschutzes weiterhin verwendet, allerdings werden die Texte sukzessive stärker auf die Betrachtung von Informationssicherheit ausgerichtet.

Aufgabe der Informationssicherheit ist der angemessene Schutz der Grundwerte Vertraulichkeit, Integrität (Unverfälschtheit) und Verfügbarkeit von Informationen. Dazu gehört auch die Absicherung der Informationsverarbeitung, also insbesondere der IT. Außerdem schließt dies auch die Authentizität und Nicht-Abstreitbarkeit von Informationen und Nachrichten als Spezialfälle der Integrität ein.

Die Planungs- und Lenkungsaufgabe, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen, wird als Informationssicherheitsmanagement bezeichnet. Aus den gleichen Gründen, die oben für die Begriffe "Informationssicherheit" und "IT-Sicherheit" genannt sind, wird in vielen BSI-Dokumenten statt Informationssicherheitsmanagement (oder der Kurzform IS-Management) meistens noch der kürzere Begriff "IT-Sicherheitsmanagement" verwendet.

2.2 Übersicht über den Informationssicherheitsprozess

Die Vorgehensweise nach IT-Grundschutz bietet Hilfestellung beim Aufbau und bei der Aufrechterhaltung des Prozesses Informationssicherheit in einer Institution, indem Wege und Methoden für das generelle Vorgehen, aber auch für die Lösung spezieller Probleme aufgezeigt werden.

Für die Gestaltung des Sicherheitsprozesses ist ein systematisches Vorgehen erforderlich, damit ein angemessenes Sicherheitsniveau erreicht werden kann. Im Rahmen des IT-Grundschutzes besteht der Sicherheitsprozess aus folgenden Phasen:

- Initiierung des Sicherheitsprozesses
  - Übernahme der Verantwortung durch die Leitungsebene
  - Konzeption und Planung des Sicherheitsprozesses
  - Erstellung der Leitlinie zur Informationssicherheit
  - Aufbau einer geeigneten Organisationsstruktur für das Informationssicherheitsmanagement
  - Bereitstellung von finanziellen, personellen und zeitlichen Ressourcen
  - Einbindung aller Mitarbeiter in den Sicherheitsprozess
- Erstellung einer Sicherheitskonzeption
- Umsetzung der Sicherheitskonzeption
- Aufrechterhaltung der Informationssicherheit im laufenden Betrieb und kontinuierliche Verbesserung

Informationssicherheitsverantwortliche können die Vorgehensweise nach IT-Grundschutz und die IT-Grundschutz-Kataloge aus verschiedenen Gründen und Zielsetzungen anwenden. Dementsprechend ist auch die Reihenfolge und Intensität der einzelnen Phasen abhängig vom bereits vorhandenen Sicherheitsumfeld und dem jeweiligen Blickwinkel der Anwender. Beispielsweise werden bei einer regulären Überarbeitung des Sicherheitskonzepts häufig andere Schwerpunkte als bei der Integration neuer Geschäftsprozesse gesetzt.

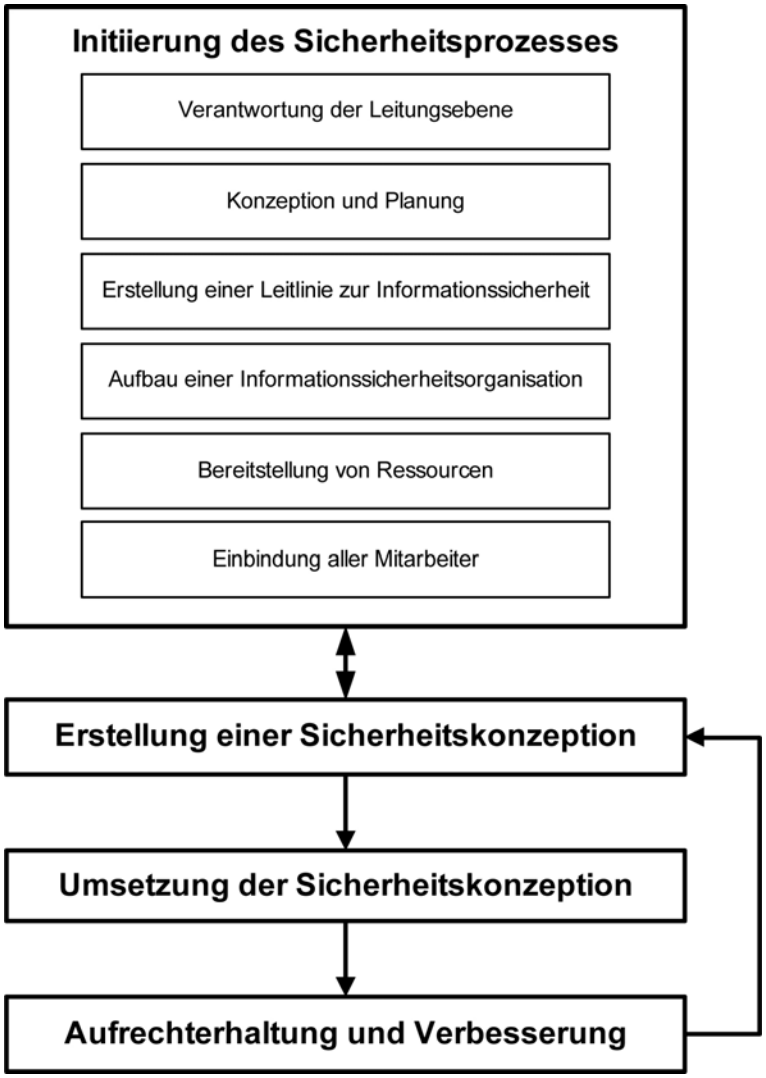


Abbildung 1: Phasen des Sicherheitsprozesses

Einige dieser Phasen können auch parallel durchgeführt werden, z. B. kann die Konzeption und Planung des Sicherheitsprozesses gleichzeitig zur Etablierung der Informationssicherheitsorganisation erfolgen oder die Schulung und Sensibilisierung kann während des gesamten Prozesses angelegt werden. In diesem Fall müssen die vorgezogenen Phasen mit den neuen Ergebnissen zeitnah aktualisiert werden.

Im Folgenden wird eine kurze Darstellung über die Phasen des Sicherheitsprozesses gegeben.

Initiierung des Sicherheitsprozesses

Die Leitungsebene muss den Sicherheitsprozess initiieren, steuern und kontrollieren. Hierfür sind einerseits strategische Leitaussagen zur Informationssicherheit und andererseits organisatorische Rahmenbedingungen erforderlich. Wie ein funktionierender Sicherheitsprozess aufgebaut und welche Organisationsstrukturen dafür sinnvoll sind, wird in Kapitel 3 beschrieben.

Erstellung einer Sicherheitskonzeption

Um eine Sicherheitskonzeption nach IT-Grundschutz zu erstellen, sind eine Reihe von Schritten notwendig, die im Detail in Kapitel 4 beschrieben sind. Die wichtigsten Schritte sind:

- Strukturanalyse
- Schutzbedarfsfeststellung
- Auswahl und Anpassung von Maßnahmen
- Basis-Sicherheitscheck
- Ergänzende Sicherheitsanalyse

Umsetzung von Sicherheitskonzepten

Ein ausreichendes Sicherheitsniveau lässt sich nur erreichen, wenn bestehende Schwachstellen ermittelt, der Status quo in einem Sicherheitskonzept festgehalten, erforderliche Maßnahmen identifiziert und diese Maßnahmen insbesondere auch konsequent umgesetzt werden. In Kapitel 5 wird beschrieben, was bei der Umsetzungsplanung von Sicherheitsmaßnahmen beachtet werden muss.

Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit

Ziel des Sicherheitsmanagements ist es, das angestrebte Sicherheitsniveau zu erreichen und dieses auch dauerhaft aufrechtzuerhalten und zu verbessern. Daher müssen der Sicherheitsprozess und die Organisationsstrukturen für Informationssicherheit regelmäßig daraufhin überprüft werden, ob sie angemessen, wirksam und effizient sind. Ebenso ist zu überprüfen, ob die Maßnahmen des Sicherheitskonzepts praxisnah sind und ob sie korrekt umgesetzt wurden. In Kapitel 6 wird überblicksartig dargestellt, welche Aktionen für die Aufrechterhaltung und Verbesserung der Informationssicherheit ergriffen werden sollten.

Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz

Die Vorgehensweise nach IT-Grundschutz und die IT-Grundschutz-Kataloge werden nicht nur für die Sicherheitskonzeption, sondern auch zunehmend als Referenz im Sinne eines Sicherheitsstandards verwendet. Durch eine Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz kann eine Institution nach innen und außen hin dokumentieren, dass sie sowohl ISO 27001 als auch IT-Grundschutz in der erforderlichen Tiefe umgesetzt hat. Kapitel 7 liefert einen kurzen Überblick, welche Schritte hierfür notwendig sind und welche Bedingungen für eine erfolgreiche Zertifizierung erfüllt werden müssen.

2.3 Anwendung der IT-Grundschutz-Kataloge

Nachdem die Leitungsebene mit der Erstellung der Leitlinie zur Informationssicherheit und den Aufbau der Informationssicherheitsorganisation den Sicherheitsprozess auf der strategischen Ebene definiert hat, wird dieser mit Hilfe der Sicherheitskonzeption auf der operativen Ebene fortgeführt. Somit ist die Erstellung einer Sicherheitskonzeption eine der zentralen Aufgaben des Informationssicherheitsmanagements. Aufbauend auf den Ergebnissen der vorherigen Phase werden hier die erforderlichen Sicherheitsmaßnahmen identifiziert und im Sicherheitskonzept dokumentiert.

Um den sehr heterogenen Bereich der IT einschließlich der Einsatzumgebung besser strukturieren und aufbereiten zu können, verfolgt der IT-Grundschutz das Baukastenprinzip. Die einzelnen Bausteine, die in den IT-Grundschutz-Katalogen beschrieben werden, spiegeln typische Bereiche und Aspekte der Informationssicherheit in einer Institution wider, von übergeordneten Themen, wie dem IS-Management, der Notfallvorsorge oder der Datensicherungskonzeption bis hin zu speziellen Komponenten einer IT-Umgebung. Die IT-Grundschutz-Kataloge umfassen die Gefährdungslage und die Maßnahmenempfehlungen für verschiedene Komponenten, Vorgehensweisen und IT-Systeme, die jeweils in einem Baustein zusammengefasst werden. Das BSI überarbeitet und aktualisiert regelmäßig die bestehenden Bausteine, um die Empfehlungen auf dem Stand der Technik zu halten. Darüber hinaus wird das bestehende Werk regelmäßig um weitere Bausteine erweitert.

Die Bausteine spielen eine zentrale Rolle in der Methodik des IT-Grundschutzes. Sie sind einheitlich aufgebaut, um ihre Anwendung zu vereinfachen. Jeder Baustein beginnt mit einer kurzen Beschreibung der betrachteten Komponente, der Vorgehensweise bzw. des IT-Systems. Im Anschluss daran wird die Gefährdungslage dargestellt. Die Gefährdungen sind dabei nach den Bereichen höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen und vorsätzliche Handlungen unterteilt.

Bei den in den IT-Grundschutz-Katalogen aufgeführten Maßnahmen handelt es sich um Standard-Sicherheitsmaßnahmen, also um diejenigen Maßnahmen, die für die jeweiligen Bausteine nach dem Stand der Technik umzusetzen sind, um eine angemessene Basis-Sicherheit zu erreichen. Dabei stellen die Maßnahmen, die für die Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz gefordert werden, das Minimum dessen dar, was in jedem Fall vernünftigerweise an Sicherheitsvorkehrungen umzusetzen ist. Diese Maßnahmen werden in den IT-Grundschutz-Katalogen mit A, B und C gekennzeichnet. Die als "zusätzlich" gekennzeichneten Maßnahmen haben sich ebenfalls in der Praxis bewährt, sie richten sich jedoch an Anwendungsfälle mit erhöhten Sicherheitsanforderungen. Darüber hinaus gibt es auch noch mit "W" gekennzeichnete Maßnahmen, die dem Wissenstransfer dienen.

Sicherheitskonzepte, die mit Hilfe des IT-Grundschutzes erstellt werden, sind kompakt, da innerhalb des Konzepts jeweils nur auf die entsprechenden Maßnahmen in den IT-Grundschutz-Katalogen referenziert werden muss. Dies fördert die Verständlichkeit und die Übersichtlichkeit. Um die Maßnahmenempfehlungen leichter umsetzen zu können, sind die Sicherheitsmaßnahmen in den Katalogen detailliert beschrieben. Bei der verwendeten Fachterminologie wird darauf geachtet, dass die Beschreibungen für diejenigen verständlich sind, die die Maßnahmen realisieren müssen.

Um die Realisierung der Maßnahmen zu vereinfachen, werden die Texte der IT-Grundschutz-Kataloge konsequent auch in elektronischer Form zur Verfügung gestellt. Darüber hinaus wird die Realisierung der Maßnahmen auch durch Hilfsmittel und Musterlösungen unterstützt, die teilweise durch das BSI und teilweise auch von Anwendern des IT-Grundschutzes bereitgestellt werden.

Weiterführende Informationen finden sich in den einleitenden Kapiteln der IT-Grundschutz-Kataloge sowie in Kapitel 4.4 dieses Standards.

3 Initiierung des Sicherheitsprozesses

Um ein angemessenes und ausreichendes Niveau der Informationssicherheit in der Institution zu erzielen bzw. dieses aufrechtzuerhalten, ist einerseits ein geplantes Vorgehen und andererseits eine adäquate Organisationsstruktur erforderlich. Darüber hinaus ist es notwendig, Sicherheitsziele und eine Strategie zur Erreichung dieser Ziele zu definieren sowie einen kontinuierlichen Sicherheitsprozess einzurichten. Aufgrund der Bedeutung, der weit reichenden Konsequenzen der zu treffenden Entscheidungen und der Verantwortung muss dieses Thema von der obersten Leitungsebene initiiert werden.

3.1 Übernahme von Verantwortung durch die Leitungsebene

Die oberste Leitungsebene jeder Behörde und jedes Unternehmens ist dafür verantwortlich, dass alle Geschäftsbereiche zielgerichtet und ordnungsgemäß funktionieren und dass Risiken frühzeitig erkannt und minimiert werden. Dies kann auch, je nach Organisationsform und Geschäftsbereich, in verschiedenen Gesetzen geregelt sein. Mit der steigenden Abhängigkeit der Geschäftsprozesse von der Informationstechnik steigen also auch die Anforderungen, dass die Informationssicherheit nach innen und außen gewährleistet ist.

Die Leitungsebene muss den Sicherheitsprozess initiieren, steuern und kontrollieren. Die Verantwortung für Informationssicherheit verbleibt dort, die Aufgabe "Informationssicherheit" wird allerdings typischerweise an einen IT-Sicherheitsbeauftragten delegiert. Dabei ist eine intensive Beteiligung der Führungsebene im "Managementprozess Informationssicherheit" erforderlich. Nur so kann das Informationssicherheitsmanagement sicherstellen, dass keine untragbaren Risiken bestehen und Ressourcen an der richtigen Stelle investiert werden. Die oberste Leitungsebene ist somit diejenige Instanz, die die Entscheidung über den Umgang mit Risiken treffen und die entsprechenden Ressourcen zur Verfügung stellen muss.

Die Tatsache, dass die Leitungsebene hinsichtlich der Prävention und Behandlung von Sicherheitsrisiken die Verantwortung trägt, wird leider oft nicht in allen Führungskreisen rechtzeitig erkannt. Dementsprechend sind die Zuständigkeiten und Verantwortlichkeiten bezüglich Informationssicherheitsthemen häufig nicht geklärt. Rechtzeitige Information über mögliche Risiken beim Umgang mit Informationen, Geschäftsprozessen und IT kann von der Geschäftsführung oder Behördenleitung nach einem Sicherheitsvorfall als Bringschuld der IT- oder Sicherheitsexperten gesehen werden. Aus diesem Grund ist es für diese empfehlenswert, die oberste Leitungsebene über mögliche Risiken und Konsequenzen aufgrund fehlender Informationssicherheit aufzuklären. Auf jeden Fall ist aber die Leitungsebene dafür verantwortlich, sicherzustellen, dass die Informationen sie rechtzeitig und im nötigen Umfang erreichen. Zu den sicherheitsrelevanten Themen gehören beispielsweise:

- Die Sicherheitsrisiken für die Institution und deren Informationen sowie die damit verbundenen Auswirkungen und Kosten sollten aufgezeigt werden.
- Die Auswirkungen von Sicherheitsvorfällen auf die kritischen Geschäftsprozesse sollten dargestellt werden.
- Die Sicherheitsanforderungen, die sich aus gesetzlichen und vertraglichen Vorgaben ergeben, müssen beschrieben werden.
- Die für die Branche typischen Standard-Vorgehensweisen zur Informationssicherheit sollten vorgestellt werden.
- Die Vorteile einer Zertifizierung, um gegenüber Kunden, Geschäftspartnern und Aufsichtsstellen den Grad der erreichten Informationssicherheit nachzuweisen, sollten erläutert werden.

Da häufig den Aussagen unbeteiligter Dritter mehr Gewicht bemessen wird als denen eigener Mitarbeiter, kann es oft sinnvoll sein, für die Sensibilisierung der Geschäftsleitung bzw. der Behördenleitung hinsichtlich der Informationssicherheit externe Berater hinzuzuziehen.

Die Leitungsebene trägt zwar die Verantwortung für die Erreichung der Sicherheitsziele, der Sicherheitsprozess muss aber von allen Beschäftigten in einer Organisation mitgetragen und mitgestaltet werden. Idealerweise sollten dabei folgende Prinzipien eingehalten werden:

- Die Initiative für Informationssicherheit geht von der Behörden- bzw. Unternehmensleitung aus.
- Die Gesamtverantwortung für Informationssicherheit verbleibt bei der obersten Leitungsebene.
- Die Aufgabe "Informationssicherheit" wird durch die Behörden- bzw. Unternehmensleitung aktiv unterstützt.
- Die Behörden- bzw. Unternehmensleitung benennt die für Informationssicherheit zuständigen Mitarbeiter und stattet diese mit den erforderlichen Kompetenzen und Ressourcen aus.
- Die Leitungsebene übernimmt auch im Bereich Informationssicherheit eine Vorbildfunktion. Dazu gehört unter anderem, dass auch die Leitungsebene alle vorgegebenen Sicherheitsregeln beachtet.

Die Leitungsebene muss sich vor allem dafür einsetzen, dass Informationssicherheit in alle relevanten Geschäftsprozesse bzw. Fachverfahren und Projekte integriert wird. Der IT-Sicherheitsbeauftragte braucht hierbei erfahrungsgemäß die volle Unterstützung der Behörden- oder Unternehmensleitung, um unter dem überall herrschenden Erfolgsdruck von den jeweiligen Fachverantwortlichen in jede wesentliche Aktivität eingebunden zu werden.

Die Leitungsebene muss die Ziele sowohl für das Informationssicherheitsmanagement als auch für alle anderen Bereiche so setzen, dass das angestrebte Sicherheitsniveau in allen Bereichen mit den bereitgestellten Ressourcen (Personal, Zeit, Finanzmittel) erreichbar ist.

Aktionspunkt zu 3.1 Übernahme von Verantwortung durch die Leitungsebene
• Die Leitungsebene wird über mögliche Risiken und Konsequenzen aufgrund fehlender Informationssicherheit aufgeklärt. • Die Leitungsebene übernimmt die Gesamtverantwortung für Informationssicherheit. • Die Leitungsebene initiiert den Informationssicherheitsprozess innerhalb der Institution.

3.2 Konzeption und Planung des Sicherheitsprozesses

Um ein angemessenes Sicherheitsniveau erreichen und aufrechterhalten zu können, ist es notwendig, einen kontinuierlichen Informationssicherheitsprozess zu etablieren und eine angemessene Strategie für Informationssicherheit (IS-Strategie) festzulegen. Eine IS-Strategie dient der Planung des weiteren Vorgehens, um die gesetzten Sicherheitsziele zu erreichen. Sie wird vom Management vorgegeben und basiert auf den Geschäftszielen eines Unternehmens bzw. dem Auftrag einer Behörde. Das Management gibt grundlegende Sicherheitsziele vor und legt fest, welches Informationssicherheitsniveau im Hinblick auf die Geschäftsziele und Fachaufgaben angemessen ist. Die dafür erforderlichen Mittel müssen ebenfalls von der Leitungsebene zur Verfügung gestellt werden.

3.2.1 Ermittlung von Rahmenbedingungen

Die grundsätzlichen Ziele und Aufgaben einer Institution sind die Grundlage für alle Geschäftsprozesse bzw. Fachverfahren und Aktivitäten, einschließlich der Informationssicherheit. Um eine angemessene IS-Strategie festzulegen, sollte daher jede Institution ihre wichtigsten Geschäftsprozesse und Fachaufgaben sowie deren Bedarf an Informationssicherheit ermitteln. Mittlerweile gibt es kaum noch Bereiche, in denen wesentliche Geschäftsprozesse ohne IT-Unterstützung funktionsfähig sind. Die Zusammenhänge zwischen Geschäftsabläufen und den dort verarbeiteten Informationen sowie der eingesetzten Informationstechnik bilden die Basis für die Entscheidung, welches Sicherheitsniveau zum Schutz der Informationen und für die Informationstechnik jeweils angemessen ist. Im Folgenden wird dieser Entscheidungsprozess näher erläutert.

Zu jedem Geschäftsprozess und jeder Fachaufgabe muss ein Ansprechpartner benannt werden, der als sogenannter Informationseigentümer für alle Fragen der Informationsverarbeitung im Rahmen dieses Geschäftsprozesses verantwortlich ist. Die Fachverantwortlichen oder Informationseigentümer sind beispielsweise zuständig für die Delegation von Aufgaben und den Umgang mit Informationen im Rahmen der von ihnen betreuten Geschäftsprozesse. Zu jedem Geschäftsprozess und jeder Fachaufgabe muss festgelegt werden, wie kritisch, also wie schutzbedürftig, die verarbeiteten Informationen sind. Dem Schutzbedarf jedes Geschäftsprozesses muss abschließend von der Geschäftsleitung bzw. der Behördenleitung zugestimmt werden, da sich hieraus Sicherheitsanforderungen ableiten und dafür Ressourcen gebunden werden müssen.

Über die Analyse der Geschäftsprozesse lassen sich Aussagen über die Auswirkungen von Sicherheitsvorfällen auf die Geschäftstätigkeit ableiten. In vielen Fällen wird es ausreichen, mit einer sehr groben Beschreibung der Geschäftsprozesse zu arbeiten.

Folgende Fragen sollten sich beantworten lassen:

- Welche Geschäftsprozesse gibt es in der Organisation und wie hängen diese mit den Geschäftszielen zusammen?
- Welche Geschäftsprozesse hängen von einer funktionierenden, also einer ordnungsgemäß und anforderungsgerecht arbeitenden Informationstechnik ab?
- Welche Informationen werden für diese Geschäftsprozesse verarbeitet?
- Welche Informationen sind besonders wichtig und damit in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit schützenswert und warum (z. B. personenbezogene Daten, Kundendaten, strategische Informationen, Geheimnisse wie Entwicklungsdaten, Patente, Verfahrensbeschreibungen)?

Eine Vielzahl interner Rahmenbedingungen können Auswirkungen auf die Informationssicherheit haben und müssen ermittelt werden. Es geht zu diesem frühen Zeitpunkt nicht darum, detailliert die Informationstechnik zu beschreiben. Es sollte aber eine grobe Übersicht vorliegen, welche Informationen für einen Geschäftsprozess mit welchen Anwendungen und IT-Systemen verarbeitet werden.

Daneben müssen ebenso alle externen Rahmenbedingungen ermittelt werden, die Auswirkungen auf die Informationssicherheit haben, wie beispielsweise

- gesetzliche Rahmenbedingungen (nationale und internationale Gesetze und Bestimmungen),
- Umwelteinflüsse, beispielsweise aufgrund der geografischen Lage oder aufgrund von sozialen und kulturellen Rahmenbedingungen,
- Anforderungen von Kunden, Lieferanten und Geschäftspartnern, aktuelle Marktlage, Wettbewerbssituation und weitere relevante marktspezifische Abhängigkeiten,
- branchenspezifische Sicherheitsstandards.

Um alle relevanten Rahmenbedingungen für jeden wesentlichen Geschäftsprozess möglichst schnell und umfassend zu ermitteln, empfiehlt es sich, dass ein kurzes Sicherheitsgespräch (Brainstorming) zu jedem Geschäftsprozess durchgeführt wird. Diese Sicherheitsgespräche sollten unter der Leitung des IT-Sicherheitsbeauftragten mit dem jeweiligen Informationseigentümer bzw. Fachverantwortlichen sowie dem entsprechenden IT-Verantwortlichen durchgeführt werden. Die Ergebnisse sollten nach einem vorher festgelegten Schema dokumentiert werden.

3.2.2 Formulierung von allgemeinen Informationssicherheitszielen

Zu Beginn jedes Sicherheitsprozesses sollten die Informationssicherheitsziele sorgfältig bestimmt werden. Anderenfalls besteht die Gefahr, dass Sicherheitsstrategien und -konzepte erarbeitet werden, die die eigentlichen Anforderungen der Institution verfehlen. Dies kann bedeuten, dass ungewollte Risiken eingegangen werden, aber auch, dass zu viele Ressourcen in nicht passende oder zu aufwendige Sicherheitsmaßnahmen investiert werden.

Aus den grundsätzlichen Zielen der Institution und den allgemeinen Rahmenbedingungen sollten daher zunächst allgemeine Sicherheitsziele abgeleitet werden. Aus diesen werden später bei der Erstellung des Sicherheitskonzeptes und bei der Ausgestaltung der Informationssicherheitsorganisation konkrete Sicherheitsanforderungen an den Umgang mit Informationen und den IT-Betrieb abgeleitet. Mögliche allgemeine Sicherheitsziele einer Institution könnten z. B. sein:

- Hohe Verlässlichkeit des Handelns, auch in Bezug auf den Umgang mit Informationen (Verfügbarkeit, Integrität, Vertraulichkeit),
- Gewährleistung des guten Rufs der Institution in der Öffentlichkeit,
- Erhaltung der in Technik, Informationen, Arbeitsprozesse und Wissen investierten Werte,
- Sicherung der hohen, möglicherweise unwiederbringlichen Werte der verarbeiteten Informationen,
- Sicherung der Qualität der Informationen, z. B. wenn sie als Basis für weitreichende Entscheidungen dienen,
- Gewährleistung der aus gesetzlichen Vorgaben resultierenden Anforderungen,
- Reduzierung der im Schadensfall entstehenden Kosten (sowohl durch Schadensvermeidung wie Schadensverhütung) und
- Sicherstellung der Kontinuität der Arbeitsabläufe innerhalb der Institution.

Um die Sicherheitsziele definieren zu können, sollte zunächst abgeschätzt werden, welche Geschäftsprozesse bzw. Fachverfahren und Informationen für die Aufgabenerfüllung notwendig sind und welcher Wert diesen beigemessen wird. Dabei ist es wichtig, klarzustellen, wie stark die Aufgabenerfüllung innerhalb der Institution von der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und von der eingesetzten IT und deren sicheren Funktionieren abhängt. Für die Definition der Sicherheitsziele ist es sinnvoll, die zu schützenden Grundwerte Verfügbarkeit, Integrität und Vertraulichkeit ausdrücklich zu benennen und eventuell zu priorisieren. Diese Aussagen werden im Lauf des Sicherheitsprozesses bei der Wahl der Sicherheitsmaßnahmen und Strategien eine entscheidende Rolle spielen.

Die Bestimmung der Informationssicherheitsziele und des angestrebten Sicherheitsniveaus ist jedoch nur der Anfang des Informationssicherheitsprozesses. Konkrete Entscheidungen über Ressourcen und Investitionen, die sich im Laufe des Sicherheitsprozesses ergeben, müssen in einem späteren Schritt auch von der obersten Leitungsebene bewilligt werden. Dies bedeutet, dass an dieser Stelle keine detaillierte Analyse des Informationsverbundes und der möglichen Kosten von Sicherheitsmaßnahmen erfolgen muss, sondern lediglich die Aussage, was für die Institution von besonderer Bedeutung ist und warum.

3.2.3 Bestimmung des angemessenen Sicherheitsniveaus der Geschäftsprozesse

Zur besseren Verständlichkeit der Informationssicherheitsziele kann das angestrebte Sicherheitsniveau für einzelne, besonders hervorgehobene Geschäftsprozesse bzw. Bereiche der Institution in Bezug auf die Grundwerte der Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) dargestellt werden. Dies ist für die spätere Formulierung der detaillierten Sicherheitskonzeption hilfreich.

Nachstehend sind einige beispielhafte Kriterien zur Bestimmung eines angemessenen Sicherheitsniveaus aufgeführt. Anhand derjenigen Aussagen, die am ehesten zutreffen, lässt sich das Sicherheitsniveau (normal, hoch oder sehr hoch) bestimmen. In dieser Phase des Sicherheitsprozesses geht es um die Formulierung der ersten richtungweisenden Aussagen, die in den späteren Phasen als Grundlage dienen werden und nicht um eine detaillierte Schutzbedarfsfeststellung.

Sehr hoch:

- Der Schutz vertraulicher Informationen muss unbedingt gewährleistet sein und in sicherheitskritischen Bereichen strengen Vertraulichkeitsanforderungen genügen.

- Die Informationen müssen im höchsten Maße korrekt sein.
- Die zentralen Aufgaben der Institution sind ohne IT-Einsatz nicht durchführbar. Knappe Reaktionszeiten für kritische Entscheidungen fordern ständige Präsenz der aktuellen Informationen, Ausfallzeiten sind nicht akzeptabel.
- Der Schutz personenbezogener Daten muss unbedingt gewährleistet sein. Anderenfalls kann es zu einer Gefahr für Leib und Leben oder für die persönliche Freiheit des Betroffenen kommen.

Insgesamt gilt: Der Ausfall der IT führt zum totalen Zusammenbruch der Institution oder hat schwerwiegende Folgen für breite gesellschaftliche oder wirtschaftliche Bereiche.

Hoch:

- Der Schutz vertraulicher Informationen muss hohen Anforderungen genügen und in sicherheitskritischen Bereichen stärker ausgeprägt sein.
- Die verarbeiteten Informationen müssen korrekt sein, auftretende Fehler müssen erkennbar und vermeidbar sein.
- In zentralen Bereichen der Institution laufen zeitkritische Vorgänge oder es werden dort Massenaufgaben wahrgenommen, die ohne IT-Einsatz nicht zu erledigen sind. Es können nur kurze Ausfallzeiten toleriert werden.
- Der Schutz personenbezogener Daten muss hohen Anforderungen genügen. Anderenfalls besteht die Gefahr, dass der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt wird.

Insgesamt gilt: Im Schadensfall tritt Handlungsunfähigkeit zentraler Bereiche der Institution ein; Schäden haben erhebliche Beeinträchtigungen der Institution selbst oder betroffener Dritter zur Folge.

Normal:

- Der Schutz von Informationen, die nur für den internen Gebrauch bestimmt sind, muss gewährleistet sein.
- Kleinere Fehler können toleriert werden. Fehler, die die Aufgabenerfüllung erheblich beeinträchtigen, müssen jedoch erkenn- oder vermeidbar sein.
- Längere Ausfallzeiten, die zu Terminüberschreitungen führen, sind nicht zu tolerieren.
- Der Schutz personenbezogener Daten muss gewährleistet sein. Anderenfalls besteht die Gefahr, dass der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt wird.

Insgesamt gilt: Schäden haben Beeinträchtigungen der Institution zur Folge.

Für die Formulierung der Informationssicherheitsziele ist die Mitwirkung der Leitungsebene unbedingt notwendig. Für diesen im Sicherheitsprozess grundlegenden Schritt kann auch die Einbeziehung eines externen Informationssicherheitsexperten sinnvoll sein. Zur Bestimmung des angestrebten Sicherheitsniveaus müssen die Ziele der Institution in Bezug auf ihre Sicherheitsanforderungen betrachtet werden, jedoch unter Berücksichtigung der Tatsache, dass in der Regel begrenzte Ressourcen für die Implementierung von Sicherheitsmaßnahmen zur Verfügung stehen. Aus diesem Grund ist es von besonderer Bedeutung, den tatsächlichen Bedarf an Verfügbarkeit, Integrität und Vertraulichkeit zu identifizieren, da ein hohes Sicherheitsniveau in der Regel auch mit hohem Implementierungsaufwand verbunden ist. Es ist außerdem empfehlenswert, die formulierten Anforderungen zu priorisieren, wenn dies zu diesem Zeitpunkt bereits möglich ist. Dies wird bei der Ressourcenplanung in späteren Phasen des Sicherheitsprozesses eine Entscheidungsgrundlage bilden.

Hinweis zur Beschreibungstiefe

In dieser frühen Phase des Informationssicherheitsprozesses geht es nicht um eine detaillierte Betrachtung aller Anwendungen und IT-Systeme oder eine aufwendige Risikoanalyse. Wichtig ist, eine

Übersicht zu haben, welche Sicherheitsanforderungen aufgrund der Geschäftsprozesse oder Fachverfahren an die Informationstechnik gestellt werden. Zum Beispiel sollten sich nach der Bestimmung des angestrebten Sicherheitsniveaus die folgenden Fragen beantworten lassen:

- Welche Informationen sind in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit besonders kritisch für die Institution?
- Welche kritischen Aufgaben der Institution können ohne Unterstützung durch IT nicht, nur unzureichend oder mit erheblichem Mehraufwand ausgeführt werden?
- Welche wesentlichen Entscheidungen der Institution beruhen auf Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationsverarbeitungssystemen?
- Welche Auswirkungen können absichtliche oder ungewollte Sicherheitszwischenfälle haben?
- Werden mit der eingesetzten IT Informationen verarbeitet, deren Vertraulichkeit besonders zu schützen ist?
- Hängen wesentliche Entscheidungen von der Korrektheit, Aktualität und Verfügbarkeit von Informationen ab, die mit IT verarbeitet werden?
- Welche gesetzlichen Anforderungen (z. B. Datenschutz) haben besondere Maßnahmen zur Folge?

Die Beschreibungen des angestrebten Sicherheitsniveaus sollten auf das jeweilige Umfeld angepasst sein. Kurze Begründungen sind für die Motivation darauf aufbauender Maßnahmen hilfreich. Dies könnte beispielsweise für ein Krankenhaus heißen: "In der Röntgenabteilung ist ein sehr hohes Informationssicherheitsniveau notwendig, weil von der korrekten Funktion der IT-Systeme Menschenleben abhängen."

Aktionspunkte zu 3.2 Konzeption und Planung des Sicherheitsprozesses
• Ansprechpartner für alle Geschäftsprozesse und Fachaufgaben benennen
• Grobeinschätzung der Wertigkeit von Informationen, Geschäftsprozesse und Fachaufgaben durchführen
• Rahmenbedingungen ermitteln
• Bedeutung der Geschäftsprozesse, Fachaufgaben und Informationen abschätzen
• Allgemeine Informationssicherheitsziele festlegen
• Zustimmung der Leitungsebene einholen

3.3 Erstellung einer Leitlinie zur Informationssicherheit

Die Leitlinie zur Informationssicherheit beschreibt allgemeinverständlich, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit innerhalb der Institution hergestellt werden soll. Sie beinhaltet die von der Institution angestrebten Informationssicherheitsziele sowie die verfolgte Sicherheitsstrategie. Die Sicherheitsleitlinie beschreibt damit auch über die Sicherheitsziele das angestrebte Sicherheitsniveau in einer Behörde oder einem Unternehmen. Sie ist somit Anspruch und Aussage zugleich, dass dieses Sicherheitsniveau auf allen Ebenen der Institution erreicht werden soll.

Die Erstellung der Sicherheitsleitlinie sollte in folgenden Schritten vollzogen werden:

3.3.1 Verantwortung der Behörden- bzw. Unternehmensleitung für die Sicherheitsleitlinie

Mit der Leitlinie zur Informationssicherheit wird dokumentiert, welche strategische Position die Institutionsleitung zur Erreichung der Informationssicherheitsziele auf allen Ebenen der Organisation einnimmt.

Da die Sicherheitsleitlinie ein zentrales Strategiepapier für die Informationssicherheit einer Institution darstellt, muss sie so gestaltet sein, dass sich alle adressierten Organisationseinheiten mit ihrem Inhalt identifizieren können. An ihrer Erstellung sollten daher möglichst viele Bereiche beteiligt werden. Jede Institution muss letztendlich aber selbst entscheiden, welche Abteilungen und Hierarchieebenen an der Formulierung der Sicherheitsleitlinie mitwirken.

Es empfiehlt sich, bei der Erarbeitung der Sicherheitsleitlinie das Fachwissen der folgenden Organisationseinheiten zu nutzen: Fachverantwortliche für wichtige Anwendungen, IT-Betrieb, Sicherheit (Informations-, IT- und Infrastruktur-Sicherheit), Datenschutzbeauftragter, Personalabteilung, Personal- bzw. Betriebsrat, Revision, Vertreter für Finanzfragen, Rechtsabteilung.

3.3.2 Festlegung des Geltungsbereichs und Inhalt der Sicherheitsleitlinie

In der Informationssicherheitsleitlinie muss beschrieben werden, für welche Bereiche diese gelten soll. Der Geltungsbereich kann die gesamte Institution umfassen oder aus Teilbereichen dieser bestehen. Wichtig ist jedoch dabei, dass die betrachteten Geschäftsaufgaben und –prozesse in dem Geltungsbereich komplett enthalten sind. Insbesondere bei größeren Organisationen ist die Festlegung des Geltungsbereichs keine triviale Aufgabe. Eine Orientierung nach Verantwortlichkeiten kann dabei behilflich sein.

Die Sicherheitsleitlinie sollte kurz und bündig formuliert sein, da sich mehr als 20 Seiten in der Praxis nicht bewährt haben. Sie sollte mindestens die folgenden Informationen beinhalten:

- Stellenwert der Informationssicherheit und Bedeutung der wesentlichen Informationen und der IT für die Aufgabenerfüllung,
- Bezug der Informationssicherheitsziele zu den Geschäftszielen oder Aufgaben der Institution,
- Sicherheitsziele und die Kernelemente der Sicherheitsstrategie für die eingesetzte IT,
- Zusicherung, dass die Sicherheitsleitlinie von der Institutionsleitung durchgesetzt wird, und Leitaussagen zur Erfolgskontrolle und
- Beschreibung der für die Umsetzung des Informationssicherheitsprozesses etablierten Organisationsstruktur.

Zusätzlich können z. B. noch folgende Aussagen hinzukommen:

- Zur Motivation können einige, für die Geschäftsprozesse wichtige, Gefährdungen angerissen und die wichtigsten gesetzlichen Regelungen und sonstige wichtige Rahmenbedingungen (wie vertragliche Vereinbarungen) genannt werden.
- Die wesentlichen Aufgaben und Zuständigkeiten im Sicherheitsprozess sollten aufgezeigt werden (insbesondere für das IS-Management-Team, den IT-Sicherheitsbeauftragten, die IT-Anwender und die IT-Administratoren). Außerdem sollten die Organisationseinheiten oder Rollen benannt werden, die als Ansprechpartner für Sicherheitsfragen fungieren.
- Programme zur Förderung der Informationssicherheit durch Schulungs- und Sensibilisierungsmaßnahmen können angekündigt werden.

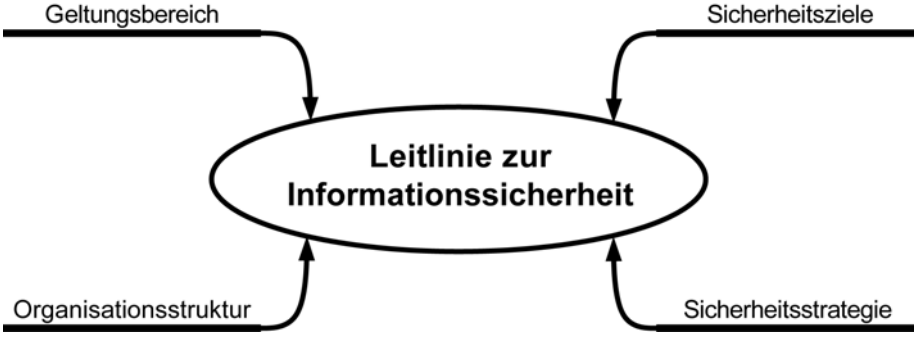


Abbildung 2: Inhalte der Sicherheitsleitlinie

3.3.3 Einberufung einer Entwicklungsgruppe für die Sicherheitsleitlinie

Falls es innerhalb der Institution bereits ein IS-Management-Team gibt, so sollte dieses die Informationssicherheitsleitlinie entwickeln bzw. überprüfen und überarbeiten. Danach wird dieser Entwurf der Behörden- bzw. Unternehmensleitung zur Genehmigung vorgelegt.

Befindet sich das Informationssicherheitsmanagement erst im Aufbau, so sollte eine Entwicklungsgruppe zur Erarbeitung der Sicherheitsleitlinie eingerichtet werden. Diese Gruppe kann im Laufe des Sicherheitsprozesses die Funktion des IS-Management-Teams übernehmen. Sinnvollerweise sollten in dieser Entwicklungsgruppe Vertreter der IT-Anwender, Vertreter des IT-Betriebs und ein oder mehrere in Sachen Informationssicherheit ausreichend vorgebildete Mitarbeiter mitwirken. Idealerweise sollte zeitweise auch ein Mitglied der Leitungsebene, das die Bedeutung der Informationsverarbeitung für die Institution einschätzen kann, hinzugezogen werden.

3.3.4 Bekanntgabe der Sicherheitsleitlinie

Es ist wichtig, dass die Behörden- bzw. Unternehmensleitung ihre Zielsetzungen und Erwartungshaltungen durch Bekanntgabe der Sicherheitsleitlinie unterstreicht und den Stellenwert sowie die Bedeutung der Informationssicherheit in der gesamten Organisation verdeutlicht. Alle Mitarbeiter sollten daher die Inhalte der Sicherheitsleitlinie kennen und nachvollziehen können. Neuen Mitarbeitern sollte die Sicherheitsleitlinie erläutert werden, bevor sie Zugang zur Informationsverarbeitung erhalten.

Da die Verantwortung der Behörden- bzw. Unternehmensleitung in Bezug auf die Sicherheitsleitlinie entscheidend ist, sollte die Leitlinie schriftlich fixiert sein. Die Behörden- bzw. Unternehmensleitung sollte ihr formell zugestimmt haben. Die Inhalte der Sicherheitsleitlinie sollten also innerhalb der Institution nicht nur bekannt sein, sondern auch möglichst einfach zugreifbar sein, z. B. im Intranet der Institution. Wenn diese vertrauliche Aussagen enthält, sollten diese in eine Anlage zur Leitlinie verlagert werden, die deutlich als vertraulich gekennzeichnet ist.

Schließlich sollten alle Mitarbeiter darauf aufmerksam gemacht werden, dass nicht nur bei der Aufgabenerfüllung allgemein, sondern auch bei der Erfüllung der Aufgabe "Informationssicherheit" von jedem Mitarbeiter ein engagiertes, kooperatives sowie verantwortungsbewusstes Handeln erwartet wird.

3.3.5 Aktualisierung der Sicherheitsleitlinie

Die Leitlinie zur Informationssicherheit sollte in regelmäßigen Abständen auf ihre Aktualität hin überprüft und gegebenenfalls angepasst werden. Hierbei sollte beispielsweise überlegt werden, ob sich Geschäftsziele oder Aufgaben und damit Geschäftsprozesse geändert haben, ob wesentliche IT-Verfahren geändert worden sind, ob die Organisationsstruktur neu ausgerichtet wurde oder ob neue IT-Systeme eingeführt worden sind. Bei den häufig rasanten Entwicklungen im Bereich der IT einerseits und der Sicherheitslage andererseits empfiehlt es sich, die Sicherheitsleitlinie spätestens alle zwei Jahre zu überdenken.

Aktionspunkte zu 3.3 Erstellung einer Sicherheitsleitlinie

- Auftrag der Leitungsebene zur Erarbeitung einer Sicherheitsleitlinie einholen
- Geltungsbereich festlegen
- Entwicklungsgruppe für die Sicherheitsleitlinie einberufen
- Inkraftsetzung der Sicherheitsleitlinie durch die Leitungsebene veranlassen
- Sicherheitsleitlinie bekannt geben
- Sicherheitsleitlinie regelmäßig überprüfen und gegebenenfalls aktualisieren

3.4 Organisation des Sicherheitsprozesses

Das angestrebte Sicherheitsniveau kann nur erreicht werden, wenn der Informationssicherheitsprozess institutionsweit umgesetzt wird. Dieser übergreifende Charakter des Sicherheitsprozesses macht es notwendig, Rollen innerhalb der Institution festzulegen und den Rollen die entsprechenden Aufgaben zuzuordnen. Diese Rollen müssen dann qualifizierten Mitarbeitern übertragen und von diesen ausgeführt werden. Nur so kann gewährleistet werden, dass alle wichtigen Aspekte berücksichtigt und sämtliche anfallenden Aufgaben effizient und effektiv erledigt werden.

Die Aufbauorganisation, die zur Förderung und Durchsetzung des Informationssicherheitsprozesses erforderlich ist, wird als Informationssicherheitsorganisation oder kurz IS-Organisation bezeichnet.

Wie viele Personen, in welcher Organisationsstruktur und mit welchen Ressourcen mit Informationssicherheit beschäftigt sind, hängt von der Größe, Beschaffenheit und Struktur der jeweiligen Institution ab. Auf jeden Fall sollte als zentraler Ansprechpartner für die Koordination, Verwaltung und Kommunikation des Prozesses Informationssicherheit ein IT-Sicherheitsbeauftragter benannt sein. In größeren Institutionen gibt es darüber hinaus typischerweise weitere Personen, die verschiedene Teilaufgaben für Informationssicherheit wahrnehmen. Um deren Tätigkeiten aufeinander abzustimmen, sollte ein IS-Management-Team aufgebaut werden, das sämtliche übergreifenden Belange der Informationssicherheit regelt und Pläne, Vorgaben und Richtlinien erarbeitet.

Um den direkten Zugang zur Institutionsleitung sicherzustellen, sollten diese Rollen als Stabsstelle organisiert sein. Auf Leitungsebene sollte die Aufgabe Informationssicherheit eindeutig einem verantwortlichen Manager zugeordnet sein, an den der IT-Sicherheitsbeauftragte berichtet.

Unabhängig davon, wie eine optimale Struktur für die eigene IS-Organisation zu gestalten ist, sind die drei folgenden Grundregeln dabei unbedingt zu beachten.

Grundregeln bei der Definition von Rollen im Informationssicherheitsmanagement

- Die Gesamtverantwortung für die ordnungsgemäße und sichere Aufgabenerfüllung (und damit für die Informationssicherheit) verbleibt bei der Leitungsebene.
- Es ist mindestens eine Person (typischerweise als IT-Sicherheitsbeauftragter) zu benennen, die den Informationssicherheitsprozess fördert und koordiniert.
- Jeder Mitarbeiter ist gleichermaßen für seine originäre Aufgabe wie für die Aufrechterhaltung der Informationssicherheit an seinem Arbeitsplatz und in seiner Umgebung verantwortlich.

3.4.1 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse

Das Management der Informationssicherheit ist zwar nur eine von vielen wichtigen Managementaufgaben, hat jedoch Einfluss auf nahezu alle Bereiche einer Institution. Daher muss das Informationssicherheitsmanagement vernünftig in bestehende Organisationsstrukturen integriert und Ansprechpartner festgelegt werden. Aufgaben und Zuständigkeiten müssen klar voneinander abgegrenzt sein. Es muss dabei gewährleistet sein, dass nicht nur bei einzelnen Maßnahmen, sondern bei allen strategischen Entscheidungen die notwendigen Sicherheitsaspekte berücksichtigt werden (zum Beispiel beim Thema Outsourcing oder bei der Nutzung neuer elektronischer Vertriebskanäle). Um dies sicherzustellen, ist es wichtig, dass die IS-Organisation bei allen Projekten, die Auswirkungen auf die Informationssicherheit haben könnten, rechtzeitig beteiligt wird.

Vor allem in größeren Organisationen existiert bereits häufig ein übergreifendes Risikomanagementsystem. Da IT-Risiken zu den wichtigsten operationellen Risiken gehören, sollten die Methoden zum Management von IT-Risiken mit den bereits etablierten Methoden abgestimmt werden.

3.4.2 Aufbau der Informationssicherheitsorganisation

In Abhängigkeit von der Institutionsgröße bieten sich verschiedene Möglichkeiten für die Aufbauorganisation des Informationssicherheitsmanagements an.

In den nachstehenden Abbildungen werden drei davon aufgezeigt. Die erste Abbildung zeigt die Struktur für die IS-Organisation in einer großen Institution. Die zweite Abbildung zeigt den Aufbau in einer mittelgroßen Institution, in der das IS-Management-Team und der IT-Sicherheitsbeauftragte zusammengefasst wurden. Die dritte Abbildung zeigt eine Struktur für die IS-Organisation in einer kleinen Institution, in der alle Aufgaben vom IT-Sicherheitsbeauftragten wahrgenommen werden.

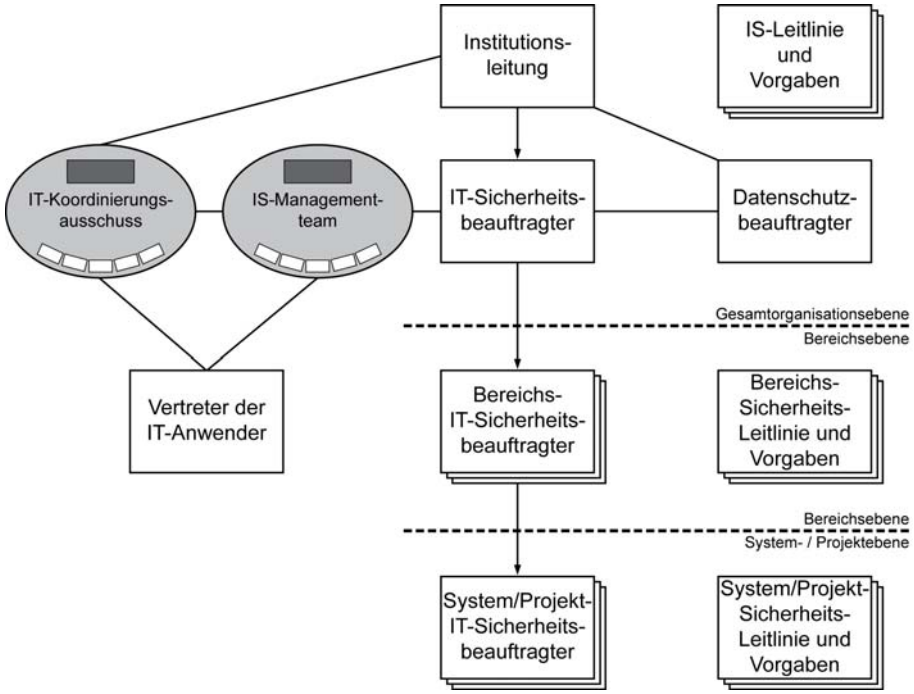


Abbildung 3.1: Aufbau einer IS-Organisation in einer großen Institution

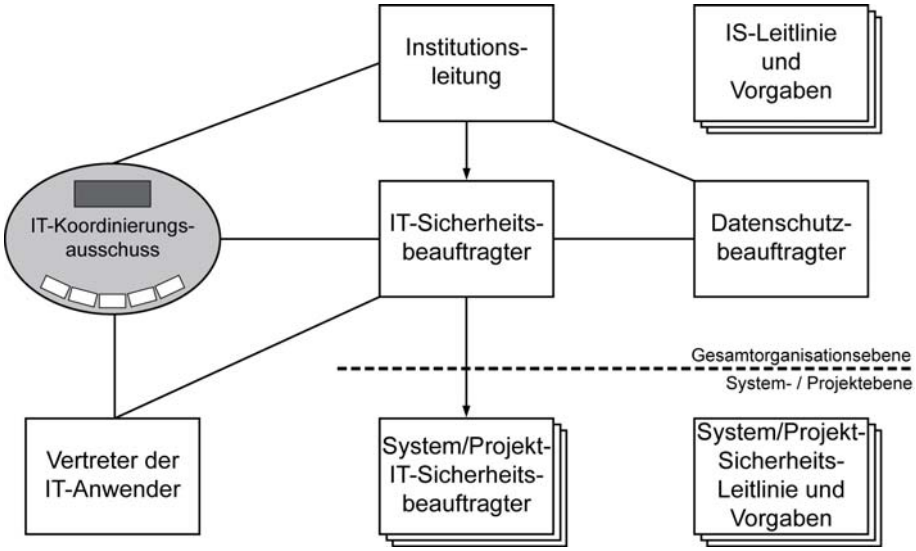


Abbildung 3.2: Aufbau der IS-Organisation in einer mittelgroßen Institution

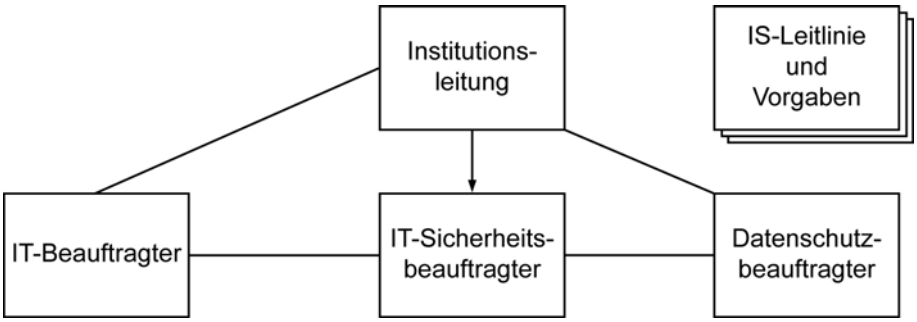


Abbildung 3.3: Aufbau der IS-Organisation in einer kleinen Institution

An dieser Stelle sei deutlich darauf hingewiesen, dass die in den Abbildungen dargestellten zentralen Rollen nicht unbedingt von verschiedenen Personen wahrgenommen werden müssen. Die personelle Ausgestaltung richtet sich nach der Größe der jeweiligen Institution, den vorhandenen Ressourcen und dem angestrebten Sicherheitsniveau. Die Ressourcenplanung für die Unterstützung der Informationssicherheit muss so erfolgen, dass das beschlossene Sicherheitsniveau auch tatsächlich erreicht werden kann.

3.4.3 Aufgaben, Verantwortungen und Kompetenzen in der IS-Organisation

IT-Sicherheitsbeauftragte und IS-Management-Team müssen klar definierte Aufgaben, Verantwortungen und Kompetenzen haben, die von der Leitungsebene festzulegen sind. Um ihre Aufgabe wahrnehmen zu können, sollten sie bei allen relevanten Verfahren und Entscheidungen beteiligt werden. Die Rollen sind so in die Organisationsstruktur einzubinden, dass alle Beteiligten untereinander kommunizieren können. Mit der Wahrnehmung der Aufgaben als IT-Sicherheitsbeauftragte bzw. im IS-Management-Team sollte qualifiziertes Personal betraut werden. Bei Bedarf können unterstützend Aufgaben an Bereichs-IT-Sicherheitsbeauftragte, Projekt- sowie IT-System-Sicherheitsbeauftragte delegiert werden.

3.4.4 Der IT-Sicherheitsbeauftragte

Informationssicherheit wird häufig vernachlässigt, so dass es hinter dem Tagesgeschäft zurücksteckt. Dadurch besteht bei unklarer Aufteilung der Zuständigkeiten die Gefahr, dass Informationssicherheit grundsätzlich zu einem "Problem anderer Leute" wird. Damit wird die Verantwortung für Informationssicherheit so lange hin und her geschoben, bis keiner sie mehr zu haben glaubt. Um dies zu vermeiden, sollte ein Haupt-Ansprechpartner für alle Aspekte rund um Informationssicherheit, ein IT-Sicherheitsbeauftragter, ernannt werden, der die Aufgabe "Informationssicherheit" koordiniert und innerhalb der Institution vorantreibt. Ob es neben diesem weitere Personen mit Sicherheitsaufgaben gibt und wie die Informationssicherheit organisiert ist, hängt von der Art und Größe der Institution ab.

Die Rolle des Verantwortlichen für Informationssicherheit wird je nach Art und Ausrichtung der Institution anders genannt. Häufige Titel sind IT-Sicherheitsbeauftragter oder kurz IT-SiBe, Chief Security Officer (CSO), Chief Information Security Officer (CISO) oder Information Security Manager. Mit dem Titel "Sicherheitsbeauftragter" werden dagegen häufig die Personen bezeichnet, die für Arbeitsschutz, Betriebssicherheit oder Werkschutz zuständig sind.

Um einen Sicherheitsprozesses erfolgreich planen, umsetzen und aufrechterhalten zu können, müssen die Verantwortlichkeiten klar definiert werden. Es müssen also Rollen definiert sein, die die verschiedenen Aufgaben für die Erreichung der Informationssicherheitsziele wahrnehmen müssen. Außerdem müssen Personen benannt sein, die qualifiziert sind und denen ausreichend Ressourcen zur Verfügung stehen, um diese Rollen auszufüllen.

Zuständigkeiten und Aufgaben

Der IT-Sicherheitsbeauftragte ist zuständig für die Wahrnehmung aller Belange der Informationssicherheit innerhalb der Institution. Die Hauptaufgabe des IT-Sicherheitsbeauftragten besteht darin, die Behörden- bzw. Unternehmensleitung bei deren Aufgabenwahrnehmung bezüglich der Informations-

sicherheit zu beraten und diese bei der Umsetzung zu unterstützen. Seine Aufgaben umfassen unter anderen:

- den Informationssicherheitsprozess zu steuern und bei allen damit zusammenhängenden Aufgaben mitzuwirken,
- die Leitungsebene bei der Erstellung der Leitlinie zur Informationssicherheit zu unterstützen,
- die Erstellung des Sicherheitskonzepts, des Notfallvorsorgekonzepts und anderer Teilkonzepte und System-Sicherheitsrichtlinien zu koordinieren sowie weitere Richtlinien und Regelungen zur Informationssicherheit zu erlassen,
- die Realisierung von Sicherheitsmaßnahmen zu initiieren und zu überprüfen,
- der Leitungsebene und dem IS-Management-Team über den Status quo der Informationssicherheit zu berichten,
- sicherheitsrelevante Projekte zu koordinieren,
- Sicherheitsvorfälle zu untersuchen und
- Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit zu initiieren und koordinieren.

Der IT-Sicherheitsbeauftragte ist außerdem bei allen größeren Projekten, die deutliche Auswirkungen auf die Informationsverarbeitung haben, sowie bei der Einführung neuer Anwendungen und IT-Systeme zu beteiligen, um die Beachtung von Sicherheitsaspekten in den verschiedenen Projektphasen zu gewährleisten.

Anforderungsprofil

Zur Erfüllung dieser Aufgaben ist es wünschenswert, dass der IT-Sicherheitsbeauftragte über Wissen und Erfahrung in den Gebieten Informationssicherheit und IT verfügt. Da diese Aufgabe eine Vielzahl von Fähigkeiten erfordert, sollte bei der Auswahl außerdem darauf geachtet werden, dass die folgenden Qualifikationen vorhanden sind:

- Identifikation mit den Zielsetzungen der Informationssicherheit, Überblick über Aufgaben und Ziele der Institution
- Kooperations- und Teamfähigkeit, aber auch Durchsetzungsvermögen (Kaum eine Aufgabe erfordert so viel Fähigkeit und Geschick im Umgang mit anderen Personen: Die Leitungsebene muss in zentralen Fragen des Sicherheitsprozesses immer wieder eingebunden werden. Entscheidungen müssen eingefordert werden und die Mitarbeiter müssen, eventuell mit Hilfe des Bereichs-IT-Sicherheitsbeauftragten, in den Sicherheitsprozess mit eingebunden werden.)
- Erfahrungen im Projektmanagement, idealerweise im Bereich der Systemanalyse und Kenntnisse über Methoden zur Risikobewertung

Ein IT-Sicherheitsbeauftragter muss außerdem die Bereitschaft mitbringen, sich in neue Gebiete einzuarbeiten und Entwicklungen in der IT zu verfolgen. Er sollte sich so aus- und fortbilden, dass er die erforderlichen Fachkenntnisse für die Erledigung seiner Aufgaben besitzt.

Kooperation und Kommunikation

Die Zusammenarbeit mit den Mitarbeitern ebenso wie mit Externen verlangt viel Geschick, da diese zunächst von der Notwendigkeit der (für sie manchmal etwas lästigen) Sicherheitsmaßnahmen überzeugt werden müssen. Ein ebenfalls sehr sensibles Thema ist die Befragung der Mitarbeiter nach sicherheitskritischen Vorkommnissen und Schwachstellen. Um den Erfolg dieser Befragungen zu garantieren, müssen die Mitarbeiter davon überzeugt werden, dass ehrliche Antworten nicht zu Problemen für sie selbst führen.

Die Kommunikationsfähigkeiten des IT-Sicherheitsbeauftragten sind nicht nur gegenüber den Mitarbeiter gefordert. Genauso wichtig ist es, dass der IT-Sicherheitsbeauftragte in der Lage ist, seine

fachliche Meinung gegenüber der Behörden- oder Unternehmensleitung zu vertreten. Er muss so selbstbewusst und kommunikationsfähig sein, um gelegentlich auch Einspruch gegen eine Entscheidung einzulegen, die mit dem Ziel eines sicheren IT-Betriebs nicht vereinbar ist.

Unabhängigkeit

Es ist empfehlenswert, die Position des IT-Sicherheitsbeauftragten organisatorisch als Stabsstelle einzurichten, also als eine direkt der Leitungsebene zugeordnete Position, die von keinen anderen Stellen Weisungen bekommt. Es ist z. B. problematisch, wenn ein "aktiver" Administrator sie zusätzlich zu seinen normalen Aufgaben wahrnimmt, da es mit hoher Wahrscheinlichkeit zu Interessenskonflikten kommen wird. Die Personalunion kann dazu führen, dass er als IT-Sicherheitsbeauftragter Einspruch gegen Entscheidungen einlegen müsste, die ihm sein Leben als Administrator wesentlich erleichtern würden oder die gar von seinem Fachvorgesetzten stark favorisiert werden. In jedem Fall muss der IT-Sicherheitsbeauftragte das direkte und jederzeitige Vorspracherecht bei der Behörden- bzw. Unternehmensleitung haben, um diese über Sicherheitsvorfälle, -risiken und –maßnahmen informieren zu können. Er muss aber auch über das Geschehen in der Institution, soweit es einen Bezug zu seiner Tätigkeit hat, umfassend und frühzeitig unterrichtet werden.

Personalunion mit dem Datenschutzbeauftragten

Eine häufige Frage ist, ob die Position des IT-Sicherheitsbeauftragten gleichzeitig vom Datenschutzbeauftragten wahrgenommen werden kann (zu dessen Aufgaben siehe unten). Die beiden Rollen schließen sich nicht grundsätzlich aus, es sind allerdings einige Aspekte im Vorfeld zu klären:

- Die Schnittstellen zwischen den beiden Rollen sollten klar definiert und dokumentiert werden. Außerdem sollten auf beiden Seiten direkte Berichtswege zur Leitungsebene existieren. Weiterhin sollte überlegt werden, ob konfliktträchtige Themen zusätzlich noch nachrichtlich an die Revision weitergeleitet werden sollten.
- Es muss sichergestellt sein, dass der IT-Sicherheitsbeauftragte ausreichend Ressourcen für die Wahrnehmung beider Rollen hat. Gegebenenfalls muss er durch entsprechende Erfüllungsgehilfen unterstützt werden.

Es darf nicht vergessen werden, dass auch der IT-Sicherheitsbeauftragte einen qualifizierten Vertreter benötigt.

3.4.5 Das IS-Management-Team

Das IS-Management-Team unterstützt den IT-Sicherheitsbeauftragten, indem es übergreifende Maßnahmen in der Gesamtorganisation koordiniert, Informationen zusammenträgt und Kontrollaufgaben durchführt. Die genaue Ausprägung hängt von der Größe der jeweiligen Institution, dem angestrebten Sicherheitsniveau und den vorhandenen Ressourcen ab. Im Extremfall besteht das IS-Management-Team nur aus einer einzigen Person, dem IT-Sicherheitsbeauftragten, dem in diesem Fall sämtliche Aufgaben im Sicherheitsprozess obliegen.

Aufgaben des IS-Management-Teams sind insbesondere:

- Informationssicherheitsziele und -strategien zu bestimmen sowie die Leitlinie zur Informationssicherheit zu entwickeln,
- die Umsetzung der Sicherheitsleitlinie zu überprüfen,
- den Sicherheitsprozess zu initiieren, zu steuern und zu kontrollieren,
- bei der Erstellung des Sicherheitskonzepts mitzuwirken,
- zu überprüfen, ob die im Sicherheitskonzept geplanten Sicherheitsmaßnahmen wie beabsichtigt funktionieren sowie geeignet und wirksam sind,
- die Schulungs- und Sensibilisierungsprogramme für Informationssicherheit zu konzipieren sowie
- den IT-Koordinierungsausschuss und die Leitungsebene in Fragen der Informationssicherheit zu beraten.

Zusammensetzung des Teams

Um seine Aufgaben erfüllen zu können, sollte sich das IS-Management-Team aus Personen zusammensetzen, die Kenntnisse in Informationssicherheit, technische Kenntnisse über IT-Systeme sowie Erfahrung mit Organisation und Verwaltung haben. Darüber hinaus sollte das IS-Management-Team die unterschiedlichen Aufgabenbereiche einer Organisation widerspiegeln. Im IS-Management-Team sollten mindestens folgende Rollen vertreten sein: ein IT-Verantwortlicher, der IT-Sicherheitsbeauftragte und ein Vertreter der Anwender. Da häufig auch personenbezogene Daten betroffen sind, sollte der Datenschutzbeauftragte ebenfalls Mitglied des IS-Management-Teams sein. Gibt es in der Organisation bereits ein ähnliches Gremium, könnten dessen Aufgaben entsprechend erweitert werden. Um die Bedeutung der Informationssicherheit zu unterstreichen, ist es jedoch ratsam, ein IS-Management-Team einzurichten und dieses mit angemessenen Ressourcen auszustatten.

3.4.6 Bereichs-IT-Sicherheitsbeauftragte, Projekt- bzw. IT-System-Sicherheitsbeauftragte

Bei großen Organisationen kann es erforderlich sein, in den verschiedenen Bereichen eigene IT-Sicherheitsbeauftragte einzusetzen. Der Bereichs-IT-Sicherheitsbeauftragte ist für alle Sicherheitsbelange der Geschäftsprozesse, Anwendungen und IT-Systeme in seinem Bereich (z. B. Abteilung oder Außenstelle) verantwortlich. Je nach Größe des zu betreuenden Bereiches kann die Aufgabe des Bereichs-IT-Sicherheitsbeauftragten von einer Person übernommen werden, die bereits mit ähnlichen Aufgaben betraut ist, z. B. dem Bereichs-IT-Beauftragten (falls vorhanden). Auf jeden Fall ist bei der Auswahl des Bereichs-IT-Sicherheitsbeauftragten darauf zu achten, dass er die Aufgaben, Gegebenheiten und Arbeitsabläufe in dem zu betreuenden Bereich gut kennt.

Die verschiedenen Geschäftsprozesse, Anwendungen und IT-Systeme einer Institution haben oft verschiedene Sicherheitsanforderungen, die unter Umständen in spezifischen Sicherheitsleitlinien zusammengefasst sind und unterschiedlicher Sicherheitsmaßnahmen bedürfen. Analoges trifft für den Projekt-Sicherheitsbeauftragten zu, mit dem Unterschied, dass es sich bei den Aufgaben um projektspezifische statt IT-systemspezifische handelt.

Als Aufgaben der Projekt-, IT-System- bzw. Bereichs-Sicherheitsbeauftragten sind festzuhalten:

- die Vorgaben des IT-Sicherheitsbeauftragten umsetzen,
- die Sicherheitsmaßnahmen gemäß IT-System-Sicherheitsleitlinie oder anderer spezifischer Sicherheitsleitlinien umsetzen,
- projekt- oder IT-systemspezifische Informationen zusammenfassen und an den IT-Sicherheitsbeauftragten weiterleiten,
- als Ansprechpartner der Mitarbeiter vor Ort dienen,
- bei der Auswahl der Sicherheitsmaßnahmen zur Umsetzung der spezifischen Sicherheitsleitlinien mitwirken,
- Information über Schulungs- und Sensibilisierungsbedarf von Beschäftigten ermitteln,
- Protokolldateien regelmäßig kontrollieren und auswerten sowie
- eventuell auftretende sicherheitsrelevante Zwischenfälle an den IT-Sicherheitsbeauftragten melden.

Anforderungsprofil

Folgende Qualifikationen sollten vorhanden sein:

- detaillierte IT-Kenntnisse, da diese die Gespräche mit Mitarbeitern vor Ort erleichtern und bei der Suche nach Sicherheitsmaßnahmen für die speziellen IT-Systeme von Nutzen sind, sowie
- Kenntnisse im Projektmanagement, die bei der Organisation von Benutzerbefragungen und der Erstellung von Plänen zur Umsetzung und der Kontrolle von Sicherheitsmaßnahmen hilfreich sind.

3.4.7 IT-Koordinierungsausschuss

Der IT-Koordinierungsausschuss ist in der Regel keine Dauereinrichtung in einer Institution, sondern wird bei Bedarf (z. B. zur Planung größerer IT-Projekte) einberufen. Er hat die Aufgabe, das Zusammenspiel zwischen dem IS-Management-Team, dem Vertreter der IT-Anwender, dem IT-Sicherheitsbeauftragten und der Behörden- bzw. Unternehmensleitung zu koordinieren.

3.4.8 Der Datenschutzbeauftragte

Der Datenschutz wird oft nachrangig behandelt, da er vermeintlich die effektive Informationsverarbeitung behindert, obwohl er in Deutschland und in vielen anderen Ländern auf gesetzlichen Vorschriften beruht und Verletzungen des damit verbundenen informationellen Selbstbestimmungsrechts empfindliche Geldbußen und Freiheitsstrafen nach sich ziehen kann.

Oft werden die Aufgaben des Datenschutzbeauftragten Personen übertragen, die aber bereits eine andere Rolle innehaben, mit der in der neuen Funktion auch eine Interessenkollision auftreten kann, indem sie sich beispielsweise in ihrer ursprünglichen Funktion selbst kontrollieren (z. B. IT-Leiter).

Um dies zu vermeiden, sollte ein kompetenter und qualifizierter Ansprechpartner für Datenschutzfragen ernannt werden, der alle Aspekte des Datenschutzes innerhalb der Institution begleitet und für eine angemessene Umsetzung und ausreichende Kontrolle sorgt. In dieser Funktion arbeitet er eng mit dem IT-Sicherheitsbeauftragten zusammen, gehört zum IS-Management-Team, ist weisungsunabhängig und berichtet direkt der Behörden- bzw. Unternehmensleitung.

Bei angemessener Verwirklichung wird der Datenschutz Arbeitsabläufe im Ergebnis eher fördern als erschweren. Wenn nämlich eine Behörde bzw. ein Unternehmen zu viele personenbezogene Daten sammelt, personenbezogene Daten zu spät löscht oder unberechtigt übermittelt, verstößt sie nicht nur gegen Datenschutzrecht, sondern verursacht auch erhöhten Verwaltungsaufwand und Mehrkosten. Vor allem ist der Datenschutz ein wichtiges Element eines bürger- und kundenfreundlichen Verhaltens, weil er die Verfahrensabläufe transparent macht.

Jede Institution sollte einen Datenschutzbeauftragten ernennen. In vielen Bereichen ist die Bestellung eines Datenschutzbeauftragten sogar gesetzlich vorgeschrieben. Auch in Institutionen, die keinen Datenschutzbeauftragten benannt haben, muss die Einhaltung der datenschutzrechtlichen Anforderungen sichergestellt sein. Dies kann auch durch das IS-Management-Team oder die interne Revision erfolgen.

Anforderungsprofil

Zum Datenschutzbeauftragten kann nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Zur Aufgabenerfüllung gehören technische, organisatorische und rechtliche Kenntnisse. Der Datenschutzbeauftragte muss die jeweiligen gesetzlichen Regelungen, bereichsspezifische datenschutzrechtliche Regelungen und die für die Institution einschlägigen Spezialvorschriften kennen und sicher anwenden können. Eine wichtige Rechtsnorm ist in Deutschland insbesondere das Bundesdatenschutzgesetz. Der Datenschutzbeauftragte sollte ferner gute Kenntnisse der Organisation und vertiefte Kenntnisse der Informationstechnik besitzen. Soweit ihm die fachliche Qualifikation in Teilbereichen noch fehlt, ist ihm Gelegenheit zu geben, sich entsprechend weiterzubilden. Mit den Aufgaben und der Arbeitsweise seiner Behörde bzw. seines Unternehmens sollte der Datenschutzbeauftragte möglichst aus eigener Erfahrung gut vertraut sein, um seinen Kontroll- und Beratungsaufgaben nachkommen zu können.

Der Datenschutzbeauftragte muss nicht ausschließlich mit diesen Funktionen betraut sein. Je nach Art und Umfang der personenbezogenen Datenverarbeitung und der damit verbundenen Datenschutzprobleme kann es angebracht sein, ihm daneben weitere Aufgaben zu übertragen. Dies wird besonders bei kleineren Institutionen in Betracht kommen. Besonders ist darauf zu achten, dass keine Interessenkonflikte oder Abhängigkeiten entstehen, die seine Aufgabenerfüllung gefährden. Möglich ist auch die Zusammenlegung der Funktionen des Datenschutzbeauftragten mit denen des IT-Sicherheitsbeauftragten.

Einbeziehungspflicht

Der Datenschutzbeauftragte muss das direkte und jederzeitige Vortragsrecht bei der Behörden- bzw. Unternehmensleitung haben und über das Geschehen in der Behörde bzw. dem Unternehmen, soweit es einen Bezug zu seiner Tätigkeit hat, umfassend und frühzeitig unterrichtet werden. Er ist an datenschutzrelevanten Vorgängen zu beteiligen, und Planungen, die den Umgang mit personenbezogenen Daten betreffen, sind ihm bekannt zu geben. Bei Bedarf muss er von anderen Mitarbeitern mit weitergehenden rechtlichen oder technischen Kenntnissen unterstützt werden.

Zuständigkeiten und Aufgaben

Der Datenschutzbeauftragte soll dazu beitragen, dass seine Institution den Erfordernissen des Datenschutzes umfassend Rechnung trägt. Er hat die Einhaltung der Vorschriften des Datenschutzes in allen Bereichen zu überwachen. Er nimmt seine Aufgaben im Wesentlichen durch Beratung und Kontrollen wahr. Seine vorrangige Aufgabe ist die Beratung. Für die Mitarbeiter sollte der Datenschutzbeauftragte Ansprechpartner in allen Fragen des Datenschutzes sein, an den sie sich jederzeit vertrauensvoll wenden können. Bei Schwachstellen und Versäumnissen sollte er zunächst gemeinsam mit den Beteiligten nach konstruktiven Lösungen suchen.

Der Datenschutzbeauftragte hilft der Behörden- bzw. Unternehmensleitung, ihre Verantwortung für die Wahrung des Persönlichkeitsschutzes wahrzunehmen und Zwischenfälle zu vermeiden, die dem Ansehen der Institution abträglich wären. Er sollte auch Kontakt zum Personal- bzw. Betriebsrat halten. Eine gute Zusammenarbeit ist nicht nur wegen der Sensibilität der Personaldatenverarbeitung wünschenswert.

Der spezielle Zuschnitt der Aufgaben des Datenschutzbeauftragten richtet sich im Einzelfall nach den zu erfüllenden Aufgaben, aber auch nach Größe, dem Aufbau und der Gliederung der jeweiligen Behörde bzw. des Unternehmens.

Aktionspunkte zu 3.4 Aufbau einer IS-Organisation
• Rollen für die Gestaltung des Informationssicherheitsprozesses festlegen
• Aufgaben und Verantwortungsbereiche den Rollen zuordnen
• Personelle Ausstattung der Rollen festlegen
• IS-Organisation dokumentieren
• Informationssicherheitsmanagement in die organisationsweiten Abläufe und Prozesse integrieren

3.5 Bereitstellung von Ressourcen für die Informationssicherheit

Bedrohungen können Schäden und damit Kosten verursachen, Risikovorsorge kostet aber auch Ressourcen – ein effektives Risikomanagement hilft, diese Kosten zu steuern. Ein angemessenes Maß an Informationssicherheit ist immer nur mit einem entsprechenden Aufwand zu erreichen und aufrechtzuerhalten. Deshalb ist beim Festlegen des Sicherheitsniveaus und bei der Formulierung konkreter Sicherheitsanforderungen für die jeweilige Institution darauf zu achten, dass das angestrebte Sicherheitsniveau auch wirtschaftlich sinnvoll ist.

3.5.1 Kosteneffiziente Sicherheitsstrategie

Bei der Ausgestaltung der Sicherheitsstrategie sind von vornherein Wirtschaftlichkeitsaspekte zu berücksichtigen. Stellt sich heraus, dass die notwendigen Sicherheitsmaßnahmen mit den zur Verfügung stehenden Ressourcen nicht umzusetzen sind, muss die Strategie geändert werden. Wenn Anspruch und finanzielle Möglichkeiten zu weit auseinander liegen, müssen Geschäftsprozesse oder die Art und Weise des IT-Betriebs grundsätzlich überdacht werden.

Die Erfahrung zeigt, dass das Verhältnis zwischen dem Aufwand, der zur Erhöhung des Sicherheitsniveaus erforderlich ist, und dem dadurch erreichten Sicherheitsgewinn immer ungünstiger wird, je höher das angestrebte Sicherheitsniveau ist. Absolut perfekte Informationssicherheit ist nicht erreich-

bar. Das nachstehende Diagramm soll verdeutlichen, wie viel Aufwand in Relation zum angestrebten Sicherheitsniveau zu betreiben ist. Dieser Aufwand bietet eine Orientierung für die personellen, zeitlichen und monetären Ressourcen, die zur Erreichung dieses Sicherheitsniveaus notwendig sind.

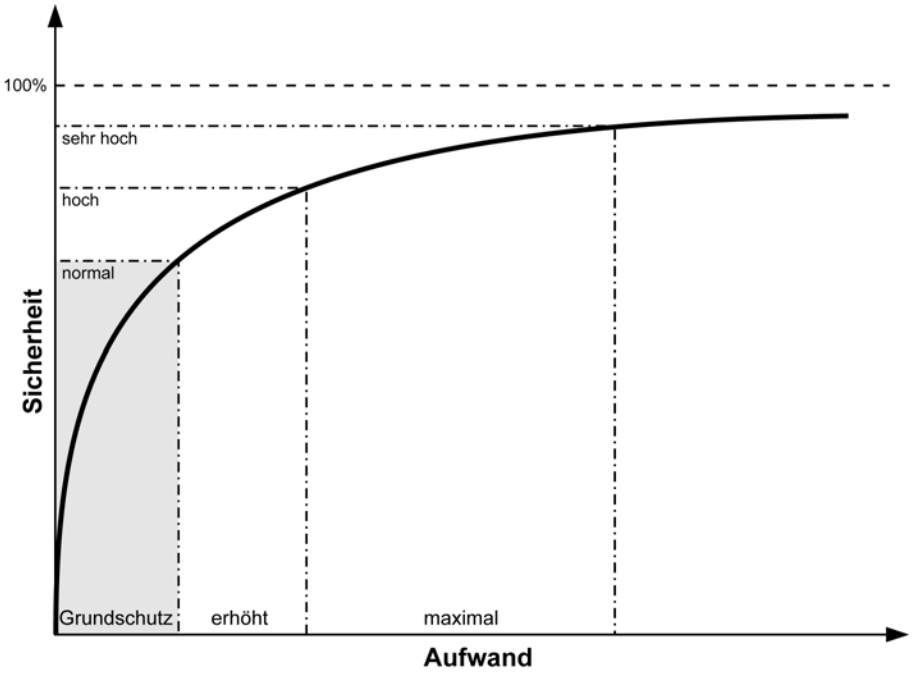


Abbildung 4: Aufwand-Nutzen-Relation für Informationssicherheit

Es ist unbedingt notwendig, bei der Auswahl der einzelnen Schritte im Sicherheitsprozess auf die Kosten-Nutzen-Aspekte jeder Maßnahme genau zu achten. Zur erheblichen Verbesserung des Sicherheitsniveaus tragen oft einfache organisatorische Regelungen bei, die ohne viel Aufwand oder zusätzliche technische Ausrüstung zu implementieren sind. Erst nachdem diese elementaren Sicherheitsmaßnahmen realisiert wurden, ist die Investition in technische und aufwendige Sicherheitsinfrastrukturen sinnvoll.

Informationssicherheit erfordert finanzielle, personelle und zeitliche Ressourcen, die vom Management den formulierten Anforderungen entsprechend bereitgestellt werden müssen. Häufig werden mit IT-Sicherheit ausschließlich technische Lösungen verbunden. Auch dies ist ein Grund, besser den Begriff Informationssicherheit zu benutzen. Vor allem ist es aber wichtig, darauf hinzuweisen, dass Investitionen in personelle Ressourcen und organisatorische Regelungen häufig effektiver sind als Investitionen in Sicherheitstechnik. Technik alleine löst keine Probleme, technische Maßnahmen müssen immer in einen geeigneten organisatorischen Rahmen eingebunden werden.

3.5.2 Ressourcen für die IS-Organisation

Umfragen zur Informationssicherheit zeigen, dass die Berufung eines IT-Sicherheitsbeauftragten häufig die effektivste Sicherheitsmaßnahme ist. Nach der Bestellung eines IT-Sicherheitsbeauftragten geht in den meisten Institutionen die Anzahl an Sicherheitsvorfällen signifikant zurück. Damit der IT-Sicherheitsbeauftragte seinen Aufgaben nachkommen kann, muss er vor allem ausreichend Zeit für seine Arbeit zugebilligt bekommen. In kleineren Institutionen ist es möglich, dass ein Mitarbeiter die Aufgaben des IT-Sicherheitsbeauftragten in Personalunion neben seinen eigentlichen Tätigkeiten wahrnimmt.

Nur wenige Institutionen, entweder sehr große oder solche mit einem hohen Bedarf an Informationssicherheit, werden die Möglichkeit haben, hauptamtliche Stellen für ein IS-Management-Team bereitstellen zu können. Im Allgemeinen werden diese Aufgaben von den Mitarbeitern neben den originären Aufgaben wahrzunehmen sein. Eine Ausnahme stellt hier jedoch die erstmalige Einrichtung des Sicherheitsprozesses dar. Wenn möglich, sollten die Mitglieder des IS-Management-Teams

während dieser Phase weitgehend von ihren sonstigen Aufgaben freigestellt werden. Es hängt von der Aufgabenverteilung zwischen dem IS-Management-Team und dem IT-Sicherheitsbeauftragten ab, ob und inwieweit diese Freistellung auch danach noch sinnvoll ist. Die letztendliche Entscheidung hierfür liegt bei der Behörden- bzw. Unternehmensleitung. In jedem Fall sollte das IS-Management-Team regelmäßig tagen, um eine kontinuierliche Steuerung des Sicherheitsprozesses zu gewährleisten.

Die Einrichtung eines IS-Management-Teams hat den Vorteil, dass verschiedene Organisationseinheiten in den Sicherheitsprozess einbezogen und Kompetenzen gebündelt werden. Dadurch kann Informationssicherheit schneller in allen Organisationseinheiten umgesetzt werden und es entstehen weniger Reibungsverluste. Beispielsweise könnten die folgenden Organisationseinheiten beteiligt werden und die Sicherheitsaktivitäten koordinieren: Informationssicherheit, Revision, IT-Administration, IT-Leitung, Datenschutz, Personal-/Betriebsrat, Fachabteilung, Haus- und Gebäudetechnik, Rechtsabteilung, Finanzabteilung.

Zugriff auf externe Ressourcen

In der Praxis fehlt den internen Sicherheitsexperten häufig die Zeit, um alle sicherheitsrelevanten Einflussfaktoren und Rahmenbedingungen (z. B. gesetzliche Anforderungen oder technische Fragen) zu analysieren. Teilweise fehlen ihnen auch die entsprechenden Grundlagen. In diesen Fällen ist es sinnvoll, auf externe Experten zurückzugreifen. Dies muss von den internen Sicherheitsexperten dokumentiert werden, damit die Leitungsebene die erforderlichen Ressourcen bereitstellt.

Auch das Auslagern von Teilen des IT-Betriebs oder bestimmter Dienstleistungen, wie beispielsweise dem Firewall-Betrieb, kann die Informationssicherheit erhöhen, wenn dadurch auf Spezialisten zurückgegriffen werden kann, die intern nicht zur Verfügung stehen. Der Baustein B 1.11 Outsourcing der IT-Grundschutz-Kataloge gibt Empfehlungen, was hierbei aus Sicherheitssicht zu beachten ist.

3.5.3 Ressourcen für die Überprüfung der Informationssicherheit

Weiterhin müssen ausreichend Ressourcen bereitgestellt werden, damit die Wirksamkeit und Eignung von Sicherheitsmaßnahmen systematisch überprüft werden können. Nach Möglichkeit sollte auch geprüft werden, ob die eingesetzten Ressourcen in einem sinnvollen Verhältnis zum Sicherheitsnutzen stehen. Stellt sich z. B. heraus, dass die Sicherung bestimmter IT-Systeme unwirtschaftlich hohe Kosten verursacht, sollten alternative Maßnahmen gesucht werden. Es kann beispielsweise sinnvoll sein, bestimmte IT-Systeme nicht an unsichere Netze anzuschließen, wenn der Aufwand zur Sicherung zu hoch ist.

3.5.4 Ressourcen für den IT-Betrieb

Grundvoraussetzung für einen sicheren IT-Betrieb ist, dass dieser reibungslos funktioniert, also vernünftig geplant und organisiert ist. Für den IT-Betrieb müssen daher ausreichende Ressourcen zur Verfügung gestellt werden. Typische Probleme des IT-Betriebs (knappe Ressourcen, überlastete Administratoren oder eine unstrukturierte und schlecht gewartete IT-Landschaft) müssen in der Regel gelöst werden, damit die eigentlichen Sicherheitsmaßnahmen wirksam und effizient umgesetzt werden können.

Aktionspunkte zu 3.5 Bereitstellung von Ressourcen für die Informationssicherheit

- Angemessenheit und Wirtschaftlichkeit im gesamten Sicherheitsprozess berücksichtigen
- Gleichgewicht zwischen organisatorischer und technischer Informationssicherheit sicherstellen
- Angemessene Ressourcen für den IT-Betrieb, das Informationssicherheitsmanagement und die Überprüfung der Informationssicherheit einfordern
- Gegebenenfalls auf externe Ressourcen zurückgreifen

3.6 Einbindung aller Mitarbeiter in den Sicherheitsprozess

Informationssicherheit betrifft ohne Ausnahme alle Mitarbeiter. Jeder Einzelne kann durch verantwortungs- und sicherheitsbewusstes Handeln dabei helfen, Schäden zu vermeiden und zum Erfolg beitragen. Sensibilisierung für Informationssicherheit und fachliche Schulungen der Mitarbeiter sind daher eine Grundvoraussetzung für Informationssicherheit. Auch das Arbeitsklima, gemeinsame Wertvorstellungen und das Engagement der Mitarbeiter beeinflussen entscheidend die Informationssicherheit.

Bei allen Mitarbeitern, internen wie externen, müssen von der Personalauswahl bis zum Weggang der Mitarbeiter ebenfalls Aspekte der Informationssicherheit beachtet werden.

3.6.1 Schulung und Sensibilisierung

Alle Mitarbeiter müssen in Hinblick auf die Bedeutung von Sicherheitsmaßnahmen und ihre Anwendung geschult und sensibilisiert werden. Dafür müssen Schulungskonzepte für verschiedene Zielgruppen (z. B. Administratoren, Manager, Anwender, Wachpersonal) erstellt werden. Die Schulungen zu Informationssicherheit müssen dabei in bestehende Schulungskonzepte integriert werden.

Grundsätzlich müssen alle Mitarbeiter, die neu eingestellt oder denen neue Aufgaben zugewiesen wurden, gründlich eingearbeitet und ausgebildet werden. Bei der Gestaltung bzw. Auswahl der entsprechenden Schulungsmaßnahmen sollten alle relevanten Sicherheitsaspekte integriert werden. Auch erfahrene IT-Benutzer sollten in regelmäßigen Abständen ihr Wissen auffrischen und ergänzen.

Mitarbeiter müssen regelmäßig für Informationssicherheit sensibilisiert werden, um das Bewusstsein für die Risiken im alltäglichen Umgang mit Informationen zu schärfen. Um eine wirksame Sensibilisierung für Informationssicherheit zu erreichen, ist es beispielsweise sinnvoll, ein Sicherheitsforum im Intranet einzurichten, in dem Tipps zu Sicherheitsmaßnahmen und aktuelle Schadensfälle veröffentlicht werden, den Mitarbeitern Workshops oder Vorträge zu Informationssicherheit anzubieten oder Fachzeitschriften verfügbar zu machen.

3.6.2 Kommunikation, Einbindung und Meldewege

Damit die Mitarbeiter auch nach den Schulungs- und Sensibilisierungsmaßnahmen den Bezug zu Sicherheitsthemen behalten, ist es wichtig, Ansprechpartner zu Sicherheitsfragen festzulegen und diese Zuständigkeiten bekannt zu machen. Nur so können die Mitarbeiter aktiv unterstützt werden und Sicherheitsrichtlinien und -konzepte in der Praxis und auf Dauer umsetzen. Dazu gehört auch die Definition von Melde- und Eskalationswegen für Sicherheitsvorfälle. Jeder Mitarbeiter muss wissen, wie er sich bei Verdacht auf einen Sicherheitsvorfall verhalten muss und wer der zuständige Ansprechpartner ist. Zusätzlich muss es möglich sein, diese Informationen schnell und unter allen Umständen in Erfahrung zu bringen, beispielsweise auch, wenn keine IT mehr zur Verfügung steht.

Mitarbeiter müssen über den Sinn von Sicherheitsmaßnahmen aufgeklärt werden. Dies ist besonders wichtig, wenn sie Komfort- oder Funktionseinbußen zur Folge haben. Im Einzelfall können gerade Sicherheitsmaßnahmen mitbestimmungspflichtig sein, so dass eine Beteiligung von Personal- oder Betriebsrat sogar vorgeschrieben ist.

Werden Mitarbeiter frühzeitig bei Planung von Sicherheitsmaßnahmen oder der Gestaltung organisatorischer Regelungen beteiligt, hat dies mehrere Vorteile:

- Das vorhandene Wissen und Ideen aus der eigenen Institution werden besser ausgenutzt.
- Die Praxistauglichkeit und Effizienz von Sicherheitsmaßnahmen oder organisatorischen Regelungen wird erhöht.
- Die Bereitschaft, Vorgaben und Maßnahmen im Alltagsbetrieb tatsächlich zu befolgen, steigt.
- Das Arbeitsklima wird positiv beeinflusst, wenn Mitarbeiter sich in die Entscheidungen des Managements eingebunden fühlen.

3.6.3 Aufgabenwechsel oder Weggang von Mitarbeitern

Wenn Mitarbeiter die Institution verlassen, andere Aufgaben übernehmen oder Zuständigkeiten verlieren, muss dies durch geeignete Sicherheitsmaßnahmen begleitet und dokumentiert werden. In der Regel müssen mehrere Stellen in einer Institution über den Aufgabenwechsel oder den Weggang eines Mitarbeiters informiert werden und entsprechende Aktionen durchführen, wie z. B. die Rückgabe von Schlüsseln und Ausweisen einfordern, die Zugriffsrechte auf Anwendungen und Informationen anpassen, die Pförtner und weiteres Personal informieren usw. Damit keine Sicherheitsrisiken entstehen, sollte das Identitäts- und Berechtigungsmanagement als Prozess klar definiert sein, z. B. in Form einer Anleitung oder Checkliste. Wenn der Mitarbeiter Funktionen im Sicherheitsprozess hatte, so müssen hier auch die entsprechenden Unterlagen wie beispielsweise der Notfallplan aktualisiert werden.

Des Weiteren ist es sinnvoll, die Mitarbeiter im Vorfeld (z. B. im Rahmen einer Dienstvereinbarung) über ihre Verpflichtungen bei einem Aufgabenwechsel oder bei der Beendung des Arbeitsverhältnisses zu informieren. Hierzu gehört unter anderem ein Hinweis auf ihre Verschwiegenheitspflichten.

Aktionspunkte zu 3.6 Einbindung aller Mitarbeiter in den Sicherheitsprozess

- Frühzeitig die Mitarbeiter und den Personal- bzw. Betriebsrat bei der Planung und Gestaltung von Sicherheitsmaßnahmen und Regelungen beteiligen
- Alle Mitarbeiter für die sie betreffenden Aspekte der Informationssicherheit schulen und regelmäßig sensibilisieren
- Alle Mitarbeiter über den Sinn von Sicherheitsmaßnahmen aufklären
- Ansprechpartner zu Sicherheitsfragen festlegen und Zuständigkeiten bekannt geben
- Melde- und Eskalationswege für Sicherheitsvorfälle festlegen und bekannt geben
- Sicherstellen, dass bei Ausscheiden oder Aufgabenwechsel von Mitarbeitern die erforderlichen Sicherheitsmaßnahmen eingehalten werden

4 Erstellung einer Sicherheitskonzeption nach IT-Grundschutz

Eines der Ziele des IT-Grundschutzes ist es, eine pragmatische und effektive Vorgehensweise zur Erzielung eines normalen Sicherheitsniveaus anzubieten, das auch als Basis für ein höheres Sicherheitsniveau dienen kann. Nachdem ein Informationssicherheitsprozess initiiert wurde und die Sicherheitsleitlinie und Informationssicherheitsorganisation definiert wurden, wird die Sicherheitskonzeption für die Institution erstellt. Zu diesem Zweck werden in den IT-Grundschutz-Katalogen für typische Komponenten von Geschäftsprozessen, Anwendungen und IT-Systeme organisatorische, personelle, infrastrukturelle und technische Standard-Sicherheitsmaßnahmen empfohlen. Diese sind in Bausteinen strukturiert, so dass sie modular aufeinander aufsetzen.

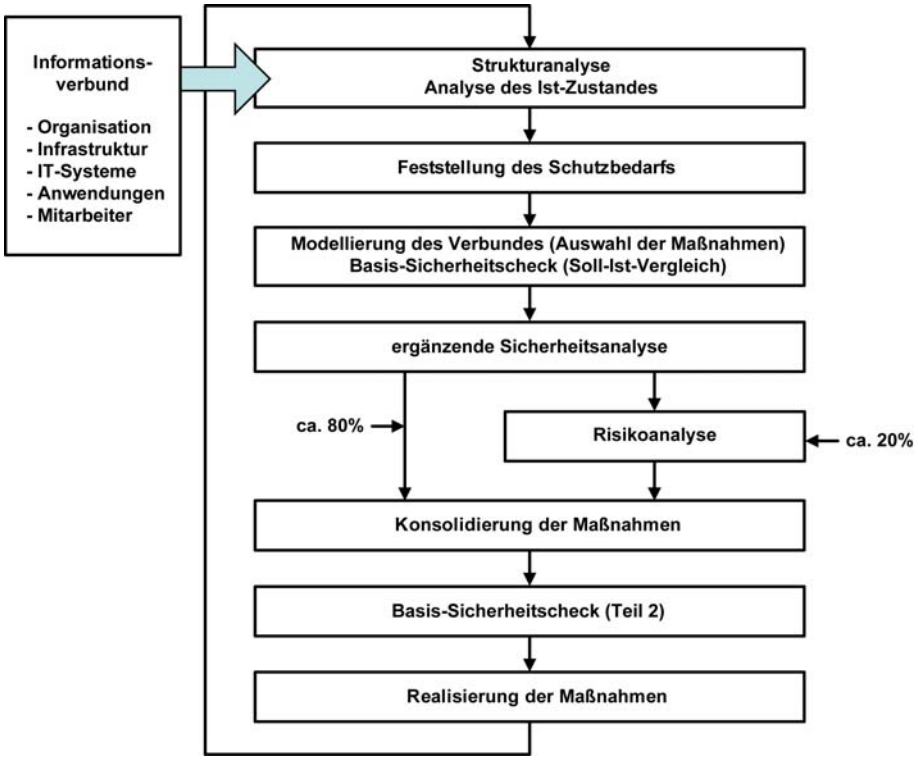


Abbildung 5: Erstellung der Sicherheitskonzeption im Informationssicherheitsmanagement

Die Methodik des IT-Grundschutzes

Bei der traditionellen Risikoanalyse werden zunächst die Bedrohungen ermittelt und mit Eintrittswahrscheinlichkeiten bewertet, um dann die geeigneten Sicherheitsmaßnahmen auszuwählen und anschließend noch das verbleibende Restrisiko bewerten zu können. Diese Schritte sind beim IT-Grundschutz bereits für jeden Baustein durchgeführt und die für typische Einsatzszenarien passenden Sicherheitsmaßnahmen ausgewählt worden. Bei Anwendung des IT-Grundschutzes reduziert sich die Analyse auf einen Soll-Ist-Vergleich zwischen den in den IT-Grundschutz-Katalogen empfohlenen und den bereits realisierten Maßnahmen. Dabei festgestellte fehlende oder nur unzureichend umgesetzte Maßnahmen zeigen die Sicherheitsdefizite auf, die es durch die empfohlenen Maßnahmen zu beheben gilt. Erst bei einem signifikant höheren Schutzbedarf muss zusätzlich eine ergänzende Sicherheitsanalyse unter Beachtung von Kosten- und Wirksamkeitsaspekten durchgeführt werden. In der Regel reicht es hierbei aus, die Maßnahmenempfehlungen der IT-Grundschutz-Kataloge durch entsprechende individuelle, qualitativ höherwertige Maßnahmen zu ergänzen. Hierzu ist im BSI-Standard 100-3 "Risikoanalyse auf der Basis von IT-Grundschutz" [BSI3] eine im Vergleich zu traditionellen Risikoanalyse-Methoden einfachere Vorgehensweise beschrieben.

Die Erstellung einer Sicherheitskonzeption nach IT-Grundschutz gliedert sich grob in folgende Bereiche:

Definition des Geltungsbereichs

Die Umsetzung von IT-Grundschutz in einem einzelnen großen Schritt ist oft ein zu ehrgeiziges Ziel. Viele kleine Schritte und ein langfristiger, kontinuierlicher Verbesserungsprozess ohne hohe Investitionskosten zu Beginn sind oft Erfolg versprechender. So kann es besser sein, zunächst nur in ausgewählten Bereichen das erforderliche Sicherheitsniveau umzusetzen. Von diesen Keimzellen ausgehend sollte dann kontinuierlich die Sicherheit in der Gesamtorganisation verbessert werden.

Zunächst muss daher der Bereich festgelegt werden, für den die Sicherheitskonzeption erstellt und umgesetzt werden soll. Dies können beispielsweise bestimmte Organisationseinheiten einer Institution sein. Es könnten aber auch Bereiche sein, die definierte Geschäftsprozesse oder Fachaufgaben bearbeiten, inklusive der dafür notwendigen Infrastruktur.

Im IT-Grundschutz wird der Geltungsbereich für die Sicherheitskonzeption auch als "Informationsverbund" bezeichnet.

Strukturanalyse

Für die Erstellung eines Sicherheitskonzepts und insbesondere für die Anwendung der IT-Grundschutz-Kataloge ist es erforderlich, das Zusammenspiel der Geschäftsprozesse, der Anwendungen und der vorliegenden Informationstechnik zu analysieren und zu dokumentieren. Aufgrund der heute üblichen starken Vernetzung von IT-Systemen bietet sich ein Netztopologieplan als Ausgangsbasis für die weitere technische Analyse an. Die folgenden Aspekte müssen berücksichtigt werden:

- im Informationsverbund betriebene Anwendungen und die dadurch gestützten Geschäftsprozesse,
- die organisatorischen und personellen Rahmenbedingungen für den Informationsverbund,
- im Informationsverbund eingesetzte vernetzte und nicht-vernetzte IT-Systeme,
- die Kommunikationsverbindungen zwischen den IT-Systemen und nach außen,
- die vorhandene Infrastruktur.

Die einzelnen Schritte der Strukturanalyse werden im Detail in Kapitel 4.2 dieses Dokuments in Form einer Handlungsanweisung beschrieben.

Schutzbedarfsfeststellung

Zweck der Schutzbedarfsfeststellung ist es, zu ermitteln, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist. Hierzu werden für jede Anwendung und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit entstehen können. Wichtig ist es dabei auch, die möglichen Folgeschäden realistisch einzuschätzen. Bewährt hat sich eine Einteilung in die drei Schutzbedarfskategorien "normal", "hoch" und "sehr hoch".

Die einzelnen Schritte der Schutzbedarfsfeststellung werden im Detail in Kapitel 4.3 dieses Dokuments erläutert.

Auswahl und Anpassung von Maßnahmen

Voraussetzung für die Anwendung der IT-Grundschutz-Kataloge auf einen Informationsverbund sind detaillierte Unterlagen über seine Struktur und den Schutzbedarf der darin enthaltenen Zielobjekte. Diese Informationen sollten über die zuvor beschriebenen Arbeitsschritte ermittelt werden. Um geeignete Sicherheitsmaßnahmen für den vorliegenden Informationsverbund identifizieren zu können, müssen anschließend die Bausteine der IT-Grundschutz-Kataloge auf die Zielobjekte und Teilbereiche abgebildet werden.

Dieser Vorgang der Modellierung wird in Kapitel 4.4 detailliert beschrieben.

Basis-Sicherheitscheck

Der Basis-Sicherheitscheck ist ein Organisationsinstrument, welches einen schnellen Überblick über das vorhandene Sicherheitsniveau bietet. Mit Hilfe von Interviews wird der Status quo eines bestehenden (nach IT-Grundschutz modellierten) Informationsverbunds in Bezug auf den Umsetzungsgrad

von Sicherheitsmaßnahmen des IT-Grundschutzes ermittelt. Als Ergebnis liegt ein Katalog vor, in dem für jede relevante Maßnahme der Umsetzungsstatus "entbehrlich", "ja", "teilweise" oder "nein" erfasst ist. Durch die Identifizierung von noch nicht oder nur teilweise umgesetzten Maßnahmen werden Verbesserungsmöglichkeiten für die Sicherheit der betrachteten Geschäftsprozesse und der Informationstechnik aufgezeigt.

Kapitel 4.5 beschreibt einen Aktionsplan für die Durchführung eines Basis-Sicherheitschecks. Dabei wird sowohl den organisatorischen Aspekten als auch den fachlichen Anforderungen bei der Projektdurchführung Rechnung getragen.

Weiterführende Sicherheitsmaßnahmen

Die Standard-Sicherheitsmaßnahmen nach IT-Grundschutz bieten im Normalfall einen angemessenen und ausreichenden Schutz. Bei hohem oder sehr hohem Schutzbedarf kann es jedoch sinnvoll sein, zu prüfen, ob zusätzlich oder ersatzweise höherwertige Sicherheitsmaßnahmen erforderlich sind. Dies gilt auch, wenn besondere Einsatzbedingungen vorliegen oder wenn Komponenten verwendet werden, die nicht mit den existierenden Bausteinen der IT-Grundschutz-Kataloge abgebildet werden können. Hierzu ist zunächst im Rahmen einer *ergänzenden Sicherheitsanalyse* zu entscheiden, ob für die jeweils betroffenen Bereiche eine Risikoanalyse durchgeführt werden muss.

Eine Methode für Risikoanalysen ist die im BSI-Standard 100-3 "Risikoanalyse auf der Basis von IT-Grundschutz" beschriebene Vorgehensweise. In Kapitel 4.6 wird diese Methode überblicksartig dargestellt. Die erfolgreiche Durchführung einer Risikoanalyse hängt entscheidend von den Fachkenntnissen des Projektteams ab. Daher ist es häufig sinnvoll, fachkundiges externes Personal hinzuzuziehen.

4.1 Definition des Geltungsbereichs

Vor der Erstellung einer Sicherheitskonzeption muss zuerst festgelegt werden, welchen Bereich der Institution sie abdecken soll, also welchen Geltungsbereich sie haben soll. Dieser kann identisch mit dem Geltungsbereich der Leitlinie zur Informationssicherheit sein, es kann jedoch auch sinnvoll sein, Sicherheitskonzeptionen für kleinere Bereiche zu entwickeln. Dies kann beispielsweise der Fall sein, wenn der Aufwand für eine Gesamterstellung im ersten Schritt als zu hoch eingeschätzt wird und bestimmte Geschäftsprozesse gemäß der Sicherheitsleitlinie priorisiert behandelt werden müssen.

Es sollten nicht nur technische, sondern auch organisatorische Aspekte bei der Abgrenzung des Geltungsbereichs berücksichtigt werden, damit die Verantwortung und die Zuständigkeiten eindeutig festgelegt werden können. In jedem Fall sollte klar sein, welche Informationen, Fachaufgaben oder Geschäftsprozesse in der Sicherheitskonzeption explizit betrachtet werden.

Bei der Abgrenzung des Geltungsbereichs für die Sicherheitskonzeption müssen folgende Faktoren berücksichtig werden:

- Der Geltungsbereich sollte möglichst alle Bereiche, Aspekte und Komponenten umfassen, die zur Unterstützung der Fachaufgaben, Geschäftsprozesse oder Organisationseinheiten dienen und deren Verwaltung innerhalb der Institution stattfindet.
- Wenn dies nicht möglich ist, weil Teile der betrachteten Fachaufgaben oder Geschäftsprozesse organisatorisch von externen Partnern abhängig sind, beispielsweise im Rahmen von Outsourcing, sollten die Schnittstellen klar definiert werden, damit dies im Rahmen der Sicherheitskonzeption berücksichtigt werden kann.

Informationsverbund

Der Geltungsbereich für die Erstellung der Sicherheitskonzeption wird im Folgenden "Informationsverbund" genannt (oder auch "IT-Verbund"). Die Bezeichnung IT-Verbund beschreibt die eher technische Sicht auf den Geltungsbereich. Einem IT-Verbund werden aber nicht nur IT-Komponenten zugeordnet, sondern auch Informationen, organisatorische Regelungen, Aufgabenbereiche und Zuständigkeiten sowie physische Infrastruktur. Daher ist der Begriff Informationsverbund treffender.

Somit umfasst ein Informationsverbund die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein Informationsverbund kann dabei als Ausprägung die gesamte Informationsverarbeitung einer Institution oder auch einzelne Bereiche, die durch organisatorische oder technische Strukturen (z. B. Abteilungsnetz) oder gemeinsame Geschäftsprozesse bzw. Anwendungen (z. B. Personalinformationssystem) gegliedert sind, umfassen.

Für die Erstellung der Sicherheitskonzeption werden die Bestandteile des betrachteten Informationsverbundes erfasst und seine Struktur analysiert. Ein systematisches Vorgehen für diese Strukturanalyse wird im nächsten Abschnitt beschrieben.

Aktionspunkte zu 4.1 Definition des Geltungsbereichs für die Sicherheitskonzeption
• Festlegen, welche kritischen Geschäftsprozesse, Fachaufgaben oder Teile der Institution der Geltungsbereich beinhalten soll • Den Geltungsbereich eindeutig abgrenzen • Schnittstellen zu externen Partnern beschreiben

4.2 Strukturanalyse

Die Strukturanalyse dient der Vorerhebung von Informationen, die für die weitere Vorgehensweise in der Erstellung eines Sicherheitskonzepts nach IT-Grundschutz benötigt werden. Dabei geht es um die Erfassung der Bestandteile (Informationen, Anwendungen, IT-Systeme, Räume, Kommunikationsnetze), die zur Erfüllung der im Geltungsbereich festgelegten Geschäftsprozesse oder Fachaufgaben benötigt werden.

Dazu müssen geschäftskritische Informationen und Anwendungen ermittelt und die betroffenen IT-Systeme, Räume und Netze erfasst werden. Die klassische Vorgehensweise ist, zuerst die Anwendungen und ausgehend davon die weiteren betroffenen Objekte zu ermitteln. Dieser Ansatz hat den Nachteil, dass es häufig schwierig ist, abstrakte Anwendungen losgelöst von konkreten technischen Komponenten zu erfassen. Daher kann es in einigen Fällen zweckmäßig sein, abweichend von der hier dargestellten Reihenfolge zunächst die IT-Systeme zu erheben, da sich die Anwendungen häufig anhand der betrachteten IT-Systeme leichter ermitteln lassen.

Zu beachten ist, dass die Objekte und Daten, die im Rahmen einer Strukturanalyse erfasst werden, meist nicht nur für den Sicherheitsprozess, sondern auch für betriebliche Aspekte und die Verwaltung erforderlich sind. Es sollte daher geprüft werden, ob bereits Datenbanken oder Übersichten gepflegt werden, die im Rahmen der Strukturanalyse als Datenquellen genutzt werden können. In vielen Institutionen werden beispielsweise Datenbanken für die Inventarisierung, das Konfigurationsmanagement oder die Gestaltung von Geschäftsprozessen betrieben. Dadurch können sich Synergien ergeben.

Die Strukturanalyse gliedert sich in folgende Teilaufgaben:

- Erfassung der zum Geltungsbereich zugehörigen Geschäftsprozesse, Anwendungen und Informationen
- Netzplanerhebung
- Erhebung von IT-Systemen und ähnlichen Objekten
- Erfassung der Räume

Bei allen Teilaufgaben ist zu beachten, dass es häufig nicht zweckmäßig ist, jedes Objekt einzeln zu erfassen. Stattdessen sollten ähnliche Objekte zu Gruppen zusammengefasst werden.

4.2.1 Komplexitätsreduktion durch Gruppenbildung

Die Strukturanalyse liefert wichtige Grunddaten für den gesamten Sicherheitsprozess. Der Informationsverbund setzt sich meist aus vielen Einzelobjekten zusammen, die bei der Konzeption berücksichtigt werden müssen. Wenn alle logischen und technischen Objekte einzeln erfasst werden, besteht jedoch die Gefahr, dass die Ergebnisse der Strukturanalyse aufgrund der Datenmenge und der Komplexität nicht handhabbar sind. Ähnliche Objekte sollten deshalb sinnvoll zu Gruppen zusammengefasst werden.

Bei technischen Komponenten hat eine konsequente Gruppenbildung zudem den Vorteil, dass die Administration wesentlich vereinfacht wird, wenn es nur wenige Grundkonfigurationen gibt. Durch eine möglichst hohe Standardisierung innerhalb einer IT-Umgebung wird außerdem die Zahl potentieller Sicherheitslücken reduziert und die Sicherheitsmaßnahmen für diesen Bereich können ohne Unterscheidung verschiedenster Schwachstellen umgesetzt werden. Dies kommt nicht nur der Informationssicherheit zugute, sondern spart auch Kosten.

Objekte können dann ein und derselben Gruppe zugeordnet werden, wenn die Objekte alle

- vom gleichen Typ sind,
- ähnlich konfiguriert sind,
- ähnlich in das Netz eingebunden sind (im Fall von IT-Systemen z. B. am gleichen Switch),
- ähnlichen administrativen und infrastrukturellen Rahmenbedingungen unterliegen,
- ähnliche Anwendungen bedienen und
- den gleichen Schutzbedarf aufweisen.

Aufgrund der genannten Voraussetzungen für die Gruppenbildung kann bezüglich Informationssicherheit davon ausgegangen werden, dass eine Stichprobe aus einer Gruppe in der Regel den Sicherheitszustand der Gruppe repräsentiert.

Wichtigstes Beispiel für die Gruppierung von Objekten ist sicherlich die Zusammenfassung von Clients. In der Regel gibt es in einer Institution eine große Anzahl von Clients, die sich jedoch gemäß obigem Schema in eine überschaubare Anzahl von Gruppen aufteilen lassen. Dies gilt analog auch für Räume und andere Objekte. In großen Informationsverbünden, wo aus Gründen der Redundanz oder des Durchsatzes viele Server die gleiche Aufgabe wahrnehmen, können durchaus auch Server zu Gruppen zusammengefasst werden.

Die Teilaufgaben der Strukturanalyse werden nachfolgend beschrieben und durch ein begleitendes Beispiel erläutert. Eine ausführliche Version des Beispiels findet sich in den Hilfsmitteln zum IT-Grundschutz auf den BSI-Webseiten. Bei allen Teilaufgaben sollten jeweils Objekte zu Gruppen zusammengefasst werden, wenn dies sinnvoll und zulässig ist.

Aktionspunkte zu 4.2.1 Komplexitätsreduktion durch Gruppenbildung
• Bei allen Teilaufgaben der Strukturanalyse gleichartige Objekte zu Gruppen zusammenfassen
• Typ und Anzahl der jeweils zusammengefassten Objekte vermerken

4.2.2 Erfassung der Anwendungen und der zugehörigen Informationen

Ausgehend von jedem Geschäftsprozess bzw. jeder Fachaufgabe, die im Informationsverbund enthalten ist, müssen in dieser Phase die damit zusammenhängenden Anwendungen und Informationen identifiziert werden. Anwendungen sind Verfahren, die zur Unterstützung von Geschäftsprozessen und Fachaufgaben in Behörden und Unternehmen dienen.

Die geeignete Granularität für die betrachteten Anwendungen muss in jeder Institution individuell gewählt werden. Ziel sollte dabei sein, eine optimale Transparenz und Effizienz bei der Strukturana-

lyse und der Schutzbedarfsfeststellung zu erreichen. Auch die in den IT-Grundschutz-Katalogen betrachteten Bausteine aus der Schicht der Anwendungen können für diesen Schritt Aufschluss geben.

Zur weiteren Reduzierung des Aufwands kann die Strukturanalyse des Informationsverbundes auf die Anwendungen und Informationen beschränkt werden, die für die betrachteten Geschäftsprozesse oder Fachaufgaben erforderlich sind. Dabei sollte darauf geachtet werden, dass zumindest diejenigen Anwendungen und Informationen berücksichtigt werden, die aufgrund der Anforderungen der betrachteten Geschäftsprozesse oder Fachaufgaben ein Mindestniveau an

- Geheimhaltung (Vertraulichkeit) oder
- Korrektheit und Unverfälschtheit (Integrität) oder
- Verfügbarkeit

erfordern.

Um dies sicherzustellen, sollten bei der Erfassung der Anwendungen die Benutzer bzw. die für die Anwendung Verantwortlichen sowie die für den Geschäftsprozess Verantwortlichen nach ihrer Einschätzung befragt werden.

Aufgrund der steigenden Komplexität von Anwendungen ist es jedoch oft für die Fachverantwortlichen nicht klar, welche Abhängigkeiten zwischen einem Geschäftsprozess oder einer Fachaufgabe zu einer konkreten Anwendung bestehen. Es sollte also für jede einzelne Fachaufgabe festgestellt werden, welche Anwendungen für ihre Abwicklung notwendig sind und auf welche Daten dabei zugegriffen wird. In einer gemeinsamen Sitzung der Fachabteilung, der Verantwortlichen der einzelnen Anwendungen und der unterstützenden IT-Abteilung können diese Abhängigkeiten erfasst werden.

Falls abweichend von der hier vorgeschlagenen Reihenfolge zuerst die IT-Systeme erfasst wurden, ist es häufig hilfreich, die Anwendungen an erster Stelle orientiert an den IT-Systemen zusammenzutragen. Aufgrund ihrer Breitenwirkung sollte dabei mit den Servern begonnen werden. Um ein möglichst ausgewogenes Bild zu bekommen, kann anschließend diese Erhebung auf Seiten der Clients und Einzelplatz-Systeme vervollständigt werden. Abschließend sollte noch festgestellt werden, welche Netzkoppelelemente welche Anwendungen unterstützen.

Um die späteren Zuordnungen zu erleichtern, sollten die Anwendungen durchnummeriert werden. Da viele IT-Sicherheitsbeauftragte gleichzeitig auch als Datenschutzbeauftragte für den Schutz personenbezogener Daten zuständig sind, bietet es sich an, an dieser Stelle schon zu vermerken, ob die beschriebene Anwendung personenbezogene Daten speichert und/oder verarbeitet. Der Schutzbedarf einer Anwendung resultiert in der Regel aus dem Schutzbedarf der damit verarbeiteten Informationen. Daher sollte die Art dieser Informationen auch in der Tabelle dokumentiert werden.

Weiterhin empfiehlt es sich, bei den Anwendungen zu vermerken, welche Geschäftsprozesse sie unterstützen. Der Verantwortliche und die Benutzer der Anwendung sollten ebenfalls erfasst werden, um Ansprechpartner für Sicherheitsfragen leichter identifizieren bzw. betroffene Benutzergruppen schnell erreichen zu können.

Es empfiehlt sich, bei der Erfassung der Anwendungen auch Datenträger und Dokumente mitzubetrachten und diese ähnlich wie Anwendungen zu behandeln. Sofern sie nicht fest mit einer Anwendung oder einem IT-System verknüpft sind, müssen Datenträger und Dokumente gesondert in die Strukturanalyse integriert werden. Natürlich ist es dabei nicht zweckmäßig, alle Datenträger einzeln zu erfassen. Zum einen sollten nur Datenträger und Dokumente mit einem Mindest-Schutzbedarf betrachtet und zum anderen sollten möglichst Gruppen gebildet werden. Beispiele für Datenträger und Dokumente, die im Rahmen der Strukturanalyse gesondert erfasst werden sollten, sind

- Archiv- und Backup-Datenträger,
- Datenträger für den Austausch mit externen Kommunikationspartnern,
- USB-Sticks für den mobilen Einsatz,
- Notfallhandbücher, die in ausgedruckter Form vorgehalten werden,

- Mikrofilme,
- wichtige Verträge mit Partnern und Kunden.

Erfassung der Abhängigkeiten zwischen Anwendungen

Optional kann zur besseren Übersicht die Abhängigkeit von Anwendungen untereinander dargestellt werden. Beispielsweise können Bestellungen nicht abschließend bearbeitet werden, wenn keine Informationen über den Lagerbestand zur Verfügung stehen.

Zur Dokumentation der Ergebnisse bietet sich die Darstellung in tabellarischer Form oder die Nutzung entsprechender Software-Produkte an.

Beispiel: Bundesamt für Organisation und Verwaltung (BOV) - Teil 1

Im Folgenden wird anhand einer fiktiven Behörde, dem BOV, beispielhaft dargestellt, wie die erfassten Anwendungen dokumentiert werden können. Zu beachten ist, dass die Struktur des BOV im Hinblick auf Informationssicherheit keineswegs optimal ist. Sie dient lediglich dazu, die Vorgehensweise bei der Anwendung des IT-Grundschutzes zu illustrieren. Hier wird nur ein Überblick gegeben, das komplette Beispiel findet sich unter den Hilfsmitteln zum IT-Grundschutz.

Das BOV sei eine fiktive Behörde mit 150 Mitarbeitern, von denen 130 an Bildschirmarbeitsplätzen arbeiten. Räumlich besteht eine Aufteilung des Bundesamts in die Hauptstelle Bonn und eine Außenstelle in Berlin, wo unter anderem die Teilaufgaben Grundsatz, Normung und Koordinierung wahrgenommen werden. Von den insgesamt 130 Mitarbeitern mit IT-gestützten Arbeitsplätzen sind 90 in Bonn und 40 in Berlin tätig.

Um die Dienstaufgaben leisten zu können, sind alle Arbeitsplätze vernetzt worden. Die Außenstelle Berlin ist über eine angemietete Standleitung angebunden. Alle zu Grunde liegenden Richtlinien und Vorschriften sowie Formulare und Textbausteine sind ständig für jeden Mitarbeiter abrufbar. Alle relevanten Arbeitsergebnisse werden in eine zentrale Datenbank eingestellt. Entwürfe werden ausschließlich elektronisch erstellt, weitergeleitet und unterschrieben. Zur Realisierung und Betreuung aller benötigten Funktionalitäten ist in Bonn ein IT-Referat installiert worden.

Die Geschäftsprozesse des BOV werden elektronisch gepflegt und sind nach einem zweistufigen Schema benannt. Hinter dem Kürzel GP wird die Nummer des Hauptprozesses angegeben, die Nummer des Unterprozesses folgt nach einem Bindestrich, zum Beispiel GP0-2.

Nachfolgend wird ein Auszug aus der Erfassung der Anwendungen und der zugehörigen Informationen für das fiktive Beispiel BOV dargestellt:

Nr.	Anwendung	Art der Information *	Verantwortlich	Benutzer	Geschäftsprozesse
A1	Personaldatenverarbeitung	P	Z1	Z1	GP0-1, GP0-2
A2	Beihilfeabwicklung	P	Z2	alle	GP0-2
A3	Reisekostenabrechnung	P/V/F	Z2	alle	GP0-1, GP0-3
A4	Benutzer-Authentisierung	P/S	IT1	alle	GP0, GP5, GP6
A5	Systemmanagement	S	IT3	IT3	alle
A6	Bürokommunikation	P/V/F/S	IT3	alle	alle
A7	zentrale Dokumentenverwaltung	P/V/F/S	Z1	alle	GP0, GP5
A8	USB-Sticks zum Datenträgeraustausch	P/V/F	IT3	IT3	GP0-1, GP0-3

* Legende:

- P = personenbezogene Daten
- V = verwaltungsspezifische Informationen des BOV, beispielsweise Organisationsstrukturen und Dienstanweisungen

- F = fachliche Informationen des BOV, beispielsweise Korrespondenz mit den Kunden
- S = systemspezifische/technische Informationen, beispielsweise Konfigurationsdateien von IT-Systemen

Die Art der Information wird hier für jede Anwendung kurz miterfasst, um schneller einschätzen zu können, welcher Schutzbedarf sich für die jeweiligen Anwendungen ergibt, die diese Informationen verarbeiten. Die für die Art der Informationen in obiger Tabelle benutzten Kategorien sind Beispiele und keine Empfehlungen für die Kategorisierung von Informationen.

Aktionspunkte zu 4.2.2 Erfassung der Anwendungen und der zugehörigen Informationen

- Mit Einbeziehung der Fachabteilung, der Verantwortlichen für die Anwendungen und der unterstützenden IT-Abteilung herausfinden, welche Anwendungen für die betrachteten Geschäftsprozesse oder Fachaufgaben erforderlich sind
- Übersicht über die Anwendungen erstellen und mit eindeutigen Nummern oder Kürzeln kennzeichnen
- Für jede Anwendung die entsprechenden Geschäftsprozesse, verarbeitete Informationen, Verantwortliche und gegebenenfalls Benutzer vermerken
- Für jede Anwendung vermerken, inwieweit personenbezogene Daten mit ihr verarbeitet werden

4.2.3 Netzplanerhebung

Einen geeigneten Ausgangspunkt für die weitere technische Analyse stellt ein Netzplan (beispielsweise in Form eines Netztopologieplans) dar. Ein Netzplan ist eine graphische Übersicht über die im betrachteten Bereich der Informations- und Kommunikationstechnik eingesetzten Komponenten und deren Vernetzung. Netzpläne oder ähnliche graphische Übersichten sind auch aus betrieblichen Gründen in den meisten Institutionen vorhanden. Im Einzelnen sollte der Plan in Bezug auf die Informationssicherheit mindestens folgende Objekte darstellen:

- IT-Systeme, d. h. Client- und Server-Computer, aktive Netzkomponenten (wie Switches, Router, WLAN Access Points), Netzdrucker etc.
- Netzverbindungen zwischen diesen Systemen, d. h. LAN-Verbindungen (wie Ethernet, Token-Ring), WLANs, Backbone-Techniken (wie FDDI, ATM) etc.
- Verbindungen des betrachteten Bereichs nach außen, d. h. Einwahl-Zugänge über ISDN oder Modem, Internet-Anbindungen über analoge Techniken oder Router, Funkstrecken oder Mietleitungen zu entfernten Gebäuden oder Liegenschaften etc.

Zu jedem der dargestellten Objekte gehört weiterhin ein Minimalsatz von Informationen, die einem zugeordneten Katalog zu entnehmen sind. Für jedes IT-System sollten zumindest

- eine eindeutige Bezeichnung (beispielsweise der vollständige Hostname oder eine Identifikationsnummer),
- Typ und Funktion (beispielsweise Datenbank-Server für Anwendung X),
- die zugrunde liegende Plattform (d. h. Hardware-Plattform und Betriebssystem),
- der Standort (beispielsweise Gebäude- und Raumnummer),
- der zuständige Administrator,
- die vorhandenen Kommunikationsschnittstellen (z. B. Internet-Anschluss, Bluetooth, WLAN-Adapter) sowie
- die Art der Netzanbindung und die Netzadresse

vermerkt sein. Nicht nur für die IT-Systeme selbst, sondern auch für die Netzverbindungen zwischen den Systemen und für die Verbindungen nach außen sind bestimmte Informationen erforderlich, nämlich

- die Art der Verkabelung bzw. Kommunikationsanbindung (z. B. Lichtwellenleiter oder WLAN basierend auf IEEE 802.11),
- die maximale Datenübertragungsrate (z. B. 100 Mbps),
- die auf den unteren Schichten verwendeten Netzprotokolle (z. B. Ethernet, TCP/IP),
- bei Außenanbindungen: Details zum externen Netz (z. B. Internet, Name des Providers).

Virtuelle IT-Systeme und virtuelle Netzverbindungen, beispielsweise Virtuelle LANs (VLANs) oder Virtuelle Private Netze (VPNs), sollten ebenfalls in einem Netzplan dargestellt werden, wenn die dadurch realisierten logischen (virtuellen) Strukturen wesentlich von den physischen Strukturen abweichen. Aus Gründen der Übersichtlichkeit kann es zweckmäßig sein, die logischen (virtuellen) Strukturen in einem separaten Netzplan darzustellen.

Es empfiehlt sich, Bereiche mit unterschiedlichem Schutzbedarf zu kennzeichnen.

Der Netzplan sollte möglichst in elektronischer Form erstellt und gepflegt werden. Hat die Informationstechnik in der Institution einen gewissen Umfang überschritten, bietet es sich an, bei der Erfassung und Pflege des Netzplans auf geeignete Hilfsprogramme zurückzugreifen, da die Unterlagen eine erhebliche Komplexität aufweisen können und ständigem Wandel unterzogen sind.

Aktualisierung des Netzplans

Da die IT-Struktur in der Regel ständig an die Anforderungen der Institution angepasst wird und die Pflege des Netzplans entsprechende Ressourcen bindet, ist der Netzplan der Institution nicht immer auf dem aktuellen Stand. Vielmehr werden in der Praxis oftmals nur größere Änderungen an der IT-Struktur einzelner Bereiche zum Anlass genommen, den Plan zu aktualisieren.

Im Hinblick auf die Verwendung des Netzplans für die Strukturanalyse besteht demnach der nächste Schritt darin, den vorliegenden Netzplan (bzw. die Teilpläne, wenn der Gesamtplan aus Gründen der Übersichtlichkeit aufgeteilt wurde) mit der tatsächlich vorhandenen IT-Struktur abzugleichen und gegebenenfalls auf den neuesten Stand zu bringen. Hierzu sind die IT-Verantwortlichen und Administratoren der einzelnen Anwendungen und Netze zu konsultieren. Falls Programme für ein zentralisiertes Netz- und Systemmanagement zum Einsatz kommen, sollte auf jeden Fall geprüft werden, ob diese Programme bei der Erstellung eines Netzplans Unterstützung anbieten. Zu beachten ist jedoch, dass Funktionen zur automatischen oder halbautomatischen Erkennung von Komponenten temporär zusätzlichen Netzverkehr erzeugen. Es muss sichergestellt sein, dass dieser Netzverkehr nicht zu Beeinträchtigungen des IT-Betriebs führt. Ebenso sollte das Ergebnis von automatischen bzw. halbautomatischen Erkennungen stets daraufhin geprüft werden, ob wirklich alle relevanten Komponenten ermittelt wurden.

Beispiel: Bundesamt für Organisation und Verwaltung (BOV) - Teil 2

Nachfolgend wird für die fiktive Behörde BOV beispielhaft dargestellt, wie ein Netzplan aussehen kann:

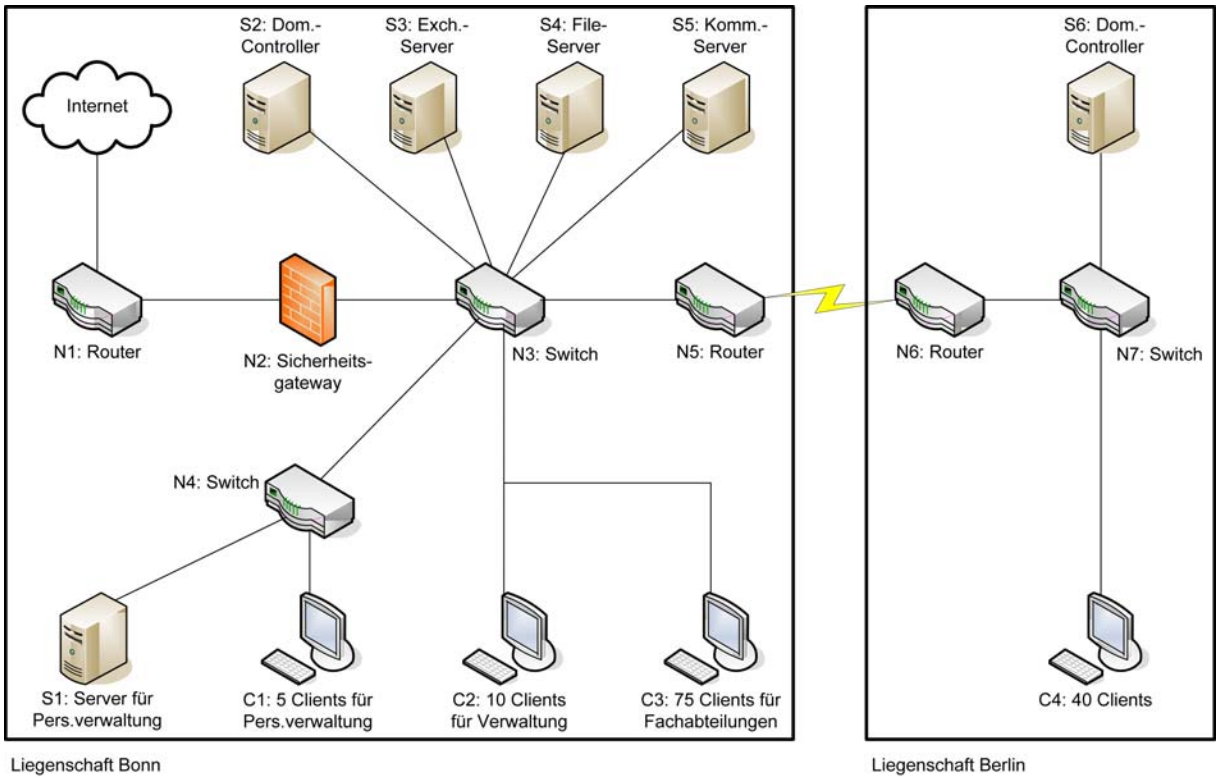


Abbildung 6: Beispiel eines Netzplans im Rahmen der Strukturanalyse

In dem dargestellten Netzplan sind die IT-Systeme durch eine Nummer (Server, Clients und aktive Netzkomponenten in der Form S*n*, C*n* bzw. N*n*) und die Funktion gekennzeichnet.

Sowohl in Berlin als auch in Bonn wurden die Clients in geeignete Gruppen zusammengefasst. Zwar sind alle 130 Clients nahezu gleich konfiguriert, sie unterscheiden sich jedoch im Hinblick auf die zu verarbeitenden Informationen, die Anwendungen, die Einbindung in das Netz und die infrastrukturellen Rahmenbedingungen. Die Gruppe C1 repräsentiert die 5 Clients in der Personalabteilung. Diese haben Zugriff auf den Server S1 der Personalabteilung in Bonn. C2 und C3 fassen die 10 Clients der Verwaltungsabteilung bzw. die 75 Clients der Fachabteilungen in Bonn zusammen. Sie unterscheiden sich lediglich im Hinblick auf die genutzten Anwendungsprogramme. Schließlich werden durch die Gruppe C4 die Clients der Fachabteilungen in der Liegenschaft Berlin dargestellt. Von den Gruppen C1 bis C3 unterscheiden sie sich durch die umgebende Infrastruktur und die abweichende Einbindung in das Gesamtnetz.

Aktionspunkte zu 4.2.3 Netzplanerhebung:

- Existierende graphische Darstellungen des Netzes, beispielsweise Netztopologiepläne, sichten
- Netzpläne gegebenenfalls aktualisieren oder neu erstellen
- Existierende Zusatzinformationen über die enthaltenen IT-Systeme sichten und gegebenenfalls aktualisieren und vervollständigen
- Existierende Zusatzinformationen über die enthaltenen Kommunikationsverbindungen sichten und gegebenenfalls aktualisieren und vervollständigen

4.2.4 Erhebung der IT-Systeme

Im Hinblick auf die später durchzuführende Schutzbedarfsfeststellung und Modellierung des Informationsverbunds sollte eine Liste der vorhandenen und geplanten IT-Systeme in tabellarischer Form aufgestellt werden. Der Begriff IT-System umfasst dabei nicht nur Computer im engeren Sinn, sondern auch aktive Netzkomponenten, Netzdrucker, TK-Anlagen, etc. Die technische Realisierung eines IT-Systems steht im Vordergrund, beispielsweise Einzelplatz-PC, Windows Server 2003, Client

unter Windows XP, Unix-Server, TK-Anlage usw. An dieser Stelle soll nur das System als solches erfasst werden (z. B. Unix-Server), nicht die einzelnen Bestandteile, aus denen das IT-System zusammengesetzt ist (also nicht Rechner, Tastatur, Bildschirm etc.).

Die vollständige und korrekte Erfassung der vorhandenen und geplanten IT-Systeme dient nicht nur der Erstellung eines Sicherheitskonzepts. Auch für die Überprüfung, Wartung, Fehlersuche und Instandsetzung von IT-Systemen ist sie notwendig.

Zu erfassen sind sowohl die vernetzten als auch die nicht vernetzten IT-Systeme, insbesondere also auch solche, die nicht im zuvor betrachteten Netzplan aufgeführt sind. IT-Systeme, die im Netzplan zu einer Gruppe zusammengefasst worden sind, können weiterhin als ein Objekt behandelt werden. Auch bei den IT-Systemen, die nicht im Netzplan aufgeführt sind, ist zu prüfen, ob sie sinnvoll zusammengefasst werden können. Möglich ist dies beispielsweise bei einer größeren Anzahl von nicht vernetzten Einzelplatz-PCs, die die im Abschnitt 4.2.1 genannten Bedingungen für eine Gruppierung erfüllen.

Bei dieser Erfassung sollten folgende Informationen vermerkt werden, die für die nachfolgende Arbeit nützlich sind:

- eine eindeutige Bezeichnung des IT-Systems,
- Beschreibung (Typ und Funktion),
- Plattform (z. B. Hardware-Architektur/Betriebssystem),
- bei Gruppen: Anzahl der zusammengefassten IT-Systeme,
- Aufstellungsort des IT-Systems,
- Status des IT-Systems (in Betrieb, im Test, in Planung) und
- Anwender bzw. Administratoren des IT-Systems.

Anschließend werden die Anwendungen jeweils denjenigen IT-Systemen zugeordnet, die für deren Ausführung benötigt werden. Dies können die IT-Systeme sein, auf denen die Anwendungen verarbeitet werden, oder auch diejenigen, die Daten dieser Anwendungen transferieren. Das Ergebnis ist eine Übersicht, in der die Zusammenhänge zwischen den wichtigen Anwendungen und den entsprechenden IT-Systemen dargestellt werden.

Beispiel: Bundesamt für Organisation und Verwaltung (BOV) - Teil 3

Als Beispiel ist in der folgenden Tabelle ein Auszug aus der Liste der IT-Systeme im BOV aufgeführt. Die vollständige Liste findet sich unter den Hilfsmitteln zum IT-Grundschutz auf der BSI-Webseite.

Nr.	Beschreibung	Plattform	Anzahl	Aufstellungsort	Status	Anwender
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	Gruppe von Clients der Personaldatenverarbeitung	Windows Vista	5	Bonn, R 1.02 - R 1.06	in Betrieb	Personalreferat
C2	Gruppe von Clients in der Verwaltungsabteilung	Windows Vista	10	Bonn, R 1.07 - R 1.16	in Betrieb	Verwaltungsabteilung
C6	Gruppe der Laptops für den Standort Berlin	Laptop unter Windows Vista	2	Berlin, R 2.01	in Betrieb	alle IT-Anwender in der Außenstelle Berlin
N1	Router zum Internet-	Router	1	Bonn, R	in	alle IT-Anwen-

Nr.	Beschreibung	Plattform	Anzahl	Aufstellungsort	Status	Anwender
	Zugang			3.09	Betrieb	der
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
T1	TK-Anlage für Bonn	ISDN-TK-Anlage	1	Bonn, B.02	in Betrieb	alle Mitarbeiter in der Hauptstelle Bonn

Die IT-Systeme bzw. Gruppen S1, S2, C1, C2, N1, N2 und N3 sind direkt dem Netzplan entnommen. Demgegenüber hinzugekommen sind die nicht vernetzten IT-Systeme C6 (Laptop) und T1 (TK-Anlage).

Nachfolgend wird ein Auszug aus der Zuordnung der Anwendungen zu den betroffenen IT-Systemen für das fiktive Beispiel BOV dargestellt:

Beschreibung der Anwendungen		**IT-Systeme**						
Nr.	**Anwendung / Informationen**	S1	S2	S3	S4	S5	S6	S7
A1	Personaldatenverarbeitung	X						
A2	Beihilfeabwicklung	X						
A3	Reisekostenabrechnung	X						
A4	Benutzer-Authentisierung		X				X	
A5	Systemmanagement		X					
A6	Bürokommunikation			X				
A7	zentrale Dokumentenverwaltung				X			
A8	USB-Sticks zum Datenträgeraustausch							

Legende: Ai X Sj = Die Ausführung der Anwendung Ai hängt vom IT-System Sj ab.

Aktionspunkte zu 4.2.4 Erhebung der IT-Systeme

- Prüfen, ob existierende Datenbanken oder Übersichten über die vorhandenen oder geplanten IT-Systeme als Ausgangsbasis für die weitere Vorgehensweise geeignet sind
- Liste der vernetzten und nicht-vernetzten IT-Systeme erstellen beziehungsweise aktualisieren und vervollständigen
- IT-Systeme beziehungsweise IT-System-Gruppen mit eindeutigen Nummern oder Kürzeln kennzeichnen
- Die Anwendungen den IT-Systemen (Servern, Clients, Netzkoppelelementen etc.) zuordnen, die für ihre Ausführung benötigt werden

4.2.5 Erfassung der Räume

Die betrachteten Geschäftsprozesse und Fachaufgaben werden nicht nur auf definierten IT-Systemen betrieben, sondern auch innerhalb der Grenzen der räumlichen Infrastruktur einer Institution. Je nach Größe der Institution und vielen anderen Faktoren kann sich eine Institution in einem allein genutzten Gebäude oder auch nur auf einer Etage befinden. Viele Institutionen nutzen Liegenschaften, die weit verstreut sind oder mit anderen Nutzern geteilt werden müssen. Häufig sind Geschäftsprozesse und Fachaufgaben auch in fremden Räumlichkeiten angesiedelt, zum Beispiel im Rahmen von Dienstleistungsverträgen.

In ein Sicherheitskonzept müssen alle Liegenschaften einbezogen werden, innerhalb derer die betrachteten Geschäftsprozesse und Fachaufgaben betrieben werden. Dazu gehören Betriebsgelände,

Gebäude, Etagen, Räume sowie die Wegstrecke zwischen diesen. Alle Kommunikationsverbindungen, die über für Dritte zugängliche Gelände verlaufen, müssen als Außenverbindungen behandelt werden. Dies gilt auch für drahtlose Kommunikationsverbindungen, wenn nicht ausgeschlossen werden kann, dass Dritte darauf zugreifen können.

Für die weitere Vorgehensweise der Modellierung nach IT-Grundschutz und für die Planung des Soll-Ist-Vergleichs ist es hilfreich, eine Übersicht über die Liegenschaften, vor allem die Räume, zu erstellen, in denen IT-Systeme aufgestellt oder die für den IT-Betrieb genutzt werden. Dazu gehören Räume, die ausschließlich dem IT-Betrieb dienen (wie Serverräume, Datenträgerarchive), solche, in denen unter anderem IT-Systeme betrieben werden (wie Büroräume), aber auch die Wegstrecken, über die Kommunikationsverbindungen laufen. Wenn IT-Systeme statt in einem speziellen Technikraum in einem Schutzschrank untergebracht sind, ist der Schutzschrank wie ein Raum zu erfassen.

Hinweis: Bei der Erhebung der IT-Systeme sind schon die Aufstellungsorte miterfasst worden.

Zusätzlich muss untersucht werden, ob schutzbedürftige Informationen in weiteren Räumen aufbewahrt werden. Diese Räume müssen dann ebenfalls erhoben werden. Hierbei müssen auch Räume erfasst werden, in denen nicht-elektronische schutzbedürftige Informationen aufbewahrt werden, also beispielsweise Aktenordner oder Mikrofilme. Die Art der verarbeiteten Informationen muss anhand dieser Dokumentation nachvollziehbar sein.

Beispiel: Bundesamt für Organisation und Verwaltung (BOV) - Teil 4

Im folgenden Ausschnitt wird anhand des fiktiven Beispiels BOV gezeigt, wie eine tabellarische Übersicht über die Räume aussehen könnte. Hier ist bereits Platz für die Schutzbedarfsermittlung der Räume vorgesehen, ausgefüllt werden diese Spalten aber erst in einem späteren Schritt.

Raum			**IT / Informationen**	**Schutzbedarf**		
Bezeichnung	**Art**	**Lokation**	**IT-Systeme / Datenträger**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**
R U.02	Datenträger-archiv	Gebäude Bonn	Backup-Datenträger (Wochensicherung der Server S1 bis S5)			
R B.02	Technikraum	Gebäude Bonn	TK-Anlage			
R 1.01	Serverraum	Gebäude Bonn	S1, N4			
R 1.02 - R 1.06	Büroräume	Gebäude Bonn	C1			
R 3.11	Schutzschrank im Raum R 3.11	Gebäude Bonn	Backup-Datenträger (Tagessicherung der Server S1 bis S5)			
R E.03	Serverraum	Gebäude Berlin	S6, N6, N7			
R 2.01 - R 2.40	Büroräume	Gebäude Berlin	C4, einige mit Faxgeräten			

Aktionspunkte zu 4.2.4 Erfassung der Räume

- Liste aller bei der Erfassung der IT-Systeme notierten Liegenschaften, Gebäude und Räume erstellen
- Weitere Räume ergänzen, in denen schutzbedürftige Informationen aufbewahrt oder auf andere Weise verarbeitet werden

4.3 Schutzbedarfsfeststellung

Ziel der Schutzbedarfsfeststellung ist es, für die erfassten Objekte im Informationsverbund zu entscheiden, welchen Schutzbedarf sie bezüglich Vertraulichkeit, Integrität und Verfügbarkeit besitzen. Dieser Schutzbedarf orientiert sich an den möglichen Schäden, die mit einer Beeinträchtigung der betroffenen Anwendungen und damit der jeweiligen Geschäftsprozesse verbunden sind.

Die Schutzbedarfsfeststellung für den Informationsverbund gliedert sich in mehrere Schritte:

- Definition der Schutzbedarfskategorien
- Schutzbedarfsfeststellung für Anwendungen
- Schutzbedarfsfeststellung für IT-Systeme
- Schutzbedarfsfeststellung für Räume
- Schutzbedarfsfeststellung für Kommunikationsverbindungen
- Schlussfolgerungen aus den Ergebnissen der Schutzbedarfsfeststellung

Nach der Definition der Schutzbedarfskategorien wird anhand von typischen Schadensszenarien zunächst der Schutzbedarf der Geschäftsprozesse und Anwendungen bestimmt. Anschließend wird daraus der Schutzbedarf der einzelnen IT-Systeme, Räume und Kommunikationsverbindungen abgeleitet.

Die Vorgehensweise hierfür wird in den folgenden Abschnitten detailliert dargestellt.

4.3.1. Definition der Schutzbedarfskategorien

Da der Schutzbedarf meist nicht quantifizierbar ist, beschränkt sich der IT-Grundschutz im Weiteren auf eine qualitative Aussage, indem der Schutzbedarf in drei Kategorien unterteilt wird:

Schutzbedarfskategorien	
"normal"	Die Schadensauswirkungen sind begrenzt und überschaubar.
"hoch"	Die Schadensauswirkungen können beträchtlich sein.
"sehr hoch"	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Die nachfolgenden Schritte erläutern, wie für Geschäftsprozesse und die dahinter liegenden Anwendungen jeweils die adäquate Schutzbedarfskategorie ermittelt werden kann.

Die Schäden, die bei dem Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit für einen Geschäftsprozess bzw. eine Anwendung einschließlich ihrer Daten entstehen können, lassen sich typischerweise folgenden Schadensszenarien zuordnen:

- Verstoß gegen Gesetze/Vorschriften/Verträge,
- Beeinträchtigung des informationellen Selbstbestimmungsrechts,
- Beeinträchtigung der persönlichen Unversehrtheit,
- Beeinträchtigung der Aufgabenerfüllung,
- negative Innen- oder Außenwirkung und
- finanzielle Auswirkungen.

Häufig treffen dabei für einen Schaden mehrere Schadensszenarien zu. So kann beispielsweise der Ausfall einer Anwendung die Aufgabenerfüllung beeinträchtigen, was direkte finanzielle Einbußen nach sich zieht und gleichzeitig auch zu einem Imageverlust führt.

Um die Schutzbedarfskategorien "normal", "hoch" und "sehr hoch" voneinander abgrenzen zu können, bietet es sich an, die Grenzen für die einzelnen Schadensszenarien zu bestimmen. Zur Orientierung, welchen Schutzbedarf ein potentieller Schaden und seine Folgen erzeugen, dienen die folgenden Tabellen. Die Tabellen sollten von der jeweiligen Institution auf ihre eigenen Gegebenheiten angepasst werden.

Schutzbedarfskategorie "normal"	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen • Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung erscheint nicht möglich.
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit ist größer als 24 Stunden.
5. Negative Innen- oder Außenwirkung	• Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
6. Finanzielle Auswirkungen	• Der finanzielle Schaden bleibt für die Institution tolerabel.

Schutzbedarfskategorie "hoch"	
1. Verstoß gegen Gesetze/Vorschriften/Verträge	• Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen • Vertragsverletzungen mit hohen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. • Die maximal tolerierbare Ausfallzeit liegt zwischen einer und 24 Stunden.
5. Negative Innen- oder Außenwirkung	• Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
6. Finanzielle Auswirkungen	• Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.

Schutzbedarfskategorie "sehr hoch"	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Fundamentaler Verstoß gegen Vorschriften und Gesetze • Vertragsverletzungen, deren Haftungsschäden ruinös sind
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. • Gefahr für Leib und Leben
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.
5. Negative Innen- oder Außenwirkung	• Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, ist denkbar.
6. Finanzielle Auswirkungen	• Der finanzielle Schaden ist für die Institution existenzbedrohend.

Wenn bei individuellen Betrachtungen festgestellt wird, dass über diese sechs Schadensszenarien hinaus weitere in Frage kommen, sollten diese entsprechend ergänzt werden. Für alle Schäden, die sich nicht in diese Szenarien abbilden lassen, muss ebenfalls eine Aussage getroffen werden, wo die Grenzen zwischen "normal", "hoch" oder "sehr hoch" zu ziehen sind.

Darüber hinaus sollten die individuellen Gegebenheiten der Institution berücksichtigt werden: Bedeutet in einem Großunternehmen ein Schaden in Höhe von 200.000,- Euro gemessen am Umsatz und am IT-Budget noch einen geringen Schaden, so kann für ein Kleinunternehmen schon ein Schaden in Höhe von 10.000,- Euro existentiell bedrohlich sein. Daher kann es sinnvoll sein, eine prozentuale Größe als Grenzwert zu definieren, der sich am Gesamtumsatz, am Gesamtgewinn oder an einer ähnlichen Bezugsgröße orientiert.

Ähnliche Überlegungen können bezüglich der Verfügbarkeitsanforderungen angestellt werden. So kann beispielsweise ein Ausfall von 24 Stunden Dauer in der Schutzbedarfskategorie "normal" als noch tolerabel eingeschätzt werden. Tritt jedoch eine Häufung dieser Ausfälle ein, z. B. mehr als einmal wöchentlich, so kann dies in der Summe nicht tolerierbar sein. Die anhand der Schutzbedarfskategorien festgelegten Verfügbarkeitsanforderungen sollten daher bei Bedarf konkretisiert werden.

Zur Einschätzung des Schutzbedarfs im Bereich "Beeinträchtigungen des informationellen Selbstbestimmungsrechts" gibt es auch von einigen deutschen Landesbeauftragten für den Datenschutz konkrete Beispiele, die in Schutzstufenkonzepten erläutert werden.

Bei der Festlegung der Grenze zwischen "normal" und "hoch" sollte berücksichtigt werden, dass für den normalen Schutzbedarf die Standard-Sicherheitsmaßnahmen des IT-Grundschutzes ausreichen sollten. Die getroffenen Festlegungen sind in geeigneter Weise im Sicherheitskonzept zu dokumentieren, da hiervon die Auswahl von Sicherheitsmaßnahmen und damit meist Folgekosten abhängen.

Aktionspunkte zu 4.3.1 Definition der Schutzbedarfskategorien

- Typische Schadensszenarien für die Definition von Schutzbedarfskategorien betrachten
- Schutzbedarfskategorien "normal", "hoch" und "sehr hoch" definieren beziehungsweise an die eigene Institution anpassen

4.3.2 Schutzbedarfsfeststellung für Anwendungen

Ausgehend von der Möglichkeit, dass Vertraulichkeit, Integrität oder Verfügbarkeit einer Anwendung oder der zugehörigen Informationen verloren gehen, werden die maximalen Schäden und Folgeschäden betrachtet, die aus einer solchen Situation entstehen können. Unter der Fragestellung "Was wäre, wenn ... ?" werden *aus Sicht der Anwender* realistische Schadensszenarien entwickelt und die zu erwartenden materiellen oder ideellen Schäden beschrieben. Die Höhe dieser möglichen Schäden bestimmt letztendlich dann den Schutzbedarf der Anwendung. Dabei ist es unbedingt erforderlich, die jeweiligen Verantwortlichen und die Benutzer der betrachteten Anwendungen nach ihrer persönlichen Einschätzung zu befragen. Sie haben im Allgemeinen eine gute Vorstellung darüber, welche Schäden entstehen können, und können für die Erfassung wertvolle Hinweise geben.

In die Schutzbedarfsfeststellung müssen auch die in der Strukturanalyse erfassten Gruppen von Datenträgern und Dokumenten einbezogen werden.

Um die Ermittlung der möglichen Schäden und Auswirkungen zu vereinfachen, werden im Anhang dieses Standards entsprechende Fragestellungen vorgestellt. Diese Anregungen erheben nicht den Anspruch auf Vollständigkeit, sie dienen lediglich zur Orientierung. Um die individuelle Aufgabenstellung und die Situation der Institution zu berücksichtigen, müssen diese Fragen gegebenenfalls entsprechend ergänzt und angepasst werden.

Die Festlegung des Schutzbedarfs der betrachteten Anwendungen ist eine Entscheidung im Rahmen des Risikomanagements und hat oft weitreichende Auswirkungen auf das Sicherheitskonzept für den betrachteten Informationsverbund. Der Schutzbedarf der Anwendungen fließt in die Schutzbedarfsfeststellung der betroffenen technischen und infrastrukturellen Objekte, wie zum Beispiel Server und Räume, ein.

Um die Ergebnisse der Schutzbedarfsfeststellung und die daraus resultierenden Entscheidungen im Rahmen des Informationssicherheitsmanagements später jederzeit nachvollziehen zu können, müssen die Ergebnisse der Schutzbedarfsfeststellung der Anwendungen gut dokumentiert werden. Dabei ist

darauf zu achten, dass nicht nur die Festlegung des Schutzbedarfs dokumentiert wird, sondern auch die entsprechenden Begründungen. Diese Begründungen erlauben es später, die Festlegungen zu überprüfen und weiter zu verwenden.

Beispiel: Bundesamt für Organisation und Verwaltung (BOV) - Teil 5

In der nachfolgenden Tabelle werden für das fiktive Beispiel BOV die wesentlichen Anwendungen, deren Schutzbedarf und die entsprechenden Begründungen erfasst.

Anwendung			Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**pers. Daten**	**Grundwert**	**Schutzbedarf**	**Begründung**
A1	Personaldaten-verarbeitung	X	Vertraulichkeit	hoch	Personaldaten sind besonders schutzbedürftige personenbezogene Daten, deren Bekanntwerden die Betroffenen erheblich beeinträchtigen können.
			Integrität	normal	Der Schutzbedarf ist normal, da Fehler rasch erkannt und die Daten nachträglich korrigiert werden können.
			Verfügbarkeit	normal	Ausfälle bis zu einer Woche können mittels manueller Verfahren überbrückt werden.
A2	Beihilfeabwicklung	X	Vertraulichkeit	hoch	Beihilfedaten sind besonders schutzbedürftige personenbezogene Daten, die zum Teil auch Hinweise auf Erkrankungen und ärztliche Befunde enthalten. Ein Bekanntwerden kann die Betroffenen erheblich beeinträchtigen.
			Integrität	normal	Der Schutzbedarf ist normal, da Fehler rasch erkannt und die Daten nachträglich korrigiert werden können.
			Verfügbarkeit	normal	Ausfälle bis zu einer Woche können mittels manueller Verfahren überbrückt werden.

An dieser Stelle kann es sinnvoll sein, über diese Informationen hinaus den Schutzbedarf auch aus einer gesamtheitlichen Sicht der Geschäftsprozesse oder Fachaufgaben zu betrachten. Dazu bietet es sich an, den Zweck einer Anwendung in einem Geschäftsprozess oder in einer Fachaufgabe zu beschreiben und daraus wiederum deren Bedeutung abzuleiten. Diese Bedeutung kann wie folgt klassifiziert werden:

Die Bedeutung der Anwendung ist für den Geschäftsprozess bzw. die Fachaufgabe:

- **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.

Der Vorteil, eine solche ganzheitliche Zuordnung vorzunehmen, liegt insbesondere darin, dass bei der Schutzbedarfsfeststellung die Leitungsebene als Regulativ für den Schutzbedarf der einzelnen Anwendungen agieren kann. So kann es sein, dass ein Verantwortlicher für eine Anwendung deren

Schutzbedarf aus seiner Sicht als "normal" einschätzt, die Leitungsebene aus Sicht des Geschäftsprozesses bzw. der Fachaufgabe diese Einschätzung jedoch nach oben korrigiert.

Diese optionalen Angaben sollten ebenfalls tabellarisch oder mit Hilfe entsprechender Software-Produkte dokumentiert werden.

Aktionspunkt zu 4.3.2 Schutzbedarfsfeststellung für Anwendungen
• Schutzbedarf der erfassten Anwendungen anhand von Schadensszenarien und Fragenkatalogen ermitteln • Schutzbedarf der Anwendungen und die entsprechenden Begründungen tabellarisch dokumentieren

4.3.3 Schutzbedarfsfeststellung für IT-Systeme

Um den Schutzbedarf eines IT-Systems festzustellen, müssen zunächst die Anwendungen betrachtet werden, die in direktem Zusammenhang mit dem IT-System stehen. Eine Übersicht, welche Anwendungen für die unterschiedlichen IT-Systeme relevant sind, wurde im Rahmen der Strukturanalyse (siehe Kapitel 4.2.4) ermittelt. Der Schutzbedarf der Anwendungen (siehe Kapitel 4.3.2) fließt in die Schutzbedarfsfeststellung für die jeweils betroffenen IT-Systeme ein.

Zur Ermittlung des Schutzbedarfs des IT-Systems müssen nun die möglichen Schäden der relevanten Anwendungen in ihrer Gesamtheit betrachtet werden. Im Wesentlichen bestimmt der Schaden bzw. die Summe der Schäden mit den schwerwiegendsten Auswirkungen den Schutzbedarf eines IT-Systems **(Maximumprinzip)**.

Bei der Betrachtung der möglichen Schäden und ihrer Folgen muss auch beachtet werden, dass IT-Anwendungen eventuell Arbeitsergebnisse anderer Anwendungen als Input nutzen. Eine, für sich betrachtet, weniger bedeutende Anwendung A kann wesentlich an Wert gewinnen, wenn eine andere, wichtige Anwendung B auf ihre Ergebnisse angewiesen ist. In diesem Fall muss der ermittelte Schutzbedarf der Anwendung B auch auf die Anwendung A übertragen werden. Handelt es sich dabei um Anwendungen verschiedener IT-Systeme, dann müssen Schutzbedarfsanforderungen des einen IT-Systems auch auf das andere übertragen werden **(Beachtung von Abhängigkeiten)**.

Werden mehrere Anwendungen bzw. Informationen auf einem IT-System verarbeitet, so ist zu überlegen, ob durch Kumulation mehrerer (z. B. kleinerer) Schäden auf einem IT-System ein insgesamt höherer Gesamtschaden entstehen kann. Dann erhöht sich der Schutzbedarf des IT-Systems entsprechend **(Kumulationseffekt)**.

Beispiel: Auf einem Netz-Server befinden sich sämtliche für die Kundendatenerfassung benötigten Anwendungen einer Institution. Der Schaden bei Ausfall einer dieser Anwendungen wurde als gering eingeschätzt, da genügend Ausweichmöglichkeiten vorhanden sind. Fällt jedoch der Server (und damit alle Anwendungen, die diesen Server benötigen) aus, so ist der dadurch entstehende Schaden deutlich höher zu bewerten. Die Aufgabenerfüllung kann unter Umständen nicht mehr innerhalb der notwendigen Zeitspanne gewährleistet werden. Daher ist auch der Schutzbedarf dieser "zentralen" Komponente entsprechend höher zu bewerten.

Auch der umgekehrte Effekt kann eintreten. So ist es möglich, dass eine Anwendung einen hohen Schutzbedarf besitzt, ihn aber deshalb nicht auf ein betrachtetes IT-System überträgt, weil auf diesem IT-System nur unwesentliche Teilbereiche der Anwendung laufen. Hier ist der Schutzbedarf zu relativieren **(Verteilungseffekt)**.

Beispiele: Der Verteilungseffekt tritt hauptsächlich bezüglich des Grundwertes Verfügbarkeit auf. So kann bei redundanter Auslegung von IT-Systemen der Schutzbedarf der Einzelkomponenten niedriger sein als der Schutzbedarf der Gesamtanwendung. Auch im Bereich der Vertraulichkeit sind Verteilungseffekte vorstellbar: Falls sichergestellt ist, dass ein Client nur unkritische Daten einer hochvertraulichen Datenbankanwendung abrufen kann, so besitzt der Client im Vergleich zum Datenbank-Server unter Umständen einen geringeren Schutzbedarf.

Darstellung der Ergebnisse

Die Ergebnisse der Schutzbedarfsfeststellung der IT-Systeme sollten wiederum in einer Tabelle festgehalten werden. Darin sollte verzeichnet sein, welchen Schutzbedarf jedes IT-System bezüglich Vertraulichkeit, Integrität und Verfügbarkeit hat. Der Gesamt-Schutzbedarf eines IT-Systems leitet sich wiederum aus dem Maximum des Schutzbedarfs bezüglich der drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit ab. Ein IT-System ist also hochschutzbedürftig, wenn es bezüglich eines oder mehrerer Grundwerte den Schutzbedarf "hoch" hat. Es ist im Allgemeinen aber sinnvoll, den Schutzbedarf eines IT-Systems für alle drei Grundwerte einzeln zu dokumentieren, da sich hieraus typischerweise verschiedene Arten von Sicherheitsmaßnahmen ergeben.

Bei einem IT-System kann sich beispielsweise der hohe Gesamt-Schutzbedarf daraus ableiten, dass der Schutzbedarf bezüglich Vertraulichkeit hoch ist, bezüglich Integrität und Verfügbarkeit allerdings normal. Dann kann zwar der Gesamt-Schutzbedarf mit hoch angegeben werden, dies zieht aber nicht nach sich, dass dadurch der Schutzbedarf bezüglich Integrität und Verfügbarkeit angehoben werden muss.

Die Festlegungen des Schutzbedarfs der IT-Systeme müssen begründet werden, damit die Entscheidungen auch für Außenstehende nachvollziehbar sind. Hier kann auf die Schutzbedarfsfeststellung der Anwendungen zurückverwiesen werden.

Beispiel: Bundesamt für Organisation und Verwaltung (BOV) - Teil 6

Die Ergebnisse der Schutzbedarfsfeststellung für die IT-Systeme können beispielsweise wie folgt dokumentiert werden (Auszug):

IT-System		Schutzbedarfsfeststellung		
Nr	**Beschreibung**	**Grundwert**	**Schutzbedarf**	**Begründung**
S1	Server für Personalverwaltung	Vertraulichkeit	hoch	Maximumprinzip
		Integrität	normal	Maximumprinzip
		Verfügbarkeit	normal	Maximumprinzip
S2	Domänen-Controller	Vertraulichkeit	normal	Maximumprinzip
		Integrität	hoch	Maximumprinzip
		Verfügbarkeit	normal	Gemäß der Schutzbedarfsfeststellung für Anwendung A4 ist von einem hohen Schutzbedarf für diesen Grundwert auszugehen. Zu berücksichtigen ist aber, dass diese Anwendung auf zwei Rechnersysteme verteilt ist. Eine Authentisierung über den zweiten Domänen-Controller S6 in Berlin ist für die Mitarbeiter des Bonner Standortes ebenfalls möglich. Ein Ausfall des Domänen-Controllers S2 kann bis zu 72 Stunden hingenommen werden. Der Schutzbedarf ist aufgrund dieses Verteilungseffekts daher "normal".

Hinweis: Besitzen die meisten Anwendungen auf einem IT-System nur einen normalen Schutzbedarf und sind nur eine oder wenige hochschutzbedürftig, so sollte in Erwägung gezogen werden, die hochschutzbedürftigen Anwendungen auf ein isoliertes IT-System auszulagern, da dies wesentlich gezielter abgesichert werden kann und somit häufig kostengünstiger ist. Eine solche Alternative kann dem Management zur Entscheidung vorgelegt werden.

Aktionspunkte zu 4.3.3 Schutzbedarfsfeststellung für IT-Systeme

- Schutzbedarf der IT-Systeme anhand des Schutzbedarfs der Anwendungen ermitteln
- Abhängigkeiten, das Maximumprinzip und gegebenenfalls den Kumulations- beziehungsweise Verteilungseffekt berücksichtigen
- Pro IT-System(-Gruppe) die Ergebnisse für Vertraulichkeit, Integrität und Verfügbarkeit sowie die Begründungen dokumentieren

4.3.4 Schutzbedarfsfeststellung für Räume

Aus den Ergebnissen der Schutzbedarfsfeststellung der Anwendungen und der IT-Systeme sollte abgeleitet werden, welcher Schutzbedarf für die jeweiligen Liegenschaften bzw. Räume resultiert. Dieser Schutzbedarf leitet sich aus dem Schutzbedarf der im jeweiligen Raum installierten IT-Systeme, verarbeiteten Informationen oder der Datenträger, die in diesem Raum gelagert und benutzt werden, nach dem Maximum-Prinzip ab. Dabei sollten eventuelle Abhängigkeiten und ein möglicher Kumulationseffekt berücksichtigt werden, wenn sich in einem Raum eine größere Anzahl von IT-Systemen, Datenträgern usw. befindet, wie typischerweise bei Serverräumen, Rechenzentren oder Datenträgerarchiven. Für jede Schutzbedarfseinschätzung sollte eine Begründung dokumentiert werden.

Hilfreich ist auch hier eine tabellarische Erfassung der notwendigen Informationen, aufbauend auf der bereits vorher erstellten Übersicht über die erfassten Räume.

Beispiel: Bundesamt für Organisation und Verwaltung (BOV) - Teil 7

Die folgende Tabelle zeigt einen Auszug aus den Ergebnissen der Schutzbedarfsfeststellung für die Räume des fiktiven Beispiels BOV:

Raum			IT / Informationen	Schutzbedarf		
Bezeichnung	**Art**	**Lokation**	**IT-Systeme / Datenträger**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**
R U.02	Datenträger-archiv	Gebäude Bonn	Backup-Datenträger (Wochensicherung der Server S1 bis S5)	hoch	hoch	normal
R B.02	Technikraum	Gebäude Bonn	TK-Anlage	normal	normal	hoch
R 1.01	Serverraum	Gebäude Bonn	S1, N4	hoch	hoch	normal
R 1.02 - R 1.06	Büroräume	Gebäude Bonn	C1	hoch	normal	normal
R 3.11	Schutzschrank im Raum R 3.11	Gebäude Bonn	Backup-Datenträger (Tagessicherung der Server S1 bis S5)	hoch	hoch	normal
R E.03	Serverraum	Gebäude Berlin	S6, N6, N7	normal	hoch	hoch
R 2.01 - R 2.40	Büroräume	Gebäude Berlin	C4, einige mit Faxgeräten	normal	normal	normal

Aktionspunkte zu 4.3.4 Schutzbedarfsfeststellung für Räume

- Schutzbedarf der Räume aus dem Schutzbedarf der IT-Systeme und Anwendungen ableiten
- Abhängigkeiten, das Maximumprinzip und gegebenenfalls den Kumulationseffekt berücksichtigen
- Ergebnisse und Begründungen nachvollziehbar dokumentieren

4.3.5 Schutzbedarfsfeststellung für Kommunikationsverbindungen

Nachdem die Schutzbedarfsfeststellung für die betrachteten Anwendungen, IT-Systeme und Räume abgeschlossen wurde, wird nun der Schutzbedarf bezüglich der Vernetzungsstruktur erarbeitet. Grundlage für die weiteren Überlegungen ist der in Kapitel 4.2.3 erarbeitete Netzplan des zu untersuchenden Informationsverbunds.

Um die Entscheidungen vorzubereiten, auf welchen Kommunikationsstrecken kryptographische Sicherheitsmaßnahmen eingesetzt werden sollten, welche Strecken redundant ausgelegt sein sollten und über welche Verbindungen Angriffe durch Innen- und Außentäter zu erwarten sind, müssen die Kommunikationsverbindungen analysiert werden. Hierbei werden folgende Kommunikationsverbindungen als kritisch gewertet:

- Kommunikationsverbindungen, die Außenverbindungen darstellen, d. h. die in oder über unkontrollierte Bereiche führen (z. B. ins Internet oder über öffentliches Gelände). Dazu können auch drahtlose Kommunikationsverbindungen gehören, da es hierbei schwierig ist, zu verhindern, dass auf diese von öffentlichem Gelände aus zugegriffen wird. Bei Außenverbindungen besteht die Gefahr, dass durch externe Angreifer Penetrationsversuche auf das zu schützende System vorgenommen oder Computer-Viren bzw. trojanische Pferde eingespielt werden können. Darüber hinaus können unter Umständen Innentäter über eine solche Verbindung vertrauliche Informationen nach außen übertragen. Auch in Bezug auf den Grundwert Verfügbarkeit sind Außenverbindungen oft besonders gefährdet.
- Kommunikationsverbindungen, über die hochschutzbedürftige Informationen übertragen werden, wobei dies sowohl Informationen mit einem hohen Anspruch an Vertraulichkeit wie auch Integrität oder Verfügbarkeit sein können. Diese Verbindungen können das Angriffsziel vorsätzlichen Abhörens oder vorsätzlicher Manipulation sein. Darüber hinaus kann der Ausfall einer solchen Verbindung die Funktionsfähigkeit wesentlicher Teile des Informationsverbundes beeinträchtigen.
- Kommunikationsverbindungen, über die bestimmte hochschutzbedürftige Informationen nicht übertragen werden dürfen. Hierbei kommen insbesondere vertrauliche Informationen in Betracht. Wenn beispielsweise Netzkoppelelemente ungeeignet oder falsch konfiguriert sind, kann der Fall eintreten, dass über eine solche Verbindung die Informationen, die gerade nicht übertragen werden sollen, trotzdem übertragen und damit angreifbar werden.

Bei der Erfassung der kritischen Kommunikationsverbindungen kann wie folgt vorgegangen werden. Zunächst werden sämtliche "Außenverbindungen" als kritische Verbindungen identifiziert und erfasst. Anschließend werden sämtliche Verbindungen untersucht, die von einem IT-System mit hohem oder sehr hohem Schutzbedarf ausgehen. Dabei werden diejenigen Verbindungen identifiziert, über die hochschutzbedürftige Informationen übertragen werden. Danach werden die Verbindungen untersucht, über die diese hochschutzbedürftigen Daten weiter übertragen werden. Abschließend sind die Kommunikationsverbindungen zu identifizieren, über die derlei Informationen nicht übertragen werden dürfen. Zu erfassen sind dabei:

- die Verbindungsstrecke,
- ob es sich um eine Außenverbindung handelt,
- ob hochschutzbedürftige Informationen übertragen werden und ob der Schutzbedarf aus der Vertraulichkeit, Integrität oder Verfügbarkeit resultiert und
- ob hochschutzbedürftige Informationen nicht übertragen werden dürfen.

Die Entscheidungen, welche Kommunikationsverbindungen als kritisch zu betrachten sind, sollten tabellarisch dokumentiert oder graphisch im Netzplan hervorgehoben werden.

Beispiel: Bundesamt für Organisation und Verwaltung (BOV) - Teil 8

Für das fiktive Beispiel BOV ergeben sich folgende kritischen Verbindungen:

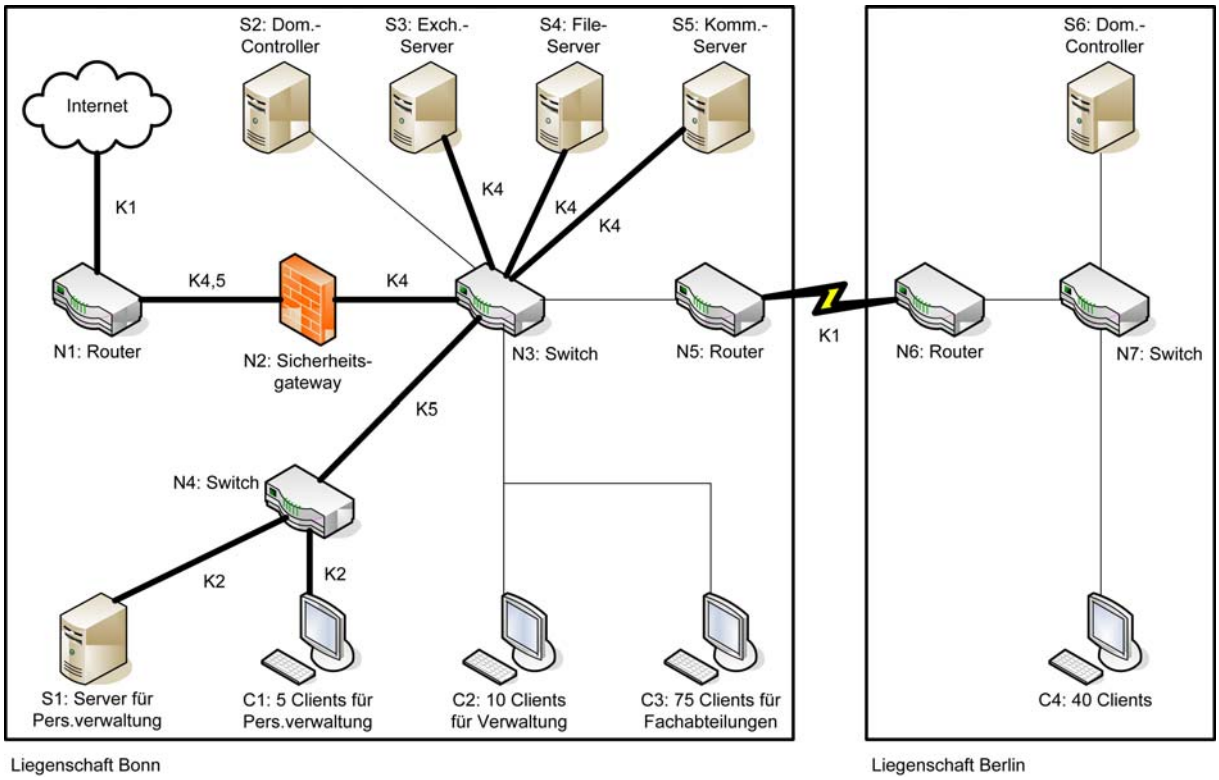


Abbildung 7: Beispiel eines Netzplans mit kritischen Verbindungen

In der graphischen Darstellung sind die kritischen Verbindungen durch "fette" Linien markiert. Die Zahlen nach dem Buchstaben "K" neben den Linien kennzeichnen den Grund (bzw. die Gründe), warum die jeweilige Verbindung kritisch ist, und sind in den Spaltenköpfen der nachfolgenden Tabelle erläutert.

	Kritisch aufgrund				
Verbindung	**K 1 Außenverbindung**	**K 2 hohe Vertraulichkeit**	**K 3 hohe Integrität**	**K 4 hohe Verfügbarkeit**	**K 5 keine Übertragung**
N1 - Internet	X				
N5 - N6	X				
S1 - N4		X			
S3 - N3				X	
S4 - N3				X	
S5 - N3				X	
C1 - N4		X			
N1 - N2				X	X
N2 - N3				X	
N4 - N3					X

Bei dieser Erhebung sollte besonders darauf geachtet werden, dass die erstellte Übersicht vollständig ist. Nur **eine** übersehene kritische Verbindung kann die Gesamtsicherheit unterlaufen. Außenverbindungen können beispielsweise über Festverbindungen, DSL-Zugänge, Fax-Anschlüsse, drahtlose Netze und ISDN-Schnittstellen aufgebaut werden. Viele moderne Laptops haben integrierte Schnittstellen für Modem- und Funk-Verbindungen. Multifunktionsgeräte, die zum Scannen, Kopieren und Drucken eingesetzt werden können, haben häufig ein eingebautes Modem, um Fax-Funktionen bereitstellen zu können. Wenn solche oder ähnliche Kommunikationswege genutzt werden, müssen sie systematisch in den Sicherheitsprozess integriert werden.

Aktionspunkte zu 4.3.5 Schutzbedarfsfeststellung für Kommunikationsverbindungen
• Außenverbindungen erfassen • Verbindungen, über die kritische Informationen übertragen werden, identifizieren • Verbindungen, über die bestimmte Informationen nicht übertragen werden dürfen, ermitteln • Alle kritischen Kommunikationsverbindungen in tabellarischer oder graphischer Form dokumentieren

4.3.6 Schlussfolgerungen aus den Ergebnissen der Schutzbedarfsfeststellung

Die bei der Schutzbedarfsfeststellung erzielten Ergebnisse bieten einen Anhaltspunkt für die weitere Vorgehensweise der Sicherheitskonzeption. Für den Schutz, der von den im IT-Grundschutz empfohlenen Standard-Sicherheitsmaßnahmen ausgeht, wird bezüglich der Schutzbedarfskategorien Folgendes angenommen:

Schutzwirkung von Standard-Sicherheitsmaßnahmen nach IT-Grundschutz	
Schutzbedarfskategorie "normal"	Standard-Sicherheitsmaßnahmen nach IT-Grundschutz sind im Allgemeinen ausreichend und angemessen.
Schutzbedarfskategorie "hoch"	Standard-Sicherheitsmaßnahmen nach IT-Grundschutz bilden einen Basisschutz, sind aber unter Umständen alleine nicht ausreichend. Weitergehende Maßnahmen können auf Basis einer ergänzenden Sicherheitsanalyse ermittelt werden.
Schutzbedarfskategorie "sehr hoch"	Standard-Sicherheitsmaßnahmen nach IT-Grundschutz bilden einen Basisschutz, reichen aber alleine im Allgemeinen nicht aus. Die erforderlichen zusätzlichen Sicherheitsmaßnahmen müssen individuell auf der Grundlage einer ergänzenden Sicherheitsanalyse ermittelt werden.

Außer bei hohem oder sehr hohem Schutzbedarf muss eine ergänzende Sicherheitsanalyse auch dann durchgeführt werden, wenn die Objekte des betrachteten Informationsverbundes

- mit den existierenden Bausteinen des IT-Grundschutzes nicht hinreichend abgebildet (modelliert) werden können oder
- in Einsatzszenarien (Umgebung, Anwendung) betrieben werden, die im Rahmen des IT-Grundschutzes nicht vorgesehen sind.

Ausführliche Informationen zur ergänzenden Sicherheitsanalyse finden sich in Kapitel 4.6.

Bereiche mit unterschiedlichem Schutzbedarf

Bei der Schutzbedarfsfeststellung zeigt sich häufig, dass es Bereiche innerhalb des betrachteten Informationsverbunds gibt, in denen Informationen verarbeitet werden, die einen hohen oder sehr hohen Schutzbedarf haben. Auch wenn nur wenige, herausgehobene Daten besonders schutzbedürftig sind, führt die starke Vernetzung und Kopplung von IT-Systemen und Anwendungen schnell dazu, dass sich der höhere Schutzbedarf nach dem Maximumprinzip auf andere Bereiche überträgt.

Um Risiken und Kosten eindämmen, sollten daher Sicherheitszonen zur Trennung von Bereichen mit unterschiedlichem Schutzbedarf eingerichtet werden. Solche Sicherheitszonen können sowohl räumlich, als auch technisch oder personell ausgeprägt sein.

Beispiele:

- Räumliche Sicherheitszonen: Um nicht jeden einzelnen Büroraum permanent abschließen oder überwachen zu müssen, sollten Zonen mit starkem Besucherverkehr von hoch-schutzbedürftigen Bereichen getrennt werden. So sollten sich Besprechungs-, Schulungs- oder Veranstaltungsräume

ebenso wie eine Kantine, die externes Publikum anzieht, in der Nähe des Gebäudeeingangs befinden. Der Zugang zu Gebäudeteilen mit Büros kann dann von einem Pförtner einfach überwacht werden. Besonders sensitive Bereiche wie eine Entwicklungsabteilung sollten mit einer zusätzlichen Zugangskontrolle z. B. über Chipkarten abgesichert werden.

- Technische Sicherheitszonen: Um vertrauliche Daten auf bestimmte Bereiche innerhalb eines LANs zu begrenzen und um zu verhindern, dass Störungen in bestimmten Komponenten oder Angriffe die Funktionsfähigkeit beeinträchtigen, ist es hilfreich, das LAN in mehrere Teilnetze aufzuteilen (siehe auch M 5.77 Bildung von Teilnetzen in den IT-Grundschutz-Katalogen).
- Personelle Sicherheitszonen: Grundsätzlich sollten an jede Person immer nur so viele Rechte vergeben werden, wie es für die Aufgabenwahrnehmung erforderlich ist. Darüber hinaus gibt es auch verschiedene Rollen, die eine Person nicht gleichzeitig wahrnehmen sollte. So sollte ein Revisor weder gleichzeitig in der Buchhaltung noch in der IT-Administration arbeiten, da er sich nicht selber kontrollieren kann und darf. Um die Vergabe von Zugangs- und Zutrittsrechte zu vereinfachen, sollten Personengruppen, die nicht miteinander vereinbare Funktionen wahrnehmen, in getrennten Gruppen oder Abteilungen arbeiten.

Bei der Planung neuer Geschäftsprozesse, Fachaufgaben oder Anwendungen sollte frühzeitig geprüft werden, ob es zweckmäßig ist, Sicherheitszonen einzurichten. Häufig kann dadurch in allen folgenden Phasen bis hin zur Revision viel Arbeit gespart werden.

Aktionspunkte zu 4.3.6 Schlussfolgerungen aus den Ergebnissen der Schutzbedarfsfeststellung
• Prüfen, ob Objekte mit erhöhten Sicherheitsanforderungen in Sicherheitszonen konzentriert werden können • Objekte mit erhöhten Sicherheitsanforderungen für eine ergänzende Sicherheitsanalyse vormerken

4.4 Auswahl und Anpassung von Maßnahmen

Nachdem die notwendigen Informationen aus der Strukturanalyse und der Schutzbedarfsfeststellung vorliegen, besteht die nächste zentrale Aufgabe darin, den betrachteten Informationsverbund mit Hilfe der vorhandenen Bausteine aus den IT-Grundschutz-Katalogen nachzubilden. Als Ergebnis wird ein IT-Grundschutz-Modell des Informationsverbunds erstellt, das aus verschiedenen, gegebenenfalls auch mehrfach verwendeten Bausteinen besteht und eine Abbildung zwischen den Bausteinen und den sicherheitsrelevanten Aspekten des Informationsverbunds beinhaltet.

4.4.1 Die IT-Grundschutz-Kataloge

Die IT-Grundschutz-Kataloge [GSK] können in der jeweils aktuellen Fassung vom BSI-Webserver heruntergeladen werden.

Bausteine

Die IT-Grundschutz-Kataloge enthalten die Gefährdungslage und die Maßnahmenempfehlungen für verschiedene Komponenten, Vorgehensweisen und IT-Systeme, die jeweils in einem Baustein zusammengefasst werden.

In jedem Baustein wird zunächst die zu erwartende Gefährdungslage beschrieben, wobei sowohl die typischen Gefährdungen als auch die pauschalisierten Eintrittswahrscheinlichkeiten berücksichtigt wurden. Diese Gefährdungslage ist Teil einer vereinfachten Risikoanalyse für typische Umgebungen der Informationsverarbeitung und bildet die Grundlage, auf der das BSI ein spezifisches Maßnahmenbündel aus den Bereichen Infrastruktur, Personal, Organisation, Hard- und Software, Kommunikation und Notfallvorsorge erarbeitet hat. Der Vorteil dabei ist, dass die Anwender bei typischen Anwendungsfällen keine aufwendigen Analysen benötigen, um das für einen durchschnittlichen Schutzbedarf notwendige Sicherheitsniveau zu erreichen. Vielmehr ist es in diesem Fall ausreichend, die für die

betrachteten Anwendungen, IT-Systeme oder Geschäftsprozesse relevanten Bausteine zu identifizieren und die darin empfohlenen Maßnahmen konsequent und vollständig umzusetzen. Auch wenn besondere Komponenten oder Einsatzumgebungen vorliegen, die im IT-Grundschutz nicht hinreichend behandelt werden, bieten die IT-Grundschutz-Kataloge dennoch eine wertvolle Arbeitshilfe. Die dann notwendige, ergänzende Sicherheitsanalyse kann sich auf die spezifischen Gefährdungen dieser Komponenten oder Rahmenbedingungen konzentrieren.

Um den Innovationsschüben und Versionswechseln im IT-Bereich Rechnung zu tragen, sind die IT-Grundschutz-Kataloge mit Hilfe der Baustein-Struktur modular aufgebaut und damit leicht erweiterbar und aktualisierbar.

Die Bausteine sind in die folgenden Schichten gruppiert:

B 1: Übergreifende Aspekte

B 2: Infrastruktur

B 3: IT-Systeme

B 4: Netze

B 5: Anwendungen

Gefährdungskataloge

Dieser Bereich enthält die ausführlichen Beschreibungen der Gefährdungen, die in den einzelnen Bausteinen als Gefährdungslage genannt wurden. Die Gefährdungen sind in fünf Kataloge gruppiert:

G 1: Höhere Gewalt

G 2: Organisatorische Mängel

G 3: Menschliche Fehlhandlungen

G 4: Technisches Versagen

G 5: Vorsätzliche Handlungen

Maßnahmenkataloge

Dieser Teil beschreibt die in den Bausteinen der IT-Grundschutz-Kataloge zitierten Sicherheitsmaßnahmen ausführlich. Die Maßnahmen sind in sechs Kataloge gruppiert:

M 1: Infrastruktur

M 2: Organisation

M 3: Personal

M 4: Hard- und Software

M 5: Kommunikation

M 6: Notfallvorsorge

4.4.2 Modellierung eines Informationsverbunds

Das erstellte IT-Grundschutz-Modell ist unabhängig davon, ob der Informationsverbund aus bereits im Einsatz befindlichen IT-Systemen besteht oder ob es sich um einen Informationsverbund handelt, der sich erst im Planungsstadium befindet. Jedoch kann das Modell unterschiedlich verwendet werden:

- Das IT-Grundschutz-Modell eines bereits realisierten Informationsverbundes identifiziert über die verwendeten Bausteine die relevanten Standard-Sicherheitsmaßnahmen. Es kann in Form eines **Prüfplans** benutzt werden, um einen Soll-Ist-Vergleich durchzuführen.

- Das IT-Grundschutz-Modell eines geplanten Informationsverbundes stellt hingegen ein **Entwicklungskonzept** dar. Es beschreibt über die ausgewählten Bausteine, welche Standard-Sicherheitsmaßnahmen bei der Realisierung des Informationsverbunds umgesetzt werden müssen.

Die Einordnung der Modellierung und die möglichen Ergebnisse verdeutlicht das folgende Bild:

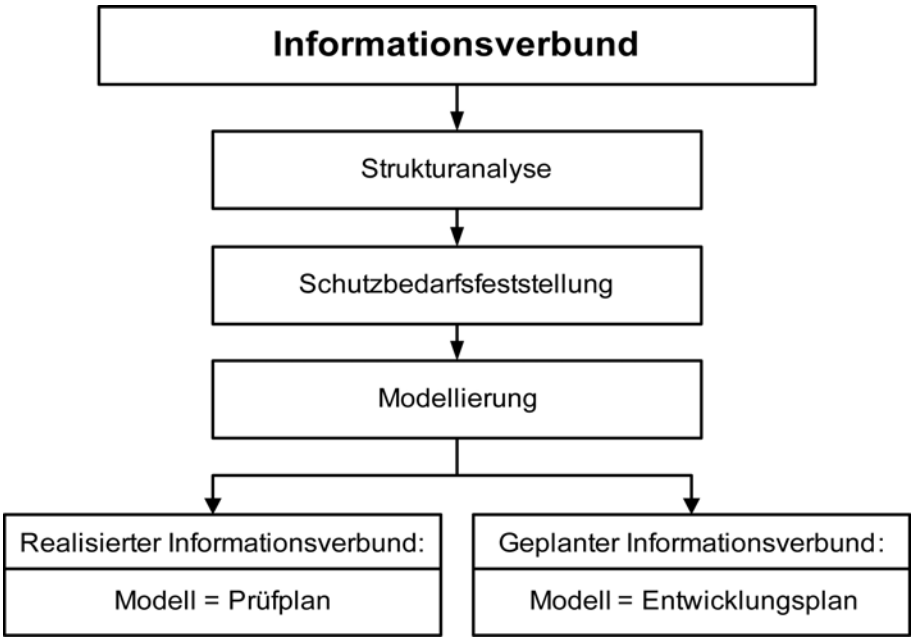


Abbildung 8: Ergebnis der Modellierung nach IT-Grundschutz

Typischerweise wird ein im Einsatz befindlicher Informationsverbund sowohl realisierte als auch in Planung befindliche Anteile besitzen. Das resultierende IT-Grundschutz-Modell beinhaltet dann sowohl einen Prüfplan wie auch Anteile eines Entwicklungskonzepts. Alle im Prüfplan bzw. im Entwicklungskonzept vorgesehenen Sicherheitsmaßnahmen bilden dann gemeinsam die Basis für die Erstellung des Sicherheitskonzepts. Dazu gehören neben den bereits umgesetzten Sicherheitsmaßnahmen die bei Durchführung des Soll-Ist-Vergleichs als unzureichend oder fehlend identifizierte Maßnahmen, sowie diejenigen, die sich für die in Planung befindlichen Anteile des Informationsverbunds ergeben.

Für die Abbildung eines im Allgemeinen komplexen Informationsverbundes auf die Bausteine der IT-Grundschutz-Kataloge bietet es sich an, die Sicherheitsaspekte gruppiert nach bestimmten Themen zu betrachten.

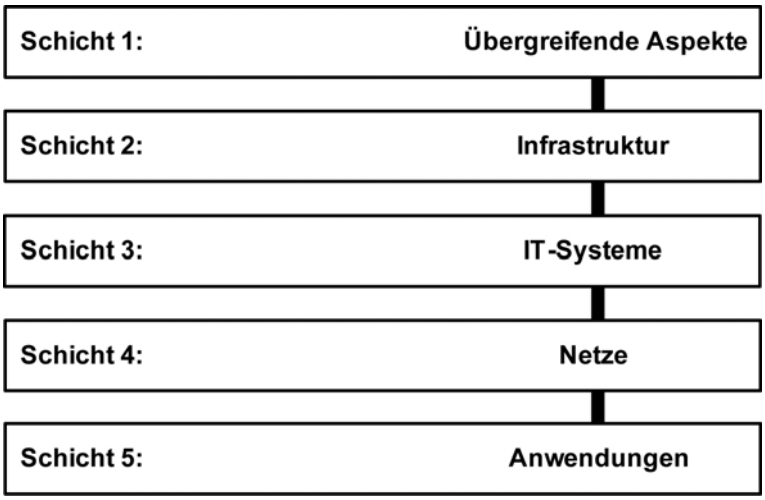


Abbildung 9: Schichten des IT-Grundschutz-Modells

Die Sicherheitsaspekte eines Informationsverbunds werden wie folgt den einzelnen Schichten zugeordnet:

- Schicht 1 umfasst die übergreifenden Sicherheitsaspekte, die für sämtliche oder große Teile des Informationsverbunds gleichermaßen gelten. Dies betrifft insbesondere übergreifende Konzepte und die daraus abgeleiteten Regelungen. Typische Bausteine der Schicht 1 sind unter anderem *Sicherheitsmanagement, Organisation, Datensicherungskonzept* und *Computer-Viren-Schutzkonzept*.
- Schicht 2 befasst sich mit den baulich-technischen Gegebenheiten, in der Aspekte der infrastrukturellen Sicherheit zusammengeführt werden. Dies betrifft insbesondere die Bausteine *Gebäude, Serverraum, Schutzschränke* und *Häuslicher Arbeitsplatz*.
- Schicht 3 betrifft die einzelnen IT-Systeme des Informationsverbunds, die ggf. in Gruppen zusammengefasst wurden. Hier werden die Sicherheitsaspekte sowohl von Clients als auch von Servern, aber auch von Einzelplatz-Systemen behandelt. In diese Schicht fallen beispielsweise die Bausteine *TK-Anlage, Laptop,* sowie *Client unter Windows XP*.
- Schicht 4 betrachtet die Vernetzungsaspekte, die sich nicht auf bestimmte IT-Systeme, sondern auf die Netzverbindungen und die Kommunikation beziehen. Dazu gehören zum Beispiel die Bausteine *Heterogene Netze, WLAN,* sowie *Remote Access*.
- Schicht 5 schließlich beschäftigt sich mit den eigentlichen Anwendungen, die im Informationsverbund genutzt werden. In dieser Schicht können unter anderem die Bausteine *E-Mail, Webserver, Faxserver* und *Datenbanken* zur Modellierung verwendet werden.

Die Einteilung in diese Schichten hat folgende Vorteile:

- Die Komplexität der Informationssicherheit wird reduziert, indem eine sinnvolle Aufteilung der Einzelaspekte vorgenommen wird.
- Da übergeordnete Aspekte und gemeinsame infrastrukturelle Fragestellungen getrennt von den IT-Systemen betrachtet werden, werden Redundanzen vermieden, weil diese Aspekte nur einmal bearbeitet werden müssen und nicht wiederholt für jedes IT-System.
- Die einzelnen Schichten sind so gewählt, dass auch die Zuständigkeiten für die betrachteten Aspekte gebündelt sind. Hauptsächlich betrifft Schicht 1 Grundsatzfragen des sicheren Umgangs mit Informationen, Schicht 2 den Bereich Haustechnik, Schicht 3 die Ebene der Administratoren und IT-Benutzer, Schicht 4 die Netz- und Systemadministratoren und Schicht 5 schließlich die Anwendungsverantwortlichen und -betreiber.
- Aufgrund der Aufteilung der Sicherheitsaspekte in Schichten können Einzelaspekte in resultierenden Sicherheitskonzepten leichter aktualisiert und erweitert werden, ohne dass andere Schichten umfangreich tangiert werden.

Die Modellierung nach IT-Grundschutz besteht nun darin, für die Bausteine einer jeden Schicht zu entscheiden, ob und wie sie zur Abbildung des Informationsverbunds herangezogen werden können. Je nach betrachtetem Baustein können die Zielobjekte dieser Abbildung von unterschiedlicher Art sein: einzelne Geschäftsprozesse oder Komponenten, Gruppen von Komponenten, Gebäude, Liegenschaften, Organisationseinheiten usw.

Das IT-Grundschutz-Modell, also die Zuordnung von Bausteinen zu Zielobjekten sollte in Form einer Tabelle mit folgenden Spalten dokumentiert werden:

- Nummer und Titel des Bausteins
- Zielobjekt oder Zielgruppe: Dies kann z. B. die Identifikationsnummer einer Komponente oder einer Gruppe bzw. der Name eines Gebäudes oder einer Organisationseinheit sein.
- Ansprechpartner: Diese Spalte dient zunächst nur als Platzhalter. Der Ansprechpartner wird nicht im Rahmen der Modellierung, sondern erst bei der Planung des eigentlichen Soll-Ist-Vergleichs im Basis-Sicherheitscheck ermittelt.

- Hinweise: In dieser Spalte können Randinformationen und Begründungen für die Modellierung dokumentiert werden.

Beispiel: Bundesamt für Organisation und Verwaltung (BOV) - Teil 9

Die folgende Tabelle ist ein Auszug aus der Modellierung für das fiktive Bundesamt BOV:

Nr.	Titel des Bausteins	Zielobjekt/ Zielgruppe	Ansprechpartner	Hinweise
B 1.1	Organisation	Standort Bonn		Der Baustein Organisation muss für die Standorte Bonn und Berlin separat bearbeitet werden, da in Berlin eigene organisatorische Regelungen gelten.
B 1.1	Organisation	Standort Berlin		
B 1.2	Personal	gesamtes BOV		Die Personalverwaltung des BOV erfolgt zentral in Bonn.
B 2.5	Datenträgerarchiv	R U.02 (Bonn)		In diesem Raum werden die Backup-Datenträger aufbewahrt.
B 3.203	Laptop	C5		Die Laptops in Bonn bzw. Berlin werden jeweils in einer Gruppe zusammengefasst.
B 3.203	Laptop	C6		
B 5.4	Webserver	S5		S5 dient als Server für das Intranet.
B 5.7	Datenbanken	S5		Auf dem Server S5 kommt eine Datenbank zum Einsatz.

Eine detaillierte Beschreibung der Vorgehensweise zur Modellierung eines Informationsverbunds findet sich in den IT-Grundschutz-Katalogen im Kapitel "Schichtenmodell und Modellierung". Dabei wird besonderer Wert auf die Randbedingungen gelegt, wann ein einzelner Baustein sinnvollerweise eingesetzt werden soll und auf welche Zielobjekte er anzuwenden ist.

4.4.3 Anpassung von Maßnahmen

Über die Modellierung wurden die Bausteine der IT-Grundschutz-Kataloge ausgewählt, die für die einzelnen Zielobjekte des betrachteten Informationsverbunds umzusetzen sind. In den Bausteinen werden Sicherheitsmaßnahmen vorgeschlagen, die typischerweise für diese Komponenten geeignet und angemessen sind.

Für die Erstellung eines Sicherheitskonzeptes oder für ein Audit müssen jetzt die einzelnen Maßnahmen durchgearbeitet werden. IT-Grundschutz-Maßnahmen sind einerseits so formuliert, dass sie in möglichst vielen Umgebungen anwendbar sind, und andererseits, dass die Maßnahmenbeschreibungen ausführlich genug sind, um als Umsetzungshilfe dienen zu können.

Dies bedeutet aber auch, dass die vorgeschlagenen Maßnahmen noch an die jeweiligen Rahmenbedingungen einer Institution angepasst werden müssen. Es kann beispielsweise sinnvoll sein,

- Maßnahmen weiter zu konkretisieren, also z. B. um technische Details zu ergänzen,
- Maßnahmen dem Sprachgebrauch der Institution anzupassen, also z. B. andere Rollenbezeichnungen zu verwenden,
- aus Maßnahmen die im betrachteten Bereich nicht relevanten Empfehlungen zu streichen.

Generell sollten die Maßnahmentexte immer sinngemäß umgesetzt werden. Alle Änderungen gegenüber den IT-Grundschutz-Katalogen sollten dokumentiert werden, damit die Gründe auch später noch nachvollziehbar sind.

Um den Anwendern die zielgruppengerechte Anpassung der IT-Grundschutz-Texte zu erleichtern, werden sämtliche Texte, Bausteine, Gefährdungen, Maßnahmen, Tabellen und Hilfsmittel auch in elektronischer Form zur Verfügung gestellt. Damit können diese Texte bei der Erstellung eines Sicherheitskonzeptes und bei der Realisierung von Maßnahmen weiterverwendet werden.

Bei der Sichtung der Maßnahmen kann sich auch ergeben, dass einzelne vorgeschlagene IT-Grundschutz-Maßnahmen unter den konkreten Rahmenbedingungen entbehrlich sind. Dies kann beispielsweise der Fall sein, wenn den entsprechenden Gefährdungen mit anderen adäquaten Maßnahmen entgegengewirkt wird, oder die Maßnahmenempfehlungen nicht relevant sind (z. B. weil Dienste nicht aktiviert wurden). Zusätzliche oder gestrichene Sicherheitsmaßnahmen sollten im Sicherheitskonzept dokumentiert werden. Dies erleichtert auch die Durchführung des Basis-Sicherheitschecks.

Bei der Auswahl und Anpassung der Maßnahmen ist zu beachten, dass diese immer angemessen sein müssen. Angemessen bedeutet:

- Wirksamkeit (Effektivität): Sie müssen vor den möglichen Gefährdungen wirksam schützen, also den identifizierten Schutzbedarf abdecken.
- Eignung: Sie müssen in der Praxis tatsächlich umsetzbar sein, dürfen also z. B. nicht die Organisationsabläufe behindern oder andere Sicherheitsmaßnahmen aushebeln.
- Praktikabilität: Sie sollen leicht verständlich, einfach anzuwenden und wenig fehleranfällig sein.
- Akzeptanz: Sie müssen für alle Benutzer anwendbar (barrierefrei) sein und dürfen niemanden diskriminieren oder beeinträchtigen.
- Wirtschaftlichkeit: Mit den eingesetzten Mitteln sollte ein möglichst gutes Ergebnis erreicht werden. Die Maßnahmen sollten also einerseits das Risiko bestmöglich minimieren und andererseits in geeignetem Verhältnis zu den zu schützenden Werten stehen.

Aktionspunkte zu 4.4 Auswahl und Anpassung von Maßnahmen
• Kapitel "Schichtenmodell und Modellierung" aus den IT-Grundschutz-Katalogen systematisch durcharbeiten • Für jeden Baustein der IT-Grundschutz-Kataloge ermitteln, auf welche Zielobjekte er im betrachteten Informationsverbund anzuwenden ist • Zuordnung von Bausteinen zu Zielobjekten ("IT-Grundschutz-Modell") sowie die entsprechenden Ansprechpartner dokumentieren • Zielobjekte, die nicht geeignet modelliert werden können, für eine ergänzende Sicherheitsanalyse vormerken • Maßnahmentexte aus den identifizierten Bausteinen sorgfältig lesen und gegebenenfalls anpassen

4.5 Basis-Sicherheitscheck

Für die nachfolgenden Betrachtungen wird vorausgesetzt, dass für einen ausgewählten Informationsverbund folgende Teile des Sicherheitskonzepts nach IT-Grundschutz erstellt wurden:

Anhand der Strukturanalyse des Informationsverbundes wurde eine Übersicht über die vorhandene IT, deren Einsatzorte und die unterstützten Anwendungen erstellt. Darauf aufbauend wurde anschließend die Schutzbedarfsfeststellung durchgeführt, deren Ergebnis eine Übersicht über den Schutzbedarf der Anwendungen, der IT-Systeme, der genutzten Räume und der Kommunikationsverbindungen ist. Mit Hilfe dieser Informationen wurde die Modellierung des Informationsverbundes nach IT-Grundschutz durchgeführt. Das Ergebnis war eine Abbildung des betrachteten Informationsverbundes auf Bausteine des IT-Grundschutzes.

Die Modellierung nach IT-Grundschutz wird nun als Prüfplan benutzt, um anhand eines Soll-Ist-Vergleichs herauszufinden, welche Standard-Sicherheitsmaßnahmen ausreichend oder nur unzureichend umgesetzt sind.

Dieses Kapitel beschreibt, wie bei der Durchführung des Basis-Sicherheitschecks vorgegangen werden sollte. Der Basis-Sicherheitscheck besteht aus drei unterschiedlichen Schritten. Im ersten Schritt werden die organisatorischen Vorbereitungen getroffen, insbesondere die relevanten Ansprechpartner für den Soll-Ist-Vergleich ausgewählt. Im zweiten Schritt wird der eigentliche Soll-Ist-Vergleich mittels Interviews und stichprobenartiger Kontrolle durchgeführt. Im letzten Schritt werden die erzielten Ergebnisse des Soll-Ist-Vergleichs einschließlich der erhobenen Begründungen dokumentiert.

Nachfolgend werden die Schritte des Basis-Sicherheitschecks detailliert beschrieben.

4.5.1 Organisatorische Vorarbeiten für den Basis-Sicherheitscheck

Für die reibungslose Durchführung des Soll-Ist-Vergleichs sind einige Vorarbeiten erforderlich. Zunächst sollten alle hausinternen Papiere, z. B. Organisationsverfügungen, Arbeitshinweise, Sicherheitsanweisungen, Handbücher und "informelle" Vorgehensweisen, die die sicherheitsrelevanten Abläufe regeln, gesichtet werden. Diese Dokumente können bei der Ermittlung des Umsetzungsgrades hilfreich sein, insbesondere bei Fragen nach bestehenden organisatorischen Regelungen. Weiterhin ist zu klären, wer gegenwärtig für deren Inhalt zuständig ist, um später die richtigen Ansprechpartner bestimmen zu können.

Als Nächstes sollte festgestellt werden, ob und in welchem Umfang externe Stellen bei der Ermittlung des Umsetzungsstatus beteiligt werden müssen. Dies kann beispielsweise bei externen Rechenzentren, vorgesetzten Behörden, Firmen, die Teile von Geschäftsprozessen oder des IT-Betriebes als Outsourcing-Dienstleistung übernehmen, oder Baubehörden, die für infrastrukturelle Maßnahmen zuständig sind, erforderlich sein.

Ein wichtiger Schritt vor der Durchführung des eigentlichen Soll-Ist-Vergleichs ist die Ermittlung geeigneter Interviewpartner. Hierzu sollte zunächst für jeden einzelnen Baustein, der für die Modellierung des vorliegenden Informationsverbunds herangezogen wurde, ein Hauptansprechpartner festgelegt werden.

- Bei den Bausteinen der Schicht 1 "Übergreifende Aspekte" ergibt sich ein geeigneter Ansprechpartner in der Regel direkt aus der im Baustein behandelten Thematik. Beispielsweise sollte für den Baustein B 1.2 *Personal* ein Mitarbeiter der zuständigen Personalabteilung als Ansprechpartner ausgewählt werden. Bei den konzeptionellen Bausteinen, z. B. Baustein B 1.4 *Datensicherungskonzept*, steht im Idealfall der Mitarbeiter zur Verfügung, der für die Fortschreibung des entsprechenden Dokuments zuständig ist. Anderenfalls sollte derjenige Mitarbeiter befragt werden, zu dessen Aufgabengebiet die Fortschreibung von Regelungen in dem betrachteten Bereich gehören.
- Im Bereich der Schicht 2 "Infrastruktur" sollte die Auswahl geeigneter Ansprechpartner in Abstimmung mit der Abteilung Innerer Dienst/Haustechnik vorgenommen werden. Je nach Größe der betrachteten Institution können beispielsweise unterschiedliche Ansprechpartner für die Infrastrukturbereiche Gebäude und Schutzschränke zuständig sein. In kleinen Institutionen kann in vielen Fällen der Hausmeister Auskunft geben. Zu beachten ist im Bereich Infrastruktur, dass hier unter Umständen externe Stellen zu beteiligen sind. Dies betrifft insbesondere größere Institutionen.
- In Bausteinen der Schicht 3 "IT-Systeme" und Schicht 4 "Netze" werden in den zu prüfenden Sicherheitsmaßnahmen verstärkt technische Aspekte behandelt. In der Regel kommt daher der Administrator derjenigen Komponente bzw. Gruppe von Komponenten, der der jeweilige Baustein bei der Modellierung zugeordnet wurde, als Hauptansprechpartner in Frage.
- Für die Bausteine der Schicht 5 "Anwendungen" sollten die Betreuer bzw. die Verantwortlichen der einzelnen Anwendungen als Hauptansprechpartner ausgewählt werden.

In vielen Fällen kann der Hauptansprechpartner nicht zu allen Fragen des jeweiligen Bausteins umfassend Auskunft geben. Dann ist es vorteilhaft, eine oder auch mehrere zusätzliche Personen in das Interview einzubeziehen. Hinweise dazu, welche Mitarbeiter hinzugezogen werden sollten, lassen sich den Einträgen "Verantwortlich für Initiierung" und "Verantwortlich für Umsetzung", die sich am Anfang jeder Maßnahmenbeschreibung befinden, entnehmen.

Für die anstehenden Interviews mit den Systemverantwortlichen, Administratoren und sonstigen Ansprechpartnern sollte ein Terminplan erstellt werden. Besonderes Augenmerk gilt hier der Terminkoordination mit Personen aus anderen Organisationseinheiten oder anderen Institutionen. Außerdem ist es sinnvoll, Ausweichtermine mit abzustimmen.

Je nach Größe der Projektgruppe sollten für die Durchführung der Interviews Teams mit verteilten Aufgaben gebildet werden. Es hat sich bewährt, in Gruppen mit je zwei Personen zu arbeiten. Dabei notiert eine Person die Ergebnisse und Anmerkungen zu den Antworten, die andere stellt die notwendigen Fragen.

Aktionspunkte zu 4.5.1 Organisatorische Vorarbeiten des Basis-Sicherheitschecks

- Hausinterne Dokumente mit Verfügungen und Regelungen sichten und Zuständigkeiten für diese Unterlagen klären
- Feststellen, in welchem Umfang externe Stellen beteiligt werden müssen
- Hauptansprechpartner für jeden in der Modellierung angewandten Baustein festlegen
- Terminplan für Interviews abstimmen
- Team für Interviews zusammenstellen

4.5.2 Durchführung des Soll-Ist-Vergleichs

Sind alle erforderlichen Vorarbeiten erledigt, kann die eigentliche Erhebung an den zuvor festgesetzten Terminen beginnen. Hierzu werden die Maßnahmen des jeweiligen Bausteins, für den die Interviewpartner zuständig sind, der Reihe nach durchgearbeitet.

Als Antworten bezüglich des Umsetzungsstatus der einzelnen Maßnahmen kommen folgende Aussagen in Betracht:

"entbehrlich"	-	Die Umsetzung der Maßnahmenempfehlungen ist in der vorgeschlagenen Art nicht notwendig, weil andere adäquate Maßnahmen gegen die entsprechenden Gefährdungen wirken (z. B. Maßnahmen, die nicht im IT-Grundschutz aufgeführt sind, aber dieselbe Wirkung erzielen), oder weil die Maßnahmenempfehlungen nicht relevant sind (z. B. weil Dienste nicht aktiviert wurden).
"ja"	-	Alle Empfehlungen in der Maßnahme sind vollständig, wirksam und angemessen umgesetzt.
"teilweise"	-	Einige der Empfehlungen sind umgesetzt, andere noch nicht oder nur teilweise.
"nein"	-	Die Empfehlungen der Maßnahme sind größtenteils noch nicht umgesetzt.

Es ist nicht zu empfehlen, bei den Interviews den Text der Maßnahmenempfehlung vorzulesen, da er nicht für ein Zwiegespräch konzipiert wurde. Deshalb ist die inhaltliche Kenntnis des Bausteins für den Interviewer notwendig, ergänzend sollten vorher griffige Checklisten mit Stichworten erstellt werden. Um im Zweifelsfall Unstimmigkeiten klären zu können, ist es jedoch sinnvoll, den Volltext der Maßnahmen griffbereit zu haben. Es ist aber nicht empfehlenswert, während des Interviews die Antworten direkt in einen PC einzugeben, da es alle Beteiligten ablenkt und für ungewollte Unterbrechungen der Kommunikation sorgt.

Es schafft eine entspannte, aufgelockerte und produktive Arbeitsatmosphäre, das Interview mit einleitenden Worten zu beginnen und den Zweck des Basis-Sicherheitschecks kurz vorzustellen. Es bietet sich an, mit der Maßnahmenüberschrift fortzufahren und die Maßnahme kurz zu erläutern. Besser als einen Monolog zu führen ist es, dem Gegenüber die Möglichkeit zu geben, auf die bereits umgesetzten Maßnahmenteile einzugehen, und danach noch offene Punkte zu besprechen.

Die Befragungstiefe richtet sich zunächst nach dem Niveau von Standard-Sicherheitsmaßnahmen, darüber hinausgehende Aspekte hochschutzbedürftiger Anwendungen sollten erst nach Abschluss des Basis-Sicherheitschecks betrachtet werden. Falls der Bedarf besteht, die in den Interviews gemachten Aussagen zu verifizieren, bietet es sich an, stichprobenartig die entsprechenden Regelungen und Konzepte zu sichten, im Bereich Infrastruktur gemeinsam mit dem Ansprechpartner die zu untersuchenden Objekte vor Ort zu besichtigen sowie Client- bzw. Servereinstellungen an ausgewählten IT-Systemen zu überprüfen.

Zum Abschluss jeder Maßnahme sollte den Befragten das Ergebnis (Umsetzungsstatus der Maßnahme: entbehrlich/ja/teilweise/nein) mitgeteilt und diese Entscheidung erläutert werden.

Aktionspunkte zu 4.5.2 Durchführung des Soll-Ist-Vergleichs

- Je nach Fachgebiet vorab Checklisten erstellen
- Zielsetzung des Basis-Sicherheitschecks den Interviewpartnern erläutern
- Umsetzungsstatus der einzelnen Maßnahmen erfragen
- Antworten anhand von Stichproben am Objekt verifizieren
- Ergebnisse den Befragten mitteilen

4.5.3 Dokumentation der Ergebnisse

Die Ergebnisse des Basis-Sicherheitschecks sollten so dokumentiert werden, dass sie für alle Beteiligten nachvollziehbar sind und als Grundlage für die Umsetzungsplanung der defizitären Maßnahmen genutzt werden können. Um die Dokumentation der Ergebnisse des Basis-Sicherheitschecks zu erleichtern, bietet das BSI zwei Hilfsmittel an.

Dies ist zum einen das GSTOOL des BSI. Diese Software unterstützt die gesamte Vorgehensweise nach IT-Grundschutz, beginnend bei der Stammdatenerfassung, über die Schutzbedarfsfeststellung, die ergänzende Sicherheits- und Risikoanalyse sowie den Soll-Ist-Vergleich (Basis-Sicherheitscheck) bis hin zur Umsetzung der Maßnahmen. Hierdurch ergeben sich komfortable Möglichkeiten zur Auswertung und Revision der Ergebnisse, z. B. die Suche nach bestimmten Einträgen, Generierung von Reports, Kostenauswertungen sowie Statistikfunktionen.

Außerdem stehen als Hilfsmittel zum IT-Grundschutz Formulare zur Verfügung. Zu jedem Baustein der IT-Grundschutz-Kataloge gibt es eine Datei im Word-Format, in der tabellarisch für jede Maßnahme des Bausteins die Ergebnisse des Soll-Ist-Vergleichs erfasst werden können.

Zunächst sollten in die dafür vorgesehenen Felder im GSTOOL oder in den Formularen

- die Nummer und die Bezeichnung der Komponente oder Gruppe von Komponenten, der der Baustein bei der Modellierung zugeordnet wurde,
- der Standort der zugeordneten Komponente bzw. Gruppe von Komponenten,
- das Erfassungsdatum und der Name des Erfassers und
- die befragten Ansprechpartner

eingetragen werden. Die eigentlichen Ergebnisse des Soll-Ist-Vergleichs werden in der auf dem Formular vorbereiteten Tabelle erfasst. Dabei sollten zu jeder Maßnahme des jeweiligen Bausteins die Felder wie folgt ausgefüllt werden:

- Umsetzungsgrad (entbehrlich/ja/teilweise/nein)
  Hier wird der im Interview ermittelte Umsetzungsstatus der jeweiligen Maßnahme erfasst.
- Umsetzung bis
  Dieses Feld wird während des Basis-Sicherheitschecks im Allgemeinen nicht ausgefüllt. Es dient als Platzhalter, um in der Realisierungsplanung an dieser Stelle zu dokumentieren, bis zu welchem Termin die Maßnahme vollständig umgesetzt sein soll.
- verantwortlich
  Falls es bei der Durchführung des Soll-Ist-Vergleichs eindeutig ist, welcher Mitarbeiter für die vollständige Umsetzung einer defizitären Maßnahme verantwortlich sein wird, so kann dies in diesem Feld dokumentiert werden. Falls die Verantwortung nicht eindeutig erkennbar ist, sollte das Feld freigelassen werden. Im Zuge der späteren Realisierungsplanung wird dann ein Verantwortlicher bestimmt, dessen Name hier eingetragen werden kann.
- Bemerkungen / Begründung für Nicht-Umsetzung
  Bei Maßnahmen, deren Umsetzung entbehrlich erscheint, ist hier die Begründung bzw. die Ersatzmaßnahme zu nennen. Bei Maßnahmen, die noch nicht oder nur teilweise umgesetzt sind, sollte in diesem Feld dokumentiert werden, welche Empfehlungen der Maßnahme noch umgesetzt werden müssen. In dieses Feld sollten auch alle anderen Bemerkungen eingetragen werden, die bei der Beseitigung von Defiziten hilfreich oder im Zusammenhang mit der Maßnahme zu berücksichtigen sind.
- Kostenschätzung
  Bei Maßnahmen, die noch nicht oder nur teilweise umgesetzt sind, kann in dieses Feld eine Schätzung eingetragen werden, welchen finanziellen und personellen Aufwand die Beseitigung der Defizite erfordert.

Aktionspunkte zu 4.5.3 Dokumentation der Ergebnisse
• Stamminformationen über jedes Zielobjekt in Tool, Datenbank oder Formular eintragen
• Informationen zum Basis-Sicherheitscheck und zum Umsetzungsstatus eintragen
• Felder beziehungsweise Platzhalter für die Realisierungsplanung vorsehen

4.6 Ergänzende Sicherheitsanalyse

Die Standard-Sicherheitsmaßnahmen des IT-Grundschutzes sind in der Regel für typische Geschäftsprozesse, Anwendungen und IT-Systeme mit normalem Schutzbedarf angemessen und ausreichend. In bestimmten Fällen müssen die IT-Grundschutz-Maßnahmen jedoch mit Hilfe einer Risikoanalyse um spezielle Sicherheitsmaßnahmen ergänzt werden.

4.6.1 Zweistufiger Ansatz der IT-Grundschutz-Vorgehensweise

Aus Effizienzgründen verfolgt der IT-Grundschutz eine zweistufige Vorgehensweise. Während der ersten Stufe wird der Schutzbedarf der Objekte des Informationsverbundes ermittelt. Mit Hilfe der Modellierung werden den Zielobjekten typische Gefährdungen und entsprechende Standard-Sicherheitsmaßnahmen zugeordnet. Dabei wird pauschal von einem üblichen Einsatzszenario und von einem normalen Schutzbedarf ausgegangen. Anhand der Bausteine der IT-Grundschutz-Kataloge kann auf diese Weise das Sicherheitsniveau des Informationsverbundes schnell und effizient erhöht werden. Zusammenfassend dient die erste Stufe dazu, Sicherheitsmaßnahmen aufzuzeigen, die den elementaren Risiken entgegenwirken, die in der Praxis nahezu immer auftreten. In der ersten Stufe der IT-Grundschutz-Vorgehensweise wird also bereits eine grundlegende Risikobehandlung durchgeführt.

Darüber hinaus wird in einer zweiten Stufe untersucht, ob weitere relevante Risiken für den Informationsverbund zu berücksichtigen sind.

4.6.2 Vorgehensweise zur ergänzenden Sicherheitsanalyse

Die ergänzende Sicherheitsanalyse ist für alle Zielobjekte des Informationsverbundes durchzuführen, die

- einen hohen oder sehr hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit haben oder
- mit den existierenden Bausteinen der IT-Grundschutz-Kataloge nicht hinreichend abgebildet (modelliert) werden können oder
- in Einsatzszenarien (z. B. in Umgebungen oder mit Anwendungen) betrieben werden, die im Rahmen des IT-Grundschutzes nicht vorgesehen sind.

Das Ziel ist dabei, für die einzelnen Zielobjekte jeweils zu entscheiden, ob weitere Risikobetrachtungen erforderlich sind. Beispiele für Anwendungen oder IT-Systeme, für die eine ergänzende Sicherheitsanalyse empfehlenswert ist, sind das Online-Banking-Angebot eines Finanzdienstleisters und IT-Systeme mit speziellen Echtzeitbetriebssystemen.

Um den Aufwand zu verringern, sollte bei der ergänzenden Sicherheitsanalyse eine geeignete Gruppenbildung der Zielobjekte vorgenommen werden. Dies gilt beispielsweise auch für kritische Kommunikationsverbindungen. Solche Verbindungen können häufig zu kritischen Netzbereichen, Teilnetzen, Kommunikationssträngen etc. zusammengefasst werden.

In einem **Management-Report** ist für jedes Zielobjekt beziehungsweise für jede Gruppe von Zielobjekten, die eine oder mehrere der obigen Eigenschaften hat, stichhaltig zu begründen, ob eine weitere Risikobetrachtung erforderlich ist oder nicht. Die Zielobjekte, die eine weitere Risikobetrachtung erforderlich machen, werden zu Risikobereichen zusammengefasst. Es soll dabei deutlich werden, für welche Bereiche eine zusätzliche Risikobetrachtung erforderlich ist.

Grundlage für die im Rahmen der ergänzenden Sicherheitsanalyse zu treffenden Entscheidungen sind die übergeordneten Geschäftsziele der Institution, die Risikogrundsätze sowie gegebenenfalls auch die Ressourcenpriorisierung. Der Management-Report wird der Institutionsleitung kommuniziert und muss von ihr verabschiedet werden. Die Verantwortung liegt somit bei dem Management.

Beispiel: Bundesamt für Organisation und Verwaltung (BOV) – Teil 10

Aufgrund der Schutzbedarfsfeststellung und der besonderen Einsatzbedingungen müssen im BOV eine Reihe von ergänzenden Sicherheitsanalysen durchgeführt werden. Die folgende Tabelle zeigt einen Ausschnitt aus den Ergebnissen:

Zielobjekt	Ergänzende Sicherheitsanalyse, Auszüge aus dem Management-Report
Domänen-Controller S2	Aufgrund seiner zentralen administrativen Funktion bestehen an den Domänen-Controller S2 hohe Anforderungen in Bezug auf Integrität. Das System verfügt bereits über einige interne Mechanismen zum Schutz vor absichtlichen oder unabsichtlichen Manipulationen. Einige technische Zusatzmaßnahmen wurden geprüft, wegen mangelnder Kompatibilität mit anderen eingesetzten Produkten jedoch wieder verworfen. Die IT-Leitung schlägt deshalb vor, den erhöhten Sicherheitsanforderungen des Systems S2 auf organisatorischer Ebene durch häufige und regelmäßige Audits der IT-Revision Rechnung zu tragen. Auf eine weiterführende Risikoanalyse für S2 kann in diesem Fall verzichtet werden.
Kritische Kommunikationsverbindungen N1-N2/Internet	Die Gefährdungslage, die sich durch die Anbindung des BOV an das Internet ergibt, hat sich im Berichtszeitraum stetig erhöht. Hervorzuheben sind hier insbesondere die Problemfelder Spam und Schadsoftware. Die IT-Leitung empfiehlt deshalb, für die Internet-Anbindung eine Risikoanalyse durchzuführen.
Kritische Kommunikationsverbindungen N3-S3/S4/S5/N2	An die genannten Kommunikationsverbindungen bestehen erhöhte Anforderungen in Bezug auf Verfügbarkeit. Im Zuge der technischen Neustrukturierung, die für das nächste Quartal geplant und genehmigt ist, wird der zentrale Switch N3 abgelöst. Die neue Struktur wird redundant ausgelegt sein, um Single-Points-of-Failure konsequent zu vermeiden. Da es sich bei den genannten kritischen Kommunikationsverbindungen deshalb nur noch um Übergangslösungen handelt, empfiehlt die IT-Leitung, auf eine Risikoanalyse für diese Verbindungen vorerst zu verzichten.
Serverraum R E.03 in Berlin	Die Anforderungen an die Verfügbarkeit der in R E.03 in Berlin betriebenen Informationstechnik sind erheblich. Eine Risikoanalyse für diesen Serverraum liegt zwar vor, ist jedoch veraltet. Die IT-Leitung empfiehlt deshalb, für R E.03 in Berlin eine neue Risikoanalyse durchzuführen.

Der vollständige Management-Report wird der Leitungsebene zur Verabschiedung vorgelegt.

Hinweis: Die in obiger Tabelle aufgeführten Vorschläge der IT-Leitung des BOV sind Beispiele und keine Empfehlungen des BSI für diesen fiktiven Anwendungsfall.

4.6.3 Risikoanalyse auf der Basis von IT-Grundschutz

Eine Risikoanalyse im Kontext der Informationssicherheit hat die Aufgabe, relevante Gefährdungen für den Informationsverbund zu identifizieren und die daraus möglicherweise resultierenden Risiken abzuschätzen. Das Ziel ist es, die Risiken durch angemessene Gegenmaßnahmen auf ein akzeptables Maß zu reduzieren, die Restrisiken transparent zu machen und dadurch das Gesamtrisiko systematisch zu steuern.

Im Rahmen der IT-Grundschutz-Vorgehensweise entscheidet die Leitungsebene auf der Basis des Management-Reports der ergänzenden Sicherheitsanalyse, für welche Zielobjekte eine Risikoanalyse durchgeführt wird. Der mit der Durchführung von Risikoanalysen verbundene Aufwand konzentriert

sich somit auf die Bereiche, bei denen die Institution eine solche Risikoanalyse für zweckdienlich und gewinnbringend einschätzt.

Für die Umsetzung der Entscheidungen, die in der ergänzenden Sicherheitsanalyse getroffen wurden, empfiehlt das BSI die Anwendung einer *Risikoanalyse auf der Basis von IT-Grundschutz*, wie sie im BSI-Standard 100-3 beschrieben ist.

Die dort beschriebene Methodik lässt sich wie folgt in den IT-Grundschutz-Prozess integrieren:

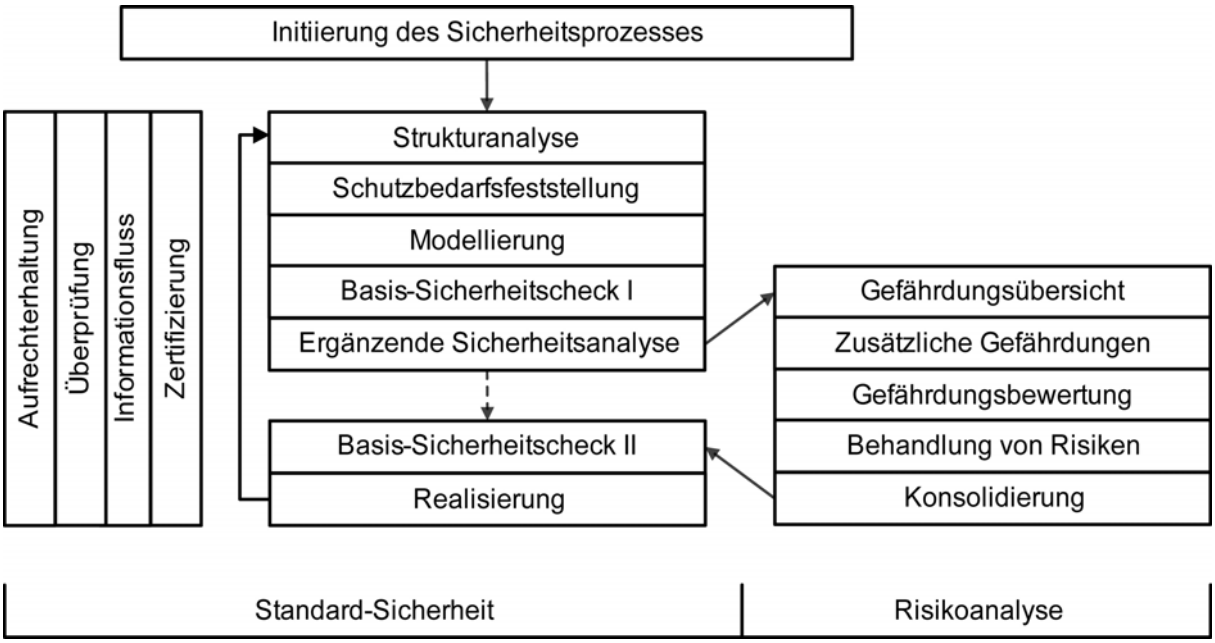


Abbildung 10: Integration der Risikoanalyse in den IT-Grundschutz-Prozess

Im Vordergrund steht die Frage: Welchen Gefährdungen für den Informationsverbund ist durch die Standard-Sicherheitsmaßnahmen des IT-Grundschutzes noch nicht ausreichend oder sogar noch gar nicht Rechnung getragen?

Zur Beantwortung dieser Frage empfiehlt die *Risikoanalyse auf der Basis von IT-Grundschutz* folgende zusätzliche Arbeitsschritte, die hier kurz im Überblick aufgeführt sind:

- Erstellung der Gefährdungsübersicht
  In diesem ersten Arbeitsschritt wird für jedes zu analysierende Zielobjekt eine Liste der jeweils relevanten IT-Grundschutz-Gefährdungen zusammengestellt.
- Ermittlung zusätzlicher Gefährdungen
  Die aus den IT-Grundschutz-Katalogen entnommenen Gefährdungen werden in diesem Schritt durch zusätzliche Gefährdungen ergänzt, die sich aus dem spezifischen Einsatzszenario ergeben. Dies erfolgt im Rahmen eines gemeinsamen Brainstormings.
- Gefährdungsbewertung
  Für jedes Zielobjekt und für jede Gefährdung wird geprüft, ob die bislang vorgesehenen Sicherheitsmaßnahmen einen ausreichenden Schutz bieten. Die Prüfkriterien sind dabei Vollständigkeit, Mechanismenstärke und Zuverlässigkeit.
- Maßnahmenauswahl zur Behandlung von Risiken
  Die Leitungsebene muss vorgeben, wie die erkannten Risiken behandelt werden sollen. In der Regel werden dazu Vorschläge und Optionen vom IS-Management ausgearbeitet. Es gibt folgende Optionen zur Behandlung von Risiken:
  - Risiken können durch entsprechende Sicherheitsmaßnahmen reduziert werden.

- Risiken können vermieden werden (z. B. durch Umstrukturierung von Geschäftsprozessen oder des Informationsverbundes).
- Risiken können verlagert werden (z. B. durch Outsourcing oder Versicherungen).
- Risiken können akzeptiert werden.

Die Entscheidungen, wie die verschiedenen Sicherheitsrisiken zu behandeln sind, sind im Sicherheitskonzept zu dokumentieren. Dabei muss auch das Restrisiko bewertet und nachvollziehbar dokumentiert werden.

- Konsolidierung des Sicherheitskonzepts
  Bevor der originäre IT-Grundschutz-Prozess fortgesetzt werden kann, muss das erweiterte Sicherheitskonzept konsolidiert werden. Dabei werden die Eignung, das Zusammenwirken, die Benutzerfreundlichkeit und die Angemessenheit der Sicherheitsmaßnahmen insgesamt überprüft.

Außerdem wird in der *Risikoanalyse auf der Basis von IT-Grundschutz* erläutert, wie die Methodik anzuwenden ist, wenn der Informationsverbund Zielobjekte umfasst, für die in den IT-Grundschutz-Katalogen bislang kein geeigneter Baustein enthalten ist.

Eine ausführliche Darstellung der Methodik findet sich im BSI-Standard 100-3.

Wichtig: Die *Risikoanalyse auf der Basis von IT-Grundschutz* ist eine Vorgehensweise, um bei Bedarf Sicherheitsvorkehrungen zu ermitteln, die über die in den IT-Grundschutz-Katalogen genannten Maßnahmen hinausgehen. Obwohl diese Methodik gegenüber vielen anderen ähnlichen Verfahren vereinfacht wurde, ist sie oft mit erheblichem Aufwand verbunden. Um schnellstmöglich die wichtigsten Sicherheitsprobleme zu beseitigen, ist es manchmal zweckmäßig, *zuerst* die IT-Grundschutz-Maßnahmen vollständig umzusetzen und erst *danach* eine Risikoanalyse durchzuführen (abweichend von obigem Schema). Dadurch müssen zwar insgesamt einige Schritte öfter durchlaufen werden, die IT-Grundschutz-Maßnahmen werden jedoch früher umgesetzt. Diese alternative Reihenfolge bietet sich besonders dann an, wenn

1. der betrachtete Informationsverbund bereits realisiert und in Betrieb ist und
2. die vorliegenden Zielobjekte mit den existierenden Bausteinen der IT-Grundschutz-Kataloge hinreichend modelliert werden können.

Für geplante Informationsverbünde oder für solche mit untypischen Techniken bzw. Einsatzszenarien wird dagegen die oben abgebildete, originäre Reihenfolge empfohlen. Die folgende Tabelle fasst die jeweiligen Vor- und Nachteile der beiden alternativen Reihenfolgen zusammen:

Risikoanalyse direkt nach dem Basis-Sicherheitscheck	**Risikoanalyse erst nach vollständiger Umsetzung der IT-Grundschutz-Maßnahmen**
Mögliche Vorteile: • Es wird Mehraufwand vermieden, da keine Maßnahmen umgesetzt werden, die im Rahmen der Risikoanalyse eventuell durch stärkere Maßnahmen ersetzt werden. • Eventuell erforderliche Hochsicherheitsmaßnahmen werden früher identifiziert und umgesetzt.	Mögliche Vorteile: • IT-Grundschutz-Maßnahmen werden früher umgesetzt, da die Risikoanalyse häufig aufwendig ist. • Elementare Sicherheitslücken werden vorrangig behandelt, bevor fortgeschrittene Gefährdungen analysiert werden.

Risikoanalyse direkt nach dem Basis-Sicherheitscheck	**Risikoanalyse erst nach vollständiger Umsetzung der IT-Grundschutz-Maßnahmen**
Mögliche Nachteile: • IT-Grundschutz-Maßnahmen werden später umgesetzt, da die Risikoanalyse häufig aufwendig ist. • Eventuell werden elementare Sicherheitslücken vernachlässigt, während fortgeschrittene Gefährdungen analysiert werden.	Mögliche Nachteile: • Es kann Mehraufwand entstehen, da eventuell einige IT-Grundschutz-Maßnahmen umgesetzt werden, die später im Rahmen der Risikoanalyse durch stärkere Maßnahmen ersetzt werden. • Eventuell erforderliche Hochsicherheitsmaßnahmen werden erst später identifiziert und umgesetzt.

Wichtig ist außerdem, dass eine *Risikoanalyse auf der Basis von IT-Grundschutz* häufig leichter durchzuführen ist, wenn sie nacheinander auf kleine Teilaspekte des Informationsverbunds angewandt wird. Als ersten Schritt kann die Analyse beispielsweise auf die baulich-physische Infrastruktur beschränkt werden, das heißt auf den Schutz vor Brand, Wasser und unbefugtem Zutritt sowie auf die ordnungsgemäße Strom- und Klimaversorgung.

In vielen Behörden und Unternehmen existieren bereits Verfahren zur Risikoanalyse beziehungsweise zur Risikobehandlung. Um eine einheitliche Methodik zu erreichen, kann es in solchen Fällen zweckmäßig sein, die vorhandenen Verfahren auf die Informationssicherheit auszudehnen und gegebenenfalls nur Teilaspekte des BSI-Standards 100-3 anzuwenden. International haben sich eine Reihe von unterschiedlichen Ansätzen zur Durchführung von Risikoanalysen im Bereich der Informationssicherheit etabliert. Diese Verfahren unterscheiden sich beispielsweise in Bezug auf den Detaillierungsgrad, die Formalisierung und die thematischen Schwerpunkte. Abhängig von den Rahmenbedingungen einer Institution und der Art des Informationsverbunds kann es zweckmäßig sein, alternativ zum BSI-Standard 100-3 ein anderes etabliertes Verfahren oder eine angepasste Methodik für die Analyse von Informationsrisiken zu verwenden.

Die grundsätzliche Vorgehensweise der Institution zur Durchführung von Risikoanalysen sollte in einer Richtlinie dokumentiert und durch die Leitungsebene verabschiedet werden. Die **Richtlinie für die Durchführung von Risikoanalysen** sollte unter anderem folgende Aspekte umfassen:

- Unter welchen Voraussetzungen kann im Rahmen der ergänzenden Sicherheitsanalyse entschieden werden, auf eine Risikoanalyse zu verzichten?
- Unter welchen Voraussetzungen muss in jedem Fall eine Risikoanalyse durchgeführt werden?
- Welche Methodik beziehungsweise welcher Standard wird für die Durchführung von Risikoanalysen herangezogen?
- Wie wird die gewählte Methodik auf die speziellen Belange der Institution angepasst?
- Welche Organisationseinheiten sind für welche Teilaufgaben der Risikoanalyse verantwortlich?
- Auf welche Weise werden Risikoanalysen in den Sicherheitsprozess integriert, beispielsweise vor oder nach Umsetzung der IT-Grundschutz-Maßnahmen?
- Welche Berichtspflichten bestehen im Rahmen von Risikoanalysen?

Aktionspunkte zu 4.6 Ergänzende Sicherheitsanalyse
• Grundsätzliche Vorgehensweise der Institution zur Durchführung von Risikoanalysen in einer Richtlinie dokumentieren und der Leitungsebene zur Verabschiedung vorlegen • Ermitteln, für welche Zielobjekte oder Gruppen von Zielobjekten eine Risikoanalyse durchgeführt werden soll

- Management-Report für die ergänzende Sicherheitsanalyse erstellen
- Management-Report der Leitungsebene zur Verabschiedung vorlegen
- Falls erforderlich, BSI-Standard 100-3 "Risikoanalyse auf der Basis von IT-Grundschutz" systematisch durcharbeiten
- Ergebnisse der Risikoanalysen in das Sicherheitskonzept integrieren

5 Umsetzung der Sicherheitskonzeption

In diesem Kapitel werden verschiedene Aspekte vorgestellt, die bei der Planung und Realisierung von Sicherheitsmaßnahmen beachtet werden müssen. Dabei wird beschrieben, wie die Umsetzung von Sicherheitsmaßnahmen geplant, durchgeführt, begleitet und überwacht werden kann.

Bei der Erstellung der Sicherheitskonzeption sind für den untersuchten Informationsverbund die Strukturanalyse, die Schutzbedarfsfeststellung und die Modellierung erfolgt. Ebenso liegen zu diesem Zeitpunkt die Ergebnisse des Basis-Sicherheitschecks, also des daran anschließenden Soll-Ist-Vergleichs, vor. Sollte für ausgewählte Bereiche eine Risikoanalyse durchgeführt worden sein, so sollten die dabei erarbeiteten Maßnahmenvorschläge ebenfalls vorliegen und nachfolgend berücksichtigt werden.

Für die Realisierung der Maßnahmen stehen in der Regel nur beschränkte Ressourcen an Geld und Personal zur Verfügung. Ziel der nachfolgend beschriebenen Schritte ist daher, eine möglichst effiziente Umsetzung der vorgesehenen Sicherheitsmaßnahmen zu erreichen. Ein Beispiel zur Erläuterung der Vorgehensweise findet sich am Ende dieses Kapitels.

5.1 Sichtung der Untersuchungsergebnisse

In einer Gesamtsicht sollten zuerst die fehlenden oder nur teilweise umgesetzten IT-Grundschutz-Maßnahmen ausgewertet werden. Dazu bietet es sich an, aus den Ergebnissen des Basis-Sicherheitschecks alle nicht umgesetzten bzw. nur teilweise umgesetzten Maßnahmen zu extrahieren und in einer Tabelle zusammenzufassen.

Durch Risikoanalysen können eventuell weitere zu realisierende Maßnahmen identifiziert worden sein. Diese sollten ebenfalls tabellarisch erfasst werden. Diese zusätzlichen Maßnahmen sollten den vorher betrachteten Zielobjekten der Modellierung und den entsprechenden IT-Grundschutz-Bausteinen thematisch zugeordnet werden.

5.2 Konsolidierung der Maßnahmen

In diesem Schritt werden zunächst die noch umzusetzenden Sicherheitsmaßnahmen konsolidiert. Falls zusätzliche Risikoanalysen durchgeführt wurden, können hierdurch Sicherheitsmaßnahmen hinzugekommen sein, die Maßnahmen aus den IT-Grundschutz-Katalogen ergänzen oder auch ersetzen. Hierbei wird geprüft, für welche IT-Grundschutz-Maßnahmen die Umsetzung entfallen kann, da zu realisierende höherwertige Sicherheitsmaßnahmen sie ersetzen.

Da im IT-Grundschutz für eine Vielzahl von verschiedenen Organisationsformen und technischen Ausgestaltungen Empfehlungen gegeben werden, müssen die ausgewählten Maßnahmen eventuell noch konkretisiert bzw. an die organisatorischen und technischen Gegebenheiten der Institution angepasst werden. Außerdem sollten alle Sicherheitsmaßnahmen noch einmal daraufhin überprüft werden, ob sie auch geeignet sind: Sie müssen vor den möglichen Gefährdungen wirksam schützen, aber auch in der Praxis tatsächlich umsetzbar sein, dürfen also z. B. nicht die Organisationsabläufe behindern oder andere Sicherheitsmaßnahmen aushebeln. In solchen Fällen kann es notwendig werden, bestimmte IT-Grundschutz-Maßnahmen durch adäquate andere Sicherheitsmaßnahmen zu ersetzen.

Um auch später noch nachvollziehen zu können, wie die konkrete Maßnahmenliste erstellt und verfeinert wurde, sollte dies geeignet dokumentiert werden.

Weiterführende Hinweise zur Konsolidierung der Sicherheitsmaßnahmen finden sich außerdem im BSI-Standard 100-3.

Beispiele:

- In einer Risikoanalyse wurde festgestellt, dass zusätzlich zu den IT-Grundschutz-Maßnahmen auch eine chipkartengestützte Authentisierung und lokale Verschlüsselung der Festplatten an

Clients der Personaldatenverarbeitung notwendig sind. Diese zusätzliche Maßnahme würde die Maßnahme M 4.48 *Passwortschutz unter NT-basierten Windows-Systemen* für die Clients der Personaldatenverarbeitung ersetzen.

- Im Basis-Sicherheitscheck wurde festgestellt, dass die Maßnahme M 1.24 *Vermeidung von wasserführenden Leitungen* nicht realisiert und aufgrund der baulichen Gegebenheiten nicht wirtschaftlich umsetzbar ist. Stattdessen sollten als Ersatzmaßnahme unter den wasserführenden Leitungen Wasser ableitende Bleche installiert werden, die gleichzeitig von einem Wassermelder überwacht werden. Die Meldung wird beim Pförtner aufgeschaltet, so dass im Schadensfall der entstehende Wasserschaden zügig entdeckt und eingegrenzt werden kann.

5.3 Kosten- und Aufwandsschätzung

Da das Budget zur Umsetzung von Sicherheitsmaßnahmen praktisch immer begrenzt ist, sollte für jede zu realisierende Maßnahme festgehalten werden, welche Investitionskosten und welcher Personalaufwand dafür benötigt werden. Hierbei sollte zwischen einmaligen und wiederkehrenden Investitionskosten bzw. Personalaufwand unterschieden werden. An dieser Stelle zeigt sich häufig, dass Einsparungen bei der Technik einen hohen fortlaufenden Personaleinsatz verursachen.

In diesem Zusammenhang ist zu ermitteln, ob alle identifizierten Maßnahmen wirtschaftlich umsetzbar sind. Falls es Maßnahmen gibt, die nicht finanzierbar sind, sollten Überlegungen angestellt werden, durch welche Ersatzmaßnahmen sie ersetzt werden können oder ob das Restrisiko, das durch die fehlende Maßnahme entsteht, tragbar ist. Diese Entscheidung ist ebenfalls zu dokumentieren.

Stehen die geschätzten Ressourcen für Kosten und Personaleinsatz zur Verfügung, so kann zum nächsten Schritt übergegangen werden. In vielen Fällen muss jedoch noch eine Entscheidung herbeigeführt werden, wie viel Ressourcen für die Umsetzung der Sicherheitsmaßnahmen eingesetzt werden sollen. Hierfür bietet es sich an, für die Entscheidungsebene (Management, IT-Leiter, IT-Sicherheitsbeauftragter, ...) eine Präsentation vorzubereiten, in der die Ergebnisse der Sicherheitsuntersuchung dargestellt werden. Geordnet nach Schutzbedarf sollten die festgestellten Schwachstellen (fehlende oder unzureichend umgesetzte Sicherheitsmaßnahmen) zur Sensibilisierung vorgestellt werden. Darüber hinaus bietet es sich an, die für die Realisierung der fehlenden Maßnahmen anfallenden Kosten und den zu erwartenden Aufwand aufzubereiten. Im Anschluss an diese Präsentation sollte eine Entscheidung über das Budget erfolgen.

Kann kein ausreichendes Budget für die Realisierung aller fehlenden Maßnahmen bereitgestellt werden, so sollte aufgezeigt werden, welches Restrisiko dadurch entsteht, dass einige Maßnahmen nicht oder verzögert umgesetzt werden. Zu diesem Zweck können die sogenannten Kreuzreferenztabellen aus den Hilfsmitteln zum IT-Grundschutz hinzugezogen werden. Die Kreuzreferenztabellen geben für jeden Baustein eine Übersicht darüber, welche Maßnahmen gegen welche Gefährdungen wirken. Analog lässt sich anhand dieser Tabellen ebenfalls ermitteln, welche Gefährdungen aus den IT-Grundschutz-Katalogen nicht ausreichend abgedeckt werden. Das entstehende Restrisiko sollte für zufällig eintretende oder absichtlich herbeigeführte Gefährdungen transparent beschrieben und der Leitungsebene zur Entscheidung vorgelegt werden. Die weiteren Schritte können erst nach der Entscheidung der Leitungsebene, dass das Restrisiko tragbar ist, erfolgen, da die Leitungsebene die Verantwortung für die Konsequenzen tragen muss.

5.4 Festlegung der Umsetzungsreihenfolge der Maßnahmen

Wenn das vorhandene Budget oder die personellen Ressourcen nicht ausreichen, um sämtliche fehlenden Maßnahmen sofort umsetzen zu können, muss eine Umsetzungsreihenfolge festgelegt werden. Bei der Festlegung der Reihenfolge sollten folgende Aspekte berücksichtigt werden:

- Die Umsetzungsreihenfolge sollte sich zunächst an der Lebenszyklus-Einordnung der Maßnahmen orientieren. In jedem Baustein gibt es eine Übersicht, welche Maßnahmen in welcher Lebenszyklus-Phase, also in welcher zeitlichen Reihenfolge umgesetzt werden sollten. Natürlich

sollte mit den Maßnahmen der Phase "Planung und Konzeption" begonnen werden, bevor diejenigen aus den Phasen "Umsetzung" und "Betrieb" bearbeitet werden.

- Zu jeder Maßnahme wird außerdem eine Einstufung angegeben, inwieweit sie für die IT-Grundschutz-Qualifizierung erforderlich ist. Die Qualifizierungsstufe (A-Einstieg, B-Aufbau, C-Zertifikat, Z-Zusätzlich, W-Wissen) einer Maßnahme gibt häufig Hinweise auf den Stellenwert, den die jeweilige Maßnahme im Sicherheitskonzept hat. A-Maßnahmen sind in vielen Fällen besonders wichtig und sollten deshalb vorrangig umgesetzt werden.
- Bei einigen Maßnahmen ergibt sich durch logische Zusammenhänge eine zwingende zeitliche Reihenfolge. So sind zwar die Maßnahmen M 2.25 *Dokumentation der Systemkonfiguration* und M 2.26 *Ernennung eines Administrators und eines Vertreters* beide sehr wichtig, aber ohne Administrator kann M 2.25 kaum umgesetzt werden.
- Manche Maßnahmen erzielen eine große Breitenwirkung, manche jedoch nur eine eingeschränkte lokale Wirkung. Oft ist es sinnvoll, zuerst auf die Breitenwirkung zu achten.
- Es gibt Bausteine, die auf das angestrebte Sicherheitsniveau eine größeren Einfluss haben als andere. Maßnahmen eines solchen Bausteins sollten bevorzugt behandelt werden, insbesondere wenn hierdurch Schwachstellen in hochschutzbedürftigen Bereichen beseitigt werden. So sollten immer zunächst die Server abgesichert werden (unter anderem durch Umsetzung des Bausteins B 3.101 *Allgemeiner Server*) und dann erst die angeschlossenen Clients.
- Bausteine mit auffallend vielen nicht umgesetzten Maßnahmen repräsentieren Bereiche mit vielen Schwachstellen. Sie sollten ebenfalls bevorzugt behandelt werden.

Die Entscheidung, welche Sicherheitsmaßnahmen ergriffen oder verschoben werden und wo Restrisiken akzeptiert werden, sollte auch aus juristischen Gründen sorgfältig dokumentiert werden. In Zweifelsfällen sollten hierfür weitere Meinungen eingeholt und diese ebenfalls dokumentiert werden, um in späteren Streitfällen die Beachtung der erforderlichen Sorgfaltspflicht belegen zu können.

5.5 Festlegung der Aufgaben und der Verantwortung

Nach der Bestimmung der Reihenfolge für die Umsetzung der Maßnahmen muss anschließend festgelegt werden, wer bis wann welche Maßnahmen realisieren muss. Ohne eine solche Festlegung verzögert sich die Realisierung erfahrungsgemäß erheblich bzw. unterbleibt ganz. Dabei ist darauf zu achten, dass der als verantwortlich Benannte ausreichende Fähigkeiten und Kompetenzen zur Umsetzung der Maßnahmen besitzt und dass ihm die erforderlichen Ressourcen zur Verfügung gestellt werden.

Ebenso ist festzulegen, wer für die Überwachung der Realisierung verantwortlich ist bzw. an wen der Abschluss der Realisierung der einzelnen Maßnahmen zu melden ist. Typischerweise wird die Meldung an den IT-Sicherheitsbeauftragten erfolgen. Der Fortschritt der Realisierung sollte regelmäßig nachgeprüft werden, damit die Realisierungsaufträge nicht verschleppt werden.

Der nun fertig gestellte Realisierungsplan sollte mindestens folgende Informationen umfassen:

- Beschreibung des Zielobjektes als Einsatzumfeld,
- Nummer des betrachteten Bausteins,
- Maßnahmentitel bzw. Maßnahmenbeschreibung,
- Terminplanung für die Umsetzung,
- Budget-Rahmen,
- Verantwortliche für die Umsetzung und
- Verantwortliche für die Überwachung der Realisierung.

5.6 Realisierungsbegleitende Maßnahmen

Überaus wichtig ist es, notwendige realisierungsbegleitende Maßnahmen rechtzeitig zu konzipieren und für die Realisierung mit einzuplanen. Zu diesen Maßnahmen gehören insbesondere Sensibilisierungsmaßnahmen, die darauf zielen, die Belange der Informationssicherheit zu verdeutlichen und die von neuen Sicherheitsmaßnahmen betroffenen Mitarbeiter über die Notwendigkeit und die Konsequenzen der Maßnahmen zu unterrichten.

Darüber hinaus müssen die betroffenen Mitarbeiter geschult werden, die neuen Sicherheitsmaßnahmen korrekt um- und einzusetzen. Wird diese Schulung unterlassen, können die Maßnahmen oft nicht umgesetzt werden und verlieren ihre Wirkung, wenn sich die Mitarbeiter unzureichend informiert fühlen, was oft zu einer ablehnenden Haltung gegenüber der Informationssicherheit führt.

Beispiel: Bundesamt für Organisation und Verwaltung (BOV) – Teil 11

Die obigen Schritte werden nachfolgend anhand des fiktiven Beispiels BOV auszugsweise beschrieben. In folgender Tabelle werden einige zu realisierende Maßnahmen einschließlich der Kostenschätzungen dargestellt.

Zielobjekt	Baustein	Maßnahme	Status	Kosten	Bemerkung
Gesamte Organisation	B 1.9	M 2.11 Regelung des Passwortgebrauchs	T	a) 0,- Euro b) 2 PT c) 0,- Euro/Jahr d) 0,5 PT/Jahr	
Serverraum R 3.10	B 2.4	Z 1 Installation von Wasser ableitenden Blechen mit Überwachung mittels eines Wassermelders und Aufschaltung auf den Pförtner	N	a) 4000,- Euro b) 3 PT c) 0,- Euro/Jahr d) 1 PT/Jahr	Ersetzt Maßnahme M 1.24
Server S4	B 3.101	M 1.28 Lokale unterbrechungsfreie Stromversorgung	N	a) 1000,- Euro b) 1 PT c) 0,- Euro/Jahr d) 0,5 PT/Jahr	
Gruppe Clients C1	B 3.207	Z 2 chipkartengestützte Authentisierung und lokale Verschlüsselung der Festplatten	N	a) 1400,- Euro b) 2 PT c) 0,- Euro/Jahr d) 2 PT/Jahr	Diese zusätzliche Maßnahme ersetzt die Maßnahme M 4.1 in Baustein B 1.9.
...					

Legende:

- Maßnahme
  Z 1 = Zusatzmaßnahme 1 (zusätzlich zu IT-Grundschutz-Maßnahmen)
- Status (= Umsetzungsstatus)
  T = Teilweise erfüllt, N = Nicht realisiert
- Kosten:
  a) = einmalige Investitionskosten
  b) = einmaliger Personalaufwand (PT = Personentage)
  c) = wiederkehrende Investitionskosten
  d) = wiederkehrender Personalaufwand (PT = Personentage)

Als nächstes wird der tabellarische Realisierungsplan (Auszug) dargestellt, der sich nach der Managemententscheidung aus obiger Tabelle ergeben würde.

Realisierungsplan (Stand 01.09.20xy)						
Zielobjekt	**Baust**	**Maßnahme**	**Umset-**	**Verant-**	**Budget-**	**Bemer-**

Realisierungsplan (Stand 01.09.20xy)						
	ein		**zung bis**	**wortlich**	**Rahmen**	**kung**
Gesamte Organisation	B 1.9	M 2.11 Regelung des Passwortgebrauchs	31.12. 20xy	a) Herr Müller b) Frau Meier	a) 0,- Euro b) 2 PT c) 0,- Euro/Jahr d) 0,5 PT/Jahr	
Serverraum R 3.10	B 2.4	Z 1 Installation von Wasser ableitenden Blechen mit Überwachung mittels eines Wassermelders und Aufschaltung auf den Pförtner	30.04. 20xy	a) Herr Schmitz b) Herr Hofmann	a) 1000,- Euro b) 2 PT c) 0,- Euro/Jahr d) 1 PT/Jahr	Installation der Bleche lediglich unter frisch- und abwasserführenden Leitungen
Server S4	B 3.101	M 1.28 Lokale unterbrechungsfreie Stromversorgung	31.10. 20xy	a) Herr Schulz b) Frau Meier	a) 500,- Euro b) 1 PT c) 0,- Euro/Jahr d) 0,5 PT/Jahr	
Gruppe Clients C1	B 3.207	Z 2 chipkartengestützte Authentisierung und lokale Verschlüsselung der Festplatten	31.12. 20xy	a) Herr Schulz b) Frau Meier	a) 1400,- Euro b) 2 PT c) 0,- Euro/Jahr d) 2 PT/Jahr	
...						

Legende:

- Verantwortlich:
  a) = Verantwortlich für die Umsetzung der Maßnahme
  b) = Verantwortlich für die Kontrolle der Umsetzung
- Budget-Rahmen: Für die Realisierung der Maßnahme stehen zur Verfügung
  a) = einmalige Investitionskosten
  b) = einmaliger Personalaufwand (PT = Personentage)
  c) = wiederkehrende Investitionskosten
  d) = wiederkehrender Personalaufwand (PT = Personentage)

Anhand dieser Informationen kann die Umsetzung der Maßnahmen überwacht und gesteuert werden.

Aktionspunkte zu 5 Umsetzung der Sicherheitskonzeption

- Fehlende oder nur teilweise umgesetzte IT-Grundschutz-Maßnahmen sowie ergänzende Sicherheitsmaßnahmen in einer Tabelle zusammenfassen
- Sicherheitsmaßnahmen konsolidieren, das heißt, überflüssige Maßnahmen streichen, allgemeine Maßnahmen an die Gegebenheiten anpassen und alle Maßnahmen auf Eignung prüfen
- Einmalige und wiederkehrende Kosten und Aufwand für die umzusetzenden Maßnahmen ermitteln
- Ersatzmaßnahmen für nicht finanzierbare oder nicht leistbare Maßnahmen ermitteln
- Entscheidung herbeiführen, welche Ressourcen für die Umsetzung der Maßnahmen eingesetzt werden sollen
- Gegebenenfalls Restrisiko aufzeigen und Entscheidung der Leitungsebene darüber einholen
- Umsetzungsreihenfolge für die Maßnahmen festlegen, begründen und dokumentieren
- Termine für die Umsetzung festlegen und Verantwortung zuweisen

- Verlauf der Umsetzung und Einhaltung der Termine überwachen
- Betroffene Mitarbeiter schulen und sensibilisieren

6 Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit

Um den Informationssicherheitsprozess aufrecht zu erhalten und kontinuierlich verbessern zu können, müssen nicht nur angemessene Sicherheitsmaßnahmen implementiert und Dokumente fortlaufend aktualisiert werden, sondern auch der IS-Prozess selbst muss regelmäßig auf seine Wirksamkeit und Effizienz hin überprüft werden. Dabei sollte regelmäßig eine Erfolgskontrolle und Bewertung des IS-Prozesses durch die Leitungsebene stattfinden (Managementbewertung). Bei Bedarf (z. B. bei der Häufung von Sicherheitsvorfällen oder gravierenden Änderung der Rahmenbedingungen) muss auch zwischen den Routineterminen getagt werden. Alle Ergebnisse und Beschlüsse müssen nachvollziehbar dokumentiert werden.

6.1 Überprüfung des Informationssicherheitsprozesses in allen Ebenen

Die Überprüfung des Informationssicherheitsprozesses ist unabdingbar, damit einerseits Fehler und Schwachstellen erkannt und abgestellt werden können und andererseits der IS-Prozess in Bezug auf seine Effizienz optimiert werden kann. Ziel dabei ist unter anderem die Verbesserung der Praxistauglichkeit von Strategie, Maßnahmen und organisatorischen Abläufen.

Die wesentlichen Aspekte, die dabei betrachtet werden müssen, werden im Folgenden dargestellt.

6.1.1 Methoden zur Überprüfung des Informationssicherheitsprozesses

Zur Effizienzprüfung und Verbesserung des Informationssicherheitsprozesses sollten Verfahren und Mechanismen eingerichtet werden, die einerseits die Realisierung der beschlossenen Maßnahmen und andererseits ihre Wirksamkeit und Effizienz überprüfen. Die Informationssicherheitsstrategie sollte daher auch Leitaussagen zur Messung der Zielerreichung machen. Grundlagen für solche Messungen können beispielsweise sein:

- Detektion, Dokumentation und Auswertung von Sicherheitsvorfällen
- Durchführung von Übungen und Tests zur Simulation von Sicherheitsvorfällen und Dokumentation der Ergebnisse
- interne und externe Audits, Datenschutzkontrollen
- Zertifizierung nach festgelegten Sicherheitskriterien

Die Erfolgskontrolle der umgesetzten Maßnahmen sollte im Rahmen von internen Audits erfolgen. Dabei ist es wichtig, dass solche Audits nicht von denjenigen durchgeführt werden, die die Sicherheitskonzeption entwickelt haben. Hierfür kann es sinnvoll sein, externe Experten mit der Durchführung solcher Prüfungsaktivitäten zu beauftragen.

Da der Aufwand bei Audits von der Komplexität und Größe des Informationsverbunds abhängt, sind die Anforderungen auch für kleine Institutionen sehr gut umzusetzen. Ein jährlicher technischer Check von IT-Systemen, eine Durchsicht vorhandener Dokumentationen, um die Aktualität zu prüfen, und ein Workshop, bei dem Probleme und Erfahrungen mit dem Sicherheitskonzept besprochen werden, kann unter Umständen in kleinen Institutionen schon ausreichend sein.

6.1.2 Überprüfung der Umsetzung der Sicherheitsmaßnahmen

Anhand der Aufgabenliste und der zeitlichen Planung, die im Realisierungsplan enthalten sein müssen, kann überprüft werden, ob und inwieweit dieser eingehalten wurde. Wichtige Voraussetzung für die Einhaltung der geplanten Sicherheitsmaßnahmen ist die angemessene Ressourcenplanung. Daher ist es sinnvoll, bei der Überprüfung darauf zu achten, ob ausreichende finanzielle und personelle Ressourcen zur Verfügung gestellt wurden. Die Überprüfung des Informationssicherheitsprozesses dient nicht nur zur Kontrolle der Aktivitäten im Rahmen des Sicherheitskonzeptes, sondern auch zur rechtzeitigen

Wahrnehmung von Planungsfehlern und zur Anpassung der Sicherheitsstrategie, wenn sich diese als unrealistisch erweist.

Nach der Realisierung und Einführung von neuen Sicherheitsmaßnahmen sollte durch den IT-Sicherheitsbeauftragten insbesondere geprüft werden, ob die notwendige Akzeptanz seitens der Mitarbeiter vorhanden ist. Stellt sich heraus, dass die neuen Maßnahmen nicht akzeptiert werden, ist ein Misserfolg vorprogrammiert. Die Ursachen sind herauszuarbeiten und abzustellen. Hierzu reicht meist schon eine zusätzliche Aufklärung der Betroffenen.

Sicherheitsrevision

Die im IT-Grundschutz enthaltenen Sicherheitsmaßnahmen können auch für die Revision der Informationssicherheit genutzt werden. Hierzu wird die gleiche Vorgehensweise wie beim Basis-Sicherheitscheck empfohlen. Hilfreich und arbeitsökonomisch ist es, für jeden Baustein der IT-Grundschutz-Kataloge anhand der Maßnahmentexte eine speziell auf die eigene Institution angepasste Checkliste zu erstellen. Dies erleichtert die Revision und verbessert die Reproduzierbarkeit der Ergebnisse.

Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz

Eine Zertifizierung ist eine weitere Methode, um die Erreichung der Sicherheitsziele und die Umsetzung der Sicherheitsmaßnahmen zu überprüfen. Hierbei begutachten qualifizierte unabhängige Stellen das Management und die Umsetzung von Informationssicherheit. Durch eine Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz erhält eine Institution nachvollziehbare, wiederholbare und vergleichbare Auditergebnisse. Hierüber kann außerdem dokumentiert werden, dass die Institution sowohl ISO 27001 als auch IT-Grundschutz in der erforderlichen Tiefe umgesetzt hat.

6.1.3 Eignung der Informationssicherheitsstrategie

Um den Informationssicherheitsprozess erfolgreich steuern und lenken zu können, muss die Leitungsebene einen Überblick darüber haben, inwieweit die Sicherheitsziele mit Hilfe der eingesetzten Sicherheitsstrategie tatsächlich erreicht werden konnten.

Aktualität von Sicherheitszielen, Rahmenbedingungen und Sicherheitskonzeption

In einer längeren Perspektive ist es auch notwendig, die gesetzten Sicherheitsziele und Rahmenbedingungen zu überprüfen. Gerade in schnelllebigen Branchen ist eine entsprechende Anpassung der Sicherheitsleitlinie und der Sicherheitsstrategie von elementarer Bedeutung.

Auch betriebliche Änderungen (z. B. Einsatz neuer IT-Systeme, Umzug), organisatorische Änderungen (z. B. Outsourcing) und Änderungen gesetzlicher Anforderungen müssen schon bei ihrer Planungsphase mit in die Sicherheitskonzeption einbezogen werden. Die Sicherheitskonzeption und die dazugehörigen Dokumentation muss nach jeder relevanten Änderung aktualisiert werden. Dies muss auch im Änderungsprozess der Institution berücksichtigt werden. Dafür muss der Informationssicherheitsprozess in das Änderungsmanagement der Institution integriert werden.

Wirtschaftlichkeitsbetrachtung

Ein anderer Punkt, der unter konstanter Beobachtung bleiben sollte, ist die Wirtschaftlichkeit der Sicherheitsstrategie und von spezifischen Sicherheitsmaßnahmen. Die Kosten für die Informationssicherheit sind zwar sehr schwer zu ermitteln, es ist aber oft hilfreich, für die weitere Planung zu überprüfen, ob die tatsächlich angefallenen Kosten den ursprünglich geplanten Kosten entsprechen oder ob alternativ andere, ressourcenschonendere Sicherheitsmaßnahmen eingesetzt werden können. Ebenso ist es wichtig, regelmäßig den Nutzen der vorhandenen Sicherheitsmaßnahmen herauszuarbeiten.

Rückmeldungen von Internen und Externen

Rückmeldungen über Fehler und Schwachstellen in den Prozessen kommen im Allgemeinen nicht nur von der Informationssicherheitsorganisation oder der Revision, sondern auch von Mitarbeitern, Geschäftspartnern, Kunden oder Partnern. Die Institution muss daher eine wirksame Vorgehensweise festlegen, um mit Beschwerden und anderen Rückmeldungen von Internen und Externen umzugehen.

Beschwerden von Kunden oder Mitarbeitern können dabei auch ein Indikator für Unzufriedenheit sein. Es sollte möglichst bereits entstehender Unzufriedenheit entgegengewirkt werden, da bei zufriedenen Mitarbeitern die Gefahr von fahrlässigen oder vorsätzlichen Handlungen, die den Betrieb stören können, geringer ist.

Es muss daher ein klar definiertes Verfahren und eindeutig festgelegte Kompetenzen für den Umgang mit Beschwerden und für die Rückmeldung von Problemen an die zuständige Instanz geben. So sollte auf Beschwerden schnellstmöglich geantwortet werden, damit die Hinweisgeber sich auch ernst genommen fühlen. Die gemeldeten Probleme müssen bewertet und der Handlungsbedarf eingeschätzt werden. Die Institution muss daraufhin angemessene Korrekturmaßnahmen zur Beseitigung der Ursachen von Fehlern ergreifen, um deren erneutes Auftreten zu verhindern.

6.1.4 Übernahme der Ergebnisse in den Informationssicherheitsprozess

Die Ergebnisse der Erfolgskontrolle sind für die Verbesserung des IS-Prozesses notwendig. Es kann sich dabei herausstellen, dass die Sicherheitsziele, die Sicherheitsstrategie oder das Sicherheitskonzept geändert und die Informationssicherheitsorganisation den Erfordernissen angepasst werden sollten. Unter Umständen ist es sinnvoll, grundlegende Änderungen an der IT-Umgebung vorzunehmen oder Geschäftsprozesse zu verändern, z. B. wenn Sicherheitsziele unter den bisherigen Rahmenbedingungen nicht oder nur umständlich (also mit hohem finanziellen oder personellen Aufwand) erreicht werden können. Wenn größere Veränderungen vorgenommen und umfangreiche Verbesserungen umgesetzt werden, schließt sich der Management-Kreislauf wieder und es wird erneut mit der Planungsphase begonnen.

Die Überprüfungen zu den einzelnen Themen müssen von geeigneten Personen durchgeführt werden, die die notwendige Kompetenz und Unabhängigkeit gewährleisten können. Vollständigkeits- und Plausibilitätskontrollen sollten nicht durch die Ersteller der Konzepte durchgeführt werden.

Die grundsätzliche Vorgehensweise der Institution zur Überprüfung und Verbesserung des Informationssicherheitsprozesses sollte in einer entsprechenden Richtlinie dokumentiert und von der Leitungsebene verabschiedet werden. In der **Richtlinie zur Überprüfung und Verbesserung des Informationssicherheitsprozesses** sollte insbesondere geregelt werden, wie interne Audits im Bereich der Informationssicherheit durchzuführen sind und wie die Ergebnisse in den Änderungsprozess einfließen. Prüfergebnisse und -berichte sind im Allgemeinen als hochvertraulich zu betrachten und müssen daher besonders gut geschützt werden.

Aktionspunkte zu 6.1 Überprüfung des Informationssicherheitsprozesses in allen Ebenen

- Grundsätzliche Vorgehensweise der Institution zur Überprüfung und Verbesserung des Informationssicherheitsprozesses in einer entsprechenden Richtlinie dokumentieren und der Leitungsebene zur Verabschiedung vorlegen
- Messung der Zielerreichung in die Sicherheitsstrategie integrieren
- Einhaltung des Realisierungsplans prüfen
- Realisierung der beschlossenen Maßnahmen überprüfen
- Wirksamkeit und Effizienz der beschlossenen Maßnahmen überprüfen
- Prüfen, ob die Sicherheitsmaßnahmen akzeptiert werden und gegebenenfalls nachbessern
- Rollenkonflikt zwischen Ersteller und Prüfer beachten
- Vertraulichkeit der Untersuchungsergebnisse sicherstellen
- Eignung und Aktualität von Sicherheitszielen, -strategien und -konzeption prüfen
- Angemessenheit der bereitgestellten Ressourcen und die Wirtschaftlichkeit der Sicherheitsstrategie und -maßnahmen überprüfen
- Ergebnisse der Überprüfungen in Form von Verbesserungen in den Informationssicherheitspro-

zess einfließen lassen

6.2 Informationsfluss im Informationssicherheitsprozess

Im Rahmen der Überprüfung und Verbesserung des Informationssicherheitsprozesses entstehen in der Regel verschiedene Berichte, Audit-Reports, Ergebnisse von Sicherheitstests, Meldungen über sicherheitsrelevante Ereignisse und weitere Dokumente zur Informationssicherheit der Institution. Die Dokumente müssen aussagekräftig und für die jeweilige Zielgruppe verständlich sein. Da nicht alle diese Informationen für die Leitungsebene geeignet sind, ist es eine Aufgabe des IT-Sicherheitsbeauftragten und des IS-Management-Teams, diese Informationen zu sammeln, zu verarbeiten und entsprechend kurz und übersichtlich aufzubereiten.

6.2.1 Berichte an die Leitungsebene

Damit die Unternehmens- bzw. Behördenleitung die richtigen Entscheidungen bei der Steuerung und Lenkung des Informationssicherheitsprozesses treffen kann, benötigt sie Eckpunkte über den Stand der Informationssicherheit. Diese Eckpunkte sollten in Management-Berichten aufbereitet werden, die unter anderem folgende Punkte abdecken:

- Ergebnisse von Audits und Datenschutzkontrollen
- Berichte über Sicherheitsvorfälle
- Berichte über bisherige Erfolge und Probleme beim Informationssicherheitsprozess

Die Leitungsebene muss von der IS-Organisation regelmäßig in angemessener Form über die Ergebnisse der Überprüfungen und den Status des IS-Prozesses informiert werden. Dabei sollten Probleme, Erfolge und Verbesserungsmöglichkeiten aufgezeigt werden. Die Leitungsebene nimmt die Management-Berichte zur Kenntnis und veranlasst eventuell notwendige Maßnahmen.

6.2.2 Dokumentation im Informationssicherheitsprozess

Aus zahlreichen Gründen ist die Dokumentation des IS-Prozesses auf allen Ebenen entscheidend für dessen Erfolg. Nur durch ausreichende Dokumentation

- werden getroffene Entscheidungen nachvollziehbar,
- sind Prozesse wiederholbar und standardisierbar,
- können Schwächen und Fehler erkannt und zukünftig vermieden werden.

Abhängig vom Gegenstand und vom Verwendungszweck einer Dokumentation können folgende Arten von Dokumentationen unterschieden werden:

- Technische Dokumentation und Dokumentation von Arbeitsabläufen (Zielgruppe: Experten)

  Hier wird der aktuelle Stand von Geschäftsprozessen und der damit verbundenen IT-Systeme und Anwendungen beschrieben. Oft ist der Detaillierungsgrad technischer Dokumentationen ein Streitthema. Ein pragmatischer Ansatz ist, dass andere Personen mit vergleichbarer Expertise in diesem Bereich die Dokumentation nachvollziehen können müssen und dass der Administrator zwar auf sein Wissen, aber nicht auf sein Gedächtnis angewiesen sein muss, um die Systeme und Anwendungen wiederherzustellen. Bei Sicherheitsübungen und bei der Behandlung von Sicherheitsvorfällen sollte die Qualität der vorhandenen Dokumentationen bewertet und die gewonnenen Erkenntnisse zur Verbesserung genutzt werden. Zu solcher Art von Dokumentationen gehören unter anderem:

  - Installations- und Konfigurationsanleitungen
  - Anleitungen für den Wiederanlauf nach einem Sicherheitsvorfall
  - Dokumentation von Test- und Freigabeverfahren

    - Anweisungen für das Verhalten bei Störungen und Sicherheitsvorfällen

- Anleitungen für Mitarbeiter (Zielgruppe: Mitarbeiter)

  Sicherheitsmaßnahmen müssen für die Mitarbeiter verständlich in Form von Richtlinien dokumentiert werden. Darüber hinaus müssen die Mitarbeiter über die Existenz und Bedeutung dieser Richtlinien informiert und entsprechend geschult sein. Diese Gruppe von Dokumentationen umfasst beispielsweise:

  - Arbeitsabläufe und organisatorische Vorgaben
  - Richtlinien zur Nutzung des Internets
  - Verhalten bei Sicherheitsvorfällen

- Aufzeichnung von Management-Entscheidungen (Zielgruppe: Leitungsebene)

  Grundlegende Entscheidungen zum Informationssicherheitsprozess und zur Sicherheitsstrategie müssen aufgezeichnet werden, damit diese jederzeit nachvollziehbar und wiederholbar sind.

- Gesetze und Regelungen (Zielgruppe: Leitungsebene)

  Für die Informationsverarbeitung können eine Vielzahl unterschiedlicher Gesetze, Regelungen und Anweisungen relevant sein. Es sollte dokumentiert werden, welche Gesetze, Regelungen und Anweisungen im vorliegenden Fall besondere Anforderungen an Geschäftsprozesse, den IT-Betrieb oder an die Informationssicherheit stellen und welche konkreten Konsequenzen sich daraus ergeben.

Es muss sichergestellt werden, dass alle Dokumentationen auf dem aktuellen Stand gehalten werden. Dafür muss die Dokumentation in den Änderungsprozess einbezogen werden.

6.2.3 Informationsfluss und Meldewege

Für die Aufrechterhaltung des Informationssicherheitsprozesses ist die zeitnahe Aktualisierung der Meldewege und der Festlegungen für den Informationsfluss von elementarer Bedeutung. Darüber hinaus bieten die Ergebnisse aus durchgeführten Übungen, Tests und Audits auch eine nützliche Grundlage für die Verbesserung des Informationsflusses.

Grundsätzliche Festlegungen zum Informationsfluss und zu den Meldewegen in Bezug auf den Informationssicherheitsprozess sollten in einer entsprechenden Richtlinie dokumentiert und von der Leitungsebene verabschiedet werden. In der **Richtlinie zum Informationsfluss und zu den Meldewegen** sollten insbesondere die für den Informationssicherheitsprozess kritischen Informationsflüsse geregelt werden. Dabei ist zwischen Hol- und Bringschuld zu unterscheiden.

Nutzung von Synergieeffekten für den Informationsfluss

Viele Institutionen haben bereits Prozesse für die Bereitstellung von Dienstleistungen oder den IT-Support definiert. Häufig gelingt es, Synergieeffekte zu nutzen und Aspekte der Informationssicherheit in bereits bestehende Prozesse einzugliedern. Beispielsweise könnten Meldewege für IT-Sicherheitsvorfälle in den IT-Support integriert werden oder die Kapazitätsplanung um Aspekte der Notfallvorsorge erweitert werden.

Viele Informationen, die aus Sicherheitsgründen erhoben werden, können auch zu anderen Zwecken genutzt werden. Ebenso haben Sicherheitsmaßnahmen auch andere positive Nebeneffekte, besonders die Optimierung von Prozessen zahlt sich aus. Beispielsweise ist die Bestimmung von Informationseigentümern oder die Einstufung von Informationen nach einheitlichen Bewertungskriterien für viele Bereiche einer Institution relevant. Ein Überblick über die Abhängigkeit von Geschäftsprozessen von IT-Systemen und Anwendungen ist ebenfalls nicht nur für das Sicherheitsmanagement sinnvoll. Zum Beispiel kann dadurch häufig auch eine exakte Zuordnung von IT-Kosten, die oftmals als Gemeinkosten umgelegt werden, auf einzelne Geschäftsprozesse oder Produkte erfolgen.

Aktionspunkte zu 6.2 Informationsfluss im Informationssicherheitsprozess

- Grundsätzliche Festlegungen zum Informationsfluss und zu den Meldewegen in Bezug auf den Informationssicherheitsprozess in einer entsprechenden Richtlinie dokumentieren und der Leitungsebene zur Verabschiedung vorlegen
- Leitungsebene über die Ergebnisse von Überprüfungen und den Status des Informationssicherheitsprozesses informieren
- Gegebenenfalls Entscheidungen über erforderliche Korrekturmaßnahmen einholen
- Alle Teilaspekte des gesamten Informationssicherheitsprozesses nachvollziehbar dokumentieren und die Dokumentation auf dem aktuellen Stand halten
- Bei Bedarf die Qualität der Dokumentation bewerten und gegebenenfalls nachbessern oder aktualisieren
- Meldewege, die den Informationssicherheitsprozess betreffen, auf dem aktuellen Stand halten
- Synergien zwischen dem Informationssicherheitsprozess und anderen Managementprozessen ausfindig machen

7 Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz

Um die erfolgreiche Umsetzung von IT-Grundschutz nach außen transparent machen zu können, hat das BSI ein Zertifizierungsschema für Informationssicherheit entwickelt. Dieses Schema berücksichtigt die Anforderungen an Managementsysteme für die Informationssicherheit aus ISO/IEC 27001. Das ISO 27001-Zertifikat auf der Basis von IT-Grundschutz oder auch ein Auditor-Testat bietet Unternehmen und Behörden die Möglichkeit, ihre Bemühungen um Informationssicherheit transparent zu machen. Dies kann sowohl gegenüber Kunden als auch gegenüber Geschäftspartnern als Qualitätsmerkmal dienen und somit zu einem Wettbewerbsvorteil führen.

Dabei sind die Interessen an einer ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz vielfältig:

- Dienstleister möchten mit Hilfe dieses Zertifikats einen vertrauenswürdigen Nachweis führen, dass sie die Maßnahmen gemäß IT-Grundschutz realisiert haben.
- Kooperierende Unternehmen möchten sich darüber informieren, welchen Grad von Informationssicherheit ihre Geschäftspartner zusichern können.
- Von Institutionen, die neu an ein Netz angeschlossen werden, wird der Nachweis darüber verlangt, dass sie eine ausreichende Informationssicherheit besitzen, damit durch den Anschluss ans Netz keine untragbaren Risiken entstehen.
- Institutionen möchten dem Kunden bzw. Bürger gegenüber ihre Bemühungen um eine ausreichende Informationssicherheit deutlich machen.

Da der IT-Grundschutz mit der in diesem Dokument beschriebenen Vorgehensweise zum Sicherheitsmanagement und den in den IT-Grundschutz-Katalogen enthaltenen Empfehlungen von Standard-Sicherheitsmaßnahmen inzwischen einen Quasi-Standard für Informationssicherheit darstellt, bietet es sich an, dies als allgemein anerkanntes Kriterienwerk für Informationssicherheit zu verwenden.

Grundlage für die Vergabe eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz ist die Durchführung eines Audits durch einen externen, beim BSI zertifizierten Auditor. Das Ergebnis des Audits ist ein Auditbericht, der der Zertifizierungsstelle vorgelegt wird, die über die Vergabe des ISO 27001-Zertifikats auf der Basis von IT-Grundschutz entscheidet. Kriterienwerke des Verfahrens sind neben der Norm ISO 27001 die in diesem Dokument beschriebene IT-Grundschutz-Vorgehensweise und die IT-Grundschutz-Kataloge des BSI.

Über ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz wird zunächst nachgewiesen, dass IT-Grundschutz im betrachteten Informationsverbund erfolgreich umgesetzt worden ist. Darüber hinaus zeigt ein solches Zertifikat auch, dass in der jeweiligen Institution

- Informationssicherheit ein anerkannter Wert ist,
- ein funktionierendes IS-Management vorhanden ist und außerdem
- zu einem bestimmten Zeitpunkt ein definiertes Sicherheitsniveau erreicht wurde.

Weitere Informationen zur Zertifizierung nach ISO 27001 und zur Zertifizierung als ISO 27001-Auditor auf der Basis von IT-Grundschutz finden sich auf dem Web-Angebot des BSI (siehe [ZERT]).

Aktionspunkte zu 7 Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz
• Informationen des BSI zum Qualifizierungsschema und zum Schema für die ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz lesen • Prüfen, ob die Bemühungen um Informationssicherheit anhand eines Auditor-Testats oder anhand eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz transparent gemacht werden sollen • Gegebenenfalls prüfen, ob das Informationssicherheitsmanagement und der Sicherheitszustand

die entsprechenden Voraussetzungen erfüllen

- Gegebenenfalls den Qualifizierungs- beziehungsweise Zertifizierungsprozess initiieren

Anhang

Erläuterungen zu den Schadensszenarien

Im Folgenden sind für die in Kapitel 4.3.1 definierten Schadensszenarien beispielhafte Fragestellungen aufgeführt. Diese Fragen sollen als Hilfsmittel für die Schutzbedarfsfeststellung dienen, vor allem im Bereich der Anwendungen. Anhand der individuellen Anforderungen sollten die Fragen angepasst und ergänzt werden.

Schadensszenario "Verstoß gegen Gesetze/Vorschriften/Verträge"

Sowohl aus dem Verlust der Vertraulichkeit als auch der Integrität und ebenso der Verfügbarkeit können derlei Verstöße resultieren. Die Schwere des Schadens ist dabei oftmals abhängig davon, welche rechtlichen Konsequenzen daraus für die Institution entstehen können.

Beispiele für relevante Gesetze sind (in Deutschland):

Grundgesetz, Bürgerliches Gesetzbuch, Strafgesetzbuch, Bundesdatenschutzgesetz und Datenschutzgesetze der Länder, Sozialgesetzbuch, Handelsgesetzbuch, Personalvertretungsgesetz, Betriebsverfassungsgesetz, Urheberrechtsgesetz, Patentgesetz, Informations- und Kommunikationsdienstegesetz (IuKDG), Gesetz zur Kontrolle und Transparenz im Unternehmen (KonTraG).

Beispiele für relevante Vorschriften sind:

Verwaltungsvorschriften, Verordnungen und Dienstvorschriften.

Beispiele für Verträge:

Dienstleistungsverträge im Bereich Datenverarbeitung, Verträge zur Wahrung von Betriebsgeheimnissen.

Fragen:

Verlust der Vertraulichkeit

- Erfordern gesetzliche Auflagen die Vertraulichkeit der Daten?
- Ist im Falle einer Veröffentlichung von Informationen mit Strafverfolgung oder Regressforderungen zu rechnen?
- Sind Verträge einzuhalten, die die Wahrung der Vertraulichkeit bestimmter Informationen beinhalten?

Verlust der Integrität

- Erfordern gesetzliche Auflagen die Integrität der Daten?
- In welchem Maße wird durch einen Verlust der Integrität gegen Gesetze bzw. Vorschriften verstoßen?

Verlust der Verfügbarkeit

- Sind bei Ausfall der Anwendung Verstöße gegen Vorschriften oder sogar Gesetze die Folge?
- Schreiben Gesetze die dauernde Verfügbarkeit bestimmter Informationen vor?
- Gibt es Termine, die bei Einsatz der Anwendung zwingend einzuhalten sind?
- Gibt es vertragliche Bindungen für bestimmte einzuhaltende Termine?

Schadensszenario "Beeinträchtigung des informationellen Selbstbestimmungsrechts"

Bei der Implementation und dem Betrieb von IT-Systemen und Anwendungen besteht die Gefahr einer Verletzung des informationellen Selbstbestimmungsrechts bis hin zu einem Missbrauch personenbezogener Daten.

Beispiele für die Beeinträchtigung des informationellen Selbstbestimmungsrechts sind:

- Unzulässige Erhebung personenbezogener Daten ohne Rechtsgrundlage oder Einwilligung,
- unbefugte Kenntnisnahme bei der Datenverarbeitung bzw. der Übermittlung von personenbezogenen Daten,
- unbefugte Weitergabe personenbezogener Daten,
- Nutzung von personenbezogenen Daten zu einem anderen als dem bei der Erhebung zulässigen Zweck und
- Verfälschung von personenbezogenen Daten in IT-Systemen oder bei der Übertragung.

Die folgenden Fragen können zur Abschätzung möglicher Folgen und Schäden herangezogen werden:

Fragen:

Verlust der Vertraulichkeit

- Welche Schäden können für den Betroffenen entstehen, wenn seine personenbezogenen Daten nicht vertraulich behandelt werden?
- Werden personenbezogene Daten für unzulässige Zwecke verarbeitet?
- Ist es im Zuge einer zulässigen Verarbeitung personenbezogener Daten möglich, aus diesen Daten z. B. auf den Gesundheitszustand oder die wirtschaftliche Situation einer Person zu schließen?
- Welche Schäden können durch den Missbrauch der gespeicherten personenbezogenen Daten entstehen?

Verlust der Integrität

- Welche Schäden würden für den Betroffenen entstehen, wenn seine personenbezogenen Daten unabsichtlich verfälscht oder absichtlich manipuliert würden?
- Wann würde der Verlust der Integrität personenbezogener Daten frühestens auffallen?

Verlust der Verfügbarkeit

- Können bei Ausfall der Anwendung oder bei einer Störung einer Datenübertragung personenbezogene Daten verloren gehen oder verfälscht werden, so dass der Betroffene in seiner gesellschaftlichen Stellung beeinträchtigt wird oder gar persönliche oder wirtschaftliche Nachteile zu befürchten hat?

Schadensszenario "Beeinträchtigung der persönlichen Unversehrtheit"

Die Fehlfunktion von IT-Systemen oder Anwendungen kann unmittelbar die Verletzung, die Invalidität oder den Tod von Personen nach sich ziehen. Die Höhe des Schadens ist am direkten persönlichen Schaden zu messen.

Beispiele für solche Anwendungen und IT-Systeme sind:

- medizinische Überwachungsrechner,
- medizinische Diagnosesysteme,
- Flugkontrollrechner und
- Verkehrsleitsysteme.

Fragen:

Verlust der Vertraulichkeit

- Kann durch das Bekanntwerden von Daten eine Person physisch oder psychisch geschädigt werden?

Verlust der Integrität

- Können Menschen durch manipulierte Programmabläufe oder Daten gesundheitlich gefährdet werden?

Verlust der Verfügbarkeit

- Bedroht der Ausfall der Anwendung oder des IT-Systems unmittelbar die persönliche Unversehrtheit von Personen?

Schadensszenario "Beeinträchtigung der Aufgabenerfüllung"

Gerade der Verlust der Verfügbarkeit einer Anwendung oder der Integrität der Daten kann die Aufgabenerfüllung in einer Institution erheblich beeinträchtigen. Die Schwere des Schadens richtet sich hierbei nach der zeitlichen Dauer der Beeinträchtigung und nach dem Umfang der Einschränkungen der angebotenen Dienstleistungen.

Beispiele hierfür sind:

- Fristversäumnisse durch verzögerte Bearbeitung von Verwaltungsvorgängen,
- verspätete Lieferung aufgrund verzögerter Bearbeitung von Bestellungen,
- fehlerhafte Produktion aufgrund falscher Steuerungsdaten und
- unzureichende Qualitätssicherung durch Ausfall eines Testsystems.

Fragen:

Verlust der Vertraulichkeit

- Gibt es Daten, deren Vertraulichkeit die Grundlage für die Aufgabenerfüllung ist (z. B. Strafverfolgungsinformationen, Ermittlungsergebnisse)?

Verlust der Integrität

- Können Datenveränderungen die Aufgabenerfüllung in der Art einschränken, dass die Institution handlungsunfähig wird?
- Entstehen erhebliche Schäden, wenn die Aufgaben trotz verfälschter Daten wahrgenommen werden? Wann werden unerlaubte Datenveränderungen frühestens erkannt?
- Können verfälschte Daten in der betrachteten Anwendung zu Fehlern in anderen Anwendungen führen?
- Welche Folgen entstehen, wenn Daten fälschlicherweise einer Person zugeordnet werden, die in Wirklichkeit diese Daten nicht erzeugt hat?

Verlust der Verfügbarkeit

- Kann durch den Ausfall der Anwendung die Aufgabenerfüllung der Institution so stark beeinträchtigt werden, dass die Wartezeiten für die Betroffenen nicht mehr tolerabel sind?
- Sind von dem Ausfall dieser Anwendung andere Anwendungen betroffen?
- Ist es für die Institution bedeutsam, dass der Zugriff auf Anwendungen nebst Programmen und Daten ständig gewährleistet ist?

Schadensszenario "Negative Innen- oder Außenwirkung"

Durch den Verlust einer der Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit in einer Anwendung können verschiedenartige negative Innen- oder Außenwirkungen entstehen, zum Beispiel:

- Ansehensverlust einer Institution,
- Vertrauensverlust gegenüber einer Institution,
- Demoralisierung der Mitarbeiter,
- Beeinträchtigung der wirtschaftlichen Beziehungen zusammenarbeitender Institutionen,
- verlorenes Vertrauen in die Arbeitsqualität einer Institution und
- Einbuße der Konkurrenzfähigkeit.

Die Höhe des Schadens orientiert sich an der Schwere des Vertrauensverlustes oder des Verbreitungsgrades der Innen- oder Außenwirkung.

Die Ursachen für solche Schäden können vielfältiger Natur sein:

- Handlungsunfähigkeit einer Institution durch IT-Ausfall,
- fehlerhafte Veröffentlichungen durch manipulierte Daten,
- Fehlbestellungen durch mangelhafte Lagerhaltungsprogramme,
- Nichteinhaltung von Verschwiegenheitserklärungen,
- Schuldzuweisungen an die falschen Personen,
- Verhinderung der Aufgabenerfüllung einer Abteilung durch Fehler in anderen Bereichen,
- Weitergabe von Fahndungsdaten an interessierte Dritte und
- Zuspielen vertraulicher Informationen an die Presse.

Fragen:

Verlust der Vertraulichkeit

- Welche Konsequenzen ergeben sich für die Institution durch die unerlaubte Veröffentlichung der für die Anwendung gespeicherten schutzbedürftigen Daten?
- Kann der Vertraulichkeitsverlust der gespeicherten Daten zu einer Schwächung der Wettbewerbsposition führen?
- Entstehen bei Veröffentlichung von vertraulichen gespeicherten Daten Zweifel an der amtlichen Verschwiegenheit?
- Können Veröffentlichungen von Daten zur politischen oder gesellschaftlichen Verunsicherung führen?
- Können Mitarbeiter durch die unzulässige Veröffentlichungen von Daten das Vertrauen in ihre Institution verlieren?

Verlust der Integrität

- Welche Schäden können sich durch die Verarbeitung, Verbreitung oder Übermittlung falscher oder unvollständiger Daten ergeben?
- Wird die Verfälschung von Daten öffentlich bekannt?
- Entstehen bei einer Veröffentlichung von verfälschten Daten Ansehensverluste?
- Können Veröffentlichungen von verfälschten Daten zur politischen oder gesellschaftlichen Verunsicherung führen?

- Können verfälschte Daten zu einer verminderten Produktqualität und damit zu einem Ansehensverlust führen?

Verlust der Verfügbarkeit

- Schränkt der Ausfall der Anwendung die Informationsdienstleistungen für Externe ein?
- Verhindert der Ausfall von Anwendungen die Erreichung von Geschäftszielen?
- Ab wann wird der Ausfall der Anwendung extern bemerkt?

Schadensszenario "Finanzielle Auswirkungen"

Unmittelbare oder mittelbare finanzielle Schäden können durch den Verlust der Vertraulichkeit schutzbedürftiger Daten, die Veränderung von Daten oder den Ausfall von Anwendungen entstehen. Beispiele dafür sind:

- unerlaubte Weitergabe von Forschungs- und Entwicklungsergebnissen,
- Manipulation von finanzwirksamen Daten in einem Abrechnungssystem,
- Ausfall eines IT-gesteuerten Produktionssystems und dadurch bedingte Umsatzverluste,
- unerlaubte Einsichtnahme in Marketingstrategiepapiere oder Umsatzzahlen,
- Ausfall eines Buchungssystems einer Reisegesellschaft,
- Ausfall eines E-Commerce-Servers,
- Zusammenbruch des Zahlungsverkehrs einer Bank,
- Diebstahl oder Zerstörung von Hardware.

Die Höhe des Gesamtschadens setzt sich zusammen aus den direkt und indirekt entstehenden Kosten, etwa durch Sachschäden, Schadenersatzleistungen und Kosten für zusätzlichen Aufwand (z. B. Wiederherstellung).

Fragen:

Verlust der Vertraulichkeit

- Kann die Veröffentlichung vertraulicher Informationen Regressforderungen nach sich ziehen?
- Gibt es in der Anwendung Daten, aus deren Kenntnis ein Dritter (z. B. Konkurrenzunternehmen) finanzielle Vorteile ziehen kann?
- Werden mit der Anwendung Forschungsdaten gespeichert, die einen erheblichen Wert darstellen? Was passiert, wenn sie unerlaubt kopiert und weitergegeben werden?
- Können durch vorzeitige Veröffentlichung von schutzbedürftigen Daten finanzielle Schäden entstehen?

Verlust der Integrität

- Können durch Datenmanipulationen finanzwirksame Daten so verändert werden, dass finanzielle Schäden entstehen?
- Kann die Veröffentlichung falscher Informationen Regressforderungen nach sich ziehen?
- Können durch verfälschte Bestelldaten finanzielle Schäden entstehen (z. B. bei Just-in-Time Produktion)?
- Können verfälschte Daten zu falschen Geschäftsentscheidungen führen?

Verlust der Verfügbarkeit

- Wird durch den Ausfall der Anwendung die Produktion, die Lagerhaltung oder der Vertrieb beeinträchtigt?
- Ergeben sich durch den Ausfall der Anwendung finanzielle Verluste aufgrund von verzögerten Zahlungen bzw. Zinsverlusten?
- Wie hoch sind die Reparatur- oder Wiederherstellungskosten bei Ausfall, Defekt, Zerstörung oder Diebstahl des IT-Systems?
- Kann es durch Ausfall der Anwendung zu mangelnder Zahlungsfähigkeit oder zu Konventionalstrafen kommen?
- Wie viele wichtige Kunden wären durch den Ausfall der Anwendung betroffen?