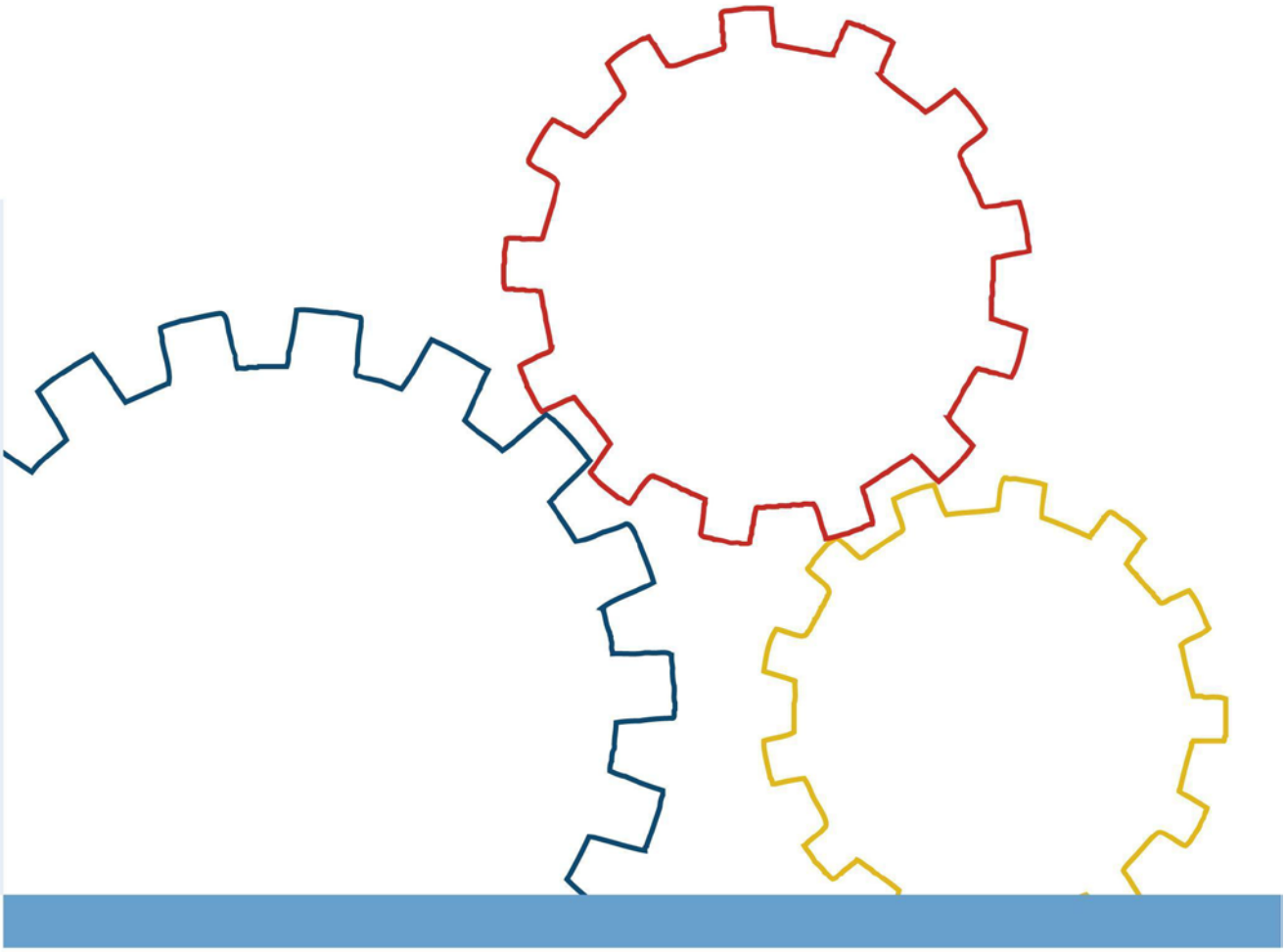
Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Standard 200-2

IT-Grundschutz-Methodik



www.bsi.bund.de/grundschutz

Version 1.0

BSI-Standard 200-2

IT-Grundschutz-Methodik

Version 1.0, Oktober 2017

Inhaltsverzeichnis

1 Einleitung

1.1 Versionshistorie

Der BSI-Standard 200-2 löst den BSI-Standard 100-2 ab.

Stand	Version	Änderungen
März 2017	CD 1.0	Neukonzeption basierend auf BSI-Standard 100-2 • Im Rahmen der Modernisierung des IT-Grundschutzes wurden neben der Standard-Absicherung die Vorgehensweisen zur Basis-Absicherung und Kern-Absicherung eingefügt • Erweiterung um Virtualisierung, Cloud-, ICS- und IoT-Absicherung • Klarstellung der Rollen und Aufgaben von IT-SiBe und ISB • Anpassungen an Fortschreibung der ISO-Standards • Informationsklassifizierung stärker herausgearbeitet • Informationsfluss im Informationssicherheitsprozess überarbeitet, Angleichung mit 100-4 • Beispiel BoV durch RECPLAST ausgetauscht
Oktober 2017	Version 1.0	Einarbeitung von Anwender-Kommentaren • im Wesentlichen sprachliche Präzisierungen • Änderung des Begriffs "Aktiva" in "Assets"

1.2 Zielsetzung

Mit dem BSI-Standard 200-2 stellt das BSI eine Methodik für ein effektives Management von Informationssicherheit zur Verfügung. Diese kann an die Anforderungen von Institutionen verschiedenster Art und Größe angepasst werden. Im BSI-Standard 200-2 wird dies über die drei Vorgehensweisen "Standard-Absicherung", "Basis-Absicherung" und "Kern-Absicherung" realisiert.

Die Methodik baut auf dem BSI-Standard 200-1 *Managementsysteme für die Informationssicherheit (ISMS)* (siehe [BSI1]) und damit auch auf ISO 27001 [27001] auf. In diesem Dokument wird aufgezeigt, wie der im BSI-Standard 200-1 vorgestellte grundlegende Rahmen für ein Informationssicherheitsmanagementsystem durch IT-Grundschutz konkretisiert wird. Ein Managementsystem für die Informationssicherheit (ISMS) ist das geplante und organisierte Vorgehen, um ein angemessenes Sicherheitsniveau für die Informationssicherheit zu erzielen und aufrechtzuerhalten.

Der IT-Grundschutz ist ein etablierter Standard zum Aufbau und zur Aufrechterhaltung eines angemessenen Schutzes aller Informationen einer Institution. Die vom BSI kontinuierlich weiterentwickelte Methodik bietet sowohl Anleitungen für den Aufbau eines ISMS, als auch eine umfassende Basis für die Risikoanalyse, die Überprüfung des vorhandenen Sicherheitsniveaus und die Implementierung eines angemessenen Grades an Informationssicherheit.

Eines der wichtigsten Ziele des IT-Grundschutzes ist es, den Aufwand im Informationssicherheits-prozess zu reduzieren. Dazu werden bekannte Ansätze und Methoden zur Verbesserung der Informationssicherheit gebündelt und kontinuierlich aktualisiert. Ergänzend veröffentlicht das BSI im IT-Grundschutz-Kompendium Bausteine mit konkreten Sicherheitsanforderungen für typische Geschäftsprozesse, Anwendungen, Systeme, Kommunikationsverbindungen und Räume, die nach Bedarf in der eigenen Institution eingesetzt werden können. Im IT-Grundschutz werden alle Bereiche

einer Institution betrachtet, dazu gehören Produktion und Fertigung mit Industrial Control Systems (ICS) ebenso wie Komponenten aus dem Bereich Internet of Things (IoT).

Durch die Umsetzung von organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsanforderungen wird mit der Vorgehensweise "Standard-Absicherung" ein Sicherheitsniveau für die betrachteten Geschäftsprozesse erreicht, das für den normalen Schutzbedarf angemessen und ausreichend ist, um geschäftsrelevante Informationen zu schützen. Bei der Umsetzung der Vorgehensweise "Basis-Absicherung" wird ein Sicherheitsniveau erreicht, das zwar deutlich unter dem der Standard-Absicherung liegt, aber eine gute Grundlage für ISMS-Einsteiger bietet. Mit der Vorgehensweise "Kern-Absicherung" können besonders schützenswerte Informationen und Geschäftsprozesse vorrangig abgesichert werden.

Die IT-Grundschutz-Methodik wird regelmäßig erweitert und an die aktuellen Entwicklungen angepasst, die sich durch neue Prozesse, Normen und Regularien, vor allem aber durch die stetig fortschreitende Digitalisierung ergeben. Aufgrund des engen Erfahrungsaustauschs mit den Anwendern des IT-Grundschutzes fließen stetig neue Anforderungen und Aspekte in die Veröffentlichungen ein. Die Anwender können daher mit aktuellen Empfehlungen an einem ISMS für ihre Institution arbeiten und typische Sicherheitsprobleme schnell identifizieren und beheben.

1.3 Adressatenkreis

Der BSI-Standard 200-2 richtet sich primär an Sicherheitsverantwortliche, -beauftragte, -experten, -berater und alle Interessierte, die mit dem Management von Informationssicherheit betraut sind. Er ist zugleich eine sinnvolle Grundlage für IT- und ICS-Verantwortliche, Führungskräfte und Projektmanager, die dafür Sorge tragen, dass Aspekte der Informationssicherheit in ihrer Institution bzw. in ihren Projekten ausreichend berücksichtigt werden.

Der IT-Grundschutz bietet Institutionen jeder Größe und Sparte eine kosteneffektive und zielführende Methode zum Aufbau und zur Umsetzung der für sie angemessenen Informationssicherheit. Der Begriff "Institution" wird im folgenden Text 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 werden und an die Rahmenbedingungen angepasst werden sollten.

Im IT-Grundschutz wird vorausgesetzt, dass die Informations- und Kommunikationstechnik ebenso wie vorhandene industrielle Steuerungs- und Automatisierungstechnik von Fachpersonal administriert wird, dass es also einen IT-Betrieb mit klar definierten Rollen gibt. Dieser kann von einem einzelnen Administrator bis hin zu einer oder mehreren IT-Abteilungen reichen. Davon ausgehend sind die verschiedenen Aktivitäten im Sicherheitsprozess beschrieben.

1.4 Anwendungsweise

Im BSI-Standard 200-1 *Managementsysteme für Informationssicherheit (ISMS)* wird beschrieben, mit welchen Methoden Informationssicherheit in einer Institution generell initiiert und gesteuert werden kann. Der vorliegende BSI-Standard 200-2 bietet konkrete Hilfestellungen, wie ein Managementsystem für die Informationssicherheit Schritt für Schritt eingeführt werden kann: Im Fokus stehen einzelne Phasen dieses Prozesses sowie bewährte Best-Practice-Lösungen.

Die IT-Grundschutz-Methodik bietet ein umfangreiches Gerüst für ein ISMS und muss auf die individuellen Rahmenbedingungen einer Institution angepasst werden, damit ein geeignetes Managementsystem für die Informationssicherheit aufgebaut werden kann. Für einen kontinuierlichen und effektiven Prozess für Informationssicherheit müssen eine ganze Reihe von Aktionen durchgeführt werden. Hierfür bieten die IT-Grundschutz-Methodik und das IT-Grundschutz-Kompendium Hinweise und praktische Umsetzungshilfen.

Des Weiteren bietet dieser Standard die Möglichkeit einer Zertifizierung. Damit kann eine Institution nicht nur die Umsetzung von IT-Grundschutz, sondern auch die Qualität des eigenen ISMS mit Hilfe

eines ISO 27001 Zertifikates auf Basis von IT-Grundschutz nachweisen. Das Zertifikat dient zugleich anderen Institutionen als Kriterium, um sich über den Reifegrad eines ISMS einer anderen Institution informieren zu können.

Eine Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz kann auch als Sicherheitsanforderung für mögliche Kooperationspartner verwendet werden, um das erforderliche Niveau an Informationssicherheit bei der anderen Institution zu definieren.

Auch wenn als Grundlage für das ISMS eine andere Methodik angewendet wird, ist es trotzdem möglich, von IT-Grundschutz zu profitieren. So bietet der IT-Grundschutz auch Lösungsansätze für einzelne Aufgabenstellungen, beispielsweise für die Erstellung von Konzepten oder die Durchführung von Revisionen und Zertifizierungen im Bereich Informationssicherheit. Je nach Anwendungsbereich bilden bereits einzelne Bausteine, Umsetzungshinweise oder weitere Hilfsmittel, die der IT-Grundschutz zur Verfügung stellt, hilfreiche Grundlagen für die Arbeit des Sicherheitsmanagements.

1.5 Aufbau des BSI-Standards 200-2

Kapitel 2 enthält die wichtigsten Schritte für die Einführung eines ISMS sowie der Erstellung einer Sicherheitskonzeption.

In Kapitel 3 wird beschrieben, wie die grundlegende Phase der Initiierung des Informationssicherheitsprozesses aussehen kann und welche Hintergrundinformationen erforderlich sind, um eine fundierte Entscheidung über die für die Institution geeignete Vorgehensweise zur Absicherung ihrer Informationen und Geschäftsprozesse zu treffen. Als wesentliche Grundlage für die weiteren Aktivitäten ist eine Leitlinie zur Informationssicherheit zu erstellen.

Für den Sicherheitsprozess müssen geeignete Organisationsstrukturen aufgebaut und ein funktionierendes Sicherheitsmanagement muss eingerichtet werden, siehe Kapitel 4.

Im Rahmen eines funktionierenden Sicherheitsprozesses müssen diverse Dokumentationen erstellt werden. Was hierbei zu beachten ist, ist in Kapitel 5 beschrieben.

In Kapitel 6 wird aufgezeigt, wie vorzugehen ist, wenn als Vorgehensweise die Basis-Absicherung ausgewählt wurde. Die Basis-Absicherung verfolgt das Ziel, als Einstieg in den IT-Grundschutz zunächst eine breite, grundlegende Erst-Absicherung über alle Geschäftsprozesse bzw. Fachverfahren einer Institution zu erzielen. Nach der Festlegung des Geltungsbereichs muss eine Auswahl und Zuordnung der IT-Grundschutz-Bausteine erfolgen und die Reihenfolge ihrer Anwendung festgelegt werden. Mit einem IT-Grundschutz-Check wird geprüft, inwieweit die Basis-Anforderungen bereits umgesetzt sind. Anschließend müssen konkrete Maßnahmen zur Erfüllung der offenen Anforderungen abgeleitet und umgesetzt werden. Durch die Auswahl einer der nachfolgenden Vorgehensweisen sollte das so erreichte Sicherheitsniveau aufrechterhalten und verbessert werden.

Wie ein vorgezogener Schutz der essentiellen Assets nach IT-Grundschutz mit der Kern-Absicherung erzielt werden kann, wird in Kapitel 7 aufgezeigt. Die Vorgehensweise orientiert sich dabei stark an den Schritten der Vorgehensweise zur Standard-Absicherung, die im Folgenden beschrieben wird.

Kapitel 8 beschreibt die Vorgehensweise zur Standard-Absicherung. Dabei wird aufgezeigt, wie zunächst die Grundinformationen über einen Informationsverbund erhoben werden und diese durch Gruppenbildung reduziert werden können. Anschließend muss ausgehend von den Geschäftsprozessen der Schutzbedarf für Anwendungen, IT-Systeme, Kommunikationsverbindungen und Räume festgestellt werden. Aus den Empfehlungen des IT-Grundschutz-Kompendiums müssen ferner die für den jeweiligen Informationsverbund passenden Bausteine und Anforderungen ausgewählt, also die Modellierung nach IT-Grundschutz durchgeführt werden. Aus den ausgewählten Anforderungen müssen Sicherheitsmaßnahmen abgeleitet werden. Vor der Realisierung von Sicherheitsmaßnahmen müssen vorhandene und zusätzliche Sicherheitsmaßnahmen, die beispielsweise durch die Risikoanalyse auf der Basis von IT-Grundschutz gemäß BSI-Standard 200-3 (siehe [BSI3]) ermittelt wurden, in das Sicherheitskonzept integriert werden.

Wie die Umsetzung der identifizierten und konsolidierten Sicherheitsmaßnahmen durchgeführt werden sollte, wird anschließend in Kapitel 9 beschrieben.

Die wesentliche Aufgabe eines ISMS ist es, die Aufrechterhaltung der Informationssicherheit zu gewährleisten und diese fortlaufend zu verbessern. Dieses Thema wird im Kapitel 10 angegangen.

Die Vorgehensweisen nach IT-Grundschutz und das IT-Grundschutz-Kompendium werden nicht nur für die Sicherheitskonzeption, sondern auch als Referenz im Sinne eines Sicherheitsstandards verwendet. Durch eine Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz kann eine Institution nach innen und außen hin dokumentieren, dass sie sowohl ISO 27001 als auch IT-Grundschutz in der erforderlichen Tiefe umgesetzt hat. Kapitel 11 liefert einen kurzen Überblick, welche Schritte hierfür notwendig sind und welche Bedingungen für eine erfolgreiche Zertifizierung erfüllt werden müssen.

2 Informationssicherheitsmanagement mit IT-Grundschutz

Informationen sind ein wesentlicher Wert für Unternehmen und Behörden und müssen daher angemessen geschützt werden. Die meisten Informationen werden heutzutage mit Informationstechnik (IT) erstellt, gespeichert, transportiert oder weiterverarbeitet. Moderne Geschäftsprozesse sind heute in Wirtschaft und Verwaltung ohne IT-Unterstützung längst nicht mehr vorstellbar. In Produktion und Fertigung hat mit Industrial Control Systems (ICS) die Informations- und Kommunikationstechnik ebenso Einzug gehalten wie über Internet of Things (IoT) in fast jedem anderem Bereich.

Unzureichend geschützte Informationen stellen einen häufig unterschätzten Risikofaktor dar, der für eine Institution existenzbedrohend werden kann. Dabei ist ein vernünftiger Informationsschutz ebenso wie eine Grundsicherung der IT schon mit verhältnismäßig geringen Mitteln zu erreichen.

2.1 Ganzheitliches Konzept

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

Informationssicherheit ist nicht nur eine Frage der Technik, sondern hängt in erheblichem Maße von den organisatorischen und personellen Rahmenbedingungen ab. Der IT-Grundschutz trägt dem Rechnung, indem er über die auf dem Stand der Technik basierenden Bausteine sowohl technische als auch nicht-technische Sicherheitsanforderungen für typische Geschäftsbereiche, Anwendungen und Systeme beschreibt. Im Vordergrund stehen dabei praxisnahe und handlungsorientierte Sicherheitsanforderungen mit dem Ziel, die Einstiegshürde in den Sicherheitsprozess so niedrig wie möglich zu halten und hochkomplexe Vorgehensweisen zu vermeiden.

Unter dem Dach des IT-Grundschutzes werden mit der Basis-, der Standard- und der Kern-Absicherung verschiedene Vorgehensweisen angeboten, um den Institutionen je nach Art und Größe passende Instrumente zum Schutz ihrer Informationsverbünde in die Hand zu geben.

2.2 Managementsystem für die Informationssicherheit

Im BSI-Standard 200-2 wird dargestellt, wie ein effizientes Managementsystem für die Informationssicherheit aufgebaut und wie das IT-Grundschutz-Kompendium im Rahmen dieser Aufgabe verwendet werden kann. Die Vorgehensweisen nach IT-Grundschutz in Kombination mit dem IT-Grundschutz-Kompendium bieten eine systematische Methodik zur Erarbeitung von Sicherheitskonzepten und praxiserprobten Sicherheitsmaßnahmen, die in zahlreichen Behörden und Unternehmen erfolgreich eingesetzt werden.

Die Bausteine im IT-Grundschutz-Kompendium 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 Informations- und Kommunikationstechnik miteinander verknüpft. Dies geht einher mit einer steigenden Komplexität der technischen Systeme und mit einer hohen Abhängigkeit vom korrekten Funktionieren der Technik. Daher ist ein geplantes und organisiertes Vorgehen aller Beteiligten notwendig, um ein angemessenes und ausreichendes Sicherheitsniveau durchzusetzen und aufrechtzuerhalten. Eine Verankerung dieses Prozesses in allen Geschäftsbereichen kann nur gewährleistet werden, wenn dieser zur Aufgabe der obersten Leitungs-

bzw. Managementebene wird. Die oberste Managementebene ist verantwortlich für das zielgerichtete und ordnungsgemäße Funktionieren einer Institution und damit auch für die Gewährleistung der Informationssicherheit nach innen und außen. Daher muss diese den Sicherheitsprozess initiieren, steuern und kontrollieren. Dazu gehören strategische Leitaussagen zur Informationssicherheit, konzeptionelle Vorgaben und auch organisatorische Rahmenbedingungen sowie ausreichende Ressourcen, um Informationssicherheit innerhalb aller Geschäftsprozesse erreichen zu können.

2.3 Verantwortung für die Informationssicherheit

Die Verantwortung für Informationssicherheit verbleibt in jedem Fall bei der obersten Managementebene, die Aufgabe "Informationssicherheit" wird allerdings typischerweise an einen Beauftragten für Informationssicherheit delegiert. In den IT-Grundschutz-Dokumenten wurde bisher die Bezeichnung IT-Sicherheitsbeauftragter verwendet, da dieser Begriff in Unternehmen und Behörden lange Zeit der am weitesten verbreitete war. Die Bezeichnung Informationssicherheitsbeauftragter oder kurz IS-Beauftragter (ISB) ist allerdings treffender und ersetzt daher im IT-Grundschutz die alte Bezeichnung. Andere Varianten sind CISO (Chief Information Security Officer) oder Informationssicherheitsmanager (ISM).

Informationssicherheit umfasst den umfangreicheren Bereich des Schutzes von Informationen, zwar in und mit IT, aber auch ohne IT bzw. über IT hinaus. Somit ist IT-Sicherheit ein Teilbereich der Informationssicherheit und beschäftigt sich gezielt mit dem Schutz der eingesetzten IT. In großen Institutionen kann es weiterhin neben dem ISB auch einen dedizierten Beauftragten für IT-Sicherheit geben. Dieser ist dann typischerweise im IT-Bereich tätig, während der ISB unmittelbar der Leitungsebene zuarbeitet.

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

2.4 Elemente des IT-Grundschutz

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

Ergänzend zu den in diesem Standard beschriebenen Vorgehensweisen nach IT-Grundschutz werden im IT-Grundschutz-Kompendium Sicherheitsanforderungen nach dem Stand der Technik formuliert. IT-Grundschutz verfolgt dabei einen ganzheitlichen Ansatz. Durch die geeignete Umsetzung von organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsanforderungen wird mit der Standard-Absicherung ein Sicherheitsniveau erreicht, das für den normalen Schutzbedarf angemessen und ausreichend ist, um geschäftsrelevante Informationen zu schützen. Bei der Umsetzung der Basis-Absicherung wird ein Sicherheitsniveau erreicht, das zwar deutlich unter dem der Standard-Absicherung liegt, aber eine gute Grundlage für Einsteiger bietet. Mit der Kern-Absicherung können hochschutzbedürftige Informationen und Geschäftsprozesse vorrangig geschützt werden. Für typische Prozesse, Anwendungen und Komponenten in der Informations-, Kommunikations- und Fertigungstechnik finden sich in den Bausteinen des IT-Grundschutz-Kompendiums geeignete "Bündel" mit Sicherheitsanforderungen zur Basis-, Standard- und Kern-Absicherung.

Diese Bausteine sind entsprechend ihrem jeweiligen Fokus in prozess- und systemorientierte Bausteine aufgeteilt und nach zusammengehörigen Themen in ein Schichtenmodell einsortiert. Die prozessorientierten Bausteine finden sich in den folgenden Schichten:

- ISMS *(Managementsysteme für Informationssicherheit)*
- ORP *(Organisation und Personal)*
- CON *(Konzepte und Vorgehensweisen)*
- OPS *(Betrieb)*
- DER *(Detektion und Reaktion)*

Die systemorientierten Bausteine sind in die folgenden Schichten gruppiert:

- INF *(Infrastruktur)*
- NET *(Netze und Kommunikation)*
- SYS *(IT-Systeme)*
- APP *(Anwendungen)*
- IND *(Industrielle IT)*

Jeder Baustein enthält eine kurze Beschreibung der Thematik und des Ziels, das mit der Umsetzung des Bausteins erreicht werden soll, sowie eine Abgrenzung zu anderen Bausteinen, die einen thematischen Bezug haben. Weiterhin gibt es einen kurzen Überblick über die spezifischen Gefährdungen des betrachteten Themengebietes. Die konkreten Sicherheitsanforderungen für die Basis-, Standard- und Kern-Absicherung bilden den Hauptteil.

Zusätzlich kann es zu den Bausteinen des IT-Grundschutz-Kompendiums Umsetzungshinweise geben. Diese beschreiben, wie die Anforderungen der Bausteine in der Praxis erfüllt werden können, und enthalten dafür passende Sicherheitsmaßnahmen mit detaillierten Beschreibungen, die auf dem Erfahrungsschatz von BSI und IT-Grundschutz-Anwendern basieren.

2.5 Thematische Abgrenzung

Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl in IT-Systemen, aber auch auf Papier oder in Köpfen gespeichert sein. IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung. Das Aktionsfeld der klassischen IT-Sicherheit wird bei der Cyber-Sicherheit auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein. Der Begriff "Informationssicherheit" statt IT-Sicherheit oder Cyber-Sicherheit ist daher umfassender. IT-Grundschutz verfolgt seit langem einen ganzheitlichen Ansatz, mit dem auch geschäftsrelevante Informationen und Geschäftsprozesse geschützt werden, die nicht oder nur teilweise mit IT unterstützt werden. Da aber in der Literatur noch überwiegend der Begriff "IT-Sicherheit" zu finden ist, wird er auch in dieser sowie in anderen Publikationen des IT-Grundschutzes weiterhin verwendet, allerdings werden die Texte sukzessive stärker auf die Betrachtung von Informationssicherheit ausgerichtet.

Aufgabe der Informationssicherheit ist der angemessene Schutz der Grundwerte Vertraulichkeit, Integrität (Unverfälschtheit) und Verfügbarkeit von Informationen. Dazu gehört auch die Absicherung der Informationsverarbeitung, also insbesondere der IT. Darüber hinaus müssen auch die Systeme einbezogen werden, die häufig nicht unmittelbar als IT-Systeme wahrgenommen werden, wie beispielsweise ICS- und IoT-Systeme. Außerdem schließt dies auch die Authentizität und Nicht-Abstreitbarkeit als Spezialfälle der Integrität ein. Je nach Anwendungsfall kann es hilfreich sein, weitere Grundwerte in die Betrachtungen mit einzubeziehen. Im Bereich Datenschutz werden, im Rahmen des Standard-Datenschutzmodells (siehe [SDM]), weitere Schutzziele herangezogen, nämlich

Datenminimierung, Intervenierbarkeit (als technische Gestaltung von Verfahren zur Ausübung der Betroffenenrechte), Transparenz und Nichtverkettung (als Sicherung der Zweckbindung).

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

2.6 Übersicht über den Informationssicherheitsprozess

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

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

- Initiierung des Sicherheitsprozesses
  - Übernahme der Verantwortung durch die Leitungsebene
  - Konzeption und Planung des Sicherheitsprozesses
  - Bereitstellung von finanziellen, personellen und zeitlichen Ressourcen
  - Entscheidung für eine Vorgehensweise
- Erstellung der Leitlinie zur Informationssicherheit
- Aufbau einer geeigneten Organisationsstruktur für das Informationssicherheitsmanagement
- Erstellung einer Sicherheitskonzeption
- Umsetzung der Sicherheitskonzeption
- Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit
  - Fortentwicklung des ISMS
  - Erweiterung der gewählten Vorgehensweise

Die ganzheitliche Umsetzung von Informationssicherheit (Standard-Absicherung) 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 die dringend erforderlichen Sicherheitsvorkehrungen umzusetzen (Basis-Absicherung) oder in Bereichen mit höchsten Sicherheitsanforderungen schnell das erforderliche hohe Sicherheitsniveau zu erreichen (Kern-Absicherung). Von diesen Keimzellen ausgehend sollte dann kontinuierlich die Sicherheit in der Gesamtorganisation verbessert werden.

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

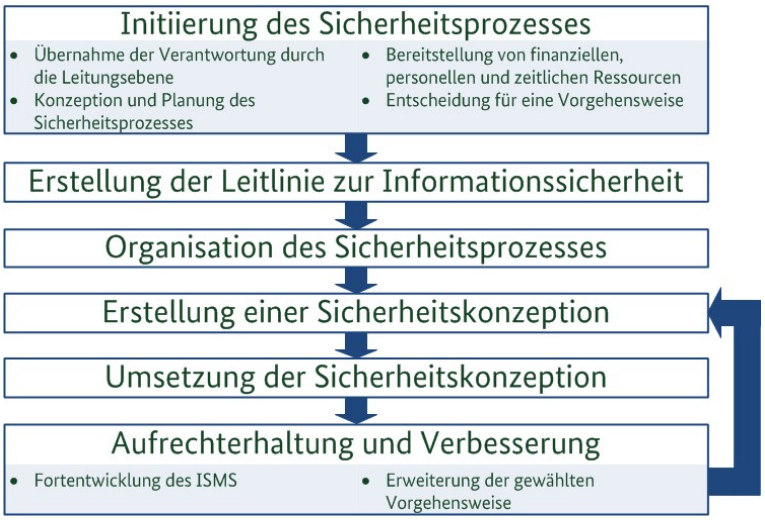


Abbildung 1: Phasen des Sicherheitsprozesses

Einige der Phasen können auch parallel durchgeführt werden, z. B. kann die Konzeption und Planung des Sicherheitsprozesses gleichzeitig zum Aufbau der Informationssicherheitsorganisation erfolgen. In diesem Fall müssen die vorgezogenen Phasen mit den neuen Ergebnissen zeitnah aktualisiert werden.

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

Initiierung des Sicherheitsprozesses

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

Erstellung der Leitlinie zur Informationssicherheit

Eine wesentliche Grundlage für die Ausgestaltung des Sicherheitsprozesses ist die Leitlinie zur Informationssicherheit. Sie beschreibt, welche Sicherheitsziele und welches Sicherheitsniveau die Institution anstrebt, was die Motivation hierfür ist und mit welchen Maßnahmen und mit welchen Strukturen dies erreicht werden soll. Alle Mitarbeiter sollten daher die Inhalte der Sicherheitsleitlinie kennen und nachvollziehen können. Was für die Leitlinie und andere Dokumente im Sicherheitsprozess zu beachten ist, wird in Kapitel 3.4 beschrieben.

Aufbau einer geeigneten Organisationsstruktur

Für das Informationssicherheitsmanagement muss eine für Größe und Art der Institution geeignete Organisationsstruktur aufgebaut werden, siehe Kapitel 4.

Erstellung einer Sicherheitskonzeption

Nachdem ein Informationssicherheitsprozess initiiert wurde und die Sicherheitsleitlinie und Informationssicherheitsorganisation definiert wurden, wird die Sicherheitskonzeption für die Institution erstellt. Als Grundlage hierfür finden sich in den Bausteinen des IT-Grundschutz-Kompendiums für typische Komponenten von Geschäftsprozessen, Anwendungen, IT-Systeme und weitere Objekte entsprechende Sicherheitsanforderungen nach dem Stand der Technik. Diese sind thematisch in Bausteine strukturiert, so dass sie modular aufeinander aufsetzen.

Abhängig davon, ob eine Basis-, Standard- oder Kern-Absicherung angestrebt ist, sehen die einzelnen Aktivitäten zur Erstellung einer Sicherheitskonzeption etwas anders aus, grundsätzlich basieren sie aber alle auf den Vorarbeiten, die mit der Erstellung des IT-Grundschutz-Kompendiums geleistet worden sind.

Bei Anwendung des IT-Grundschutzes wird ein Soll-Ist-Vergleich zwischen den Sicherheitsanforderungen aus den relevanten Bausteinen des IT-Grundschutz-Kompendiums und den in der Institution bereits realisierten Maßnahmen durchgeführt. Dabei festgestellte fehlende oder nur unzureichend erfüllte Anforderungen zeigen die Sicherheitsdefizite auf, die es durch die Umsetzung von aus den Anforderungen abgeleiteten Maßnahmen zu beheben gilt.

Nur bei einem signifikant höheren Schutzbedarf muss zusätzlich eine Risikoanalyse unter Beachtung von Kosten- und Wirksamkeitsaspekten durchgeführt werden. In der Regel reicht es hierbei aus, die Sicherheitsanforderungen des IT-Grundschutz-Kompendiums durch entsprechende individuelle, qualitativ höherwertige Maßnahmen zu ergänzen. Hierzu ist im BSI-Standard 200-3 *Risikoanalyse auf der Basis von IT-Grundschutz* (siehe [BSI3]) eine im Vergleich zu traditionellen Risikoanalyse-Methoden einfachere Vorgehensweise beschrieben.

Umsetzung von Sicherheitskonzepten

Ein ausreichendes Sicherheitsniveau lässt sich nur erreichen, wenn bestehende Defizite ermittelt, der Status quo in einem Sicherheitskonzept festgehalten, erforderliche Maßnahmen identifiziert und diese Maßnahmen insbesondere auch konsequent umgesetzt werden. In Kapitel 9 wird beschrieben, was bei der Umsetzungsplanung von Sicherheitsmaßnahmen beachtet werden muss.

Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit

Ziel des Sicherheitsmanagements ist es, das angestrebte Sicherheitsniveau zu erreichen und dieses auch dauerhaft aufrechtzuerhalten und zu verbessern. Daher müssen der Sicherheitsprozess und die Organisationsstrukturen für Informationssicherheit regelmäßig daraufhin überprüft werden, ob sie angemessen, wirksam und effizient sind. Ebenso ist zu überprüfen, ob die Maßnahmen des Sicherheitskonzepts noch zum Informationsverbund passen, ob sie praxisnah sind und ob sie korrekt umgesetzt wurden. In Kapitel 10 wird überblicksartig dargestellt, welche Aktionen für die Aufrechterhaltung und Verbesserung der Informationssicherheit ergriffen werden sollten. Dazu gehört auch, zu überlegen, ob die gewählte Vorgehensweise ergänzt oder erweitert werden soll, beispielsweise von Basis- auf Standard-Absicherung oder von Kern-Absicherung eines eingegrenzten Bereiches auf einen größeren Informationsverbund.

2.7 Anwendung des IT-Grundschutz-Kompendiums

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

Um die sehr heterogenen Ausgestaltungen von Institution der verschiedenen Branchen und Größenordnung sowie der von ihnen eingesetzten IT- oder ICS-Systeme einschließlich der Einsatzumgebung besser strukturieren und aufbereiten zu können, verfolgt der IT-Grundschutz das Baukastenprinzip. Die einzelnen Bausteine, die im IT-Grundschutz-Kompendium beschrieben werden, spiegeln typische Bereiche und Aspekte der Informationssicherheit in einer Institution wider, von übergeordneten Themen, wie dem IS-Management, der Notfallvorsorge oder der Datensicherungskonzeption bis hin zu speziellen Komponenten einer IT- oder ICS-Umgebung. Das IT-Grundschutz-Kompendium beschreibt die spezifische Gefährdungslage und die Sicherheitsanforderungen für verschiedene Komponenten, Vorgehensweisen und Systeme, die jeweils in einem Baustein zusammengefasst werden. Das BSI überarbeitet und aktualisiert zusammen mit vielen engagierten Anwendern regelmäßig die bestehenden Bausteine, um die Empfehlungen auf dem Stand der Technik zu halten. Darüber hinaus wird das bestehende Werk regelmäßig um weitere Bausteine ergänzt. Anwender können Bausteine vorschlagen oder erstellen. Unter Federführung des IT-Grundschutz-Teams des BSI werden diese dann zunächst als Community Draft aufbereitet, in die dann weitere Anregungen einfließen können, bevor sie ins IT-Grundschutz-Kompendium aufgenommen werden.

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 Systems inklusive Zielsetzung sowie einer Abgrenzung zu anderen Bausteinen mit thematischem Bezug. Im Anschluss daran wird die spezifische Gefährdungslage dargestellt.

Danach folgen die Sicherheitsanforderungen gegliedert nach Basis- und Standard-Anforderungen sowie Anforderungen bei erhöhtem Schutzbedarf. Die im IT-Grundschutz-Kompendium aufgeführten Basis- und Standard-Anforderungen stellen zusammengenommen den Stand der Technik dar. Diese müssen für die Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz erfüllt werden.

In den Anforderungen werden die in Versalien geschriebenen Modalverben "SOLLTE" und "MUSS" in ihren jeweiligen Formen sowie den zugehörigen Verneinungen genutzt, um deutlich zu machen, wie die jeweiligen Anforderungen zu interpretieren sind. Die hier genutzte Definition basiert auf [RFC2119] sowie DIN 820-2:2012, Anhang H [820-2].

MUSS / DARF NUR:	Dieser Ausdruck bedeutet, dass es sich um eine Anforderung handelt, die unbedingt erfüllt werden muss (uneingeschränkte Anforderung).
DARF NICHT / DARF KEIN:	Dieser Ausdruck bedeutet, dass etwas in keinem Fall getan werden darf (uneingeschränktes Verbot).
SOLLTE:	Dieser Ausdruck bedeutet, dass eine Anforderung normalerweise erfüllt werden muss, es aber Gründe geben kann, dies doch nicht zu tun. Dies muss aber sorgfältig abgewogen und stichhaltig begründet werden.
SOLLTE NICHT / SOLLTE KEIN:	Dieser Ausdruck bedeutet, dass etwas normalerweise nicht getan werden sollte, es aber Gründe gibt, dies doch zu tun. Dies muss aber sorgfältig abgewogen und stichhaltig begründet werden.

Sicherheitskonzepte, die mit Hilfe des IT-Grundschutzes erstellt werden, sind kompakt, da innerhalb des Konzepts jeweils nur auf die entsprechenden Sicherheitsanforderungen im IT-Grundschutz-Kompendium referenziert werden muss. Dies fördert die Verständlichkeit und die Übersichtlichkeit. Um die Sicherheitsanforderungen leichter umsetzen zu können, gibt es zu vielen Bausteinen des IT-Grundschutz-Kompendiums zusätzlich Umsetzungshinweise. Diese beschreiben, wie die Anforderungen der Bausteine in der Praxis erfüllt werden können, und enthalten dafür passende Sicherheitsmaßnahmen mit einer detaillierten Beschreibung. Bei der verwendeten Fachterminologie wird darauf geachtet, dass die Beschreibungen für diejenigen verständlich sind, die die Maßnahmen realisieren müssen. Zu beachten ist, dass es sich bei den Umsetzungshinweisen um Hilfestellungen zur Erfüllung der Anforderungen des jeweiligen Bausteins und nicht um verbindliche Vorgaben handelt.

Hinweis: Die umfangreichen Informationen rund um IT-Grundschutz ersetzen nicht den gesunden Menschenverstand. Informationssicherheit zu verstehen, umzusetzen und zu leben, sollte Priorität haben. Das IT-Grundschutz-Kompendium bietet zu vielen Aspekten eine Menge an Informationen und Empfehlungen. Bei deren Bearbeitung sollte immer im Auge behalten werden, dass aus diesen die für die jeweilige Institution und ihre Rahmenbedingungen geeigneten Sicherheitsanforderungen ausgewählt und angepasst werden. Weiterführende Informationen zur Anpassung der Baustein-Anforderungen finden sich in Kapitel 8.3.6. Weder die Anforderungen der Bausteine des IT-Grundschutz-Kompendiums noch die Maßnahmen der Umsetzungshinweise sollten als pure Checklisten zur Statusfeststellung genutzt werden, sondern mit Augenmaß an die individuellen Bedingungen adaptiert werden.

Um die Realisierung der Maßnahmen zu vereinfachen, werden die IT-Grundschutz-Texte konsequent auch in elektronischer Form zur Verfügung gestellt. Darüber hinaus wird die Realisierung der Sicherheitsanforderungen und Maßnahmen auch durch Hilfsmittel und Musterlösungen unterstützt,

die teilweise durch das BSI und teilweise auch von Anwendern des IT-Grundschutzes bereitgestellt werden.

3 Initiierung des Sicherheitsprozesses

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

3.1 Übernahme von Verantwortung durch die Leitungsebene

Die oberste Leitungsebene jeder Behörde und jedes Unternehmens ist dafür verantwortlich, dass alle Geschäftsbereiche zielgerichtet und ordnungsgemäß funktionieren und dass Risiken frühzeitig erkannt und minimiert werden. Mit der steigenden Abhängigkeit der Geschäftsprozesse von der Informationsverarbeitung steigen also auch die Anforderungen, dass die Informationssicherheit nach innen und außen gewährleistet ist.

Die oberste Leitungsebene muss den Sicherheitsprozess initiieren, steuern und kontrollieren. Die Leitungsebene ist diejenige Instanz, die die Entscheidung über den Umgang mit Risiken treffen und die entsprechenden Ressourcen zur Verfügung stellen muss. Die Verantwortung für Informationssicherheit verbleibt dort. Die operative Aufgabe "Informationssicherheit" wird allerdings typischerweise an einen Informationssicherheitsbeauftragten (ISB) delegiert.

In der Einstiegsphase in den Sicherheitsprozess ist typischerweise noch keine Sicherheitsorganisation aufgebaut und häufig auch noch nicht der spätere ISB benannt. Für die Initiierung des Sicherheitsprozesses muss aber zumindest ein Verantwortlicher für Informationssicherheit benannt werden, der die ersten Schritte zur Konzeption und Planung des Einstiegs in Informationssicherheit durchführt.

Rechtzeitige Unterrichtung über mögliche Risiken beim Umgang mit Informationen, Geschäftsprozessen und IT kann von der Geschäftsführung oder Behördenleitung nach einem Sicherheitsvorfall als Bringschuld der IT- oder Sicherheitsexperten gesehen werden. Aus diesem Grund ist es für die Inhaber dieser Rollen empfehlenswert, die oberste Leitungsebene über mögliche Risiken und Konsequenzen aufgrund fehlender Informationssicherheit nachweislich aufzuklären. Auf jeden Fall ist aber die Leitungsebene ebenfalls dafür verantwortlich, sicherzustellen, dass alle entscheidungsrelevanten Informationen sie rechtzeitig und im nötigen Umfang erreichen. Zu den sicherheitsrelevanten Themen gehören beispielsweise:

- die Sicherheitsrisiken für die Institution und deren Informationen sowie die damit verbundenen Auswirkungen und Kosten,
- die Auswirkungen von Sicherheitsvorfällen auf die kritischen Geschäftsprozesse,
- die Sicherheitsanforderungen, die sich aus gesetzlichen und vertraglichen Vorgaben ergeben,
- die für die Branche typischen Standard-Vorgehensweisen zur Informationssicherheit,
- der aktuelle Stand der Informationssicherheit im Sinne eines Reifegrades und daraus abgeleitete Handlungsempfehlungen.

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.

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

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

Aktionspunkte zu 3.1 Übernahme von Verantwortung durch die Leitungsebene
• Die Leitungsebene informiert sich über mögliche Risiken und Konsequenzen aufgrund fehlender Informationssicherheit. • Die Leitungsebene übernimmt die Gesamtverantwortung für Informationssicherheit. • Die Leitungsebene initiiert den Informationssicherheitsprozess innerhalb der Institution und benennt einen Verantwortlichen für Informationssicherheit.

3.2 Konzeption und Planung des Sicherheitsprozesses

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

3.2.1 Ermittlung von Rahmenbedingungen

Um eine angemessene IS-Strategie festzulegen, müssen alle relevanten Rahmenbedingungen identifiziert werden. Daher sollte jede Institution ihre wichtigsten Geschäftsprozesse und Fachaufgaben sowie deren Bedarf an Informationssicherheit ermitteln. Dazu gehört auch die Analyse der Stakeholder (also der relevanten internen und externen Parteien), von Geschäftszielen, Aufgaben und deren Anforderungen an Sicherheit. Die Zusammenhänge zwischen Geschäftsabläufen und den dort verarbeiteten Informationen sowie der eingesetzten Informationstechnik bilden die Basis für die Entscheidung, welches Sicherheitsniveau zum Schutz der Informationen und für die Informationstechnik jeweils angemessen ist.

Die Ermittlung von Rahmenbedingungen ist eine wesentliche Grundlage für die weiteren Betrachtungen der Informationssicherheit, da hierdurch identifiziert werden kann, wo wichtige Hintergrundinformationen fehlen, um die Bedeutung der Informationssicherheit für die Institution korrekt einschätzen zu können. Außerdem wird dadurch ein erstes Self-Assessment möglich, da bei der Zusammenstellung der Hintergrundinformationen bereits deutlich wird, wo Konfliktpotential liegt und wo Aktivitäten erforderlich sind.

Allgemeine Einflussfaktoren

Informationssicherheit dient der Institution zur Erreichung der Geschäftsziele. Daher müssen die sich hieraus abgeleiteten Einflussfaktoren betrachtet werden:

- Geschäftsziele: Welche Faktoren sind wesentlich für den Erfolg des Unternehmens oder der Behörde? Welche Produkte, Angebote und Aufträge bilden die Grundlage der Geschäftstätigkeit? Was sind die generellen Ziele der Institution? Welche Rolle spielt Informationssicherheit hierbei?
- Organisationsstruktur: Wie ist die Institution organisiert und strukturiert? Welche Managementsysteme sind vorhanden (beispielsweise Risikomanagement oder Qualitätsmanagement)?
- Zusammenarbeit mit Externen: Was sind die wichtigsten internen und externen Kunden, Partner und einflussnehmenden Gremien? Was sind deren grundlegenden Anforderungen und

Erwartungen an die Informationssicherheit der Institution? Was sind die wichtigsten Dienstleister und Zulieferer? Welche Rolle spielen diese für die Informationssicherheit der Institution?

- Strategischer Kontext: Was sind die wesentlichen Herausforderungen für die Institution? Wie ist die Wettbewerbsposition? Wie beeinflusst dies den Risikoappetit der Institution und den Umgang mit Informationssicherheit?

Interne Rahmenbedingungen

Viele interne Rahmenbedingungen können Auswirkungen auf die Informationssicherheit haben und müssen folglich ermittelt werden. Über die Analyse der Geschäftsprozesse und Fachaufgaben lassen sich Aussagen über die Auswirkungen von Sicherheitsvorfällen auf die Geschäftstätigkeit und die Aufgabenerfüllung ableiten. Es geht zu diesem frühen Zeitpunkt nicht darum, detailliert die Informationstechnik zu beschreiben. Es sollte aber eine grobe Übersicht vorliegen, welche Informationen für einen Geschäftsprozess mit welchen Anwendungen und IT-Systemen verarbeitet werden.

Oft gibt es in Institutionen schon Übersichten von Geschäftsprozessen, Objekten oder Datensammlungen, die für betriebliche Aspekte oder die Verwaltung benötigt werden. Falls vorhanden, können vorhandene Prozesslandkarten, Geschäftsverteilungspläne, Datenbanken, Übersichten, Netzpläne und Inventarisierungstools genutzt werden, um die wesentlichen Geschäftsprozesse zu identifizieren. Werden diese Übersichten berücksichtigt, sollte darauf geachtet werden, dass hierdurch der Detaillierungsgrad der Erfassung nicht zu tief wird, damit der Umfang für einen ersten Überblick und als Grundlage für spätere Entscheidungen nicht zu umfangreich ist.

Folgende Aspekte sollten bedacht werden:

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

Zu jedem Geschäftsprozess und jeder Fachaufgabe muss ein verantwortlicher Ansprechpartner benannt werden, der als sogenannter Informationseigentümer für alle Fragen der Informationsverarbeitung im Rahmen dieses Geschäftsprozesses verantwortlich ist.

Externe Rahmenbedingungen

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

- gesetzliche Rahmenbedingungen (nationale und internationale Gesetze und Bestimmungen),
- Anforderungen von Kunden, Lieferanten und Geschäftspartnern, aktuelle Marktlage, Wettbewerbssituation und weitere relevante marktspezifische Abhängigkeiten,
- branchenspezifische Sicherheitsstandards.

Brainstorming

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 ISB mit den jeweiligen Informationseigentümern bzw. Fachverantwortlichen sowie dem

entsprechenden IT-Verantwortlichen durchgeführt werden. Ob insgesamt eine oder mehrere Besprechungen erforderlich sind, hängt von der Größe und Komplexität der Institution ab.

Es sollten vorrangig geschäftskritische Informationen und Kernprozesse ermittelt und die zugehörigen Anwendungen, IT-Systeme, Netze und Räume erfasst werden. Dabei sollten ausgehend von den Kernprozessen der Institution die wesentlichen unterstützenden Prozesse und die hauptsächlich betroffenen Objekte ermittelt werden. Es hat sich gezeigt, dass es schwer fällt, abstrakte Prozesse losgelöst von konkreten technischen Komponenten zu betrachten. Daher kann es gegebenenfalls sinnvoll sein, nicht nur aus Prozesssicht kommend die Assets zu ermitteln, sondern auch aus Sicht der bekannten Assets zu ermitteln, welche Prozesse diese verwenden. Dieses optionale Vorgehen ist besonders dann sinnvoll, wenn keine vollständige Prozesslandkarte vorhanden ist und die Geschäftsführung Schwierigkeiten hat, diese zu definieren.

Die Teilnahme der Leitungsebene am Brainstorming ist nicht zwingend notwendig. Viel wichtiger ist es, dass jeder Teilnehmer für den Bereich, den er vertritt, auskunftsfähig ist und die wesentlichen Geschäftsprozesse seines Bereiches sowie die eingesetzten Assets benennen kann. Die Erstaufnahme sollte typischerweise nicht länger als einen halben Tag beanspruchen. Die Ergebnisse sollten nach einem vorher festgelegten Schema dokumentiert und an die Leitungsebene berichtet werden.

3.2.2 Formulierung von allgemeinen Informationssicherheitszielen

Zu Beginn jedes Sicherheitsprozesses sollten die Informationssicherheitsziele sorgfältig bestimmt werden. Anderenfalls besteht die Gefahr, dass Sicherheitsstrategien und -konzepte erarbeitet werden, die die eigentlichen Anforderungen der Institution verfehlen.

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

- Hohe Verlässlichkeit des Handelns, auch in Bezug auf den Umgang mit Informationen (Verfügbarkeit, Integrität, Vertraulichkeit),
- Gewährleistung des guten Rufs der Institution in der Öffentlichkeit,
- Erhaltung der in Technik, Informationen, Arbeitsprozesse und Wissen investierten Werte,
- Sicherung der hohen, möglicherweise unwiederbringlichen Werte der verarbeiteten Informationen,
- Gewährleistung der aus gesetzlichen Vorgaben resultierenden Anforderungen,
- Schutz von natürlichen Personen hinsichtlich ihrer körperlichen und geistigen Unversehrtheit.

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

An dieser Stelle muss keine detaillierte Analyse des Informationsverbundes und der möglichen Kosten von Sicherheitsmaßnahmen erfolgen, sondern lediglich die Aussage, was für die Institution von besonderer Bedeutung ist und warum.

3.2.3 Bestimmung des angemessenen Sicherheitsniveaus der Geschäftsprozesse

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

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

Sehr hoch:

- Der Schutz vertraulicher Informationen muss unbedingt gewährleistet sein und in sicherheitskritischen Bereichen strengen Vertraulichkeitsanforderungen genügen. Die Offenlegung besonders kritischer oder hoch vertraulicher Information kann zu schweren Folgen für den Weiterbestand der Institution führen.
- Die Informationen müssen im höchsten Maße korrekt sein.
- Die zentralen Aufgaben der Institution sind ohne IT-Einsatz nicht durchführbar. Knappe Reaktionszeiten für kritische Entscheidungen fordern ständige Präsenz der aktuellen Informationen, Ausfallzeiten sind nicht akzeptabel.
- Der Schutz personenbezogener Daten muss unbedingt gewährleistet sein. Anderenfalls kann es zu einer Gefahr für Leib und Leben oder für die persönliche Freiheit des Betroffenen kommen.

Insgesamt gilt: Der Ausfall der IT oder wesentlicher Geschäftsprozesse oder die Offenlegung bzw. Manipulation von kritischen Informationen führt zum Zusammenbruch der Institution oder hat schwerwiegende Folgen für breite gesellschaftliche oder wirtschaftliche Bereiche.

Hoch:

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

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

Normal:

- Der Schutz von Informationen, die nur für den internen Gebrauch bestimmt sind, muss gewährleistet sein.
- Informationen sollten korrekt sein. Kleinere Fehler können toleriert werden. Fehler, die die Aufgabenerfüllung erheblich beeinträchtigen, müssen jedoch erkenn- oder vermeidbar sein.
- Längere Ausfallzeiten, die zu Terminüberschreitungen führen, sind nicht zu tolerieren.

- Der Schutz personenbezogener Daten muss gewährleistet sein. Anderenfalls besteht die Gefahr, dass der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt wird.

Insgesamt gilt: Schäden haben Beeinträchtigungen der Institution zur Folge.

Hinweis:

Jede Institution sollte die Formulierungen auf ihre individuellen Gegebenheiten anpassen. Es kann auch sinnvoll sein, weitere Kategorien zu definieren, beispielsweise um Abgrenzungen nach oben oder unten deutlicher zu machen. Die Sicherheitsziele spiegeln auch wieder, welche Sicherheitskultur in einer Institution vorhanden ist, also wie mit Sicherheitsrisiken und –maßnahmen umgegangen wird.

Für die Formulierung der Informationssicherheitsziele ist die Mitwirkung der Leitungsebene unbedingt notwendig. Zur Bestimmung des angestrebten Sicherheitsniveaus müssen die Ziele der Institution in Bezug auf ihre Anforderungen zur Sicherheit betrachtet werden, jedoch unter Berücksichtigung der Tatsache, dass in der Regel begrenzte Ressourcen für die Implementierung von Sicherheitsmaßnahmen zur Verfügung stehen. Aus diesem Grund ist es von besonderer Bedeutung, den tatsächlichen Bedarf an Verfügbarkeit, Integrität und Vertraulichkeit zu identifizieren, da ein hohes Sicherheitsniveau in der Regel auch mit hohem Implementierungsaufwand verbunden ist. Es ist außerdem empfehlenswert, die formulierten Anforderungen zu priorisieren, wenn dies zu diesem Zeitpunkt bereits möglich ist.

Hinweis zur Beschreibungstiefe

In dieser frühen Phase des Informationssicherheitsprozesses geht es nicht um eine detaillierte Betrachtung aller Anwendungen und IT-Systeme oder eine aufwendige Risikoanalyse. Wichtig ist, eine Übersicht zu haben, welche Anforderungen zur Sicherheit aufgrund der Geschäftsprozesse oder Fachverfahren an die Informationstechnik gestellt werden. Zum Beispiel sollten sich nach der Bestimmung des angestrebten Sicherheitsniveaus die folgenden Fragen beantworten lassen:

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

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

3.2.4 Ersterfassung der Prozesse, Anwendungen und IT-Systeme

Die Ergebnisse der vorherigen Schritte, also der Ermittlung von Rahmenbedingungen, der Formulierung von Informationssicherheitszielen und der Bestimmung des angemessenen Sicherheitsniveaus der Geschäftsprozesse sollten als Nächstes in einer Übersicht der vorhandenen Assets der Institution konsolidiert werden.

Diese Übersicht dient als Entscheidungshilfe für die Auswahl einer geeigneten Vorgehensweise und ist die Basis für die späteren Schritte, wie die Auswahl der relevanten IT-Grundschutz-Bausteine bei der Basis-Absicherung oder die Strukturanalyse bei der Standard-Absicherung. Hierbei sollte die Erstaufnahme der Prozesse, Anwendungen und IT-Systeme so weit vollständig sein, dass sie als Entscheidungshilfe für die Auswahl der geeigneten Vorgehensweise zur Absicherung der Institution verwendet werden kann, sie ist aber bei weitem nicht so umfangreich wie das Ergebnis einer Strukturanalyse.

Die Ersterfassung liefert als Ergebnis eine vergleichsweise schnell und ressourcenschonend erstellbare Übersicht. Die bei der Standard-Absicherung durchzuführende Strukturanalyse kann darauf aufsetzen und liefert ein vollständigeres Bild des abzusichernden Informationsverbunds.

Im Rahmen der Ersterfassung müssen ausgehend von den wesentlichen Geschäftsprozessen und Fachverfahren die Anwendungen, IT-Systeme, Netzkomponenten, Räume und ähnliche Objekte identifiziert werden, die für die Durchführung der Geschäftsprozesse wesentlich sind. Hierbei sollten nicht nur die primären Abhängigkeiten betrachtet werden, also die für einen Geschäftsprozess direkt benötigten Applikationen und IT-Systeme. Auch sekundäre Abhängigkeiten, d. h. die kritischen Unterstützungsprozesse bzw. -systeme (wie Gebäudetechnik, Logistik usw.) sollten bei der Betrachtung berücksichtigt werden.

Wenn möglich, sollte zu diesem Zeitpunkt abgeschätzt werden, ob die identifizierten Objekte ein höheres Sicherheitsniveau als "normal" erfordern.

Dabei ist es häufig nicht zweckmäßig, jedes Objekt einzeln zu erfassen, da Informationsverbünde meist aus vielen Einzelobjekten bestehen. Stattdessen sollten ähnliche Objekte sinnvoll zu Gruppen zusammengefasst werden. Für die Ersterfassung kann es auch einfacher sein, in einem zweiten Schritt eine grafische Netzübersicht zu erstellen und ausgehend von dieser die IT-Systeme zu erfassen. Hierbei geht es nicht um Vollständigkeit oder Form. Das Ziel ist eine stark vereinfachte Netzübersicht.

Bei der Ersterfassung sollten auch nur die wesentlichen Objekte erfasst werden, nicht jede einzelne IT-Komponente. Beispielsweise sollten bei der Erstaufnahme keine typischen Büroräume erfasst werden, Serverräume mit ihrem speziellen meist höheren Sicherheitsniveau sollten aber mit aufgenommen werden.

Erfassung der relevanten Objekte

Ausgehend von jedem Geschäftsprozess bzw. jeder Fachaufgabe, die im Informationsverbund enthalten ist, sollten folgende Objekte tabellarisch mit einen eindeutigen Bezeichner und mindestens folgenden Hinweisen erfasst werden:

- Geschäftsprozess oder Fachaufgabe: Name und (falls erforderlich) Beschreibung, fachverantwortliche Stelle
- Anwendung: Name, (falls erforderlich) Beschreibung und dazugehöriger Geschäftsprozess
- IT-, ICS-Systeme und sonstige Objekte: Name, Plattform und sofern sinnvoll Aufstellungsort
- für die Aufrechterhaltung des Betriebes wesentliche Räume, die dadurch ein höheres Sicherheitsniveau erfordern (z. B. Rechenzentrum, Serverräume): Art, Raumnummer und Gebäude

Virtuelle IT-Systeme und Netze sollten wie physische Strukturen behandelt werden, sollten aber geeignet gekennzeichnet sein.

Abschätzung des Sicherheitsniveaus

Für spätere Betrachtungen kann es sich als sinnvoll erweisen, schon zu einem frühen Zeitpunkt das angestrebte Sicherheitsniveau der einzelnen Assets abzuschätzen. Die eigentliche Schutzbedarfsfeststellung sollte allerdings zu einem späteren Zeitpunkt erfolgen. Diese Abschätzung

des Sicherheitsniveaus bietet eine grobe Orientierung für den zu erwartenden Aufwand und erleichtert eine geeignete Gruppenbildung der identifizierten Assets.

Die bisher identifizierten Objekte, bei denen ein höheres Sicherheitsniveau als "normal" angestrebt wird, sollten in der bereits erstellten Tabelle gekennzeichnet werden.

Erstellung eines grafischen Netzplans

Auf Grundlage der erfassten Informationen sollte ein rudimentärer Netzplan als Übersicht erstellt werden. Wenn ein aktueller Netzplan vorhanden ist, kann natürlich dieser genutzt werden. Ein Netzplan ist eine grafische Übersicht über die im betrachteten Bereich der Informations- und Kommunikationstechnik eingesetzten Komponenten und deren Vernetzung. Im Gegensatz zu einem vollständigen oder vereinfachten Netzplan, wie er in der später folgenden Strukturanalyse erstellt wird, dient diese Netzübersicht vielmehr als Überblick, die die weitere Diskussion vereinfacht und zeigt, ob essentielle IT-Systeme vergessen wurden. Im Einzelnen sollte der Plan in Bezug auf die Informationssicherheit mindestens folgende Objekte darstellen:

- IT-Systeme, d. h. Clients und Server, aktive Netzkomponenten
- Netzverbindungen zwischen diesen Systemen
- Verbindungen des betrachteten Bereichs nach außen

Die grafische Netzübersicht sollte sich aber nicht auf physische Komponenten beschränken, sondern auch virtualisierte Strukturen beinhalten. Hierbei können entweder virtuelle Strukturen (geeignet gekennzeichnet) direkt in der grafischen Netzübersicht aufgenommen werden oder bei unübersichtlichen Architekturen in eine separate Netzübersicht eingetragen werden.

Ein Beispiel für eine Ersterfassung einschließlich einer Netzübersicht ist in den Hilfsmitteln zum IT-Grundschutz zu finden. In der später durchzuführenden Strukturanalyse werden die hier gewonnenen Ergebnisse präzisiert und vervollständigt.

Aktionspunkte zu 3.2 Konzeption und Planung des Sicherheitsprozesses
• Ansprechpartner für alle Geschäftsprozesse und Fachaufgaben benennen • Grobeinschätzung der Wertigkeit und des Sicherheitsniveaus von Informationen, Geschäftsprozessen und Fachaufgaben durchführen • Interne und externe Rahmenbedingungen ermitteln • Bedeutung der Geschäftsprozesse, Fachaufgaben und Informationen abschätzen • Allgemeine Informationssicherheitsziele festlegen • Konsolidierte Übersicht der vorhandenen Assets mit den zuvor gewonnenen Erkenntnissen erstellen • Zustimmung der Leitungsebene einholen

3.3 Entscheidung für Vorgehensweise

Der IT-Grundschutz bietet verschiedene Vorgehensweisen an, die sich an unterschiedliche Anwendergruppen richten und unterschiedliche Ziele verfolgen: Basis-, Standard- und Kernabsicherung. In diesem Schritt erfolgt die Auswahl der für die Institution optimalen Vorgehensweise basierend auf der bereits vorliegenden Entscheidungshilfe unter Zuhilfenahme der oben durchgeführten Ersterfassung.

Bei der Basis-Absicherung handelt es sich um eine grundlegende Absicherung der Geschäftsprozesse und Ressourcen einer Institution. Sie ermöglicht einen ersten Einstieg in den Sicherheitsprozess, um schnellstmöglich die größten Risiken zu senken. Im nächsten Schritt können die tatsächlichen

Sicherheitsanforderungen im Detail analysiert werden. Diese Vorgehensweise ist daher besonders für kleinere Institutionen geeignet, die noch am Anfang ihres Sicherheitsprozesses stehen.

Die Kern-Absicherung dient als weitere Einstiegsvorgehensweise dem Schutz der essentiellen Geschäftsprozesse und Ressourcen einer Institution. Diese Vorgehensweise unterscheidet sich vom klassischen IT-Grundschutz durch die Fokussierung auf einen kleinen, aber sehr wichtigen Teil eines Informationsverbundes, die sogenannten Kronjuwelen. Die Kern-Absicherung ist vor allem für Institutionen geeignet, die einige wenige Geschäftsprozesse identifiziert haben, die wesentlich für den Fortbestand der Institution sind und vorrangig abgesichert werden müssen.

Die dritte und vom BSI präferierte Vorgehensweise ist die Standard-Absicherung. Diese entspricht in den Grundzügen der bekannten und bewährten IT-Grundschutz-Vorgehensweise.

Die Basis-Absicherung und die Kern-Absicherung sind jeweils Methoden, um zunächst zeitnah die wichtigsten Sicherheitsempfehlungen für den ausgewählten Einsatzbereich identifizieren und umsetzen zu können. Ziel muss es sein, mittelfristig ein vollständiges Sicherheitskonzept gemäß der Standard-Absicherung zu erstellen.

3.3.1 Basis-Absicherung

Die Basis-Absicherung verfolgt das Ziel, als Einstieg in den IT-Grundschutz zunächst eine breite, grundlegende Erst-Absicherung über alle relevanten Geschäftsprozesse bzw. Fachverfahren einer Institution zu erlangen. Diese Vorgehensweise ist für Institutionen empfehlenswert, bei denen folgende Punkte zutreffen:

- Die Umsetzung von Informationssicherheit steht noch am Anfang, d. h. die Informationssicherheit hat bisher nur einen niedrigen Reifegrad erreicht.
- Die Geschäftsprozesse haben kein deutlich erhöhtes Gefährdungspotential bezüglich der Informationssicherheit.
- Das angestrebte Sicherheitsniveau ist normal.
- Es sind keine Assets vorhanden, deren Diebstahl, Zerstörung oder Kompromittierung einen existenzbedrohenden Schaden für die Institution bedeutet.
- Kleinere Sicherheitsvorfälle können toleriert werden – also solche, die zwar Geld kosten oder anderweitig Schaden verursachen, aber in der Summe nicht existenzbedrohend sind.

Mit der Basis-Absicherung können zeitnah zunächst die wichtigsten Sicherheitsanforderungen umgesetzt werden, um darauf aufbauend zu einem späteren Zeitpunkt das Sicherheitsniveau weiter zu erhöhen, beispielsweise indem alle Bereiche mit der Standard-Absicherung oder kritische Geschäftsprozesse mit der Kern-Absicherung geschützt werden.

3.3.2 Kern-Absicherung

Über die Kern-Absicherung kann eine Institution als Einstieg in den IT-Grundschutz bzw. den Sicherheitsprozess zunächst besonders gefährdete Geschäftsprozesse und Assets vorrangig absichern. Diese Vorgehensweise ist empfehlenswert, wenn für eine Institution folgende Punkte überwiegend zutreffen:

- Die Menge der Geschäftsprozesse mit deutlich erhöhtem Schutzbedarf ist überschaubar bzw. umfasst nur einen kleinen Anteil aller Geschäftsprozesse der Institution.
- Die Institution kann die Geschäftsprozesse, die ein deutlich erhöhtes Gefährdungspotential bezüglich der Informationssicherheit haben, zügig identifizieren und eindeutig abgrenzen.
- Die Institution besitzt eindeutig benennbare Assets, deren Diebstahl, Zerstörung oder Kompromittierung einen existenzbedrohenden Schaden für die Institution bedeuten würde (sogenannte Kronjuwelen). Diese sollen vorrangig geschützt werden.
- Kleinere Sicherheitsvorfälle, die Geld kosten oder anderweitig Schaden verursachen, aber keinen existenzbedrohenden Schaden verursachen, sind für die Institution akzeptabel.

Mit der Kern-Absicherung können zeitnah die wichtigsten Ressourcen und Geschäftsprozesse abgesichert werden. So kann in einem ersten Schritt zunächst der kritischste Geschäftsprozess abgesichert werden, um in weiteren Schritten wahlweise die nächsten kritischen Geschäftsprozesse abzusichern oder für alle Bereiche der Institution die Basis- oder Standard-Absicherung zu beginnen. Eine Zertifizierung nach ISO 27001 ist für den betrachteten abgegrenzten Informationsverbund grundsätzlich möglich.

3.3.3 Standard-Absicherung

Die Standard-Absicherung entspricht im Wesentlichen der klassischen IT-Grundschutz-Vorgehensweise. Mit der Standard-Absicherung kann eine Institution umfassend und tiefgehend abgesichert werden. Dies sollte grundsätzlich das Ziel jeglicher Anwendung des IT-Grundschutzes sein, auch wenn zuvor zunächst eine der beiden bereits genannten anderen Vorgehensweisen gewählt wurde. Ein direkter Einstieg in den Sicherheitsprozess mit der Standard-Absicherung ist empfehlenswert, wenn für die Institution die folgenden Punkten überwiegend zutreffen:

- Die Institution arbeitet bereits mit dem IT-Grundschutz.
- Es wurden schon Sicherheitskonzepte nach IT-Grundschutz oder ISO 27001 erstellt.
- Die Umsetzung von Informationssicherheit hat in der Institution bereits einen ausreichenden Reifegrad erreicht, so dass in wesentlichen Bereichen bereits Sicherheitsmaßnahmen vorhanden sind und keine grundlegende Erst-Absicherung mehr notwendig ist.
- Es besteht kein Handlungsbedarf, einzelne Geschäftsprozesse vordringlich abzusichern, die ein deutlich höheres Gefährdungspotential bezüglich der Informationssicherheit besitzen (vergleiche Kern-Absicherung).
- Die Institution hat keine Assets, deren Diebstahl, Zerstörung oder Kompromittierung einen unmittelbar existenzbedrohenden Schaden nach sich ziehen könnte und die daher vorrangig abgesichert werden sollten.
- Sicherheitsvorfälle, die wahrnehmbar die Aufgabenerfüllung beeinträchtigen, Geld kosten oder anderweitig erkennbaren Schaden verursachen, sind für die Institution nicht akzeptabel, auch wenn sie noch keinen existenzbedrohenden Schaden verursachen.

Die Standard-Absicherung ist die Vorgehensweise, die grundsätzlich angestrebt werden sollte, um alle Bereiche einer Institution angemessen und umfassend zu schützen. Auch für eine angestrebte Zertifizierung des Informationsverbundes nach ISO 27001 ist diese Vorgehensweise (bzw. die Kern-Absicherung) die erforderliche Grundlage.

3.3.4 Festlegung des Geltungsbereichs

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

Neben der Vorgehensweise muss also auch festgelegt werden, wie der damit zu schützende Informationsverbund aussehen soll. Dieser kann die gesamte Institution umfassen oder aus Teilbereichen bestehen. Als Informationsverbund können beispielsweise bestimmte Organisationseinheiten einer Institution betrachtet werden. Es könnten aber auch Bereiche sein, die definierte Geschäftsprozesse bearbeiten, inklusive der dafür notwendigen Infrastruktur. Wichtig ist jedoch dabei, dass die betrachteten Geschäftsprozesse komplett im Geltungsbereich enthalten sind.

Während bei der Basis- und Standard-Absicherung der Geltungsbereich häufig die gesamte Institution umfasst, wird sich bei der Kern-Absicherung auf einige herausragende, besonders geschäftskritische Prozesse konzentriert.

Es kann auch sinnvoll sein, Sicherheitskonzeptionen für mehrere kleinere Bereiche zu entwickeln. Dies kann beispielsweise der Fall sein, wenn der Aufwand für eine Gesamtabsicherung im ersten Schritt als zu hoch eingeschätzt wird und bestimmte Geschäftsprozesse priorisiert behandelt werden müssen. Hierfür könnte beispielsweise Bereiche identifiziert werden, für die parallel oder nacheinander Basis-, Standard- bzw. Kern-Absicherungen durchgeführt werden.

So könnte eine Institution beschließen, zunächst für einen kleinen Bereich mit besonders gefährdeten Assets die Kern-Absicherung umzusetzen. Damit aber auch für die restliche Institution ein Mindestmaß an Sicherheit vorhanden ist, soll dort die Basis-Absicherung garantiert werden.

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

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

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

Aktionspunkte zu 3.3.4 Definition des Geltungsbereichs für die Sicherheitskonzeption
• Festlegen, welche kritischen Geschäftsprozesse, Fachaufgaben oder Teile der Institution der Geltungsbereich beinhalten soll • Den Geltungsbereich eindeutig abgrenzen • Schnittstellen zu externen Partnern beschreiben

3.3.5 Management-Entscheidung

Der von der Leitungsebene benannte Verantwortliche für Informationssicherheit muss basierend auf den ermittelten Rahmenbedingungen, den formulierten Sicherheitszielen und dem angestrebten Sicherheitsniveau einen Vorschlag erarbeiten, wie die weiteren Schritte zur Erreichung der kurzfristigen sowie der langfristigen Sicherheitsziele aussehen sollte. Das Management muss auf dieser Grundlage entscheiden, für welche Bereiche der Institution welche Vorgehensweise zu deren Absicherung gewählt werden soll.

Es sollte anschließend dokumentiert werden, für welchen Bereich mit welchem Zeitplan eine Basis-, Standard- bzw. Kernabsicherung umgesetzt werden soll. Die entsprechenden Geltungsbereiche des Informationsverbunds müssen festgelegt werden.

Die folgende Übersicht zeigt die wichtigsten Vor- und Nachteile der einzelnen Vorgehensweisen auf.

Basis-Absicherung

Pro Der Aufwand ist verhältnismäßig niedrig. Dadurch ist ein schneller Einstieg in Informationssicherheit möglich. So lässt sich schnell eine grundlegende Erst-Absicherung erzielen.

Contra Durch pauschale Erfüllung der Erst-Anforderungen wird nur ein niedriges Sicherheitsniveau erreicht. Eventuell ist das erzielbare Schutzniveau nicht hoch genug für die tatsächlichen Sicherheitsanforderungen. Eine Zertifizierung nach ISO 27001 ist auf dieser Basis nicht möglich.

Kern-Absicherung

Pro Die Kern-Absicherung ermöglicht eine volle Fokussierung auf die Kronjuwelen, also die existentiell wichtigen Assets der Institution. Die Umsetzung ist schneller als bei der Einbeziehung aller Geschäftsprozesse. Eine Zertifizierung nach ISO 27001 ist für den betrachteten abgegrenzten Informationsverbund grundsätzlich möglich.

Contra Kronjuwelen können unter Umständen nicht isoliert betrachtet werden, wodurch umfangreichere Anteile der Institution einbezogen werden müssen. Alle nicht als kritisch eingestuften Geschäftsprozesse bleiben zunächst unbeachtet. Dabei besteht die Gefahr, dass einerseits wichtige Bereiche übersehen und somit gänzlich ungeschützt gelassen werden. Andererseits können kumulierte Risiken übersehen werden.

Standard-Absicherung

Pro Die Standard-Absicherung bietet ein hohes und an die vorhandenen Geschäftsprozesse spezifisch angepasstes Sicherheitsniveau. Es wird ein gleichmäßiges Sicherheitsniveau über die gesamte Institution erzielt. Das erreichte Sicherheitsniveau ist mit dem anderer Institutionen gut vergleichbar. Eine Zertifizierung nach ISO 27001 und eine Messbarkeit des ISMS sind möglich. Es werden alle notwendigen Ressourcen der Institution vollständig betrachtet.

Contra Der Aufwand ist bei einem niedrigen Reifegrad der vorhandenen Informationssicherheit höher als bei den beiden anderen Vorgehensweisen.

Aktionspunkte zu 3.3.5 Management-Entscheidung
• Erarbeitung einer Management-Vorlage zur Entscheidungsfindung • Entscheidung, für welche Bereiche der Institution welche Vorgehensweise zu deren Absicherung gewählt werden soll • Dokumentation der Entscheidung und des Zeitplans für die Umsetzung

3.4 Erstellung einer Leitlinie zur Informationssicherheit

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

Die Erstellung der Sicherheitsleitlinie sollte in folgenden Schritten vollzogen werden:

3.4.1 Verantwortung der Behörden- bzw. Unternehmensleitung für die Sicherheitsleitlinie

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

Da die Sicherheitsleitlinie ein zentrales Strategiepapier für die Informationssicherheit einer Institution darstellt, muss sie so gestaltet sein, dass sich alle adressierten Organisationseinheiten mit ihrem Inhalt identifizieren können. An ihrer Erstellung sollten daher möglichst viele Bereiche beteiligt werden.

Jede Institution muss letztendlich aber selbst entscheiden, welche Abteilungen und Hierarchieebenen an der Formulierung der Sicherheitsleitlinie mitwirken.

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

3.4.2 Einberufung einer Entwicklungsgruppe für die Sicherheitsleitlinie

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

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

3.4.3 Festlegung des Geltungsbereichs und Inhalt der Sicherheitsleitlinie

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

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

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

Zusätzlich können z. B. noch folgende Aussagen hinzukommen:

- Zur Motivation können einige, für die Geschäftsprozesse wichtige, Gefährdungen angerissen und die wichtigsten gesetzlichen Regelungen und sonstige wichtige Rahmenbedingungen (wie vertragliche Vereinbarungen) genannt werden.
- Die wesentlichen Aufgaben und Zuständigkeiten im Sicherheitsprozess sollten aufgezeigt werden (insbesondere für das IS-Management-Team, den IS-Beauftragten, die Mitarbeiter und den IT-Betrieb, ausführliche Informationen zu den einzelnen Rollen finden sich in Kapitel 4 *Organisation des Sicherheitsprozesses*). Außerdem sollten die Organisationseinheiten oder Rollen benannt werden, die als Ansprechpartner für Sicherheitsfragen fungieren.
- Programme zur Förderung der Informationssicherheit durch Schulungs- und Sensibilisierungsmaßnahmen können angekündigt werden.

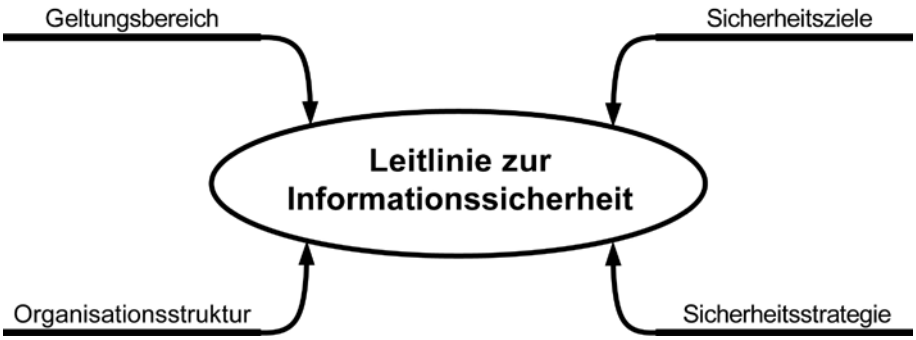


Abbildung 2: Inhalte der Sicherheitsleitlinie

3.4.4 Bekanntgabe der Sicherheitsleitlinie

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

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

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

3.4.5 Aktualisierung der Sicherheitsleitlinie

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

Aktionspunkte zu 3.4 Erstellung einer Sicherheitsleitlinie
• Auftrag der Leitungsebene zur Erarbeitung einer Sicherheitsleitlinie einholen • Entwicklungsgruppe für die Sicherheitsleitlinie einberufen • Geltungsbereich und Inhalte festlegen • Inkraftsetzung der Sicherheitsleitlinie durch die Leitungsebene veranlassen • Sicherheitsleitlinie bekannt geben • Sicherheitsleitlinie regelmäßig überprüfen und gegebenenfalls aktualisieren

4 Organisation des Sicherheitsprozesses

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

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

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

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

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

Grundregeln bei der Definition von Rollen im Informationssicherheitsmanagement

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

4.1 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse

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

Vor allem in größeren Institutionen existiert bereits häufig ein übergreifendes Risikomanagementsystem. Da Informationssicherheits-Risiken ebenso wie IT-Risiken zu den wichtigsten operationellen Risiken gehören, sollten die Methoden zum Informationssicherheitsmanagement und zum Management von Risiken mit den bereits etablierten Methoden und Managementsystemen abgestimmt werden, siehe hierzu auch BSI-Standard 200-3 *Risikoanalyse auf der Basis von IT-Grundschutz*.

4.2 Aufbau der Informationssicherheitsorganisation

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

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

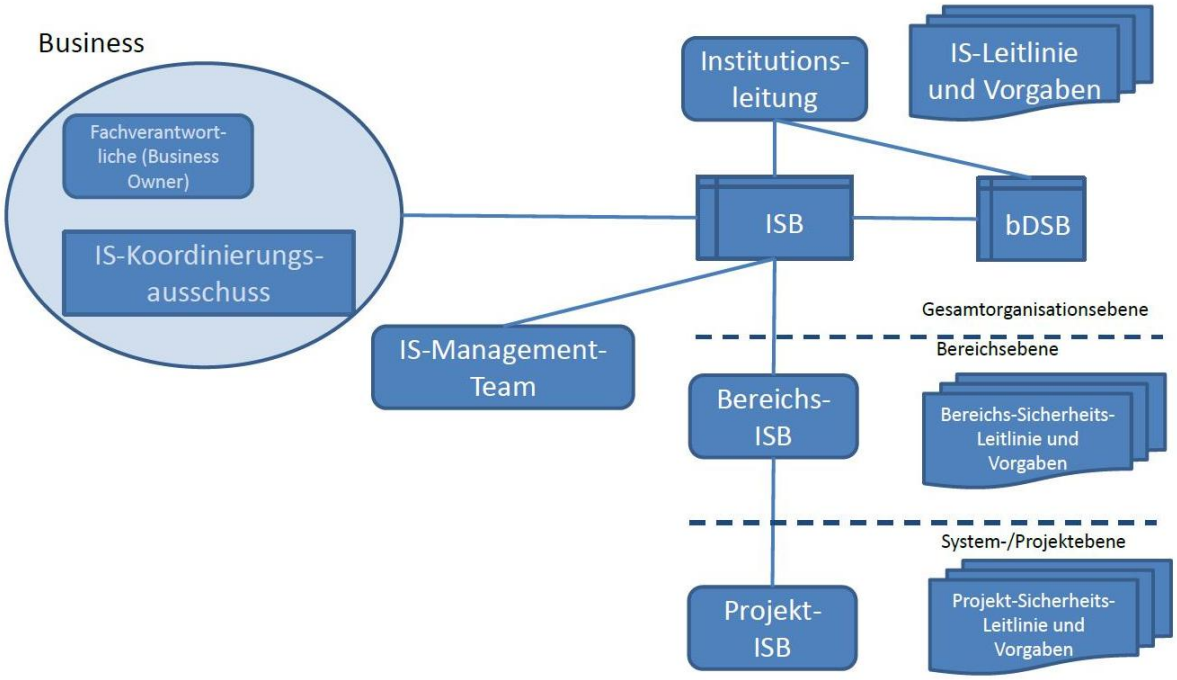


Abbildung 3: Aufbau einer IS-Organisation in einer großen Institution

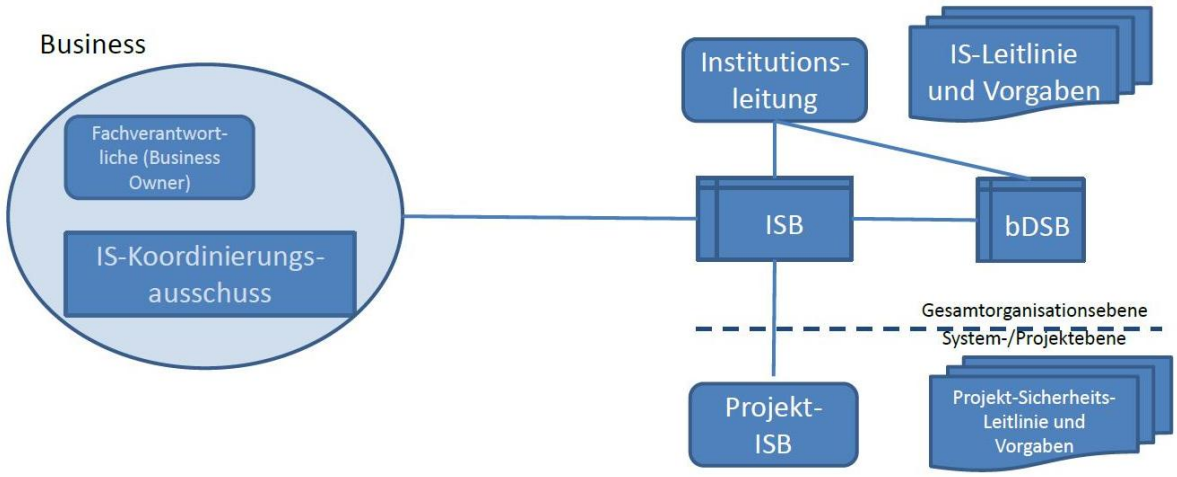


Abbildung 4: Aufbau der IS-Organisation in einer mittelgroßen Institution

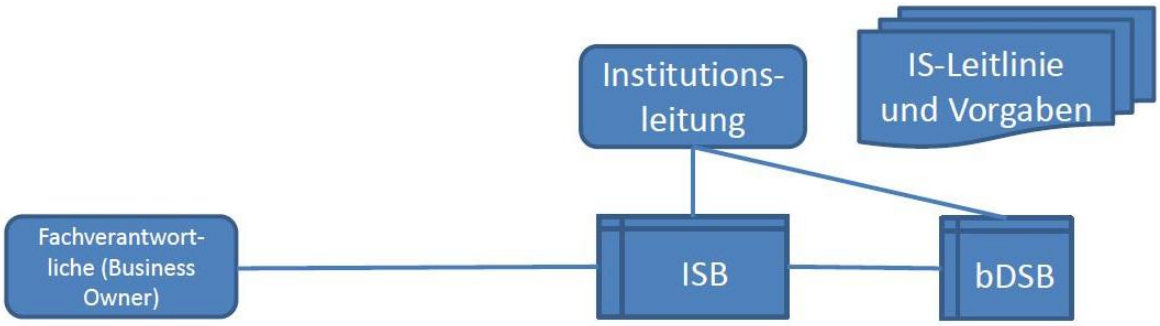


Abbildung 5: Aufbau der IS-Organisation in einer kleinen Institution

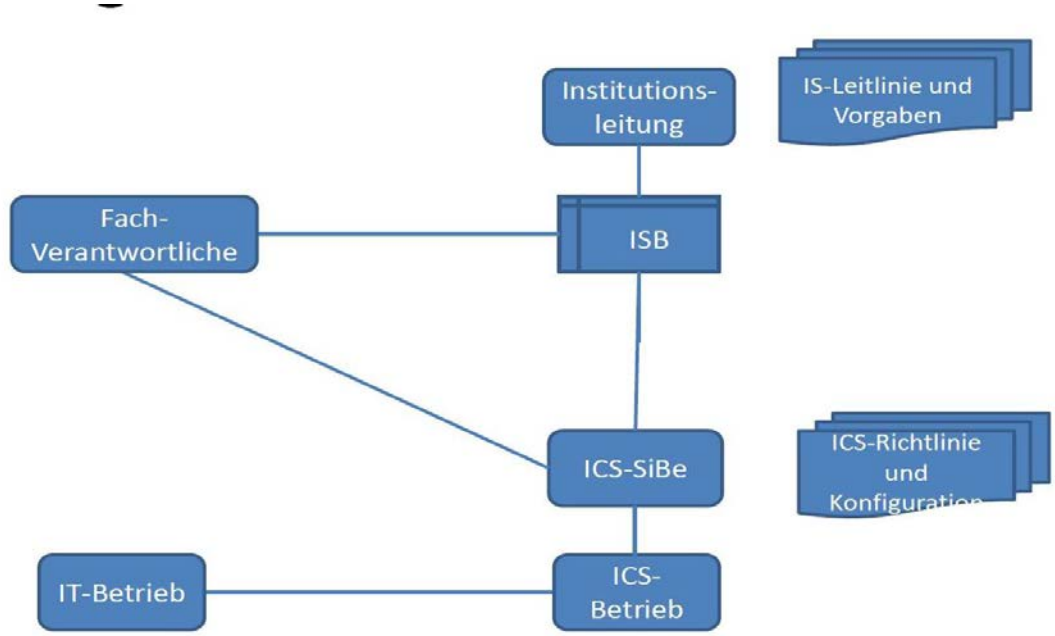


Abbildung 6: Aufbau der IS-Organisation mit integriertem ICS-Bereich

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

4.3 Aufgaben, Verantwortungen und Kompetenzen in der IS-Organisation

Der Informationssicherheit-Beauftragte und das IS-Management-Team müssen klar definierte Aufgaben, Verantwortungsbereiche und Kompetenzen haben, die von der Leitungsebene festzulegen sind. Um ihre Aufgabe wahrnehmen zu können, sollten sie bei allen relevanten Verfahren und Entscheidungen beteiligt werden. Die Rollen sind so in die Organisationsstruktur einzubinden, dass alle Beteiligten untereinander kommunizieren können. Außerdem muss geklärt sein, wer im Rahmen des Sicherheitsmanagements mit welchen internen und externen Stellen wann worüber kommuniziert sowie welche Kommunikationskanäle für die jeweiligen Ansprechpartner genutzt werden und wie diese geschützt werden (siehe hierzu auch Kapitel 5.2 *Informationsfluss im Informationssicherheitsprozess*).

Mit der Wahrnehmung der Aufgaben als Sicherheitsbeauftragte bzw. im IS-Management-Team sollte qualifiziertes Personal betraut werden. Bei Bedarf können unterstützend Aufgaben an weitere Rollen wie beispielsweise

- Bereichs-ISB (Informationssicherheitsbeauftragter für einen Bereich, Abteilung, Außenstelle, o. ä.)
- Projekt-ISB sowie
- ICS-ISB (Informationssicherheitsbeauftragter für den Bereich der industriellen Steuerung)

delegiert werden.

4.4 Der Informationssicherheitsbeauftragte

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

Die Rolle des Verantwortlichen für Informationssicherheit wird je nach Art und Ausrichtung der Institution anders genannt. Häufige Titel sind neben Informationssicherheitsbeauftragter auch Chief Information Security Officer (CISO) oder Informationssicherheitsmanager (ISM). In den IT-Grundschutz-Dokumenten wurde bisher die Bezeichnung IT-Sicherheitsbeauftragter (IT-SiBe) verwendet, da dieser Begriff in Unternehmen und Behörden lange Zeit der am weitesten verbreitete war. Mit dem Titel "Sicherheitsbeauftragter" werden dagegen häufig diejenigen Personen bezeichnet, die für Arbeitsschutz, Betriebssicherheit oder Werkschutz zuständig sind.

Aus diesen Titeln folgt aber auch häufig ein anderes Rollenverständnis. So macht der Titel Informationssicherheitsbeauftragter statt IT-Sicherheitsbeauftragter deutlich, dass diese Person sich um die Absicherung aller Arten von Informationen kümmert und nicht nur um IT-bezogene Aspekte. Informationssicherheit sollte aber immer Teil des operationellen Risikomanagements einer Institution sein. Aus diesem Grund ersetzt die Bezeichnung „Informationssicherheitsbeauftragter“ (ISB) im IT-Grundschutz in diesem Zusammenhang die Bezeichnung „IT-Sicherheitsbeauftragter“ (IT-SiBe).

Eng damit zusammen hängt auch die Frage, wo der Sicherheitsbeauftragte organisatorisch verankert ist. Es ist empfehlenswert, die Position des Informationssicherheitsbeauftragten direkt der obersten Leitungsebene zuzuordnen. Es ist davon abzuraten, den Sicherheitsbeauftragten in der IT-Abteilung zu verankern, da es hierbei zu Rollenkonflikten kommen kann.

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

Zuständigkeiten und Aufgaben

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

- den Informationssicherheitsprozess zu steuern und bei allen damit zusammenhängenden Aufgaben mitzuwirken,

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

Der ISB ist außerdem bei allen größeren Projekten, die deutliche Auswirkungen auf die Informationsverarbeitung haben könnten, zu beteiligen, um die Beachtung von Sicherheitsaspekten in den verschiedenen Projektphasen zu gewährleisten. So sollte der ISB bei der Planung und Einführung neuer Anwendungen und IT-Systeme ebenso beteiligt sein wie bei neuen ICS-Komponenten oder wesentlichen Änderungen der Infrastruktur.

Anforderungsprofil

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

- Identifikation mit den Zielsetzungen der Informationssicherheit, Überblick über Aufgaben und Ziele der Institution.
- Kooperations- und Teamfähigkeit, aber auch Durchsetzungsvermögen (Kaum eine Aufgabe erfordert so viel Fähigkeit und Geschick im Umgang mit anderen Personen: Die Leitungsebene muss in zentralen Fragen des Sicherheitsprozesses immer wieder eingebunden werden. Entscheidungen müssen eingefordert werden und die Mitarbeiter müssen, eventuell mit Hilfe des Bereichs-Sicherheitsbeauftragten, in den Sicherheitsprozess mit eingebunden werden.)
- Erfahrungen im Projektmanagement, idealerweise im Bereich der Systemanalyse und Kenntnisse über Methoden zur Risikoanalyse.
- Grundlegende Kenntnisse über die Prozesse und Fachaufgaben innerhalb der Institution und soweit erforderlich, Grundkenntnisse in den Bereichen IT und ICS.
- Ein Informationssicherheitsbeauftragter muss außerdem die Bereitschaft mitbringen, sich in neue Gebiete einzuarbeiten und Entwicklungen in der IT zu verfolgen. Er sollte sich so aus- und fortbilden, dass er die erforderlichen Fachkenntnisse für die Erledigung seiner Aufgaben besitzt.

Kooperation und Kommunikation

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

Die Kommunikationsfähigkeiten des Informationssicherheitsbeauftragten sind nicht nur gegenüber den Mitarbeitern gefordert. Genauso wichtig ist es, dass der ISB 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 den Sicherheitszielen nicht vereinbar ist.

Der Informationssicherheitsbeauftragte muss seine Kommunikationsfähigkeit derart einsetzen können, dass es in anderen Fachbereichen nicht zu Missverständnissen kommt. Hierzu ist es besonders wichtig, die jeweils anderen Sprachwelten und Kulturen zu verstehen und zu respektieren. So verwenden beispielsweise Ansprechpartner aus dem Bereich der industriellen Steuerung andere Begriffe für das IT-Equipment als IT-Experten.

Unabhängigkeit

Es ist empfehlenswert, die Position des Informationssicherheitsbeauftragten organisatorisch als Stabsstelle einzurichten, also als eine direkt der Leitungsebene zugeordnete Position, die von keinen anderen Stellen Weisungen bekommt. In jedem Fall muss der ISB das direkte und jederzeitige Vorspracherecht bei der Behörden- bzw. Unternehmensleitung haben, um diese über Sicherheitsvorfälle, -risiken und –maßnahmen informieren zu können. Er muss aber auch über das Geschehen in der Institution, soweit es einen Bezug zu seiner Tätigkeit hat, umfassend und frühzeitig unterrichtet werden.

Der Informationssicherheitsbeauftragte sollte nicht organisatorisch der IT-Abteilung zugeordnet sein. Die Erfahrung zeigt, dass dies häufig dazu führt, dass die Aufgabe Informationssicherheit auf IT-Absicherung reduziert wird und der ganzheitliche Schutz von Informationen in den Hintergrund gerückt wird. Dadurch kann es vorkommen, dass Informationen solange angemessen geschützt werden, wie sie ausschließlich auf IT-Systemen verarbeitet werden, aber sie beispielsweise nach dem Ausdrucken ungeschützt am Drucker liegenbleiben. Ein anderes Problem ist der inhärente Aufgabenkonflikt. Es ist z. B. problematisch, wenn ein "aktiver" Administrator die Rolle des Informationssicherheitsbeauftragten zusätzlich zu seinen normalen Aufgaben wahrnimmt, da es mit hoher Wahrscheinlichkeit zu Interessenskonflikten kommen wird. Die Personalunion kann dazu führen, dass er als Informationssicherheitsbeauftragter Einspruch gegen Entscheidungen einlegen müsste, die ihm sein Leben als Administrator wesentlich erleichtern würden oder die gar von seinem Fachvorgesetzten stark favorisiert werden (siehe auch Kapitel 4.10 *Zusammenspiel mit anderen Organisationseinheiten und Managementdisziplinen*).

Personalunion mit dem Datenschutzbeauftragten

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

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

Es darf nicht vergessen werden, dass auch der Informationssicherheitsbeauftragte einen qualifizierten Vertreter benötigt.

4.5 Das IS-Management-Team

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

Aufgaben des IS-Management-Teams sind insbesondere:

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

Zusammensetzung des Teams

Um seine Aufgaben erfüllen zu können, sollte sich das IS-Management-Team aus Personen zusammensetzen, die Kenntnisse in Informationssicherheit, technische Kenntnisse über die in der Institution eingesetzen IT-, ICS- und IoT-Systeme sowie Erfahrung mit Organisation und Verwaltung haben. Darüber hinaus sollte das IS-Management-Team die unterschiedlichen Aufgabenbereiche und Geschäftsprozesse einer Institution kennen. In großen Institutionen ist es sinnvoll, wenn die verschiedenen Fachbereiche einer Institution jeweils einen Vertreter im IS-Management-Team haben. Diese Person übernimmt die Vertretung im IS-Management-Team neben ihren Fachaufgaben, bringt die Expertise aus dem Fachbereich ein und wird dadurch gleichzeitig Ansprechpartner für Sicherheitsfragen der Mitarbeiter aus diesem Bereich.

4.6 Bereichs- und Projekt-Sicherheitsbeauftragte bzw. Beauftragter für IT-Sicherheit

Bei großen Institutionen kann es erforderlich sein, in den verschiedenen Bereichen eigene Sicherheitsbeauftragte einzusetzen.

Bereichs-Sicherheitsbeauftragter

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

Beauftragter für IT-Sicherheit

In großen Institutionen kann es auch einen Beauftragten für die IT-Sicherheit geben, der für die Sicherheit der IT zuständig ist. Der ISB gestaltet das Informationssicherheitsmanagement und erstellt die generellen Sicherheitsziele und -vorgaben, ein Beauftragter für die IT-Sicherheit sorgt dafür, dass diese technisch umgesetzt werden. Ein Beauftragter für die IT-Sicherheit ist typischerweise im IT-Betrieb tätig, während der ISB unmittelbar der Leitungsebene zuarbeitet.

Projekt-Sicherheitsbeauftragter

Für große Projekte sollte ein Projekt-Sicherheitsbeauftragter benannt werden, um sowohl den Sicherheitsbedarf innerhalb des Projektes zu klären als auch die sichere Einbindung der Projektergebnisse in die Geschäftsprozesse der Institution zu ermöglichen. Der Projekt-Sicherheitsbeauftragter kann ein Mitarbeiter des Projektes oder ein Mitglied des IS-Management-Teams sein. Die Verantwortung für Informationssicherheit liegt immer beim Projektleiter bzw. der

Leitungsebene. Der ISB bzw. der Projekt-Sicherheitsbeauftragte unterstützt die Projektleitung in Fragen der Informationssicherheit. Dementsprechend müssen auch durch die Projektleitung die erforderlichen Ressourcen für Informationssicherheit eingeplant und bereitgestellt werden.

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

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

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

Folgende Qualifikationen sollten vorhanden sein:

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

4.7 Der ICS-Informationssicherheitsbeauftragte (ICS-ISB)

Institutionen mit industriellen Steuerungskomponenten (ICS) sollten aufgrund gesetzlicher und organisatorischer Maßnahmen einen Verantwortlichen für die Umsetzung von Anforderungen der Informationssicherheit für diesen Bereich benennen.

Industrielle Steuerungssysteme bringen zahlreiche Sicherheitsanforderungen mit sich, die sich grundlegend von denen der allgemeinen Büro-IT unterscheiden. Im ICS-Bereich werden IT-Systeme und Anwendungen oftmals über einen sehr langen Zeitraum eingesetzt. Der Lebenszyklus dieser Objekte beträgt häufig mehr als 10 Jahre.

Innerhalb von ICS-Bereichen finden aber auch vermehrt Anwendungen und IT-Systeme aus dem Bereich der Büro-IT Einsatz. Diese werden jedoch für ihren Anwendungszweck länger als die in Büro-Umgebungen übliche Zeitdauer verwendet.

Um die speziellen Anforderungen im Bereich der industriellen Steuerung abzudecken und um die Sicherheitsorganisation aus dem Bereich der industriellen Steuerung in das Gesamt-ISMS einzubinden, sollte die Institution einen ICS-Informationssicherheitsbeauftragten (ICS-ISB) benennen. Dieser sollte Mitglied im IS-Management-Team sein. Außerdem sollte er im IS-Koordinierungsausschuss (siehe Kapitel 4.8 *IS-Koordinierungsausschuss*) vertreten sein. Zwar betrifft das Thema der industriellen Steuerung nicht alle Bereiche, aber aufgrund möglicher Veränderungen in der Büro-IT können Synergien für die produzierenden Bereiche ausgenutzt werden.

Je nach Größe der Institution kann es sinnvoll sein, die Aufgaben für das Gesamt-ISMS und das ISMS im ICS-Bereich auf verschiedene personelle Ressourcen aufzuteilen.

Die Sicherheitsorganisation der industriellen Steuerung sollte in die Sicherheitsorganisation der gesamten Institution eingebunden und betrieben werden. Um Synergien zu nutzen und Fehlplanungen sowie Risiken zu vermeiden, muss eine enge Kooperation zwischen dem ICS-ISB und dem ISB stattfinden. Weitere Ansprechpartner innerhalb der Institution sind insbesondere die Mitarbeiter der Haustechnik und die IT-Experten.

Welche Struktur für eine Sicherheitsorganisation im Bereich ICS geeignet ist, hängt stark von den vorhandenen Strukturen und eingespielten Prozessen in einer Institution ab. Grundlegend muss die Kommunikation zwischen allen beteiligten Parteien sichergestellt werden. Alle Parteien müssen ein grundlegendes Verständnis für die jeweiligen Besonderheiten des anderen Bereichs aufbringen. Nur durch vorangegangenes Verständnis für die Kultur und Sprache der jeweiligen Bereiche können Missverständnisse vermieden werden.

Als Aufgaben des ICS-Informationssicherheitsbeauftragten sind festzuhalten:

- die allgemein gültigen Sicherheitsvorgaben der Informationssicherheitsleitlinie und weiterer Richtlinien im Bereich ICS umsetzen,
- gemeinsame Ziele aus dem Bereich der industriellen Steuerung und dem Gesamt-ISMS verfolgen und Projekte aktiv unterstützen,
- für den ICS-Bereich Risikoanalysen durchführen, die den Vorgaben des Risikomanagements entsprechen,
- Sicherheitsrichtlinien und Konzepte für den ICS-Bereich unter Einbeziehung der Anforderungen aus Safety und Security erstellen und schulen,
- eng mit dem Informationssicherheitsbeauftragten kooperieren,
- als Ansprechpartner für ICS-Sicherheit für die Mitarbeiter vor Ort und in der gesamten Institution dienen,
- ICS-Sicherheitsmaßnahmen erstellen und bei der Umsetzung mitwirken,
- notwendige Dokumente zur ICS-Sicherheit erstellen und diese kommunizieren,
- Informationen über Schulungs- und Sensibilisierungsbedarf der Beschäftigten im ICS-Bereich ermitteln und Aktivitäten initiieren, und
- Sicherheitsvorfälle im ICS-Bereich zusammen mit dem Informationssicherheitsbeauftragten bearbeiten.

Folgende Qualifikationen sollten beim ICS-ISB vorhanden sein:

- spezielle Kenntnisse zu den Prozessen innerhalb der Institution und der industriellen Steuerung,
- ausreichende IT-Kenntnisse, um Fragen der Mitarbeiter vor Ort, der IT-Experten und weiterer Parteien umfassend beantworten zu können,
- Kenntnisse zu Bedrohungen und Schwachstellen innerhalb der industriellen Steuerung,
- Kenntnisse zu Gefährdungen für die Büro-IT, die innerhalb des ICS-Bereichs eingesetzt wird,
- Kenntnisse zum Projektmanagement, sowie
- Kenntnisse zu den Themen Change Management und Notfallmanagement.

4.8 IS-Koordinierungsausschuss

Der IS-Koordinierungsausschuss ist in der Regel keine Dauereinrichtung in einer Institution, sondern wird bei Bedarf (z. B. zur Planung größerer Projekte) einberufen. Er hat die Aufgabe, das Zusam-

menspiel zwischen dem IS-Management-Team, den Fachverantwortlichen, dem Sicherheitsbeauftragten und der Behörden- bzw. Unternehmensleitung zu koordinieren.

Ebenso wie den IS-Koordinierungsausschuss gibt es in vielen Institutionen einen IT-Koordinierungsausschuss. Auch dieser ist keine Dauereinrichtung. Dessen Aufgabe ist es, das Zusammenspiel zwischen den Vertretern der IT-Anwender, dem ISB und der Behörden- bzw. Unternehmensleitung zu koordinieren.

Es bietet sich an, die beiden Koordinierungsausschüsse soweit möglich zusammenarbeiten zu lassen und sie auch personell weitgehend identisch zu besetzen.

Zusammensetzung des IS-Koordinierungsausschusses

Der IS-Koordinierungsausschuss sollte die unterschiedlichen Aufgabenbereiche einer Institution widerspiegeln. Im IS-Koordinierungsausschuss sollten mindestens folgende Rollen vertreten sein: ein IT-Verantwortlicher, der Informationssicherheitsbeauftragte und Vertreter der Anwender. Da häufig auch personenbezogene Daten betroffen sind, sollte der Datenschutzbeauftragte ebenfalls Mitglied des IS-Koordinierungsausschusses sein. Wenn die Institution einen ICS-Informationssicherheitsbeauftragten hat, sollte auch dieser im IS-Koordinierungsausschuss vertreten sein. Gibt es in der Institution bereits ein ähnliches Gremium, könnten dessen Aufgaben entsprechend erweitert werden. Um die Bedeutung der Informationssicherheit zu unterstreichen, ist es jedoch ratsam, einen IS-Koordinierungsausschuss einzurichten und diesen regelmäßig einzuberufen.

4.9 Der Datenschutzbeauftragte

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

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

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

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

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

Anforderungsprofil

Zum Datenschutzbeauftragten kann nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Zur Aufgabenerfüllung gehören technische, organisatorische und rechtliche Kenntnisse. Als Methodik zur effektiven und vollständigen Aufgabenerfüllung empfehlen die deutschen Datenschutz-Aufsichtsbehörden die Anwendung des Standard-Datenschutzmodells [SDM]. Der Datenschutzbeauftragte muss die jeweiligen gesetzlichen

Regelungen, bereichsspezifische datenschutzrechtliche Regelungen und die für die Institution einschlägigen Spezialvorschriften kennen und sicher anwenden können. Wichtige Rechtsnormen für den Datenschutz sind in Deutschland insbesondere das Bundesdatenschutzgesetz und die EU-Datenschutz-Grundverordnung. Der Datenschutzbeauftragte sollte ferner gute Kenntnisse der Organisation und vertiefte Kenntnisse der Informationstechnik besitzen. Soweit ihm die fachliche Qualifikation in Teilbereichen noch fehlt, ist ihm Gelegenheit zu geben, sich entsprechend weiterzubilden. Mit den Aufgaben und der Arbeitsweise seiner Behörde bzw. seines Unternehmens sollte der Datenschutzbeauftragte möglichst aus eigener Erfahrung gut vertraut sein, um seinen Kontroll- und Beratungsaufgaben nachkommen zu können.

Der Datenschutzbeauftragte muss nicht ausschließlich mit diesen Funktionen betraut sein. Je nach Art und Umfang der personenbezogenen Datenverarbeitung und der damit verbundenen Datenschutzprobleme kann es angebracht sein, ihm daneben weitere Aufgaben zu übertragen. Dies wird besonders bei kleineren Institutionen in Betracht kommen. Besonders ist darauf zu achten, dass keine Interessenkonflikte oder Abhängigkeiten entstehen, die seine Aufgabenerfüllung gefährden. Möglich ist auch die Zusammenlegung der Funktionen des Datenschutzbeauftragten mit denen des Informationssicherheitsbeauftragten, zu den Rahmenbedingungen siehe auch Kapitel 4.4 *Der Informationssicherheitsbeauftragte*.

Einbeziehungspflicht

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

Zuständigkeiten und Aufgaben

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

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

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

4.10 Zusammenspiel mit anderen Organisationseinheiten und Managementdisziplinen

In den meisten Institutionen gibt es neben dem Informationssicherheitsmanagement auch andere Bereiche, die Aufgaben im Bereich der Informationssicherheit wahrnehmen oder vergleichbare Aufgaben haben, so dass es sinnvoll ist, ein koordiniertes Vorgehen und Schnittstellen abzustimmen. Diese Bereiche sind häufig als getrennte Disziplinen und teilweise auch in anderen Organisationseinheiten organisiert. Gemeinsam ist diesen Bereichen, dass sie alle unter verschiedenen Blickwinkeln das Ziel verfolgen, Werte der Institution zu schützen. Daher führen viele dieser

Bereiche bereits "Schutz" im Namen. Beispielsweise gehören hierzu neben dem Informationssicherheitsmanagement die Themenfelder Datenschutz, Objektschutz, Personenschutz, Geheimschutz, Notfallmanagement oder Risikomanagement. So kann es neben dem Informationssicherheitsbeauftragten nicht nur einen Datenschutzbeauftragten geben, sondern außerdem noch einen Geheimschutzbeauftragten, einen Notfallbeauftragten oder einen Revisor. In Institutionen mit einem Produktionsbereich ist auch die Zusammenarbeit mit den Verantwortlichen für die Produkt- und Anlagensicherheit wichtig.

Zusammenarbeit mit dem IT-Betrieb

Viele Teilaufgaben des Sicherheitsmanagements hängen unmittelbar mit Aufgaben des IT-Betriebs zusammen. Der ISB erstellt Vorgaben für den sicheren Betrieb von IT-Systemen und Netzen, der IT-Betrieb muss diese umsetzen. Daher müssen das Sicherheitsmanagement und der IT-Betrieb eng zusammenarbeiten und sich regelmäßig über Vorgehensweisen abstimmen, ebenso wie über aktuelle Gefährdungen und neu umzusetzende Sicherheitsanforderungen. In größeren Institutionen kann es daher sinnvoll sein, als Ansprechpartner des ISB im IT-Betrieb einen Beauftragten für IT-Sicherheit zu ernennen. Dieser wird häufig als IT-Sicherheitsbeauftragter, IT-Sicherheitsmanager oder auch IT-Sicherheitskoordinator bezeichnet.

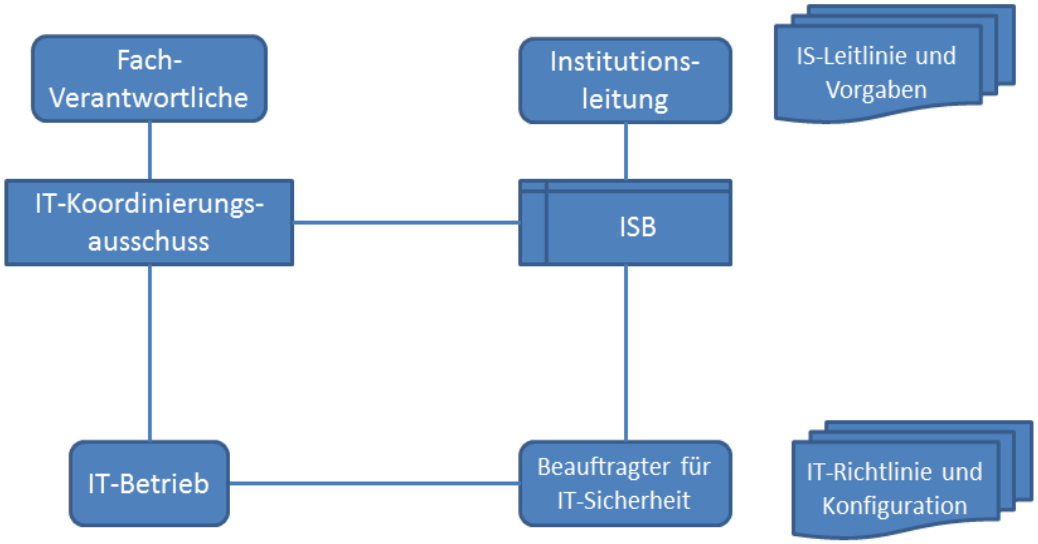


Abbildung 7: IS-Organisation und IT-Betrieb

Rollenkonflikte vermeiden

Bei der Ausgestaltung der Rollen und der Verteilung der Aufgaben ist darauf zu achten, welche Aufgaben in Personalunion wahrgenommen werden können und wo es zu Rollenkonflikten kommen kann. Aus Sicht des Informationssicherheitsmanagements ist zu klären, inwieweit der ISB weitere Rollen übernehmen kann, wie z. B. die des Notfallbeauftragten.

Diese Rollen schließen sich nicht grundsätzlich aus. Ausschlaggebend sind jedoch Faktoren wie die Größe und Ausrichtung der Institution, die Durchdringung der Geschäftsprozesse mit IT und die Ausprägung des Sicherheitsmanagements.

Grundsätzlich sind bei der Übernahme weiterer Aufgaben folgende Aspekte im Vorfeld zu klären:

- Die Schnittstellen zwischen den verschiedenen Rollen sollten klar definiert und dokumentiert werden.
- Bei Eintritt konfliktträchtiger Themen sollte eine Instanz benannt sein, die diese klären kann, z. B. die Innenrevision.
- Es muss sichergestellt sein, dass Personen mit mehreren Rollen ausreichend qualifiziert sind und genügend Ressourcen für ihre Aufgaben zur Verfügung haben.

Es gibt aber auch Rollen, die sich nicht ohne weiteres mit den Aufgaben des Informationssicherheitsmanagements kombinieren lassen. Dazu können z. B. Rollen wie Revisor oder Auditor gehören, auch das hängt aber immer vom konkreten Aufgabenumfeld ab. Grundsätzlich besteht bei einer kontrollierenden Tätigkeit immer das Problem, dass die Kontrollierenden nichts überprüfen sollten, was sie selber konzeptioniert haben.

4.11 Einbindung externer Dienstleister

Unter Umständen kann es erforderlich sein, externe Sicherheitsexperten in der internen Sicherheitsorganisation einzusetzen. Wenn wesentliche Rollen in der ISB nicht durch interne Mitarbeiter wahrgenommen werden können, müssen hierfür qualifizierte Externe beauftrag t werden. Die notwendigen Qualifikationen sind in den Abschnitten dieses Kapitels beschrieben.

Insbesondere in kleinen Unternehmen oder Behörden kann es unter Umständen zweckmäßig sein, die Rolle des Informationssicherheitsbeauftragten nicht durch einen eigenen Mitarbeiter zu besetzten, sondern hierfür auf die Dienstleistung eines externen ISB zurückzugreifen.

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

Aktionspunkte zu 4 Organisation des Sicherheitsprozesses

- Rollen für die Gestaltung des Informationssicherheitsprozesses festlegen
- Aufgaben und Verantwortungsbereiche den Rollen zuordnen
- Personelle Ausstattung der Rollen festlegen
- IS-Organisation dokumentieren
- Informationssicherheitsmanagement in die organisationsweiten Abläufe und Prozesse integrieren
- Wenn erforderlich, externe Experten hinzuziehen

5 Dokumentation im Sicherheitsprozess

Vor und während des Sicherheitsprozesses wird eine Vielzahl verschiedener Dokumente und Beschreibungen erstellt. Hierbei sollte immer darauf geachtet werden, dass der Aufwand für die Erstellung von Dokumentationen in einem angemessenen Rahmen bleibt. Die Dokumentation des Sicherheitsprozesses sollte so aussagekräftig sein, dass auch später noch nachvollziehbar ist, was zu früheren Zeitpunkten entschieden und umgesetzt wurde.

Dieses Kapitel beschreibt idealtypische Anforderungen und Methoden bei der Dokumentation des Sicherheitsprozesses. Abhängig von der gewählten IT-Grundschutz-Vorgehensweise und den vorhandenen Rahmenbedingungen kann und sollte der Dokumentationsprozess angepasst werden. Insbesondere bei der Basis-Absicherung sollte der Dokumentationsprozess möglichst einfach und zweckmäßig gehalten werden.

Wenn eine spätere Zertifizierung des ISMS angestrebt ist, müssen einige Dokumente zwingend erstellt werden (siehe Kapitel 11 *Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz*). Davon abgesehen, sollte der Dokumentationsaufwand möglichst minimiert werden. Wenn es im IT-Grundschutz heißt, dass etwas dokumentiert werden muss, ist es hierfür meistens nicht erforderlich, eigenständige Dokumente zu erstellen. Im Allgemeinen reicht es, die notwendigen Informationen an geeigneter Stelle zu notieren, beispielsweise in einem Wiki, in vorhandenen Texten oder Tabellen.

5.1 Klassifikation von Informationen

Um Informationen angemessen schützen zu können, muss deren Bedeutung für die Institution klar sein. Um sich innerhalb einer Institution, aber auch mit anderen Institutionen einfacher darüber austauschen zu können, welchen Wert bestimmte Arten von Informationen haben, wird ein Klassifikationsschema benötigt, in dem beschrieben ist, welche Abstufungen der Wertigkeit es gibt und wie die verschiedenen Stufen gegeneinander abgegrenzt sind.

Eine sinnvolle Vorgehensweise ist es daher, ein Klassifikationsschema zu erarbeiten, das es allen Mitarbeitern ermöglicht, daraus für jede Art Information die korrekte Einstufung abzuleiten, ohne dass diese dafür explizit gekennzeichnet werden muss. Das Klassifikationsschema sollte nicht zu kompliziert gewählt sein, so dass es einfach verständlich und anwendbar ist.

Es bietet es sich an, von den Grundwerten der Informationssicherheit auszugehen und Informationen in Bezug auf ihre Vertraulichkeit, Integrität und Verfügbarkeit zu klassifizieren. Je nach Institution können hier auch weitere oder andere Parameter verwendet werden, beispielsweise wenn diese bereits in der Institution in anderen Zusammenhängen verwendet wurden. Ein Nachteil davon, das Klassifikationsschema zu erweitern, ist, dass die Klassifizierung komplexer wird. Damit wird es für die Mitarbeiter schwieriger, die Abgrenzung zwischen den einzelnen Stufen nachzuvollziehen und das Schema anzuwenden. Ein weiterer Nachteil ist, dass es schwieriger ist, ein gemeinsames Verständnis über die Klassifizierung von Informationen mit anderen Institutionen aufzubauen.

Um die Vertraulichkeit zu klassifizieren, wird häufig zwischen *offen*, *intern*, *vertraulich*, und *streng vertraulich* abgestuft. Bei der Verfügbarkeit kann beispielsweise eine Klassifikation über die zu erwartende bzw. die tolerierbare Dauer bis zur Wiederherstellung bei einem Ausfall getroffen werden, etwa *eine Stunde*, *ein Tag*, *eine Woche*, *ein Monat*. Schwieriger ist es, die Integrität zu klassifizieren, etwa in *essentiell*, *wichtig* und *normal*. Kriterien können hierfür beispielsweise die möglichen Auswirkungen bei Integritätsverlust und deren Schweregrad sein oder der betriebene Aufwand zur Sicherstellung der Integrität.

In einfachen Fällen, etwa auch im Kontext der Basis-Absicherung, kann anfangs bereits eine zweistufige Klassifizierung ausreichend sein, beispielsweise indem nur zwischen internen ("alles im Intranet") und öffentlichen Informationen unterschieden wird. In diesem Fall empfiehlt es sich, die für die Veröffentlichung vorgesehenen Informationen, aber auch nur diese, als solche zu klassifizieren ("offen").

Diese Klassifikation ist eine wesentliche Voraussetzung, um später adäquate Sicherheitsmaßnahmen auszuwählen und anzuwenden.

Kennzeichnung: Es ist erstrebenswert, alle Informationen bereits bei ihrer Generierung zu kennzeichnen, um diese konsequent während ihres gesamten Lebenszyklus angemessen schützen zu können. Dies ist aber erfahrungsgemäß schwierig. Die Erfahrung zeigt, dass ein Klassifikationsschema einfach aufzubauen ist, aber es schwierig ist, dies im laufenden Betrieb am Leben zu erhalten, so dass es von allen Mitarbeitern konsequent und einheitlich angewendet wird. Außerdem ist zu berücksichtigen, dass sich die Klassifikation im Lebenszyklus der Informationen ändern kann.

Ein positiver Nebeneffekt der Klassifizierung von Daten ist, dass dabei auffällt, welche Daten überflüssig oder veraltet sind bzw. nicht genutzt werden. Konsequente Klassifikation hilft, den Datenmüll zu reduzieren.

Um einen funktionierenden Prozess zur Klassifikation von Informationen aufzubauen und zu betreiben, sollten dafür geeignete Rollen eingerichtet werden und deren Aufgaben festgelegt werden.

Die folgende Tabelle zeigt ein umfangreiches Beispiel zu möglichen Rollen, um notwendige Aufgaben zu verdeutlichen. Auch hier können in der Praxis geeignete Anpassungen vorgenommen werden. Es sollte immer mindestens die Rolle eines Verantwortlichen für den Klassifikationsprozess geben, sowie die Rollen derjenigen, die diesen Prozess einhalten bzw. umsetzen.

Rolle	**deutsche Rollenbe-zeichnung**	**Wer kann die Rolle übernehmen?**	**Aufgaben**
Data Creator	Ersteller	jeder Mitarbeiter	• erzeugt Daten • Erst-Klassifikation
Data Owner	Fachverantwort-licher	Fachverantwort-licher / Linien-Vorgesetzer	• konkretisiert Regelungen zur Klassifikation in seinem Bereich • klärt Einstufungsfragen mit Erstellern • überwacht Klassifikationsprozess seitens Ersteller
Data User	Benutzer	jeder Mitarbeiter	• benutzt Daten • beachtet Regeln zur Klassifikation • gibt Feedback zu Einstufungshöhen
Data Auditor	Klassifikations-Verantwortlicher	Anforderungs-manager / Compliance Manager	• erstellt institutionsweite Klassifikationsstrategie und -vorgaben • stellt Hilfsmittel und Erläuterungen zur Verfügung • klärt Einstufungsfragen mit Fachverantwortlichen und Benutzern • überwacht Klassifikationsprozess seitens Fachverantwortlichen • stimmt sich ab mit: Risikomanagement, ISB,

Rolle	deutsche Rollenbe-zeichnung	Wer kann die Rolle übernehmen?	Aufgaben
			Datenschutzbeauftragter

Tabelle: Aufgaben und Prozesse bei der Klassifizierung von Daten

Ein typisches Beispiel für ein Klassifikationsschema ist die im staatlichen Geheimschutz benutzte Einteilung in

- VS-NUR FÜR DEN DIENSTGEBRAUCH
- VS-VERTRAULICH
- GEHEIM
- STRENG GEHEIM

Dieses Schema fokussiert allerdings auf den kleinen Bereich der Verschlusssachen (VS), also der im öffentlichen Interesse geheimhaltungsbedürftigen Informationen oder Gegenstände. Es lässt daher große Lücken bei der Vielzahl der Informationen, die typischerweise in einem Unternehmen oder in einer Behörde anfallen, die aber ebenfalls geschützt werden müssen. In Institutionen, in denen Verschlusssachen nur einen geringen Anteil der verarbeiteten Daten darstellen, ist es daher sinnvoll, für den großen Anteil der geschäftsrelevanten und teilweise geschäftskritischen Informationen ein eigenes Klassifikationsschema zu haben.

Aktionspunkte zu 5.1 Klassifikation von Informationen

- Klassifikationsschema erstellen, das korrekte, unkomplizierte und nachvollziehbare Einstufung von Informationen ermöglicht

5.2 Informationsfluss im Informationssicherheitsprozess

In den verschiedenen Schritten des Informationssicherheitsprozesses entsteht eine Vielzahl verschiedener Berichte, Konzepte, Richtlinien, Meldungen über sicherheitsrelevante Ereignisse und weiterer Dokumente zur Informationssicherheit der Institution. Die Dokumente müssen aussagekräftig und für die jeweilige Zielgruppe verständlich sein. Da nicht alle diese Informationen für die Leitungsebene geeignet sind, ist es eine Aufgabe des ISB, diese Informationen zu sammeln, zu verarbeiten und entsprechend kurz und übersichtlich aufzubereiten.

Dieses Kapitel beschreibt umfassend die wesentlichen Aspekte bezüglich einer angemessenen Dokumentation sowie eines angemessenen Informationsflusses. Die Beachtung dieser Aspekte unterstützt bei der Erstellung einer guten Dokumentation. Sie sind bewährt und empfehlenswert und müssen den Gegebenheiten der Institution angepasst werden. Dies gilt insbesondere im Kontext der Basis-Absicherung. Im Rahmen einer Zertifizierung werden sie verbindlich, ansonsten sind sie als Best-Practise zu verstehen.

5.2.1 Berichte an die Leitungsebene

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

- Status und Umsetzungsgrad des Sicherheitskonzeptes
- Ergebnisse von Audits und Datenschutzkontrollen (siehe auch Datenschutz-Grundverordnung [DSGVO])
- Berichte über Sicherheitsvorfälle

- Berichte über bisherige Erfolge und Probleme beim Informationssicherheitsprozess
- Berichte über die Reduzierung bestehender Umsetzungsdefizite und der damit verbundenen Risiken (Risikobehandlungsplan, siehe BSI-Standard 200-3)

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

Ebenso erarbeitet der Sicherheitsbeauftragte das Sicherheitskonzept und sorgt für dessen Umsetzung und regelmäßige Aktualisierung. Die Freigabe des Sicherheitskonzepts erfolgt durch die Leitungsebene.

5.2.2 Dokumentation im Informationssicherheitsprozess

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

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

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

- Dokumente für das Sicherheitsmanagement (Zielgruppe: Sicherheitsmanagement)

Im Rahmen der verschiedenen Aktivitäten des Informationssicherheitsmanagements entstehen Konzepte, Richtlinien, Berichte und weitere Dokumente. Nur durch eine ausreichende Dokumentation werden getroffene Entscheidungen nachvollziehbar, Handlungen wiederholbar und Schwächen erkannt, so dass sie in Zukunft vermieden werden können.

Die Menge und Ausprägung der Dokumentation hängt von den Notwendigkeiten der jeweiligen Institutionen ab und kann sehr unterschiedlich sein. Beispiele für zu erstellende Dokumente sind:

  - Sicherheitskonzept mit den Berichten zur Risikoanalyse,
  - Schulungs- und Sensibilisierungskonzept,
  - Audit- oder Revisionsberichte.

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

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

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

- Anleitungen für Mitarbeiter (Zielgruppe: Mitarbeiter)

Das Dokument, das die grundlegenden Aussagen zum Umgang mit Informationssicherheit in der Institution enthält, ist die Leitlinie zur Informationssicherheit.

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

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

- Aufzeichnung von Management-Entscheidungen (Zielgruppe: Leitungsebene)

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

- Gesetze und Regelungen (Zielgruppe: Leitungsebene)

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

- Referenzdokumente für die Zertifizierung (Zielgruppe: Institutionen mit dem Ziel der Zertifizierung)

  Strebt eine Institution eine Zertifizierung an, so müssen verschiedene Dokumente für die Auditierung erstellt und aktualisiert werden. Diese Dokumente werden den Auditoren und der Zertifizierungsstelle im BSI überreicht, bewertet und darauf aufbauend die Entscheidung für oder gegen ein Zertifikat getroffen. Die erforderlichen Dokumente für die Zertifizierung werden im Internet in der Liste der Referenzdokumente gepflegt. Dazu gehören beispielsweise Richtlinien zur Risikoanalyse, zur Lenkung von Dokumenten und Aufzeichnungen, zur Auditierung des Managementsystems für Informationssicherheit und zur Lenkung von Korrektur- und Vorbeugungsmaßnahmen.

- Dokumentation im ICS-Bereich (Zielgruppe: Anwender)

  Viele der Dokumente zur Informationssicherheit aus dem IT-Bereich können für den Bereich der industriellen Steuerung übernommen werden. Einige der Dokumente aus dem IT-Bereich lassen sich jedoch nicht ohne weiteres für den Bereich der industriellen Steuerung übertragen. Hier müssen entsprechend der Anforderungen Dokumente für den ICS-Bereich neu erstellt, modifiziert oder geändert werden. Häufig ist es sinnvoll, für den Bereich der industriellen Steuerung eine abgeleitete Leitlinie für die Informationssicherheit und eigene Richtlinien und Arbeitsanweisungen zu erstellen. Zu beachten ist, dass alle abgeleiteten Dokumente in das ISMS der Institution integriert werden sollten.

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

5.2.3 Anforderungen an die Dokumentation

Eine angemessene Dokumentation des Informationssicherheitsprozesses sollte eine Reihe von Anforderungen bezüglich Kennzeichnung, Detailtiefe, Aktualisierungen, Medium, Sicherheit und Datenschutz erfüllen. Diese werden nachfolgend detailliert beschrieben.

Mindestanforderung an die Kennzeichnung der Dokumente zum Sicherheitsmanagement

Die Dokumente, die im Rahmen des Sicherheitsmanagements erstellt, bearbeitet und verwaltet werden, müssen aussagekräftig und für die jeweilige Zielgruppe verständlich sein. Es sollte, soweit

sinnvoll, ein einheitlicher Aufbau der Dokumente genutzt werden. Dies dient dem besseren Verständnis und der einfacheren Handhabung. Die Dokumente müssen so gekennzeichnet sein, dass sie im Bedarfsfall schnell gefunden und zugeordnet werden können. Daher müssen mindestens folgende Angaben vorhanden sein:

- Eindeutige Bezeichnung (aussagekräftiger Titel),
- Ersteller / Autor / Dokumenteninhaber,
- Funktion des Erstellers,
- Versionsnummer,
- letzte Überarbeitung, nächste geplante Überarbeitung,
- freigegeben am / durch,
- Klassifizierung (vertrauliche Inhalte müssen klassifiziert, als solche gekennzeichnet und die Dokumente sicher verwahrt werden) und
- berechtigte Rollen (Verteilerkreis).

Optional können folgende Informationen mit aufgenommen werden:

- Quellenangaben,
- Aufbewahrungszeitraum und
- eine Änderungsübersicht.

Externe Dokumente, die für das Sicherheitsmanagement relevant sind, müssen ebenfalls angemessen gekennzeichnet und verwaltet werden.

Detailtiefe

Für die Detailtiefe der einzelnen Dokumente gilt das Prinzip „dem Ziel und Zweck angemessen". Strategiedokumente, wie die Leitlinie, sollten kurz und prägnant, jedoch aussagekräftig gehalten werden. Die bei der Konzeption anfallenden Dokumente sollten detaillierte Informationen enthalten, um die daraus abgeleiteten Entscheidungen nachvollziehen zu können. Alle Entscheidungen sowie die Informationen, auf denen die Entscheidungen basieren, müssen dokumentiert werden.

Für Richtlinien und Handlungsanweisungen für Mitarbeiter gilt in besonderem Maße, dass sie klar und verständlich gehalten werden müssen. Oftmals sind für bestimmte Bereiche einfache Checklisten ausreichend. Diese ermöglichen einen schnellen Überblick und helfen dabei, nichts zu vergessen und die Reihenfolge einzelner Schritte einzuhalten.

Änderungsmanagement

Alle Dokumente zum Sicherheitsmanagement sollen regelmäßig aktualisiert werden. Dafür empfiehlt es sich, ein Änderungsmanagement-Verfahren aufzusetzen, mit dem alle Änderungen erfasst, bewertet, freigeben und nachvollzogen werden können. Dazu sind für alle Dokumente klare schriftliche Änderungsmanagement-Anweisungen vorzugeben. Das Verfahren sollte des Weiteren festlegen, wie Anwender Änderungsvorschläge einbringen können und wie diese dann beurteilt und gegebenenfalls berücksichtigt werden. Das Änderungsmanagement des Sicherheitsmanagements ist in das übergreifende Änderungsmanagement der Institution zu integrieren.

Für die Aktualisierung der einzelnen Dokumente sollten Intervalle vorgegeben werden. Für den überwiegenden Teil der Dokumente hat sich eine jährliche Überprüfung bewährt.

Die Mechanismen, die das Änderungsmanagement anstoßen, sind in die entsprechenden Prozesse (z. B. Personalverwaltung, Hausverwaltung, Inventarisierung) zu integrieren. Der Sicherheitsbeauftragte ist steuernd tätig. Die Verantwortung für die Aktualisierungen und Durchführung der Änderungsanforderungen für ein einzelnes Dokument trägt der jeweilige Dokumenteneigentümer.

Dokumentationsmedium

Dokumente zum Sicherheitsmanagement müssen nicht immer in Papierform vorliegen. Zur Dokumentation können auch lokale oder internetbasierte Software-Tools genutzt werden. Diese speichern alle nötigen Informationen und sind von verschiedenen Standorten aus sowie kollaborativ nutzbar.

Das Dokumentationsmedium sollte je nach Bedarf, Phase (Planung, Umsetzung oder Prüfung) oder Teilaufgabe gewählt werden. Auch die Zielpersonen der Dokumente und deren Vertrautheit mit den unterschiedlichen Medien sollte in die Überlegung eingeschlossen werden. Während die einen die Arbeit mit Papier bevorzugen, ist für die anderen das einfache Suchen oder Filtern in elektronischen Dokumenten unverzichtbar.

Sicherheit und Datenschutz

Da die Dokumente zum Sicherheitsmanagement sowohl sensitive Daten über die Institution als auch personenbezogene Daten beinhalten, muss die Informationssicherheit und der Datenschutz gewährleistet werden. Neben der Verfügbarkeit ist auch die Integrität und insbesondere die Vertraulichkeit der Dokumente zu garantieren. Die verschiedenen Dokumente des Sicherheitsmanagements sollten in Bezug auf ihre Vertraulichkeit eingestuft, entsprechend gekennzeichnet und durch geeignete Maßnahmen geschützt werden.

Die jeweils berechtigten Empfänger sollten in den Dokumenten genannt werden. Der Zugriff auf die Dokumente ist auf die Personen zu beschränken, die die enthaltenen Informationen für ihre Tätigkeit benötigen ("Need-to-know-Prinzip"). Eine sinnvolle Modularisierung der Dokumente ist daher empfehlenswert. Das ermöglicht eine auf die Empfänger ausgerichtete Verteilung der Informationen. Es sollte in der Institution einen Überblick über die Anzahl der klassifizierten Dokumente, deren Art (z. B. Papier oder DVD) und deren Verteilung geben, wie auch über deren korrekte und vollständige Aktualisierung und Vernichtung bzw. Rücknahme.

5.2.4 Informationsfluss und Meldewege

Über die verschiedenen Aktivitäten im Rahmen des Sicherheitsmanagements müssen alle Betroffenen zeitnah informiert werden. Allerdings ist es auch nicht sinnvoll, Detailinformationen über den Sicherheitsprozess beliebig zu streuen. Daher muss geklärt sein, welche Personen mit welchen internen und externen Stellen wann über welche Details des Sicherheitsprozesses kommunizieren. Außerdem muss festgelegt werden, welche Kommunikationskanäle für die jeweiligen Ansprechpartner genutzt und wie diese geschützt werden.

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

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

Nutzung von Synergieeffekten für den Informationsfluss

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

Viele Informationen, die aus Sicherheitsgründen erhoben werden, können auch zu anderen Zwecken genutzt werden. Ebenso haben Sicherheitsmaßnahmen auch andere positive Nebeneffekte, besonders die Optimierung von Prozessen zahlt sich aus. Beispielsweise ist die Bestimmung von Informationseigentümern oder die Einstufung von Informationen nach einheitlichen Bewertungskriterien für viele

Bereiche einer Institution relevant. Ein Überblick über die Abhängigkeit der Geschäftsprozesse von IT- bzw. ICS-Systemen und Anwendungen ist ebenfalls nicht nur für das Sicherheitsmanagement sinnvoll. Zum Beispiel kann dadurch häufig auch eine exakte Zuordnung von IT-Kosten, die oftmals als Gemeinkosten umgelegt werden, auf einzelne Geschäftsprozesse oder Produkte erfolgen.

Aktionspunkte zu 5.2 Informationsfluss im Informationssicherheitsprozess

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

6 Erstellung einer Sicherheitskonzeption nach der Vorgehensweise Basis-Absicherung

Die Erstellung der Sicherheitskonzeption für die Institution erfolgt nach der Vorgehensweise Basis-Absicherung, wenn die folgenden Voraussetzungen erfüllt sind:

- ein Informationssicherheitsprozess wurde initiiert,
- die Sicherheitsleitlinie und Informationssicherheitsorganisation wurden definiert,
- eine Übersicht der vorhandenen Assets der Institution wurde erstellt,
- die Basis-Absicherung wurde als IT-Grundschutz-Vorgehensweise ausgewählt.

Für die Sicherheitskonzeption sollten für die Komponenten von Geschäftsprozessen, Anwendungen und IT-Systemen organisatorische, personelle, infrastrukturelle und technische Anforderungen aus dem IT-Grundschutz-Kompendium erfüllt werden. Diese sind in Bausteine strukturiert, so dass sie modular aufeinander aufsetzen.

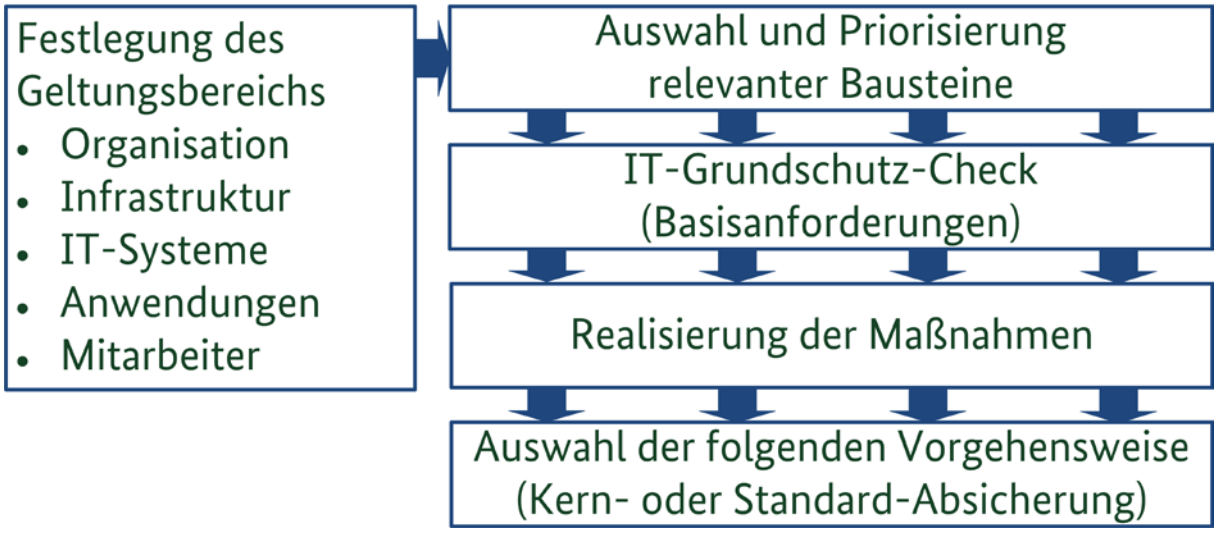


Abbildung 8: Basis-Absicherung

Die Erstellung einer Sicherheitskonzeption nach der Basis-Absicherung gliedert sich in folgende Aktionsfelder, die anschließend tiefer vorgestellt werden:

- Festlegung des Geltungsbereichs:
  Es muss der Informationsverbund festgelegt werden, für den die Sicherheitskonzeption erstellt und umgesetzt werden soll.
- Auswahl und Priorisierung:
  Der betrachtete Informationsverbund muss mit Hilfe der vorhandenen Bausteine aus dem IT-Grundschutz-Kompendium nachgebildet werden.
- IT-Grundschutz-Check:
  In diesem Schritt wird überprüft, ob die Basis-Anforderungen nach IT-Grundschutz bereits ganz oder teilweise umgesetzt sind und welche Sicherheitsmaßnahmen noch fehlen.
- Realisierung:
  Für die bisher nicht erfüllten Basis-Anforderungen müssen geeignete Sicherheitsmaßnahmen festgelegt und umgesetzt werden.
- Auswahl der folgenden Vorgehensweise:
  Die Basis-Absicherung dient als Einstiegsvorgehensweise. Es muss daher festgelegt werden, zu

welchem Zeitpunkt und mit welcher IT-Grundschutz-Vorgehensweise das Sicherheitsniveau angehoben werden soll.

Im Unterschied zur Standard-Absicherung sind die Aktionsfelder bei der Basis-Absicherung kein geschlossener Zyklus, sondern eine Einstiegsvorgehensweise, die mit der Standard-Absicherung fortgeführt werden kann (eventuell mit der Kern-Absicherung als Zwischenschritt).

6.1 Festlegung des Geltungsbereichs für die Basis-Absicherung

Bei der Erstellung einer Sicherheitskonzeption muss als erstes festgelegt werden, welchen Bereich der Institution sie abdecken soll (Geltungsbereich).

Der Geltungsbereich kann die gesamte Institution umfassen oder auch nur einzelne Bereiche. Auf jeden Fall muss der Geltungsbereich klar abgegrenzt sein und sinnvoll in sich abgeschlossen sein, mit wenigen, eindeutig definierten Schnittstellen. So könnte eine Institution beispielsweise für eine neu hinzugekommene Abteilung mit ihren Geschäftsprozessen und Assets zunächst die Basis-Absicherung umsetzen. Vertiefende Informationen zur Abgrenzung des Geltungsbereichs sind im Kapitel 3.4.3 *Festlegung des Geltungsbereichs und Inhalt der Sicherheitsleitlinie* zu finden.

Informationsverbund

Der Geltungsbereich für die Erstellung der Sicherheitskonzeption wird im Folgenden "Informationsverbund" genannt. Ein Informationsverbund umfasst die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein Informationsverbund kann dabei als Ausprägung die gesamte Informationsverarbeitung einer Institution oder auch einzelne Bereiche umfassen, die nach organisatorischen oder technischen Strukturen (z. B. Abteilungsnetz) oder gemeinsamen Geschäftsprozessen bzw. Anwendungen (z. B. Personalinformationssystem) gegliedert sind. Für die Erstellung der Sicherheitskonzeption werden auf Grundlage der bereits während der Vorarbeiten erfolgten Ersterfassung (siehe Kapitel 3.2.4 *Ersterfassung der Prozesse, Anwendungen und IT-Systeme*) die relevanten Bestandteile des betrachteten Informationsverbundes identifiziert.

6.2 Auswahl und Priorisierung für die Basis-Absicherung

Der nächste Schritt besteht darin, den betrachteten Informationsverbund mit Hilfe der in der Ersterfassung identifizierten Prozesse, Anwendungen, IT-Systeme, Kommunikationsverbindungen und Räume und den vorhandenen Bausteinen aus dem IT-Grundschutz-Kompendium nachzubilden. Das Ergebnis ist ein IT-Grundschutz-Modell des Informationsverbunds, das aus verschiedenen, gegebenenfalls auch mehrfach verwendeten Bausteinen besteht und durch die Verwendung der Bausteine die sicherheitsrelevanten Aspekten des Informationsverbunds beinhaltet.

6.2.1 Modellierung nach IT-Grundschutz

Um einen im Allgemeinen komplexen Informationsverbund nach IT-Grundschutz zu modellieren, müssen die passenden Bausteine des IT-Grundschutz-Kompendiums ausgewählt und umgesetzt werden. Um die Auswahl zu erleichtern, sind die Bausteine in dem IT-Grundschutz-Kompendium zunächst in prozess- und systemorientierte Bausteine aufgeteilt. Ein Überblick über die Struktur des IT-Grundschutz-Kompendiums mit den System- und Prozess-Bausteinen ist in Kapitel 8.3.1 *Das IT-Grundschutz-Kompendium* zu finden.

Die Modellierung nach IT-Grundschutz besteht nun darin, für die Bausteine einer jeden Schicht zu entscheiden, ob und wie sie zur Abbildung des Informationsverbunds herangezogen werden können. Je nach betrachtetem Baustein können die Zielobjekte dieser Abbildung von unterschiedlicher Art sein: einzelne Geschäftsprozesse oder Komponenten, Gruppen von Komponenten, Gebäude, Liegenschaften, Organisationseinheiten usw. Können einzelne Zielobjekte nicht mit vorhandenen Bausteinen unmittelbar abgebildet werden, muss gewährleistet sein, dass ähnliche, verallgemeinerte Bausteine berücksichtigt werden.

6.2.2 Reihenfolge der Baustein-Umsetzung

Um grundlegende Risiken abzudecken und eine ganzheitliche Informationssicherheit aufzubauen, müssen die essentiellen Sicherheitsanforderungen frühzeitig erfüllt und entsprechende Sicherheitsmaßnahmen umgesetzt werden. Daher wird im IT-Grundschutz eine Reihenfolge für die umzusetzenden Bausteine vorgeschlagen.

Im IT-Grundschutz-Kompendium wird im Kapitel *Schichtenmodell und Modellierung* beschrieben, wann ein einzelner Baustein sinnvollerweise eingesetzt werden soll und auf welche Zielobjekte er anzuwenden ist. Außerdem sind die Bausteine danach gekennzeichnet, ob sie vor- oder nachrangig umgesetzt werden sollten.

Diese Kennzeichnung zeigt nur die sinnvolle zeitliche Reihenfolge für die Umsetzung der jeweiligen Anforderungen der Bausteine auf und stellt keine Gewichtung der Bausteine untereinander dar. Grundsätzlich müssen alle für den jeweiligen Informationsverbund relevanten Bausteine des IT-Grundschutz-Kompendiums umgesetzt werden.

Die Kennzeichnung der Bausteine stellt außerdem nur eine Empfehlung dar, in welcher Reihenfolge die verschiedenen Bausteine sinnvoll umgesetzt werden könnten. Jede Institution kann hier eine abweichende, für sich sinnvolle Reihenfolge festlegen.

6.2.3 Zuordnung von Bausteinen

Die Zuordnung von Bausteinen zu Zielobjekten sollte in Form einer Tabelle mit folgenden Spalten dokumentiert werden:

- Vollständiger Titel des Bausteins (z. B. SYS.3.1 *Laptop*)
- Zielobjekt: 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 IT-Grundschutz-Check ermittelt.
- Reihenfolge: Es sollte die Umsetzungsreihenfolge (R1, R2, R3) des Bausteins eingetragen werden.
- Hinweise: In dieser Spalte können Randinformationen und Begründungen für die Modellierung dokumentiert werden.

6.2.4 Ermittlung konkreter Maßnahmen aus Anforderungen

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

Für die Erstellung eines Sicherheitskonzeptes oder für ein Audit müssen jetzt die einzelnen Anforderungen bearbeitet und zur Erfüllung geeignete Sicherheitsmaßnahmen formuliert werden, hierbei unterstützen die zu vielen Bausteinen zugehörigen Umsetzungshinweise. Vertiefende Informationen hierzu sind in Kapitel 8.3.6 *Anpassung der Baustein-Anforderungen* zu finden.

6.3 IT-Grundschutz-Check für Basis-Absicherung

Schon bevor eine IT-Grundschutz-Vorgehensweise ausgewählt wurde, wurden während der Vorarbeiten in der Erstaufnahme (siehe Kapitel 3.2.4 *Ersterfassung der Prozesse, Anwendungen und IT-Systeme*) die geschäftskritischen Informationen und Kernprozesse der Institution ermittelt und die betroffenen Anwendungen, IT-Systeme, Netze und Räume erfasst. Der betrachtete Informationsverbund wurde mit Hilfe der vorhandenen Bausteine aus dem IT-Grundschutz-Kompendium nachgebildet. Die Auswahl und Priorisierung der IT-Grundschutz-Bausteine (wie im

vorigen Kapitel beschrieben) wird nun als Prüfplan benutzt, um anhand eines Soll-Ist-Vergleichs herauszufinden, welche Basis-Anforderungen ausreichend oder nur unzureichend erfüllt sind.

Bei dem hier anzuwendenden IT-Grundschutz-Check für die Basis-Absicherung müssen nur die Basis-Anforderungen erfüllt sein. Für eine Standard- oder Kern-Absicherung ist innerhalb dieser Vorgehensweisen ein separater IT-Grundschutz-Check durchzuführen, bei dem die Standard-Anforderungen der betreffenden Bausteine hinzukommen. Um Mehraufwände zu vermeiden und Synergieeffekte erzielen zu können, sollten die Ergebnisse des für die Basis-Absicherung durchzuführenden IT-Grundschutz-Checks so aufbereitet sein, dass sie direkt in die Standard- oder Kernabsicherung integriert werden können.

Unabhängig von der IT-Grundschutz-Vorgehensweise besteht der IT-Grundschutz-Check aus drei unterschiedlichen Schritten. Im ersten Schritt werden die organisatorischen Vorbereitungen getroffen, insbesondere die relevanten Ansprechpartner für den Soll-Ist-Vergleich werden ausgewählt. Im zweiten Schritt wird der eigentliche Soll-Ist-Vergleich mittels Interviews und Stichproben durchgeführt. Im letzten Schritt werden die erzielten Ergebnisse des Soll-Ist-Vergleichs einschließlich der erhobenen Begründungen dokumentiert.

Organisatorische Vorarbeiten für den IT-Grundschutz-Check

Zunächst sollten alle hausinternen Papiere, die die sicherheitsrelevanten Abläufe regeln, gesichtet werden. Diese Dokumente können bei der Ermittlung des Umsetzungsgrades hilfreich sein.

Die geeigneten Interviewpartner müssen identifiziert werden. Für jeden Baustein, der für die Modellierung des Informationsverbunds herangezogen wurde, sollte ein Hauptansprechpartner festgelegt werden. Bei den Anforderungen in den Bausteinen werden die Rollen genannt, die für die Umsetzung der Anforderungen zuständig sind. Hieraus können die geeigneten Ansprechpartner für die jeweilige Thematik in der Institution identifiziert werden. Für die Bausteine der Schicht APP *(Anwendungen)* sind dies beispielsweise die Betreuer der einzelnen Anwendungen.

Als Nächstes sollte festgestellt werden, ob und in welchem Umfang externe Stellen bei der Ermittlung des Umsetzungsstatus beteiligt werden müssen. Dies kann beispielsweise bei Firmen, die Teile von Geschäftsprozessen oder des IT-Betriebes als Outsourcing-Dienstleistung übernehmen, erforderlich sein.

Für die anstehenden Interviews 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.

Durchführung des Soll-Ist-Vergleichs

Bei der Erhebung des erreichten Sicherheitsstatus werden die Sicherheitsanforderungen des jeweiligen Bausteins der Reihe nach durchgearbeitet. Diese können vollständig, teilweise oder nicht erfüllt sein. Als Umsetzungsstatus ist daher jeweils eine der folgenden Aussagen möglich:

"entbehrlich"	Die Erfüllung der Anforderung ist in der vorgeschlagenen Art nicht notwendig, weil die Anforderung im betrachteten Informationsverbund nicht relevant ist (z. B. weil Dienste nicht aktiviert wurden).
"ja"	Zu der Anforderung wurden geeignete Maßnahmen vollständig, wirksam und angemessen umgesetzt.
"teilweise"	Die Anforderung wurde nur teilweise umgesetzt.
"nein"	Die Anforderung wurde noch nicht erfüllt, also geeignete Maßnahmen sind größtenteils noch nicht umgesetzt.

Es ist sinnvoll, bei den Interviews nicht nur die Bausteintexte, sondern auch die Umsetzungshinweise oder andere ergänzende Materialien griffbereit zu haben. Den Befragten sollte der Zweck des IT-Grundschutz-Checks kurz vorgestellt werden. Es bietet sich an, mit den Anforderungsüberschriften fortzufahren und die Anforderung kurz zu erläutern. Dem Gesprächspartner sollte die Möglichkeit

gegeben werden, auf die bereits umgesetzten Anforderungen und Maßnahmen einzugehen, und danach noch offene Punkte zu besprechen.

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

Dokumentation der Ergebnisse

Die Ergebnisse des IT-Grundschutz-Checks sollten so dokumentiert werden, dass sie für alle Beteiligten nachvollziehbar sind und als Grundlage für die Umsetzungsplanung der defizitären Anforderungen und Maßnahmen genutzt werden können. Es sollten geeignete Hilfsmittel genutzt werden, die bei der Erstellung und Aktualisierung aller im Sicherheitsprozess erforderlichen Dokumente unterstützen, beispielsweise spezielle IT-Grundschutz-Tools oder selbst entwickelte Tabellen. Als Hilfsmittel stehen auch auf den IT-Grundschutz-Webseiten Formulare für die jeweiligen Bausteine zur Verfügung.

Die Ergebnisse des Soll-Ist-Vergleichs sollten tabellarisch erfasst werden. Dabei sollten zu jeder Anforderung des jeweiligen Bausteins folgende Informationen festgehalten werden:

- Umsetzungsgrad (entbehrlich/ja/teilweise/nein)
- Verantwortliche: Welche Mitarbeiter sind für die vollständige Umsetzung einer defizitären Anforderung verantwortlich? Bis wann ist diese umzusetzen?
- Bemerkungen: Ein solches Feld ist wichtig, um getroffene Entscheidungen später nachvollziehen zu können. Bei Anforderungen, deren Umsetzung entbehrlich erscheint, ist hier die Begründung zu nennen. Bei Anforderungen, die noch nicht oder nur teilweise umgesetzt sind, sollte in diesem Feld dokumentiert werden, welche Maßnahmen noch umgesetzt werden müssen. In dieses Feld sollten auch alle anderen Bemerkungen eingetragen werden, die bei der Beseitigung von Defiziten hilfreich oder im Zusammenhang mit der Anforderung zu berücksichtigen sind.
- Defizite / Kostenschätzung: Für Anforderungen, die nicht oder nur teilweise erfüllt wurden, ist das damit verbundene Risiko in geeigneter Form zu ermitteln und zu dokumentieren. Außerdem sollte geschätzt werden, welchen finanziellen und personellen Aufwand die Beseitigung der Defizite erfordert.

Diese Schritte werden detailliert im Kapitel 8.4 *IT-Grundschutz-Check* beschrieben.

6.4 Realisierung

In diesem Kapitel wird beschrieben, wie für die Basis-Absicherung aus den Anforderungen die Sicherheitsmaßnahmen abgeleitet und wie diese dann geplant, durchgeführt, begleitet und überwacht werden können. Es liegen die Ergebnisse des IT-Grundschutz-Checks, also des Soll-Ist-Vergleichs, vor.

Generell müssen für die Basis-Absicherung alle identifizierten Basis-Anforderungen erfüllt werden. Auch für die Erfüllung der Basis-Anforderungen stehen in der Regel nur beschränkte Ressourcen an Geld und Personal zur Verfügung. Ziel der nachfolgend beschriebenen Schritte ist daher, eine möglichst effiziente Erfüllung der vorgesehenen Basis-Anforderungen zu erreichen, eine vollständige Beschreibung für alle IT-Grundschutz-Vorgehensweisen ist im Kapitel 9 *Umsetzung der Sicherheitskonzeption* zu finden:

- Sichtung der Untersuchungsergebnisse:
  In einer Gesamtsicht sollten zuerst die fehlenden oder nur teilweise erfüllten Basis-Anforderungen ausgewertet werden.
- Konsolidierung der Basis-Anforderungen
  In diesem Schritt werden zunächst die noch zu erfüllenden Basis-Anforderungen konsolidiert.
- Kosten- und Aufwandsschätzung
  Es sollte für jede zu erfüllende Basis-Anforderung festgehalten werden, welche Investitionskosten und welcher Personalaufwand dafür benötigt werden.

- Festlegung der Umsetzungsreihenfolge der Basis-Anforderungen:
  Wenn das vorhandene Budget oder die personellen Ressourcen nicht ausreichen, um sämtliche fehlenden Basis-Anforderungen sofort erfüllen zu können, muss eine Umsetzungsreihenfolge festgelegt werden.
- Festlegung der Aufgaben und der Verantwortung
  Es muss festgelegt werden, wer bis wann welche Basis-Anforderungen erfüllen muss.
- Realisierungsbegleitende Basis-Anforderungen
  Überaus wichtig ist es, notwendige realisierungsbegleitende Basis-Anforderungen, wie Schulungen, rechtzeitig zu konzipieren und für die Realisierung mit einzuplanen.

6.5 Auswahl einer folgenden Vorgehensweise

Informationssicherheit muss gelebt werden. Um das Sicherheitsniveau aufrecht zu erhalten und kontinuierlich verbessern zu können, müssen nicht nur die erforderlichen Sicherheitsmaßnahmen umgesetzt und fortlaufend aktualisiert werden, sondern auch der gesamte Prozess der Informationssicherheit muss regelmäßig auf seine Wirksamkeit und Effizienz hin überprüft werden.

Die Basis-Absicherung ist eine IT-Grundschutz-Vorgehensweise für den Einstieg, um zunächst zeitnah die wichtigsten Sicherheitsempfehlungen für den ausgewählten Einsatzbereich identifizieren und umsetzen zu können. Ziel ist es daher, mittelfristig ein vollständiges Sicherheitskonzept gemäß der Standard-Absicherung zu erstellen. Als Zwischenschritt könnte nach der Basis-Absicherung und vor der Standard-Absicherung die nun erstellte Sicherheitskonzeption um die Kern-Absicherung ergänzt werden.

Nachdem die Basis-Absicherung realisiert wurde, sollte zeitnah entschieden werden, wann mit dem notwendigen Verbesserungsprozess begonnen wird. In Abhängigkeit der Sicherheitsansprüche und der verfügbaren Ressourcen ist zu entscheiden, ob im nächsten Schritt eine Sicherheitskonzeption nach der Standard- oder der Kern-Absicherung erstellt werden soll. Informationen zur Auswahl sind in Kapitel 3.3 *Entscheidung für Vorgehensweise* zu finden.

7 Erstellung einer Sicherheitskonzeption nach der Vorgehensweise Kern-Absicherung

Der IT-Grundschutz des BSI bietet einen ganzheitlichen Schutz aller geschäftsrelevanten Informationen einer Institution. Für Institutionen, die noch großen Handlungsbedarf im Bereich Informationssicherheit haben, kann es zielführend sein, sich anfangs auf die Absicherung der essentiellen Assets zu beschränken und erst nachfolgend Sicherheit in der Breite umzusetzen. Dieses Kapitel beschreibt, wie vorzugehen ist, wenn als Vorgehensweise die Kern-Absicherung ausgewählt wurde.

Nachdem ein Informationssicherheitsprozess initiiert, die wesentlichen Rahmenbedingungen sowie die zu schützenden Prozesse, Anwendungen und IT-Systeme identifiziert wurden sowie eine Vorgehensweise ausgewählt wurde, wird die Sicherheitskonzeption für die Institution erstellt. Zu diesem Zweck werden im IT-Grundschutz-Kompendium für typische Komponenten von Geschäftsprozessen, Anwendungen, IT-Systemen und anderen Objekten organisatorische, personelle, infrastrukturelle und technische Standard-Sicherheitsanforderungen gestellt. Diese sind in Bausteinen strukturiert, so dass sie modular aufeinander aufsetzen.

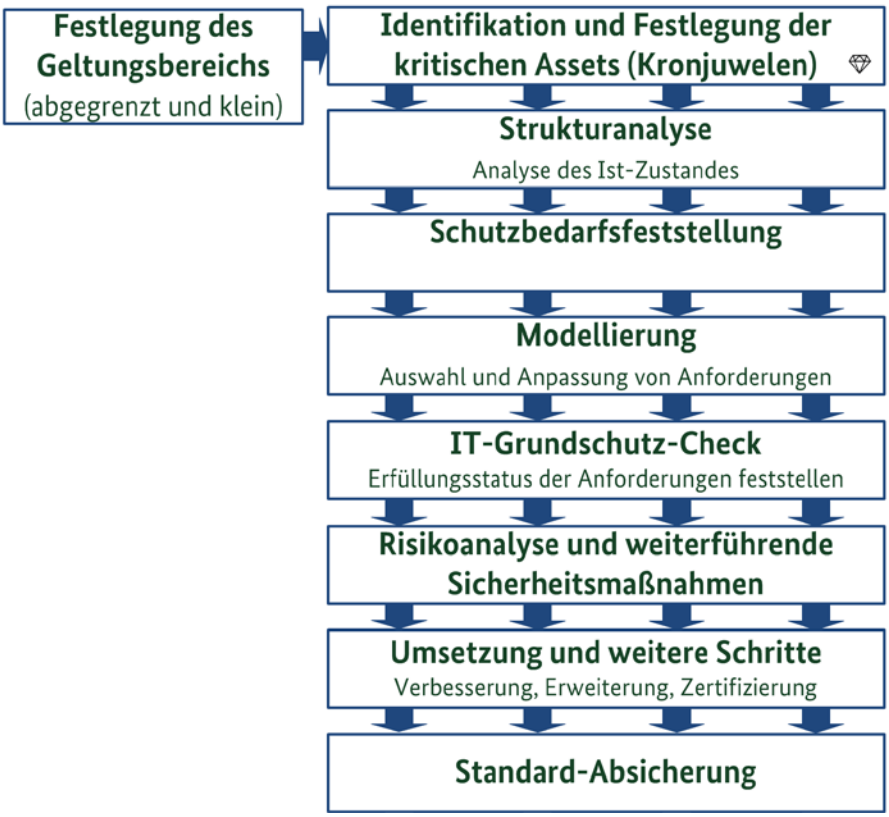


Abbildung 9: Kern-Absicherung

7.1 Die Methodik der Kern-Absicherung

Die Vorgehensweise "Kern-Absicherung" des IT-Grundschutzes konzentriert sich auf den Schutz von besonders schützenswerten Assets, den sogenannten "Kronjuwelen". Bei Anwendung der Kern-Absicherung erfolgt ein Soll-Ist-Vergleich zwischen den im IT-Grundschutz-Kompendium aufgestellten und den bereits in der Institution erfüllten Anforderungen für die Absicherung dieser Kronjuwelen. Dabei nicht oder nur unzureichend erfüllte Anforderungen zeigen die Sicherheitsdefizite auf, die es durch entsprechende Maßnahmen zu beheben gilt.

Das mit der Kern-Absicherung erstellte Sicherheitskonzept ist die Basis für ein umfangreicheres Sicherheitskonzept, wie es mit der Standard-Absicherung (siehe Kapitel 8) erstellt und etabliert werden kann.

Da sich die Kern-Absicherung auf die besonders schützenswerten Assets konzentriert, ist hier grundsätzlich von einem erhöhten Schutzbedarf auszugehen. Daher müssen die in den relevanten Bausteinen des IT-Grundschutz-Kompendiums aufgeführten Basis- und Standard-Anforderungen komplett umgesetzt werden. Darauf aufbauend muss bei erhöhtem Schutzbedarf eine Risikoanalyse unter Beachtung von Kosten- und Wirksamkeitsaspekten durchgeführt werden, damit ganzheitlich die relevanten Risiken im Bereich der Kronjuwelen behandelt werden können. Dabei können die in den Bausteinen exemplarisch aufgeführten Anforderungen für erhöhten Schutzbedarf als Grundlage genommen werden, um entsprechende individuelle Maßnahmen zu ergänzen.

Hierzu ist im BSI-Standard 200-3 *Risikoanalyse auf der Basis von IT-Grundschutz* eine im Vergleich zu traditionellen Risikoanalyse-Methoden einfachere Vorgehensweise beschrieben.

Die Kern-Absicherung, bei der der Schutz von Kronjuwelen im Fokus steht, ist kein alleinstehendes Projekt, sondern Teil des Sicherheitsprozesses. Die Kern-Absicherung kann nur dann als Projekt betrachtet werden, wenn sie anschließend in die Standard-Absicherung integriert wird. Solange dies nicht der Fall ist, muss regelmäßig der Prozess Kern-Absicherung überprüft und verbessert werden.

Die Erstellung einer Sicherheitskonzeption für eine Kern-Absicherung nach IT-Grundschutz gliedert sich grob in folgende Bereiche:

- Festlegung des Geltungsbereichs für die Kern-Absicherung
- Identifikation und Festlegung der kritischen Assets (Kronjuwelen)
- Strukturanalyse
- Schutzbedarfsfeststellung
- Modellierung: Auswahl und Anpassung von Anforderungen
- IT-Grundschutz-Check
- Risikoanalyse und weiterführende Sicherheitsmaßnahmen
- Umsetzung und weitere Schritte

7.2 Festlegung des Geltungsbereichs für die Kern-Absicherung

Die ganzheitliche Umsetzung von Informationssicherheit, wie dies mit der Standard-Absicherung erfolgt, ist in einem einzelnen großen Schritt oft ein zu ehrgeiziges Ziel. Viele kleine Schritte und ein langfristiger, kontinuierlicher Verbesserungsprozess ohne hohe Investitionskosten zu Beginn sind oft Erfolg versprechender. Daher konzentriert sich die Kern-Absicherung auf die besonders schützenswerten Assets und Ressourcen der Institution. Von diesem ausgewählten und beschränkten Bereich der Institution ausgehend sollte dann kontinuierlich die Sicherheit in der Gesamtinstitution verbessert werden.

Zunächst muss daher dieser Bereich festgelegt werden, für den die Sicherheitskonzeption erstellt und umgesetzt werden soll. Dieser umfasst unter anderem alle (Teil-)Geschäftsprozesse, Anwendungen, IT-Systeme, Infrastrukturen, die für die Bearbeitung der besonders kritischen Geschäftsprozesse und Informationen benötigt werden. Dazu gehören unter Umständen auch ICS-Systeme. Der betrachtete Geltungsbereich für die Sicherheitskonzeption wird im IT-Grundschutz generell als "Informationsverbund" bezeichnet. Die Kern-Absicherung betrachtet somit einen bewusst eingeschränkten Informationsverbund.

Bei der Kern-Absicherung ist es besonders wichtig, den Informationsverbund nicht nur klar abzugrenzen, sondern ihn auch möglichst klein zu halten. Jedes weitere Zielobjekt, das einem Informationsverbund hinzugefügt wird, erhöht die Komplexität der Absicherung. Daher kann es in Zweifelsfällen zielführender sein, die kritischen Objekte in kleinen, überschaubaren Bereichen zu betreiben, die vom Rest der Institution abgeschottet sind. Beispielsweise ist es sinnvoller, geschäftskritische Informationen in getrennten IT-Umgebungen zu verarbeiten und dafür Unbequemlichkeiten in Kauf zu nehmen, statt die im höchsten Maße schutzbedürftigen

Geschäftsprozesse mit vielen Anwendungen aus der gewohnten Büroumgebung zu verknüpfen und damit alle mit ihnen vernetzten Komponenten auf dem dann erforderlichen hohen Sicherheitsniveau absichern zu müssen.

7.3 Identifikation und Festlegung der kritischen Assets (Kronjuwelen)

Als Kronjuwelen werden diejenigen Geschäftsprozesse und die Informationen bezeichnet, die am wichtigsten für den Erhalt der Institution sind. Es ist wichtig, die mögliche Menge der schützenswerten Daten gezielt einzugrenzen.

Zu den kritischen Assets gehören üblicherweise:

- Informationen, die wesentlich zur erfolgreichen Durchführung von essentiellen Geschäftsprozessen sind.
- Informationen und Geschäftsprozesse, die ein deutlich erhöhtes Gefährdungspotential bezüglich der Informationssicherheit haben. Dies betrifft Vertraulichkeit, Integrität UND Verfügbarkeit.
- Informationen und Geschäftsprozesse, deren Diebstahl, Zerstörung, Kompromittierung oder Beeinträchtigung einen existenzbedrohenden Schaden für die Institution bedeutet und die vorrangig geschützt werden sollen.

Die folgenden weiteren Charakteristika für Kronjuwelen helfen bei der Identifikation und Eingrenzung der kritischen Assets:

- Als Kronjuwelen werden Informationen oder Geschäftsprozesse bezeichnet, nicht Dienstleistungen, Anwendungen, IT-Systeme oder ähnliche Objekte.
- Die Menge der Informationen und Geschäftsprozesse mit deutlich erhöhtem Schutzbedarf ist überschaubar bzw. umfasst nur einen kleinen Anteil aller Geschäftsprozesse der Institution. Nur wenige Assets ragen in ihrer Bedeutung für die Fachaufgaben bzw. Geschäftstätigkeit deutlich aus der Masse heraus und können einen hohen Schaden für die Institution verursachen.
- Kronjuwelen können auch in Formen vorliegen, die nicht auf den ersten Blick offensichtlich sind: es können einzelne Dateien, Datensammlungen, strukturierte oder unstrukturierte Informationen bis hin zu handschriftlichen Notizen oder Gesprächen sein, aber auch Wissen und Fähigkeiten einzelner Mitarbeiter können dazu gehören.
- Kronjuwelen sind häufig die Informationen, für die es wünschenswert erscheint, das vorhandene Klassifikationsschema um noch höhere Kategorien zu erweitern.
- Es ist davon auszugehen, dass der Schutzbedarf der Kronjuwelen und aller damit verknüpften Ressourcen im Informationsverbund mindestens "hoch" ist.
- Der Schutzbedarf von Kronjuwelen kann sich mit der Zeit verändern. Typisches Beispiel sind hier Informationen über Produktneuerungen oder Jahresabschluss-Berichte.
- Es muss bei Kronjuwelen häufig zwischen verschiedenen "Besitzern" der Information unterschieden werden. Diese können unterschiedliche Rollen und Verantwortlichkeiten haben. Insbesondere betrifft dies "Zuständigkeit" (Responsibility) versus "Rechenschaftspflicht" (Accountability).
- Der Schutzbedarf von Kronjuwelen kann sogar als so hoch eingestuft sein, dass die Sicherheitsbeauftragten nicht die Berechtigungen bekommen, diese selber einzusehen, aber den Auftrag haben, sie zu schützen.
- Es sind alle elementaren Gefährdungen des IT-Grundschutz-Kompendiums relevant, häufig liegt ein besonderer Fokus auf Angreifer. Darüber dürfen aber Ursachen wie Umwelteinflüsse oder menschliche Fehlhandlungen nicht vergessen werden.

Die Festlegung, bei welchen Assets es sich um Kronjuwelen handelt, erfolgt typischerweise durch die Leitungsebene. Die Entscheidung, bestimmte Informationen als Kronjuwelen einzustufen, führt

unmittelbar dazu, dass adäquate Sicherheitsmaßnahmen für diese ergriffen werden müssen. Diese sind natürlich entsprechend dem herausragenden Schutzbedarf der Kronjuwelen folgend umfangreich und damit tendenziell aufwändig und teuer. Fachverantwortliche, Sicherheitsbeauftragte und andere Instanzen können vorschlagen, diese Informationen als Kronjuwelen einzustufen, die Entscheidung muss durch die Leitungsebene erfolgen.

Jede Institution sollte zur besseren Einordnung für sich individuell Beispiele für Kronjuwelen erarbeiten. Außerdem sollten auch Beispiele zur Abgrenzung von Kronjuwelen zu wichtigen Informationen erstellt werden. Nachfolgend sind einige typische Beispiele für Kronjuwelen aus der Praxis aufgeführt:

- Details über anstehende geschäftliche Entscheidungen, z. B. Strategiepapiere für Firmenaufkäufe, Finanzierungspläne.
- Details über Produktentwicklungen, z. B. Hintergrundmaterial zu Patentanträgen, Designentwürfe, und so weiter.
- Informationen über Standorte geschützter Pflanzen, gefährdeter Personen oder geheimer Anlagen.
- Administrative Zugriffsdaten für Server (wenn nicht auffindbar, ist kein schneller Zugriff möglich).
- Kryptomaterial, z. B. Masterschlüssel für institutionsweit eingesetzte kryptographische Verfahren.
- Baupläne oder Rezepturen für Produkte.

Anmerkung: Das geheime Familienrezept einer Koffein-Brause ist ein in der Öffentlichkeit immer wieder thematisiertes Beispiel für ein "Kronjuwel". Wird dies offengelegt (Verlust der Vertraulichkeit), würde das einen großen Pressewirbel auslösen, aber die Existenz der Firma nicht gefährden, sondern eventuell sogar zur Produktwerbung beitragen. In diesem Kontext wird auch deutlich, dass manche Kronjuwelen zu "heiß" sein können, um für einen Angreifer oder Konkurrenten wertvoll zu sein. Eine unbemerkte Änderung der Rezepturen (Verlust der Integrität) könnte aber zu einem schweren Imageschaden führen. Der vollständige Verlust der Rezeptur würde schließlich zu einem Produktionsstillstand führen und wäre damit das schwerwiegendste Problem.

Es kann Kronjuwelen geben, bei denen nicht ein einzelner Prozess oder ein Objekt im Fokus steht, sondern wo die Kronjuwelen durch die Kumulation wichtiger geschäftskritischer Werte entstehen. Beispiel: Wenn bei einem Buchverlag der streng vertrauliche Entwurf des letzten Bands einer Erfolgsreihe an die Öffentlichkeit gelangt, ist das ein schwerwiegender Sicherheitsvorfall. Werden allerdings alle Daten der für das Geschäftsjahr geplanten Bestseller vernichtet und somit deren Veröffentlichung verhindert, kann das zur wirtschaftlichen Katastrophe für den Verlag führen.

Es kann Kronjuwelen geben, bei denen nicht ein einzelner Prozess oder ein Objekt höchste Verfügbarkeit aufweisen muss, sondern wo die Verfügbarkeit der Produktionskette oder sogar der Schutzeinrichtungen selber abzusichern ist. Ein Beispiel hierfür sind die Prozesse zur Energieerzeugung in einem Kernkraftwerk.

7.4 Strukturanalyse

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

- die für die Kern-Absicherung im eingeschränkten Informationsverbund betriebenen Anwendungen und die dadurch gestützten Geschäftsprozesse,
- die organisatorischen und personellen Rahmenbedingungen für diesen Informationsverbund,

- im Informationsverbund eingesetzte vernetzte und nicht-vernetzte IT-Systeme,
- die Kommunikationsverbindungen zwischen den IT-Systemen und nach außen,
- die vorhandene Infrastruktur.

Die einzelnen Schritte der Strukturanalyse werden im Detail in Kapitel 8.1 dieses Dokuments in Form einer Handlungsanweisung beschrieben.

7.5 Schutzbedarfsfeststellung

Zweck der Schutzbedarfsfeststellung ist es, zu ermitteln, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist. Hierzu werden für jede Anwendung und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit entstehen können. Wichtig ist es dabei auch, die möglichen Folgeschäden realistisch einzuschätzen. Bewährt hat sich eine Einteilung in die drei Schutzbedarfskategorien "normal", "hoch" und "sehr hoch". Grundsätzlich ist bei den Assets, die durch eine Kern-Absicherung geschützt werden sollen, von einem Schutzbedarf der Kategorien "hoch" und "sehr hoch" auszugehen. Trotzdem muss der Schutzbedarf dieser wenigen, besonders geschäftskritischen Assets dediziert eingeschätzt werden.

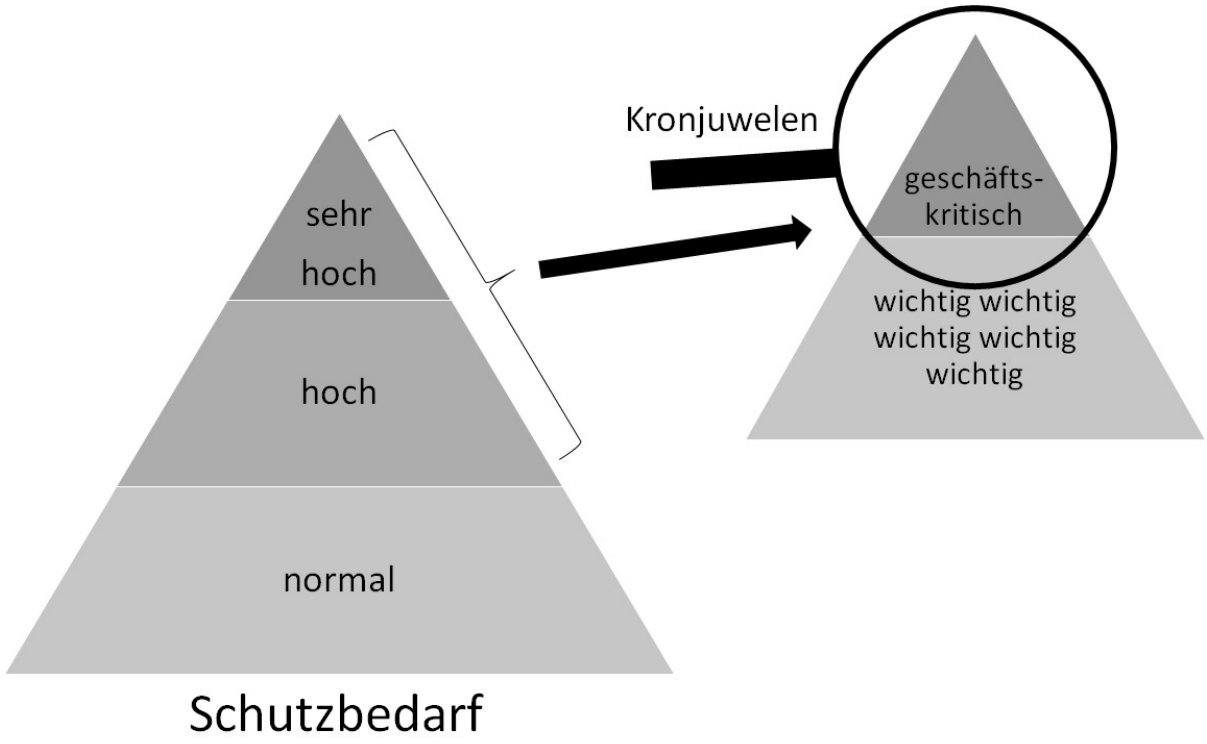


Abbildung 10: Schutzbedarf und Kronjuwelen

Neben den als Kronjuwelen identifizierten Assets gibt es typischerweise weitere Assets mit hohem oder sehr hohem Schutzbedarf, die auch angemessen zu schützen sind.

Die einzelnen Schritte der Schutzbedarfsfeststellung werden im Detail in Kapitel 8.2 dieses Dokuments erläutert, wobei zu beachten ist, dass bei der Kern-Absicherung der Fokus auf hohen und sehr hohen Schutzbedarf liegt.

7.6 Modellierung: Auswahl und Anpassung von Anforderungen

Voraussetzung für die Anwendung des IT-Grundschutz-Kompendiums auf einen Informationsverbund sind detaillierte Unterlagen über seine Struktur und den Schutzbedarf der darin enthaltenen Zielobjekte. Diese Informationen sollten über die zuvor beschriebenen Arbeitsschritte ermittelt werden. Um geeignete Sicherheitsmaßnahmen für den vorliegenden Informationsverbund

identifizieren zu können, müssen anschließend die Bausteine des IT-Grundschutz-Kompendiums auf die Zielobjekte und Teilbereiche abgebildet werden.

Dieser Vorgang der Modellierung wird in Kapitel 8.3 detailliert beschrieben.

7.7 IT-Grundschutz-Check

Der IT-Grundschutz-Check ist ein Organisationsinstrument, welches einen schnellen Überblick über das vorhandene Sicherheitsniveau bietet. Mit Hilfe von Interviews wird der Status quo eines bestehenden (nach IT-Grundschutz modellierten) Informationsverbunds in Bezug auf den Grad der Erfüllung der Sicherheitsanforderungen des IT-Grundschutzes ermittelt. Als Ergebnis liegt ein Katalog vor, in dem für jede relevante Anforderung der Erfüllungsstatus "ja", "teilweise","nein" oder "entbehrlich" (mit Begründung, nicht möglich bei Basis-Anforderungen) erfasst ist. Durch die Identifizierung von noch nicht oder nur teilweise erfüllten Anforderungen werden Verbesserungsmöglichkeiten für die Sicherheit der betrachteten Geschäftsprozesse und der Informationstechnik aufgezeigt.

Kapitel 8.4 beschreibt einen Aktionsplan für die Durchführung eines IT-Grundschutz-Checks. Dabei wird sowohl den organisatorischen Aspekten als auch den fachlichen Anforderungen bei der Projektdurchführung Rechnung getragen.

7.8 Risikoanalyse und weiterführende Sicherheitsmaßnahmen

Die Erfüllung der Standard-Anforderungen nach IT-Grundschutz bietet im Normalfall einen angemessenen und ausreichenden Schutz. Bei hohem oder sehr hohem Schutzbedarf, wie er im Rahmen der Kern-Absicherung regelmäßig auftritt, ist zu prüfen, ob sich zusätzliche Sicherheitsanforderungen ergeben und damit zusätzliche oder ersatzweise höherwertige Sicherheitsmaßnahmen erforderlich sind. Dies gilt auch, wenn besondere Einsatzbedingungen vorliegen oder wenn Komponenten verwendet werden, die nicht mit den existierenden Bausteinen des IT-Grundschutz-Kompendiums abgebildet werden können. Dann ist zu entscheiden, ob für die jeweils betroffenen Bereiche eine Risikoanalyse durchgeführt werden muss, um angemessene Sicherheitsmaßnahmen zu identifizieren.

Eine Methode für Risikoanalysen ist die im BSI-Standard 200-3 *Risikoanalyse auf der Basis von IT-Grundschutz* beschriebene Vorgehensweise. In Kapitel 8.5 wird diese Methode überblicksartig dargestellt. Die erfolgreiche Durchführung einer Risikoanalyse hängt entscheidend von den Fachkenntnissen des Projektteams ab. Daher ist es häufig sinnvoll, fachkundiges externes Personal hinzuzuziehen.

7.9 Umsetzung und weitere Schritte

Die identifizierten und konsolidierten Sicherheitsmaßnahmen für die Kern-Absicherung müssen im Anschluss umgesetzt werden. Was hierbei zu beachten ist, ist in Kapitel 9 *Umsetzung der Sicherheitskonzeption* beschrieben.

Zu den Aufgaben eines ISMS gehört es nicht nur, im betrachteten Informationsverbund die Informationssicherheit aufrechtzuerhalten, sondern diese sollte auch fortlaufend verbessert werden (siehe Kapitel 10). Für die Kern-Absicherung bedeutet dies, dass natürlich regelmäßig überprüft werden muss, ob die getroffenen Sicherheitsvorkehrungen noch der aktuellen Gefährdungslage entsprechen. Außerdem sollte überlegt werden, dass nach der erfolgreichen Absicherung der Kronjuwelen auch weitere Bereiche der Institution angemessen geschützt werden sollten. Hierfür kann beispielsweise auf weitere Bereiche die Basis- oder die Standard-Absicherung angewendet werden oder auch der Informationsverbund der Kern-Absicherung erweitert werden.

Wenn die Kern-Absicherung in einem abgegrenzten Informationsverbund erfolgreich umgesetzt wurde, kann dies auch über eine Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz nach innen und außen hin demonstriert werden. Welche Schritte hierfür notwendig sind und welche Bedingungen für eine erfolgreiche Zertifizierung erfüllt werden müssen, ist in Kapitel 11 *Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz* beschrieben.

8 Erstellung einer Sicherheitskonzeption nach der Vorgehensweise Standard-Absicherung

Eines der Ziele der Standard-Absicherung des IT-Grundschutzes ist es, eine pragmatische und effektive Vorgehensweise zur Erzielung eines normalen Sicherheitsniveaus anzubieten, das auch als Basis für ein höheres Sicherheitsniveau dienen kann.

Nachdem ein Informationssicherheitsprozess initiiert, die Sicherheitsleitlinie und Informationssicherheitsorganisation definiert wurden, wird die Sicherheitskonzeption für die Institution erstellt. Als Grundlage hierfür finden sich in den Bausteinen des IT-Grundschutz-Kompendiums für typische Komponenten von Geschäftsprozessen, Anwendungen, IT-Systemen etc. Sicherheitsanforderungen nach dem Stand der Technik. Diese sind in Bausteinen strukturiert, so dass sie modular aufeinander aufsetzen.

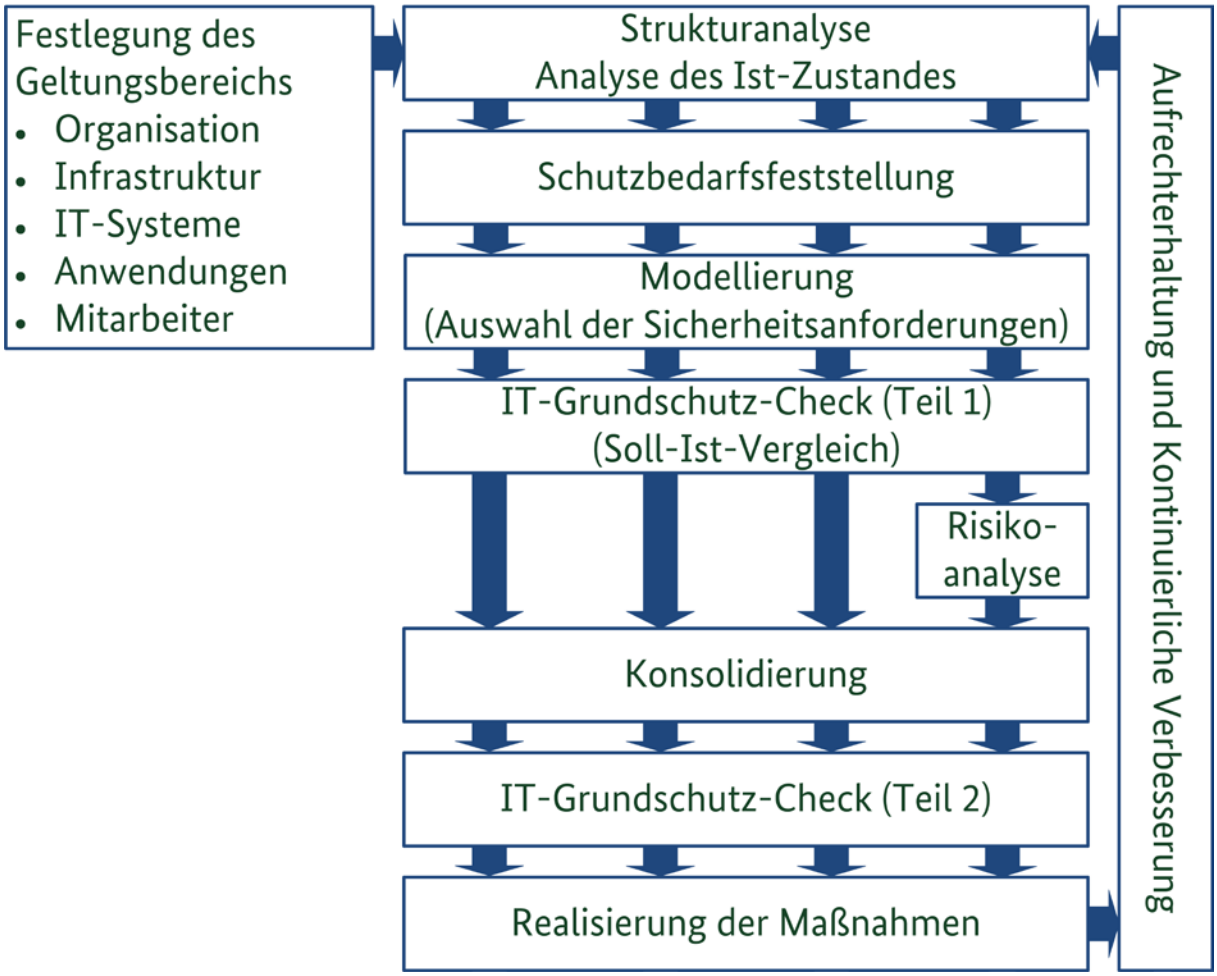


Abbildung 11: Erstellung der Sicherheitskonzeption bei der Standard-Absicherung

Die Durchführung einer Standard-Absicherung nach IT-Grundschutz gliedert sich in die folgenden Aktionsfelder:

Festlegung des Geltungsbereichs

Bei der Entscheidung für die weitere Vorgehensweise (siehe Kapitel 3.3) wurde auch der Geltungsbereich festgelegt, für den die Sicherheitskonzeption erstellt und umgesetzt werden soll. Dies können beispielsweise bestimmte Organisationseinheiten einer Institution sein. Es könnten aber auch Bereiche sein, die definierte Geschäftsprozesse oder Fachaufgaben bearbeiten, inklusive der dafür notwendigen Infrastruktur. Im IT-Grundschutz wird der Geltungsbereich für die Sicherheitskonzeption auch als "Informationsverbund" bezeichnet. Die Bestandteile des betrachteten

Informationsverbunds sind die mit den passenden Bausteinen des IT-Grundschutz-Kompendiums abzusichernden Komponenten.

Strukturanalyse

Für die Erstellung eines Sicherheitskonzepts nach der Vorgehensweise Standard-Absicherung und insbesondere für die Anwendung des IT-Grundschutz-Kompendiums ist es erforderlich, das Zusammenspiel der Geschäftsprozesse, der Anwendungen und der vorliegenden Informationstechnik zu analysieren und zu dokumentieren. Aufgrund der heute üblichen starken Vernetzung von IT-Systemen, die sich auch auf die Bereiche ICS und IoT erstreckt, bietet sich ein Netztopologieplan als Ausgangsbasis für die weitere technische Analyse an. Die folgenden Aspekte müssen berücksichtigt werden:

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

Die einzelnen Schritte der Strukturanalyse werden im Detail in Kapitel 8.1 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 angemessen ist. Hierzu werden für jede Anwendung und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit entstehen können. Wichtig ist es dabei auch, die möglichen Folgeschäden realistisch einzuschätzen. Bewährt hat sich eine Einteilung in die drei Schutzbedarfskategorien "normal", "hoch" und "sehr hoch".

Die einzelnen Schritte der Schutzbedarfsfeststellung werden im Detail in Kapitel 8.2 dieses Dokuments erläutert.

Auswahl von Anforderungen und Anpassung von Maßnahmen (Modellierung)

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

Dieser Vorgang der Modellierung wird in Kapitel 8.3 detailliert beschrieben.

IT-Grundschutz-Check

Der IT-Grundschutz-Check ist ein Organisationsinstrument, welches einen schnellen Überblick über das vorhandene Sicherheitsniveau bietet. Mit Hilfe von Interviews wird der Status quo eines bestehenden (nach IT-Grundschutz modellierten) Informationsverbunds in Bezug auf den Umsetzungsgrad der Sicherheitsanforderungen des IT-Grundschutz-Kompendiums ermittelt. Als Ergebnis liegt ein Katalog vor, in dem für jede relevante Anforderung der Umsetzungsstatus "entbehrlich", "ja", "teilweise" oder "nein" erfasst ist. Durch die Identifizierung von noch nicht oder nur teilweise erfüllten Anforderungen werden Verbesserungsmöglichkeiten für die Sicherheit der betrachteten Geschäftsprozesse und der Informationstechnik aufgezeigt.

Kapitel 8.4 beschreibt einen Aktionsplan für die Durchführung eines IT-Grundschutz-Checks. Dabei wird sowohl den organisatorischen Aspekten als auch den fachlichen Anforderungen bei der Projektdurchführung Rechnung getragen.

Risikoanalyse

Durch die Umsetzung der Sicherheitsanforderungen der Standard-Absicherung wird im Normalfall für einen Informationsverbund ein angemessener und ausreichender Schutz erzielt. Bei hohem oder sehr hohem Schutzbedarf kann es jedoch sinnvoll sein, zu prüfen, ob zusätzlich oder ersatzweise höherwertige Sicherheitsmaßnahmen erforderlich sind. Dies gilt auch, wenn besondere Einsatzbedingungen vorliegen oder wenn Komponenten verwendet werden, die nicht mit den existierenden Bausteinen des IT-Grundschutz- Kompendiums abgebildet werden können. In diesen Fällen ist eine Risikoanalyse durchzuführen. Sie sollte in regelmäßigen Abständen aktualisiert werden, damit auch geänderte Gefährdungslagen erkannt werden.

Eine Methode für Risikoanalysen ist die im BSI-Standard 200-3 *Risikoanalyse auf der Basis von IT-Grundschutz* beschriebene Vorgehensweise. In Kapitel 8.5 wird diese Methode überblicksartig dargestellt. Die erfolgreiche Durchführung einer Risikoanalyse hängt entscheidend von den Fachkenntnissen des Projektteams ab. Daher ist es häufig sinnvoll, fachkundiges externes Personal hinzuzuziehen.

Reihenfolge der Bearbeitung

Die verschiedenen Aktivitäten, die zur Erstellung einer Sicherheitskonzeption erforderlich sind, also Strukturanalyse, Schutzbedarfsfeststellung, Modellierung eines Informationsverbunds, IT-Grundschutz-Check, Risikoanalyse, müssen nicht zwingend nacheinander abgearbeitet werden. Diese Aktionsfelder können, soweit dies je nach vorhandenen Rahmenbedingungen und Größe des Sicherheitsteams möglich ist, auch unabhängig und zeitgleich durchgeführt werden.

8.1 Strukturanalyse

Die Strukturanalyse dient der Vorerhebung von Informationen, die für die weitere Vorgehensweise in der Erstellung eines Sicherheitskonzepts nach IT-Grundschutz benötigt werden. Dabei geht es um die Erfassung der Bestandteile (Geschäftsprozesse, Informationen, Anwendungen, IT- und ICS-Systeme, Räume, Kommunikationsnetze), die zur Betrachtung des Geltungsbereichs benötigt werden.

Hinweis: Häufig sind die Geschäftsprozesse noch nicht, nicht durchgängig oder nicht aktuell erfasst. Dann müssen zuerst die relevanten Geschäftsprozesse identifiziert werden, z. B. durch Auswertung von Geschäftsverteilungsplänen, Aufgabenbeschreibungen oder anderen organisationsbeschreibenden Papieren.

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

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

Die Strukturanalyse gliedert sich in folgende Teilaufgaben:

- Erfassung der zum Geltungsbereich zugehörigen Geschäftsprozesse, Anwendungen und Informationen
- Netzplanerhebung
- Erhebung von IT-, ICS- und IoT-Systemen und ähnlichen Objekten
- Erfassung der Räume und Gebäude (für den ICS-Bereich sind auch die produzierenden Räumlichkeiten berücksichtigen)

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

8.1.1 Komplexitätsreduktion durch Gruppenbildung

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

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

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

- vom gleichen Typ sind,
- ähnliche Aufgaben haben,
- ähnlichen Rahmenbedingungen unterliegen und
- den gleichen Schutzbedarf aufweisen.

Bei technischen Objekten bietet sich eine Gruppenbildung außerdem immer dann an, wenn sie

- ähnlich konfiguriert sind,
- ähnlich in das Netz eingebunden sind (z. B. im gleichen Netzsegment) und
- ähnlichen administrativen und infrastrukturellen Rahmenbedingungen unterliegen,
- ähnliche Anwendungen bedienen und
- den gleichen Schutzbedarf aufweisen.

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

Wichtigstes Beispiel für die Gruppierung von Objekten ist sicherlich die Zusammenfassung von Clients. In der Regel gibt es in einer Institution eine große Anzahl von Clients, die sich jedoch gemäß obigem Schema in eine überschaubare Anzahl von Gruppen aufteilen lassen. Auch in produzierenden und gewerblichen Bereichen ist es empfehlenswert, Objekte zu gruppieren, wenn diese vergleichbar konfiguriert und eingesetzt werden (z. B. Handscanner, Arbeitsplatz-PCs). Dies gilt analog auch für Räume und andere Objekte. In großen Informationsverbünden, wo aus Gründen der Redundanz oder des Durchsatzes viele Server die gleiche Aufgabe wahrnehmen, können durchaus auch Server zu Gruppen zusammengefasst werden.

Zunehmend werden IT-Systeme virtualisiert. Da hierbei typischerweise viele virtuelle Maschinen (VMs) auf einem Virtualisierungsserver betrieben werden, ist eine sinnvolle Strukturanalyse bei virtualisierten Infrastrukturen oder Cloud Computing nur durch geeignete Gruppenbildung möglich. Für die Gruppenbildung gelten bei Virtualisierung die selben Regeln wie für physische Zielobjekte. Prinzipiell können auch solche VMs zu einer Gruppe zusammengefasst werden, die auf verschiedenen physischen IT-Systemen laufen, wenn sie ähnliche Aufgaben erfüllen, ähnlich konfiguriert sind und denselben Schutzbedarf aufweisen.

In der Regel bestehen Cloud Computing Plattformen aus homogenen Hard- und Software-Komponenten. Aufgrund der Homogenität kann eine Vielzahl von Aufgaben automatisiert und zentral durchgeführt werden. Eine Gruppenbildung, beispielsweise anhand des Schutzbedarfs, ist beim Cloud Computing zwingend erforderlich.

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

Aktionspunkte zu 8.1.1 Komplexitätsreduktion durch Gruppenbildung
• Bei allen Teilaufgaben der Strukturanalyse gleichartige Objekte zu Gruppen zusammenfassen • Typ und Anzahl der jeweils zusammengefassten Objekte vermerken

8.1.2 Erfassung der Geschäftsprozesse und der zugehörigen Informationen

Eine der Hauptaufgaben des Sicherheitsmanagements ist es, der Leitungsebene die Informationssicherheitsrisiken aufzuzeigen und damit Transparenz zu schaffen, wo Entscheidungs- oder Handlungsbedarf erforderlich ist. Hierzu muss sich der ISB einen Überblick über die für die Institution wesentlichen Geschäftsprozesse bzw. Fachaufgaben verschaffen und darstellen, was Informationssicherheitsrisiken bzw. IT-Risiken für diese Geschäftsprozesse bedeuten.

Somit ist sinnvoll, einen Bezug zwischen den Geschäftsprozessen und der Wertschöpfung einer Institution und den zu schützenden Informationen sowie der verwendeten IT bzw. den verwendeten Anwendungen herzustellen. Hierfür müssen die Geschäftsprozesse und deren Abhängigkeit von den wichtigsten Anwendungen dokumentiert werden.

Auf Basis des definierten Informationsverbunds sind in einem ersten Schritt die dort enthaltenen zentralen Geschäftsprozesse oder Fachaufgaben zu erfassen und zu dokumentieren. Hierbei ist darauf zu achten, dass eine sinnvolle Granularität gewählt wird. Dies bedeutet, dass nicht nur ein einzelner Hauptprozess wie z. B. Personalmanagement, sondern auch die zugehörigen wichtigsten Sub-Prozesse wie z. B. Personalgewinnung, Mitarbeiterverwaltung, Personalentwicklung, etc. erfasst werden, sofern diese Bestandteil des Informationsverbunds sind. Eine zu detaillierte Dokumentation z. B. durch Auflistung von Sub-Sub-Prozessen sollte jedoch vermieden werden. Auch im ICS-Bereich müssen für die Strukturanalyse die Geschäftsprozesse mit den zugehörigen Informationen erfasst werden. Hier ist insbesondere darauf zu achten, dass neben dem Kernprozess der Produktion auch weitere Nebenprozesse wie z. B. die logistischen Prozesse für den Warenfluss und der Instandhaltung berücksichtigt werden.

Die einzelnen Prozesse sind wie folgt zu erfassen:

- eindeutiger Bezeichner
- Name
- Prozessverantwortlicher / Fachabteilung
- kurze Beschreibungen des Prozesses oder der Fachaufgabe und der dort verarbeiteten Informationen
- wichtige, für den Prozesse benötigte Anwendung(en)

Um die wesentlichen Geschäftsprozesse zu identifizieren, kann in vielen Institutionen auf bestehende Prozesslandkarten zurückgegriffen werden. Wenn die Geschäftsprozesse noch nicht, nicht durchgängig oder nicht aktuell erfasst wurden, sollten zunächst Geschäftsverteilungspläne, Aufgabenbeschreibungen oder andere organisationsbeschreibende Papiere ausgewertet werden, um die relevanten Geschäftsprozesse zu identifizieren. Daneben kann das Verfahrensverzeichnis des Datenschutzbeauftragten ein weiterer Startpunkt für die Erfassung der Prozesse, Fachaufgaben und nachfolgenden Anwendungen sein, auch wenn dies lediglich die Verfahren und Anwendungen abbildet, welche personenbezogene Daten verarbeiten. Sollten noch keine Prozessbeschreibungen vorliegen, sind kurze Workshops oder Interviews mit den Fachverantwortlichen sinnvoll.

Es kann durchaus sinnvoll sein, die Erhebung der Prozesse und Fachaufgaben mit der Erhebung der Anwendungen zu koppeln, um damit redundante Fragen insbesondere in den Fachabteilungen zu vermeiden.

Aktionspunkte zu 8.1.2 Erfassung der Geschäftsprozesse und der zugehörigen Informationen
• Überblick über die Geschäftsprozesse erstellen • Geschäftsprozesse mit eindeutigen Nummern oder Kürzeln kennzeichnen • Zusammenhang zwischen Geschäftsprozessen und Anwendungen darstellen

8.1.3 Erfassung der Anwendungen und der zugehörigen Informationen

Ausgehend von jedem Geschäftsprozess bzw. jeder Fachaufgabe, die im Informationsverbund enthalten ist, müssen in dieser Phase die damit zusammenhängenden Anwendungen und die damit verarbeiteten Informationen identifiziert werden. Anwendungen dienen der IT-technischen Unterstützung von Geschäftsprozessen und Fachaufgaben in Behörden und Unternehmen.

Die geeignete Granularität für die betrachteten Anwendungen muss in jeder Institution individuell gewählt werden. Ziel sollte dabei sein, eine optimale Transparenz und Effizienz bei der Strukturanalyse und der Schutzbedarfsfeststellung zu erreichen. Auch die im IT-Grundschutz-Kompendium betrachteten Bausteine aus der Schicht der Anwendungen können für diesen Schritt Aufschluss geben

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

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

erfordern.

Bei der Erfassung der Anwendungen sollten auch die Benutzer bzw. die für die Anwendung Verantwortlichen sowie die für den Geschäftsprozess Verantwortlichen befragt werden, wie sie das erforderliche Sicherheitsniveau einschätzen.

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

Falls abweichend von der hier vorgeschlagenen Reihenfolge zuerst die IT-Systeme erfasst wurden, ist es häufig hilfreich, die Anwendungen an erster Stelle orientiert an den IT-Systemen zusammenzutragen. Aufgrund ihrer Breitenwirkung sollte dabei mit den Servern begonnen werden. Um ein möglichst ausgewogenes Bild zu bekommen, kann anschließend diese Erhebung auf Seiten der Clients und Einzelplatz-Systeme vervollständigt werden. Abschließend sollte noch festgestellt werden, welche Netzkoppelelemente welche Anwendungen unterstützen. Für die Erfassung der Anwendungen auf einem Standard-Client hat sich in der Praxis bewährt, seitens der unterstützenden IT-Abteilung die Standard-Software der Clients als Paket zu betrachten. So wird die Standard-Software nicht vergessen. Oftmals wird diese als selbstverständlich angesehen und deren Anwendung wird in Interviews nicht mehr explizit genannt (z. B. die E-Mail-Anwendung oder Bürokommunikation).

Ausgehend von den Anwendungen können die zugehörigen Geschäftsprozesse auch im Nachgang erfasst werden (siehe Kapitel 8.1.2). Der Verantwortliche und die Benutzer der Anwendung sollten ebenfalls erfasst werden, um Ansprechpartner für Sicherheitsfragen leichter identifizieren bzw. betroffene Benutzergruppen schnell erreichen zu können.

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

- Archiv- und Backup-Datenträger,
- Datenträger für den Austausch mit externen Kommunikationspartnern,
- Massenspeicher für den mobilen Einsatz (z. B. USB-Sticks oder externe Festplatten),
- Notfallhandbücher, die in ausgedruckter Form vorgehalten werden,
- Mikrofilme,
- wichtige Verträge mit Partnern und Kunden.

Es darf nicht vergessen werden, virtualisierte Anwendungen im Rahmen der Strukturanalyse mit zu erfassen.

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

Beispiel: RECPLAST GmbH

Im Folgenden wird anhand einer fiktiven Institution, der RECPLAST GmbH, beispielhaft dargestellt, wie die erfassten Anwendungen dokumentiert werden können. Zu beachten ist, dass die Struktur der RECPLAST GmbH im Hinblick auf Informationssicherheit keineswegs optimal ist. Sie dient lediglich dazu, die Vorgehensweise bei der Anwendung des IT-Grundschutzes zu illustrieren. In diesem Dokument werden anhand der RECPLAST GmbH die einzelnen Aktivitäten zur Erstellung einer Sicherheitskonzeption erläutert. Das komplette Beispiel findet sich unter den Hilfsmitteln zum IT-Grundschutz.

Die RECPLAST GmbH ist eine fiktive Institution mit ca. 500 Mitarbeitern, von denen 130 an Bildschirmarbeitsplätzen arbeiten. Räumlich ist die RECPLAST GmbH aufgeteilt in zwei Standorte innerhalb von Bonn, wo unter anderem die administrativen und produzierenden Aufgaben wahrgenommen werden, und drei Vertriebsstandorte in Deutschland.

Um die Geschäftsprozesse zu optimieren, sind alle Arbeitsplätze vernetzt worden. Die Außenstelle in Bonn ist über eine angemietete Standleitung an die Zentrale angebunden. Die Vertriebsstandorte sind

mit abgesicherten Verbindungen über das Internet an die Zentrale angebunden. Alle für die Aufgabenerfüllung und die Informationssicherheit wesentlichen Richtlinien und Vorschriften sowie Formulare und Textbausteine sind ständig für jeden Mitarbeiter über das Intranet abrufbar. Alle relevanten Arbeitsergebnisse werden in eine zentrale Datenbank eingestellt. Entwürfe werden ausschließlich elektronisch erstellt, weitergeleitet und unterschrieben. Die Realisierung und Betreuung aller benötigten Funktionalitäten übernimmt eine IT-Abteilung in Bonn.

Die Geschäftsprozesse der RECPLAST werden elektronisch gepflegt und sind nach einem zweistufigen Schema benannt. Hinter dem Kürzel GP wird die Nummer des Hauptprozesses angegeben, zum Beispiel GP002. Ein Geschäftsprozess sollte immer beschrieben werden, damit ein einheitliches Verständnis für die Abgrenzung eines Prozesses vorhanden ist. Optional kann eine Prozess-Art erfasst werden. Diese dient lediglich zur Übersicht, welche Prozesse für eine Institution hauptsächlich zum Fortbestand beitragen. Die Unterstützungsprozesse sind jedoch ebenso wichtig, diese sind jedoch eher für den allgemeinen Betrieb einer Institution erforderlich.

Nachfolgend ist ein Auszug aus der Erfassung der Geschäftsprozesse und der dazugehörigen Informationen für die RECPLAST GmbH abgebildet:

A.1 Geschäftsprozesse der RECPLAST GmbH

Bezeichnung	Beschreibung des Prozesses	Prozess-Art	Prozess-verantwortlicher	Mitarbeiter
GP001	**Produktion:** Die Produktion der Kunststoffartikel umfasst alle Phasen von der Materialbereitstellung bis hin zur Einlagerung des produzierten Materials. Hierzu gehören innerhalb der Produktion die internen Transportwege, die Produktion und Fertigung der verschiedenen Komponenten und das Verpacken der Teile.	Kerngeschäft	Leiter Produktion	Alle Mitarbeiter
GP002	Angebotswesen: In der Angebotsabwicklung werden die Kundenanfragen für Produkte verarbeitet. Im Regelfall werden Kundenanfragen formlos per E-Mail oder Fax geschickt. Die Angebote werden elektronisch erfasst und ein schriftliches Angebot per Post an den Kunden versendet.	Unterstützender Prozess	Leiter Angebotswesen	Vertrieb
GP003	**Auftragsabwicklung:** Kunden schicken die Bestellungen im Regelfall per Fax oder E-Mail. Alle Belege müssen ausgedruckt und elektronisch erfasst werden. Eine Auftragsbestätigung erhält der Kunde nur, wenn er dies ausdrücklich wünscht oder der Produktionsprozess von der üblichen Produktionszeit abweicht.	Kerngeschäft	Leiter Auftragsabwicklung	Vertrieb
GP004	**Einkaufsabteilung:** In der Einkaufsabteilung werden alle erforderlichen Artikel bestellt, die nicht für den Produktionsprozess erforderlich sind. In dieser Abteilung werden externe Projekte verhandelt, IT-Verträge gestaltet und Verbrauchsmaterial im organisatorischen Umfeld (Papier, Toner, etc.) beschafft.	Unterstützender Prozess	Leiter Einkaufsabteilung	Einkauf
GP005	**Disposition:** In der Disposition werden alle für die Produktion benötigten Materialien (Kunststoffe, Schrauben, Tüten, etc.) beschafft. Hierzu liegen normalerweise Rahmenverträge vor. Geplant wird in diesem Umfeld anhand von Jahresplanmengen und verschiedenen Bestellwerten.	Kerngeschäft	Leiter Disposition	Disposition, Produktion

Abbildung 12: Auszug aus den Geschäftsprozessen der RECPLAST GmbH

Strukturanalyse der Anwendungen:

Der zuständige Informationssicherheitsbeauftragte der RECPLAST GmbH erfasst in der Strukturanalyse neben den Geschäftsprozessen auch alle weiteren Objekte, die zur Institution selbst gehören. Dazu gehören auch die Anwendungen, die zur Aufrechterhaltung der bereits erfassten Geschäftsprozesse benötigt werden.

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

A.1 Strukturanalyse der RECPLAST GmbH									
Bezeichnung	Beschreibung des Zielobjektes / der Gruppe der Zielobjekte	Plattform / Baustein	Ort	Gebäude	Raum	Anzahl	Status	Benutzer	Verantwortlich / Administrator
A003	**Textverarbeitung, Tabellenkalkulation:** Alle geschäftlichen Informationen werden in einem Office-Produkt verarbeitet, Geschäftsbriefe, Analysen oder Präsentationen	Office-Produkt 2010	-	-	-	130	in Betrieb	Alle Mitarbeiter	IT-Betrieb
A004	**Chat-Anwendung:** Eine Chat-Anwendung soll den Kontakt zwischen den Mitarbeitern vereinfachen. Die E-Mails werden standardmäßig nur zwei Mal pro Tag abgerufen. Diese Anwendung wird als virtualisierte Anwendung eingesetzt.	Standardsoftware	-	-	-	130	in Betrieb	Alle Mitarbeiter	IT-Betrieb
A008	**Active Directory:** Diese Anwendung soll dem IT-Betrieb die Arbeit erleichtern und doppelte Benutzereingaben reduzieren.	Active Directory	Bonn	BG	Büro	5	Test	Administratoren	IT-Betrieb

Abbildung 13: Auszug aus der Strukturanalyse der RECPLAST GmbH (Anwendungen)

Der Zusammenhang zwischen den Geschäftsprozessen zu den Anwendungen muss immer dargestellt werden. Diese Zuordnung sollte idealerweise mit Tools durchgeführt werden, um bei der üblichen Vielzahl von Prozessen und Anwendungen die Übersichtlichkeit und Aktualität zu gewährleisten.

Am Beispiel der RECPLAST GmbH wird nachfolgend dargestellt, dass für einen Prozess normalerweise mehrere Anwendungen eingesetzt werden:

A.1 Zuordnungen Geschäftsprozesse zu Anwendungen der RECPLAST GmbH										
Geschäftsprozess / Anwendung	A001	A002	A003	A004	A005	A006	A007	A008	A009	A010
GP001	x					x	x			x
GP002					x	x	x		x	
GP003					x	x	x		x	
GP004			x	x		x	x	x	x	
GP005			x			x	x	x	x	

Abbildung 14: Zuordnung der Geschäftsprozesse zu den Anwendungen der RECPLAST GmbH

Aktionspunkte zu 8.1.3 Erfassung der Anwendungen und der zugehörigen Informationen

- Unter Einbeziehung der Verantwortlichen bzw. der Nutzer der Anwendungen herausfinden, welche Anwendungen für die betrachteten Geschäftsprozesse erforderlich sind
- Übersicht über die Anwendungen erstellen und mit eindeutigen Nummern oder Kürzeln kennzeichnen

8.1.4 Netzplanerhebung

Einen geeigneten Ausgangspunkt für die weitere technische Analyse stellt ein Netzplan (beispielsweise in Form eines Netztopologieplans) dar. Ein Netzplan ist eine graphische Übersicht über die im betrachteten Bereich der Informations- und Kommunikationstechnik eingesetzten Komponenten und deren Vernetzung. Netzpläne oder ähnliche graphische Übersichten sind auch aus

betrieblichen Gründen in den meisten Institutionen vorhanden. Im Einzelnen sollte der Plan in Bezug auf die Informationssicherheit mindestens folgende Objekte darstellen:

- IT-Systeme, d. h. Client- und Server-Computer, aktive Netzkomponenten (wie Switches, Router, WLAN Access Points), Netzdrucker etc.
- ICS- und IoT-Komponenten mit Netz-Anschluss, d. h. Clients, Handscanner, Industriedrucker, Geräte mit speicherprogrammierbarer Steuerung (SPS), Schaltschränke etc.
- Netzverbindungen zwischen diesen Systemen, d. h. LAN-Verbindungen (wie Ethernet), WLANs, Backbone-Techniken (wie 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 und sonstige Geräte sollten zumindest

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

vermerkt sein. Bei Außenanbindungen oder drahtlosen Kommunikationsverbindungen (WLAN, UMTS, LTE, ...) sollten zusätzlich Details zum externen Netz (z. B. Internet, Geschäftspartner, Name des Providers für die Datenübertragung sowie die Art der Leitung z. B. MPLS, Leased Line, VPN) aufgenommen werden.

Virtuelle IT-Systeme (virtuelle Switches, virtuelle Server etc.) und virtuelle Netzverbindungen, beispielsweise Virtuelle LANs (VLANs) oder Virtuelle Private Netze (VPNs), sollten ebenfalls in einem Netzplan dargestellt werden. Hierbei sind virtuelle IT-Systeme gemäß ihrem Typ und Einsatzzweck genauso wie physische IT-Systeme zu behandeln. Darüber hinaus muss die Zuordnung von virtuellen IT-Systemen zu physischen Host-Systemen nachvollziehbar sein. Um die Übersichtlichkeit zu verbessern, ist es bei zunehmender Größe eines Netzes sinnvoll, den Netzplan in mehrere Teilnetzpläne aufzuteilen.

Eine Cloud-Infrastruktur setzt sich aus einer Vielzahl von Elementen zusammen. Neben den physischen (mit CPU, Arbeitsspeicher und anderer Hardware) und ggf. virtuellen Servern zählen noch Netze und Speicherlösungen dazu. Die aufgezählten Bereiche verfügen in der Regel über eine Verwaltungssoftware.

Für den Bereich Netze sollten die eingesetzten Netzmanagement-Tools eine automatische Erzeugung von Netzplänen unterstützen. Neben physischen sollten auch virtuelle IT-Systeme (z. B. virtuelle Switches, virtuelle Router, virtuelle Sicherheitsgateways) automatisch abgebildet werden können.

Der ICS-Bereich kann als eigenständiges Netz betrieben werden. Bei der Erfassung der Netzverbindungen sollten dabei auch die Schnittstellen erfasst werden (Auflistung der erlaubten und gesperrten Schnittstellen). Auch die Internetanbindung aus dem ICS-Bereich heraus sollte erfasst werden. Die Trennung der Netze zwischen dem Office-Bereich und dem ICS-Bereich sollte im Netzplan dargestellt werden.

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

Aktualisierung des Netzplans

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

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

Der Bereich der industriellen Steuerung sollte ebenfalls in den Netzplan integriert werden. Ansprechpartner sind neben den IT-Verantwortlichen und Administratoren auch die Mitarbeiter der Haustechnik.

Ein bereinigter Netzplan ist auch an anderen Stellen hilfreich. So kann er genutzt werden, um Dritten schnell die Geschäftsprozess- und IT-Strukturen innerhalb der Institution darzustellen, da in einem bereinigten Netzplan der Detaillierungsgrad auf das notwendige Maß reduziert wird. Auch für eine Zertifizierung ist ein bereinigter Netzplan eine sinnvolle Grundlage.

Beispiel: RECPLAST GmbH

Die Netzpläne in der RECPLAST GmbH werden in der IT-Abteilung mit einem Tool verwaltet. Die Darstellung aller Netzpläne ist sehr detailliert und oftmals für Dritte sehr unübersichtlich. Die RECPLAST GmbH nutzt deshalb für die Darstellung der Zielobjekte einen bereinigten Netzplan.

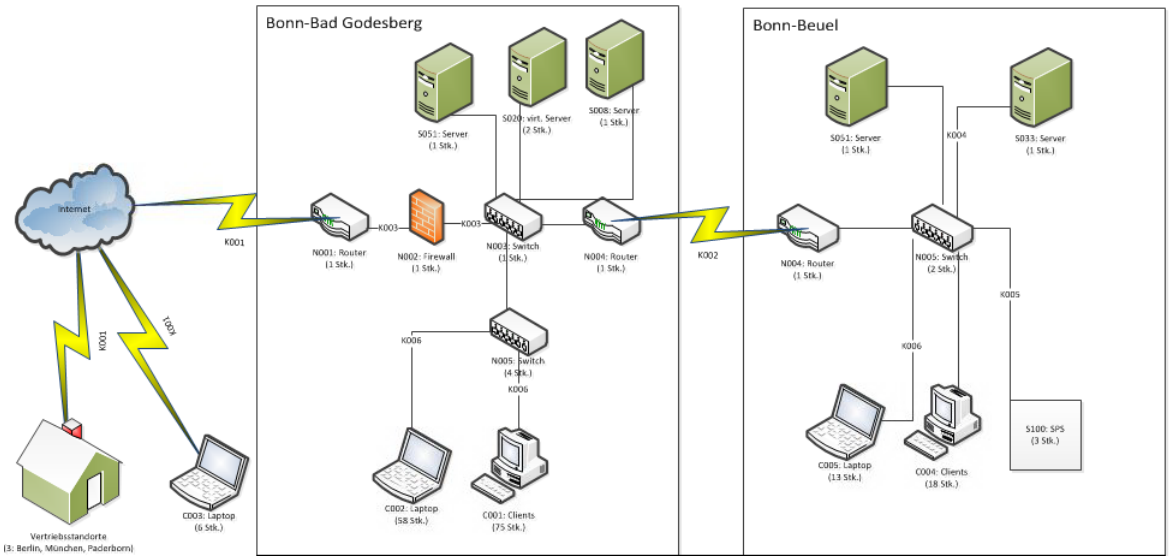


Abbildung 15: Auszug aus dem bereinigten Netzplan der RECPLAST GmbH (Teilausschnitt)

Aktionspunkte zu 8.1.4 Netzplanerhebung

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

8.1.5 Erhebung der IT-Systeme

Im Hinblick auf die später durchzuführende Schutzbedarfsfeststellung und Modellierung des Informationsverbunds sollte eine Liste der vorhandenen und geplanten IT-Systeme in tabellarischer Form aufgestellt werden. Der Begriff IT-System umfasst dabei nicht nur Computer im engeren Sinn, sondern auch die IoT- und ICS-Geräte, aktive Netzkomponenten, Netzdrucker, TK-Anlagen, Smartphones, virtuelle IT-Systeme etc. Die technische Realisierung eines IT-Systems steht im Vordergrund, beispielsweise Apple MacBook, Client unter Windows, Linux-Server, TK-Anlage usw. An dieser Stelle sollen nur die Systeme als solches erfasst werden (z. B. Linux-Server), nicht die einzelnen Bestandteile, aus denen die IT-Systeme zusammengesetzt sind (also nicht Rechner, Tastatur, Bildschirm etc.).

Hinweis:

Für einen ordnungsmäßigen IT-Betrieb ist eine vollständige und korrekte Erfassung der vorhandenen und geplanten IT-Systeme notwendig, beispielsweise für die Überprüfung, Wartung, Fehlersuche und Instandsetzung von IT-Systemen. Für die Erstellung eines Sicherheitskonzepts reicht es, sich einen Überblick über die gruppierten IT-Systeme zu verschaffen.

Zu erfassen sind sowohl die vernetzten als auch die nicht vernetzten IT-Systeme, insbesondere also auch solche, die nicht im zuvor betrachteten Netzplan aufgeführt sind. IT-Systeme, die im Netzplan zu einer Gruppe zusammengefasst worden sind, können weiterhin als ein Objekt behandelt werden. Auch bei den IT-Systemen, die nicht im Netzplan aufgeführt sind, ist zu prüfen, ob sie sinnvoll zusammengefasst werden können. Möglich ist dies beispielsweise bei einer größeren Anzahl von nicht vernetzten Einzelplatz-PCs, die die im Kapitel 8.1.1 *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 der IT-Systeme bzw. der jeweiligen Gruppe (bei Gruppen sollte auch die Anzahl der zusammengefassten IT-Systeme vermerkt sein),
- Beschreibung (z. B. Funktion, Typ),
- Plattform (z. B. Hardware-Architektur/Betriebssystem),
- Aufstellungsort der IT-Systeme (z. B. Ort, Gebäude, Raum),
- Status der IT-Systeme (in Betrieb, im Test, in Planung) und
- Benutzer bzw. Administratoren der IT-Systeme.

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

Beispiel: RECPLAST GmbH

A.1 Strukturanalyse der RECPLAST GmbH									
Bezeichnung	Beschreibung des Zielobjektes / der Gruppe der Zielobjekte	Plattform / Baustein	Ort	Gebäude	Raum	Anzahl	Status	Benutzer	Verantwortlich / Administrator
N001	**Router Internetanbindung:** Dieser Router regelt die Kommunikation zwischen dem Internet und den internen Prozessen	Router und Switches	Bonn	BG	Serverraum	1	in Betrieb	Administratoren	IT-Betrieb
N002	**Firewall Internet-Eingang:** Diese Firewall dient als Schutz zwischen dem Internet und dem internen Netz	Firewall	Bonn	BG	Serverraum	1	in Betrieb	Administratoren	IT-Betrieb
N003	**Switch – Verteilung** Der Datenfluss in Richtung Internet und internes Netz wird über den Switch gesteuert	Router und Switches	Bonn	BG	Serverraum	1	in Betrieb	Administratoren	IT-Betrieb
N004	**Router Bonn BG – Beuel** Über eine Standleitung sind die beiden Standorte in Bonn verbunden. Diese Router sichern die Verbindung ab.	Router und Switches	Bonn	-	Serverraum	2	in Betrieb	Administratoren	IT-Betrieb
S008	**Print-Server:** Server für die Druckerdienste, die zentral gesteuert werden.	Windows Server 2012	Bonn	BG	Serverraum	1	in Betrieb	Alle Mitarbeiter	IT-Betrieb
S020	**Virtueller Server (Konfiguration 1):** Auf dem Server können bis zu 20 virtuelle Server konfiguriert werden. Für die Verwaltung der virtualisierten Systeme wird eine Anwendung eingesetzt.	Server unter Unix	Bonn	BG	Serverraum	2	in Betrieb	Administratoren	IT-Betrieb
S033	**Server Produktion:** Die zentralen Daten für die Produktion werden auf diesem Server verarbeitet.	Server unter Unix	Bonn	Beuel	Serverraum	1	in Betrieb	Mitarbeiter Produktion	IT-Betrieb

Abbildung 16: Auszug aus der Strukturanalyse der RECPLAST GmbH (IT-Systeme)

Für die Zuordnung der Anwendungen zu den IT-Systemen setzt die RECPLAST GmbH ein Tool ein, da die Pflege in Form einer Tabelle aufwendig ist. Jede Änderung, sei es ein IT-System oder eine Anwendung, muss immer dokumentiert werden. Diese Zuordnung ist für die später folgende Schutzbedarfsfeststellung erforderlich.

8.1.6 Erhebung der ICS-Systeme

In Institutionen mit Produktion und Fertigung müssen auch die Industriellen Steuerungssysteme (ICS), die von der Institution eingesetzt werden, erhoben werden.

Oftmals werden in der Produktion und Fertigung neben IT-Systemen noch eine Reihe weiterer Geräte eingesetzt. Alle ICS-Geräte sollten entsprechend erfasst werden.

Im ICS-Bereich gibt es Arbeitsplatz-PCs, die auch hier zu Gruppen zusammengefasst werden sollten. Oftmals sind diese PCs mit den gleichen Anwendungen wie die der Büroumgebung ausgestattet. Darüber hinaus sind auf einigen PCs spezielle Anwendungen installiert. Zu vielen PC-Arbeitsplätzen gehört ein Drucker und neben der Standard-Peripherie (Maus, Tastatur) werden weitere periphere Endgeräte (z. B. Handscanner) eingesetzt, die mit den Arbeitsplatz-PCs direkt verbunden sind. Bei allen peripheren Endgeräten müssen die Kommunikationsverbindungen (z. B. Bluetooth) ebenfalls berücksichtigt werden.

Im Bereich der Produktion und Fertigung werden weitere Endgeräte eingesetzt. Für die industrielle Steuerung gibt es spezielle Endgeräte, z. B. Geräte mit speicherprogrammierbaren Steuerungen (SPSen), WLAN-Module für Industriemaschinen, selbstfahrende Gabelstapler (Flurfahrzeuge).

Bei der Erfassung der ICS-Systeme sollten folgende Informationen vermerkt werden, die für die nachfolgenden Schritte erforderlich sind:

- eine eindeutige Bezeichnung der ICS-Systeme bzw. der jeweilige Geräte-Gruppe (die Anzahl der Geräte in den Gruppen sollte ebenfalls vermerkt sein),
- Beschreibung (Typ und Funktion),

- Plattform (z. B. Betriebssystem, Art der (Netz-)Anbindung),
- Aufstellungsort der Geräte (z. B. Gebäude, Halle, Raum)
- Status der ICS-Systeme (in Betrieb, im Test, in Planung) und
- Verantwortliche für den Betrieb der ICS-Systeme.

Beispiel: RECPLAST GmbH

In der folgenden Tabelle sind Beispiele für ICS-Systeme aufgelistet:

A.1 Strukturanalyse der RECPLAST GmbH									
Bezeichnung	Beschreibung des Zielobjektes / der Gruppe der Zielobjekte	Plattform / Baustein	Ort	Gebäude	Raum	Anzahl	Status	Benutzer	Verantwortlich / Administrator
S100	**SPS:** Die Maschinensteuerung für die Produktionsanlagen wird über die SPS programmiert.	SPS	Bonn	Beuel	Produktion	3	in Betrieb	Haustechnik	Haustechnik
S101	**SCADA:** Das Computersystem ermöglicht die Überwachung der Produktionsprozesse	SCADA / HMI	Bonn	Beuel	Produktionshalle	1	in Betrieb	Alle Mitarbeiter	Haustechnik
S103	**Server für Betriebsdatenerfassung:** Der Server wird für die Anwendung BDE benötigt. Dieser Server ist mit den Produtionsanlagen verbunden.	Server unter Unix	Bonn	Beuel	Serverraum	1	in Betrieb	Alle Mitarbeiter	IT-Betrieb

Abbildung 17: Auszug aus der Strukturanalyse der RECPLAST GmbH (ICS-Systeme)

8.1.7 Erhebung sonstiger Geräte

In Institutionen werden je nach Branche unterschiedlichste Geräte eingesetzt, um die Geschäftsprozesse zu unterstützen. Neben IT-Systemen, die unmittelbar als solche zu identifizieren sind, können auch viele andere Arten von Geräten Einfluss auf die Informationssicherheit haben. Zu solchen Geräten gehören beispielsweise Geräte mit Funktionalitäten aus dem Bereich IoT.

Auch Geräte wie Klimaanlagen, Gefahrenmeldeanlagen oder Kaffeemaschinen, die nicht der direkten Unterstützung der Informationsverarbeitung oder anderer Geschäftsprozesse dienen, können die Informationssicherheit beeinträchtigen, z. B. wenn ein Kabelbrand Folgeschäden nach sich zieht, aber auch, wenn Geräte dieser Art zur besseren Ressourcensteuerung ins IT-Netz integriert werden.

Daher sollte die Institution einen Überblick darüber haben, welche Geräte wo eingesetzt werden und welche Anforderungen an die Informationssicherheit sich hieraus ergeben können, wie regelmäßige Überprüfung der Betriebssicherheit, Wartung oder Einspielen von Patches.

Für die IT-Grundschutz-Modellierung sollten die Geräte mit IoT-Funktionalität erfasst werden, die vernetzt sind, insbesondere auch solche, die nicht im zuvor betrachteten Netzplan aufgeführt sind. Solche Geräte sollten möglichst zu Gruppen zusammengefasst und als ein Objekt behandelt werden.

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

- eine eindeutige Bezeichnung der Geräte bzw. der jeweiligen Gruppe (bei Gruppen sollte auch die Anzahl der zusammengefassten Geräte vermerkt sein),
- Beschreibung (Typ und Funktion),
- Plattform (z. B. Betriebssystem, Art der Netzanbindung),
- Aufstellungsort der Geräte,
- Status der IT-Systeme (in Betrieb, im Test, in Planung) und
- Verantwortliche für den Betrieb der Geräte.

Internet of Things (IoT)

IoT-Geräte sind häufig dadurch gekennzeichnet, dass sie überschaubare, begrenzte Außenmaße haben, oftmals preislich unterhalb von Grenzen liegen, die einen aufwendigen Beschaffungsvorgang in Institutionen nach sich ziehen, und/oder die Internet-Funktionalität nicht hervorsticht. Daher ist es wahrscheinlich, dass bei jeder Art von Übersicht oder Bestandserhebung IoT-Geräte übersehen werden. Es ist wichtig, sich darüber einen Überblick zu verschaffen,

- welche IoT-Geräte in der Institution derzeit oder demnächst eingesetzt werden und
- wer die Akteure in der Institution sind, die typischerweise IoT-Geräte nutzen und mit diesen ins Gespräch zu kommen.

Dafür kann es ein sinnvoller Ansatz für den ISB sein, in verschiedene Räumlichkeiten der Institution zu gehen und zu überlegen, welche der dort vorhandenen Komponenten Strom benötigen und ob diese über IT-Netze vernetzt sein könnten. Der ISB sollte insbesondere mit den Kollegen der Haustechnik, aber auch den anderen Geräte-Verantwortlichen sprechen und sich die Funktionalitäten der verschiedenen Geräte erläutern lassen. Die Vernetzung könnte beispielsweise über IT-Verkabelung oder WLAN mit dem LAN erfolgen, über Mobilfunk mit dem Internet, aber auch über freie WLANs in der Umgebung oder andere Funkschnittstellen wie Bluetooth erfolgen. Zusätzlich sollten regelmäßig Netzscans durchgeführt werden und dabei nach nicht zuordenbaren Geräten gesucht werden.

Geräte mit IoT-Funktionalitäten können in Institutionen beispielsweise sein:

- Durch Mitarbeiter oder Externe mitgebrachte private Geräte, z. B. Smartwatches, digitale Bilderrahmen, Wetterstationen, Fitnessarmbänder und andere Gadgets.
- Durch die Institution beschaffte und betriebene Geräte wie Brand-, Gas- und andere Warnmelder, Kaffeemaschinen oder Elemente der Gebäudesteuerung. Die Übergänge zu ICS-Systemen sind hier fließend.

Dabei sind IoT-Geräte nicht immer auf den ersten Blick als solche zu erkennen, beispielsweise wenn die IoT-Funktionalität kein kaufentscheidendes Merkmal ist, aber für den Hersteller dadurch eine für ihn gewinnbringende Datensammlung möglich wird, z. B. über Art und Menge der Verbrauchsmaterialien.

Ein Beispiel für Geräte, in denen sich IoT-Funktionalitäten verstecken könnten, sind Komfortmöbel, die sich automatisch an die jeweiligen Benutzer anpassen und nicht nur lokal die Einstellungen speichern, sondern diese über IT-Netze mit anderen Arbeitsplätzen austauschen, so dass Mitarbeiter an beliebigen Arbeitsplätzen arbeiten können ("Smart Workplaces").

Beispiel: RECPLAST GmbH

In der folgenden Tabelle sind Beispiele für sonstige und IoT-Geräte aufgeführt:

A.1 Strukturanalyse der RECPLAST GmbH									
Bezeichnung	Beschreibung des Zielobjektes / der Gruppe der Zielobjekte	Plattform / Baustein	Ort	Gebäude	Raum	Anzahl	Status	Benutzer	Verantwortlich / Administrator
S200	**Alarmanlage BG:** Die Alarmanlage wird von der Pforte aus gesteuert. Zuständig für die Liegenschaft in Bad Godesberg.	Alarmanlage	Bonn	BG	Pforte	1	in Betrieb	Pförtner, Arbeitssicherheits-fachkraft	Haustechnik
S201	**Alarmanlage Beuel:** Die Alarmanlage wird seit 1996 eingesetzt und erfüllt die Grundlagen einer Alarmanlage. Mit dieser Alarmanlage wird die Liegenschaft in Beuel abgedeckt.	Alarmanlage	Bonn	Beuel	Pforte	1	in Betrieb	Arbeitssicherheits-fachkraft	Haustechnik
S202	**Video-Überwachung:** Rund um das Gelände in der Liegenschaft Bad Godesberg sind die Türen und teilweise die Fenster mit Kameras überwacht. Innen wird jeder Notausgang bewacht.	Server unter Unix	Bonn	Beuel	Serverraum	1	in Betrieb	Pforte	IT-Betrieb
S203	**Kühlschrank IT-Abteilung:** In der IT-Abteilung ist ein Kühlschrank, der mittels einer internen Kamera und einer App eine Inventarliste führt.	Kühlschrank	Bonn	BG	Teeküche EG	1	in Betrieb	IT-Abteilung	Haustechnik

Abbildung 18: Auszug aus der Strukturanalyse der RECPLAST GmbH (sonstige und IoT-Geräte)

Aktionspunkte zu 8.1.5, 8.1.6 und 8.1.7 Erhebung der IT-, ICS-Systeme und sonstige Geräte

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

8.1.8 Erfassung der Räume

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

In ein Sicherheitskonzept müssen alle Liegenschaften einbezogen werden, innerhalb derer die betrachteten Geschäftsprozesse und Fachaufgaben betrieben werden. Dazu gehören Betriebsgelände, Gebäude, Etagen, Räume sowie die Wegstrecke zwischen diesen. Alle Kommunikationsverbindungen, die über für Dritte zugängliche Gelände verlaufen, müssen als Außenverbindungen behandelt werden. Dies gilt auch für drahtlose Kommunikationsverbindungen, wenn nicht ausgeschlossen werden kann, dass Dritte darauf zugreifen können. Nicht vergessen werden sollten auch Räumlichkeiten, die außerhalb der offiziellen Liegenschaften liegen, die aber auch sporadisch oder regelmäßig genutzt werden, um dort Geschäftsprozesse und Fachaufgaben zu bearbeiten. Dazu gehören beispielsweise Telearbeitsplätze oder temporär angemietete Arbeitsplätze und Lagerflächen.

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-, ICS- oder IoT-Systeme aufgestellt oder die für deren Betrieb genutzt werden. Dazu gehören Räume, die ausschließlich dem IT-Betrieb dienen (wie Serverräume, Datenträgerarchive), solche, in denen unter anderem IT-, ICS- oder IoT-Systeme betrieben werden (wie Büroräume oder Werkhallen), aber auch die Wegstrecken, über die Kommunikationsverbindungen laufen. Wenn IT-Systeme statt in einem speziellen Technikraum in einem Schutzschrank untergebracht sind, ist der Schutzschrank wie ein Raum zu erfassen.

Hinweis: Bei der Erhebung der IT-, ICS- und IoT-Systeme sind schon die Aufstellungsorte miterfasst worden.

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

Beispiel: RECPLAST GmbH

Im folgenden Ausschnitt wird anhand des fiktiven Beispiels der RECPLAST GmbH gezeigt, wie eine tabellarische Übersicht über die Räume aussehen könnte. Räume können wie alle Zielobjekte gruppiert werden. Dies ist möglich, sofern die Räume eine ähnliche Ausstattung und vergleichbare Sicherheitsanforderungen haben.

A.1 Strukturanalyse der RECPLAST GmbH

Bezeichnung	Beschreibung des Zielobjektes / der Gruppe der Zielobjekte	Plattform / Baustein	Ort	Gebäude	Raum	Anzahl	Status	Benutzer	Verantwortlich / Administrator
R001	**Büroraum** Ein Standard-Büroraum enthält Schreibtische, Schränke, die erforderliche Verkabelung, Präsenzmelder für die Alarmanlage. Die Büroräume sind abschließbar. Die Anzahl der Mitarbeiter je Büroraum ist begrenzt auf ein bis sechs Mitarbeiter.	Büroraum	Bonn	BG	-	27	in Betrieb	Alle Mitarbeiter	Gebäudemanagement
R002	**Besprechungsräume:** Verteilt in der Liegenschaft Bad Godesberg gibt es Besprechungsräume, die mit Tischen, Stühlen, Schränken und Verkabelung bestückt sind. In diesen Räumen dürfen sich Besucher in Begleitung von Mitarbeitern aufhalten.	Besprechungsraum	Bonn	BG	-	5	in Betrieb	Alle Mitarbeiter	Gebäudemanagement
R003	**Häuslicher Arbeitsplatz:** Einige Mitarbeiter dürfen von ihrem Wohnort aus arbeiten. Der häusliche Arbeitsplatz muss vor Dritten so geschützt sein, dass alle Firmenunterlagen sicher verschlossen werden können. Der ISB kontrolliert mit vorheriger Ankündigung einen häuslichen Arbeitsplatz.	Telearbeit	mobiler Arbeitsplatz	-	-	27	in Betrieb	Telearbeitnehmer	ISB
R004	**Mobiler Arbeitsplatz:** Alle Mitarbeiter, die ein Notebook als IT-System nutzen, können mobil arbeiten. Dies ist innerhalb als auch außerhalb der Räumlichkeiten der RECPLAST GmbH gestattet. Es müssen hierzu verbindliche Richtlinien eingehalten werden. Firmenunterlagen dürfen nur begrenzt mitgenommen werden.	Mobiler Arbeitsplatz	mobiler Arbeitsplatz	-	-	75	in Betrieb	Führungskräfte, Mitarbeiter	IT-Betrieb

Abbildung 19: Auszug aus der Strukturanalyse der RECPLAST GmbH (Räume)

Aktionspunkte zu 8.1.8 Erfassung der Räume

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

8.2 Schutzbedarfsfeststellung

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

Die Schutzbedarfsfeststellung für den Informationsverbund gliedert sich in mehrere Schritte:

- Definition der Schutzbedarfskategorien
- Schutzbedarfsfeststellung für Geschäftsprozesse und Anwendungen
- Schutzbedarfsfeststellung für IT-Systeme, IoT- und ICS-Geräte
- Schutzbedarfsfeststellung für Gebäude, Räume, Werkhallen, etc.
- Schutzbedarfsfeststellung für Kommunikationsverbindungen
- Schlussfolgerungen aus den Ergebnissen der Schutzbedarfsfeststellung

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

Die Vorgehensweise hierfür wird in den folgenden Abschnitten detailliert dargestellt.

8.2.1 Definition der Schutzbedarfskategorien

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

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

Hinweis:

Es kann für eine Institution auch sinnvoll sein, weitere Kategorien zu definieren. Beispielsweise kann eine Abstufung nach unten, z. B. "unkritisch", eingeführt werden. (Diese könnte wie folgt definiert sein: "Schäden an Ressourcen der Schutzbedarfskategorie "unkritisch" haben keine oder nur minimale Beeinträchtigungen der Institution zur Folge.")

Werden nur ein oder zwei Kategorien genutzt, ist die damit erreichbare Abstufung meist nicht granular genug. Werden dagegen fünf oder mehr Schutzbedarfskategorien verwendet, ist eine klare Unterscheidung zwischen den einzelnen Stufen schwieriger. Zudem ist die Zuordnung von Ressourcen zu einer der möglichen Schutzbedarfskategorien schwer nachvollziehbar und es steigt dadurch auch der Aufwand sowohl bei der Zuordnung als auch bei Revisionen.

Eine andere Möglichkeit ist es, für Vertraulichkeit andere Kategorien als für Integrität oder Verfügbarkeit zu nutzen. Einige Institutionen unterteilen beispielsweise Vertraulichkeit in die Kategorien "offen", "intern", "vertraulich" und "geheim", aber die Kategorien Integrität oder Verfügbarkeit nur in zwei Stufen "normal" und "kritisch".

Wenn mehr als drei Schutzbedarfskategorien definiert werden, so ist zu überlegen, welche der neu definierten Kategorien den Schutzbedarfskategorien „hoch“ bzw. „sehr hoch“ entsprechen, denn diese Information wird zur Überprüfung der Entscheidung benötigt, welche Objekte in die Risikoanalyse aufgenommen werden.

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

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

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

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

Hinweis: Auch die Art und Anzahl der betrachteten Szenarien können individuell angepasst werden. Je nach Institution gibt es unterschiedliche Schwerpunkte, auf die sich das Sicherheitsmanagement konzentrieren kann. So könnte das Szenario "Beeinträchtigung des informationellen Selbstbestimmungsrechts" entfallen, wenn beispielsweise in der Institution das Datenschutz-Management dieses Szenario bereits ausreichend betrachtet hat. In vielen Institutionen kann das Szenario "Beeinträchtigung der persönlichen Unversehrtheit" weggelassen werden, es sei denn, es handelt sich um ein Unternehmen, bei dem Fehlfunktionen von IT-Systemen unmittelbar Personenschäden nach sich ziehen können. Dies könnte beispielsweise im Gesundheitswesen oder in Produktionsbereichen der Fall sein.

Es könnten auch zusätzliche Szenarien betrachtet werden wie beispielsweise

- Einschränkung der Dienstleistungen für Dritte oder
- Auswirkungen auf weitere Infrastrukturen außerhalb des eigenen Informationsverbundes (z. B. Rechenzentren, IT-Betrieb von Kunden oder Dienstleistern).

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

Schutzbedarfskategorie "normal"	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen • Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung erscheint nicht möglich.
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit liegt zwischen 24 und 72 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.

Tabelle 1: Schutzbedarfskategorie „normal“

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

Tabelle 2: Schutzbedarfskategorie „hoch“

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

Tabelle 3: Schutzbedarfskategorie „sehr hoch“

Wenn bei individuellen Betrachtungen festgestellt wird, dass über diese sechs Schadensszenarien hinaus weitere in Frage kommen, sollten diese entsprechend ergänzt werden. Für alle Schäden, die sich nicht in diese Szenarien abbilden lassen, muss ebenfalls eine Aussage getroffen werden, wo die Grenzen zwischen "normal", "hoch" oder "sehr hoch" zu ziehen sind.
Darüber hinaus sollten die individuellen Gegebenheiten der Institution berücksichtigt werden: Bedeutet in einem Großunternehmen ein Schaden in Höhe von 200.000,- Euro gemessen am Umsatz noch einen geringen Schaden, so kann für ein Kleinunternehmen schon ein Schaden in Höhe von 10.000,- Euro existentiell bedrohlich sein. Daher kann es sinnvoll sein, eine prozentuale Größe als Grenzwert zu definieren, der sich am Gesamtumsatz, am Gesamtgewinn oder an einer ähnlichen Bezugsgröße orientiert.

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

Es kann erforderlich sein, für den Bereich ICS die Schutzbedarfskategorien separat festzulegen, aber diese auf die des restlichen Informationsverbundes abzustimmen. In produzierenden Bereichen ist es beispielsweise oftmals erforderlich, für die jeweiligen Kategorien kürzere Ausfallzeiten festzulegen als im Bereich der Büro-IT. Zeitliche Vorgaben können z. B. aus Wartungsverträgen abgeleitet werden. Unter Umständen müssen auch andere Punkte angepasst werden. Auch im Datenschutz muss der Schutzbedarf festgelegt werden, um angemessen technische und organisatorische Schutzmaßnahmen bestimmen und konfigurieren zu können. Das Standard-Datenschutzmodell (SDM) bietet eine ganze Reihe an Kriterien, um das Risiko eines Grundrechtseingriffs, und daraus folgend des Schutzbedarfs, anhand von drei Stufen zu bestimmen. Das SDM bietet zudem Hilfestellungen, sollten die Schutzbedarfe aus Sicht der Informationssicherheit und des Datenschutzes nicht übereinstimmen.

Bei der Festlegung der Grenze zwischen "normal" und "hoch" sollte berücksichtigt werden, dass für den normalen Schutzbedarf die Basis- und Standard-Sicherheitsanforderungen des IT-Grundschutzes ausreichen sollten. Die getroffenen Festlegungen sind in geeigneter Weise im Sicherheitskonzept zu

dokumentieren, da hiervon die Auswahl von Sicherheitsmaßnahmen und damit meist Folgekosten abhängen.

Aktionspunkte zu 8.2.1 Definition der Schutzbedarfskategorien
• Typische Schadensszenarien für die Definition von Schutzbedarfskategorien betrachten • Schutzbedarfskategorien "normal", "hoch" und "sehr hoch" definieren beziehungsweise an die eigene Institution anpassen

8.2.2 Vorgehen bei der Schutzbedarfsfeststellung

Zunächst wird der Schutzbedarf der Geschäftsprozesse und Anwendungen bestimmt. Anschließend wird daraus der Schutzbedarf der einzelnen Objekte (z. B. IT-Systeme, Räume und Kommunikationsverbindungen) abgeleitet.

Die Grundlage zur Bestimmung des Schutzbedarfs verschiedener Objekte ist der Schutzbedarf der Geschäftsprozesse und der zugehörigen Informationen. Der für diese ermittelte Schutzbedarf vererbt sich auf die für deren Verarbeitung genutzten Objekte, also Anwendungen, IT-Systeme, ICS- und sonstige Geräte, Räume und Kommunikationsverbindungen (**Vererbung**).

Zur Ermittlung des Schutzbedarfs eines Objektes müssen die möglichen Schäden der relevanten Teilobjekte in ihrer Gesamtheit betrachtet werden. Beispielsweise müsste bei einem IT-System beleuchtet werden, welche Auswirkungen Schäden bei den darauf betriebenen Anwendungen und den damit verarbeiteten Informationen haben. Im Wesentlichen bestimmt der Schaden bzw. die Summe der Schäden mit den schwerwiegendsten Auswirkungen den Schutzbedarf eines Objektes **(Maximumprinzip)**.

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

Werden mehrere Anwendungen bzw. Informationen auf einem IT-System (oder in einem Raum oder über eine Kommunikationsverbindung) 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 Objektes, also hier des IT-Systems, entsprechend **(Kumulationseffekt)**.

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

Auch der umgekehrte Effekt kann eintreten. So ist es möglich, dass eine Anwendung einen hohen Schutzbedarf besitzt, ihn aber deshalb nicht auf ein betrachtetes IT-System überträgt, weil auf diesem IT-System nur unwesentliche Teilbereiche der Anwendung laufen. Hier ist der Schutzbedarf zu relativieren **(Verteilungseffekt)**. Der Verteilungseffekt kann natürlich auch bei anderen Zielobjekten wie Räumen, Gebäuden oder Kommunikationsverbindungen auftreten.

Beispiel: Der Verteilungseffekt tritt hauptsächlich bezüglich des Grundwertes Verfügbarkeit auf. So kann bei redundanter Auslegung von IT-Systemen der Schutzbedarf der Einzelkomponenten niedriger

sein als der Schutzbedarf der Gesamtanwendung. Auch im Bereich der Vertraulichkeit sind Verteilungseffekte vorstellbar: Falls sichergestellt ist, dass ein Client nur unkritische Daten einer hochvertraulichen Datenbankanwendung abrufen kann, so besitzt der Client im Vergleich zum Datenbank-Server unter Umständen einen geringeren Schutzbedarf.

Ein Verteilungseffekt tritt häufig auf, wenn bei der Einrichtung oder dem Aufbau von Zielobjekten durch entsprechende Redundanzen bereits den Anforderungen an einen hohen Schutzbedarf Rechnung getragen wurde. Dies ist im Grunde ein Vorgriff auf Betrachtungen, die im Rahmen der Risikoanalyse erforderlich sind. Deshalb sollten im Rahmen der Schutzbedarfsfeststellung getroffene Entscheidungen sorgfältig dokumentiert werden.

Beispiel: Bei Anwendungen, die im Hinblick auf Verfügbarkeit hohen Schutzbedarf haben, wurden bereits Redundanzen vorgesehen, unter anderem Ausweicharbeitsplätze in Nachbargebäuden. Durch die entstandenen Verteilungseffekte haben diese Arbeitsplätze normalen Schutzbedarf bezüglich Verfügbarkeit, solange ausreichend Ausweicharbeitsplätze zur Verfügung stehen.

Die Schutzbedarfsfeststellung ist ein **iterativer Prozess**. Bereits ganz am Anfang, bei der ersten Diskussion darüber, welche Geschäftsprozesse und Informationen welche Bedeutung für die Institution haben, wird eine erste, grobe Schutzbedarfsfeststellung durchgeführt. Auch nach Durchführung von Risikoanalysen sollte die Schutzbedarfsfeststellung erneut angeschaut werden, ob sie angepasst werden muss, da sich während der Risikoanalyse und der Auswahl von Maßnahmen neue Erkenntnisse für den Schutzbedarf von Assets ergeben können.

8.2.3 Schutzbedarfsfeststellung für Geschäftsprozesse und Anwendungen

Um den Schutzbedarf in den verschiedenen Bereichen eines Informationsverbundes zu bestimmen, muss zunächst der Schutzbedarf der Geschäftsprozesse und der zugehörigen Informationen ermittelt werden. Darauf aufbauend wird daraus der Schutzbedarf der einzelnen Anwendungen, IT-Systeme, ICS- und sonstigen Geräte, Räume und Kommunikationsverbindungen abgeleitet.

Um den Schutzbedarf der Geschäftsprozesse zu ermitteln, sollte zunächst die Bedeutung der einzelnen Geschäftsprozesse für die Institution beleuchtet werden. Davon ausgehend sollte hinterfragt werden, welche Abhängigkeiten zwischen Geschäftsprozessen und Anwendungen bestehen und wie die sich daraus ergebenden Risiken entschärft werden können. Hierzu hat es sich bewährt, mit der Fragestellung "Was wäre, wenn...?" zusammen mit den Anwendern realistische Schadensszenarien zu diskutieren und die zu erwartenden materiellen oder ideellen Schäden zu beschreiben. Oft führt dies auch dazu, dass kritische Abhängigkeiten zwischen Geschäftsprozessen und weiteren Zielobjekten aufgedeckt werden, die vorher nicht im Fokus standen.

Aus dem Schutzbedarf der Geschäftsprozesse ergibt sich der Schutzbedarf der Anwendungen, die für deren Erledigung eingesetzt werden.

Hinweis: Zur Einschätzung des Schutzbedarfs sollten die geeigneten Ansprechpartner gesucht werden, es ist nicht erforderlich, größere Gruppe von Benutzern zu befragen. Beispielsweise ist es zur Bewertung des Schutzbedarfs bestimmter zentraler Dienste wie zum Beispiel DNS oder E-Mail ausreichend, den Schutzbedarf durch die Organisationseinheit festlegen zu lassen, die als Dienstanbieter für die Institution auftritt (meist die IT-Abteilung oder das Provider-Management). Der Schutzbedarf dieser Dienste ist in der Institution zu kommunizieren. Wird ein höherwertiger Schutzbedarf der Dienste durch einzelne Fachabteilungen benötigt, so sind mögliche Lösungen zwischen Fachabteilung, Sicherheitsmanagement und dem Betreiber oder Anbieter des Dienstes zu erörtern. Ein IT-Dienstleister kann im Regelfall seine Services nicht für jede mögliche Schutzbedarfskategorie bereitstellen. Deshalb wird er seine Dienste mit einer von ihm festgelegten Schutzbedarfseignung anbieten. Der Informationseigentümer muss bei Nutzung eines Services für seinen Geschäftsprozess entscheiden, ob die ihm vom IT-Dienstleister angebotene Schutzbedarfseignung ausreicht oder ob zusätzliche Sicherheitsmaßnahmen infolge höheren Schutzbedarfs umgesetzt werden müssen.

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

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

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

Bei komplexen Geschäftsprozessen, insbesondere wenn diese hohen oder sehr hohen Schutzbedarf haben, kann es sinnvoll sein, diese in Teilprozesse zu zerlegen. Wenn dabei der Bereich mit hohem oder sehr hohem Schutzbedarf auf wenige Teilprozesse eingegrenzt werden kann, hat das den Vorteil, dass sich der hohe bzw. sehr hohe Schutzbedarf auf wenige Objekte vererbt.

Um die Ergebnisse der Schutzbedarfsfeststellung und die daraus resultierenden Entscheidungen im Rahmen des Informationssicherheitsmanagements später jederzeit nachvollziehen zu können, müssen die Ergebnisse der Schutzbedarfsfeststellung der Geschäftsprozesse und Anwendungen gut dokumentiert werden. Dabei ist darauf zu achten, dass nicht nur die Festlegung des Schutzbedarfs dokumentiert wird, sondern auch die entsprechenden Begründungen. Diese Begründungen erlauben es später, die Festlegungen zu überprüfen und weiter zu verwenden.

Beispiel: RECPLAST GmbH
In der nachfolgenden Tabelle werden für das Unternehmen RECPLAST GmbH die wesentlichen Anwendungen, deren Schutzbedarf und die entsprechenden Begründungen erfasst.

A.2 Schutzbedarfsfeststellung der RECPLAST GmbH

Bezeichnung	Beschreibung des Zielobjektes / der Gruppe der Zielobjekte	Plattform / Baustein	Vertraulichkeit	Begründung für die Vertraulichkeit	Integrität	Begründung für die Integrität	Verfügbarkeit	Begründung für die Verfügbarkeit
A003	Textverarbeitung, Tabellenkalkulation	Office-Produkt 2010	normal	Die Anwendung selbst enthält keine Informationen.	normal	Die Anwendung selbst enthält keine Informationen	normal	Die Anwendung wird lokal installiert. Die Lizenzen sind entsprechend aufgehoben, so dass eine Neuinstallation schnell ermöglicht werden kann. Eine Ausfallzeit von mehr als 24 Stunden ist
A007	Lotus Notes	Lotus Notes	hoch	Über das E-Mailsystem werden viele, teilweise vertrauliche Informationen versendet. Durch die Anwendung werden alle E-Mails verschlüsselt.	normal	Durch eine Signatur kann die Integrität einer E-Mail festgestellt werden.	sehr hoch	Das Mailsystem sollte auch dann zur Verfügung stehen, falls andere Kommunikationsmittel ausfallen (z. B. Faxserver)
C002	Laptop Verwaltung	Client unter Windows 10	normal	Maximumprinzip Auf dem Arbeitsplatzrechner werden keine Informationen gespeichert	normal	Maximumprinzip Auf dem Arbeitsplatzrechner werden keine Informationen gespeichert	hoch	Es ist ein Ausfall von höchstens 4 Stunden tolerierbar.
G003	Vertrieb Berlin	Gebäude	hoch	Maximumprinzip In dem Gebäude werden grundsätzlich alle Informationen verarbeitet	hoch	Maximumprinzip In dem Gebäude werden grundsätzlich alle Informationen verarbeitet	hoch	Maximumprinzip In dem Gebäude werden grundsätzlich alle Informationen verarbeitet
K001	Internet - Bonn BG	-	hoch	Maximumprinzip	hoch	Maximumprinzip	hoch	Maximumprinzip
R003	Häuslicher Arbeitsplatz	Telearbeit	hoch	Maximumprinzip	hoch	Maximumprinzip	hoch	Maximumprinzip
N001	Router Internetanbindung	Router und Switches	hoch	Der Router stellt den Anschluss zwischen dem Internet und dem Produktionsnetz dar.	normal	Zutritt, Zugang und Zugriff nur für autorisierte Personen möglich	normal	Ersatzgerät liegt auf Lager und kann schnell durch den IT-Betrieb ausgetauscht werden
S020	Virtueller Server (Konfiguration 1)	Server unter Unix	normal	Die Server sind im eigenen Serverraum mit Zugriff-, Zugangs- und Zutrittsberechtigung	normal	Die Server sind im eigenen Serverraum mit Zugriff-, Zugangs- und Zutrittsberechtigung	normal	Durch die Redundanz der Server kann bei Ausfall eines Servers der Dienst von einem anderen Server übernommen werden.

Abbildung 20: Auszug aus der Schutzbedarfsfeststellung der RECPLAST GmbH

An dieser Stelle kann es sinnvoll sein, über diese Informationen hinaus den Schutzbedarf auch aus einer gesamtheitlichen Sicht der Geschäftsprozesse oder Fachaufgaben zu betrachten. Dazu bietet es

sich an, den Zweck einer Anwendung in einem Geschäftsprozess oder in einer Fachaufgabe zu beschreiben und daraus wiederum deren Bedeutung abzuleiten. Diese Bedeutung kann wie folgt klassifiziert werden:

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

- **normal:** Der Geschäftsprozess bzw. die Fachaufgabe kann mit tolerierbarem Mehraufwand mit anderen Mitteln (z. B. manuell) durchgeführt werden.
- **hoch:** Der Geschäftsprozess bzw. die Fachaufgabe kann nur mit deutlichem Mehraufwand mit anderen Mitteln durchgeführt werden.
- **sehr hoch:** Der Geschäftsprozess bzw. die Fachaufgabe kann ohne die Anwendung überhaupt nicht durchgeführt werden.

Der Vorteil, eine solche ganzheitliche Zuordnung vorzunehmen, liegt insbesondere darin, dass bei der Schutzbedarfsfeststellung die Leitungsebene als Regulativ für den Schutzbedarf der einzelnen Anwendungen agieren kann. So kann es sein, dass ein Verantwortlicher für eine Anwendung deren Schutzbedarf aus seiner Sicht als "normal" einschätzt, die Leitungsebene aus Sicht des Geschäftsprozesses bzw. der Fachaufgabe diese Einschätzung jedoch nach oben korrigiert.

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

Aktionspunkt zu 8.2.3 Schutzbedarfsfeststellung für Geschäftsprozesse und Anwendungen

- Schutzbedarf der erfassten Geschäftsprozesse und Anwendungen anhand von Schadensszenarien und Fragenkatalogen ermitteln
- Schutzbedarf der Geschäftsprozesse und Anwendungen und die entsprechenden Begründungen tabellarisch dokumentieren

8.2.4 Schutzbedarfsfeststellung für IT-Systeme

Um den Schutzbedarf eines IT-Systems festzustellen, müssen zunächst die Anwendungen betrachtet werden, die in direktem Zusammenhang mit dem IT-System stehen. Eine Übersicht, welche Anwendungen für die unterschiedlichen IT-Systeme relevant sind, wurde im Rahmen der Strukturanalyse (siehe Kapitel 8.1) ermittelt. Der Schutzbedarf der Geschäftsprozesse und Anwendungen (siehe Kapitel 8.2.3) fließt in die Schutzbedarfsfeststellung für die jeweils betroffenen IT-Systeme ein. Hierbei ist darauf zu achten, dass nicht nur die IT-Systeme berücksichtigt werden, auf denen die jeweilige Anwendung installiert ist. Vielmehr ist auch der Datenfluss der Anwendung zu beachten, über den der Schutzbedarf der Anwendung auf die dazwischenliegenden Netzkomponenten vererbt wird.

Zur Ermittlung des Schutzbedarfs eines IT-Systems müssen nun die möglichen Schäden der relevanten Anwendungen in ihrer Gesamtheit betrachtet werden. Die Ergebnisse der Schutzbedarfsfeststellung der IT-Systeme sollten wiederum in einer Tabelle festgehalten werden. Darin sollte verzeichnet sein, welchen Schutzbedarf jedes IT-System bezüglich Vertraulichkeit, Integrität und Verfügbarkeit hat. Der Gesamt-Schutzbedarf eines IT-Systems leitet sich wiederum aus dem Maximum des Schutzbedarfs bezüglich der drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit ab. Ein IT-System ist also hochschutzbedürftig, wenn es bezüglich eines oder mehrerer Grundwerte den Schutzbedarf "hoch" hat. Der Schutzbedarf eines IT-Systems sollte für alle drei Grundwerte einzeln dokumentiert werden, da sich hieraus typischerweise verschiedene Arten von Sicherheitsmaßnahmen ergeben.

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

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

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

A.2 Schutzbedarfsfeststellung der RECPLAST GmbH								
Bezeichnung	Beschreibung des Zielobjektes / der Gruppe der Zielobjekte	Plattform / Baustein	Vertraulichkeit	Begründung für die Vertraulichkeit	Integrität	Begründung für die Integrität	Verfügbarkeit	Begründung für die Verfügbarkeit
N001	Router Internetanbindung	Router und Switches	hoch	Zutritt, Zugang und Zugriff nur für autorisierte Personen möglich	normal	Zutritt, Zugang und Zugriff nur für autorisierte Personen möglich	normal	Ersatzgerät liegt auf Lager und kann schnell durch den IT-Betrieb ausgetauscht werden
N002	Firewall Internet-Eingang	Firewall	hoch	Die Konfigurationseigenschaften müssen vertraulich bleiben. Diese regeln den Datenverkehr zwischen dem Internet und der RECPLAST	normal	Zutritt, Zugang und Zugriff nur für autorisierte Personen möglich	normal	Ersatzgerät liegt auf Lager und kann schnell durch den IT-Betrieb ausgetauscht werden
N003	Switch - Verteilung	Router und Switches	normal	Zutritt, Zugang und Zugriff nur für autorisierte Personen möglich	normal	Zutritt, Zugang und Zugriff nur für autorisierte Personen möglich	normal	Ersatzgerät liegt auf Lager und kann schnell durch den IT-Betrieb ausgetauscht werden
N004	Router Bonn BG - Beuel	Router und Switches	normal	Die Konfigurationseigenschaften müssen vertraulich bleiben. Diese regeln den Datenverkehr zwischen den Standorten der RECPLAST	normal	Zutritt, Zugang und Zugriff nur für autorisierte Personen möglich	normal	Ersatzgerät liegt auf Lager und kann schnell durch den IT-Betrieb ausgetauscht werden
S008	Print-Server	Windows Server 2012	normal	Es werden keine vertraulichen Dokumente ausgedruckt.	normal	Fehlfunktionen werden durch ein Monitoring schnell erkannt, gemeldet und können sofort behoben werden	normal	Kann schnell auf einem anderen virtuellen Server installiert werden.
S020	Virtueller Server (Konfiguration 1)	Server unter Unix	normal	Die Server sind im eigenen Serverraum mit Zugriff-, Zugangs- und Zutrittsberechtigung untergebracht.	normal	Die Server sind im eigenen Serverraum mit Zugriff-, Zugangs- und Zutrittsberechtigung untergebracht.	normal	Durch die Redundanz der Server kann bei Ausfall eines Servers der Dienst von einem anderen Server übernommen werden.
S033	Server Produktion	Server unter Unix	sehr hoch	Die verarbeiteten Informationen sind für die Produktion notwendig. Insbesondere werden Stücklisten, Arbeitspläne und weitere Informationen zum Produktionsprozess auf diesem Server in einer Datenbank gespeichert.	hoch	Die Informationen auf dem Server müssen für den produzierenden Bereich vollständig und korrekt vorliegen. Insbesondere Stücklisten und Arbeitspläne dürfen nicht unbeachtet verändert werden.	sehr hoch	Der Server muss zu allen Produktionszeiten (täglich 6 - 22 Uhr) zur Verfügung stehen. Einen Ersatz-Server gibt es nicht. Wartungsarbeiten werden grundsätzlich am Wochenende vorgenommen.

Abbildung 21: Auszug aus der Schutzbedarfsfeststellung der RECPLAST GmbH (IT-Systeme)

Schutzbedarfsfeststellung bei virtualisierten Infrastrukturen

Wird Virtualisierung eingesetzt, bleibt die Schutzbedarfsfeststellung im Prinzip gleich. Um den Schutzbedarf eines IT-Systems zu bestimmen, müssen zunächst die Anwendungen betrachtet werden, die im direkten Zusammenhang mit dem IT-System stehen. In virtualisierten Infrastrukturen werden in der Regel mehrere IT-Systeme auf einem Virtualisierungsserver betrieben. Der Schutzbedarf der Anwendungen vererbt sich auf die virtuellen IT-Systeme. Die virtuellen IT-Systeme ihrerseits vererben ihren Schutzbedarf an den Virtualisierungsserver. Für den Schutzbedarf eines Virtualisierungsservers lassen sich folgende Fälle unterscheiden:

Vertraulichkeit:

Ist der Schutzbedarf der virtuellen IT-Systeme beispielsweise "normal", so vererbt sich dieser auf den Virtualisierungsserver. Er bekommt in der Regel auch den Schutzbedarf "normal". Es sollte überlegt werden, ob durch Kumulation mehrerer (z. B. kleinerer) Schäden auf dem Virtualisierungsserver ein insgesamt höherer Gesamtschaden entstehen kann. Dann erhöht sich der Schutzbedarf des Virtualisierungsservers entsprechend auf "hoch" (**Kumulationseffekt**).

Integrität:

Das Schutzziel Integrität wird nicht gesondert betrachtet und ist wie Vertraulichkeit zu behandeln.

Verfügbarkeit:

Ist der Schutzbedarf der virtuellen IT-Systeme beispielsweise "normal", dann kommt es durch den Kumulationseffekt in der Regel zu einer Erhöhung der Verfügbarkeit. Gleichzeitig bietet Virtualisierung mit Konzepten wie Cold-, Warm- oder Hot-Standby die Möglichkeit, Redundanzen zu schaffen. Dabei wird parallel zum Produktivsystem ein identisches Ersatzsystem auf einem weiteren physischen Server aufgebaut und entweder ausgeschaltet (Cold-Standby) oder kurzfristig einschaltbar gehalten, aber nicht eingesetzt (Warm-Standby) oder eingeschaltet und synchron gespiegelt mit Daten versorgt (Hot-Standby). Sind entsprechende Maßnahmen umgesetzt, dann sinkt der Schutzbedarf (**Verteilungseffekt**). Es können unter anderem folgende Fälle auftreten:

- Die virtuellen Maschinen weisen in Bezug auf Verfügbarkeit den Schutzbedarf "normal" auf, dann gibt es in der Regel eine Kumulation nach "hoch" und dann durch Verteilung sinkt der Schutzbedarf wieder auf "normal". In diesem Fall reicht der Warm-Standby-Ansatz aus.
- Die virtuellen Maschinen haben Schutzbedarf "hoch" in Bezug auf Verfügbarkeit. Wegen Kumulation kann sich ein insgesamt sehr hoher Schutzbedarf ergeben, der dann wegen Verteilung auf "hoch" gesenkt werden kann, wenn entsprechende Maßnahmen (z. B. Hot-Standby) umgesetzt werden.

Schutzbedarfsfeststellung beim Cloud Computing (IaaS-Compute)

Auch bei Cloud Computing ändert sich gegenüber der oben beschriebenen Schutzbedarfsfeststellung wenig. Bei Angeboten der Form "IaaS-Compute" werden den Benutzern virtuelle Maschinen zur Verfügung gestellt, z. B. über eine Webschnittstelle. Ähnlich wie bei Virtualisierung wird der Schutzbedarf des Virtualisierungsservers durch den Schutzbedarf der auf ihm betriebenen virtuellen IT-Systeme beeinflusst. Techniken wie Live Migration, vMotion oder XenMotion ermöglichen, dass die virtuellen Maschinen zwischen den Virtualisierungsservern verschoben werden oder Host-Systeme bei geringer Last in den Standby-Modus geschaltet oder sogar heruntergefahren werden können, um Strom zu sparen. Die Vorteile, die sich dadurch ergeben, sind unbestritten. Aber die Live Migration, also die Verschiebung von VMs zwischen Virtualisierungsservern, erschwert die Schutzbedarfsfeststellung. Daher wird empfohlen, die Cloud Computing Plattform für unterschiedliche Bereiche (Virtualisierungscluster) abhängig vom Schutzbedarf (zum Beispiel "normal" oder "hoch") auszulegen.

Anwendungen, die denselben Schutzbedarf aufweisen, sollten dann auf einem hierfür vorgesehenen Virtualisierungscluster betrieben werden. Die einzelnen Bereiche sollten untereinander physisch getrennt sein und es sollte sichergestellt sein, dass virtuelle Maschinen nicht bereichsübergreifend verschoben werden können.

Auf eine gesonderte Schutzbedarfsfeststellung für virtuelle IT-Systeme und Virtualisierungsserver kann verzichtet werden.

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

8.2.5 Schutzbedarfsfeststellung für ICS-Systeme

Im Bereich industrieller Steuerungsanlagen muss der Schutzbedarf aller ICS-Systeme festgestellt werden. Die ICS-Systeme wurden bereits in Kapitel 8.1.6 erfasst.

Bei der Feststellung des Schutzbedarfes für die ICS-Systeme muss berücksichtigt werden, dass nicht per se alle Objekte einem sehr hohen Schutzbedarf unterliegen. In enger Abstimmung ist es sinnvoll, mit den Verantwortlichen der ICS-Systeme in einem Gespräch die Schutzbedarfsfeststellung durchzuführen, da diese wissen, welche ICS-Geräte welche Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit haben. Der Schutzbedarf leitet sich hierbei aus dem Anwendungszweck der industriellen Steuerungsanlage ab.

Dabei sollte berücksichtigt werden, dass ICS-Systeme für verschiedene Aufgaben verwendet werden können. So kann in einer Produktionsstraße im Wechsel ein für ein Unternehmen wichtiges umsatzstarkes Produkt produziert werden und ein weniger umsatzstarkes Produkt. Bei der Feststellung des Schutzbedarfs müssen diese Abhängigkeiten beachtet werden (Maximumprinzip).

Für die Definition des Schutzbedarfes kann es sinnvoll sein, die für alle weiteren Schutzbedarfsfeststellungen definierten Klassifikationen zu übernehmen. Darüber hinaus können die Schutzbedarfskategorien entsprechend angepasst formuliert werden.

Beispiel: RECPLAST GmbH

Für ein IT-System aus einer Büroumgebung ist eine Ausfallzeit von bis zu 30 Stunden im normalen Bereich. Diese Ausfallzeit kann auch für den Betrieb von ICS-Systemen sinnvoll sein, möglicherweise ist es jedoch erforderlich, die Ausfallzeit für die ICS-Geräte im normalen Schutzbedarf auf 12 bis 24 Stunden zu reduzieren.

Der Schutzbedarf für jedes ICS-System wird bezüglich Vertraulichkeit, Integrität und Verfügbarkeit ermittelt. Der Gesamt-Schutzbedarf der ICS-Systeme leitet sich nach dem Maximumprinzip bezüglich der drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit ab.

Die Festlegungen des Schutzbedarfs von ICS-Systeme müssen kurz begründet werden, damit die Entscheidungen für Dritte nachvollziehbar sind.

A.2 Schutzbedarfsfeststellung der RECPLAST GmbH

Bezeichnung	Beschreibung des Zielobjektes / der Gruppe der Zielobjekte	Plattform / Baustein	Vertraulichkeit	Begründung für die Vertraulichkeit	Integrität	Begründung für die Integrität	Verfügbarkeit	Begründung für die Verfügbarkeit
S100	SPS	SPS	normal	Der Quellcode enthält nur wenige vertrauliche Informationen. Der Zugriff auf den Quellcode ist auf befugte Personen beschränkt.	sehr hoch	Die Konfigurationsdaten müssen jederzeit korrekt sein.	hoch	Die SPSen müssen jederzeit verfügbar sein. Bei Nichtverfügbarkeit kann die Produktion nicht weiterlaufen.
S101	SCADA	SCADA / HMI	normal	Der Quellcode enthält nur wenige vertrauliche Informationen. Der Zugriff auf den Quellcode ist auf befugte Personen beschränkt.	hoch	Die verarbeiteten Informationen müssen korrekt und vollständig vorhanden sein.	hoch	Ohne den Server können keine Informationen in der Produktion verarbeitet werden.
S103	Server für Betriebsdatenerfassung	Server unter Unix	normal	Maximumprinzip	sehr hoch	Die Betriebsdaten müssen zu jeder Zeit korrekt vorhanden sein	hoch	Ein Ausfall der Betriebsdatensteuerung ist bis 7 Stunden tolerierbar, da es einen entsprechenden Puffer in der Produktion gibt.
S104	Server für Betriebsdatenerfassung	Server unter Unix	normal	Maximumprinzip	sehr hoch	Die Betriebsdaten müssen zu jeder Zeit korrekt vorhanden sein	hoch	Ein Ausfall der Betriebsdatensteuerung ist bis 7 Stunden tolerierbar, da es einen entsprechenden Puffer in der Produktion gibt.

Abbildung 22: Auszug aus der Schutzbedarfsfeststellung der RECPLAST GmbH (ICS-Systeme)

8.2.6 Schutzbedarfsfeststellung für sonstige Geräte

Um den Schutzbedarf sonstiger Geräte festzustellen, muss zunächst bestimmt werden, für welche Geschäftsprozesse und Anwendungen diese Geräte eingesetzt werden und wie sich deren Schutzbedarf vererbt. Diese Informationen wurden in Kapitel 8.1.7 ermittelt. Dabei muss der Datenfluss über diese Geräte beachtet werden, über den sich der Schutzbedarf auf die dazwischenliegenden Netzkomponenten vererbt.

Um den Schutzbedarf eines Geräts zu ermitteln, müssen nun die möglichen Schäden der relevanten Geschäftsprozesse in ihrer Gesamtheit betrachtet werden. Die Ergebnisse der Schutzbedarfsfeststellung von Geräten sollten wiederum in einer Tabelle festgehalten werden, wenn diese Einfluss auf die Informationssicherheit haben. Um nicht beliebig viele Geräte in einer Institution erfassen zu müssen, sollten nur Geräte betrachtet werden, die die Informationssicherheit nennenswert beeinträchtigen könnten. Diese sollten möglichst zu Gruppen zusammengefasst und als ein Objekt behandelt werden.

Es sollte vermerkt werden, welchen Schutzbedarf jedes Gerät bezüglich Vertraulichkeit, Integrität und Verfügbarkeit hat. Der Gesamt-Schutzbedarf eines Geräts leitet sich wiederum aus dem Maximum des Schutzbedarfs bezüglich der drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit ab.

Die Festlegungen des Schutzbedarfs von Geräten müssen kurz begründet werden, damit die Entscheidungen auch für Außenstehende nachvollziehbar sind. Hier kann auf die Schutzbedarfsfeststellung der Geschäftsprozesse und Anwendungen zurückverwiesen werden.

In Institutionen werden je nach Branche unterschiedlichste Geräte eingesetzt, um die Geschäftsprozesse zu unterstützen. Neben IT-Systemen, die unmittelbar als solche zu identifizieren sind, können auch viele andere Arten von Geräten Einfluss auf die Informationssicherheit haben. Zu solchen Geräten gehören beispielsweise Geräte mit Funktionalitäten aus dem Bereich Internet of Things (IoT).

A.2 Schutzbedarfsfeststellung der RECPLAST GmbH								
Bezeichnung	Beschreibung des Zielobjektes / der Gruppe der Zielobjekte	Plattform / Baustein	Vertraulichkeit	Begründung für die Vertraulichkeit	Integrität	Begründung für die Integrität	Verfügbarkeit	Begründung für die Verfügbarkeit
S200	Alarmanlage BG	Alarmanlage	normal	Es haben keine unbefugten Personen Zugriff auf die Alarmanlage.	sehr hoch	Aufgrund der sofortigen Meldung an die Feuerwehr und den entsprechenden Sensoren ist die Korrektheit der Daten sehr wichtig.	sehr hoch	Die Alarmanlage schützt das Gebäude und muss zu jeder Zeit verfügbar sein.
S201	Alarmanlage Beuel	Alarmanlage	normal	Es haben keine unbefugten Personen Zugriff auf die Alarmanlage.	sehr hoch	Aufgrund der sofortigen Meldung an die Feuerwehr und den entsprechenden Sensoren ist die Korrektheit der Daten sehr wichtig.	sehr hoch	Die Alarmanlage schützt das Gebäude und muss zu jeder Zeit verfügbar sein.
S202	Video-Überwachung	Server unter Unix	normal	Es haben keine unbefugten Personen Zugriff auf die Videodaten.	normal	Durch überlappende Aufnahmebereiche können veränderte Aufnahmen kompensiert werden.	hoch	Ein Ausfall der Videokameras kann durch weitere Maßnahmen kompensiert werden.
S203	Kühlschrank IT-Abteilung	Kühlschrank	normal	Der Kühlschrank erfasst keine vertraulichen Daten.	normal	Die gespeicherten Daten sollten korrekt sein, jedoch wird der Kühlschrank in einem separaten Netz betrieben.	hoch	Der Kühlschrank kann bei einem Ausfall nicht geöffnet werden. Aufgrund der darin enthaltenen Lebensmittel ist ein Ausfall bis 12 Stunden tolerierbar.

Abbildung 23: Auszug aus der Schutzbedarfsfeststellung der RECPLAST GmbH (sonstige und IoT-Geräte)

Aktionspunkte zu 8.2.4, 8.2.5 und 8.2.6 Schutzbedarfsfeststellung für IT-, ICS-Systeme und sonstige Geräte

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

8.2.7 Schutzbedarfsfeststellung für Räume

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

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

Beispiel: RECPLAST GmbH
Die folgende Tabelle zeigt einen Auszug aus den Ergebnissen der Schutzbedarfsfeststellung für die Räume der RECPLAST GmbH:

A.2 Schutzbedarfsfeststellung der RECPLAST GmbH								
Bezeichnung	Beschreibung des Zielobjektes / der Gruppe der Zielobjekte	Plattform / Baustein	Vertraulichkeit	Begründung für die Vertraulichkeit	Integrität	Begründung für die Integrität	Verfügbarkeit	Begründung für die Verfügbarkeit
R001	Büroräume	Büroraum	normal	In den Büroräumen stehen ausreichend abschließbare Schränke zur Verfügung. Die Mitarbeiter sind angewiesen, vertrauliche Informationen nach Arbeitsende zu verschließen.	normal	Die Büroräume können verschlossen werden, Fremde haben keinen Zutritt	normal	Es stehen ausreichend Büroräume zur Verfügung.
R002	Besprechungsräume	Besprechungsraum	normal	In den Besprechungsräumen werden keine Unterlagen aufbewahrt.	normal	In den Besprechungsräumen werden keine Unterlagen aufbewahrt.	normal	Besprechungen können auch in anderen Räumlichkeiten durchgeführt werden.
R003	Häuslicher Arbeitsplatz	Telearbeit	normal	Am häuslichen Arbeitsplatz dürfen keine vertraulichen Dokumente bearbeitet werden.	normal	Es dürfen nur Daten am häuslichen Arbeitsplatz verarbeitet werden, deren Integrität den Schutzbedarf normal entsprechen.	normal	Ein Telearbeitsplatz wird nur sporadisch genutzt, der generelle Arbeitsplatz liegt innerhalb der RECPLAST in Büroräumen.
R004	Mobiler Arbeitsplatz	Mobiler Arbeitsplatz	normal	Mobil dürfen keine vertraulichen Dokumente bearbeitet werden.	normal	Es dürfen nur Daten am mobilen Arbeitsplatz verarbeitet werden, deren Integrität den Schutzbedarf normal entsprechen.	normal	Ein mobiler Arbeitsplatz wird nur sporadisch genutzt, der generelle Arbeitsplatz liegt innerhalb der RECPLAST in Büroräumen.

Abbildung 24: Auszug aus der Schutzbedarfsfeststellung der RECPLAST GmbH (Räume)

Aktionspunkte zu 8.2.7 Schutzbedarfsfeststellung für Räume

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

8.2.8 Schutzbedarfsfeststellung für Kommunikationsverbindungen

Nachdem die Schutzbedarfsfeststellung für die betrachteten Geschäftsprozesse, Anwendungen, IT-Systeme, ICS- und sonstigen Geräte und Räume abgeschlossen wurde, wird nun der Schutzbedarf bezüglich der Vernetzungsstruktur erarbeitet. Grundlage für die weiteren Überlegungen ist der in Kapitel 8.1.4 *Netzplanerhebung* erarbeitete Netzplan des zu untersuchenden Informationsverbunds.

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

- Kommunikationsverbindungen, die Außenverbindungen darstellen, d. h. die in oder über unkontrollierte Bereiche führen (z. B. ins Internet oder über öffentliches Gelände). Dazu können auch drahtlose Kommunikationsverbindungen gehören, da es hierbei schwierig ist, zu verhindern, dass auf diese von öffentlichem Gelände aus zugegriffen wird. Bei Außenverbindungen besteht die Gefahr, dass durch externe Angreifer Penetrationsversuche auf das zu schützende System vorgenommen oder Schadprogramme eingespielt werden können. Darüber hinaus können unter Umständen Innentäter über eine solche Verbindung vertrauliche Informationen nach außen übertragen. Auch in Bezug auf den Grundwert Verfügbarkeit sind Außenverbindungen oft besonders gefährdet. Es darf nicht vergessen werden, Außenverbindungen für die Fernadministration mit zu erfassen.
- Kommunikationsverbindungen, über die hochschutzbedürftige Informationen übertragen werden, wobei dies sowohl Informationen mit einem hohen Anspruch an Vertraulichkeit wie auch Integrität oder Verfügbarkeit sein können. Diese Verbindungen können das Angriffsziel vorsätzlichen Abhörens oder vorsätzlicher Manipulation sein. Darüber hinaus kann der Ausfall einer solchen Verbindung die Funktionsfähigkeit wesentlicher Teile des Informationsverbundes beeinträchtigen.

- Kommunikationsverbindungen, die im produzierenden Bereich eingesetzt werden, müssen im Netzplan ebenfalls mit erfasst werden. Dazu gehören (z. B. bei einer Netztrennung) die Kommunikationsverbindungen zwischen den Netzen.

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 oder einer Gruppe von IT-Systemen mit hohem oder sehr hohem Schutzbedarf ausgehen. Dabei werden diejenigen Verbindungen identifiziert, über die hochschutzbedürftige Informationen übertragen werden. Danach werden die Verbindungen untersucht, über die diese hochschutzbedürftigen Daten weiter übertragen werden. Abschließend sind die Kommunikationsverbindungen zu identifizieren, über die derlei Informationen nicht übertragen werden dürfen. Zu erfassen sind dabei:

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

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

Beispiel: RECPLAST GmbH

Für das Unternehmen RECPLAST GmbH ergeben sich die Kommunikationsverbindungen, die im Netzplan im Kapitel 8.1.4 *Netzplanerhebung* dargestellt wurden. Diese wurden bei der RECPLAST aufgrund von ähnlichen Anforderungen gruppiert und sowohl in der Strukturanalyse als auch in der Schutzbedarfsfeststellung beschrieben und bewertet. Anhand der folgenden Tabelle können die oben dargestellten Kommunikationsverbindungen nachvollzogen werden:

A.1 Strukturanalyse der RECPLAST GmbH									
Bezeichnung	Beschreibung des Zielobjektes / der Gruppe der Zielobjekte	Plattform / Baustein	Ort	Gebäude	Raum	Anzahl	Status	Benutzer	Verantwortlich / Administrator
K001	**Internet – Bonn BG** Internetverbindung für den Anschluss der RECPLAST an das Internet; dieser Anschluss ist gleichwertig mit dem Anschluss der Vertriebsstandorte an die RECPLAST	-	-	-	-	-	in Betrieb	Alle Mitarbeiter	IT-Betrieb
K002	**Standleitung Bonn BG – Bonn Beuel** Standleitung für die Anbindung der beiden Standorte in Bonn	-	-	-	-	-	in Betrieb	Alle Mitarbeiter	IT-Betrieb
K003	**Verbindungen zwischen Netzkomponenten innerhalb der RECPLAST** Verbindungen zwischen Routern, Switchen und Firewall, die in mindestens einem Schutzziel der Datenübertragung einen hohen Schutzbedarf aufweisen.	-	-	-	-	-	in Betrieb	Administratoren	IT-Betrieb
K004	**Verbindungen Netzkomponenten zu Servern innerhalb der RECPLAST** Verbindungen zwischen Netzkomponenten und Servern, die in mindestens einem Schutzziel der Datenübertragung einen hohen Schutzbedarf aufweisen.	-	-	-	-	-	in Betrieb	Administratoren	IT-Betrieb
K005	**Verbindungen Netzkomponenten zu ICS-, IoT- oder sonstigen Geräten** Verbindungen zwischen den Netzkomponenten und ICS-, IoT- oder sonstigen Geräten, die in mindestens einem Schutzziel der Datenübertragung einen hohen Schutzbedarf aufweisen.	-	-	-	-	-	in Betrieb	Administratoren	IT-Betrieb
K006	**Verbindungen Netzkomponenten zu Arbeitsplätzen innerhalb der RECPLAST** Verbindungen zwischen den Netzkomponenten und den Clients oder Laptops, die in mindestens einem Schutzziel der Datenübertragung einen hohen Schutzbedarf aufweisen.	-	-	-	-	-	in Betrieb	Administratoren	IT-Betrieb

Abbildung 25: Auszug aus der Strukturanalyse der RECPLAST GmbH (Kommunikationsverbindungen)

A.2 Schutzbedarfsfeststellung der RECPLAST GmbH								
Bezeichnung	Beschreibung des Zielobjektes / der Gruppe der Zielobjekte	Plattform / Baustein	Vertraulichkeit	Begründung für die Vertraulichkeit	Integrität	Begründung für die Integrität	Verfügbarkeit	Begründung für die Verfügbarkeit
K001	Internet - Bonn BG	-	hoch	Maximumprinzip Abgefangene Informationen können z. B. an den Wettbewerb gelangen.	hoch	Maximumprinzip Ein Großteil der Kommunikation erfolgt über das Internet. Falsche Informationen können z. B. den Ruf schädigen.	hoch	Maximumprinzip Es handelt sich hierbei um die Außenverbindung. Ohne Außenverbindung kann keine Kommunikation mehr stattfinden.
K002	Standleitung Bonn BG - Bonn Beuel	-	hoch	Maximumprinzip Die internen Informationen müssen vertraulich übertragen werden.	normal	Maximumprinzip Da die Standleitung durch die internen Administratoren abgesichert wurde, können Informationen nur mit hohem Aufwand verfälscht werden.	hoch	Maximumprinzip Ohne die Anbindung an den Produktionsstandort können dort keine Produktionsaufträge mehr bearbeitet werden.
K003	Verbindungen zwischen Netzkomponenten innerhalb der RECPLAST	-	normal	Informationen, die innerhalb der internen Netze übertragen werden, können nicht von Dritten eingesehen werden.	normal	Informationen, die innerhalb der internen Netze übertragen werden, können nicht von Dritten verändert werden.	hoch	Maximumprinzip Wenn eine interne Verbindung ausfällt, sind die Netzkomponenten nicht mehr erreichbar und der interne Datenfluss ist nicht mehr möglich.

Abbildung 26: Auszug aus der Schutzbedarfsfeststellung der RECPLAST GmbH (Kommunikationsverbindungen)

Aktionspunkte zu 8.2.8 Schutzbedarfsfeststellung für Kommunikationsverbindungen
• Außenverbindungen erfassen und in tabellarischer oder grafischer Form dokumentieren • Verbindungen, über die kritische Informationen übertragen werden, identifizieren • Alle kritischen Kommunikationsverbindungen in tabellarischer oder grafischer Form dokumentieren

8.2.9 Schlussfolgerungen aus den Ergebnissen der Schutzbedarfsfeststellung

Die bei der Schutzbedarfsfeststellung erzielten Ergebnisse bieten einen Anhaltspunkt für die weitere Vorgehensweise der Sicherheitskonzeption. Für den Schutz, der von den in den IT-Grundschutz-Bausteinen beschriebenen Sicherheitsanforderungen ausgeht, wird bezüglich der Schutzbedarfskategorien Folgendes angenommen:

Schutzwirkung von Sicherheitsanforderungen nach IT-Grundschutz	
Schutzbedarfskategorie "normal"	Sicherheitsanforderungen nach IT-Grundschutz sind im Allgemeinen ausreichend und angemessen.
Schutzbedarfskategorie "hoch"	Sicherheitsanforderungen nach IT-Grundschutz liefern eine Standard-Absicherung, sind aber unter Umständen alleine nicht ausreichend. Weitergehende Maßnahmen sollten auf Basis einer Risikoanalyse ermittelt werden.
Schutzbedarfskategorie "sehr hoch"	Sicherheitsanforderungen nach IT-Grundschutz liefern eine Standard-Absicherung, reichen aber alleine im Allgemeinen nicht aus. Die erforderlichen zusätzlichen Sicherheitsmaßnahmen müssen individuell auf der Grundlage einer Risikoanalyse ermittelt werden.

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

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

Ausführliche Informationen zur Risikoanalyse finden sich in Kapitel 8.5.

Bereiche mit unterschiedlichem Schutzbedarf

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

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

Beispiele:

- Räumliche Sicherheitszonen: Um nicht jeden einzelnen Büroraum permanent abschließen oder überwachen zu müssen, sollten Zonen mit starkem Besucherverkehr von hoch-schutzbedürftigen Bereichen getrennt werden. So sollten sich Besprechungs-, Schulungs- oder Veranstaltungsräume ebenso wie eine Kantine, die externes Publikum anzieht, in der Nähe des Gebäudeeingangs befinden. Der Zugang zu Gebäudeteilen mit Büros kann dann von einem Pförtner einfach überwacht

werden. Besonders sensitive Bereiche wie eine Entwicklungsabteilung sollten mit einer zusätzlichen Zugangskontrolle z. B. über Chipkarten abgesichert werden.

- Technische Sicherheitszonen: Um vertrauliche Daten auf bestimmte Bereiche innerhalb eines LANs zu begrenzen und um zu verhindern, dass Störungen in bestimmten Komponenten oder Angriffe die Funktionsfähigkeit beeinträchtigen, ist es hilfreich, das LAN in mehrere Teilnetze aufzuteilen (siehe auch Baustein NET.1.1 *Netzarchitektur und -design* im IT-Grundschutz-Kompendium).
- 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 nicht gleichzeitig in der Buchhaltung und 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.
- Zonenkonzept bei virtualisierten Infrastrukturen

  Wird Virtualisierung eingesetzt, dann muss dies auch im technischen Zonenkonzept berücksichtigt werden. Virtualisierung bedeutet eine Konsolidierung der Server, d. h. die Möglichkeit mehrere Server virtuell auf einem physischen Host zu betreiben. Hierbei können die eingesetzten Server unterschiedlichem Schutzbedarf unterliegen, aufgrund der verschiedenen Anwendungen und Dienste, die darauf laufen. Daher sollte vor einer Virtualisierung festgelegt werden, welche Dienste oder Anwendungen zusammen in einer virtuellen Umgebung betrieben werden dürfen und welche durch geeignete Maßnahmen separiert werden müssen. Bei der Segmentierung sollte darauf geachtet werden, dass alle Bereiche der IT-Infrastruktur ("Server", "Netze", "Storage" und "Management") erfasst sind.

  Bei der Entscheidung, welche Systeme auf einer gemeinsamen physischen Hardware virtualisiert werden dürfen, ist Folgendes zu beachten:

  - Die Server sollten aus organisatorischer Sicht und aus Sicherheitssicht sinnvoll in Zonen gruppiert werden. Zonen sollten nicht zusammen mit der Sicherheitskomponente, die für die Separierung der Zonen sorgt, virtualisiert werden.
  - Welche Komponenten zusammen auf einer gemeinsamen physischen Hardware virtualisiert werden kann, ist abhängig von Schutzbedarf und Bedarfsträger.

  Bedarfsträger können unterschiedliche Mandanten (Hosting-Szenarien), unterschiedliche Organisationseinheiten innerhalb eines Unternehmens oder einer Behörde oder unterschiedliche Verfahren sein. Im ersten Fall besteht die Herausforderung bei der Planung, ein gleiches Verständnis der Bedarfsträger über die verwendeten Schutzbedarfskategorien zu erreichen.
- Zonenkonzept beim Cloud Computing

Um dem unterschiedlichen Schutzbedarf der Anwender Rechnung zu tragen, müssen Cloud Computing Plattformen mandantenfähig sein und eine verlässliche und durchgängige Trennung der Anwender über den kompletten Cloud Computing Stack (Server, Netze, Storage und Management) gewährleisten. Neben den gängigen Sicherheitsmaßnahmen wie Schadprogramm- und Spam-Schutz, IDS und IPS sollte auf Netzebene auf eine geeignete Segmentierung geachtet werden, indem abhängig vom Schutzbedarf Sicherheitszonen definiert und eingerichtet werden.

Beispiele hierfür sind:

- Sicherheitszone für das Management der Cloud
- Sicherheitszone für die Live Migration
- Sicherheitszone für das Storage-Netz

- Sicherheitszonen für die virtuellen Maschinen

Darüber hinaus wird empfohlen, unterschiedliche Zonen für die Server-Hardware anhand des Schutzbedarfs einzurichten und diese untereinander unter Verwendung von Sicherheitsgateways zu trennen.

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

Aktionspunkte zu 8.2.9 Schlussfolgerungen aus den Ergebnissen der Schutzbedarfsfeststellung
• Prüfen, ob Objekte mit erhöhten Sicherheitsanforderungen in Sicherheitszonen konzentriert werden können • Objekte mit erhöhten Sicherheitsanforderungen für eine Risikoanalyse vormerken

8.3 Modellierung eines Informationsverbunds

Nachdem die notwendigen Informationen aus der Strukturanalyse und der Schutzbedarfsfeststellung vorliegen, besteht der nächste Schritt darin, den betrachteten Informationsverbund mit Hilfe der vorhandenen Bausteine aus dem IT-Grundschutz-Kompendium nachzubilden. Das Ergebnis ist ein IT-Grundschutz-Modell des Informationsverbunds, das aus verschiedenen, gegebenenfalls auch mehrfach verwendeten Bausteinen besteht und durch die Verwendung der Bausteine die sicherheitsrelevanten Aspekten des Informationsverbunds beinhaltet.

8.3.1 Das IT-Grundschutz-Kompendium

Das IT-Grundschutz-Kompendium (siehe [GSK]) kann in der jeweils aktuellen Fassung vom BSI-Webserver heruntergeladen werden.

Die IT-Grundschutz-Bausteine

Das IT-Grundschutz-Kompendium enthält für verschiedene Vorgehensweisen, Komponenten und IT-Systeme die Gefährdungslage, Sicherheitsanforderungen und weiterführende Informationen, die jeweils in einem Baustein zusammengefasst sind.

Um Innovationsschübe und Versionswechsel vor allem im IT-Bereich zu berücksichtigen, ist das IT-Grundschutz-Kompendium mit Hilfe der Baustein-Struktur modular aufgebaut und konzentriert sich auf die Darstellung der wesentlichen Sicherheitsanforderungen für die jeweiligen Bausteine. Damit ist es leicht erweiterbar und aktualisierbar. Übergeordnet sind die Bausteine in prozess- und systemorientierte Bausteine aufgeteilt und nach zusammengehörigen Themen in ein Schichtenmodell einsortiert.

Die prozessorientierten Bausteine sind in die folgenden Schichten gruppiert:

- ISMS *(Managementsysteme für Informationssicherheit)*
- ORP *(Organisation und Personal)*
- CON *(Konzepte und Vorgehensweisen)*
- OPS *(Betrieb)*
- DER *(Detektion und Reaktion)*

Die systemorientierten Bausteine sind in die folgenden Schichten gruppiert:

- INF *(Infrastruktur)*
- NET *(Netze und Kommunikation)*
- SYS *(IT-Systeme)*
- APP *(Anwendungen)*

- IND *(Industrielle IT)*

Gefährdungen

In jedem Baustein wird zunächst die zu erwartende spezifische Gefährdungslage beschrieben. Ergänzend hierzu befindet sich im separaten Anhang der jeweiligen Bausteine eine Auflistung der elementaren Gefährdungen, die bei der Erstellung des Bausteins berücksichtigt wurden. Diese Gefährdungsliste ist Teil einer ersten Stufe der vereinfachten Risikoanalyse für typische Umgebungen der Informationsverarbeitung und bildet die Grundlage, auf der das BSI spezifische Anforderungen zusammengestellt hat, um ein angemessenes Niveau der Informationssicherheit in einer Institution zu gewährleisten. Der Vorteil dabei ist, dass die Anwender bei typischen Anwendungsfällen keine aufwändigen oder weiterführenden Analysen benötigen, um das für einen normalen Schutzbedarf notwendige Sicherheitsniveau zu erreichen. Vielmehr ist es ausreichend, die für die betrachteten Geschäftsprozesse, und ihrer notwendigen Ressourcen relevanten Bausteine zu identifizieren und die darin empfohlenen Anforderungen konsequent und vollständig zu erfüllen.

Auch wenn besondere Komponenten oder Einsatzumgebungen vorliegen, die im IT-Grundschutz nicht hinreichend behandelt werden, bietet das IT-Grundschutz-Kompendium dennoch eine wertvolle Arbeitshilfe. Die dann notwendige Risikoanalyse kann sich auf die elementaren Gefährdungen dieser Komponenten oder Rahmenbedingungen konzentrieren.

Sicherheitsanforderungen

In jedem Baustein werden die Sicherheitsanforderungen, die für den Schutz des betrachteten Gegenstands relevant sind, aufgeführt. Sie beschreiben, *was* zu dessen Schutz zu tun ist. Die Anforderungen sind in drei Kategorien eingruppiert:

- **Basis-Anforderungen** müssen vorrangig erfüllt werden, da bei diesen Empfehlungen mit (relativ) geringem Aufwand der größtmögliche Nutzen erzielt werden kann. Es handelt sich um uneingeschränkte Anforderungen. Die Basis-Anforderungen sind ebenfalls die Grundlage für die Vorgehensweise „Basis-Absicherung".
- **Standard-Anforderungen** bauen auf den Basis-Anforderungen auf und adressieren den normalen Schutzbedarf. Sie sollten grundsätzlich erfüllt werden, aber nicht vorrangig. Die Ziele der Standard-Anforderungen müssen erreicht werden, um eine Standard-Absicherung zu erzielen. Es können sich aber durch die jeweiligen Rahmenbedingungen der Institution auch Gründe ergeben, warum eine Standard-Anforderung nicht wie beschrieben umgesetzt wird, sondern die Sicherheitsziele auf andere Weise erreicht werden. Wenn eine Standard-Anforderung durch andere Sicherheitsmaßnahmen erfüllt wird, müssen die dadurch entstehenden Auswirkungen sorgfältig abgewogen und geeignet dokumentiert werden.
- **Anforderungen bei erhöhtem Schutzbedarf** sind eine Auswahl von Vorschlägen für eine weitergehende Absicherung, die bei erhöhten Sicherheitsanforderungen oder unter bestimmten Rahmenbedingungen als Grundlage für die Erarbeitung geeigneter Anforderungen und Maßnahmen berücksichtigt werden können.

Die Bausteine wenden sich an Sicherheitsbeauftragte und Sicherheitsverantwortliche in Institutionen.

Umsetzungshinweise

Zusätzlich zu den Bausteinen des IT-Grundschutz-Kompendiums kann es Umsetzungshinweise geben. Diese beschreiben, wie die Anforderungen der Bausteine umgesetzt werden können, und enthalten dafür passende Sicherheitsmaßnahmen mit einer detaillierten Beschreibung. Die Sicherheitsmaßnahmen können als Grundlage für Sicherheitskonzeptionen verwendet werden, sollten aber unter Umständen noch an die Rahmenbedingungen der jeweiligen Institution angepasst werden.

Die Umsetzungshinweise adressieren jeweils die Personengruppen, die für die Umsetzung der Anforderungen aus den Baustein zuständig sind, beispielsweise den IT-Betrieb oder die Haustechnik. Diese Umsetzungshinweise werden für ausgewählte, vor allem für stark nachgefragte Themen bereitgestellt.

8.3.2 Modellierung eines Informationsverbunds: Auswahl von Bausteinen

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

- Das IT-Grundschutz-Modell eines bereits realisierten Informationsverbundes identifiziert über die verwendeten Bausteine die relevanten Sicherheitsanforderungen. Es kann in Form eines **Prüfplans** benutzt werden, um einen Soll-Ist-Vergleich durchzuführen.
- Das IT-Grundschutz-Modell eines geplanten Informationsverbundes stellt hingegen ein **Entwicklungskonzept** dar. Es beschreibt über die ausgewählten Bausteine, welche Sicherheitsanforderungen bei der Realisierung des Informationsverbunds erfüllt werden müssen.

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

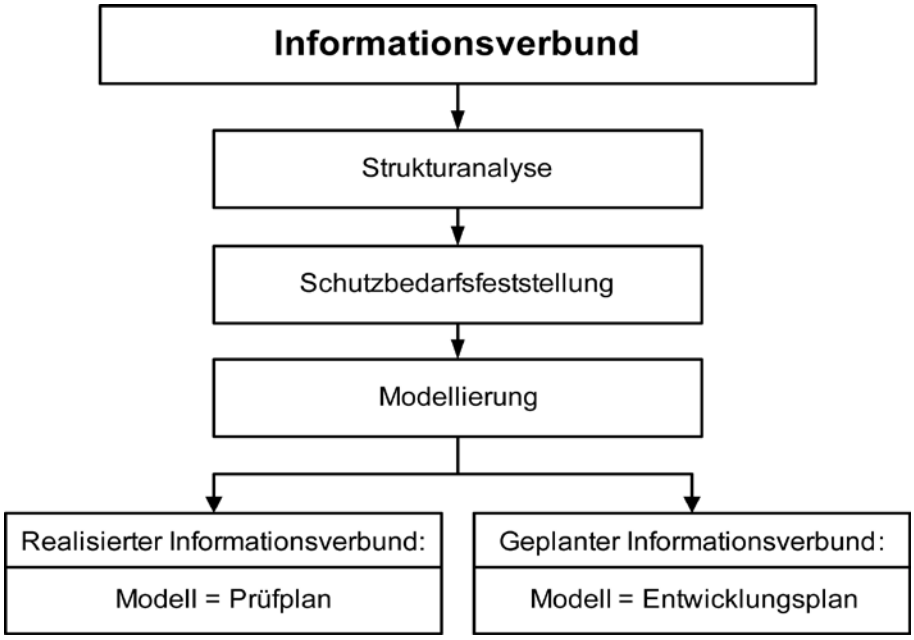


Abbildung 27: Ergebnis der Modellierung nach IT-Grundschutz

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

Um einen im Allgemeinen komplexen Informationsverbund nach IT-Grundschutz zu modellieren, müssen die passenden Bausteine des IT-Grundschutz-Kompendiums ausgewählt und umgesetzt werden. Um die Auswahl zu erleichtern, sind die Bausteine im IT-Grundschutz-Kompendium zunächst in prozess- und systemorientierte Bausteine aufgeteilt und diese jeweils in einzelne Schichten untergliedert.

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

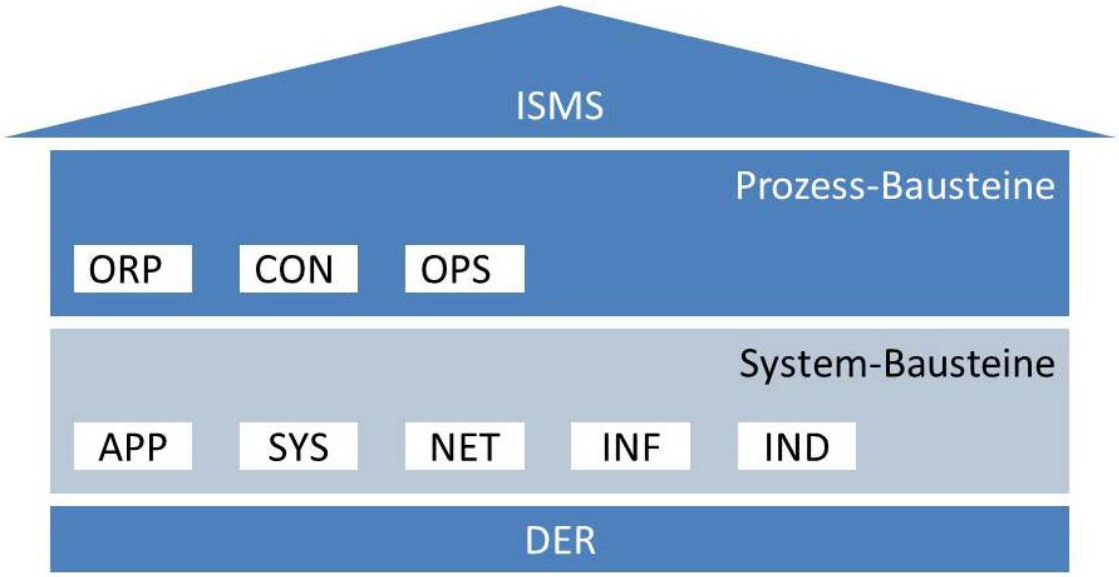


Abbildung 28: Das Schichtenmodell des IT-Grundschutzes

Prozessorientierte Bausteine:

- Die Schicht ISMS enthält als Grundlage für alle weiteren Aktivitäten im Sicherheitsprozess den Baustein *Sicherheitsmanagement.*
- In der Schicht ORP finden sich Bausteine, die organisatorische und personelle Sicherheitsaspekte abdecken, wie die Bausteine *Organisation* und *Personal*.
- Die Schicht CON enthält Bausteine, die sich mit Konzepten und Vorgehensweisen befassen. Typische Bausteine der Schicht CON sind unter anderem *Kryptokonzept* und *Datenschutz*.
- Die Schicht OPS umfasst alle Sicherheitsaspekte betrieblicher Art. Insbesondere sind dies die Sicherheitsaspekte des operativen IT-Betriebs, sowohl bei einem Betrieb im Haus, als auch bei einem IT-Betrieb, der in Teilen oder komplett durch Dritte betrieben wird. Ebenso enthält er die Sicherheitsaspekte, die bei einem IT-Betrieb für Dritte zu beachten sind. Beispiele für die Schicht OPS sind die Bausteine *Schutz vor Schadprogrammen* und *Outsourcing für Kunden.*
- In der Schicht DER finden sich alle Bausteine, die für die Überprüfung der umgesetzten Sicherheitsmaßnahmen und insbesondere für die Detektion von Sicherheitsvorfällen sowie die geeigneten Reaktionen darauf relevant sind. Typische Bausteine der Schicht DER sind *Behandlung von t Sicherheitsvorfällen* und *Forensik*.

System-Bausteine:

- Die Schicht APP beschäftigt sich mit der Absicherung von Anwendungen und Diensten, unter anderem in den Bereich Kommunikation, Verzeichnisdienste, Netzbasierte Dienste sowie Business- und Client-Anwendungen. Typische Bausteine der Schicht APP sind */ Groupware*, Office-Produkte, *Webserver* und *Browser*.
- Die Schicht SYS betrifft die einzelnen IT-Systeme des Informationsverbunds, die ggf. in Gruppen zusammengefasst wurden. Hier werden die Sicherheitsaspekte von Servern, Desktop-Systemen, Mobile Devices und sonstigen IT-Systemen wie Druckern und TK-Anlagen behandelt. Zur Schicht SYS gehören beispielsweise Bausteine zu konkreten Betriebssystemen, *Smartphones und Tablets* und *Drucker, Kopierer und Multifunktionsgeräte*.
- Die Schicht NET betrachtet die Vernetzungsaspekte, die sich nicht auf bestimmte IT-Systeme, sondern auf die Netzverbindungen und die Kommunikation beziehen. Dazu gehören zum Beispiel die Bausteine *Netzmanagement*, *Firewall* und *WLAN-Betrieb*.

- Die Schicht INF befasst sich mit den baulich-technischen Gegebenheiten, hier werden Aspekte der infrastrukturellen Sicherheit zusammengeführt. Dies betrifft unter anderem die Bausteine *Gebäude und Rechenzentrum*.
- Die Schicht IND befasst sich mit Sicherheitsaspekten industrieller IT. In diese Schicht fallen beispielsweise die Bausteine *Maschine, Sensoren und Speicherprogrammierbare Steuerung (SPS)*.

Die Einteilung in diese Schichten hat folgende Vorteile:

- Die Komplexität der Informationssicherheit wird reduziert, indem eine sinnvolle Aufteilung der Einzelaspekte vorgenommen wird.
- Da übergeordnete Aspekte und gemeinsame infrastrukturelle Fragestellungen getrennt von den IT-Systemen betrachtet werden, werden Redundanzen vermieden, weil diese Aspekte nur einmal bearbeitet werden müssen und nicht wiederholt für jedes IT-System.
- Die einzelnen Schichten sind so gewählt, dass auch die Zuständigkeiten für die betrachteten Aspekte gebündelt sind. So betreffen beispielsweise die Schichten ISMS und ORP Grundsatzfragen des sicheren Umgangs mit Informationen, Schicht INF den Bereich Haustechnik, Schicht SYS die Zuständigen für die IT-Systeme, Schicht NET die Ebene der Netzadministratoren und Schicht APP schließlich die Anwendungsverantwortlichen und -betreiber.
- Aufgrund der Aufteilung der Sicherheitsaspekte in Schichten können Einzelaspekte in resultierenden Sicherheitskonzepten leichter aktualisiert und erweitert werden, ohne dass andere Schichten umfangreich tangiert werden.

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

8.3.3 Reihenfolge der Baustein-Umsetzung

Um grundlegende Risiken abzudecken und eine ganzheitliche Informationssicherheit aufzubauen, müssen die essentiellen Sicherheitsanforderungen frühzeitig erfüllt und entsprechende Sicherheitsmaßnahmen umgesetzt werden. Daher wird im IT-Grundschutz eine Reihenfolge für die umzusetzenden Bausteine vorgeschlagen.

Im IT-Grundschutz-Kompendium ist im Kapitel *Schichtenmodell und Modellierung* beschrieben, wann ein einzelner Baustein sinnvollerweise eingesetzt werden soll und auf welche Zielobjekte er anzuwenden ist. Außerdem sind die Bausteine danach gekennzeichnet, ob sie vor- oder nachrangig umgesetzt werden sollten.

- R1: Diese Bausteine sollten vorrangig umgesetzt werden, da sie die Grundlage für einen effektiven Sicherheitsprozess bilden.
- R2: Diese Bausteine sollten als nächstes umgesetzt werden, da sie in wesentlichen Teilen des Informationsverbundes für nachhaltige Sicherheit erforderlich sind.
- R3: Diese Bausteine werden zur Erreichung des angestrebten Sicherheitsniveaus ebenfalls benötigt und müssen umgesetzt werden, es wird aber empfohlen, diese erst nach den anderen Bausteinen zu betrachten

Mit R1 sind die Bausteine gekennzeichnet, die notwendig sind, um ein grundlegendes Sicherheitsgerüst zu erreichen. Es handelt sich um die Bausteine der Bereiche

- ISMS *Managementsysteme und Informationsicherheit*
- ORP *Organisation und Persona*l

- OPS.1.1 *Kern IT-Betrieb*

Die im zweiten und dritten Schritt umzusetzenden Bausteine (R2 und R3) finden sich in allen anderen Schichten des IT-Grundschutz-Kompendiums.

Diese Kennzeichnung zeigt nur die sinnvolle zeitliche Reihenfolge für die Umsetzung der Anforderungen des jeweiligen Bausteins auf und stellt keine Gewichtung der Bausteine untereinander dar. Grundsätzlich müssen alle für den jeweiligen Informationsverbund relevanten Bausteine des IT-Grundschutz-Kompendiums umgesetzt werden.

Die Kennzeichnung der Bausteine stellt außerdem nur eine Empfehlung dar, in welcher Reihenfolge die verschiedenen Bausteine sinnvoll umgesetzt werden könnten. Jede Institution kann hier eine abweichende, für sich sinnvolle Reihenfolge festlegen.

8.3.4 Zuordnung von Bausteinen

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

- Nummer und Titel des Bausteins
- Relevanz: Diese Spalte dient der Entscheidung, ob ein Baustein für den zu modellierenden Informationsverbund relevant ist oder nicht. Sie liefert einen schnellen Überblick, ob kein Baustein vergessen wurde.
- Zielobjekt: Wenn ein Baustein für den Informationsverbund relevant ist, erfolgt über diese Spalte die Zuordnung zum Zielobjekt bzw. einer Zielobjektgruppe.
- Begründung: In dieser Spalte können Randinformationen und Begründungen für die Modellierung dokumentiert werden. Sind Bausteine für den betrachteten Informationsverbund nicht relevant, sollte dies hier explizit begründet werden.
- Ansprechpartner: Der konkrete Ansprechpartner wird nicht im Rahmen der Modellierung, sondern erst bei der Planung des eigentlichen Soll-Ist-Vergleichs im IT-Grundschutz-Check ermittelt. Basierend auf den Rollen und Verantwortlichen, die in den Bausteinen genannten werden, kann hier jedoch schon Vorarbeit geleistet werden.

Beispiel: RECPLAST GmbH

Die folgende Tabelle ist ein Auszug aus der Modellierung für das Unternehmen RECPLAST GmbH:

A.3 Modellierung der RECPLAST GmbH				
Nummer und Titel des Bausteins	**Relevanz**	**Zielobjekt**	**Begründung**	**Ansprechpartner**
APP.5.2 Microsoft Exchange / Outlook	nein		Wird nicht eingesetzt.	
APP 3.6 DNS-Server	ja	S019		
Benutzerdef.BS.1 PC für die Industriesteuerung	ja	C005		
CON.7: Informationssicherheit auf Auslandsreisen	nein		Auslandsreisen sind für Informationsverbund nicht relevant.	
INF.1 Allgemeines Gebäude	ja	G001		
INF.2 Rechenzentrum	nein		Es gibt kein Rechenzentrum.	
INF.4 IT-Verkabelung	ja	Informationsverbund		
ISMS.1 (Sicherheitsmanagement)	ja	Informationsverbund		
NET.1.1 Netz-Architektur und -design	ja	Informationsverbund		
NET.3.1 Router und Switches	ja	S033		
OPS.1.1.2 Ordnungsgemäße IT-Administration	nein		Die IT-Administration findet außerhalb des Informationsverbundes statt.	
OPS.2.4 Fernwartung	ja	Informationsverbund		
SYS.1.3 Server unter Unix	ja	S020		
SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte	ja	S048		

Abbildung 29: Auszug aus der Modellierung der RECPLAST GmbH

Eine detaillierte Beschreibung der Vorgehensweise zur Modellierung eines Informationsverbunds findet sich im IT-Grundschutz-Kompendium im Kapitel *Schichtenmodell und Modellierung*.

8.3.5 Modellierung bei Virtualisierung und Cloud-Systemen

Grundsätzlich erfolgt die Modellierung virtueller IT-Systeme nach den gleichen Regeln wie bei eigenständigen physischen IT-Systemen, d. h. es sind die Hinweise in Kapitel 2 des IT-Grundschutz-Kompendiums zu beachten. Die Zuordnung der IT-Grundschutz-Bausteine richtet sich bei IT-Komponenten in erster Linie nach der Funktion des IT-Systems (Server, Client, etc.), nach dem verwendeten Betriebssystem (Linux, Windows, etc.) und nach den darauf betriebenen Applikationen (Datenbank, Webserver, etc.).

Bei Virtualisierungssoftware gibt es Produkte, die ein unterliegendes Betriebssystem benötigen (hostbasierte Virtualisierungslösungen), und andere, die direkt auf der physischen Hardware laufen (Bare Metal Virtualisation), ohne unterliegendes Betriebssystem. Falls unterhalb der Virtualisierungsschicht ein vollwertiges und eigenständiges Betriebssystem eingesetzt wird, muss der dazu passende Baustein ebenfalls zugeordnet werden (z. B. aus SYS.1.2 *Windows-Server*), unabhängig von den virtuellen IT-Systemen.

Wurde der Hypervisor direkt auf der physischen Hardware installiert (Bare Metal Virtualization), handelt es sich hierbei um ein Zielobjekt, das im IT-Grundschutz-Kompendium nicht enthalten ist, da es sich hierbei um ein sehr spezielles Zielobjekt handelt. Daher muss eine Risikoanalyse für das entsprechende Zielobjekt durchgeführt und die Ergebnisse mit den Anforderungen des Bausteins SYS.1.5 *Virtualisierung* konsolidiert werden.

Beispiel-Szenario

Als Beispiel wird ein physischer Server S1 betrachtet, auf dem mit Hilfe einer Virtualisierungssoftware die drei virtuellen Server VM1, VM2 und VM3 betrieben werden. Als Basis-Betriebssystem kommt auf dem physischen Server S1 eine Linux-Version zum Einsatz. Die Virtualisierungsschicht ist in diesem Beispiel eine Software-Komponente, die unter Linux läuft, also eine hostbasierte Servervirtualisierung (Typ 2). Die beiden virtuellen Server VM1 und VM2 werden mit Windows 2012 betrieben, auf VM3 ist hingegen Linux installiert. Applikationen können sowohl auf den drei virtuellen Servern als auch (unter Umgehung der Virtualisierungsschicht) direkt auf dem Basis-Betriebssystem des physischen Servers S1 ablaufen. Die folgende Abbildung zeigt ein Schema dieser Beispiel-Konfiguration:

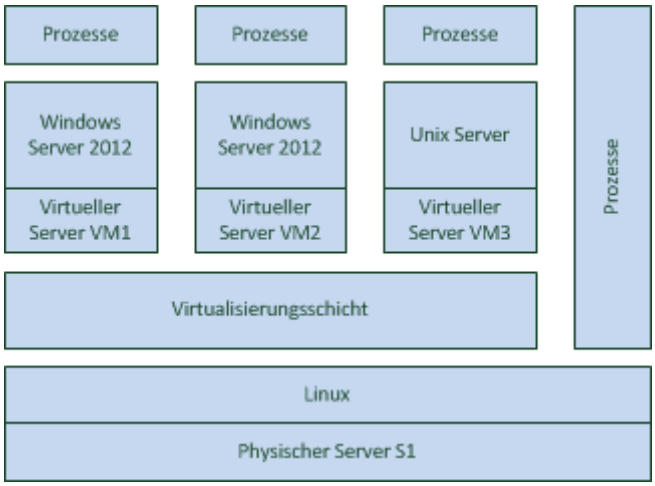


Abbildung 30: Schema einer Beispiel-Konfiguration

Baustein	Zielobjekt
SYS.1.1 *Allgemeiner Server*	S1
SYS.1.1 *Allgemeiner Server*	VM3

Baustein	Zielobjekt
SYS.1.1 *Allgemeiner Server*	Gruppe aus VM1 und VM2
SYS.1.3 *Server unter Unix*	S1
SYS.1.3 *Server unter Unix*	VM3
SYS.1.2.2 *Windows Server 2012*	Gruppe aus VM1 und VM2

Tabelle: Zuordnung Bausteine aus Virtualisierungsschicht zu Zielobjekten

Modellierung beim Cloud Computing

Um eine angemessene Gesamtsicherheit für den IT-Betrieb von Cloud-Diensten zu erreichen, müssen alle Cloud-Dienste (mit ihren zugeordneten virtuellen IT-Systemen, Netzen und weiteren Cloud-Komponenten) systematisch in der Sicherheitskonzeption berücksichtigt werden. Alle über Cloud-Dienste bereitgestellten IT-Systeme, Netze und Anwendungen, die sich einerseits in der Betriebsverantwortung und andererseits im Geltungsbereich des ISMS des Cloud-Diensteanbieters befinden, müssen in der Modellierung gemäß der IT-Grundschutz-Vorgehensweise berücksichtigt werden. Hierbei kann der Geltungsbereich des Informationsverbundes gleichzeitig als Grenze der Verantwortlichkeit verstanden werden: An der Grenze des Informationsverbundes endet die Verantwortung des Cloud-Diensteanbieters und beginnt die Verantwortung des Cloud-Anwenders. Der Umfang des Informationsverbundes unterscheidet sich dabei je nach dem Servicemodell.

Modellierung von IaaS-Angeboten

Bei IaaS (Infrastructure as a Service) ist der Cloud-Diensteanbieter für den Verwaltungsserver für die Cloud und den Virtualisierungsserver verantwortlich. Deshalb kommen bei IaaS aus den Schichten APP *(Anwendungen)* und SYS *(IT-Systeme)* nur die Verwaltungs- und die Virtualisierungssoftware als Zielobjekte vor. Für diese müssen somit die zugehörigen Bausteine ausgewählt werden. Nach der IT-Grundschutz-Vorgehensweise sind dies die Bausteine für IT-Systeme als Server (Schicht SYS.1). Für den Cloud-Verwaltungsserver müssen die Bausteine SYS 1.5 *Virtualisierung* und OPS.3.2 *Cloud-Anbieter* umgesetzt werden.

Für IaaS stellt der Cloud-Diensteanbieter nicht mehr als eine virtuelle "Hülle" über ein virtuelles Netz bereit. Die Absicherung des Netzes nach IT-Grundschutz verantwortet bei IaaS der Cloud-Diensteanbieter, wohingegen die Cloud-Anwender die IT-Systeme des Cloud-Angebotes verantworten. Für das Netz sind die passenden Bausteine aus der Schicht *Netze und Kommunikation* zu modellieren (z. B. NET.1.1 *Netzarchitektur und -design*). In der Regel wird dem virtuellen Server ein Speicherkontingent aus einem Speichernetz zugeordnet, hierfür ist der Baustein SYS.1.8 *Speicherlösungen / Cloud Storage* ebenfalls vom Cloud-Diensteanbieter umzusetzen.

Ein virtueller Server aus der Cloud, der per IaaS angeboten wird, wird durch den Cloud-Anwender konfiguriert. Die Umsetzungsverantwortung für seine Sicherheitsmaßnahmen liegt somit ebenfalls beim Cloud-Anwender. Im Hinblick auf die Abgrenzung des Informationsverbundes des Cloud-Diensteanbieters befindet sich also dieser virtuelle Server außerhalb des Informationsverbundes des Cloud-Diensteanbieters.

Die Schnittstelle zur Bereitstellung von IaaS-Cloud-Diensten (Self-Service-Portal) ist durch geeignete Mechanismen zur Netztrennung (z. B. über Netze, virtuelle Firewalls, Routing) vom Cloud-Diensteanbieter abzusichern und gegebenenfalls der Baustein APP.3.1 *Webanwendungen* umzusetzen.

Eine Modellierung der IaaS-Server als IT-Systeme im Sicherheitskonzept des Cloud-Diensteanbieters ist möglich, allerdings nicht notwendig, da die Cloud-Anwender diese IT-Systeme verwalten.

Modellierung von PaaS-Angeboten

Bei PaaS (Platform as a Service) ist der Cloud-Diensteanbieter zusätzlich zu IaaS für die sichere Bereitstellung eines virtuellen Servers und einer angebotenen Plattform verantwortlich (z. B. einer Datenbank oder eines Webservers. Dementsprechend muss der Cloud-Diensteanbieter im

Servicemodell PaaS zunächst, wie bei IaaS, den Cloud-Verwaltungsserver und dessen Verwaltungssoftware modellieren. Dort erfolgt zentral die Zuordnung des Bausteins OPS.3.2 *Cloud-Anbieter*.

Darüber hinaus muss der Cloud-Diensteanbieter ein IT-System mit dem entsprechenden Betriebssystem modellieren. Zu diesem IT-System ist je nach Cloud-Dienst auf Anwendungsschicht eine Datenbank oder ein Webserver zu modellieren.

Das PaaS-IT-System mit den verbundenen Cloud-Anwendungen muss für jeden Cloud-Mandanten modelliert werden, wobei Mandanten mit gleichen Plattformen, gleichen Anwendungen und gleichem Schutzbedarf gemäß den Vorgaben in Kapitel 8.1.1 *Komplexitätsreduktion durch Gruppenbildung* in einer Gruppe zusammengefasst werden können.

In der Praxis werden Cloud-Dienste des Servicemodells PaaS über virtuelle Profile bereitgestellt, die für mehrere Cloud-Anwender bzw. Mandanten eingesetzt werden können. Es bietet sich daher in der IT-Grundschutz-Modellierung an, diese Kombinationen in Form von Musterservern zu modellieren und pro Mandant zu verknüpfen bzw. zu vervielfachen.

Modellierung von SaaS-Angeboten

Bei SaaS (Software as a Service) müssen zunächst die für die unterliegende Cloud-Infrastruktur relevanten Zielobjekte wie bei IaaS und PaaS identifiziert und entsprechenden Bausteinen zugeordnet werden.

Im Vergleich zu PaaS werden bei SaaS weitere Anwendungen auf den Cloud-IT-Systemen modelliert (z. B. ein Webservice, eine Webanwendung oder ein SAP-System). Bei SaaS ist der Cloud-Diensteanbieter praktisch für den gesamten Cloud Computing Stack (Server, Netze, Storage, Management und Anwendungen) verantwortlich. Die SaaS-Anwendungen liegen auch in seinem Verantwortungsbereich und müssen somit in seinem Informationsverbund modelliert werden. Dabei können sowohl mehrfache Ausprägungen der selben SaaS-Anwendung als auch Gruppen von SaaS-Anwendungen gemäß den Vorgaben in Kapitel 8.1.1 zusammengefasst werden, wenn die dort angegebenen Voraussetzungen erfüllt sind.

8.3.6 Anpassung der Baustein-Anforderungen

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

Für die Erstellung eines Sicherheitskonzeptes oder für ein Audit müssen jetzt die einzelnen Anforderungen bearbeitet und darauf aufbauend geeignete Sicherheitsmaßnahmen formuliert werden.

Die Anforderungen sind knapp und präzise. Sie geben die Teilziele vor, die zusammen zur Umsetzung der Ziele eines Bausteins beitragen. Die Sicherheitsanforderungen müssen daher noch in Handlungsvorgaben für die verschiedenen Akteure im Sicherheitsprozess umgewandelt werden. Dafür müssen auf Basis der Anforderungen Sicherheitsmaßnahmen ausgearbeitet werden, die

- an die jeweiligen Rahmenbedingungen und dem Sprachgebrauch einer Institution angepasst sein müssen,
- ausreichend konkret sind, um im vorliegenden Informationsverbund angewendet zu werden, also z. B. ausreichend technische Details enthalten.

Generell sollten die Anforderungen der IT-Grundschutz-Bausteine immer sinngemäß umgesetzt werden. Alle Änderungen gegenüber dem IT-Grundschutz-Kompendium sollten dokumentiert werden, damit die Gründe auch später noch nachvollziehbar sind.

Zu vielen Bausteinen des IT-Grundschutz-Kompendiums gibt es Umsetzungshinweise, in denen zu den Sicherheitsanforderungen detailliertere Maßnahmen beschrieben sind. Diese Maßnahmen sind einerseits so allgemein formuliert, dass sie in möglichst vielen Umgebungen anwendbar sind, und

andererseits so ausführlich, dass die Maßnahmenbeschreibungen als Umsetzungshilfe dienen zu können.

Auch die in den Umsetzungshinweisen vorgeschlagenen Maßnahmen sollten noch an die jeweiligen Rahmenbedingungen einer Institution angepasst werden. Es kann beispielsweise sinnvoll sein,

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

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

Bei der Sichtung der Sicherheitsanforderungen kann sich ergeben, dass einzelne Anforderungen unter den konkreten Rahmenbedingungen nicht umgesetzt werden können. Dies kann beispielsweise der Fall sein, wenn die Anforderungen in der betrachteten Umgebung nicht relevant sind (z. B. weil Dienste nicht aktiviert wurden). In seltenen Fällen kann dies auch im Bereich der uneingeschränkt notwendigen Basis-Anforderungen vorkommen, wenn deren Umsetzung essentielle Schwierigkeiten in anderen Bereichen mit sich bringen würde. Dies könnte beispielsweise der Fall sein, wenn sich Anforderungen des Brand- und des Einbruchschutzes nicht miteinander vereinbaren lassen. Dann müssen andere Lösungen gefunden und dies nachvollziehbar dokumentiert werden.

Werden Sicherheitsanforderungen zusätzlich aufgenommen oder geändert, muss dies im Sicherheitskonzept dokumentiert werden. Dies erleichtert auch die Durchführung des IT-Grundschutz-Checks.

Bei der Auswahl und Anpassung der Sicherheitsmaßnahmen auf Basis der Anforderungen ist zu beachten, dass diese immer angemessen sein müssen. Angemessen bedeutet:

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

Aktionspunkte zu 8.3 Modellierung eines Informationsverbunds

- Kapitel *Schichtenmodell und Modellierung* aus dem IT-Grundschutz-Kompendium systematisch durcharbeiten
- Für jeden Baustein des IT-Grundschutz-Kompendiums ermitteln, auf welche Zielobjekte er im betrachteten Informationsverbund anzuwenden ist
- Zuordnung von Bausteinen zu Zielobjekten ("IT-Grundschutz-Modell") sowie die entsprechenden Ansprechpartner dokumentieren
- Zielobjekte, die nicht geeignet modelliert werden können, für eine Risikoanalyse vormerken
- Festlegung einer Reihenfolge für die Umsetzung der Bausteine

- Sicherheitsanforderungen aus den identifizierten Bausteinen sorgfältig lesen und darauf aufbauend passende Sicherheitsmaßnahmen festlegen

8.3.7 Einbindung externer Dienstleister

Viele Institutionen setzen externe oder interne Dienstleister ein, um Geschäftsprozesse ganz oder teilweise durch diese durchführen zu lassen. Grundsätzlich kann die Einbindung externer Dienstleiter auf viele Arten erfolgen, z. B. in Form von Personal, welches temporär eingesetzt wird, oder in Form von Auslagerung von IT-Systemen.

Bereits im Vorfeld der Einbindung externer Dienstleister müssen die Aufgaben im Bereich Informationssicherheit abgegrenzt und die Schnittstellen genau festgelegt werden. Aufgaben können an externe Dienstleister ausgelagert werden, die Verantwortung für die Informationssicherheit bleibt immer bei der auslagernden Institution.

Es muss geklärt sein, welche sicherheitsrelevanten Aufgaben durch den externen Dienstleister und welche durch das eigene Sicherheitsmanagement abgedeckt werden. Folgende Fragen sollten vor der Einbindung externer Dienstleister grundlegend geklärt sein:

- Welche Geschäftsprozesse, welche IT-Systeme oder welche Dienstleistungen sollen an einen externen Dienstleister ausgelagert werden?
- Welchen Schutzbedarf haben die Zielobjekte, die durch einen externen Dienstleister oder im Outsourcing verarbeitet werden?
- Auf welche Zielobjekte und welche Informationen hat der externe Dienstleister Zugriff? Hier muss einerseits berücksichtigt werden, welche Zielobjekte und Informationen im Fokus der Dienstleistungserbringung stehen, aber andererseits auch, auf welche Zielobjekte und Informationen die Dienstleister zugreifen könnten, wie z. B. Reinigungskräfte auf Informationen in Büroräumen.

Sofern sich eine Institution für die Einbindung externer Dienstleister entscheidet, müssen neben vertraglichen Rahmenbedingungen ebenfalls die Voraussetzungen für die Umsetzung der Anforderungen des IT-Grundschutzes erfüllt werden. Generell muss die Modellierung der Bausteine getrennt auf die eigene Institution und auf jeden externen Dienstleister durchgeführt werden. Die Vorgehensweise der Modellierung erfolgt wie in Kapitel 8.3.4 *Zuordnung von Bausteinen* beschrieben.

Auch bei der Einbindung externer Dienstleister muss es zu jedem Zeitpunkt für die auslagernde Institution möglich sein, die Risiken im Bereich Informationssicherheit zu identifizieren und zu kontrollieren. Informationen und Geschäftsprozesse müssen immer auf einem vergleichbaren Niveau gemäß den Sicherheitszielen der Institution geschützt werden, auch wenn externe Dienstleister (oder deren Dienstleister) diese ganz oder in Teilen verarbeiten. Außerdem ist eine hohe Ereignistransparenz erforderlich, d. h. es muss Mechanismen geben, die gewährleisten, dass Gefährdungen und Risiken, die Auswirkungen auf die Dienstleistungen haben können, erkannt und kommuniziert werden.

Hierfür ist es erforderlich, Sicherheitsanforderungen sowie die regelmäßige Überwachung von deren Einhaltung in den Verträgen aufzunehmen.

Bei der Einbindung externer Dienstleister ist es möglich, dass der Dienstleister bereits für die eingebundene Dienstleistung ein Zertifikat vorweisen kann. Hierbei muss immer berücksichtigt werden, ob der Geltungsbereich des ausgestellten Zertifikates die Dienstleistung auch tatsächlich umfasst.

8.4 IT-Grundschutz-Check

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

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

Die Modellierung nach IT-Grundschutz wird nun als Prüfplan benutzt, um anhand eines Soll-Ist-Vergleichs herauszufinden, welche Anforderungen ausreichend oder nur unzureichend erfüllt wurden.

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

Nachfolgend werden die Schritte des IT-Grundschutz-Checks detailliert beschrieben.

8.4.1 Organisatorische Vorarbeiten für den IT-Grundschutz-Check

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

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

Ein wichtiger Schritt vor der Durchführung des eigentlichen Soll-Ist-Vergleichs ist die Ermittlung geeigneter Interviewpartner. Hierzu sollte zunächst für jeden einzelnen Baustein, der für die Modellierung des vorliegenden Informationsverbunds herangezogen wurde, ein Hauptansprechpartner festgelegt werden. Bei den Anforderungen in den Bausteinen werden die Rollen genannt, die für die Umsetzung der Anforderungen zuständig sind. Hieraus können die geeigneten Ansprechpartner für die jeweilige Thematik in der Institution identifiziert werden. Im Folgenden finden sich einige Beispiele für Ansprechpartner der verschiedenen Bereiche.

- Bei den Bausteinen der Schicht ORP, CON und OPS ergibt sich ein geeigneter Ansprechpartner in der Regel direkt aus der im Baustein behandelten Thematik. Beispielsweise sollte für den Baustein ORP.2 *Personal* ein Mitarbeiter der zuständigen Personalabteilung als Ansprechpartner ausgewählt werden. Bei den konzeptionellen Bausteinen, z. B. Baustein CON.1 *Kryptokonzept*, 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 INF *(Infrastruktur)* sollte die Auswahl geeigneter Ansprechpartner in Abstimmung mit der Abteilung Innerer Dienst/Haustechnik vorgenommen werden. Je nach Größe der betrachteten Institution können beispielsweise unterschiedliche Ansprechpartner für die Infrastrukturbereiche Gebäude und Technikräume zuständig sein. In kleinen Institutionen kann in

vielen Fällen der Hausmeister Auskunft geben. Zu beachten ist im Bereich Infrastruktur, dass hier unter Umständen externe Stellen zu beteiligen sind. Dies betrifft insbesondere größere Institutionen.

- In den systemorientierten Bausteinen der Schichten SYS, NET und IND 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 APP *(Anwendungen)* sollten die Betreuer bzw. die Verantwortlichen der einzelnen Anwendungen als Hauptansprechpartner ausgewählt werden.

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 jeder Gruppe zwei Personen für die Durchführung des Interviews einzuplanen. Dabei stellt eine Person die notwendigen Fragen und die andere Person notiert die Ergebnisse und Anmerkungen, die durch den Interview-Partner gegeben werden.

Beispiel: RECPLAST GmbH

A.4 IT-Grundschutz-Check der RECPLAST GmbH				
Baustein:	**Sicherheitsmanagement**			
Anforderung	**Anforderungstitel**	**Verantwortung**	**Status**	**Umsetzung**
ISMS.1.A1	Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene	Institutionsleitung	umgesetzt	Die Geschäftsführung hat die Erstellung der Leitlinie initiiert. Die Leitlinie wurde von der Geschäftsführung unterzeichnet. Die Geschäftsführung hat die gesamte Verantwortung für das Thema Informationssicherheit übernommen und delegiert an den ISB die Umsetzung der geforderten Maßnahmen. Einmal monatlich erhält die Geschäftsführung einen Management-Report, kontrolliert den Umsetzungsstatus der Maßnahmen und initiiert ggf. weitere Maßnahmen und bewilligt das entsprechende Budget.
ISMS.1.A5	Vertragsgestaltung bei Bestellung eines externen Informationssicherheitsbeauftragten	Institutionsleitung	entbehrlich	Der Informationssicherheitsbeauftragte ist ein interner Mitarbeiter der RECPLAST GmbH.
ISMS.1.A7	Festlegung von Sicherheitsmaßnahmen	ISB	teilweise	Alle Mitarbeiter, die Maßnahmen im Sinne der Informationssicherheit umsetzen, sind verpflichtet, diese zu dokumentieren und dem ISB per E-Mail zuzusenden. Eine Auswertung und ausreichende Dokumentation der eingehenden umgesetzten Maßnahmen gibt es nicht. Umsetzungszeitpunkt für ausführliche Dokumentation: 30.04.
ISMS.1.A11	Aufrechterhaltung der Informationssicherheit	ISB	umgesetzt	Alle Dokumente und Prozesse werden einmal jährlich einem internen Audit unterzogen. Der ISB hat dafür die entsprechende fachliche Weisungsbefugnis für die Mitarbeiter, in deren Verantwortungsbereich einzelne Dokumente und Prozesse fallen.

Abbildung 31: Auszug aus dem IT-Grundschutz-Check der RECPLAST GmbH (Baustein ISMS.1)

Aktionspunkte zu 8.4.1 Organisatorische Vorarbeiten des IT-Grundschutz-Checks

- 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

8.4.2 Durchführung des Soll-Ist-Vergleichs

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

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

"entbehrlich" Die Erfüllung der Anforderung ist in der vorgeschlagenen Art nicht notwendig, weil die Anforderung im betrachteten Informationsverbund nicht relevant ist (z. B. weil Dienste nicht aktiviert wurden) oder durch Alternativmaßnahmen behandelt wurde.

Wird der Umsetzungsstatus einer Anforderung auf "entbehrlich" gesetzt, müssen über die Kreuzreferenztabelle des jeweiligen Bausteins die zugehörigen elementaren Gefährdungen identifiziert werden. Wurden Alternativmaßnahmen ergriffen, muss begründet werden, dass das Risiko, das durch alle betreffenden elementaren Gefährdungen ausgeht, angemessen minimiert wurde. Generell ist zu beachten, dass bei Basis-Anforderungen das entstehende Risiko nicht übernommen werden kann.

Anforderungen dürfen nicht auf "entbehrlich" gesetzt werden, indem das Risiko für eine im Baustein identifizierte elementare Gefährdung über die Kreuzreferenztabelle pauschal akzeptiert oder ausgeschlossen wird.

"ja" Zu der Anforderung wurden geeignete Maßnahmen vollständig, wirksam und angemessen umgesetzt.

"teilweise" Die Anforderung wurde nur teilweise umgesetzt.

"nein" Die Anforderung wurde noch nicht erfüllt, also geeignete Maßnahmen sind größtenteils noch nicht umgesetzt.

Es ist sinnvoll, bei den Interviews nicht nur die Bausteintexte, sondern auch die Umsetzungshinweise oder andere ergänzende Materialien griffbereit zu haben. Den Befragten sollte der Zweck des IT-Grundschutz-Checks kurz vorgestellt werden. Es bietet sich an, mit den Anforderungsüberschriften fortzufahren und die Anforderung kurz zu erläutern. Dem Gesprächspartner sollte die Möglichkeit gegeben werden, auf die bereits umgesetzten Anforderungen und Maßnahmen einzugehen, und danach noch offene Punkte zu besprechen.

Die Befragungstiefe richtet sich zunächst nach dem Niveau von Basis- und Standard-Anforderungen, darüber hinausgehende Aspekte hochschutzbedürftiger Anwendungen sollten erst nach Abschluss des IT-Grundschutz-Checks 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 jedes Bausteins sollte den Befragten das Ergebnis (Umsetzungsstatus der Anforderungen: entbehrlich/ja/teilweise/nein) mitgeteilt und diese Entscheidung erläutert werden.

Aktionspunkte zu 8.4.2 Durchführung des Soll-Ist-Vergleichs

- Je nach Fachgebiet vorab Checklisten erstellen
- Zielsetzung des IT-Grundschutz-Checks den Interviewpartnern erläutern
- Umsetzungsstatus der einzelnen Anforderungen erfragen
- Antworten anhand von Stichproben am Objekt verifizieren
- Ergebnisse den Befragten mitteilen

8.4.3 Dokumentation der Ergebnisse

Die Ergebnisse des IT-Grundschutz-Checks sollten so dokumentiert werden, dass sie für alle Beteiligten nachvollziehbar sind und als Grundlage für die Umsetzungsplanung der defizitären Anforderungen und Maßnahmen genutzt werden können. Der Dokumentationsaufwand sollte nicht unterschätzt werden. Daher sollten geeignete Hilfsmittel genutzt werden, die bei der Erstellung und Aktualisierung aller im Sicherheitsprozess erforderlichen Dokumente unterstützen.

Dies können zum einen geeignete IT-Grundschutz-Tools sein, also Anwendungen, die die gesamte Vorgehensweise nach IT-Grundschutz unterstützen, beginnend bei der Stammdatenerfassung, über die Schutzbedarfsfeststellung, die Risikoanalyse sowie den Soll-Ist-Vergleich (IT-Grundschutz-Check) bis hin zur Erfüllung der Anforderungen. 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-Grundschutz-Kompendiums gibt es eine Datei, in der tabellarisch für jede Anforderung des Bausteins die Ergebnisse des Soll-Ist-Vergleichs erfasst werden können.

Zur Dokumentation des IT-Grundschutz-Checks sollten erfasst werden:

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

Die eigentlichen Ergebnisse des Soll-Ist-Vergleichs sollten tabellarisch erfasst werden. Dabei sollten zu jeder Anforderung des jeweiligen Bausteins folgende Informationen festgehalten werden:

- Umsetzungsgrad (entbehrlich/ja/teilweise/nein)
  Der im Interview ermittelte Umsetzungsstatus der jeweiligen Anforderung ist zu erfassen. Im Hinblick auf eine mögliche Zertifizierung sollte außerdem erfasst werden, durch welche Maßnahmen die Anforderungen konkret erfüllt werden.
- Umsetzung bis
  Ein solches Feld ist sinnvoll, auch wenn es während eines IT-Grundschutz-Checks im Allgemeinen nicht ausgefüllt wird. Es dient als Platzhalter, um in der Realisierungsplanung an dieser Stelle zu dokumentieren, bis zu welchem Termin die Anforderung vollständig umgesetzt sein soll.
- Verantwortliche
  Falls es bei der Durchführung des Soll-Ist-Vergleichs eindeutig ist, welche Mitarbeiter für die vollständige Umsetzung einer defizitären Anforderung oder Maßnahme verantwortlich sind, sollte das namentlich in diesem Feld dokumentiert werden. Falls die Verantwortung nicht eindeutig erkennbar ist, sollte das Feld freigelassen werden. Im Zuge der späteren Realisierungsplanung ist dann ein Verantwortlicher zu bestimmen, dessen Name hier eingetragen werden kann.
- Bemerkungen / Begründungen
  Ein solches Feld ist wichtig, um getroffene Entscheidungen später nachvollziehen zu können, beispielsweise für die Zertifizierung. Bei Anforderungen, deren Umsetzung entbehrlich erscheint, ist hier die Begründung zu nennen. Bei Anforderungen, die noch nicht oder nur teilweise umgesetzt sind, sollte in diesem Feld dokumentiert werden, welche Maßnahmen noch umgesetzt werden müssen. In dieses Feld sollten auch alle anderen Bemerkungen eingetragen werden, die bei der Beseitigung von Defiziten hilfreich oder im Zusammenhang mit der Anforderung zu berücksichtigen sind.
- Defizite / Kostenschätzung
  Für Anforderungen, die nicht oder nur teilweise erfüllt wurden, ist das damit verbundene Risiko in geeigneter Form zu ermitteln und zu dokumentieren. Dies ist beispielsweise für Audits und Zertifizierungen wichtig. Bei solchen Maßnahmen sollte außerdem geschätzt werden, welchen finanziellen und personellen Aufwand die Beseitigung der Defizite erfordert.

Aktionspunkte zu 8.4.3 Dokumentation der Ergebnisse

- Stamminformationen über jedes Zielobjekt erfassen
- Informationen zum IT-Grundschutz-Check und zum Umsetzungsstatus dokumentieren
- Felder beziehungsweise Platzhalter für die Realisierungsplanung vorsehen

8.5 Risikoanalyse

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

Zweistufiger Ansatz der IT-Grundschutz-Vorgehensweise

In der Vorgehensweise nach IT-Grundschutz wird bei der Erstellung der IT-Grundschutz-Bausteine implizit eine Risikobewertung für Bereiche mit normalem Schutzbedarf durchgeführt. Hierbei werden nur solche Gefährdungen betrachtet, die nach sorgfältiger Analyse eine so hohe Eintrittswahrscheinlichkeit oder so einschneidende Auswirkungen haben, dass Sicherheitsmaßnahmen ergriffen werden müssen. Typische Gefährdungen, gegen die sich jeder schützen muss, sind z. B. Schäden durch Feuer, Einbrecher, Schadsoftware oder Hardware-Defekte. Dieser Ansatz hat den Vorteil, dass Anwender des IT-Grundschutzes für einen Großteil des Informationsverbundes keine individuelle Bedrohungs- und Schwachstellenanalyse durchführen müssen, weil diese Bewertung vorab bereits durchgeführt wurde.

In bestimmten Fällen muss jedoch eine explizite Risikoanalyse durchgeführt werden, beispielsweise wenn der betrachtete Informationsverbund Zielobjekte enthält, 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.

In diesen Fällen stellen sich folgende Fragen:

- Welchen Gefährdungen für die Informationsverarbeitung ist durch die Umsetzung der relevanten IT-Grundschutz-Bausteine noch nicht ausreichend oder sogar noch gar nicht Rechnung getragen?
- Müssen eventuell ergänzende Sicherheitsmaßnahmen, die über das IT-Grundschutz-Modell hinausgehen, eingeplant und umgesetzt werden?

Zur Beantwortung dieser Fragen empfiehlt das BSI die Anwendung einer Risikoanalyse auf der Basis von IT-Grundschutz, wie sie im BSI-Standard 200-3 beschrieben ist.

In dem Standard wird dargestellt, wie für bestimmte Zielobjekte festgestellt werden kann, ob und in welcher Hinsicht über den IT-Grundschutz hinaus Handlungsbedarf besteht, um Risiken für die Informationsverarbeitung zu reduzieren. Hierzu werden Risiken, die von elementaren Gefährdungen ausgehen, eingeschätzt und anhand einer Matrix bewertet. Die Einschätzung erfolgt über die zu erwartende Häufigkeit des Eintretens und die Höhe des Schadens, der bei Eintritt des Schadensereignisses entsteht. Aus diesen beiden Anteilen ergibt sich das Risiko. Die Methodik lässt sich wie folgt in den IT-Grundschutz-Prozess integrieren:

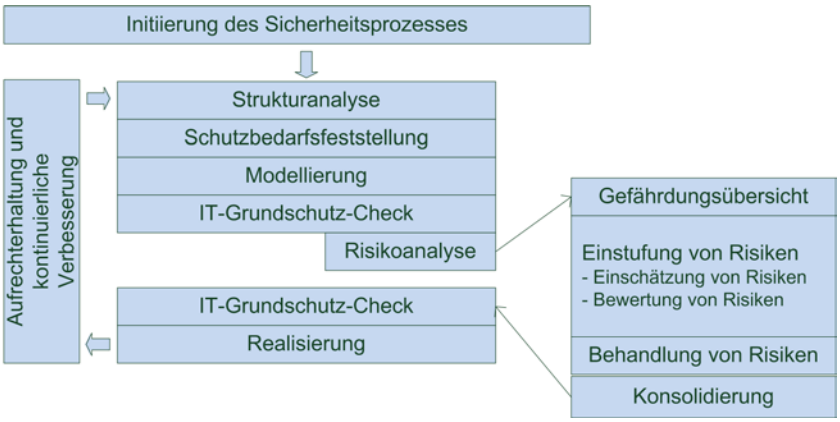


Abbildung 32: Integration der Risikoanalyse in den IT-Grundschutz-Prozess

Der Standard bietet sich an, wenn Institutionen bereits erfolgreich mit der IT-Grundschutz-Methodik arbeiten und möglichst direkt eine Risikoanalyse an die IT-Grundschutz-Analyse anschließen möchten. Hierzu empfiehlt der BSI-Standard 200-3 *Risikoanalyse auf der Basis von IT-Grundschutz* folgende zusätzliche Arbeitsschritte, die hier kurz im Überblick aufgeführt sind:

- Etablierung eines Risikomanagementprozesses
  Die Risikoanalyse ist ein wichtiger Bestandteil des Managementsystems für Informationssicherheit (ISMS). Daher sollten die Grundvoraussetzungen dafür von der Institutionsleitung vorgegeben werden. Die grundsätzliche Vorgehensweise der Institution zur Durchführung von Risikoanalysen sollte in einer Richtlinie (siehe BSI-Standard 200-3, Kapitel 2) dokumentiert und durch die Leitungsebene verabschiedet werden.

- Erstellung der Gefährdungsübersicht
  In diesem Arbeitsschritt wird für jedes zu analysierende Zielobjekt eine Liste der jeweils relevanten Gefährdungen zusammengestellt. Bei der Ermittlung von Gefährdungen geht das BSI zweistufig vor. Zunächst werden die relevanten elementaren Gefährdungen identifiziert und darauf aufbauend werden weitere mögliche Gefährdungen (zusätzliche Gefährdungen) ermittelt, die über die elementaren Gefährdungen hinausgehen und sich aus dem spezifischen Einsatzszenario ergeben. Dies erfolgt im Rahmen eines gemeinsamen Brainstormings.

- Risikoeinstufung
  Die Risikoanalyse ist zweistufig angelegt. Für jedes Zielobjekt und jede Gefährdung wird eine Bewertung unter der Annahme vorgenommen, dass bereits Sicherheitsmaßnahmen umgesetzt oder geplant worden sind. In der Regel wird es sich hierbei um Sicherheitsmaßnahmen handeln, die aus den Basis- und Standard-Anforderungen des IT-Grundschutz-Kompendiums abgeleitet worden sind. An die erste Bewertung schließt sich eine zweite an, bei der mögliche Sicherheitsmaßnahmen zur Risikobehandlung betrachtet werden. Durch einen Vorher-Nachher-Vergleich lässt sich die Wirksamkeit der Sicherheitsmaßnahmen prüfen, die zur Risikobehandlung eingesetzt worden sind.

- Behandlung von Risiken
  Abhängig vom Risikoappetit einer Institution sind jeweils unterschiedliche Risikoakzeptanzkriterien möglich. Risikoappetit bezeichnet die durch kulturelle, interne, externe oder wirtschaftliche Einflüsse entstandene Neigung einer Institution, wie sie Risiken bewertet und mit ihnen umgeht. Es gibt folgende Optionen zur Behandlung von Risiken:

  - Risiken können vermieden werden (z. B. durch Umstrukturierung von Geschäftsprozessen oder des Informationsverbundes).
  - Risiken können durch entsprechende Sicherheitsmaßnahmen reduziert werden.
  - Risiken können transferiert werden (z. B. durch Outsourcing oder Versicherungen).

Daran anschließend muss eine Institution Risikoakzeptanzkriterien festlegen und die Behandlung des Risikos darauf abbilden. Bei der Entscheidung, wie mit den identifizierten Risiken umzugehen ist, muss auf jeden Fall die Leitungsebene beteiligt werden, da sich daraus unter Umständen erhebliche Schäden ergeben oder zusätzliche Kosten entstehen können.

Die Schritte Gefährdungsbewertung und Risikobehandlung werden so lange durchlaufen, bis die Risikoakzeptanzkriterien der Institution erfüllt sind und das verbleibende Risiko ("Restrisiko") im Einklang mit den Zielen und Vorgaben der Institution steht. Das verbleibende Risiko muss anschließend der Leitungsebene zur Zustimmung vorgelegt werden ("**Risiko-Akzeptanz**"). Damit wird nachvollziehbar dokumentiert, dass die Institution sich des Restrisikos bewusst ist.

- Konsolidierung des Sicherheitskonzepts
  Bevor der originäre IT-Grundschutz-Prozess fortgesetzt werden kann, muss das erweiterte Sicherheitskonzept konsolidiert werden. Dabei werden die Eignung, das Zusammenwirken, die Benutzerfreundlichkeit und die Angemessenheit der Sicherheitsmaßnahmen insgesamt überprüft.
- Außerdem wird im BSI-Standard 200-3 *Risikoanalyse auf der Basis von IT-Grundschutz* erläutert, wie die Methodik anzuwenden ist, wenn der Informationsverbund Zielobjekte umfasst, für die im IT-Grundschutz-Kompendium bislang kein geeigneter Baustein enthalten ist.

Eine ausführliche Darstellung der Methodik findet sich im BSI-Standard 200-3.

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

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

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

Risikoanalyse direkt nach dem IT-Grundschutz-Check	**Risikoanalyse erst nach vollständiger Umsetzung der Sicherheitsmaßnahmen**
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: • Sicherheitsmaßnahmen werden früher umgesetzt, da die Risikoanalyse häufig aufwendig ist. • Elementare Sicherheitslücken werden vorrangig behandelt, bevor fortgeschrittene Gefährdungen analysiert werden.
Mögliche Nachteile: • Sicherheitsmaßnahmen werden später umgesetzt, da die Risikoanalyse häufig aufwendig ist.	Mögliche Nachteile: • Es kann Mehraufwand entstehen, da eventuell einige Sicherheitsmaßnahmen umgesetzt werden, die später im Rahmen der Risikoanalyse durch stärkere Maßnahmen

Risikoanalyse direkt nach dem IT-Grundschutz-Check	Risikoanalyse erst nach vollständiger Umsetzung der Sicherheitsmaßnahmen
• Eventuell werden elementare Sicherheitslücken vernachlässigt, während fortgeschrittene Gefährdungen analysiert werden.	ersetzt werden. • Eventuell erforderliche Hochsicherheitsmaßnahmen werden erst später identifiziert und umgesetzt.

Tabelle 7: Vor- und Nachteile der alternativen Reihenfolgen bei der Risikoanalyse

Wichtig ist außerdem, dass eine *Risikoanalyse auf der Basis von IT-Grundschutz* häufig leichter durchzuführen ist, wenn sie nacheinander auf kleine Teilaspekte des Informationsverbunds angewandt wird. Als ersten Schritt kann die Analyse beispielsweise auf die baulich-physische Infrastruktur beschränkt werden, das heißt auf den Schutz vor Brand, Wasser und unbefugtem Zutritt sowie auf die ordnungsgemäße Strom- und Klimaversorgung.
In vielen Behörden und Unternehmen existieren bereits Verfahren zur Risikoanalyse beziehungsweise zur Risikobehandlung. Um eine einheitliche Methodik zu erreichen, kann es in solchen Fällen zweckmäßig sein, die vorhandenen Verfahren auf die Informationssicherheit auszudehnen und gegebenenfalls nur Teilaspekte des BSI-Standards 200-3 anzuwenden. International haben sich eine Reihe von unterschiedlichen Ansätzen zur Durchführung von Risikoanalysen im Bereich der Informationssicherheit etabliert. Diese Verfahren unterscheiden sich beispielsweise in Bezug auf den Detaillierungsgrad, die Formalisierung und die thematischen Schwerpunkte. Abhängig von den Rahmenbedingungen einer Institution und der Art des Informationsverbunds kann es zweckmäßig sein, alternativ zum BSI-Standard 200-3 ein anderes etabliertes Verfahren oder eine angepasste Methodik für die Analyse von Informationsrisiken zu verwenden.

Aktionspunkte zu 8.5 Risikoanalyse

- Grundsätzliche Vorgehensweise der Institution zur Durchführung von Risikoanalysen in einer Richtlinie dokumentieren und der Leitungsebene zur Verabschiedung vorlegen
- Ermitteln, für welche Zielobjekte oder Gruppen von Zielobjekten eine Risikoanalyse durchgeführt werden soll
- BSI-Standard 200-3 *Risikoanalyse auf der Basis von IT-Grundschutz* systematisch durcharbeiten
- Ergebnisse der Risikoanalysen in das Sicherheitskonzept integrieren

9 Umsetzung der Sicherheitskonzeption

In diesem Kapitel werden verschiedene Aspekte vorgestellt, die bei der Planung und Realisierung von Sicherheitsmaßnahmen beachtet werden müssen. Dabei wird beschrieben, wie die Umsetzung von Sicherheitsmaßnahmen geplant, durchgeführt, begleitet und überwacht werden kann. Zu vielen Bausteinen des IT-Grundschutzes existieren Umsetzungshinweise mit beispielhaften Empfehlungen für Sicherheitsmaßnahmen, mit den die Anforderungen der Bausteine umgesetzt werden können. Diese basieren auf Best Practices und langjähriger Erfahrung von Experten aus dem Bereich der Informationssicherheit. Die Maßnahmen aus den Umsetzungshinweisen sind jedoch nicht als verbindlich zu betrachten, sondern können und sollten durch eigene Maßnahmen ergänzt oder ersetzt werden. Solche eigenen Maßnahmen sollten wiederum dem IT-Grundschutz-Team des BSI mitgeteilt werden, vor allem, wenn sie neue Aspekte enthalten, damit die Umsetzungshinweise entsprechend ergänzt werden können.

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

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

9.1 Sichtung der Untersuchungsergebnisse

In einer Gesamtsicht sollte ausgewertet werden, welche Anforderungen aus den IT-Grundschutz-Bausteinen nicht oder nur teilweise umgesetzt wurden. Dazu bietet es sich an, diese aus den Ergebnissen des IT-Grundschutz-Checks zu extrahieren und in einer Tabelle zusammenzufassen.

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

Die zu erfüllenden Anforderungen aus den IT-Grundschutz-Bausteinen müssen passend zu den organisatorischen und technischen Gegebenheiten der Institution zu Sicherheitsmaßnahmen konkretisiert werden. Die Umsetzungshinweise des IT-Grundschutzes geben dazu für viele Bausteine und Anforderungen praxisnahe Empfehlungen. Außerdem sollten alle Anforderungen und alle daraus abgeleiteten 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. Außerdem müssen sie wirtschaftlich sein, siehe unten. In solchen Fällen kann es notwendig werden, bestimmte IT-Grundschutz-Anforderungen so anzupassen, dass dieselben Sicherheitsziele erreicht werden. Basis-Anforderungen sind so elementar, dass diese im Normalfall nicht ersetzt werden können.

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

Weiterführende Hinweise zur Konsolidierung der Sicherheitsmaßnahmen finden sich außerdem im BSI-Standard 200-3 *Risikoanalyse auf der Basis von IT-Grundschutz*.

Beispiele:

- Bei einer Risikoanalyse wurde festgestellt, dass zusätzlich zu den IT-Grundschutz-Anforderungen auch eine chipkartengestützte Authentisierung und lokale Verschlüsselung der Festplatten an Clients der Personaldatenverarbeitung notwendig sind. Diese zusätzlichen Anforderungen sollten im Sicherheitskonzept ergänzt werden.
- Im Sicherheitskonzept für ein Krankenhaus wurde festgelegt, dass für alle IT-Systeme eine Authentisierung erforderlich ist und ein Time-out nach zehn Minuten erfolgt. Beim IT-Grundschutz-Check stellt sich heraus, dass die Vorgabe zu pauschal ist und in dieser Form nicht praxistauglich ist. Daher wird jetzt im Sicherheitskonzept differenziert:
  - IT-Systeme im Verwaltungsbereich erfordern eine erneute Authentisierung nach 15 Minuten Inaktivität
  - Bei IT-Systemen in Bereichen, wo Patienten- und Besucherverkehr ist, erfolgt ein Time-out nach fünf Minuten
  - Bei IT-Systemen in Behandlungsräumen wird die automatische Abmeldung deaktiviert. Die Mitarbeiter erhalten die Anweisung, sich nach Verlassen der Räume abzumelden.

9.2 Kosten- und Aufwandsschätzung

Da das Budget zur Umsetzung von Sicherheitsmaßnahmen praktisch immer begrenzt ist, sollte für jede zu realisierende Maßnahme festgehalten werden, welche Investitionskosten und welcher Personalaufwand dafür benötigt werden. Hierbei sollte zwischen einmaligen und wiederkehrenden Investitionskosten bzw. Personalaufwand unterschieden werden. An dieser Stelle zeigt sich häufig, dass Einsparungen bei technischen oder infrastrukturellen Sicherheitsmaßnahmen dazu führen, dass sie einen hohen fortlaufenden Personaleinsatz verursachen. Umgekehrt führen Einsparungen beim Personal schnell zu kontinuierlich immer größeren werden Sicherheitsdefiziten.

In diesem Zusammenhang ist zu ermitteln, ob alle im ersten Zug aus den Anforderungen abgeleiteten Maßnahmen wirtschaftlich umsetzbar sind. Falls es Maßnahmen gibt, die nicht wirtschaftlich sind, sollten Überlegungen angestellt werden, durch welche Ersatzmaßnahmen die Anforderungen dennoch erfüllt werden können. Auch bei Informationssicherheit führen häufig viele Wege zum Ziel. Oftmals gibt es verschiedene Optionen, Anforderungen mit geeigneten Maßnahmen zu erfüllen. Falls keine angemessene Maßnahme gefunden werden kann, muss das entstehende Restrisiko sowie die Entscheidung dokumentiert werden. Basis-Anforderungen müssen im Normalfall immer erfüllt werden, die Akzeptanz eines Restrisikos ist aufgrund ihrer elementaren Natur nicht vorgesehen.

Stehen die geschätzten Ressourcen für Kosten und Personaleinsatz zur Verfügung, muss üblicherweise noch eine Entscheidung herbeigeführt werden, wie viel Ressourcen für die Umsetzung der Sicherheitsmaßnahmen tatsächlich eingesetzt werden sollen. Hierfür bietet es sich an, der Leitungsebene die Ergebnisse der Sicherheitsuntersuchung darzustellen. Geordnet nach Schutzbedarf sollten die festgestellten Schwachstellen (nicht oder unzureichend erfüllte Sicherheitsanforderungen) zur Sensibilisierung vorgestellt werden. Auch auf die spezifischen Gefährdungen, die in den jeweiligen Bausteinen genannt werden, kann hierbei zurückgegriffen werden. Darüber hinaus bietet es sich an, die für die Realisierung der noch notwendigen Maßnahmen anfallenden Kosten und den zu erwartenden Aufwand aufzubereiten. Im Anschluss 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 Anforderungen nicht oder verzögert erfüllt werden. Zu diesem Zweck können die sogenannten Kreuzreferenztabellen aus den Hilfsmitteln zum IT-Grundschutz hinzugezogen werden. Die Kreuzreferenztabellen geben für jeden Baustein eine Übersicht darüber, welche Anforderungen gegen welche elementaren Gefährdungen wirken. Analog lässt sich anhand dieser Tabellen ebenfalls ermitteln, gegen welche elementaren Gefährdungen kein ausreichender Schutz besteht, wenn Anforderungen aus den Bausteinen nicht erfüllt 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.

9.3 Festlegung der Umsetzungsreihenfolge der Maßnahmen

Kapitel 8.3.3 beschreibt eine Reihenfolge, in der Bausteine umgesetzt werden sollten, von grundlegenden und übergreifenden Bausteinen bis hin zu solchen, die speziellere Themen abdecken und daher in der zeitlichen Reihenfolge eher nachrangig betrachtet werden können. Diese Reihenfolge der Baustein-Umsetzung ist vor allem bei der Basis-Absicherung wichtig. Sie kann aber auch allgemein bei der Festlegung der Umsetzungsreihenfolge für die einzelnen Maßnahmen eines Sicherheitskonzeptes herangezogen werden.

Grundsätzlich sind als Erstes die aus den Basis-Anforderungen abgeleiteten Maßnahmen umzusetzen, dann die der Standard-Anforderungen. Die zusätzlichen Maßnahmen für den erhöhten Schutzbedarf sollten erst anschließend angepasst und umgesetzt werden.

Wenn das vorhandene Budget oder die personellen Ressourcen nicht ausreichen, um sämtliche noch notwendigen Maßnahmen sofort umsetzen zu können, muss hier eine Priorisierung festgelegt werden.

Die weitere Umsetzungsreihenfolge orientiert sich daran, was für die jeweilige Institution am sinnvollsten ist. Tipps dazu sind:

- Die Umsetzungsreihenfolge kann sich daran festmachen, wann im Lebenszyklus eines Zielobjektes die jeweiligen Maßnahmen umzusetzen sind. Bei neuen Zielobjekten sind beispielsweise Maßnahmen aus den Bereichen Planung und Konzeption vor solchen umzusetzen, bei denen es um den sicheren Betrieb geht, während bei schon länger im Informationsverbund vorhandenen Zielobjekten zunächst die Absicherung des Betriebs im Vordergrund stehen sollte.
- Bei einigen Maßnahmen ergibt sich durch Abhängigkeiten und logische Zusammenhänge eine zwingende zeitliche Reihenfolge. So kann eine restriktive Rechtevergabe (Basis-Anforderung) auf einem neuen Server nur erfolgen, wenn dieser zunächst sicher installiert wurde (Standard-Anforderung). Diese Reihenfolge kann mit der Klassifikation in Basis- und Standard-Anforderungen auf den ersten Blick kollidieren. Dennoch haben Basis-Anforderungen inhaltlich stets Priorität, sofern sie bereits erfüllbar sind, im Beispiel etwa bei einem bestehenden Server.
- Manche Maßnahmen erzielen eine große Breitenwirkung, manche jedoch nur eine eingeschränkte lokale Wirkung. Oft ist es sinnvoll, zuerst auf die Breitenwirkung zu achten. Auch daher sollten bevorzugt die Basis-Anforderungen umgesetzt werden, da mit diesen die schnellste Absicherung in der Breite erreicht werden kann. Es lohnt sich aber auch durchaus, die Maßnahmen aus den verschiedenen Bereichen danach zu gewichten, wie schnell sie sich umsetzen lassen und welchen Sicherheitsgewinn sie liefern. Quick-Wins lassen sich häufig im organisatorischen Bereich finden oder durch zentrale Konfigurationseinstellungen erreichen.
- Es gibt Bausteine, die auf das angestrebte Sicherheitsniveau einen größeren Einfluss haben als andere. Maßnahmen eines solchen Bausteins sollten bevorzugt behandelt werden, insbesondere wenn hierdurch Schwachstellen in hochschutzbedürftigen Bereichen beseitigt werden. So sollten immer zunächst die Server abgesichert werden (unter anderem durch Umsetzung des Bausteins SYS.1.1 *Allgemeiner Server*) und dann erst die angeschlossenen Clients.
- Bausteine mit auffallend vielen nicht umgesetzten Anforderungen repräsentieren Bereiche mit vielen Schwachstellen. Sie sollten ebenfalls bevorzugt behandelt werden.

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

Hinweis:

Bereits einleitend wurde darauf hingewiesen, dass die Erfüllung von Anforderungen an fehlenden Ressourcen scheitern kann. Die oben angeführten Aspekte ermöglichen eine erste Priorisierung. Bei dieser Vorgehensweise werden jedoch die verbleibenden Restrisiken nicht hinreichend betrachtet. Wenn Anforderungen aus IT-Grundschutz-Bausteinen nicht erfüllt sind, ist es empfehlenswert, im Rahmen einer vereinfachten Risikoanalyse die entstandenen Defizite zu betrachten. In diesem Fall kann die in der Risikoanalyse durchzuführende Ermittlung von Gefährdungen entfallen. Dies ist bereits bei der Erstellung der Grundschutz-Bausteine geschehen. Es verbleibt somit die Bewertung des Risikos aufgrund der fehlenden Umsetzung von Anforderungen.

9.4 Festlegung der Aufgaben und der Verantwortung

Nachdem die Reihenfolge für die Umsetzung der Maßnahmen bestimmt wurde, muss anschließend festgelegt werden, wer bis wann welche Maßnahmen realisieren muss. Ohne eine solche verbindliche 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 ISB erfolgen. Der ISB muss kontinuierlich über den Fortschritt der Realisierung und über die Ergebnisse der Umsetzung informiert werden. Der ISB wiederum muss regelmäßig die Leitungsebene über den Fortschritt und die damit verbundene Absenkung vorhandener Risiken informieren.

Der Realisierungsplan sollte mindestens folgende Informationen umfassen:

- Bezeichnung des Zielobjektes als Einsatzumfeld,
- Nummer bzw. Titel des betrachteten Bausteins,
- Titel bzw. Beschreibung der zu erfüllenden Anforderung,
- Beschreibung der umzusetzenden Maßnahme bzw. Verweis auf die Beschreibung im Sicherheitskonzept,
- Terminplanung für die Umsetzung, Budgetplanung, beispielsweise für Beschaffung und Betriebskosten von Komponenten,
- Verantwortliche für die Umsetzung der Maßnahmen.

9.5 Realisierungsbegleitende Maßnahmen

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

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

Beispiel: RECPLAST GmbH

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

A.6 Realisierungsplan der RECPLAST GmbH						
Zielobjekt	**Baustein**	**Anforderungstext**	**umzusetzende Maßnahmen**	**Terminplanung**	**Budget**	**Verantwortlich für die Umsetzung**
S008 - Print-Server	SYS.1.1 Allgemeiner Server	SYS.1.1.A3 Restriktive Rechtvergabe	In der Rechtevergabe müssen die letzten Gruppenberechtigugnen aufgelöst werden.	Q3 des Jahres	- €	Herr Schmidt (IT-Betrieb)
S008 - Print-Server	SYS.1.1 Allgemeiner Server	SYS.1.1.A4 Rollentrennung	Es sind noch nicht für jeden Administrator separate Benutzer-Kennungen eingerichtet.	31.07. des Jahres	- €	Herr Schmidt (IT-Betrieb)
S008 - Print-Server	SYS.1.1 Allgemeiner Server	SYS.1.1.A8 Regelmäßige Datensicherung	Die Datensicherungen werden derzeit auf Bändern innerhalb des Serverraumes aufbewahrt. Geplant ist hierzu ein externes Backup-System. Ein Angebot für die Initialisierung liegt bereits vor (15.000 €). Die Betriebskosten müssen noch verhandelt werden.	Q1 Folgejahr	Anschaffung: 15.000 € Betriebskosten: noch offen	Frau Meyer (Einkauf)

Abbildung 33: Realisierungsplan der RECPLAST GmbH (Auszug)

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

Aktionspunkte zu 9 Umsetzung der Sicherheitskonzeption

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

10 Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit

Um den Informationssicherheitsprozess aufrecht zu erhalten und kontinuierlich verbessern zu können, müssen nicht nur angemessene Sicherheitsmaßnahmen implementiert und Dokumente fortlaufend aktualisiert werden, sondern auch der IS-Prozess selbst muss regelmäßig auf seine Wirksamkeit und Effizienz hin überprüft werden. Dabei sollte regelmäßig eine Erfolgskontrolle und Bewertung des IS-Prozesses durch die Leitungsebene stattfinden (Managementbewertung). Bei Bedarf (z. B. bei der Häufung von Sicherheitsvorfällen oder gravierenden Änderung der Rahmenbedingungen) muss auch zwischen den Routineterminen getagt werden. Alle Ergebnisse und Beschlüsse müssen nachvollziehbar dokumentiert werden. Die Dokumente müssen aussagekräftig und für die jeweilige Zielgruppe verständlich sein, siehe auch Kapitel 5.2 *Informationsfluss im Informationssicherheitsprozess*. Es ist eine Aufgabe des ISB, diese Informationen zu sammeln, zu verarbeiten und entsprechend kurz und übersichtlich für die Leitungsebene aufzubereiten.

10.1 Überprüfung des Informationssicherheitsprozesses in allen Ebenen

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

Zur Effizienzprüfung und Verbesserung des Informationssicherheitsprozesses sollten Verfahren und Mechanismen eingerichtet werden, die einerseits die Realisierung der beschlossenen Maßnahmen und andererseits ihre Wirksamkeit und Effizienz überprüfen.

Die Informationssicherheitsstrategie sollte daher auch Leitaussagen zur Messung der Zielerreichung machen, dabei sollte mindestens definiert werden:

- welche Ziele in welcher Form und sinnvoller Anzahl überwacht oder gemessen werden (WAS)
- wer für die Überwachung oder Messung der zuvor festgelegten Punkte verantwortlich ist (WER)
- wann und wie häufig die Ergebnisse auszuwerten sind (WANN)

Grundsätzlich sollte sich die Überprüfung des Informationssicherheitsprozesses auf eine sinnvolle Anzahl von Zielen beschränken. Beispiele für Methoden können sein:

- Definition, Dokumentation und Auswertung von Kennzahlen (z. B. Aktualität des Virenschutzes und Anzahl detektierte Schadsoftware, etc.)
- Detektion, Dokumentation und Auswertung von Sicherheitsvorfällen
- Durchführung von Übungen und Tests zur Simulation von Sicherheitsvorfällen und Dokumentation der Ergebnisse (z. B. Backup-Wiederherstellung)
- interne und externe Audits, Datenschutzkontrollen
- Zertifizierung nach festgelegten Sicherheitskriterien (z. B. ISO 27001 auf Basis von IT-Grundschutz)

Die erfolgreiche Umsetzung von Sicherheitsmaßnahmen sollte regelmäßig überprüft werden. Grundsätzlich ist dabei wichtig, dass Prüfungen und Audits nicht von denjenigen durchgeführt werden, die die jeweiligen Sicherheitsvorgaben entwickelt haben und dass die Leitung der Institution über den aus den Audits abgeleiteten Stand der Informationssicherheit informiert wird.

Um Betriebsblindheit zu vermeiden, kann es sinnvoll sein, externe Experten mit der Durchführung solcher Prüfungsaktivitäten zu beauftragen.

Da der Aufwand bei Audits von der Komplexität und Größe des Informationsverbunds abhängt, sind die Anforderungen auch für kleine Institutionen sehr gut umzusetzen. Mit Hilfe von automatisiertem Monitoring und Reporting kann eine kontinuierliche Analyse der Informationssicherheit bei geringer Ressourcenbelastung ermöglicht werden. Mit einer Durchsicht vorhandener Dokumentationen, um die Aktualität zu prüfen, und einem Workshop, bei dem Probleme und Erfahrungen mit dem Sicherheitskonzept besprochen werden, kann in kleinen Institutionen bereits ein ausreichender Überblick über den Status der Informationssicherheit gewonnen werden.

10.1.1 Überprüfung anhand von Kennzahlen

Kennzahlen werden in der Informationssicherheit eingesetzt, um den IS-Prozess bzw. Teilaspekte davon messbar zu machen. Sie dienen dazu, den Prozess zu optimieren und Güte, Effizienz und Effektivität der vorhandenen Sicherheitsmaßnahmen zu überprüfen.

Messungen und Kennzahlen dienen häufig der Kommunikation mit dem Management und können dem Informationssicherheitsmanagement wertvolle Argumentationshilfen liefern. Daher ist es wichtig, Messwerkzeuge so auszuwählen und durchgeführte Messungen so aufzubereiten, dass sie in das strategische Umfeld der eigenen Institution passen.

Kennzahlen zu ermitteln, bedeutet immer auch Aufwand. Dieser sollte in einer vernünftigen Relation zu den erhofften bzw. erzielten Ergebnissen stehen. Kennzahlen haben eine begrenzte Aussagekraft, da damit einzelne, meist wenige Bereiche der Informationssicherheit punktuell beleuchtet werden, nämlich meist diejenigen, in denen sich leicht Messwerte erzielen lassen. Dies betrifft im Allgemeinen die technische Sicherheit, bei der über Sensoren automatisiert Messwerte zurückgemeldet werden können, und andere, leicht quantifizierbare Aussagen, wie z. B.

- Anzahl der erkannten Schadsoftware-Muster
- Anzahl der installierten Sicherheitspatches
- Dauer der Systemausfälle
- Anzahl der durchgeführten Sicherheitsschulungen

Kennzahlen lassen sich immer unterschiedlich interpretieren, wichtig ist daher, dass im Vorfeld klar ist, welches Ziel mit Messungen verfolgt wird und wie und mit welchem Aufwand dies erreicht werden soll. Gegen dieses Ziel kann dann gemessen werden.

10.1.2 Bewertung des ISMS mit Hilfe eines Reifegradmodells

Die Wirksamkeit des Managementsystems für Informationssicherheit einer Institution sollte regelmäßig bewertet werden. Dies kann mit Hilfe eines Reifegradmodells erfolgen. Ein Reifegradmodell ermöglicht, den Fortschritt des ISMS nachvollziehbar über die Jahre hinweg zu dokumentieren, ohne sich dabei in Einzelmaßnahmen zu verlieren. Es stellt eine weitere potentielle Kennzahl zur Steuerung der Informationssicherheit in einer Institution dar. Eine beispielhafte Reifegradbewertung eines ISMS kann wie folgt aussehen:

Reifegrad	Erläuterung
0	Es existiert kein ISMS und es ist auch nichts geplant.
1	ISMS ist geplant, aber nicht etabliert.
2	ISMS ist zum Teil etabliert.
3	ISMS ist voll etabliert und dokumentiert.
4	Zusätzlich zum Reifegrad 3 wird das ISMS regelmäßig auf Effektivität überprüft.
5	Zusätzlich zum Reifegrad 4 wird das ISMS regelmäßig verbessert.

Die Bewertung des Reifegrads eines ISMS kann sich durchaus mehrdimensional anhand von Themenfeldern darstellen, beispielsweise angelehnt am Schichtenmodell des IT-Grundschutzes:

- ISMS *(Managementsysteme für Informationssicherheit)*
- ORP *(Organisation und Personal)*
- CON *(Konzepte und Vorgehensweisen)*
- OPS *(Betrieb)*
- DER *(Detektion und Reaktion)*
- INF *(Infrastruktur)*
- NET *(Netze und Kommunikation)*
- SYS *(IT-Systeme)*
- APP *(Anwendungen)*
- IND *(Industrielle IT)*

Informationssicherheit ist eine Querschnittsfunktion, welche mit nahezu allen Bereiche einer Institution verzahnt ist. Aus diesem Grund ist es notwendig, die Informationssicherheit in bestehende Prozesse einer Institution zu integrieren. Beispiele hierfür sind:

- Projektmanagement: Bereits in der Planungsphase eines Projektes muss der Schutzbedarf der zukünftig als Ergebnis zu verarbeitenden Informationen bewertet werden und darauf aufbauend geeignete Sicherheitsmaßnahmen geplant werden.
- Incident Management: Bei Störungen des IT-Betriebs mit Auswirkungen auf die Informationssicherheit muss das Vorgehen mit dem Sicherheitsmanagement abgestimmt sein. Das Security Incident Management und Störungsmanagement der IT und des Facility Managements müssen verzahnt sein.

Existieren solche Management-Prozesse nicht, ist es möglich, ein ISMS aufzubauen und zu betreiben, es wird jedoch nicht effizient funktionieren. Wenn das ISMS nicht mit dem Projektmanagement verzahnt ist, kann der Schutzbedarf neuer oder geänderter Geschäftsprozesse nur durch zyklische Abfragen (jährlich, quartalsweise) ermittelt werden. Dadurch ist es deutlich schwieriger, eine vollständige und aktuelle Schutzbedarfsfeststellung aller Zielobjekte zu erhalten. Wenn kein Störungsmanagement vorhanden ist, werden Sicherheitsvorfälle nicht erkannt bzw. nicht an die korrekte Stelle gemeldet. Der Reifegrad der Informationssicherheit hängt somit auch vom Reifegrad der anderen Management-Prozesse der Institution ab und ist keine selbstständige Größe.

Der Reifegrad der Informationssicherheit kann von Institution zu Institution sehr unterschiedlich sein. Allein aus der Tatsache, dass ein Sicherheitsmanagement vorhanden ist, kann nicht darauf geschlossen werden, dass die Institution Sicherheitsvorfälle gut bewältigen kann. Durch eine einheitliche und differenzierte Bewertung des Umsetzungsniveaus des ISMS einer Institution können verschiedene wichtige Ziele erreicht werden:

- Überprüfung, ob die einzelnen Aspekte des Sicherheitsmanagements vollständig bearbeitet und umgesetzt wurden.
- Erkennung von Verbesserungs- und Weiterentwicklungspotentialen.
- Vergleichbarkeit des Umsetzungsniveaus beim Sicherheitsmanagement zwischen verschiedenen Institutionen.
- Nachweisbarkeit des erreichten Umsetzungsniveaus gegenüber Dritten.

Zusätzlich kann die Leitungsebene die Bewertungsergebnisse auch als Kennzahlen nutzen, um das Sicherheitsmanagementsystem zu steuern und weiterzuentwickeln (siehe Kapitel 5.2.1).

Wird das Umsetzungsniveau regelmäßig beurteilt, kann die kontinuierliche Weiterentwicklung des Informationssicherheitsmanagements der Institution nachvollziehbar und effizient dokumentiert werden.

10.1.3 Überprüfung der Umsetzung der Sicherheitsmaßnahmen

Im Realisierungsplan ist für alle Maßnahmen des Sicherheitskonzeptes enthalten, wer diese bis wann umzusetzen hat (Aufgabenliste und zeitliche Planung). Anhand dessen ist eine Auswertung möglich, inwieweit diese Planungen eingehalten wurden. Die Überprüfung des Informationssicherheitsprozesses dient zur Kontrolle der Aktivitäten im Rahmen des Sicherheitskonzeptes und zur Identifizierung von Planungsfehlern.

Nach der Einführung von neuen Sicherheitsmaßnahmen sollte durch den ISB geprüft werden, ob die notwendige Akzeptanz seitens der Mitarbeiter vorhanden ist. Die Ursachen fehlender Akzeptanz sind herauszuarbeiten und abzustellen.

Sicherheitsrevision

Die Informationssicherheitsrevision (IS-Revision) ist ein Bestandteil eines jeden erfolgreichen Informationssicherheitsmanagements. Nur durch die regelmäßige Überprüfung der etablierten Sicherheitsmaßnahmen und des Informationssicherheitsprozesses können Aussagen über deren wirksame Umsetzung, Aktualität, Vollständigkeit und Angemessenheit und damit über den aktuellen Zustand der Informationssicherheit getroffen werden. Die IS-Revision ist somit ein Werkzeug zum Feststellen, Erreichen und Aufrechterhalten eines angemessenen Sicherheitsniveaus in einer Institution. Das BSI hat hierzu mit dem *Leitfaden für die IS-Revision auf Basis von IT-Grundschutz* ein Verfahren entwickelt, um den Status der Informationssicherheit in einer Institution festzustellen und Schwachstellen identifizieren zu können (siehe [BSIR]).

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

Cyber-Sicherheits-Check

Mit Hilfe eines Cyber-Sicherheits-Checks können Institutionen das aktuelle Niveau der Cybersicherheit in ihrer Institution bestimmen. Der Cyber-Sicherheits-Check richtet sich an Institutionen, die sich bislang weniger intensiv mit dem Thema Cyber-Sicherheit beschäftigt haben. Zur Durchführung eines Cyber-Sicherheits-Checks werden explizit keine obligatorischen Voraussetzungen an Dokumentenlage oder Umsetzungsstatus gestellt (siehe [CSC]).

Der Cyber-Sicherheits-Check und die zugrunde liegenden Maßnahmenziele für die Beurteilung der Cyber-Sicherheit wurden so konzipiert, dass das Risiko, einem Cyber-Angriff zum Opfer zu fallen, durch regelmäßige Durchführung eines Cyber-Sicherheits-Checks minimiert werden kann. Dabei wurde die Vorgehensweise auf Cyber-Sicherheits-Belange fokussiert.

Das BSI und die ISACA stellen einen praxisnahen Handlungsleitfaden zur Verfügung, der konkrete Vorgaben und Hinweise für die Durchführung eines Cyber-Sicherheits-Checks und die Berichtserstellung enthält. Ein besonders interessanter Mehrwert ist die Zuordnung der zu beurteilenden Maßnahmenziele zu den bekannten Standards der Informationssicherheit (IT-Grundschutz, ISO 27001, COBIT, PCI DSS).

10.1.4 Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz

Eine Zertifizierung ist eine Methode, um die Erreichung der Sicherheitsziele und die Umsetzung der Sicherheitsmaßnahmen durch qualifizierte unabhängige Stellen zu überprüfen. Durch eine Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz erhält eine Institution nachvollziehbare, wiederholbare und vergleichbare Auditergebnisse.

10.2 Eignung der Informationssicherheitsstrategie

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

Aktualität von Sicherheitszielen, Rahmenbedingungen und Sicherheitskonzeption

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

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

Wirtschaftlichkeitsbetrachtung

Unter konstanter Beobachtung sollte die Wirtschaftlichkeit der Sicherheitsstrategie und die spezifischen Sicherheitsmaßnahmen stehen. Es ist zu prüfen, ob die tatsächlich angefallenen Kosten den ursprünglich geplanten Kosten entsprechen oder ob alternativ andere, ressourcenschonendere Sicherheitsmaßnahmen eingesetzt werden können. Ebenso ist es wichtig, regelmäßig den Nutzen der vorhandenen Sicherheitsmaßnahmen herauszuarbeiten.

Rückmeldungen von Internen und Externen

Rückmeldungen über Fehler und Schwachstellen in den Prozessen kommen im Allgemeinen nicht nur von der Informationssicherheitsorganisation oder der Revision, sondern auch von Mitarbeitern, Geschäftspartnern, Kunden oder Partnern. Die Institution muss daher eine wirksame Vorgehensweise festlegen, um mit Beschwerden und anderen Rückmeldungen von Internen und Externen umzugehen. Beschwerden von Kunden oder Mitarbeitern können dabei auch ein Indikator für Unzufriedenheit sein. Es sollte möglichst bereits entstehender Unzufriedenheit entgegengewirkt werden, da bei zufriedenen Mitarbeitern die Gefahr von fahrlässigen oder vorsätzlichen Handlungen, die den Betrieb stören können, geringer ist.

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

Fortentwicklung des ISMS

Auch das ISMS muss kontinuierlich weiterentwickelt werden und an neue Erkenntnisse, die sich beispielsweise aus der Überprüfung des Informationssicherheitsprozesses ergeben haben können, angepasst werden.

Erweiterung der gewählten Vorgehensweise

Bei Einstieg in den Sicherheitsprozess hat die Leitung der Institution sich für eine Vorgehensweise entschieden, um auf Basis von IT-Grundschutz oder auch anderen Methoden ein bestimmtes Sicherheitsniveau für einen definierten Geltungsbereich zu erreichen. Wenn diese Vorgehensweise umgesetzt und die Phase der Aufrechterhaltung und kontinuierlichen Verbesserung der Informationssicherheit erreicht wurde, muss überlegt werden, ob

- die gewählte Vorgehensweise ergänzt werden soll (beispielsweise von Basis- auf Standard-Absicherung) und/oder

- der Geltungsbereich erweitert werden soll (beispielsweise von Kern-Absicherung eines eingegrenzten Bereiches auf einen größeren Informationsverbund).

Ziel sollte es sein, langfristig alle Bereiche der Institution auf ein ganzheitliches Sicherheitsniveau zu heben, das mindestens Standard-Absicherung umfasst.

10.3 Übernahme der Ergebnisse in den Informationssicherheitsprozess

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

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

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

Aktionspunkte zu 10 Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit

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

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

Um die erfolgreiche Umsetzung von IT-Grundschutz nach außen transparent machen zu können, kann sich das Unternehmen oder die Behörde nach ISO/IEC 27001 zertifizieren lassen. Das BSI hat ein Zertifizierungsschema für Informationssicherheit entwickelt, das die Anforderungen an Managementsysteme für die Informationssicherheit aus ISO/IEC 27001 berücksichtigt und als Prüfkataloge das IT-Grundschutz-Kompendium sowie die BSI-Standards 200-x zugrunde legt. Dies wird deshalb als ISO 27001-Zertifizierung auf Basis IT-Grundschutz bezeichnet. Eine solche Zertifizierung ist für die Standard-Absicherung vorgesehen sowie für die Kern-Absicherung grundsätzlich möglich. Bei einer reinen Basis-Absicherung reichen die umgesetzten Sicherheitsmaßnahmen für eine Zertifizierung nicht aus, können aber als Einstieg für eine der anderen beiden Vorgehensweisen dienen.

Das ISO 27001-Zertifikat auf der Basis von IT-Grundschutz bietet Unternehmen und Behörden die Möglichkeit, ihre Bemühungen um Informationssicherheit transparent zu machen. Dies kann sowohl gegenüber Kunden als auch gegenüber Geschäftspartnern als Qualitätsmerkmal dienen und somit zu einem Wettbewerbsvorteil führen.

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

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

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

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

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

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

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

Aktionspunkte zu 11 Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz

- Informationen zum Schema für die ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz lesen
- Prüfen, ob die Bemühungen um Informationssicherheit anhand eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz transparent gemacht werden sollen
- Gegebenenfalls prüfen, ob das Informationssicherheitsmanagement und der Sicherheitszustand die entsprechenden Voraussetzungen erfüllen
- Gegebenenfalls den Zertifizierungsprozess initiieren

12 Anhang

12.1 Erläuterungen zu den Schadensszenarien

Im Folgenden sind für die in Kapitel 8.2.1 definierten Schadensszenarien beispielhafte Fragestellungen aufgeführt. Diese Fragen sollen als Hilfsmittel für die Schutzbedarfsfeststellung dienen, vor allem im Bereich der Anwendungen. Anhand der individuellen Anforderungen sollten die Fragen angepasst und ergänzt werden.

Schadensszenario "Verstoß gegen Gesetze/Vorschriften/Verträge"

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

Beispiele für relevante Gesetze sind (in Deutschland):

> Grundgesetz, Bürgerliches Gesetzbuch, Strafgesetzbuch, Bundesdatenschutzgesetz und Datenschutzgesetze der Länder, EU-Datenschutzgrundverordnung (DSGVO [DSGVO]), 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 Informationen?
- 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 Informationen?
- In welchem Maße wird durch einen Verlust der Integrität gegen Gesetze bzw. Vorschriften verstoßen?

Verlust der Verfügbarkeit

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

Schadensszenario "Beeinträchtigung des informationellen Selbstbestimmungsrechts"

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

Beispiele für die Beeinträchtigung des informationellen Selbstbestimmungsrechts sind:

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

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

Fragen:

Verlust der Vertraulichkeit

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

Verlust der Integrität

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

Verlust der Verfügbarkeit

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

Schadensszenario "Beeinträchtigung der persönlichen Unversehrtheit"

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

Beispiele für solche Anwendungen und IT-Systeme sind:

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

Fragen:

Verlust der Vertraulichkeit

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

Verlust der Integrität

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

Verlust der Verfügbarkeit

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

Schadensszenario "Beeinträchtigung der Aufgabenerfüllung"

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

Beispiele hierfür sind:

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

Fragen:

Verlust der Vertraulichkeit

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

Verlust der Integrität

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

Verlust der Verfügbarkeit

- Gibt es Informationen, bei denen eine Einschränkung der Verfügbarkeit schwerwiegende Auswirkungen auf die Institution oder deren Geschäftsprozesse hätte?
- Kann durch den Ausfall von Anwendungen die Aufgabenerfüllung der Institution so stark beeinträchtigt werden, dass die Wartezeiten für die Betroffenen nicht mehr tolerabel sind?
- Sind von dem Ausfall dieser Anwendung andere Anwendungen betroffen?

- Ist es für die Institution bedeutsam, dass der Zugriff auf Anwendungen nebst Programmen und Daten ständig gewährleistet ist?

Schadensszenario "Negative Innen- oder Außenwirkung"

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

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

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

Die Ursachen für solche Schäden können vielfältiger Natur sein:

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

Fragen:

Verlust der Vertraulichkeit

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

Verlust der Integrität

- Welche Schäden können sich durch die Verarbeitung, Verbreitung oder Übermittlung falscher oder unvollständiger Informationen ergeben?

- Wird die Verfälschung von Informationen öffentlich bekannt?
- Entstehen bei einer Veröffentlichung von verfälschten Informationen Ansehensverluste?
- Können Veröffentlichungen von verfälschten Informationen zur politischen oder gesellschaftlichen Verunsicherung führen?
- Können verfälschte Informationen zu einer verminderten Produktqualität und damit zu einem Ansehensverlust führen?

Verlust der Verfügbarkeit

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

Schadensszenario "Finanzielle Auswirkungen"

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

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

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

Fragen:

Verlust der Vertraulichkeit

- Kann die Veröffentlichung vertraulicher Informationen Regressforderungen nach sich ziehen?
- Gibt es innerhalb von Geschäftsprozessen oder Anwendungen Informationen, aus deren Kenntnis ein Dritter (z. B. Konkurrenzunternehmen) finanzielle Vorteile ziehen kann?
- Werden mit Anwendungen Forschungsdaten gespeichert, die einen erheblichen Wert darstellen? Was passiert, wenn sie unerlaubt kopiert und weitergegeben werden?
- Können durch vorzeitige Veröffentlichung von schutzbedürftigen Informationen 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 Informationen zu falschen Geschäftsentscheidungen führen?

Verlust der Verfügbarkeit

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

12.2 Literaturverzeichnis

[27000] ISO/IEC 27000:2016, International Organization for Standardization (Hrsg.), Information technology - Security techniques – Information Security management systems – Overview and vocabulary, ISO/IEC JTC 1/SC 27, 2016

[27001] ISO/IEC 27001:2013, International Organization for Standardization (Hrsg.), Information technology – Security techniques – Information security management systems – Requirements, ISO/IEC JTC 1/SC 27, 2013

[27002] ISO/IEC 27002:2013, International Organization for Standardization (Hrsg.), Information technology – Security techniques – Code of practice for information security controls, ISO/IEC JTC 1/SC 27, 2013

[27004] ISO/IEC 27004:2016, International Organization for Standardization (Hrsg.), Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation, ISO/IEC JTC 1/SC 27, 2016

[27005] ISO/IEC 27005:2011, International Organization for Standardization (Hrsg.), Information technology – Security techniques – Information security risk management, ISO/IEC JTC 1/SC 27, 2011

[820-2] DIN 820-2:2012, Anhang H, Gestaltung von Dokumenten – Verbformen zur Formulierung von Festlegungen, NA 173-00-02 AA, 2012

[BSI1] Managementsysteme für Informationssicherheit (ISMS), BSI-Standard 200-1, Version 1.0, Oktober 2017, https://www.bsi.bund.de/grundschutz

[BSI3] Risikoanalyse auf der Basis von IT-Grundschutz, BSI-Standard 200-3, Version 1.0, Oktober 2017, https://www.bsi.bund.de/grundschutz

[BSIR] Informationssicherheitsrevision – Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz, BSI, Version 2.0, März 2010, https://www.bsi.bund.de/is-revision

[CSC] Leitfaden Cyber-Sicherheits-Check, BSI, ISACA, 07.03.2014, https://www.allianz-fuer-cybersicherheit.de

[DSGVO] Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Europäisches Parlament und der Rat der Europäischen Union, 27. April 2016

[GSK] IT-Grundschutz-Kompendium, BSI, jährlich neu, https://www.bsi.bund.de/grundschutz

[ISF] The Standard of Good Practice 2016, ISF – Information Security Forum, 2016, https://www.securityforum.org/tool/the-isf-standardrmation-security

[NIST53] NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, NIST, 2015, http://csrc.nist.gov/publications/PubsSPs.html

[RFC2119] RFC 2119 (Key words for use in RFCs to Indicate Requirement Levels), Network Working Group, Stand 1997, https://www.ietf.org/rfc/rfc2119.txt

[SDM] Standard-Datenschutzmodell (SDM), SDM-Methodik-Handbuch, Konferenz der Datenschutzbeauftragten des Bundes und der Länder, V1.0, kann von allen Webservern der deutschen Datenschutz-Aufsichtsbehörden heruntergeladen werden, z. B. https://www.datenschutz-mv.de/datenschutz/sdm/sdm.html

[ZERT] Informationen zur Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz, BSI, https://www.bsi.bund.de/iso27001-zertifikate