Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Standard 100-2
IT-Grundschutz-Vorgehensweise

Version 1.0

Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189, 53175 Bonn ▪ Postfach 200363, 53133 Bonn
Tel.: +49 (0) 1888 9582-0 ▪ Fax: +49 (0) 1888 9582-400 ▪ Internet: www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung

1.1 Versionshistorie

Stand	Version	Verfasser
Dezember 2005	1.0	BSI

1.2 Zielsetzung

Das BSI hat mit der Vorgehensweise nach IT-Grundschutz eine Methodik für ein effektives IT-Sicherheitsmanagement 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 des angemessenen IT-Sicherheitsniveaus bei 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 IT-Sicherheitsniveaus und die Implementierung der angemessenen IT-Sicherheit.

Eines der wichtigsten Ziele des IT-Grundschutzes ist es, den Aufwand im IT-Sicherheitsprozess 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 IT-Systeme, die nach Bedarf im eigenen ISMS eingesetzt werden können. Durch die geeignete Anwendung der vom IT-Grundschutz empfohlenen organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen wird ein IT-Sicherheitsniveau für die betrachteten Geschäftsprozesse erreicht, das für den normalen Schutzbedarf angemessen und ausreichend ist und als Basis für hochschutzbedürftige Geschäftsprozesse dienen kann.

1.3 Adressantenkreis

Dieses Dokument richtet sich primär an IT-Sicherheitsverantwortliche, -beauftragte, -experten, -berater und alle Interessierte, die mit dem Management von IT-Sicherheit betraut sind. Es bietet aber auch eine sinnvolle Grundlage für IT-Verantwortliche, Führungskräfte und Projektmanager, die dafür Sorge tragen, dass IT-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 Sicherheit in ihrer Informationstechnik benötigen. Der Begriff „Institutionen“ wird in diesem Zusammenhang für Unternehmen, Behörden und sonstige öffentliche oder private Organisationen verwendet. IT-Grundschutz kann 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 hierbei 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, sogenannte „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 IT-Sicherheitsprozesses 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 IT-Grundschutz kann auch als Sicherheitsanforderung für mögliche Kooperationspartner verwendet werden, um das erforderliche Niveau an IT-Sicherheit 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 IT-Sicherheit betreffende Aufgabenstellungen, beispielsweise Erstellung der IT-Sicherheitskonzeption, Revision und Zertifizierung. 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 IT-Sicherheitskonzeption.

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

Kapitel 4 beschreibt die IT-Grundschutz-Vorgehensweise zur Erstellung einer IT-Sicherheitskonzeption. Dabei wird aufgezeigt, wie zunächst die Grundinformationen über einen IT-Verbund erhoben werden und diese durch Gruppenbildung reduziert werden können. Anschließend muss dann ausgehend von den Geschäftsprozessen der Schutzbedarf für IT-Anwendungen, IT-Systeme, Kommunikationsverbindungen und Räume festgestellt werden. Aus den Empfehlungen der IT-Grundschutz-Kataloge müssen dann die für den jeweileigen IT-Verbund passenden Bausteine und Maßnahmen ausgewählt werden, also die Modellierung nach IT-Grundschutz durchgeführt werden. Vor der Realisierung von IT-Sicherheitsmaßnahmen müssen vorhandene und zusätzliche Sicherheitsmaßnahmen in die IT-Grundschutz-Vorgehensweise integriert werden.

Die wesentliche Aufgabe eines ISMS ist es, die Aufrechterhaltung der IT-Sicherheit zu gewährleisten. Dieses Thema wird im Kapitel 5 angegangen und ergänzend dazu wird die Möglichkeit dargestellt, das erreichte IT-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 IT-Sicherheitsproblemen aufzeigen zu können.

1.5 Literaturverzeichnis

[BSI1] Managementsysteme für Informationssicherheit (ISMS), BSI-Standard 100-1, Version 1.0, Dezember 2005, www.bsi.bund.de

[BSI2] IT-Grundschutz-Vorgehensweise, BSI-Standard 100-2, Version 1.0, Dezember 2005, www.bsi.bund.de

[BSI3] Risikoanalyse auf der Basis von IT-Grundschutz, BSI-Standard 100-3, Version 1.0, Februar 2004, www.bsi.bund.de

[GSHB] IT-Grundschutzhandbuch - 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] Allgemeine Informationen zum IT-Grundschutz-Zertifikat, zum Lizenzierungsschema für Auditoren und zum Zertifizierungsschema für IT-Grundschutz unter www.bsi.bund.de/gshb/zert

[13335] ISO/IEC 13335 "Management of information and communications technology security", ISO/IEC JTC1/SC27

[17799] ISO/IEC 17799:2005 "Information technology - Code of practice for information security management", ISO/IEC JTC1/SC27

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

2 IT-Sicherheitsmanagement mit IT-Grundschutz

Moderne Geschäftsprozesse sind heute in Wirtschaft und Verwaltung ohne IT-Unterstützung längst nicht mehr vorstellbar. Eine zuverlässig funktionierende Informationstechnik ist für die Aufrechterhaltung des Betriebes unerlässlich. Daher stellt eine mangelhaft geschützte Informationstechnik einen häufig unterschätzten Risikofaktor dar, der für manche Institution existenzbedrohend sein kann. Dabei ist eine Grundsicherung der IT schon mit verhältnismäßig geringen Mitteln zu erreichen.

Um zu einem bedarfsgerechten IT-Sicherheitsniveau 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 IT-Sicherheitsmanagement. IT-Sicherheitsmanagement 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.

IT-Sicherheit 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 IT-Anwendungen und IT-Systeme empfehlen. Im Vordergrund stehen dabei praxisnahe und handlungsorientierte Hinweise mit dem Ziel, die Einstiegshürde in den IT-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 bieten eine systematische Methodik zur Erarbeitung von IT-Sicherheitskonzepten und praxiserprobte Standard-Sicherheitsmaßnahmen, die bereits in zahlreichen Behörden und Unternehmen erfolgreich eingesetzt werden.

Die schon seit 1994 veröffentlichten, mittlerweile über 3000 Seiten starke 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 IT-Sicherheitsniveau durchzusetzen und aufrecht zu erhalten. 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 IT-Sicherheit nach innen und außen. Daher muss diese den IT-Sicherheitsprozess initiieren, steuern und kontrollieren. Dazu gehören strategische Leitaussagen zu IT-Sicherheit, konzeptionelle Vorgaben und auch organisatorische Rahmenbedingungen, um IT-Sicherheit innerhalb aller Geschäftsprozesse erreichen zu können.

Die Verantwortung für IT-Sicherheit verbleibt dort, die Aufgabe "IT-Sicherheit" wird allerdings typischerweise an einen IT-Sicherheitsbeauftragten delegiert.

Wenn diese Randbedingungen in einer konkreten Situation nicht gegeben sind, so sollte zunächst versucht werden, die Umsetzung der fehlenden IT-Sicherheitsmaßnahmen auf Arbeitsebene durchzuführen. In jedem Fall sollte aber darauf hingewirkt werden, die Leitungsebene für die Belange der IT-

Sicherheit zu sensibilisieren, so dass sie zukünftig ihrer Verantwortung Rechnung trägt. Der vielfach zu beobachtende sich selbst auf Arbeitsebene initiierende IT-Sicherheitsprozess führt zwar zu einer Verbesserung der Sicherheitssituation, garantiert jedoch kein dauerhaftes Fortentwickeln des IT-Sicherheitsniveaus.

Die Vorgehensweise nach IT-Grundschutz beschreibt einen Weg, wie ein IT-Sicherheitsmanagement in einer Institution aufgebaut und integriert werden kann. Wenn eine Institution ein effektives und in die Geschäftsprozesse integriertes IT-Sicherheitsmanagement 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 IT-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 IT-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 IT-Grundschutz einbeziehen zu können.

Ergänzend zu der Vorgehensweise nach IT-Grundschutz werden in den IT-Grundschutz-Katalogen Implementierungshilfen für den IT-Sicherheitsprozess in Form von Standard-Sicherheitsmaßnahmen zur Verfügung gestellt. Das Ziel dieser IT-Grundschutz-Empfehlungen ist es, durch geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen ein Sicherheitsniveau für IT-Systeme zu erreichen, das für den normalen Schutzbedarf angemessen und ausreichend ist und als Basis für hochschutzbedürftige IT-Systeme und -Anwendungen dienen kann.

In den IT-Grundschutz-Katalogen wird beschrieben, wie auf der Basis von Standard-Sicherheitsmaßnahmen IT-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 fünf Schichten aufgeteilt:

- Schicht 1 umfasst sämtliche übergreifenden IT-Sicherheitsaspekte. 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 TK-Anlage, Laptop und Mobiltelefon.
- Schicht 4 betrachtet die Vernetzungsaspekte der IT-Systeme. Beispiele sind die Bausteine Heterogene Netze, Remote Access sowie Netz- und Systemmanagement.
- Schicht 5 schließlich beschäftigt sich mit den eigentlichen IT-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 Kataloge gegliedert.

2.1 Begriffseinführung

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 daher zunehmend verwendet. 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.

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 im Folgenden meist der kürzere Begriff "IT-Sicherheitsmanagement" verwendet.

2.2 Übersicht über den IT-Sicherheitsprozess

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

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

- Initiierung des IT-Sicherheitsprozesses:
  - Verantwortung der Leitungsebene
  - Konzeption und Planung des IT-Sicherheitsprozesses
  - Auswahl und Etablierung einer geeigneten Organisationsstruktur für das IT-Sicherheitsmanagement
- Erstellung einer IT-Sicherheitskonzeption
- Umsetzung der IT-Sicherheitskonzeption
  - Realisierung der IT-Sicherheitsmaßnahmen
  - Schulung und Sensibilisierung
- Aufrechterhaltung der IT-Sicherheit im laufenden Betrieb

Abbildung: „Initiierung des IT-Sicherheitsprozesses“

Einige dieser Phasen können auch parallel durchgeführt werden, z. B. kann die Konzeption und Planung des IT-Sicherheitsprozesses gleichzeitig zur Etablierung der IT-Sicherheitsorganisation 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.

2.3 Erstellung einer IT-Sicherheitskonzeption

Die Erstellung einer IT-Sicherheitskonzeption ist eine der zentralen Aufgaben des IT-Sicherheitsmanagements. Aufbauend auf den Ergebnissen der vorherigen Phase werden hier die erforderlichen IT-Sicherheitsmaßnahmen identifiziert und im IT-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 des IT-Einsatzes wider, von übergeordneten Themen, wie dem IT-Sicherheitsmanagement, 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.

In Kapitel 3 dieses Dokumentes (sowie Baustein 1.0 der IT-Grundschutz-Kataloge) wird der IT-Sicherheitsprozess im Überblick dargestellt. Kapitel 4 beinhaltet eine detaillierte Erläuterung der vom IT-Grundschutz empfohlenen Schritte zur Erstellung der IT-Sicherheitskonzeption:

- IT-Strukturanalyse
- Schutzbedarfsfeststellung
- Auswahl der Maßnahmen: Modellierung nach IT-Grundschutz
- Basis-Sicherheitscheck
- Ergänzende Sicherheitsanalyse

IT-Sicherheitsverantwortliche können die Vorgehensweise nach IT-Grundschutz und die IT-Grundschutz-Kataloge aus verschiedenen Gründen und Zielsetzungen anwenden. Dementsprechend ist auch die Umsetzungsreihenfolge und Intensität der einzelnen vorgeschlagenen Schritte abhängig vom bereits vorhandenen IT-Sicherheitsumfeld und dem jeweiligen Blickwinkel der Anwender.

2.4 Übernahme von Verantwortung durch die Leitungsebene

Die oberste Leitungsebene jeder Behörde und jedes Unternehmens ist verantwortlich dafür, dass alle Geschäftsbereiche zielgerichtet und ordnungsgemäß funktionieren und damit auch dafür, dass die IT-Sicherheit nach innen und außen gewährleistet ist. Dies kann auch, je nach Organisationsform und Geschäftsbereich, in verschiedenen Gesetzen geregelt sein. Die Leitungsebene muss den IT-Sicherheitsprozess initiieren, steuern und kontrollieren. Die Verantwortung für IT-Sicherheit verbleibt dort, die Aufgabe "IT-Sicherheit" wird allerdings typischerweise an einen IT-Sicherheitsbeauftragten delegiert. Dabei ist eine intensive Beteiligung der Führungsebene im "Managementprozess IT-Sicherheit" erforderlich. Nur so kann das IT-Sicherheitsmanagement sicherstellen, dass keine untragbaren Risiken bestehen und Ressourcen an der richtige Stelle investiert werden. Die oberste Leitungsebene ist 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 IT-Sicherheitsrisiken die Verantwortung trägt, wird leider oft noch nicht in den Führungskreisen rechtzeitig erkannt. Dementsprechend sind die Zuständigkeiten und Verantwortlichkeiten bezüglich IT-Sicherheitsthemen häufig nicht geklärt. Rechtzeitige Information über mögliche IT-Risiken kann von der Geschäftsführung oder Behördenleitung nach einem IT-Sicherheitsvorfall als Bringschuld der IT-Verantwortlichen gesehen werden. Aus diesem Grund ist es für die IT-Verantwortlichen empfehlenswert, die Geschäftsführung bzw. Behördenleitung über mögliche Risiken und Konsequenzen aufgrund fehlender IT-Sicherheit 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 und die damit verbundenen Auswirkungen und Kosten sollten aufgezeigt werden.
- Die Auswirkungen von IT-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 IT-Sicherheit 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 diese Sensibilisierung der Geschäftsleitung bzw. der Behördenleitung hinsichtlich der IT-Sicherheit externe Berater hinzuziehen.

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

Die Leitungsebene muss sich vor allem dafür einsetzen, dass IT-Sicherheit 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 wesentlichen Aktivität eingebunden zu werden.

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

3 Initiierung des IT-Sicherheitsprozesses

Um ein angemessenes und ausreichendes IT-Sicherheitsniveau zu erzielen bzw. dieses aufrechtzuerhalten, ist einerseits ein geplantes und organisiertes Vorgehen und andererseits eine adäquate Organisationsstruktur erforderlich. Darüber hinaus ist es notwendig, IT-Sicherheitsziele und eine Strategie zur Erreichung der Ziele zu definieren, sowie einen kontinuierlichen IT-Sicherheitsprozess aufzusetzen. Aufgrund der Bedeutung, der weitreichenden Konsequenzen der zu treffenden Entscheidungen und der Verantwortung muss für dieses Thema die Initiierung von der obersten Leitungsebene ausgetragen werden.

3.1 Konzeption und Planung des IT-Sicherheitsprozesses

Um ein angemessenes IT-Sicherheitsniveau erreichen und aufrecht erhalten zu können, ist es notwendig, einen kontinuierlichen IT-Sicherheitsprozess zu etablieren und eine angemessene IT-Sicherheitsstrategie festzulegen. Eine IT-Sicherheitsstrategie dient der Planung des weiteren Vorgehens, um das gesetzte IT-Sicherheitsziel zu erreichen. Sie wird vom Management vorgegeben und basiert auf den Geschäftszielen eines Unternehmens bzw. dem Auftrag einer Behörde. Das Management gibt grundlegende IT-Sicherheitsziele vor und legt fest, welches IT-Sicherheitsniveau im Hinblick auf die Geschäftsziele und Fachaufgaben angemessen ist. Die dafür erforderlichen Mittel müssen ebenfalls von der Leitungsebene zur Verfügung gestellt werden.

3.1.1 Ermittlung von Rahmenbedingungen

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

Zu jedem Geschäftsprozess und jeder Fachanwendung 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 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 IT-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 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 (z. B. personenbezogene Daten, Kundendaten, strategische Informationen, Geheimnisse wie Entwicklungsdaten, Patente, Verfahrensbeschreibungen)?

Eine Vielzahl interner Rahmenbedingungen können Auswirkungen auf die IT-Sicherheit haben und müssen ermittelt werden. Es geht zu diesem frühen Zeitpunkt nicht darum, detailliert die Informati-

onstechnik zu beschreiben. Es sollte aber eine grobe Übersicht vorliegen, welche Informationen für einen Geschäftsprozess mit welchen IT-Anwendungen und IT-Systemen verarbeitet werden.

Daneben müssen ebenso alle externe Rahmenbedingungen ermittelt werden, die Auswirkungen auf die IT-Sicherheit haben, wie beispielsweise gesetzliche Rahmenbedingungen, Umwelteinflüsse, Anforderungen von Kunden, Lieferanten und Geschäftspartnern, branchenspezifische IT-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.

Aktionspunkte:

- Ansprechpartner für alle Geschäftsprozesse und Fachanwendungen benennen
- Grobeinschätzung der Wertigkeit von Informationen, Geschäftsprozesse und Fachanwendungen durchführen
- Rahmenbedingungen ermitteln

3.1.2 Formulierung von allgemeinen IT-Sicherheitszielen

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

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

- Hohe Verlässlichkeit des Handelns, auch in Bezug auf den Umgang mit Informationen (Verfügbarkeit, Integrität, Vertraulichkeit),
- Gewährleistung des gutes 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 IT-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 eingesetzten IT und deren sicheren Funktionieren abhängt. Für die Definition der IT-Sicherheitsziele ist es sinnvoll, die zu schützende Grundwerte Verfügbarkeit, Integrität und Vertraulichkeit ausdrücklich zu benennen und eventuell zu priorisieren.

Diese Aussagen werden im Lauf des IT-Sicherheitsprozesses bei der Wahl der IT-Sicherheitsmaßnahmen und Strategien eine entscheidende Rolle spielen.

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

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

Nachstehend sind einige beispielhafte Kriterien zur Bestimmung eines angemessenen IT-Sicherheitsniveaus aufgeführt. Anhand derjenigen Aussagen, die am ehesten zutreffen, lässt sich das IT-Sicherheitsniveau (normal, hoch oder sehr hoch) bestimmen. In dieser Phase des IT-Sicherheitsprozesses geht es um die Formulierung der ersten richtungsweisenden 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.

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.

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.

Insgesamt gilt: Schäden haben Beeinträchtigungen der Institution zur Folge.

Für die Formulierung der IT-Sicherheitsziele ist die Mitwirkung der Leitungsebene unbedingt notwendig. Für diesen im IT-Sicherheitsprozess grundlegenden Schritt kann auch die Einbeziehung eines

externen IT-Sicherheitsexperten sinnvoll sein. Zur Bestimmung des angestrebten IT-Sicherheitsniveaus müssen die Ziele der Institution in Bezug auf ihrer IT-Sicherheitsanforderungen betrachtet werden, jedoch unter Berücksichtigung der Tatsache, dass in der Regel begrenzte Ressourcen für die Implementierung von IT-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 IT-Sicherheitsniveau in der Regel auch mit hohem Implementierungsaufwand verbunden ist. Es ist an der Stelle auch empfehlenswert, die formulierten Anforderungen zu priorisieren, wenn es möglich ist. Dies wird bei der Ressourcenplanung in späteren Phasen des IT-Sicherheitsprozesses eine Entscheidungsgrundlage bilden.

Hinweis zur Beschreibungstiefe

In dieser frühen Phase des IT-Sicherheitsprozesses geht es nicht um eine detaillierte Betrachtung aller IT-Systeme und Anwendungen 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 IT-Sicherheitsniveaus die folgenden Fragen beantworten lassen:

- Welche kritischen Aufgaben der Behörde bzw. des Unternehmens können ohne Unterstützung durch IT nicht, nur unzureichend oder mit erheblichem Mehraufwand ausgeführt werden?
- Welche wesentlichen Entscheidungen der Behörde bzw. des Unternehmens beruhen auf Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationsverarbeitungssystemen?
- Welche Auswirkungen können absichtliche oder ungewollte IT-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?

Die Beschreibungen des angestrebten IT-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 IT-Sicherheitsniveau notwendig, weil von der korrekten Funktion der IT-Systeme Menschenleben abhängen."

Aktionspunkte:

- Bedeutung der Geschäftsprozesse, Fachaufgaben und Informationen abschätzen
- Allgemeine IT-Sicherheitsziele festlegen
- Zustimmung der Leitungsebene einholen

3.1.3 Erstellung einer IT-Sicherheitsleitlinie

Die IT-Sicherheitsleitlinie 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 IT-Sicherheitsziele sowie die verfolgte IT-Sicherheitsstrategie. Die IT-Sicherheitsleitlinie beschreibt damit auch über die IT-Sicherheitsziele das angestrebte IT-Sicherheitsniveau in einer Behörde oder einem Unternehmen. Sie ist somit Anspruch und Aussage zugleich, dass dieses IT-Sicherheitsniveau auf allen Ebenen der Institution erreicht werden soll.

Die Erstellung der IT-Sicherheitsleitlinie sollte in folgenden Schritten vollzogen werden:

- **Verantwortung der Behörden- bzw. Unternehmensleitung für die IT-Sicherheitsleitlinie**

Mit der IT-Sicherheitsleitlinie wird dokumentiert, welche strategische Position die Institutionsleitung zur Erreichung der IT-Sicherheitsziele auf allen Ebenen der Organisation einnimmt.

Da die IT-Sicherheitsleitlinie das zentrale Strategiepapier für die IT-Sicherheit einer Institution darstellt, muss sie so gestaltet sein, dass sich alle 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 IT-Sicherheitsleitlinie mitwirken.

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

- Festlegung des Geltungsbereichs

In der IT-Sicherheitsleitlinie 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 nicht immer eine triviale Aufgabe. Eine Orientierung nach Verantwortlichkeiten kann dabei behilflich sein.

- Inhalt der IT-Sicherheitsleitlinie

Die IT-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 IT-Sicherheit und Bedeutung der IT für die Aufgabenerfüllung,
- Bezug der IT-Sicherheitsziele zu den Geschäftszielen oder Aufgaben der Institution,
- Sicherheitsziele und die Kernelemente der Sicherheitsstrategie für die eingesetzte IT,
- Zusicherung, dass die IT-Sicherheitsleitlinie von der Institutionsleitung durchgesetzt wird, und Leitaussagen zur Erfolgskontrolle und
- Beschreibung der für die Umsetzung des IT-Sicherheitsprozesses etablierten Organisationsstruktur (vergleiche M 2.193 *Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit*).

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 IT-Sicherheitsprozess sollten aufgezeigt werden (insbesondere für das IT-Sicherheitsmanagement-Team, den IT-Sicherheitsbeauftragten, die IT-Anwender und die IT-Administratoren). Außerdem sollten die Ansprechpartner für Sicherheitsfragen benannt werden.
- Programme zur Förderung der IT-Sicherheit durch Schulungs- und Sensibilisierungsmaßnahmen können angekündigt werden.

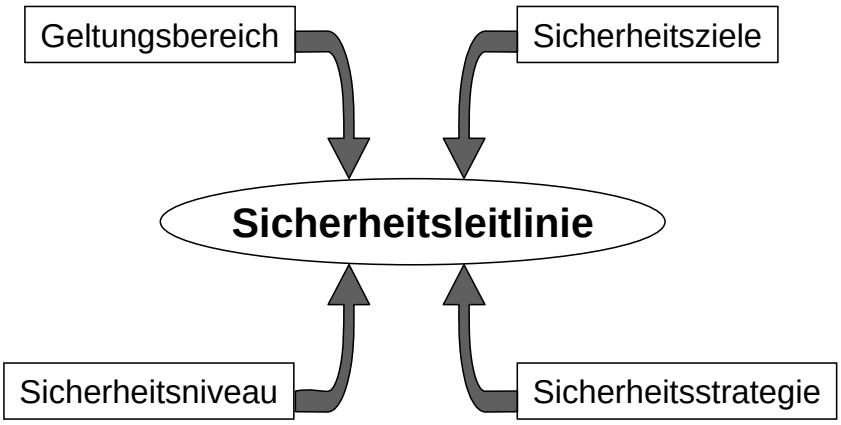


Abbildung: Inhalte der IT-Sicherheitsleitlinie

- Einberufung einer Entwicklungsgruppe für die IT-Sicherheitsleitlinie

Falls es innerhalb der Behörde oder des Unternehmens bereits ein IT-Sicherheitsmanagement-Team gibt, so sollte dieses die IT-Sicherheitsleitlinie entwickeln bzw. überprüfen und überarbeiten. Danach wird dieser Entwurf der Behörden- bzw. Unternehmensleitung zur Genehmigung vorgelegt.

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

- Bekanntgabe der IT-Sicherheitsleitlinie

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

Da die Verantwortung der Behörden- bzw. Unternehmensleitung in Bezug auf die IT-Sicherheitsleitlinie entscheidend ist, sollte die Leitlinie schriftlich fixiert sein. Die Behörden- bzw. Unternehmensleitung sollte ihr formell zugestimmt haben. Die Inhalte der IT-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 "IT-Sicherheit" von jedem Mitarbeiter ein engagiertes, kooperatives sowie verantwortungsbewusstes Handeln erwartet wird.

- **Aktualisierung der IT-Sicherheitsleitlinie**

Die IT-Sicherheitsleitlinie 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 IT-Sicherheitsleitlinie spätestens alle zwei Jahre zu überdenken.

Aktionspunkte:

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

3.2 Aufbau einer IT-Sicherheitsorganisation

Das angestrebte IT-Sicherheitsniveau kann nur erreicht werden, wenn der IT-Sicherheitsprozess institutionsweit umgesetzt wird. Dieser übergreifende Charakter des IT-Sicherheitsprozesses macht es notwendig, Rollen innerhalb der Behörde bzw. des Unternehmens 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 IT-Sicherheitsprozesses erforderlich ist, wird als IT-Sicherheitsorganisation bezeichnet.

Wie viele Personen, in welcher Organisationsstruktur und mit welchen Ressourcen mit IT-Sicherheit beschäftigt sind, hängt von der Größe, Beschaffenheit und Struktur der jeweiligen Institution ab. Auf jeden Fall sollte als zentraler Verantwortlicher für IT-Sicherheit ein IT-Sicherheitsbeauftragter benannt sein. In größeren Organisationen sollte außerdem ein IT-Sicherheitsmanagement-Team aufgebaut werden, das sämtliche übergreifenden Belange der IT-Sicherheit 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 IT-Sicherheit eindeutig einem verantwortlichen Manager zugeordnet sein, an den der IT-Sicherheitsbeauftragte berichtet.

Grundregel:

Das Wichtigste bei der Definition von Rollen im IT-Sicherheitsmanagement ist:

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

Integration der IT-Sicherheit in organisationsweite Abläufe und Prozesse

Das IT-Sicherheitsmanagement ist zwar nur eine von vielen wichtigen Managementaufgaben, hat jedoch Einfluss auf nahezu alle Bereiche einer Institution. Daher muss das IT-Sicherheitsmanagement 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 IT-Sicherheitsaspekte berücksichtigt werden (zum Beispiel über Outsourcing oder die Nutzung neuer elektronischer Vertriebskanäle). Um dies sicherzustellen ist es wichtig, dass die IT-Sicherheitsorganisation 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.

Aufbau der IT-Sicherheitsorganisation

In Abhängigkeit von der Institutionsgröße bieten sich verschiedene Möglichkeiten für die Aufbauorganisation des IT-Sicherheitsmanagements an. In den nachstehenden Abbildungen werden drei davon aufgezeigt. Die erste Abbildung zeigt die Struktur für die IT-Sicherheitsorganisation in einer großen Institution. Die zweite Abbildung zeigt den Aufbau in einer mittelgroßen Institution, in der das IT-Sicherheitsmanagement-Team und der IT-Sicherheitsbeauftragte zusammengefasst wurden. Die dritte Abbildung zeigt eine Struktur für die IT-Sicherheitsorganisation in einer kleinen Institution, in der alle Aufgaben vom IT-Sicherheitsbeauftragten wahrgenommen werden.

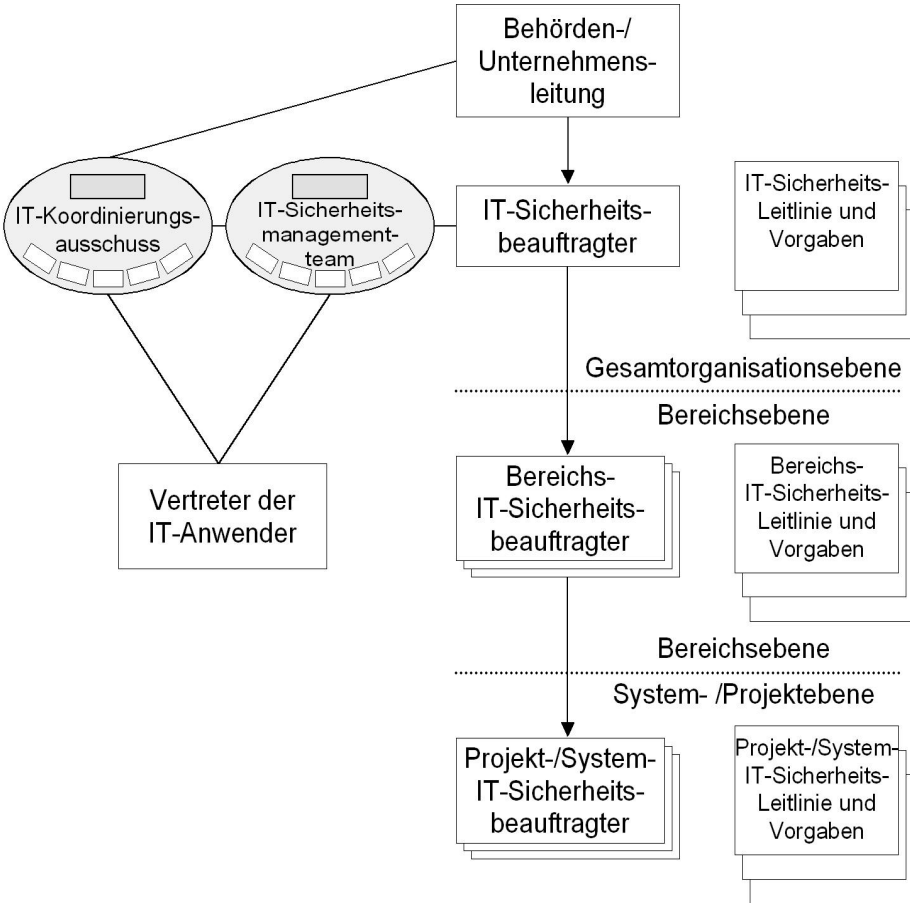


Abbildung: Aufbau der IT-Sicherheitsorganisation in einer großen Institution

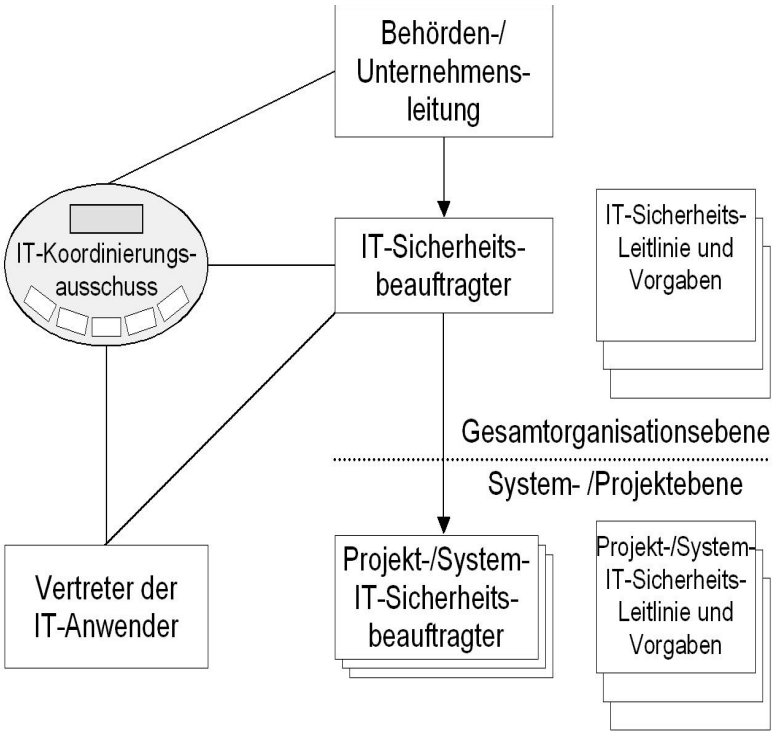


Abbildung: Aufbau der IT-Sicherheitsorganisation in einer mittelgroßen Institution

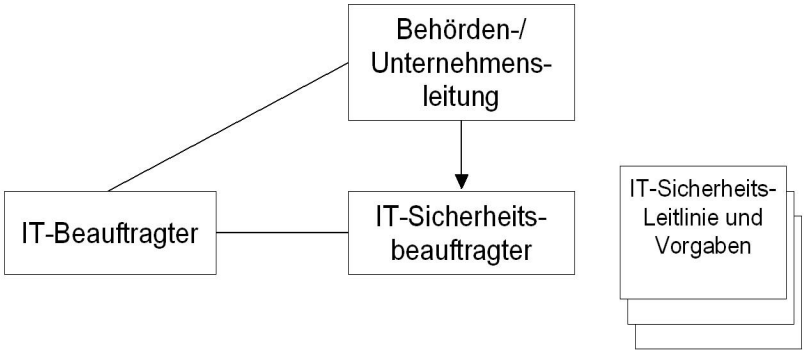


Abbildung: Aufbau der IT-Sicherheitsorganisation in einer kleinen Institution

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 IT-Sicherheitsniveau. Die Ressourcenplanung für die Unterstützung der IT-Sicherheit muss so erfolgen, dass das beschlossene IT-Sicherheitsniveau auch tatsächlich erreicht werden kann.

Aufgaben, Verantwortungen und Kompetenzen in der IT-Sicherheitsorganisation

IT-Sicherheitsbeauftragte und IT-Sicherheitsmanagement-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 dergestalt in die Organisationsstruktur einzubinden, dass alle Beteiligten untereinander kommunizieren können. Mit der Wahrnehmung der Aufgaben als IT-Sicherheitsbeauftragte bzw. im IT-Sicherheitsmanagement-Team sollte qualifiziertes Personal betraut werden. Bei Bedarf können unterstützend Aufgaben an Bereichs-IT-Sicherheitsbeauftragte, IT-Projekt- sowie IT-System-Sicherheitsbeauftragte delegiert werden.

Der IT-Sicherheitsbeauftragte

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

Um einen IT-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 IT-Sicherheitsziele wahrnehmen müssen. Außerdem müssen Personen benannt sein, die qualifiziert sind und denen ausreichend Ressourcen zur Verfügung stehen, um diese Rollen auszufüllen.

Der IT-Sicherheitsbeauftragte ist zuständig für die Wahrnehmung aller Belange der IT-Sicherheit innerhalb der Institution. Die Hauptaufgabe des IT-Sicherheitsbeauftragten besteht darin, die Behörden- bzw. Unternehmensleitung bei der Wahrnehmung deren Aufgaben bezüglich der IT-Sicherheit zu beraten und bei deren Umsetzung zu unterstützen. Seine Aufgaben umfassen unter anderen:

- den IT-Sicherheitsprozess zu steuern und bei allen damit zusammenhängenden Aufgaben mitzuwirken,
- die Leitungsebene bei der Erstellung der IT-Sicherheitsleitlinie zu unterstützen,
- die Erstellung des IT-Sicherheitskonzepts, des Notfallvorsorgekonzepts und anderer Teilkonzepte und System-Sicherheitsrichtlinien zu koordinieren, sowie weitere Richtlinien und Regelungen zur IT-Sicherheit zu erlassen,
- die Realisierung für IT-Sicherheitsmaßnahmen zu initiieren und zu überprüfen,
- der Leitungsebene und dem IT-Sicherheitsmanagement-Team über den Status Quo der IT-Sicherheit zu berichten,
- sicherheitsrelevante Projekte zu koordinieren,
- Untersuchung von IT-Sicherheitsvorfällen und
- Initiierung und Koordination von Sensibilisierungs- und Schulungsmaßnahmen.

Der IT-Sicherheitsbeauftragte ist außerdem bei allen neuen Projekten mit IT-Bezug sowie der Einführung neuer IT-Anwendungen und IT-Systeme zu beteiligen, um die Beachtung von IT-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 IT-Sicherheit 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 IT-Sicherheit, Überblick über Aufgaben und Ziele der Institution und Einsicht in die Notwendigkeit von IT-Sicherheit,
- Kooperations- und Teamfähigkeit aber auch Durchsetzungsvermögen (wenige andere Aufgaben erfordern so viel Fähigkeit und Geschick im Umgang mit anderen Personen: Die Leitungsebene muss in zentralen Fragen des IT-Sicherheitsprozesses immer wieder eingebunden werden, Entscheidungen müssen eingefordert werden und die IT-Benutzer müssen - evtl. mit Hilfe des Bereichs-IT-Sicherheitsbeauftragten - in den IT-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 IT-Benutzern verlangt viel Geschick, da diese zunächst von der Notwendigkeit der (für sie manchmal etwas lästigen) IT-Sicherheitsmaßnahmen überzeugt werden müssen. Ein ebenfalls sehr sensibles Thema ist die Befragung der IT-Benutzer nach sicherheitskritischen Vorkommnissen und Schwachstellen. Um den Erfolg dieser Befragungen zu garantieren, müssen die IT-Benutzer davon überzeugt werden, dass ehrliche Antworten nicht zu Problemen für sie selbst führen.

Die Kommunikationsfähigkeiten des IT-Sicherheitsbeauftragten sind nicht nur gegenüber den IT-Benutzern 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 Stabsaufgabe einzurichten. 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.

Datenschutzbeauftragter

Eine häufige Frage ist, ob die Position des IT-Sicherheitsbeauftragten gleichzeitig vom Datenschutzbeauftragten wahrgenommen werden kann. 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 nach oben 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.

Das IT-Sicherheitsmanagement-Team

Das IT-Sicherheitsmanagement-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 IT-Sicherheitsniveau und den vorhandenen Ressourcen ab. Im Extremfall besteht das IT-Sicherheitsmanagement-Team nur aus einer einzigen Person, dem IT-Sicherheitsbeauftragten, dem in diesem Fall sämtliche Aufgaben im IT-Sicherheitsprozess obliegen.

Aufgaben des IT-Sicherheitsmanagement-Teams sind insbesondere:

- IT-Sicherheitsziele und -strategien zu bestimmen sowie die IT-Sicherheitsleitlinie zu entwickeln,
- die Umsetzung der IT-Sicherheitsleitlinie zu überprüfen,

- den IT-Sicherheitsprozess zu initiieren, zu steuern und zu kontrollieren,
- bei der Erstellung des IT-Sicherheitskonzepts mitzuwirken,
- zu überprüfen, ob die im IT-Sicherheitskonzept geplanten IT-Sicherheitsmaßnahmen wie beabsichtigt funktionieren sowie geeignet und wirksam sind,
- die Schulungs- und Sensibilisierungsprogramme für IT-Sicherheit zu konzipieren sowie
- den IT-Koordinierungsausschuss und die Leitungsebene in IT-Sicherheitsfragen zu beraten.

Zusammensetzung des Teams

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

Nur wenige, entweder sehr große Organisationen oder solche mit einem hohen Bedarf an IT-Sicherheit, werden die Möglichkeit haben, hauptamtliche Stellen für das IT-Sicherheitsmanagement-Team bereitstellen zu können. Im allgemeinen werden diese Aufgaben neben den originären Aufgaben wahrzunehmen sein. Eine Ausnahme stellt hier jedoch die erstmalige Einrichtung des IT-Sicherheitsprozesses dar. Wenn möglich sollten die Mitglieder des IT-Sicherheitsmanagement-Teams während dieser Phase weitgehend von ihren sonstigen Aufgaben freigestellt werden. Die Entscheidung, ob und inwieweit diese Freistellung auch danach noch sinnvoll ist, hängt von der Aufgabenverteilung zwischen IT-Sicherheitsmanagement-Team und IT-Sicherheitsbeauftragten ab. Die letztendliche Entscheidung hierfür liegt bei der Behörden- bzw. Unternehmensleitung. In jedem Fall sollte das IT-Sicherheitsmanagement regelmäßig tagen, um eine kontinuierliche Steuerung des IT-Sicherheitsprozesses zu gewährleisten.

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

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

- die Vorgaben des IT-Sicherheitsbeauftragten umsetzen,
- die IT-Sicherheitsmaßnahmen gemäß IT-System-Sicherheitsleitlinie umsetzen,
- IT-systemspezifische Informationen zusammenfassen und an den IT-Sicherheitsbeauftragten weiterleiten,
- als Ansprechpartner der IT-Benutzer vor Ort dienen,

- bei der Auswahl der IT-Sicherheitsmaßnahmen zur Umsetzung der IT-System-Sicherheitsleitlinie mitwirken,
- Information über Schulungs- und Sensibilisierungsbedarf von IT-Benutzern an den IT-Sicherheitsbeauftragten ermitteln,
- Protokolldateien regelmäßig kontrollieren und auswerten, sowie
- eventuell auftretende sicherheitsrelevante Zwischenfälle an den IT-Sicherheitsbeauftragten melden.

Folgende *Qualifikationen* sollten vorhanden sein:

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

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 IT-Sicherheitsmanagement-Team, dem Vertreter der IT-Anwender, dem IT-Sicherheitsbeauftragten und der Behörden- bzw. Unternehmensleitung zu koordinieren.

Aktionspunkte:

- Rollen für die Gestaltung des IT-Sicherheitsprozesses festlegen
- Aufgaben und Verantwortungsbereiche den Rollen zuordnen
- Personelle Ausstattung der Rollen festlegen
- IT-Sicherheitsorganisation dokumentieren
- IT-Sicherheitsmanagement in die organisationsweiten Abläufe und Prozesse integrieren

3.3 Bereitstellung von Ressourcen für die IT-Sicherheit

Bedrohungen können Schäden und damit Kosten verursachen, Risikovorsorge kostet aber auch Ressourcen – ein effektives Risikomanagement hilft, diese Kosten zu steuern. Ein angemessenes Maß an IT-Sicherheit ist immer nur mit einem entsprechenden Aufwand zu erreichen und aufrechtzuerhalten. Deshalb ist beim Festlegen des IT-Sicherheitsniveaus und bei der Formulierung konkreter IT-Sicherheitsanforderungen für die jeweilige Institution darauf zu achten, dass das angestrebte IT-Sicherheitsniveau auch wirtschaftlich sinnvoll sind. Wenn es sich herausstellt, dass die gestellten Sicherheitsanforderungen nicht finanzierbar sind, müssen die Sicherheitsanforderungen, aber auch die Geschäftsprozesse und die Art und Weise des IT-Betriebs grundsätzlich überdacht werden.

Die Erfahrung zeigt, dass das Verhältnis zwischen dem Aufwand, der zur Erhöhung des IT-Sicherheitsniveaus erforderlich ist, und dem dadurch erreichten Sicherheitsgewinn immer ungünstiger wird, je höher das angestrebte IT-Sicherheitsniveau ist. Absolut perfekte IT-Sicherheit ist nicht erreichbar. Das nachstehende Diagramm soll verdeutlichen, wie viel Aufwand in Relation zum angestrebten IT-Sicherheitsniveau zu betreiben ist. Dieser Aufwand bietet eine Orientierung für die personellen, zeitlichen und monetären Ressourcen, die zur Erreichung dieses IT-Sicherheitsniveaus notwendig sind.

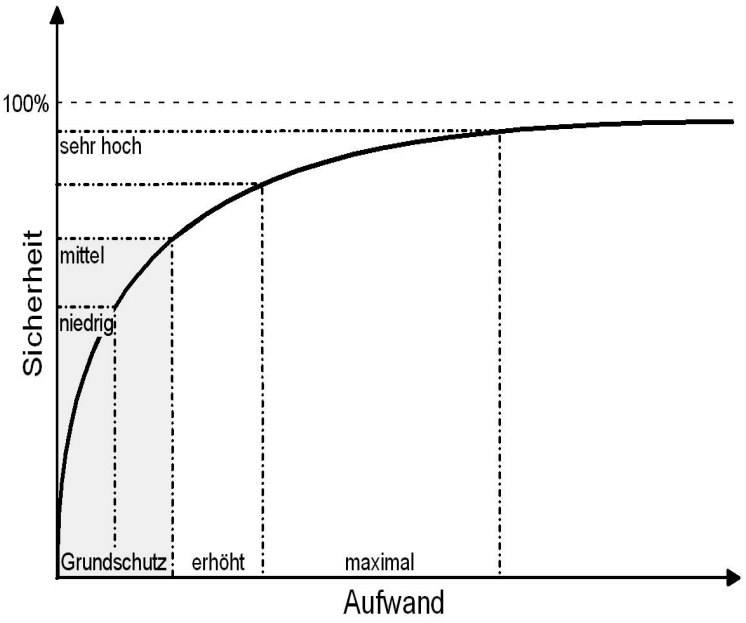


Abbildung: Aufwand-Nutzen-Relation für IT-Sicherheit

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

IT-Sicherheit 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. Daher ist es 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.

Bereitstellung von 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 IT-Sicherheitsmaßnahmen wirksam und effizient umgesetzt werden können.

Zugriff auf externe Ressourcen

In der Praxis fehlt den internen IT-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 IT-Sicherheitsexperten dokumentiert werden, damit die Leitungsebene die erforderlichen Ressourcen bereit stellt.

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

Ressourcen für das IT-Sicherheitsmanagement-Team bzw. den IT-Sicherheitsbeauftragten

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

Nur wenige Organisationen, entweder sehr große oder solche mit einem hohen Bedarf an IT-Sicherheit, werden die Möglichkeit haben, hauptamtliche Stellen für ein IT-Sicherheitsmanagement-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 IT-Sicherheitsprozesses dar. Wenn möglich, sollten die Mitglieder des IT-Sicherheitsmanagement-Teams während dieser Phase weitgehend von ihren sonstigen Aufgaben freigestellt werden.

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

Berücksichtigung von Wirtschaftlichkeitsaspekten bei der Ausarbeitung der IT-Sicherheitsstrategie

Bei der Ausgestaltung der IT-Sicherheitsstrategie sind von vornherein Wirtschaftlichkeitsaspekte zu berücksichtigen. Stellt sich heraus, dass die notwendigen IT-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 dann Geschäftsprozesse oder die Art und Weise des IT-Betriebs grundsätzlich überdacht werden.

Ressourcen für die Überprüfung der IT-Sicherheit

Die Überprüfung von Wirksamkeit und Eignung von IT-Sicherheitsmaßnahmen muss durch ausreichende Ressourcen sichergestellt werden. 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 sehr hohe Kosten verursacht hat, sind alternative Maßnahmen zu überlegen. Es kann beispielsweise sinnvoll sein, bestimmte IT-Systeme nicht an unsichere Netze anzuschließen, wenn der Aufwand zur Sicherung zu hoch ist.

Aktionspunkte:

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

3.4 Einbindung aller Mitarbeiter in den IT-Sicherheitsprozess

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

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

Schulung und Sensibilisierung

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

Ansprechpartner zu IT-Sicherheitsthemen und Meldewege

Damit die Mitarbeiter den Bezug zu IT-Sicherheitsthemen auch nach den Schulungs- und Sensibilisierungsmaßnahmen behalten ist es wichtig, Ansprechpartner zu IT-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 IT-Sicherheitsvorfälle. Jeder Mitarbeiter muss wissen, wie er sich bei Verdacht auf einen Sicherheitsvorfall verhalten muss und wer der zuständige Ansprechpartner ist oder es muss möglich sein, diese Informationen schnell und unter allen Umständen in Erfahrung zu bringen.

Beteiligung von Mitarbeitern

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.

Aufgabenwechsel oder Ausscheiden von Mitarbeitern

Wenn Mitarbeiter ausscheiden, andere Aufgaben übernehmen oder Zuständigkeiten verlieren, muss dies durch geeignete Sicherheitsmaßnahmen (z. B. Entzug von Berechtigungen, Rückgabe von Schlüsseln) begleitet und dokumentiert werden.

Aktionspunkte:

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

4 Erstellung einer IT-Sicherheitskonzeption nach IT-Grundschutz

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

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.

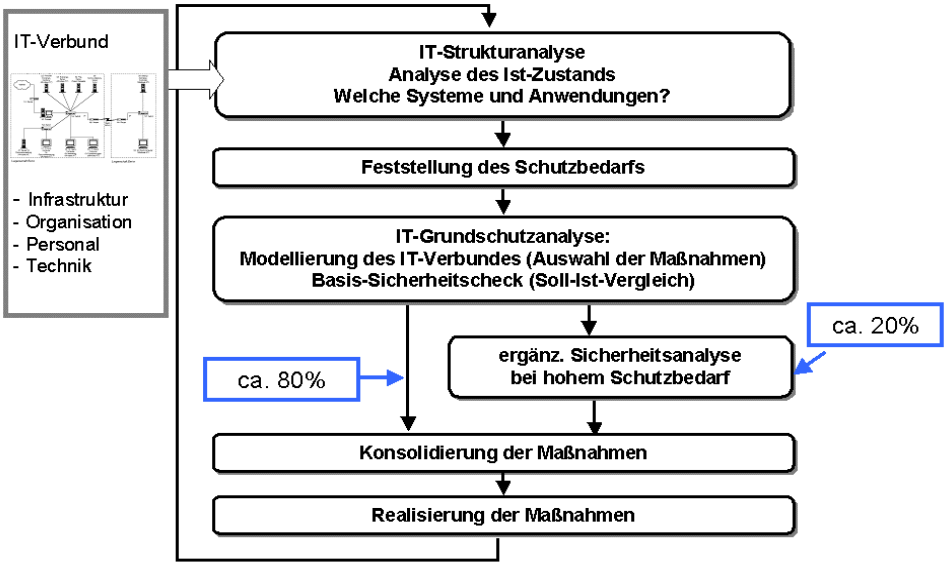


Abbildung: Erstellung der IT-Sicherheitskonzeption im IT-Sicherheitsmanagement

Die Methodik des IT-Grundschutzes

Bei der traditionellen Risikoanalyse werden zunächst die Bedrohungen ermittelt und mit Eintrittswahrscheinlichkeiten bewertet, um dann die geeigneten IT-Sicherheitsmaßnahmen auszuwählen und anschließend noch das verbleibende Restrisiko bewerten zu können. Diese Aufgabe ist beim IT-Grundschutz bereits für jeden Baustein durchgeführt worden und die für eine typische Büroumgebung passenden IT-Sicherheitsmaßnahmen ausgewählt worden. Bei Anwendung des IT-Grundschutzes reduziert sich diese Aufgabe 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. Hierbei reicht es dann aber in der Regel aus, die Maßnahmenempfehlungen der IT-Grundschutz-Kataloge durch entsprechende individuelle, qualitativ höherwertige Maßnahmen, zu ergänzen. Einen einfache Vorgehensweise hierzu ist in dem BSI-Dokument "Risikoanalyse basierend auf IT-Grundschutz" beschrieben.

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 IT-Grundschutz-Zertifizierung gefordert werden, das Minimum dessen dar, was in jedem Fall vernünftigerweise an Sicherheitsvorkehrungen umzusetzen ist. Die als "zusätzlich" gekennzeichneten Maßnahmen haben sich ebenfalls in der Praxis bewährt, sie richten sich jedoch an Anwendungsfälle mit erhöhten Sicherheitsanforderungen.

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 umsetzbar zu gestalten, 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.

Die Vorgehensweise nach IT-Grundschutz gliedert sich grob in folgende Bereiche:

Definition des IT-Verbunds

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 IT-Verbund festgelegt werden, für den die IT-Sicherheitskonzeption gelten soll. Unter einem IT-Verbund ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein IT-Verbund kann dabei als Ausprägung die gesamte IT einer Institution oder auch einzelne Bereiche, die durch organisatorische Strukturen (z. B. Abteilungsnetz) oder gemeinsame Geschäftsprozesse bzw. IT-Anwendungen (z. B. Personalinformationssystem) gegliedert sind, umfassen.

IT-Strukturanalyse

Für die Erstellung eines IT-Sicherheitskonzepts und insbesondere für die Anwendung der IT-Grundschutz-Kataloge ist es erforderlich, die Struktur 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 Analyse an. Die folgenden Aspekte müssen berücksichtigt werden:

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

Die einzelnen Schritte der IT-Strukturanalyse werden im Detail in Kapitel 4.1 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 angemes-

sen 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 4.2 dieses Dokuments erläutert.

IT-Sicherheitskonzeption

Die Informationstechnik in Behörden und Unternehmen ist heute üblicherweise durch stark vernetzte IT-Systeme geprägt. In der Regel ist es daher zweckmäßig, im Rahmen einer IT-Sicherheitsanalyse bzw. IT-Sicherheitskonzeption einen größeren IT-Verbund und nicht einzelne IT-Systeme zu betrachten. Voraussetzung für die Anwendung des IT-Grundschutz-Katalogen auf einen IT-Verbund sind detaillierte Unterlagen über seine Struktur. Diese können beispielsweise über die oben beschriebene IT-Strukturanalyse gewonnen werden. Anschließend müssen die Bausteine des IT-Grundschutzes in einem Modellierungsschritt auf die Komponenten des vorliegenden IT-Verbunds abgebildet werden.

Im Abschnitt 4.3 dieses Dokuments wird beschrieben, wie die Modellierung eines IT-Verbunds durch IT-Grundschutz-Bausteine vorgenommen werden sollte. Wie der anschließende Soll-Ist-Vergleich anhand eines Basis-Sicherheitschecks durchgeführt werden sollte, wird in Kapitel 4.4 beschrieben.

Basis-Sicherheitscheck

Der Basis-Sicherheitscheck ist ein Organisationsinstrument, welches einen schnellen Überblick über das vorhandene IT-Sicherheitsniveau bietet. Mit Hilfe von Interviews wird der Status Quo eines bestehenden (nach IT-Grundschutz modellierten) IT-Verbunds 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 Informationstechnik aufgezeigt. Kapitel 4.4 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.

IT-Sicherheitsrevision

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

Weiterführende IT-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 IT-Sicherheitsmaßnahmen erforderlich sind. Geeignete Maßnahmen für Bereiche mit höherem Schutzbedarf sollten über ergänzende Sicherheitsanalysen ausgewählt werden.

Eine Methode hierfür ist die im BSI-Dokument "Risikoanalyse basierend auf IT-Grundschutz" beschriebene Vorgehensweise. In Kapitel 4.5 wird diese Methode überblicksartig dargestellt. Die erfolgreiche Durchführung einer ergänzenden Sicherheitsanalyse hängt entscheidend von den Fachkenntnissen des Projektteams ab. Daher ist es häufig sinnvoll, fachkundiges externes Personal hinzuzuziehen.

Umsetzung von IT-Sicherheitskonzepten

Ein ausreichendes IT-Sicherheitsniveau lässt sich nur erreichen, wenn in einer Sicherheitsanalyse bestehende Schwachstellen ermittelt werden, in einem Sicherheitskonzept der Status Quo festgehalten wird, erforderliche Maßnahmen identifiziert und wenn insbesondere diese Maßnahmen auch konsequent umgesetzt werden. In Kapitel 4.6 wird beschrieben, was bei der Umsetzungsplanung von IT-Sicherheitsmaßnahmen beachtet werden muss.

Zertifizierung nach IT-Grundschutz

Die Vorgehensweise nach IT-Grundschutz und die IT-Grundschutz-Kataloge werden nicht nur für die IT-Sicherheitskonzeption, sondern auch zunehmend als Referenz im Sinne eines Sicherheitsstandards verwendet. Durch eine IT-Grundschutz-Zertifizierung bzw. -Qualifizierung kann eine Institution nach innen und außen hin dokumentieren, dass sie IT-Grundschutz in der erforderlichen Tiefe umgesetzt hat.

4.1 IT-Strukturanalyse

In den IT-Grundschutz-Katalogen werden standardisierte IT-Sicherheitsmaßnahmen für typische Büroumgebungen empfohlen. Da aber jede Büroumgebung ihre spezifischen Eigentümlichkeiten hat, müssen die IT-Sicherheitsmaßnahmen auf diese Besonderheiten angepasst werden. Sie müssen auf die zu schützenden Geschäftsprozesse, die damit verarbeitenden Informationen sowie die eingesetzten IT-Systeme und IT-Anwendungen abgestimmt werden. Es ist daher notwendig, eine Übersicht über die eingesetzten IT-Anwendungen und IT-Systeme zur Verfügung zu haben, denn viele der erforderlichen Maßnahmen sind meistens stark von der eingesetzten IT-Umgebung abhängig.

4.1.1 Erfassung des IT-Verbunds

In der Praxis werden in der Regel zunächst aus der Analyse der Geschäftsprozesse die geschäftskritischen Informationen und IT-Anwendungen ermittelt und dann die betroffenen IT-Systeme erfasst. Je nach Situation kann es aber auch sinnvoll sein, zuerst die IT-Systeme zu erfassen und anschließend die darauf betriebenen IT-Anwendungen zu betrachten.

Auch wenn so wie oben beschrieben vorgegangen wird, ist sehr zu empfehlen, auch die umgekehrte Richtung zu betrachten: Zum einen wird dabei überprüft, ob wirklich alle IT-Systeme erfasst wurden. Oftmals werden sich IT-Systeme finden, die vorher keiner IT-Anwendung zugeordnet wurden, weil ihre Bedeutung den befragten Informationseigentümern vielleicht nicht bekannt war. Zum anderen wird gezielt geprüft, welche IT-Anwendungen tatsächlich auf den IT-Systemen installiert sind. Dabei wird sich herausstellen, ob sicherheitskritische Anwendungen übersehen wurden.

Die IT-Strukturanalyse dient der Vorerhebung von Informationen, die für die weitere Vorgehensweise in der Erstellung eines IT-Sicherheitskonzepts nach IT-Grundschutz benötigt werden. Sie gliedert sich in folgende Teilaufgaben:

- Netzplanerhebung,
- Erhebung der IT-Systeme,
- Erfassung der IT-Anwendungen und der zugehörigen Informationen,
- Erfassung der IT-Räume und
- Komplexitätsreduktion durch Gruppenbildung.

Diese Teilaufgaben werden nachfolgend beschrieben und durch ein begleitendes Beispiel erläutert. Eine ausführliche Version des Beispiels findet sich in den Hilfsmitteln zum IT-Grundschutz

4.1.2 Netzplanerhebung

Auswertung eines Netzplans

Einen geeigneten Ausgangspunkt für die IT-Strukturanalyse stellt ein Netzplan (beispielsweise in Form eines Netztopologieplans) dar. Ein Netzplan ist eine graphische Übersicht über die im betrach-

teten Bereich der Informations- und Kommunikationstechnik eingesetzten Komponenten und deren Vernetzung. Im Einzelnen sollte der Plan folgende Objekte darstellen:

- IT-Systeme, d. h. Client- und Server-Computer, aktive Netzkomponenten (wie Hubs, 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 sollte 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. 10 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).

Es empfiehlt sich, Bereiche mit unterschiedlichem Schutzbedarf zu kennzeichnen.

Der Netzplan muss nicht zwangsläufig auf Papier erstellt werden. Hat die Informationstechnik im Unternehmen bzw. in der Behörde 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 Behörde bzw. des Unternehmens 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 IT-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.

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

Im Folgenden wird anhand einer fiktiven Behörde, dem BOV, beispielhaft dargestellt, wie ein bereinigter Netzplan aussehen kann. Zu beachten ist, dass die IT-Struktur des BOV im Hinblick auf IT-Sicherheit 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.

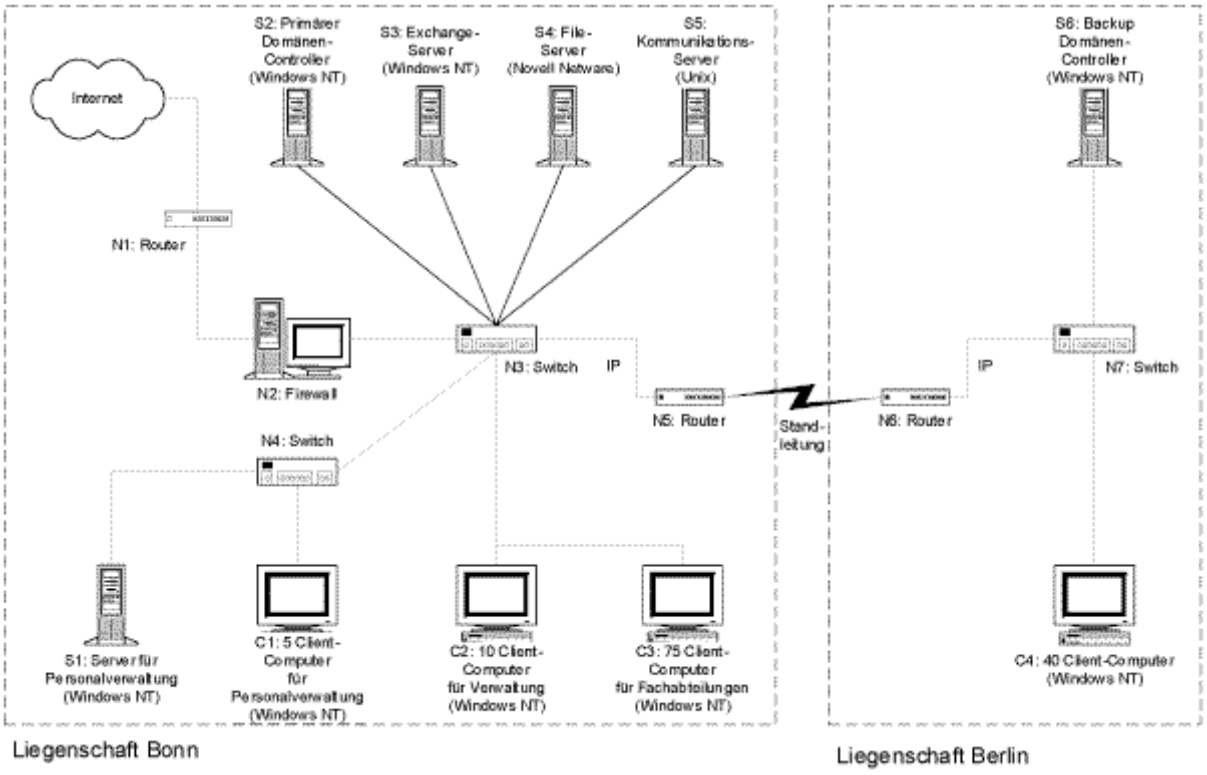


Abbildung: Beispiel eines bereinigten Netzplans

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*), die Funktion und gegebenenfalls das Betriebssystem (in Klammern) 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 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:

- 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

4.1.3 Erhebung der IT-Systeme

Im Hinblick auf die später durchzuführende Schutzbedarfsfeststellung und Modellierung des IT-Verbunds 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 NT-Server, Client unter Windows XP, Unix-Server, TK-Anlage. 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 IT-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 bei der Bereinigung des Netzplans 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 Einzelplatz-PCs, die die im Abschnitt "Komplexitätsreduktion durch Gruppenbildung" 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/Administrator des IT-Systems.

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

Als Beispiel ist in der folgenden Tabelle ein Auszug aus der Liste der IT-Systeme im BOV aufgeführt. Die vollständige Liste ist den Hilfsmitteln auf der CD-ROM beigefügt.

Nr.	Beschreibung	Plattform	Anzahl	Aufstellungsort	Status	Anwender/ Admin.
S1	Server für Personalverwaltung	Windows NT-Server	1	Bonn, R 1.01	in Betrieb	Personalreferat
S2	Primärer Domänen-Controller	Windows NT-Server	1	Bonn, R 3.10	in Betrieb	alle IT-Anwender
C1	Gruppe von Clients der Personaldatenverarbeitung	Windows NT-Workstation	5	Bonn, R 1.02 - R 1.06	in Betrieb	Personalreferat
C2	Gruppe von Clients in der Verwaltungsabteilung	Windows NT-Workstation	10	Bonn, R 1.07 - R 1.16	in Betrieb	Verwaltungsabteilung
C6	Gruppe der Laptops für den Standort Berlin	Laptop unter Windows 95	2	Berlin, R 2.01	in Betrieb	alle IT-Anwender in der Außenstelle Berlin
N1	Router zum Internet-Zugang	Router	1	Bonn, R 3.09	in Betrieb	alle IT-Anwender
N2	Firewall	Application Gateway auf Unix	1	Bonn, R 3.09	in Betrieb	alle IT-Anwender
N3	Switch	Switch	1	Bonn, R 3.09	in Betrieb	alle IT-Anwender
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).

Aktionspunkte:

- 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

4.1.4 Erfassung der IT-Anwendungen und der zugehörigen Informationen

Zur Reduzierung des Aufwands werden die jeweils wichtigsten auf den betrachteten IT-Systemen laufenden oder geplanten IT-Anwendungen erfasst. Zur effizienten Durchführung dieser Aufgabe kann auf eine vollständige Erfassung aller Anwendungen verzichtet werden, wenn sichergestellt ist, dass zumindest diejenigen IT-Anwendungen des jeweiligen IT-Systems benannt werden,

- deren Daten bzw. Informationen und Programme den höchsten Bedarf an Geheimhaltung (Vertraulichkeit) besitzen,
- deren Daten bzw. Informationen und Programme den höchsten Bedarf an Korrektheit und Unverfälschtheit (Integrität) besitzen,
- die die kürzeste tolerierbare Ausfallzeit (höchster Bedarf an Verfügbarkeit) haben.

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

Es erleichtert die Definition und Erfassung der IT-Anwendungen, wenn die IT-Anwendungen orientiert an den IT-Systemen zusammengetragen werden. 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 IT-Anwendungen unterstützen.

Zweckmäßigerweise sollten die Anwendungen zu Referenzzwecken 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 IT-Anwendung personenbezogene Daten speichert und/oder verarbeitet. Da der Schutzbedarf einer Anwendung in der Regel aus dem Schutzbedarf der damit verarbeiteten Informationen resultiert, sollte die Art dieser Informationen auch in der Tabelle dokumentiert werden.

Anschließend werden die Anwendungen jeweils denjenigen IT-Systeme zugeordnet, die für deren Ausführung benötigt werden. Dies können die IT-Systeme sein, auf denen die IT-Anwendungen verarbeitet werden, oder auch diejenigen, die Daten dieser Anwendung transferieren.

Das Ergebnis ist eine Übersicht, welche wichtigen IT-Anwendungen auf welchen IT-Systemen bearbeitet oder von welchen IT-Systemen genutzt oder übertragen werden.

Es empfiehlt sich, bei den IT-Anwendungen zu vermerken, welche Geschäftsprozesse sie unterstützen und welche Informationen verarbeitet werden. Jeder Geschäftsprozess hat einen Eigentümer bzw. Verantwortlichen. Die dazu gehörigen IT-Anwendungen haben Benutzer. Diese Informationen sollten ebenfalls erfasst werden, um Ansprechpartner für IT-Sicherheitsfragen leichter identifizieren zu können bzw. um betroffene Benutzergruppen schnell erreichen zu können.

Zur Dokumentation der Ergebnisse bietet sich die Darstellung in tabellarischer Form an.

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

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

Beschreibung der IT-Anwendungen			IT-Systeme						
Anw.-Nr.	IT-Anwendung/ Informationen	Pers.-bez. Daten	S1	S2	S3	S4	S5	S6	S7
A1	Personaldatenverarbeitung	X	X						
A2	Beihilfeabwicklung	X	X						
A3	Reisekostenabrechnung	X	X						
A4	Benutzer-Authentisierung	X		X				X	
A5	Systemmanagement			X					
A6	Exchange (E-Mail, Terminkalender)	X			X				
A7	zentrale Dokumentenverwaltung					X			

Legende: A_i X S_j = Die Ausführung der IT-Anwendung A_i hängt vom IT-System S_j ab.

Erfassung der Abhängigkeiten zwischen IT-Anwendungen

Optional kann noch zur besseren Übersicht die Abhängigkeit von IT-Anwendungen untereinander dargestellt werden (z. B. Abhängigkeit einer Anwendung von einer bestimmten Datenbank).

Aktionspunkte:

- Falls nicht alle IT-Anwendungen erfasst werden, Anwendungsverantwortliche nach ihrer Einschätzung befragen, welche IT-Anwendungen pro IT-System den höchsten Schutzbedarf haben
- Übersicht über die IT-Anwendungen erstellen und mit eindeutigen Nummern oder Kürzeln kennzeichnen

- Die IT-Anwendungen den IT-Systemen (Servern, Clients, Netzkoppelelementen etc.) zuordnen, die für ihre Ausführung benötigt werden
- Für jede IT-Anwendung die entsprechenden Geschäftsprozesse, verarbeitete Informationen, Eigentümer und gegebenenfalls Benutzer vermerken
- Für jede IT-Anwendung vermerken, inwieweit personenbezogene Daten mit ihr verarbeitet werden

4.1.5 Erfassung der Räume

Die betrachteten Geschäftsprozesse und Fachanwendungen 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 auch Liegenschaften, die weit verstreut sind oder mit anderen Nutzern geteilt werden müssen. In ein Sicherheitskonzept müssen alle Liegenschaften einbezogen werden, innerhalb derer die betrachteten Geschäftsprozesse und Fachanwendungen betrieben werden. Dazu gehören Betriebsgelände, Gebäude, Etagen, Räume sowie die Wegstrecke zwischen diesen. Alle Kommunikationsverbindungen, die über Wegstrecken gehen, die über für Dritte zugängliche Gelände verlaufen, müssen als Außenverbindungen behandelt werden.

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 Erfassung 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 erfasst werden. Die Art der verarbeiteten Informationen muss aus dieser Dokumentation nachvollziehbar sein.

In der folgenden Tabelle wird gezeigt, wie eine solche 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		
Bezeich-nung	Art	Lokation	IT-Systeme / Datenträger	Vertrau-lichkeit	Integrität	Verfüg-barkeit
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:

- 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

4.1.6 Komplexitätsreduktion durch Gruppenbildung

Der nächste Schritt besteht darin, den Netzplan um die Informationen zu bereinigen, die für die nachfolgenden Aufgaben nicht erforderlich sind, um dadurch Übersichtlichkeit zu gewinnen. Hierzu sollten jeweils gleichartige Komponenten zu einer Gruppe zusammengefasst werden, die im Netzplan durch ein einzelnes Objekt dargestellt wird.

Wenn es nur wenige Grundkonfigurationen gibt, hat eine konsequente Gruppenbildung zudem den Vorteil, dass die Administration wesentlich vereinfacht wird. 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 IT-Sicherheit zugute, sondern spart auch Kosten.

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

- vom gleichen Typ sind,
- gleich oder nahezu gleich konfiguriert sind,
- gleich oder nahezu gleich in das Netz eingebunden sind (z. B. am gleichen Switch),
- den gleichen administrativen und infrastrukturellen Rahmenbedingungen unterliegen und
- die gleichen Anwendungen bedienen,
- den gleichen Schutzbedarf aufweisen.

Aufgrund der genannten Voraussetzungen für die Gruppenbildung kann bezüglich IT-Sicherheit davon ausgegangen werden, dass eine Stichprobe aus einer Gruppe den IT-Sicherheitszustand der Gruppe repräsentiert.

Wichtigstes Beispiel für die Gruppierung von Komponenten im Netzplan ist sicherlich die Zusammenfassung von Clients. In der Regel gibt es in einem Unternehmen bzw. in einer Behörde eine große

Anzahl von Clients, die sich jedoch gemäß obigem Schema in eine überschaubare Anzahl von Gruppen aufteilen lassen. In großen IT-Verbünden, wo aus Gründen der Redundanz oder des Durchsatzes viele Server die gleiche Aufgabe wahrnehmen, können durchaus auch Server zu Gruppen zusammengefasst werden.

Nach erfolgreicher Gruppierung werden die zusammengefassten Komponenten im Netzplan durch ein Objekt dargestellt. Dabei sind Typ und Anzahl der Komponenten zu vermerken, die durch die Gruppe repräsentiert werden.

Aktionspunkte:

- Gleichartige Komponenten zu Gruppen zusammenfassen
- Bereinigten Netzplan erstellen, in dem jede Gruppe durch ein einzelnes Objekt dargestellt ist
- Typ und Anzahl der jeweils zusammengefassten Komponenten vermerken

4.2 Schutzbedarfsfeststellung

Die Schutzbedarfsfeststellung der erfassten IT-Struktur gliedert sich in vier Schritte. Nach der Definition der Schutzbedarfskategorien wird anhand von typischen Schadensszenarien zunächst der Schutzbedarf der Geschäftsprozesse und den diese unterstützenden IT-Anwendungen bestimmt. Anschließend wird daraus der Schutzbedarf der einzelnen IT-Systeme abgeleitet. Aus diesen Ergebnissen wiederum wird abschließend der Schutzbedarf der Übertragungsstrecken und der Räume, die für die IT zur Verfügung stehen, abgeleitet.

4.2.1 Schutzbedarfsfeststellung für IT-Anwendungen

Ziel der Schutzbedarfsfeststellung ist es, ausgehend von den Geschäftsprozessen für jede erfasste IT-Anwendung einschließlich ihrer Daten zu entscheiden, welchen Schutzbedarf sie bezüglich Vertraulichkeit, Integrität und Verfügbarkeit besitzt. Dieser Schutzbedarf orientiert sich an den möglichen Schäden, die mit einer Beeinträchtigung der betroffenen IT-Anwendung und damit der jeweiligen Geschäftsprozesse verbunden sind.

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 IT-Anwendungen die adäquate Schutzbedarfskategorie ermittelt werden kann.

Schritt 1: Definition der Schutzbedarfskategorien

Die Schäden, die bei dem Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit für einen Geschäftsprozess bzw. eine IT-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 Schadenskategorien zu. So kann beispielsweise der Ausfall einer IT-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	- Eine Beeinträchtigung des informationellen Selbstbestimmungsrechts würde durch den Einzelnen als tolerabel eingeschätzt werden. - Ein möglicher Missbrauch personenbezogener Daten hat nur geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.
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	- Eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich. - Ein möglicher Missbrauch personenbezogener Daten hat erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.
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	- Eine besonders bedeutende Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich. - Ein möglicher Missbrauch personenbezogener Daten würde für den Betroffenen den gesellschaftlichen oder wirtschaftlichen Ruin bedeuten.
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, evtl. sogar existenzgefährdender Art, ist denkbar.
6. Finanzielle Auswirkungen	- Der finanzielle Schaden ist für die Institution existenzbedrohend.

Individualisierung der Zuordnungstabelle

Da nicht ausgeschlossen werden kann, dass bei individuellen Betrachtungen 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 Grenze zwischen "normal", "hoch" oder "sehr hoch" zu ziehen ist.

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 am IT-Budget orientiert.

Ähnliche Überlegungen können bezüglich der Verfügbarkeitsanforderungen angestellt werden. So kann beispielsweise ein Ausfall von 24 Stunden Dauer 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.

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 IT-Sicherheitsmaßnahmen und damit Folgekosten abhängen.

Schritt 2: Betrachtung von Schadensszenarien

Ausgehend von der Möglichkeit, dass Vertraulichkeit, Integrität oder Verfügbarkeit einer IT-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 IT-Anwendung. Dabei ist es unbedingt erforderlich, die Verantwortlichen und die Benutzer der betrachteten IT-Anwendung 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.

Um die Ermittlung der möglichen Schäden zu vereinfachen, werden nachfolgend zu den genannten Schadensszenarien Fragestellungen vorgestellt, die die möglichen Auswirkungen hinterfragen. Diese Anregungen erheben nicht den Anspruch auf Vollständigkeit, sie dienen lediglich zur Orientierung. In jedem Fall müssen die individuelle Aufgabenstellung und die Situation der Institution berücksichtigt, und diese Fragen entsprechend ergänzt werden.

In der weiteren Vorgehensweise bietet es sich an, für die erfassten IT-Anwendungen die folgenden Schadensszenarien einschließlich der Fragestellungen durchzuarbeiten. Anschließend sollte anhand der oben definierten Tabellen die Festlegung des Schutzbedarfs bezüglich Vertraulichkeit, Integrität und Verfügbarkeit durch die Zuordnung zu einer Schutzbedarfskategorie vorgenommen 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:

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 IT-Anwendung Verstöße gegen Vorschriften oder sogar Gesetze die Folge? Wenn ja, in welchem Maße?

Schreiben Gesetze die dauernde Verfügbarkeit bestimmter Informationen vor?

Gibt es Termine, die bei Einsatz der IT-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 IT-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 IT-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 eines IT-Systems oder einer IT-Anwendung 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 IT-Anwendungen und -Systeme sind:

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

Fragen:

Verlust der Vertraulichkeit

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

Verlust der Integrität

Können durch manipulierte Programmabläufe oder Daten Menschen gesundheitlich gefährdet werden?

Verlust der Verfügbarkeit

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

Schadensszenario "Beeinträchtigung der Aufgabenerfüllung"

Gerade der Verlust der Verfügbarkeit einer IT-Anwendung oder der Integrität der Daten kann die Aufgabenerfüllung in einem Unternehmen oder in einer Behörde 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 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 dergestalt 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 IT-Anwendung zu Fehlern in anderen IT-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 IT-Anwendung die Aufgabenerfüllung der Institution so stark beeinträchtigt werden, dass die Wartezeiten für die Betroffenen nicht mehr tolerabel sind?

Sind von dem Ausfall dieser IT-Anwendung andere IT-Anwendungen betroffen?

Ist es für die Institution bedeutsam, dass der Zugriff auf IT-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 IT-Anwendung können verschiedenartige negative Innen- oder Außenwirkungen entstehen, zum Beispiel:

- Ansehensverlust einer Behörde bzw. eines Unternehmens,
- Vertrauensverlust gegenüber einer Behörde bzw. einem Unternehmen,
- Demoralisierung der Mitarbeiter,
- Beeinträchtigung der wirtschaftlichen Beziehungen zusammenarbeitender Unternehmen,
- verlorenes Vertrauen in die Arbeitsqualität einer Behörde bzw. eines Unternehmens und
- Einbuße der Konkurrenzfähigkeit.

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

Ursachen für diese 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 IT-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 IT-Anwendung die Informationsdienstleistungen für Externe ein?

Verhindert der Ausfall von IT-Anwendungen die Erreichung von Geschäftszielen?

Ab wann wird der Ausfall der IT-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 einer IT-Anwendung 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,
- 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 IT-Anwendung Daten, aus deren Kenntnis ein Dritter (z. B. Konkurrenzunternehmen) finanzielle Vorteile ziehen kann?

Werden mit der IT-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 IT-Anwendung die Produktion, die Lagerhaltung oder der Vertrieb beeinträchtigt?

Ergeben sich durch den Ausfall der IT-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 IT-Anwendung zu mangelnder Zahlungsfähigkeit oder zu Konventionalstrafen kommen?

Wieviele wichtige Kunden wären durch den Ausfall der IT-Anwendung betroffen?

Schritt 3: Dokumentation der Ergebnisse

Es bietet sich an, den oben ermittelten Schutzbedarf der einzelnen IT-Anwendungen in einer Tabelle zu dokumentieren. Diese zentrale Dokumentation bietet den Vorteil, dass bei der nachfolgenden Schutzbedarfsfeststellung für IT-Systeme darauf referenziert werden kann.

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 nachzuvollziehen und weiterzuverwenden.

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

In der nachfolgenden Tabelle werden die wesentlichen IT-Anwendungen, deren Schutzbedarf und die entsprechenden Begründungen erfasst.

IT-Anwendung			Schutzbedarfsfeststellung		
Nr.	Bezeichnung	pers. Daten	Grund-wert	Schutz-bedarf	Begründung
A1	Personaldaten-verarbeitung	X	Vertrau-lichkeit	hoch	Personaldaten sind besonders schutz-bedürftige 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.
			Verfüg-barkeit	normal	Ausfälle bis zu einer Woche können mittels manueller Verfahren überbrückt werden.
A2	Beihilfeabwicklung	X	Vertrau-lichkeit	hoch	Beihilfedaten sind besonders schutzbe-dürftige personenbezogene Daten, die z. T. 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.
			Verfüg-barkeit	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 IT-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 IT-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 IT-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 IT-Anwendungen agieren kann. So kann es sein, dass ein Verantwortlicher für eine IT-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 dokumentiert werden.

Aktionspunkte:

- Schutzbedarfskategorien "normal", "hoch" und "sehr hoch" definieren beziehungsweise an die eigene Institution anpassen
- Schutzbedarf der erfassten IT-Anwendungen anhand von Schadensszenarien und Fragenkatalogen ermitteln
- Schutzbedarf der IT-Anwendungen und deren Begründungen tabellarisch dokumentieren

4.2.2 Schutzbedarfsfeststellung für IT-Systeme

Um den Schutzbedarf eines IT-Systems festzustellen, müssen zunächst die IT-Anwendungen betrachtet werden, die in direktem Zusammenhang mit dem IT-System stehen. Eine Übersicht, welche IT-Anwendungen relevant sind, wurde im Schritt "Erfassung der IT-Anwendungen und der zugehörigen Informationen" ermittelt.

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

Werden mehrere IT-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 IT-Anwendungen einer Institution. Der Schaden bei Ausfall einer dieser IT-Anwendungen wurde als gering eingeschätzt, da genügend Ausweichmöglichkeiten vorhanden sind. Fällt jedoch der Server (und damit alle IT-Anwendungen) aus, so ist der dadurch entstehende Schaden deutlich höher zu bewerten. Die Aufgabenerfüllung innerhalb der notwendigen Zeitspanne kann unter Umständen nicht mehr gewährleistet werden. Daher ist auch der Schutzbedarf dieser "zentralen" Komponenten entsprechend höher zu bewerten.

Auch der umgekehrte Effekt kann eintreten. So ist es möglich, dass eine IT-Anwendung einen hohen Schutzbedarf besitzt, ihn aber deshalb nicht auf ein betrachtetes IT-System überträgt, weil auf diesem IT-System nur unwesentliche Teilbereiche der IT-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 Gegensatz zum Datenbank-Server nur einen geringen 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-Systems bezüglich Vertraulichkeit, Integrität und Verfügbarkeit hat. Der Gesamt-Schutzbedarf eines IT-System 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 der Grundwerte den Schutzbedarf "hoch" hat. Es ist im Allgemeinen aber sinnvoll, den Schutzbedarf eines IT-Systems für alle drei Grundwerte 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. Es sind also keine zusätzlichen Sicherheitsmaßnahmen für den Schutz von Integrität oder Verfügbarkeit erforderlich.

Besonderer Wert ist auf die Begründung der Einschätzungen zu legen, damit diese auch für Außenstehende nachvollziehbar sind. Hier kann auf die Schutzbedarfsfeststellung der IT-Anwendung zurückverwiesen werden.

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

Eine solche Tabelle könnte beispielsweise wie folgt aussehen:

IT-System		Schutzbedarfsfeststellung		
Nr	Beschreibung	Grundwert	Schutz bedarf	Begründung
S1	Server für Personalverwaltung	Vertraulichkeit	hoch	Maximumprinzip
		Integrität	normal	Maximumprinzip
		Verfügbarkeit	normal	Maximumprinzip
S2	Primärer 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 Backup Domänen-Controller in Berlin ist für die Mitarbeiter des Bonner Standortes ebenfalls möglich. Ein Ausfall des Primären Domänen-Controllers kann bis zu 72 Stunden hingenommen werden. Der Schutzbedarf ist aufgrund dieses Verteilungseffekts daher "normal".

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

Hilfsmittel:

Für die Durchführung der Schutzbedarfsfeststellung wurden als Hilfsmittel Formblätter entwickelt, die sich unter den Hilfsmitteln zum IT-Grundschutz befinden.

Aktionspunkte:

- Schutzbedarf der IT-Systeme anhand des Schutzbedarfs der IT-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

4.2.3 Schutzbedarfsfeststellung für Kommunikationsverbindungen

Nachdem im vorhergehenden Abschnitt die Schutzbedarfsfeststellung für die betrachteten IT-Systeme abgeschlossen wurde, soll nun der Schutzbedarf bezüglich der Vernetzungsstruktur erarbeitet werden. Grundlage für die weiteren Überlegungen ist wiederum der in Kapitel 2.1 erarbeitete Netzplan des zu untersuchenden IT-Verbunds.

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 nach den IT-Systemen die Kommunikationsverbindungen betrachtet 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 WLAN-Anbindungen 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. Darüber hinaus kann auch ein Innentäter über eine solche Verbindung vertrauliche Informationen nach außen übertragen.
- 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 IT-Verbundes beeinträchtigen.
- Kommunikationsverbindungen, über die bestimmte hochschutzbedürftige Informationen nicht übertragen werden dürfen. Hierbei kommen insbesondere vertrauliche Informationen in Betracht. Falls 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 weiterübertragen 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.
- Sinnvollerweise können die dabei erfassten Daten tabellarisch dokumentiert oder graphisch im Netzplan hervorgehoben werden.

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

Für das fiktive Beispiel BOV ergeben sich folgende kritischen Verbindungen:

In der graphischen Darstellung sind die kritischen Verbindungen durch "fette" Linien markiert. Die Zahlen 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

Besonderer Wert sollte bei dieser Erhebung darauf gelegt werden, dass die erstellte Übersicht vollständig ist. Nur **eine** übersehene kritische Verbindung kann die Gesamtsicherheit unterlaufen. So sollten zum Beispiel alle eingesetzten Modems erfasst sein, da von ihnen potentiell kritische Verbindungen nach außen ausgehen können. Oftmals jedoch werden diese Modem-Außenverbindungen als Prestige-Objekte betrachtet, deren Existenz geleugnet wird, um sich einen persönlichen Vorteil zu verschaffen. Oder Modems werden als Verbrauchsmaterial beschafft und eingestuft, ohne dass IT-Verantwortliche über deren Einsatzzweck informiert sind. Im Sinne einer vollständigen IT-Sicherheit dürfen derlei kritische Geräte und Verbindungen jedoch nicht übergangen werden.

Aktionspunkte:

- 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

4.2.4 Schutzbedarfsfeststellung für Räume

Aus den Ergebnissen der Schutzbedarfsfeststellung 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 beherbergten Datenträger nach dem Maximum-Prinzip ab. Dabei sollte zusätzlich ein möglicher Kumulationseffekt berücksichtigt werden, wenn sich in einem Raum eine größere Anzahl von IT-Systemen befindet, wie typischerweise bei Serverräumen. Zusätzlich sollte eine Begründung der Schutzbedarfseinschätzung 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

Ein Auszug aus dem Ergebnis für das BOV ist folgende Tabelle:

Raum			IT / Informationen	Schutzbedarf		
Bezeich-nung	Art	Lokation	IT-Systeme / Daten-träger	Vertrau-lichkeit	Integri-tät	Verfüg-barkeit
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 Faxge-räten	normal	normal	normal

Aktionspunkte:

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

4.2.5 Interpretation der Ergebnisse der Schutzbedarfsfeststellung

Die bei der Schutzbedarfsfeststellung erzielten Ergebnisse bieten einen Anhaltspunkt für die weitere Vorgehensweise der IT-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.

Wird der Schutzbedarf für ein IT-System als "normal" definiert, so reicht es aus, die Standardmaßnahmen nach IT-Grundschutz pauschal umzusetzen. Für IT-Systeme, Netzverbindungen und Räume mit IT-Nutzung mit "hohem" und besonders mit "sehr hohem" Schutzbedarf sollte eine ergänzende Sicherheitsanalyse eingeplant werden. Ebenso sollte bei diesen Komponenten im Soll-Ist-Vergleich der hohe Schutzbedarf bei der Bearbeitung von als "zusätzlich" gekennzeichneten Maßnahmen berücksichtigt werden. So kann beispielsweise die Maßnahme M 1.10 *Verwendung von Sicherheitstüren* in einem Serverraum mit normalem Schutzbedarf nicht notwendig, bei hohem Schutzbedarf an Vertraulichkeit aber dringend erforderlich sein.

Bereiche mit unterschiedlichem Schutzbedarf

Bei der Schutzbedarfsfeststellung zeigt sich teilweise, dass es Bereiche innerhalb des betrachteten IT-Verbunds gibt, in denen Informationen verarbeitet werden, die einen hohen oder sehr hohen Schutzbedarf haben. Ein höherer Schutzbedarf in einem Bereich überträgt sich nach Maximumprinzip auf andere Bereiche. Auch wenn daher 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 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, dass LAN in mehrere Teilnetze aufzuteilen (siehe auch M 5.77 *Bildung von Teilnetzen*).
- 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.

Wenn Bereiche mit gleichartigen Sicherheitsanforderungen bereits in der Planungsphase geeignet umstrukturiert werden, erspart dies in allen folgenden Phasen bis hin zur Revision viel Arbeit.

Aktionspunkte:

- Prüfen, ob Objekte mit erhöhten Sicherheitsanforderungen in Sicherheitszonen konzentriert werden können
- Objekte mit erhöhten Sicherheitsanforderungen für eine ergänzende Sicherheitsanalyse vormerken

4.3 Auswahl der Maßnahmen: Modellierung nach IT-Grundschutz

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

4.3.1 Die IT-Grundschutz-Kataloge

Bausteine

Die IT-Grundschutz-Kataloge umfassen 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 IT-Umgebungen 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 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 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, bietet der IT-Grundschutz 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 Kapitel gruppiert:

B 1: Übergeordnete Aspekte der IT-Sicherheit

B 2: Sicherheit der Infrastruktur

B 3: Sicherheit der IT-Systeme

B 4: Sicherheit im Netz

B 5: Sicherheit in 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 IT-Sicherheitsmaßnahmen ausführlich. Die Maßnahmen sind in sechs Maßnahmenkataloge gruppiert:

M 1: Infrastruktur

M 2: Organisation

M 3: Personal

M 4: Hard- und Software

M 5: Kommunikation

M 6: Notfallvorsorge

4.3.2 Modellierung eines IT-Verbunds

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

- Das IT-Grundschutzmodell eines bereits realisierten IT-Verbunds 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-Grundschutzmodell eines geplanten IT-Verbunds stellt hingegen ein **Entwicklungskonzept** dar. Es beschreibt über die ausgewählten Bausteine, welche Standard-Sicherheitsmaßnahmen bei der Realisierung des IT-Verbunds umgesetzt werden müssen.

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

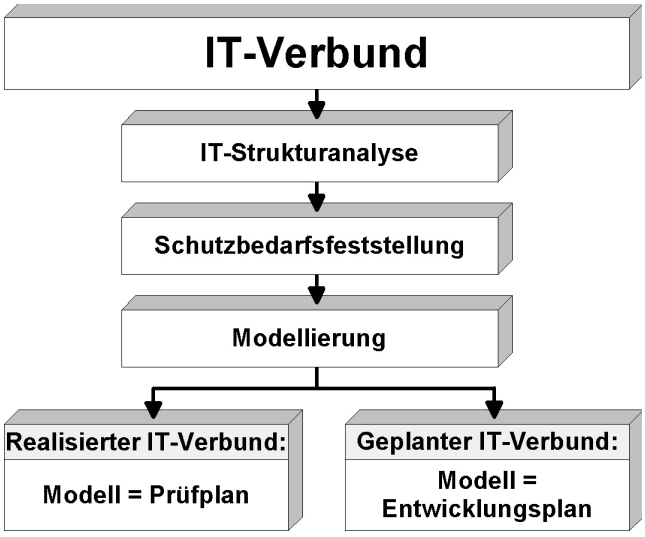


Abbildung: Ergebnis der Modellierung nach IT-Grundschutz

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

Für die Abbildung eines im Allgemeinen komplexen IT-Verbunds auf die Bausteine des IT-Grundschutzes bietet es sich an, die IT-Sicherheitsaspekte gruppiert nach bestimmten Themen zu betrachten.

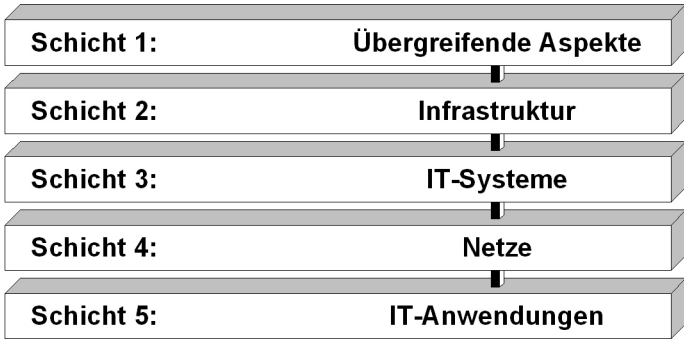


Abbildung: Schichten des IT-Grundschutzmodells

Die IT-Sicherheitsaspekte eines IT-Verbunds werden wie folgt den einzelnen Schichten zugeordnet:

- Schicht 1 umfasst die übergreifenden IT-Sicherheitsaspekte, die für sämtliche oder große Teile des IT-Verbunds gleichermaßen gelten. Dies betrifft insbesondere übergreifende Konzepte und die daraus abgeleiteten Regelungen. Typische Bausteine der Schicht 1 sind unter anderem IT-Sicherheitsmanagement, Organisation, Datensicherungskonzept und Computer-Virenschutzkonzept.
- Schicht 2 befasst sich mit den baulich-technischen Gegebenheiten, in der Aspekte der infrastrukturellen Sicherheit zusammengeführt werden. Dies betrifft insbesondere die Bausteine Gebäude, Serverraum, Schutzschrank und häuslicher Arbeitsplatz.
- Schicht 3 betrifft die einzelnen IT-Systeme des IT-Verbunds, die ggf. in Gruppen zusammengefasst wurden. Hier werden die IT-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 2000.
- Schicht 4 betrachtet die Vernetzungsaspekte der IT-Systeme, die sich nicht auf bestimmte IT-Systeme, sondern auf die Netzverbindungen und die Kommunikation beziehen. Dazu gehören zum Beispiel die Bausteine Heterogene Netze, Modem sowie Remote Access.
- Schicht 5 schließlich beschäftigt sich mit den eigentlichen IT-Anwendungen, die im IT-Verbund 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 IT-Sicherheit 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. Schicht 1 betrifft Grundsatzfragen des IT-Einsatzes, 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 IT-Anwendungsverantwortlichen und -betreiber.

- Aufgrund der Aufteilung der Sicherheitsaspekte in Schichten können Einzelaspekte in resultierenden IT-Sicherheitskonzepten leichter aktualisiert und erweitert werden, ohne dass andere Schichten umfangreich tangiert werden.

Die Modellierung nach IT-Grundschutz besteht nun daraus, für die Bausteine einer jeden Schicht zu entscheiden, ob und wie sie zur Abbildung des IT-Verbunds 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-Grundschutzmodell, 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 8

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

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

Eine detaillierte Beschreibung der Vorgehensweise zur Modellierung eines IT-Verbunds findet sich in den IT-Grundschutz-Katalogen im Kapitel "Schichtenmodell und Modellierung". Die IT-Grundschutz-Kataloge [GSHB] können in der jeweils aktuellen Fassung vom BSI-Webserver heruntergeladen werden. Dabei wird besonderer Wert auf die Randbedingungen gelegt, wann ein einzelner Baustein sinnvollerweise eingesetzt werden soll und auf welche Zielobjekte er anzuwenden ist.

Aktionspunkte:

- Kapitel "Schichtenmodell und Modellierung" aus den IT-Grundschutz-Katalogen systematisch durcharbeiten
- Für jeden Baustein der IT-Grundschutz-Kataloge ermitteln, auf welche Zielobjekte im betrachteten IT-Verbund er 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

4.4 Basis-Sicherheitscheck

Für die nachfolgenden Betrachtungen wird vorausgesetzt, dass für einen ausgewählten IT-Verbund folgende Teile des IT-Sicherheitskonzepts nach IT-Grundschutz erstellt wurden: Anhand der IT-Strukturanalyse des IT-Verbundes wurde eine Übersicht über die vorhandene IT, deren Einsatzorte und die unterstützten IT-Anwendungen erstellt. Darauf aufbauend wurde anschließend die Schutzbedarfsfeststellung durchgeführt, deren Ergebnis eine Übersicht über den Schutzbedarf der IT-Anwendungen, der IT-Systeme, der IT-genutzten Räume und der Kommunikationsverbindungen ist. Mit Hilfe dieser Informationen wurde die Modellierung des IT-Verbundes nach IT-Grundschutz durchgeführt. Das Ergebnis war eine Abbildung des betrachteten IT-Verbundes auf Bausteine des IT-Grundschutzes.

Diese 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 zentralen Aufgabe zur Erstellung eines IT-Sicherheitskonzepts nach IT-Grundschutz, der Durchführung des Basis-Sicherheitschecks, vorgegangen werden sollte. Dieser 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 diese Schritte des Basis-Sicherheitschecks detailliert beschrieben.

4.4.1 Organisatorische Vorarbeiten

Für die reibungslose Durchführung des Soll-Ist-Vergleichs sind einige Vorarbeiten erforderlich. Zunächst sollten alle hausinternen Papiere, z. B. Organisationsverfügungen, Arbeitshinweise, Sicherheitsanweisungen, Manuals und "informelle" Vorgehensweisen, die die IT-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 ggf. 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 des IT-Betriebes in Outsourcing 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 IT-Verbunds herangezogen wurde, ein Hauptansprechpartner festgelegt werden.

- Bei den Bausteinen der Schicht 1 "Übergeordnete 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 Verkabelung 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 Unternehmen und Behörden.
- 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 "IT-Anwendungen" sollten die Betreuer bzw. die Verantwortlichen der einzelnen IT-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:

- 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

4.4.2 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, da den entsprechenden Gefährdungen mit anderen adäquaten Maßnahmen entgegengewirkt wird (z. B. durch Maßnahmen, die nicht im IT-Grundschutz aufgeführt sind, aber dieselbe Wirkung erzielen), oder die Maßnahmenempfehlungen nicht relevant sind (z. B. weil Dienste nicht aktiviert wurden).
"ja"	-	Alle Empfehlungen in der Maßnahme sind vollständig und wirksam 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 auf das 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 mitgeteilt werden, wie das Ergebnis ausgefallen ist (Umsetzungsstatus der Maßnahme: entbehrlich/ja/teilweise/nein), und diese Entscheidung erläutert werden.

Aktionspunkte:

- 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

4.4.3 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 BSI-Tool zum IT-Grundschutz (GSTOOL). Dieses unterstützt die gesamte Vorgehensweise nach IT-Grundschutz, beginnend bei der Stammdatenerfassung, über die Schutzbedarfsfeststellung, den Soll-Ist-Vergleich (Basis-Sicherheitscheck) sowie die Umsetzung der Maßnahmen bis hin zur anschließenden Sicherheitsrevision. 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 des IT-Grundschutzes 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. Es wird später in der Realisierungsplanung mit dem Namen des dann als verantwortlich Bestimmten gefüllt.

- 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 sind 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:

- 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

4.5 Integration der ergänzenden Sicherheitsanalyse in die IT-Grundschutz-Vorgehensweise

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

Dazu ist für alle Zielobjekte des IT-Verbundes, die

- einen hohen oder sehr hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit haben oder
- 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,

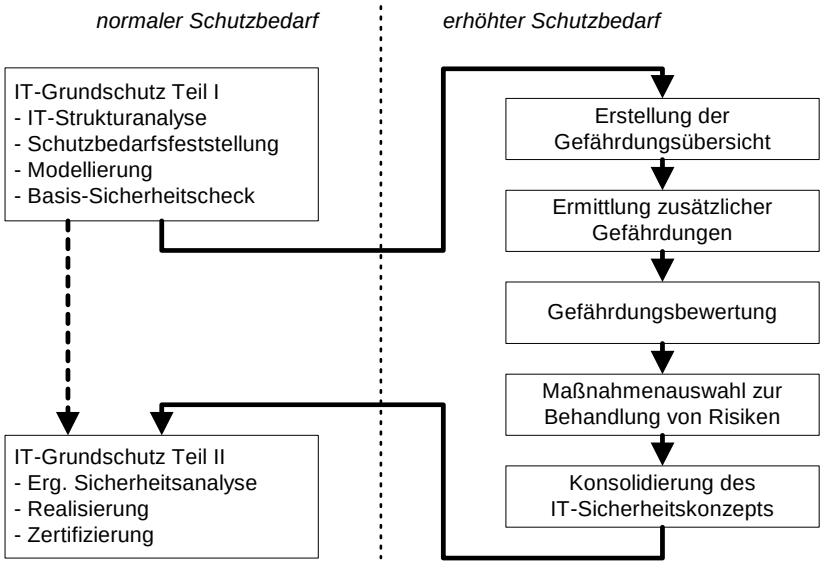
zu entscheiden, ob weitere Risikobetrachtungen erforderlich sind. Beispiele für Anwendungen oder IT-Systeme, für die eine ergänzende Sicherheitsanalyse empfehlenswert ist, sind das Online-Banking-Angebot eines Finanzdienstleisters und IT-Systeme mit speziellen Echtzeitbetriebssystemen.

In einem Management-Report ist für jedes Zielobjekt, das 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.

Der Management Report wird der Institutionsleitung kommuniziert und muss von ihr verabschiedet werden. Das Management übernimmt somit die Verantwortung.

Das BSI empfiehlt an dieser Stelle die Anwendung einer *Risikoanalyse auf der Basis von IT-Grundschutz*. Diese Vorgehensweise ist auf dem Webserver des BSI sowie auf der CD-ROM des BSI als PDF-Datei veröffentlicht.

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



Im Vordergrund steht die Frage: Welchen Gefährdungen für den IT-Verbund 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 dem IT-Grundschutz 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 Zielobjekte und für jede Gefährdung wird geprüft, ob die bislang vorgesehenen IT-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 IT-Sicherheitsmanagement 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 IT-Verbundes).
  - Risiken können verlagert werden (z. B. durch Outsourcing oder Versicherungen).
  - Risiken können akzeptiert werden.

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

- Konsolidierung des IT-Sicherheitskonzepts

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

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

Eine ausführliche Darstellung der Methodik findet sich im Originaldokument.

Wichtig: Die *Risikoanalyse auf der Basis von IT-Grundschutz* ist eine Vorgehensweise, um bei Bedarf IT-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 IT-Sicherheitsprobleme zu beseitigen, ist es manchmal zweckmäßig, *zuerst* IT-Grundschutz vollständig umzusetzen und erst *danach* eine ergänzende Sicherheitsanalyse 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 IT-Verbund bereits realisiert und in Betrieb ist und
2. die vorliegenden Zielobjekte mit den existierenden Bausteinen des IT-Grundschutzes hinreichend modelliert werden können.

Für geplante IT-Verbünde 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.
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 IT-Verbunds 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 unbefugten Zutritt sowie auf die ordnungsgemäße Strom- und Klimaversorgung.

Aktionspunkte:

- Festlegen, für welche Zielobjekte eine Risikoanalyse durchzuführen ist, und Begründung dokumentieren
- Entscheidung herbeiführen, ob die Risikoanalysen vor oder nach der Umsetzung der IT-Grundschutz-Maßnahmen durchgeführt werden
- BSI-Dokument "Risikoanalyse auf der Basis von IT-Grundschutz" systematisch durcharbeiten oder für später vormerken
- Ergebnisse der Risikoanalysen in das IT-Sicherheitskonzept integrieren

4.6 Realisierung von IT-Sicherheitsmaßnahmen

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

Bevor mit der Realisierung von IT-Sicherheitsmaßnahmen begonnen werden kann, muss für das untersuchte IT-System oder den untersuchten IT-Verbund die IT-Strukturanalyse, die Schutzbedarfsfeststellung und die Modellierung erfolgt sein. Ebenso müssen die Ergebnisse des Basis-Sicherheitschecks, also des daran anschließenden Soll-Ist-Vergleichs, vorliegen. Sollte für ausgewählte Bereiche aufgrund eines höheren Schutzbedarfs eine ergänzende Sicherheitsanalyse durchgeführt worden sein, so sollten die dabei erarbeiteten Maßnahmenvorschläge ebenfalls vorliegen und nachfolgend berücksichtigt werden.

Ist eine Vielzahl von Maßnahmen zu realisieren und stehen ggf. für die Realisierung nur beschränkte Ressourcen an Geld und Personal zur Verfügung, so kann die Realisierung der IT-Sicherheitsmaßnahmen, wie in den nachfolgenden Schritten beschrieben, vollzogen werden. Ein Beispiel zur Erläuterung der Vorgehensweise findet sich am Ende dieses Kapitels.

Sind nur wenige fehlende Maßnahmen identifiziert worden, deren Umsetzung wenig finanzielle oder personelle Ressourcen bindet, kann oft ad hoc entschieden werden, wer diese Maßnahmen bis wann umzusetzen hat. Dies kann einfach und unkompliziert in den Erfassungstabellen des Soll-Ist-Vergleichs dokumentiert werden. In diesem Fall können die nachfolgenden Schritte 1, 3 und 4 entfallen.

Schritt 1: Sichtung der Untersuchungsergebnisse

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

Durch ergänzende Sicherheitsanalysen 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.

Schritt 2: Konsolidierung der Maßnahmen

In diesem Schritt werden zunächst die noch umzusetzenden IT-Sicherheitsmaßnahmen konsolidiert. Falls zusätzliche Sicherheitsanalysen durchgeführt wurden, können hierdurch IT-Sicherheitsmaßnahmen hinzugekommen sein, die Maßnahmen aus den IT-Grundschutz-Katalogen ergänzen oder

auch ersetzen. Hierbei wird geprüft, für welche IT-Grundschutzmaßnahmen die Realisierung entfallen kann, da zu realisierende höherwertige IT-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 IT-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-Grundschutzmaßnahmen durch adäquate andere IT-Sicherheitsmaßnahmen zu ersetzen.

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

Beispiele:

- In einer ergänzenden Sicherheitsanalyse wurde festgestellt, dass zusätzlich zu den IT-Grundschutzmaßnahmen auch eine chipkartengestützte Authentisierung und lokale Verschlüsselung der Festplatten an NT-Clients der Personaldatenverarbeitung notwendig sind. Diese zusätzliche Maßnahme würde die Maßnahme M 4.48 *Passwortschutz unter Windows NT* 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.

Schritt 3: Kosten- und Aufwandsschätzung

Da das Budget zur Umsetzung von IT-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. Personalaufwänden 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, dass 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, wieviel Ressourcen für die Umsetzung der IT-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 IT-Sicherheitsmaßnahmen) zur Sensibilisierung vorgestellt werden. Darüber hinaus bietet es sich an, die für die Realisierung der fehlenden Maßnahmen entstehenden Kosten und Aufwände 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 Maßnahmen-Gefährdungs-Tabellen aus den Hilfsmitteln zum IT-Grundschutz hinzugezogen werden, um zu ermitteln, welche

Gefährdungen nicht mehr 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.

Schritt 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, in wie weit sie für die IT-Grundschutz-Qualifizierung erforderlich ist. Die Qualifizierungsstufe (A-Einstieg, B-Aufbau, C-Zertifikat, Z-Zusätzlich) einer Maßnahme gibt häufig Hinweise auf den Stellenwert, den die jeweilige Maßnahme im IT-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 (z. B. durch Umsetzung des Bausteins B 3.102 Server unter Unix) und dann erst die angeschlossenen Clients.
- Bausteine mit auffallend vielen fehlenden 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 dies ebenfalls dokumentiert werden, um in späteren Streitfällen die Beachtung der erforderlichen Sorgfaltspflicht belegen zu können.

Schritt 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,
- Budgetrahmen,
- Verantwortliche für die Umsetzung und
- Verantwortliche für die Überwachung der Realisierung.

Schritt 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 von neuen IT-Sicherheitsmaßnahmen betroffenen Mitarbeiter über die Notwendigkeit und die Konsequenzen der Maßnahmen zu unterrichten und sie für die Belange der IT-Sicherheit zu sensibilisieren.

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

Nach der Realisierung und Einführung der neuen IT-Sicherheitsmaßnahmen sollte durch den IT-Sicherheitsbeauftragten geprüft werden, ob die notwendige Akzeptanz 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.

Beispiel:

Um die obigen Schritte näher zu beschreiben, wird nachfolgend ein fiktives Beispiel auszugsweise beschrieben. Zunächst soll die Tabelle der konsolidierten, zu realisierenden Maßnahmen einschließlich der Kostenschätzungen, die als Ergebnis der Schritte 1 - 3 entsteht, dargestellt werden:

Zielobjekt	Baustein	Maßnahme	Priorität			Kosten	Bemerkung
			1	2	3		
Gesamte Organisation	B 1.9	M 2.11 Regelung des Passwortgebrauchs	T			a) 0,- Euro b) 2 AT c) 0.-Euro/Jahr d) 0 AT/Jahr	
Serverraum R 3.10	B 2.4	M 1.24 Vermeidung von wasserführenden Leitungen			F	a) 20000.- Euro b) 12 AT c) 0.- Euro/Jahr d) 0 AT/Jahr	Diese Maßnahme ist nicht wirtschaftlich umsetzbar. Ersatzweise wird Maßnahme Z 1 umgesetzt.
Serverraum R 3.10	B 2.4	Z 1 Installation von Wasser ableitenden Blechen mit Überwachung mittels eines Wassermelders und Aufschaltung auf den Pförtner				a) 4000.- Euro b) 3 AT c) 0.- Euro/Jahr d) 0 AT/Jahr	Ersetzt Maßnahme M 1.24
Server S4	B 3.10 1	M 1.28 Lokale unterbrechungsfreie Stromversorgung	F			a) 1000.- Euro b) 1 AT c) 0.-Euro/Jahr d) 0 AT/Jahr	
Gruppe Clients C1	B 3.20 7	Z 2 chipkartengestützte Authentisierung und lokale Verschlüsselung der Festplatten				a) 1400.- Euro b) 2 AT c) 0.- Euro/Jahr d) 2 AT/Jahr	Diese zusätzliche Maßnahme ersetzt die Maßnahme M 4.1 in Baustein B 1.9.
...							

Legende:

- Maßnahme

Z 1 = Zusatzmaßnahme 1 (zusätzlich zu IT-Grundschutzmaßnahmen)

- Prioritäten

T = teilweise erfüllt, F = fehlt, ist nicht realisiert

- Kosten:

a) = einmalige Investitionskosten

b) = einmaliger Personalaufwand (AT = Arbeitstage)

c) = wiederkehrende Investitionskosten

d) = wiederkehrender Personalaufwand (AT = Arbeitstage)

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

Realisierungsplan (Stand 01.09.2004)						
Zielobjekt	Baustein	Maßnahme	Umsetzung bis	Verantwortlich	Budgetrahmen	Bemerkung
Gesamte Organisation	B 1.9	M 2.11 Regelung des Passwortgebrauchs	31.12.04	a) Herr Müller b) Frau Meier	a) 0,- Euro b) 2 AT c) 0.-Euro/Jahr d) 0 AT/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	30.04.05	a) Herr Schmitz b) Herr Hofmann	a) 1000.- Euro b) 1 AT c) 0.- Euro/Jahr d) 0 AT/Jahr	Installation der Bleche lediglich unter frisch- und abwasserführenden Leitungen
Server S4	B 3.101	M 1.28 Lokale unterbrechungsfreie Stromversorgung	31.10.04	a) Herr Schulz b) Frau Meier	a) 500.- Euro b) 1 AT c) 0.-Euro/Jahr d) 0 AT/Jahr	
Gruppe Clients C1	B 3.207	Z 2 chipkartengestützte Authentisierung und lokale Verschlüsselung der Festplatten	31.12.04	a) Herr Schulz b) Frau Meier	a) 1400.- Euro b) 2 AT c) 0.- Euro/Jahr d) 2 AT/Jahr	
...						

Legende:

- Verantwortlich:

a) = Verantwortlich für die Umsetzung der Maßnahme

b) = Verantwortlich für die Kontrolle der Umsetzung

- Budgetrahmen: Für die Realisierung der Maßnahme stehen zur Verfügung

a) = einmalige Investitionskosten

b) = einmaliger Personalaufwand (AT = Arbeitstage)

c) = wiederkehrende Investitionskosten

d) = wiederkehrender Personalaufwand (AT = Arbeitstage)

Aktionspunkte:

- Fehlende oder nur teilweise umgesetzte IT-Grundschutz-Maßnahmen oder ergänzende Sicherheitsmaßnahmen in einer Tabelle zusammenfassen
- IT-Sicherheitsmaßnahmen konsolidieren, das heißt, überflüssige Maßnahmen streichen, allgemeine Maßnahmen an die Gegebenheiten anpassen und alle Maßnahmen auf Eignung prüfen
- Einmalige und wiederkehrende Kosten und Aufwände 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 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
- Prüfen, ob die IT-Sicherheitsmaßnahmen akzeptiert werden und gegebenenfalls nachbessern

5 Aufrechterhaltung der IT-Sicherheit und kontinuierliche Verbesserung

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

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

- Detektion, Dokumentation und Auswertung von IT-Sicherheitsvorfällen
- Durchführung von Übungen und Tests zur Simulation von Sicherheitsvorfällen und Dokumentation der Ergebnisse
- interne und externe Audits
- Zertifizierung nach festgelegten IT-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 IT-Verbunds abhängt, sind die Anforderungen auch für kleine Behörden und Unternehmen 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 IT-Sicherheitskonzept besprochen werden, kann unter Umständen in kleinen Institutionen schon ausreichend sein.

Aktionspunkte:

- Messung der Zielerreichung in die IT-Sicherheitsstrategie integrieren
- Realisierung der beschlossenen Maßnahmen überprüfen
- Wirksamkeit und Effizienz der beschlossenen Maßnahmen überprüfen

5.1 Überprüfung des IT-Sicherheitsprozesses in allen Ebenen

Die Überprüfung des IT-Sicherheitsprozesses ist unabdingbar, damit einerseits Fehler und Schwachstellen erkannt und abgestellt werden können und andererseits der IT-Sicherheitsprozess in Bezug auf seiner 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.

Umsetzung des Realisierungsplans

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 IT-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 IT-Sicherheitsprozesses dient nicht nur zur Kontrolle der Aktivitäten im Rahmen des IT-Sicherheitskonzeptes, sondern auch zur rechtzeitigen Wahrnehmung von Planungsfehlern und zur Anpassung der IT-Sicherheitsstrategie, wenn sich diese als unrealistisch erweist.

Eignung der IT-Sicherheitsstrategie

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

Aktualität von Sicherheitszielen, Rahmenbedingungen und Sicherheitskonzeption

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

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

Wirtschaftlichkeitsbetrachtung

Ein anderer Punkt, der unter konstanter Beobachtung bleiben sollte, ist Wirtschaftlichkeit der IT-Sicherheitsstrategie und von spezifischen IT-Sicherheitsmaßnahmen. Die Kosten für die IT-Sicherheit ist 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 IT-Sicherheitsmaßnahmen eingesetzt werden können. Ebenso ist es wichtig, regelmäßig den Nutzen der vorhandenen IT-Sicherheitsmaßnahmen herauszuarbeiten.

Übernahme der Ergebnisse in den IT-Sicherheitsprozess

Die Ergebnisse der Erfolgskontrolle sind für die Verbesserung des IT-Sicherheitsprozesses notwendig. Es kann sich dabei herausstellen, dass die IT-Sicherheitsziele, die IT-Sicherheitsstrategie oder das IT-Sicherheitskonzept geändert und die IT-Sicherheitsorganisation den Erfordernissen angepasst werden sollten. Unter Umständen ist es sinnvoll, grundlegende Änderungen an der IT-Umgebung vorzunehmen oder Geschäftsprozesse zu verändern, z. B. wenn IT-Sicherheitsziele nicht oder nur umständlich (und damit teuer) 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 notwendigen Kompetenz und Unabhängigkeit gewährleisten können. Vollständigkeits- und Plausibilitätskontrollen sollten nicht durch die Ersteller der Konzepte durchgeführt werden. Prüfergebnisse und Berichte sind im Allgemeinen als kritisch und hochvertraulich zu betrachten und müssen daher besonders gut geschützt werden.

Aktionspunkte:

- Rollenkonflikt zwischen Ersteller und Prüfer beachten und Vertraulichkeit der Untersuchungsergebnisse sicherstellen
- Einhaltung des Realisierungsplans prüfen
- 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 IT-Sicherheitsprozess einfließen lassen

5.2 Informationsfluss im IT-Sicherheitsprozess

Berichte an die Leitungsebene

Damit die Geschäfts- bzw. Behördenleitung die richtigen Entscheidungen bei der Steuerung und Lenkung des IT-Sicherheitsprozesses treffen kann, benötigt sie die dafür notwendigen Informationen. Diese sollten in Managementreporten aufbereitet werden, die unter Anderem folgende Punkte abdecken sollten:

- Ergebnisse von Audits
- Berichte über IT-Sicherheitsvorfälle
- Berichte über bisherige Erfolge und Probleme beim IT-Sicherheitsprozess

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

Dokumentation

Aus zahlreichen Gründen ist die Dokumentation des IT-Sicherheitsprozesses auf allen Ebenen entscheidend für dessen Erfolg. Dazu gehören unter Anderem, dass nur durch ausreichende Dokumentation:

- getroffene Entscheidungen nachvollziehbar werden,
- Prozesse wiederholbar sind und standardisiert werden können,
- Schwächen- und Fehler erkannt werden können, so dass sie in Zukunft vermieden werden können.

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 das Detailniveau technischer Dokumentationen ein Streitthema. Ein pragmatischer Ansatz für die Erstellung von verwendbaren Dokumentationen ist es, dass andere Personen mit vergleichbarer Expertise in diesem Bereich sie nachvollziehen können müssen und dass der Administrator zwar auf sein Wissen, aber nicht auf sein Gedächtnis angewiesen sein muss, um die Systeme und Anwendungen wieder herzustellen. Bei Sicherheitsübungen und Sicherheitsvorfällen sollte die Qualität der vorhandenen Dokumentationen bewertet werden und die gewonnenen Erkenntnisse zur Verbesserung genutzt werden. Zu solcher Art von Dokumentationen gehören:

  - Installations- und Konfigurationsanleitungen
  - Anleitungen für den Wiederanlauf nach einem Sicherheitsvorfall
  - Dokumentation von Test- und Freigabeverfahren
  - Anweisungen für das Verhalten bei Störungen und IT-Sicherheitsvorfällen

- Anleitungen für IT-Benutzer (Zielgruppe: IT-Benutzer)

IT-Sicherheitsmaßnahmen müssen für die IT-Benutzer verständlich dokumentiert werden. Darüber hinaus müssen die Mitarbeiter über die Existenz und Bedeutung dieser Richtlinien informiert sein und sie müssen entsprechend geschult sein, so dass sie diese problemlos einhalten können. Diese Gruppe von Dokumentationen umfasst:

  - Arbeitsabläufe und organisatorische Vorgaben
  - technische IT-Sicherheitsmaßnahmen
  - Verhalten bei IT-Sicherheitsvorfällen
- Aufzeichnung von Managemententscheidungen (Zielgruppe: Leitungsebene)

IT-Sicherheitsstrategie, Richtlinien und weitere grundlegende Entscheidungen zum IT-Sicherheitsprozess müssen aufgezeichnet werden, damit diese jederzeit nachvollziehbar und wiederholbar sind.

Informationsfluss und Meldewege

Für die Aufrechterhaltung des IT-Sicherheitsprozesses ist die zeitnahe Aktualisierung der Meldewege und der Vorgehensweise 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.

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 IT-Sicherheitsaspekte 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 IT-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 IT-Anwendung ist ebenfalls nicht nur für das IT-Sicherheitsmanagement sinnvoll. Er ermöglicht z. B. auch die exakte Zuordnung von IT-Kosten, die oftmals als Gemeinkosten umgelegt werden, auf einzelne Geschäftsprozesse oder Produkte.

Aktionspunkte:

- Leitungsebene über die Ergebnisse von Überprüfungen und den Status des IT-Sicherheitsprozesses informieren
- Gegebenenfalls Entscheidungen über erforderliche Korrekturmaßnahmen einholen
- Alle Teilaspekte des gesamten IT-Sicherheitsprozesses 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 IT-Sicherheitsprozess betreffen, auf dem aktuellen Stand halten
- Synergien zwischen dem IT-Sicherheitsprozess und anderen Managementprozessen ausfindig machen

5.3 IT-Grundschutz-Zertifizierung

Um die erfolgreiche Umsetzung von IT-Grundschutz-Maßnahmen nach außen transparent machen zu können, hat das BSI ein Zertifizierungsschema nach IT-Grundschutz entwickelt. Das IT-Grundschutz-Zertifikat oder auch ein IT-Grundschutz-Testat bietet Unternehmen und Behörden die Möglichkeit, ihre Bemühungen um IT-Sicherheit 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 einem IT-Grundschutz-Zertifikat vielfältig:

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

Da der IT-Grundschutz mit seinen Empfehlungen von Standard-Sicherheitsmaßnahmen inzwischen einen Quasi-Standard für IT-Sicherheit darstellt, bietet es sich an, dies als allgemein anerkanntes Kriterienwerk für IT-Sicherheit zu verwenden.

Kosten und Aufwand für den Erwerb eines IT-Grundschutz-Zertifikats sind (vergleichsweise) gering. Unter Umständen kann es allerdings für ein Unternehmen oder eine Behörde recht aufwändig sein, die Maßnahmenempfehlungen der IT-Grundschutz-Kataloge vollständig umzusetzen. Um auch diesen Organisationen eine Möglichkeit zu geben, ihr Bemühen um IT-Sicherheit nach außen hin zu verdeutlichen, gibt es **zwei Vorstufen** des IT-Grundschutz-Zertifikats:

- Das Auditor-Testat "Einstiegsstufe" kann nach Umsetzung der unabdingbaren Standard-Sicherheitsmaßnahmen des IT-Grundschutzes erteilt werden (Umsetzung aller Maßnahmen der Stufe A),
- Das Auditor-Testat "Aufbaustufe" kann nach Umsetzung der wichtigsten Standard-Sicherheitsmaßnahmen erteilt werden (Umsetzung aller Maßnahmen der Stufe A und B).

Für beide Qualifizierungsstufen ist eine Prüfung durch einen externen Auditor erforderlich. Nach der Erstellung eines Auditreports auf der Grundlage der Audit-Verfahrensbeschreibung (im Dokument "Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz - Prüfschema für ISO 27001 Audits"), in dem die Prüfung der Umsetzung aller für die Qualifizierungsstufe erforderlichen Maßnahmen dokumentiert wird, kann ein Testat durch einen lizenzierten Auditor abgegeben werden. Die Zertifizierungsstelle prüft die Auditreporte von Testaten nicht, kann sie sich aber für Rückfragen vorlegen lassen. Die Testate sind zwei Jahre gültig und können, da sie Vorstufen zum Zertifikat sind, nicht verlängert werden. Eine Re-Qualifizierung ist nur auf eine höhere Stufe möglich.

Grundlage für die Vergabe eines IT-Grundschutz-Zertifikats ist ebenfalls die Durchführung eines Audits durch einen externen, beim BSI lizenzierten Auditor. Das Ergebnis des Audits ist ein Auditreport, der der Zertifizierungsstelle vorgelegt wird, die über die Vergabe des IT-Grundschutz-Zertifikats 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 in ihrer jeweils aktuellen Fassung bzw. der unmittelbar vorhergehenden Versionen. Die Audit-Verfahrensbeschreibung beschreibt die Vorgehensweise zur Prüfung des Auditreports und zur Vergabe des IT-Grundschutz-Zertifikats.

Um als IT-Grundschutz-Auditor lizenziert zu werden, müssen Auditoren zunächst ihre fachliche Kompetenz belegen. Dazu müssen die Kenntnisse bzgl. IT-Grundschutz und Qualifizierungsschema fundiert dargelegt werden. Notwendig ist der Nachweis von mindestens zweijähriger Berufserfahrung im Umfeld IT-Sicherheit und der Bearbeitung von mindestens drei Projekten mit Bezug zum IT-Grundschutz. Darüber hinaus müssen die angehenden Auditoren an einer Schulung zum Qualifizierungsschema teilnehmen. Im Anschluss an diese Schulung wird das BSI eine Prüfung der erworbenen Kenntnisse durchführen und bei Erfolg die Lizenz vergeben. Eine Lizenz ist für einen Zeitraum von 5 Jahren gültig. Alle lizenzierten Auditoren sind vom BSI unter www.bsi.bund.de/gshb/zert veröffentlicht.

Über ein IT-Grundschutz-Zertifikat wird zunächst nachgewiesen, dass im betrachteten Verbund IT-Grundschutz erfolgreich umgesetzt worden ist. Darüber hinaus zeigt ein IT-Grundschutz-Zertifikat auch, dass in der jeweiligen Institution

- IT-Sicherheit ein anerkannter Wert ist,
- ein funktionierendes IT-Sicherheitsmanagement vorhanden ist und außerdem
- zu einem bestimmten Zeitpunkt ein definiertes IT-Sicherheitsniveau erreicht wurde.

Weitere Informationen zur Zertifizierung und zur Lizenzierung als IT-Grundschutz-Auditor finden sich unter www.bsi.bund.de/gshb/zert/schema.htm

Aktionspunkte:

- Informationen des BSI zum Qualifizierungs- und Zertifizierungsschema für IT-Grundschutz lesen
- Prüfen, ob die Bemühungen um IT-Sicherheit anhand eines IT-Grundschutz-Zertifikats oder Auditor-Testats transparent gemacht werden sollen
- Gegebenenfalls prüfen, ob das IT-Sicherheitsmanagement und der IT-Sicherheitszustand die entsprechenden Voraussetzungen erfüllen
- Gegebenenfalls den Qualifizierungs- beziehungsweise Zertifizierungsprozess initiieren