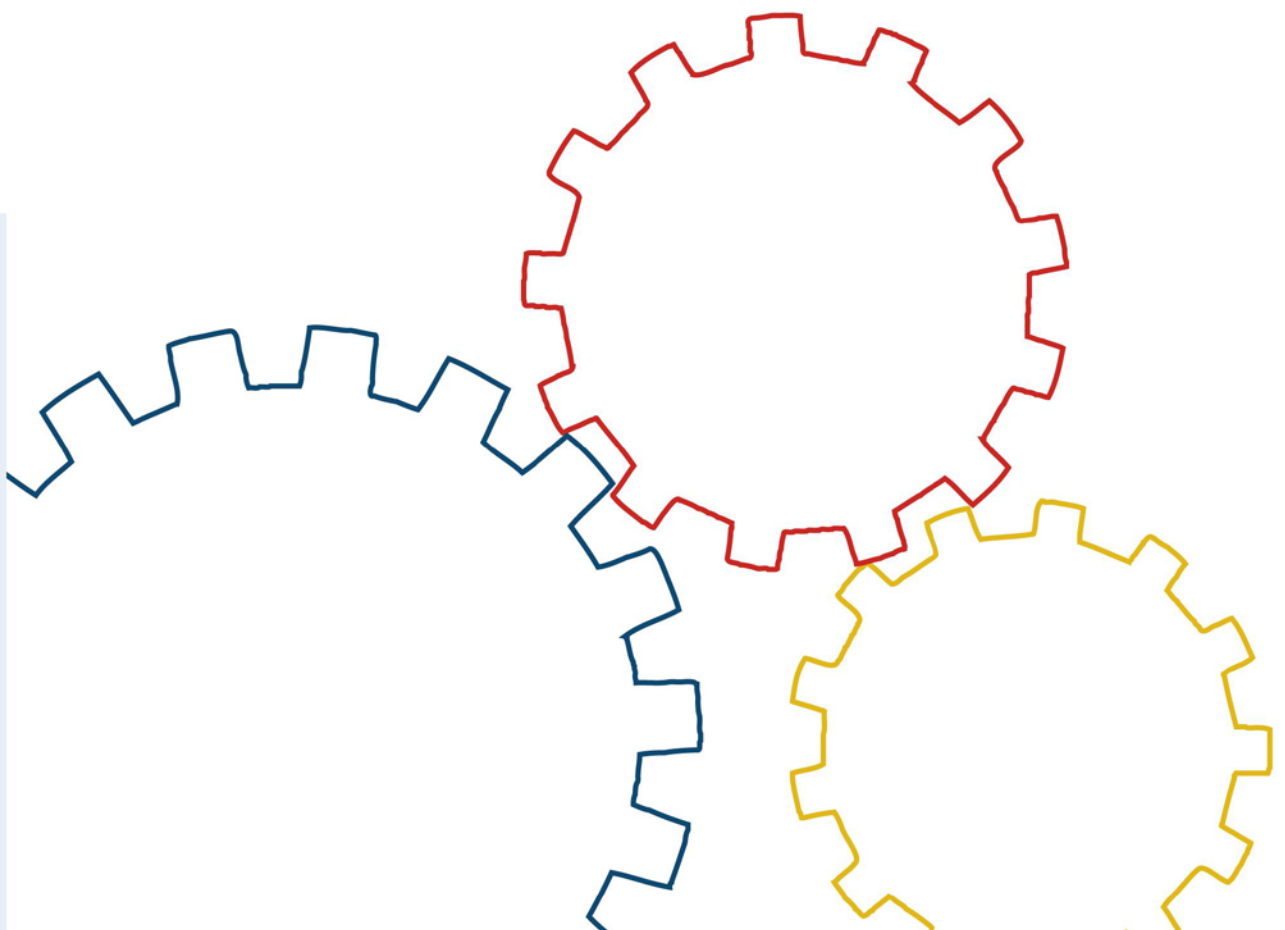




Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Standard 200-1

Managementsysteme für Informationssicherheit (ISMS)



Inhaltsverzeichnis

BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS)

1	Einleitung	
1.1	Versionshistorie	5
1.2	Zielsetzung	5
1.3	Adressatenkreis	6
1.4	Anwendungsweise	7
2	Einführung in die Informationssicherheit	
2.1	Überblick über Normen und Standards zur Informationssicherheit	8
2.1.1	ISO-Normen zur Informationssicherheit	9
2.1.2	Ausgewählte BSI-Publikationen und Standards zur Informationssicherheit	10
2.1.3	Weitere Sicherheitsstandards	12
3	ISMS-Definition und Prozessbeschreibung	15
3.1	Komponenten eines Managementsystems für Informationssicherheit	15
3.2	Prozessbeschreibung und Lebenszyklus-Modell	17
3.2.1	Der Lebenszyklus in der Informationssicherheit	17
3.2.2	Beschreibung des Prozesses Informationssicherheit	18
4	Management-Prinzipien	20
4.1	Aufgaben und Pflichten des Managements	20
4.2	Kommunikation und Wissen	22
4.3	Erfolgskontrolle im Sicherheitsprozess	24
4.4	Kontinuierliche Verbesserung des Sicherheitsprozesses	25
5	Ressourcen für Informationssicherheit	26
6	Einbindung der Mitarbeiter in den Sicherheitsprozess	27
7	Der Sicherheitsprozess	28
7.1	Planung des Sicherheitsprozesses	28
7.2	Aufbau einer Sicherheitsorganisation [DOK]	30
7.3	Umsetzung der Leitlinie zur Informationssicherheit	30
7.4	Aufrechterhaltung der Informationssicherheit	30
7.5	Kontinuierliche Verbesserung der Informationssicherheit	31
8	Sicherheitskonzept	32
8.1	Erstellung des Sicherheitskonzepts	32
8.2	Umsetzung des Sicherheitskonzepts	36
8.3	Erfolgskontrolle des Sicherheitskonzepts	36
8.4	Kontinuierliche Verbesserung des Sicherheitskonzepts	38
9	Zertifizierung des ISMS	39
10	Das ISMS auf Basis von BSI IT-Grundschutz	40
10.1	IT-Grundschutz-Methodik	40

10.2	Der Sicherheitsprozess nach IT-Grundschutz	40
10.2.1	Integrierte Risikobewertung im IT-Grundschutz.	41
10.2.2	Sicherheitskonzeption	43
11	Anhang	47
11.1	Literaturverzeichnis	47

1 Einleitung

1.1 Versionshistorie

Der BSI-Standard 200-1 löst den BSI-Standard 100-1 ab.

Stand	Version	Änderungen
April 2017	CD 1.0	Aktualisierung basierend auf BSI-Standard 100-1 <ul style="list-style-type: none"> • Anpassungen an Fortschreibung der ISO-Normen • Anpassungen an BSI-Standard 200-2 (IT-Grundschutz-Methodik)
Oktober 2017	V 1.0	Anwenderkommentare eingearbeitet <ul style="list-style-type: none"> • im Wesentlichen sprachliche Präzisierungen • Unterscheidung zwischen Norm und Standard

1.2 Zielsetzung

Die zunehmende Digitalisierung und Vernetzung der Arbeitswelt stellt Unternehmen und Behörden heute vor grundlegende Herausforderungen. Zugleich gestaltet sich die Bedrohungslage für die Informationssicherheit in Unternehmen und Behörden sehr dynamisch und vielfältig. Um Geschäftsprozesse oder Fachaufgaben mittels IT, offline oder online, sicher betreiben zu können und damit auch langfristig wettbewerbsfähig zu sein, müssen Institutionen sich zunehmend besser hinsichtlich Fragen der Informationssicherheit aufstellen. Die Entwicklungen in der Informationstechnik erfolgen heute in immer kürzer werdenden Innovationszyklen. Zugleich zeichnen sich die technischen Systeme durch eine steigende Komplexität aus. In immer mehr Bereichen des öffentlichen sowie des Geschäftslebens wächst die Abhängigkeit von funktionierender Technik. Die Vernetzung und Steuerung von Industrieanlagen, Smart Home, Internet of Things und Connected Cars werden Sicherheitsexperten und Anwender in den kommenden Jahren vor weitere Herausforderungen stellen. Die Leitung von Institutionen muss sich inzwischen zunehmend mit der Frage befassen, welche Auswirkungen z. B. ein Cyber-Angriff mit sich bringen kann. Neben der eigenen Institution können auch Kunden, Lieferanten und Geschäftspartner sowie weitere Gruppen betroffen sein. Daher ist ein geplantes und organisiertes Vorgehen aller Beteiligten notwendig, um ein angemessenes und ausreichendes Sicherheitsniveau aufzubauen, aufrechtzuerhalten sowie kontinuierlich verbessern zu können.

In der Praxis erweist es sich oft als schwierig, ein angemessenes und ausreichendes Sicherheitsniveau aufzubauen sowie langfristig aufrechtzuerhalten. Fehlende Ressourcen und knappe Budgets stellen verbunden mit der zunehmenden Komplexität der IT-Systeme die Verantwortlichen ständig vor neue Herausforderungen. Aufgrund der kürzer werdenden Entwicklungszyklen müssen auch bewährte Sicherheitsmechanismen stetig angepasst oder sogar neu konzipiert werden. Eine statische Lösung kann auf lange Sicht kein angemessenes Sicherheitsniveau gewährleisten. Die verbreitete Ansicht, Sicherheitsmaßnahmen seien zwangsläufig mit hohen Investitionen in Sicherheitstechnik und hochspezialisierte Sicherheitsexperten verbunden, ist jedoch falsch. Zu den wichtigsten Erfolgsfaktoren zählen ein gesunder Menschenverstand, durchdachte organisatorische Regelungen und zuverlässige, gut informierte Mitarbeiter, die selbstständig und routiniert Sicherheitserfordernisse umsetzen. Die Erstellung und Umsetzung eines wirksamen Sicherheitskonzepts muss deshalb jedoch nicht zwangs-

läufig unbezahlbar sein und die wirksamsten Maßnahmen können sich als überraschend einfach erweisen.

Sicherheit muss daher ein integraler Bestandteil von Planung, Konzeption und Betrieb von Geschäftsprozessen und der Informationsverarbeitung sein. Daher müssen auch umfangreiche organisatorische und personelle Maßnahmen getroffen werden. Ein Informationssicherheitsmanagement auf der Basis von IT-Grundschutz enthält neben technischen auch infrastrukturelle, organisatorische und personelle Aspekte: Nur ein ganzheitlicher Ansatz zur Erhöhung der Informationssicherheit kann eine nachhaltige Wirkung auf allen Ebenen erzielen.

Ein angemessenes Sicherheitsniveau ist in erster Linie abhängig vom systematischen Vorgehen und erst in zweiter Linie von einzelnen technischen Maßnahmen. Die folgenden Überlegungen verdeutlichen diese These und die Bedeutung der Leitungsebene im Sicherheitsprozess:

- Die Leitungsebene trägt die Verantwortung dafür, dass gesetzliche Regelungen und Verträge mit Dritten eingehalten werden und dass wichtige Geschäftsprozesse störungsfrei ablaufen.
- Die Leitungsebene ist diejenige Instanz, die über den Umgang mit Risiken entscheidet.
- Informationssicherheit hat Schnittstellen zu vielen Bereichen einer Institution und betrifft wesentliche Geschäftsprozesse und Aufgaben. Nur die Leitungsebene kann daher für eine reibungslose Integration des Informationssicherheitsmanagements in bestehende Organisationsstrukturen und Prozesse sorgen.
- Die Leitungsebene ist zudem für den wirtschaftlichen Einsatz von Ressourcen verantwortlich.

Der Leitungsebene kommt daher eine hohe Verantwortung für die Informationssicherheit zu. Fehlende Steuerung, eine ungeeignete Sicherheitsstrategie oder falsche Entscheidungen können sowohl durch Sicherheitsvorfälle als auch durch verpasste Chancen und Fehlinvestitionen weitreichende negative Auswirkungen haben. Eine intensive Beteiligung der Führungsebene ist somit unerlässlich: Informationssicherheit ist Chefsache!

Dieser Standard beschreibt daher im Folgenden Schritt für Schritt, wie ein erfolgreiches Informationssicherheitsmanagement aufgebaut sein kann und welche Aufgaben der Leitungsebene in Behörden und Unternehmen dabei zufallen.

1.3 Adressatenkreis

Dieser BSI-Standard 200-1 richtet sich primär an Verantwortliche für die Informationssicherheit, Sicherheitsbeauftragte, -experten, -berater und alle Interessierten, die mit dem Management von Informationssicherheit betraut sind. Er ist zugleich eine sinnvolle Grundlage für die Verantwortlichen für IT und Industrial Control Systems (ICS), Führungskräfte und Projektmanager, die dafür Sorge tragen, dass Aspekte des Informationssicherheitsmanagements in ihrer Institution bzw. in ihren Projekten ausreichend berücksichtigt werden.

Die Informationssicherheit effizient zu managen, ist nicht nur für große Institutionen, sondern auch für kleine und mittlere Behörden und Unternehmen sowie Selbstständige ein wichtiges Thema. Wie ein geeignetes Managementsystem für Informationssicherheit aussieht, hängt von der Größe der Institution ab. Dieser Standard mit den praxisorientierten Empfehlungen des IT-Grundschutzes hilft Verantwortlichen, die die Informationssicherheit in ihrem jeweiligen Einflussbereich verbessern möchten. Im Folgenden werden immer wieder Hinweise gegeben, wie die Empfehlungen dieses Standards je nach Größe einer Institution bedarfsgerecht angepasst werden können.

1.4 Anwendungsweise

Der vorliegende Standard beschreibt, wie ein Informationssicherheitsmanagementsystem (ISMS) aufgebaut werden kann. Ein Managementsystem umfasst alle Regelungen, die für die Steuerung und Lenkung der Institution sorgen und somit zur Zielerreichung beitragen. Ein Managementsystem für Informationssicherheit legt somit fest, mit welchen Instrumenten und Methoden die Leitungsebene einer Institution die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenken kann.

Dieser BSI-Standard beantwortet unter anderem folgende Fragen:

- Was sind die Erfolgsfaktoren beim Management von Informationssicherheit?
- Wie kann der Sicherheitsprozess vom verantwortlichen Management gesteuert und überwacht werden?
- Wie werden Sicherheitsziele und eine angemessene Sicherheitsstrategie entwickelt?
- Wie werden Sicherheitsmaßnahmen ausgewählt und Sicherheitskonzepte erstellt?
- Wie kann ein einmal erreichtes Sicherheitsniveau dauerhaft erhalten und verbessert werden?

Dieser Management-Standard stellt übersichtlich die wichtigsten Aufgaben des Sicherheitsmanagements dar. Bei der Umsetzung dieser Empfehlungen hilft das BSI mit der Methodik des IT-Grundschutzes. Der IT-Grundschutz gibt für Institutionen verschiedener Größen und Arten Schritt-für-Schritt-Anleitungen für die Entwicklung eines Informationssicherheitsmanagements in der Praxis und nennt konkrete Maßnahmen für alle Aspekte der Informationssicherheit. Die Methodik des IT-Grundschutzes wird im BSI-Standard 200-2 (siehe [BSI2]) beschrieben und ist so gestaltet, dass ein sowohl im Hinblick auf die Bedrohungslage als auch die Geschäftsziele angemessenes Sicherheitsniveau erreicht werden kann. Ergänzend dazu werden im IT-Grundschutz-Kompendium Anforderungen für die praktische Implementierung des angemessenen Sicherheitsniveaus formuliert.

Wenn in diesem Standard der Begriff „IT-System“ verwendet wird, sind damit nicht nur „klassische“ IT-Systeme, wie zum Beispiel Server, Arbeitsplatzrechner, Smartphones oder Netzkomponenten, gemeint. Der Begriff „IT-Systeme“ schließt hier auch Industrial Control Systems (ICS) ebenso wie Komponenten aus dem Bereich Internet of Things (IoT) mit ein.

2 Einführung in die Informationssicherheit

Was ist Informationssicherheit?

Informationssicherheit hat das Ziel, Informationen jeglicher Art und Herkunft zu schützen. Dabei können Informationen auf Papier, in IT-Systemen oder auch in den Köpfen der Benutzer gespeichert sein. IT-Sicherheit als Teilmenge der Informationssicherheit konzentriert sich auf den Schutz elektronisch gespeicherter Informationen und deren Verarbeitung.

Die klassischen Grundwerte der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit. Viele Anwender beziehen in ihre Betrachtungen weitere Grundwerte ein. Dies kann je nach den individuellen Anwendungsfällen auch sehr hilfreich sein. Weitere generische Oberbegriffe der Informationssicherheit sind beispielsweise Authentizität, Verbindlichkeit, Zuverlässigkeit, Resilienz und Nichtabstreitbarkeit.

Die Sicherheit von Informationen wird nicht nur durch vorsätzliche Handlungen bedroht (z. B. Schadsoftware, Abhören der Kommunikation, Diebstahl von Rechnern). Die folgenden Beispiele verdeutlichen dies:

- Durch höhere Gewalt (z. B. Feuer, Wasser, Sturm, Erdbeben) werden Datenträger und IT-Systeme in Mitleidenschaft gezogen oder der Zugang zum Rechenzentrum versperrt. Dokumente, IT-Systeme oder Dienste stehen nicht mehr wie gewünscht zur Verfügung.
- Nach einem missglückten Software-Update funktionieren Anwendungen nicht mehr oder Daten werden unbemerkt verändert.
- Ein wichtiger Geschäftsprozess verzögert sich, weil die einzigen Mitarbeiter, die mit der Anwendungssoftware vertraut sind, erkrankt sind.
- Vertrauliche Informationen werden versehentlich von einem Mitarbeiter an Unbefugte weitergegeben, weil Dokumente oder Dateien nicht als „vertraulich“ gekennzeichnet waren.

Wortwahl: IT-Sicherheit versus Informationssicherheit und Cyber-Sicherheit

Da die elektronische Verarbeitung von Informationen in nahezu allen Lebensbereichen allgegenwärtig ist, scheint die Unterscheidung, ob Informationen mit Informationstechnik, mit Kommunikationstechnik oder auf Papier verarbeitet werden, nicht mehr zeitgemäß. Der Begriff der Informationssicherheit statt IT-Sicherheit ist daher umfassender und besser geeignet. Es sollte jedoch beachtet werden, dass in der (Forschungs-)Literatur oftmals noch der Begriff „IT-Sicherheit“ verwendet wird (unter anderem, weil dieser kürzer ist), auch wenn häufig „Informationssicherheit“ gemeint ist. Das Aktionsfeld der klassischen IT-Sicherheit wird unter dem Begriff „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.

2.1 Überblick über Normen und Standards zur Informationssicherheit

Im Bereich der Informationssicherheit haben sich verschiedene Normen und Standards entwickelt, bei denen teilweise andere Zielgruppen oder Themenbereiche im Vordergrund stehen. Der Einsatz von Sicherheitsnormen und -standards in Unternehmen oder Behörden verbessert nicht nur das Sicherheitsniveau, er erleichtert auch die Abstimmung zwischen verschiedenen Institutionen darüber, wel-

che Sicherheitsmaßnahmen in welcher Form umzusetzen sind. Der folgende Überblick zeigt die Ausrichtungen der wichtigsten Normen und Standards.

2.1.1 ISO-Normen zur Informationssicherheit

Innerhalb der internationalen Normungsorganisationen ISO und IEC werden die Normen zur Informationssicherheit in der 2700x-Reihe zusammengeführt, die stetig wächst. International werden diese Normen als Standards bezeichnet. Ein Teil dieser internationalen Standards liegt auch in Übersetzungen als DIN-Normen vor.

Die wesentlichen Normen der ISO-/IEC-2700x-Reihe sind:

ISO/IEC 27000 (*Information security management systems – Overview and vocabulary*)

Diese Norm gibt einen Überblick über Managementsysteme für Informationssicherheit (ISMS) und über die Zusammenhänge der verschiedenen Normen der ISO-/IEC-2700x-Familie. Hier finden sich außerdem die grundlegenden Begriffe und Definitionen für ISMS.

ISO/IEC 27001 (*Information security management systems – Requirements*)

Die ISO-Norm 27001 ist eine internationale Norm zum Management von Informationssicherheit, die auch eine Zertifizierung ermöglicht. ISO/IEC 27001 gibt auf ca. neun Seiten normative Vorgaben zur Einführung, dem Betrieb und der Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems. In einem normativen Anhang werden mehr als 100 Maßnahmen (Controls) aufgeführt, die unter Berücksichtigung der relevanten Risiken ausgewählt werden sollten. Die Leser erhalten allerdings keine Hilfe im Hinblick auf die Umsetzung in der Praxis.

Bisher orientierten sich die Anforderungen der ISO/IEC 27001 an einem Lebenszyklusmodell, das nach der englischen Benennung der einzelnen Phasen („Plan“, „Do“, „Check“, „Act“) auch als PDCA-Zyklus bezeichnet wird. Um mit dem Annex SL (Leitfaden für die Entwicklung und Überarbeitung von ISO-Normen für Managementsysteme) kompatibel zu sein, ist bei der Überarbeitung der ISO/IEC 27001 auf eine explizite Nennung des PDCA-Zyklus verzichtet worden. Dadurch soll deutlich gemacht werden, dass die Reihenfolge der einzelnen Anforderungen in der Norm keinen Rückschluss auf deren jeweilige Wichtigkeit oder die Reihenfolge ihrer Umsetzung gibt. Alle Aktivitäten zum Aufbau und Betrieb eines ISMS lassen sich jedoch weiterhin nach dem PDCA-Zyklus durchführen.

ISO/IEC 27002 (*Code of practice for information security controls*)

Diese Norm unterstützt bei der Auswahl und Umsetzung der in der ISO/IEC 27001 beschriebenen Maßnahmen, um ein funktionierendes Sicherheitsmanagement aufzubauen und in der Institution zu verankern. Die dafür geeigneten Sicherheitsmaßnahmen werden auf den 90 Seiten der Norm ISO/IEC 27002 beschrieben. Die Empfehlungen sind in erster Linie für die Management-Ebene gedacht und enthalten daher kaum konkrete technische Hinweise. Die Umsetzung der Sicherheitsempfehlungen der ISO/IEC 27002 ist eine von vielen Möglichkeiten, die Anforderungen der ISO-Norm 27001 zu erfüllen.

ISO/IEC 27004 (*Monitoring, measurement, analysis and evaluation*)

Die ISO-Norm 27004 behandelt die Bewertung der Umsetzung und der Wirksamkeit eines ISMS anhand verschiedener Kenngrößen.

ISO/IEC 27005 (*Information security risk management*)

Diese Norm enthält Rahmenempfehlungen zum Risikomanagement für Informationssicherheit. Unter anderem unterstützt sie bei der Umsetzung der Anforderungen aus ISO/IEC 27001. Hierbei wird allerdings keine spezifische Methode für das Risikomanagement vorgegeben. Diese Norm basiert wiederum wesentlich auf der Norm ISO/IEC 31000 *Risk management – Principles and guidelines on im-*

plementation (siehe [31000]). In der unterstützenden Norm ISO/IEC 31010 *Risk assessment techniques* (siehe [31010]) wird beschrieben, wie die Risikobeurteilung in ein Risikomanagementsystem integriert werden kann und wie Risiken identifiziert, eingeschätzt, bewertet und behandelt werden können. Der Anhang B von ISO 31010 gibt einen ausführlichen Überblick über Methoden zur Risikobeurteilung; hier werden insgesamt 31 verschiedene Methoden aufgeführt.

ISO/IEC 27006 (*Requirements for bodies providing audit and certification of information security management systems*)

Die ISO-Norm 27006 spezifiziert Anforderungen an die Akkreditierung von Zertifizierungsstellen für ISMS und behandelt auch Spezifika der ISMS-Zertifizierungsprozesse.

ISO/IEC 27009 (*Sector-specific application of ISO/IEC 27001 – Requirements*)

Die ISO-Norm 27009 beschreibt, wie sektorspezifische Erweiterungen (z. B. aus den Bereichen Energie, Cloud Computing, Finanzen) zukünftig in ein ISMS nach ISO/IEC 27001 einfließen und dort als Anforderungen berücksichtigt werden können. Dazu sollen einzelne Maßnahmen aus dem Anhang der ISO/IEC 27001 erweitert bzw. ergänzt werden.

Sektorspezifische Normen (*ISO/IEC 27010 bis ISO/IEC 27019*)

Viele sektorspezifische Normen (z. B. ISO/IEC 27019 für den Energiesektor) werden basierend auf der ISO/IEC 27009 entwickelt.

Weitere Normen der ISO-2700x-Reihe

Die Normenreihe ISO 2700 x wird voraussichtlich langfristig aus den ISO-Normen 27000 bis 271xx bestehen. Alle Normen dieser Reihe behandeln verschiedene Aspekte des Sicherheitsmanagements und beziehen sich auf die Anforderungen der ISO/IEC 27001. Die weiteren Normen sollen zum besseren Verständnis und zur praktischen Anwendbarkeit der ISO/IEC 27001 beitragen. Diese beschäftigen sich beispielsweise mit der Umsetzung der ISO/IEC 27001 in der Praxis und mit Methoden zur Kontinuität von Geschäftsprozessen.

2.1.2 Ausgewählte BSI-Publikationen und Standards zur Informationssicherheit

IT-Grundschutz

Die Methodik des BSI zur Informationssicherheit ist seit 1994 der IT-Grundschutz. Der IT-Grundschutz ist eine ganzheitliche Vorgehensweise, um für Institutionen aller Arten und Größen eine angemessene Informationssicherheit umzusetzen. Mit der Kombination aus den IT-Grundschutz-Vorgehensweisen zur Basis-, Standard- und Kern-Absicherung, die im BSI-Standard 200-2 *IT-Grundschutz-Methodik* beschrieben sind, und dem IT-Grundschutz-Kompendium, in dem für die verschiedensten Einsatzumgebungen Sicherheitsanforderungen enthalten sind, bietet der IT-Grundschutz ein effizientes und effektives Handwerkszeug, um adäquate Maßnahmen zum sicheren Umgang mit Informationen für eine Institution auszuwählen und anzupassen. Der IT-Grundschutz ist von Anfang an darauf ausgelegt worden, dass er von den Anwendern modular an verschiedene Einsatzumgebungen angepasst werden kann. Dazu wird er vom BSI auch kontinuierlich aktualisiert und erweitert.

Politische Rahmenbedingungen wie das IT-Sicherheitsgesetz, das sehr dynamische Themengebiet der Informationssicherheit sowie die zunehmend professionelleren Cyberangriffe haben den Ausschlag dafür gegeben, den IT-Grundschutz erneut grundlegend zu modernisieren. Mit den vorliegenden BSI-Standards 200-1 bis 200-3 sind hieraus weitere Vorgehensweisen hervorgegangen, die einen abgestuften Einstieg in ein Sicherheitsmanagement ermöglichen. Ergänzt werden diese durch IT-Grundschutz-Bausteine, die im IT-Grundschutz-Kompendium zusammengefasst sind. Die Abbildung 1 veranschaulicht die Gliederung der IT-Grundschutz-Dokumente.

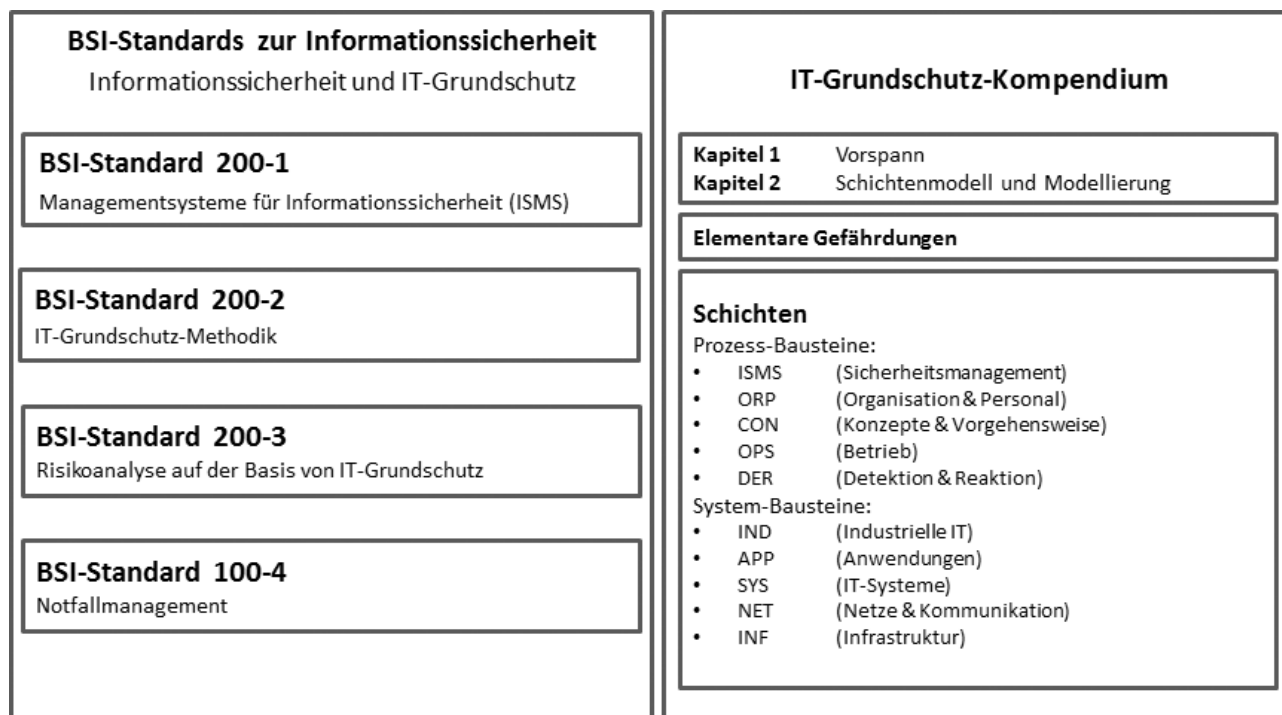


Abbildung 1: Übersicht über BSI-Publikationen zum Sicherheitsmanagement

Das IT-Grundschutz-Kompendium ist modular aufgebaut und enthält Prozess- und Systembausteine für typische Geschäftsprozesse, Anwendungen, Systeme, Kommunikationsverbindungen und Räume. Die auf die Rahmenbedingungen der eigenen Institution zutreffenden Bausteine können nach Bedarf eingesetzt werden. Im IT-Grundschutz werden alle Bereiche betrachtet, die in Institutionen vorzufinden sind. Dazu gehören neben Organisation und Personal auch IT-Betrieb, aber auch Produktion und Fertigung mit Industrial Control Systems (ICS) ebenso wie Komponenten aus dem Bereich Internet of Things (IoT).

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 ähnlichen thematischen Bezug haben. Des Weiteren gibt es einen Überblick über die spezifischen Gefährdungen des betrachteten Themengebietes. Die Sicherheitsanforderungen für die Basis-, Standard- und Kern-Absicherung bilden den Schwerpunkt eines jeden Bausteins.

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 und den Best Practices des BSI und von IT-Grundschutz-Anwendern basieren.

Die Bausteine des IT-Grundschutz-Kompendiums und die Umsetzungshinweise werden regelmäßig aktualisiert und erweitert. Daher werden sie als Printversion und zudem auch noch zusätzlich kostenfrei im Internet veröffentlicht.

BSI-Standardreihe zur Informationssicherheit: Thema IS-Management

200-1 Managementsysteme für Informationssicherheit (ISMS)

Der vorliegende Standard definiert allgemeine Anforderungen an ein ISMS. Darin wird beschrieben, mit welchen Methoden Informationssicherheit in einer Institution generell initiiert, gesteuert und überwacht werden kann. Der BSI-Standard 200-1 ist vollständig kompatibel mit der Norm ISO/IEC 27001 und berücksichtigt zudem die in der ISO-Norm ISO/IEC 27000 definierten Begriffe sowie die Empfehlungen der ISO-Norm ISO/IEC 27002. Er bietet den Lesern eine leicht verständliche und systematische Anleitung, unabhängig davon, mit welcher Methode eine Institution die Anforderungen an ein ISMS umsetzen möchte.

Das BSI stellt den Inhalt der oben genannten ISO-Normen in einem eigenen BSI-Standard dar, um einige Themen ausführlicher beschreiben zu können und so eine didaktisch bessere Darstellung der Inhalte zu ermöglichen. Zudem wurde die Gliederung so gestaltet, dass sie mit der IT-Grundschutz-Vorgehensweise kompatibel ist.

200-2 IT-Grundschutz-Methodik

Die IT-Grundschutz-Methodik beschreibt Schritt für Schritt, wie ein Managementsystem für Informationssicherheit in der Praxis aufgebaut und betrieben werden kann. Die Aufgaben des Informationssicherheitsmanagements und der Aufbau einer Organisationsstruktur für Informationssicherheit sind dabei wichtige Themen. Die IT-Grundschutz-Methodik geht sehr ausführlich darauf ein, wie ein Sicherheitskonzept in der Praxis erstellt werden kann, wie angemessene Sicherheitsanforderungen ausgewählt werden können und was bei der Umsetzung des Sicherheitskonzepts zu beachten ist. Auch die Frage, wie die Informationssicherheit im laufenden Betrieb aufrechterhalten und kontinuierlich verbessert werden kann, wird ausführlich beantwortet.

Um einen abgestuften Einstieg in ein Sicherheitsmanagement zu ermöglichen, werden je nach angestrebtem Sicherheitsniveau und zu sichernden Informationen unterschiedliche Vorgehensweisen angeboten. Abhängig davon, welche Ansätze zur Informationssicherheit bereits innerhalb der Institution verfolgt werden, kann es zweckmäßig sein, zunächst von der „vollständigen“ IT-Grundschutz-Vorgehensweise („Standard-Absicherung“) abzuweichen. Beispielsweise kann sich eine Institution als Ziel setzen, zunächst möglichst flächendeckend alle Basis-Anforderungen umzusetzen („Basis-Absicherung“), um schnellstmöglich die größten Risiken zu senken, bevor die tatsächlichen Sicherheitsanforderungen im Detail analysiert werden. Ein anderer denkbarer Ansatz ist, sich zunächst auf den Schutz der essenziellen Werte der Institution zu konzentrieren („Kern-Absicherung“).

Der IT-Grundschutz interpretiert ausgehend vom BSI-Standard 200-2 die allgemein gehaltenen Anforderungen bzw. Sicherheitsmaßnahmen der zuvor genannten ISO-Normen 27001 sowie 27002 und hilft den Anwendern bei der Umsetzung in der Praxis mit ausführlichen Hinweisen, Hintergrundinformationen und Beispielen. Die Bausteine des IT-Grundschutz-Kompendiums erklären, was gemacht werden sollte, die Umsetzungshinweise geben sehr konkrete Hinweise, wie eine Anforderung (auch auf technischer Ebene) erfüllt werden kann. Ein Vorgehen nach IT-Grundschutz ist somit eine erprobte und effiziente Möglichkeit, allen Anforderungen der oben genannten ISO-Normen nachzukommen bzw. gerecht zu werden.

200-3 Risikoanalyse auf der Basis von IT-Grundschutz

Das BSI hat eine Methodik zur Risikoanalyse auf der Basis des IT-Grundschutzes erarbeitet. Der BSI-Standard 200-3 beschreibt, wie aufbauend auf der IT-Grundschutz-Vorgehensweise eine vereinfachte Analyse von Risiken für die Informationsverarbeitung durchgeführt werden kann. Diese basiert auf den elementaren Gefährdungen, die im IT-Grundschutz-Kompendium beschrieben sind und auf deren Basis auch die IT-Grundschutz-Bausteine erstellt werden. Diese

Vorgehensweise bietet sich an, wenn Unternehmen oder Behörden bereits erfolgreich mit dem IT-Grundschutz arbeiten und möglichst nahtlos eine Risikoanalyse an die IT-Grundschutz-Analyse anschließen möchten.

100-4 Notfallmanagement

Im BSI-Standard 100-4 wird eine Methodik zur Etablierung und Aufrechterhaltung eines behörden- bzw. unternehmensweiten Notfallmanagements erläutert. Die hier beschriebene Methodik basiert dabei auf der in BSI-Standard 200-2 beschriebenen IT-Grundschutz-Vorgehensweise „Standard-Absicherung“ und ergänzt diese sinnvoll.

Leitfaden für die IS-Revision auf Basis von IT-Grundschutz

Informationssicherheitsrevision (IS-Revision) ist ein Bestandteil eines jeden erfolgreichen Informationsicherheitsmanagements. Nur durch die regelmäßige Überprüfung der etablierten Sicherheitsmaßnahmen und des Informationssicherheits-Prozesses 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 innerhalb einer Institution. Hierzu hat das BSI mit dem *Leitfaden für die IS-Revision auf Basis von IT-Grundschutz* (siehe [BSIR]) ein Verfahren entwickelt, um den Status der Informationssicherheit in einer Institution festzustellen und Schwachstellen identifizieren zu können.

2.1.3 Weitere Sicherheitsstandards

COBIT 5

COBIT 5 sieht die IT als wesentliche Grundlage einer Institution zur Erreichung der Geschäftsziele und fordert, dass die Ziele aus der Geschäftsstrategie in die Ziele der IT einfließen und die gelieferten Services den Qualitätsanforderungen der Geschäftsprozesse genügen. Ebenso wie ITIL setzt COBIT 5 auf zielgerichtete, optimierte IT-Prozesse. COBIT 5 führt den Aspekt des Prozesspotenzials ein, in dem eine Aussage darüber getroffen wird, inwieweit eine Institution dazu in der Lage ist, die geforderten Ziele verlässlich und nachhaltig zu erreichen. Aus der Gesamtbetrachtung der Reife aller 37 Prozessgebiete, die in fünf Domänen unterteilt sind, kann die Professionalität der unterstützenden IT-Prozesse abgeleitet werden. Die COBIT-Dokumente werden von der Information Systems Audit and Control Association (ISACA) herausgegeben. Bei der Entwicklung von COBIT orientierten sich die Autoren an bestehenden Normen und Standards zum Thema „Sicherheitsmanagement“, insbesondere an der Norm ISO/IEC 27002.

ITIL

Die IT Infrastructure Library (ITIL) ist eine Ansammlung mehrerer Bücher zum Thema „IT-Service-Management“. Sie wurde vom britischen Office of Government Commerce (OGC) entwickelt. Die ITIL befasst sich mit dem Management von IT Services aus Sicht des IT-Dienstleisters. Der IT-Dienstleister kann dabei sowohl eine interne IT-Abteilung als auch ein externer Service Provider sein. Das allgemeine Ziel ist die Optimierung beziehungsweise Verbesserung der Qualität von IT-Dienstleistungen und der Kosteneffizienz. Informationssicherheit wird im Rahmen der betrachteten Services aus der operativen Perspektive heraus begutachtet. Umgekehrt ist ein funktionierender IT-Betrieb ein wesentlicher Stützpfiler für das ISMS, wodurch sich viele Disziplinen der ITIL in ähnlicher Art und Weise, aber mit einem eindeutigen Fokus auf der Informationssicherheit im IT-Grundschutz und anderen Sicherheitsstandards wiederfinden.

Auf der Basis der ITIL wurde die Norm ISO/IEC 20000 erarbeitet, auf deren Grundlage wiederum ein Service-Management-System zertifiziert werden kann.

PCI DSS

Der Payment Card Industry Data Security Standard (PCI DSS) wird von einem Konsortium führender Kreditkartenorganisationen herausgegeben. Er wurde vom PCI Security Standards Council erstellt und formuliert Sicherheitsanforderungen bezüglich der Abwicklung von Kreditkartentransaktionen. Die Anforderungen des PCI DSS müssen von allen Institutionen umgesetzt werden, die Karteninhaberdaten von Kreditkarten speichern, verarbeiten oder übertragen, also z. B. von Händlern, die Kreditkartenzahlungen akzeptieren, oder von Dienstleistern, die diese im Auftrag weiterverarbeiten.

NIST

Das US-amerikanische National Institute of Standards and Technology (NIST) ist eine Bundesbehörde, die unter anderem für die Entwicklung von Standards zuständig ist. Diese Standards sind für US-Behörden verpflichtend. In der Reihe *Special Publication 800* („NIST SP 800“-Serie) veröffentlicht das NIST regelmäßig Dokumente zu einzelnen Themen der Informationssicherheit (Kryptografie, Cloud-Computing usw.), die nicht nur wertvolle Informationen liefern, sondern auch international einen weitreichenden Einfluss auf die Gestaltung der Informationssicherheit haben.

Das Dokument NIST SP 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations* stellt dabei für den Bereich Sicherheitsmanagement eine große Zahl sogenannter „Controls“ zusammen, die dazu eingesetzt werden können, Informationsverbünde zu schützen. Die Controls sind nach zusammengehörigen Themen in diverse Bereiche gegliedert (z. B. Schulung und Sensibilisierung, Berechtigungsmanagement, Infrastruktursicherheit).

ISF – The Standard of Good Practice

Das Information Security Forum (ISF) ist eine unabhängige und weltweit tätige Organisation für Informationssicherheit. Das ISF veröffentlicht mit dem *Standard of Good Practice* (SoGP) einen auf anerkannten Best Practices basierenden Leitfaden zur Informationssicherheit. Der praxisorientierte Leitfaden deckt nach eigenen Angaben die Anforderungen der Standards ISO/IEC 27002, COBIT 5, PCI DSS 3.1 und NIST Cybersecurity Framework ab. Der SoGP gliedert die verschiedenen Themen in diverse Bereiche (z. B. Security Governance, Information Risk Assessment usw.).

3 ISMS-Definition und Prozessbeschreibung

3.1 Komponenten eines Managementsystems für Informationssicherheit

Als Management wird einerseits die Leitungsebene, also die Gesamtheit der Führungskräfte einer Institution, und andererseits im allgemeinen Sprachgebrauch die Aufgabe der Führung der Institution bezeichnet. Zur Unterscheidung wird die Gruppe der verantwortlichen Führungskräfte im Folgenden als „Leitungsebene“ bezeichnet, wenn die verantwortlichen Führungskräfte gemeint sind und Verwechslungsgefahr zum „Management“ als Aktivität (Leiten, Lenken und Planen) besteht.

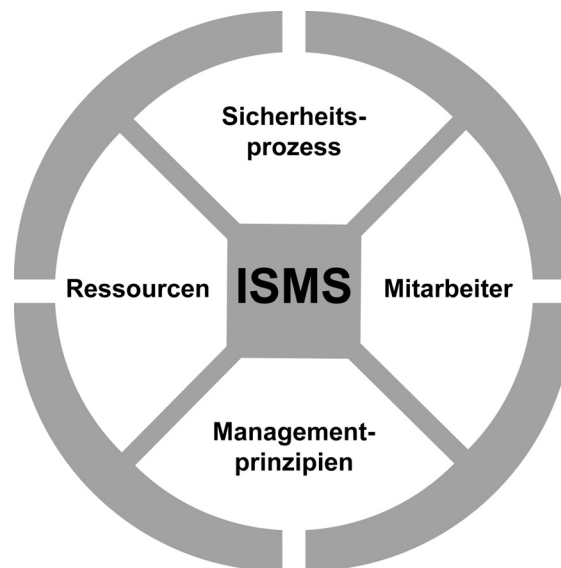


Abbildung 2: Bestandteile eines Managementsystems für Informationssicherheit (ISMS)

Ein Managementsystem umfasst alle Regelungen, die für die Steuerung und Lenkung einer Institution sorgen und letztlich zur Zielerreichung führen sollen. Der Teil des Managementsystems, der sich mit der Informationssicherheit beschäftigt, wird als Informationssicherheitsmanagementsystem (ISMS) bezeichnet. Das ISMS legt fest, mit welchen Instrumenten und Methoden die Leitungsebene die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenkt (plant, einsetzt, durchführt, überwacht und verbessert). Zu einem ISMS gehören folgende grundlegende Komponenten (siehe Abbildung 2):

- Managementprinzipien
- Ressourcen
- Mitarbeiter
- Sicherheitsprozess:
 - Leitlinie zur Informationssicherheit, in der die Sicherheitsziele und die Strategie zu ihrer Umsetzung dokumentiert sind
 - Sicherheitskonzept
 - Sicherheitsorganisation



Abbildung 3: Strategie zur Informationssicherheit als zentrale Komponente des ISMS

Die Sicherheitsstrategie dient der Orientierung für die Planung des weiteren Vorgehens, um die gesetzten Sicherheitsziele zu erreichen. Die Strategie wird von der Leitungsebene vorgegeben und basiert auf den Geschäftszielen des Unternehmens bzw. dem Auftrag der Behörde. Sicherheitsorganisation und Sicherheitskonzept sind dabei die Werkzeuge des Managements zur Umsetzung ihrer Sicherheitsstrategie.

Die Abbildungen 3 und 4 machen diesen Zusammenhang deutlich. Die Kernaspekte der Sicherheitsstrategie werden in der Leitlinie zur Informationssicherheit dokumentiert. Die Sicherheitsleitlinie ist von zentraler Bedeutung, da sie das sichtbare Bekenntnis der Leitungsebene zu ihrer Strategie enthält.



Abbildung 4: Umsetzung der Sicherheitsstrategie mithilfe des Sicherheitskonzepts und einer Sicherheitsorganisation

3.2 Prozessbeschreibung und Lebenszyklus-Modell

3.2.1 Der Lebenszyklus in der Informationssicherheit

Sicherheit ist kein unveränderbarer Zustand, der einmal erreicht wird und sich niemals wieder ändert. Jede Institution ist ständigen Veränderungen unterworfen. Viele dieser Veränderungen betreffen neben Änderungen der Geschäftsprozesse, Fachaufgaben, Infrastruktur, Organisationsstrukturen und der IT auch die Informationssicherheit. Zusätzlich zu den unübersehbaren Änderungen innerhalb einer Institution können sich außerdem externe Rahmenbedingungen verändern, z. B. gesetzliche oder vertragliche Vorgaben, aber auch die verfügbare Informations- oder Kommunikationstechnik kann sich entscheidend wandeln. Aufgrund neuer Angriffsmethoden oder Schwachstellen können Sicherheitskonzepte und -maßnahmen teilweise oder vollständig unwirksam werden. Daher ist es notwendig, Informationssicherheit aktiv zu managen, um ein einmal erreichtes Sicherheitsniveau dauerhaft aufrechtzuerhalten und kontinuierlich verbessern zu können.

Es reicht beispielsweise nicht aus, die Umsetzung von Geschäftsprozessen oder die Einführung eines neuen IT-Systems nur einmalig zu planen und die beschlossenen Sicherheitsmaßnahmen umzusetzen. Nach der Umsetzung müssen die Sicherheitsmaßnahmen regelmäßig auf ihre Wirksamkeit und Angemessenheit, aber auch auf deren Anwendbarkeit und die tatsächliche Anwendung untersucht werden. Finden sich Schwachpunkte oder Verbesserungsmöglichkeiten, müssen die Maßnahmen angepasst und verbessert werden. Es muss somit eine erneute Planung und Umsetzung der notwendigen Anpassungen und Änderungen erfolgen. Werden Geschäftsprozesse beendet oder Komponenten bzw. IT-Systeme ersetzt oder außer Betrieb genommen, sind auch dabei Sicherheitsaspekte zu beachten (z. B. Entzug von Berechtigungen oder sicheres Löschen von Festplatten). In den Umsetzungshin-

weisen zu den Bausteinen des IT-Grundschutz-Kompendiums werden die Sicherheitsmaßnahmen daher zur besseren Übersicht für die Leser in folgende Phasen eingeteilt:

- Planung und Konzeption,
- Beschaffung (falls erforderlich),
- Umsetzung,
- Betrieb (Maßnahmen zur Aufrechterhaltung der Informationssicherheit im Betrieb, dazu gehört auch die Überwachung und Erfolgskontrolle),
- Aussonderung (falls erforderlich) und
- Notfallvorsorge.

3.2.2 Beschreibung des Prozesses Informationssicherheit

Nicht nur Geschäftsprozesse und IT-Systeme haben einen solchen „Lebenszyklus“, sondern auch die Sicherheitsstrategie, das Sicherheitskonzept, die Sicherheitsorganisation und letztendlich der gesamte Sicherheitsprozess unterliegen einem solchen Lebenszyklus. Um die Dynamik des Sicherheitsprozesses möglichst einfach beschreiben zu können, wird dieser in der Literatur häufig in die folgenden Phasen eingeteilt:

1. Planung,
2. Umsetzung der Planung bzw. Durchführung des Vorhabens,
3. Erfolgskontrolle bzw. Überwachung der Zielerreichung und
4. Beseitigung von erkannten Mängeln und Schwächen bzw. Optimierung sowie Verbesserung.

Phase 4 beschreibt die umgehende Beseitigung kleinerer Mängel. Bei grundlegenden oder umfangreichen Veränderungen ist natürlich wieder mit der Planungsphase zu beginnen.

Dieses Modell wird nach der englischen Benennung der einzelnen Phasen („Plan“, „Do“, „Check“, „Act“) entsprechend auch als PDCA-Zyklus bezeichnet.

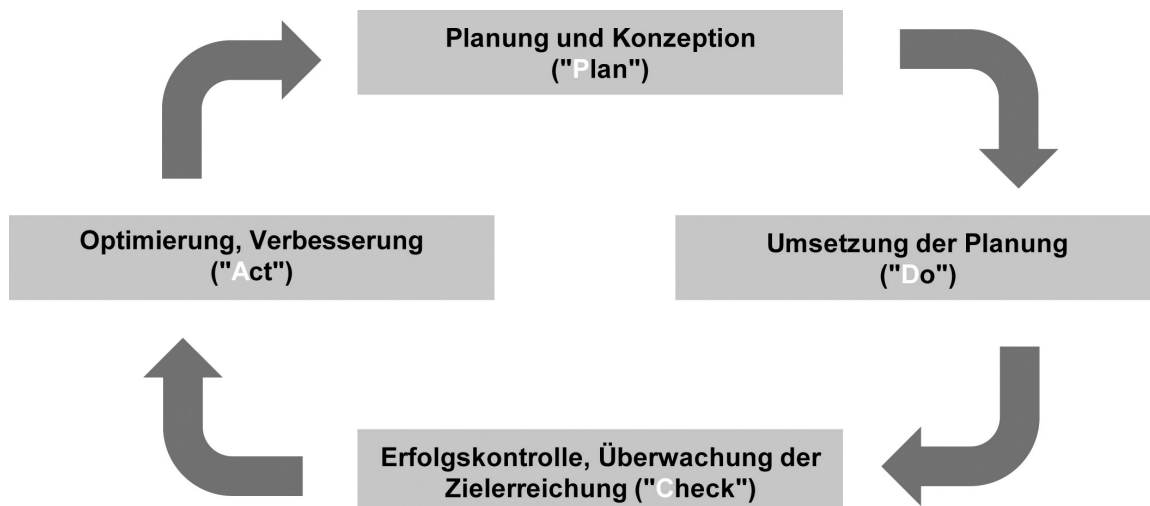


Abbildung 5: Lebenszyklus nach Deming (PDCA-Zyklus)

Der PDCA-Zyklus lässt sich prinzipiell auf alle Aufgaben innerhalb des Sicherheitsprozesses anwenden. Auch der Lebenszyklus des Sicherheitskonzepts und der Sicherheitsorganisation lässt sich so

übersichtlich beschreiben. Die entsprechenden Kapitel dieses Dokuments sind daher an die vier Phasen dieses Lebenszyklus-Modells angelehnt.

In der Planungsphase des Sicherheitsprozesses werden die Rahmenbedingungen identifiziert und analysiert, die Sicherheitsziele bestimmt und eine Sicherheitsstrategie ausgearbeitet, die grundlegende Aussagen darüber enthält, wie die gesetzten Ziele letztlich erreicht werden sollen. Umgesetzt wird die Sicherheitsstrategie mithilfe des Sicherheitskonzepts und einer geeigneten Struktur für die Sicherheitsorganisation. Sicherheitskonzept und -organisation müssen geplant, umgesetzt und einer Erfolgskontrolle unterzogen werden. Bei der Erfolgskontrolle des übergeordneten Sicherheitsprozesses wird regelmäßig überprüft, ob sich Rahmenbedingungen (zum Beispiel Gesetze, Ziele der Institution oder des Umfeldes) geändert haben und ob sich Sicherheitskonzept und -organisation als wirksam und effizient erwiesen haben.

Da unterschiedliche Institutionen jedoch über verschiedene Ausgangsbedingungen, Sicherheitsanforderungen und finanzielle Mittel verfügen, bietet diese Vorgehensweise zwar eine gute Orientierung, muss aber von jeder Behörde und jedem Unternehmen auf die eigenen Bedürfnisse angepasst werden. Jede Institution muss individuell festlegen oder konkretisieren, welche Ausprägung eines Lebenszyklus-Modells für sie angemessen ist.

Kleine Behörden und Unternehmen sollten sich hiervon jedoch nicht abschrecken lassen, da der Aufwand für den Sicherheitsprozess in der Regel von der Größe der Institution abhängt. So ist in einem sehr großen Unternehmen mit vielen beteiligten Abteilungen und Personen wahrscheinlich ein eher formaler Prozess notwendig, der genau festlegt, welche internen und externen Audits notwendig sind, wer an wen berichtet, wer Entscheidungsvorlagen erstellt und wann die Leitung über den Sicherheitsprozess berät. In einem kleinen Unternehmen hingegen kann eine jährliche Besprechung zwischen dem Geschäftsführer und seinem IT-Dienstleister, in der über die Probleme des vergangenen Jahres, die entstandenen Kosten, neue technische Entwicklungen und andere Faktoren beraten wird, bereits angemessen sein, um den Erfolg des Sicherheitsprozesses kritisch hinterfragen zu können.

4 Management-Prinzipien

Mit Informationssicherheitsmanagement oder kurz IS-Management wird die Planungs- und Lenkungsaufgabe bezeichnet, die zum sinnvollen Aufbau, zur praktischen Umsetzbarkeit und zur Sicherstellung der Effektivität eines durchdachten und planmäßigen Sicherheitsprozesses sowie aller dafür erforderlichen Sicherheitsmaßnahmen erforderlich ist. Dieses umfasst auch die Erfüllung und Einhaltung von gesetzlichen und regulatorischen Anforderungen. Es gibt verschiedene Konzepte, wie ein effizientes IS-Management aussehen kann und welche Organisationsstrukturen dafür sinnvoll sind. Unabhängig davon, wie die Ausprägung eines IS-Managementsystems aussieht, sind dafür verschiedene Prinzipien zu beachten.

Einige der hier vorgestellten Management-Prinzipien mögen banal klingen, ihre Umsetzung werden die meisten Führungskräfte also als eine Selbstverständlichkeit ansehen. Paradoxerweise sind es aber gerade immer wieder die einfachen Dinge, die in der Praxis falsch gemacht oder unterlassen werden. Disziplin, Geduld, die Übernahme von Verantwortung sowie die realistische und sorgfältige Vorbereitung von Projekten sind in vielen Organisationen zwar theoretisch anerkannte Werte, werden aber in der Praxis nicht immer gelebt. Gerade wenig spektakuläre Maßnahmen, wie Prozessoptimierung, Schulung und Sensibilisierung sowie Motivation von Mitarbeitern oder das Anfertigen von verständlichen Dokumentationen, verbessern das Sicherheitsniveau in der Praxis deutlich. Komplexe und dadurch teure Maßnahmen, Großprojekte und Investitionen in Technik werden oftmals völlig zu Unrecht als wirksamer dargestellt und sind häufig für den schlechten Ruf von Sicherheitsmaßnahmen als Kostentreiber verantwortlich. Im Folgenden werden daher Management-Prinzipien vorgestellt, deren Berücksichtigung eine gute Grundlage für ein erfolgreiches Informationssicherheitsmanagement bietet.

4.1 Aufgaben und Pflichten des Managements

Die Aufgaben und Pflichten der Leitungsebene bezüglich der Informationssicherheit lassen sich in folgenden Punkten zusammenfassen:

1. Übernahme der Gesamtverantwortung für Informationssicherheit

Die oberste Managementebene jeder Behörde und jedes Unternehmens ist für das zielgerichtete und ordnungsgemäße Funktionieren der Institution verantwortlich und damit auch für die Gewährleistung der Informationssicherheit nach innen und außen. Dies kann auch je nach Land und nach Organisationsform in verschiedenen Gesetzen geregelt sein. Die Leitungsebene, aber auch jede einzelne Führungskraft muss sich sichtbar zu ihrer Verantwortung bekennen und allen Mitarbeitern die Bedeutung der Informationssicherheit vor Augen führen.

2. Informationssicherheit initiieren, steuern und kontrollieren

Die oberste Leitungsebene muss den Sicherheitsprozess initiieren, steuern und überwachen. Dazu gehören zum Beispiel folgende Aufgaben:

- Eine Strategie zur Informationssicherheit sowie Sicherheitsziele müssen verabschiedet und kommuniziert werden. Die Sicherheitsstrategie basiert auf den Geschäftszielen des Unternehmens bzw. dem Auftrag der Behörde.
- Die Auswirkungen von Sicherheitsrisiken auf die Geschäftstätigkeit bzw. Aufgabenerfüllung müssen untersucht werden. Die Leitungsebene ist diejenige Instanz, die die Entscheidung über den Umgang mit Risiken treffen muss. Die Verantwortung für Informationssicherheit verbleibt dort.

Die operative Aufgabe „Informationssicherheit“ wird allerdings typischerweise an einen Informationssicherheitsbeauftragten (ISB) delegiert.

- Es müssen die organisatorischen Rahmenbedingungen für Informationssicherheit geschaffen, Zuständigkeiten und Befugnisse zugewiesen und kommuniziert werden.
- Für Informationssicherheit müssen ausreichende Ressourcen bereitgestellt werden. Die Sicherheitsstrategie muss mit den zur Verfügung stehenden Ressourcen in Einklang stehen.
- Die Sicherheitsstrategie muss regelmäßig überprüft und bewertet werden, z. B. kann die Zielerreichung mithilfe von Kennzahlen überwacht werden. Erkannte Schwachstellen und Fehler müssen korrigiert werden. Dazu muss ein „innovationsfreudiges“ Arbeitsklima geschaffen und der Wille zur ständigen Verbesserung innerhalb der Institution demonstriert werden.
- Mitarbeiter müssen für Sicherheitsbelange sensibilisiert werden und die Informationssicherheit als einen wichtigen Aspekt ihrer Aufgaben betrachten. Hierfür sind unter anderem passende Schulungs- und Sensibilisierungsmaßnahmen anzubieten.

3. Informationssicherheit integrieren

Informationssicherheit ist Querschnittsfunktion und muss daher in alle Prozesse und Projekte der Institution integriert werden, bei denen Informationen verarbeitet werden. Beispiele hierfür sind:

- Projektmanagement: Bereits in der Planungsphase eines Projektes muss der Schutzbedarf der zukünftig als Ergebnis zu verarbeitenden Informationen bewertet werden. Darauf aufbauend sollte die Planung geeigneter Sicherheitsmaßnahmen erfolgen.
- Incident Management: Bei Störungen des IT-Betriebs mit Auswirkungen auf die Informationssicherheit muss das weitere Vorgehen mit dem Sicherheitsmanagement abgestimmt werden. Das Security Incident Management und Störungsmanagement der IT und des Facility Managements müssen demnach miteinander 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 verknüpft 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 weitergeleitet. Der Reifegrad der Informationssicherheit hängt somit auch vom Reifegrad der anderen Management-Prozesse der Institution ab und ist keine selbstständige Größe.

4. Erreichbare Ziele setzen

Projekte scheitern oft an unrealistischen oder zu ehrgeizigen Zielvorgaben. Dies ist im Bereich Informationssicherheit auch nicht anders. Um das angemessene Sicherheitsziel zu erreichen, können viele kleine Schritte und ein langfristiger, kontinuierlicher Verbesserungsprozess ohne hohe Investitionskosten zu Beginn effizienter sein als ein groß angelegtes Projekt. So kann es zweckmäßig sein, zunächst nur in ausgewählten Bereichen das erforderliche Sicherheitsniveau umzusetzen und dort etwa in die Breite gehend mit der Basis-Absicherung oder in die Tiefe gehend mit der Kern-Absicherung aus dem IT-Grundschutz zu arbeiten. Von diesen Keimzellen ausgehend, muss dann die Sicherheit innerhalb der Institution jedoch zügig auf das angestrebte Niveau gebracht werden.

5. Sicherheitskosten gegen Nutzen abwägen

Eine der schwierigsten Aufgaben ist es, die Kosten für Informationssicherheit gegenüber dem Nutzen und den Risiken abzuwägen. Es erscheint hier sehr wichtig, zunächst in Maßnahmen zu investieren, die besonders effektiv sind oder gegen besonders hohe Risiken schützen. Die effektivsten Maßnahmen sind dabei erfahrungsgemäß jedoch nicht immer die teuersten. Es ist daher unerlässlich, die Abhängigkeit der Geschäftsprozesse und Aufgaben von der Informationsverarbeitung zu kennen, um angemessene Sicherheitsmaßnahmen auswählen zu können.

Dabei ist zu betonen, dass Informationssicherheit immer durch ein Zusammenspiel aus technischen und organisatorischen Maßnahmen erreicht wird. Die Investitionen in Technik sind unmittelbar am Budget ablesbar. Damit diese Kosten gerechtfertigt sind, müssen die Sicherheitsprodukte so eingesetzt werden, dass sie den optimalen Nutzen bieten. Dafür müssen sie aber auch zweckgerichtet ausgewählt worden sein und entsprechend bedient werden, also beispielsweise müssen sie in die ganzheitliche Sicherheitskonzeption integriert sein und die Mitarbeiter in deren Nutzung geschult sein. Häufig können technische Lösungen auch durch organisatorische Sicherheitsmaßnahmen ersetzt werden. Erfahrungsgemäß ist es aber schwieriger, sicherzustellen, dass organisatorische Maßnahmen konsequent umgesetzt werden. Zudem steigt dadurch der personelle Aufwand und belastet somit auch die Ressourcen.

6. Vorbildfunktion

Die Leitungsebene muss auch im Bereich der Informationssicherheit eine Vorbildfunktion übernehmen. Dazu gehört unter anderem, dass auch die Leitungsebene alle vorgegebenen Sicherheitsregeln beachtet, selbst an Schulungsveranstaltungen teilnimmt und andere Führungskräfte bei der Ausübung ihrer Vorbildfunktion unterstützt.

4.2 Kommunikation und Wissen

In allen Phasen des Sicherheitsprozesses ist Kommunikation ein wesentlicher Eckpfeiler, um die gesteckten Sicherheitsziele zu erreichen. Missverständnisse und Wissensmängel sind die häufigsten Ursachen für auftretende Sicherheitsprobleme. Vor diesem Hintergrund muss auf allen Ebenen und in allen Bereichen einer Institution für einen reibungslosen Informationsfluss über Sicherheitsvorkommnisse und -maßnahmen gesorgt werden. Dazu gehören die folgenden Aspekte:

- **Berichte an die Leitungsebene**
Das Management muss sich regelmäßig über Probleme, Ergebnisse von Überprüfungen und Audits, aber auch über neue Entwicklungen, geänderte Rahmenbedingungen oder Verbesserungsmöglichkeiten informieren lassen, um seiner Steuerungsfunktion nachkommen zu können. Damit die Leitungsebene die richtigen Entscheidungen bei der Steuerung und Lenkung des Informationssicherheitsprozesses treffen kann, benötigt sie Eckpunkte über den Stand der Informationssicherheit. Diese Eckpunkte sollten in Managementberichten aufbereitet und der Leitungsebene vom ISB regelmäßig und in angemessener Form übermittelt werden. Die Leitungsebene nimmt die Managementberichte zur Kenntnis und veranlasst eventuell notwendige Maßnahmen.
- **Informationsfluss**
Durch eine mangelhafte Kommunikation und fehlende Informationen kann es zu Sicherheitsproblemen, aber auch zu Fehlentscheidungen oder überflüssigen Arbeitsschritten kommen. Dies muss durch personelle Maßnahmen und organisatorische Regelungen vermieden werden. Mitarbeiter müssen über den Sinn und Zweck von Sicherheitsmaßnahmen aufgeklärt werden, vor allem, wenn diese zusätzliche Arbeit verursachen oder Komforteinbußen zur Folge haben. Des Weiteren sollten

die Mitarbeiter über die mit ihrer Arbeit verbundenen Rechtsfragen zur Informationssicherheit wie auch zum Datenschutz aufgeklärt werden. Mitarbeiter sollten außerdem in die Umsetzungsplanung von Maßnahmen einbezogen werden, um eigene Ideen einbringen und die Praxistauglichkeit beurteilen zu können.

- **Klassifikation von Informationen**

Um Informationen angemessen schützen zu können, muss deren Bedeutung für die Institution klar erkennbar 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.

- **Dokumentation**

Um die Kontinuität und Konsistenz des gesamten Sicherheitsprozesses sicherzustellen, ist es unabdingbar, diesen zu dokumentieren. Nur so bleiben die verschiedenen Prozessschritte und Entscheidungen nachvollziehbar. Zudem stellen aussagekräftige Dokumentationen sicher, dass gleichartige Arbeiten auf vergleichbare Art und Weise durchgeführt werden, also Prozesse messbar und wiederholbar werden. Zusätzlich helfen Dokumentationen dabei, grundsätzliche Schwächen im Prozess zu erkennen und die Wiederholung von Fehlern zu vermeiden. Die erforderlichen Dokumentationen erfüllen bei den verschiedenen Sicherheitsaktivitäten unterschiedliche Funktionen und sind an unterschiedliche Zielgruppen gerichtet. Folgende Dokumentationsarten lassen sich unterscheiden:

1. Technische Dokumentation und Dokumentation von Arbeitsabläufen

(Zielgruppe: Experten)

Es muss bei Störungen oder Sicherheitsvorfällen möglich sein, den gewünschten Soll-Zustand in Geschäftsprozessen sowie innerhalb der zugehörigen IT wiederherstellen zu können. Technische Einzelheiten und Arbeitsabläufe sind daher so zu dokumentieren, dass dies in angemessener Zeit möglich ist.

Beispiele hierfür sind Anleitungen zur Installation von IT-Anwendungen, zur Durchführung von Datensicherungen, zum Rückspielen einer Datensicherung, zur Konfiguration der TK-Anlage, zum Wiederanlauf eines Anwendungsservers nach einem Stromausfall, ebenso wie die Dokumentation von Test- und Freigabeverfahren und Anweisungen für das Verhalten bei Störungen und Sicherheitsvorfällen.

Arbeitsabläufe, organisatorische Vorgaben und technische Sicherheitsmaßnahmen müssen so dokumentiert werden, dass Sicherheitsvorfälle durch Unkenntnis oder Fehlhandlungen vermieden werden. Beispiele hierfür sind Sicherheitsrichtlinien für die Nutzung von E-Mail und Internet, Hinweise zur Verhinderung von Virenvorfällen oder zum Erkennen von Social Engineering sowie Verhaltensregeln für Mitarbeiter beim Verdacht eines Sicherheitsvorfalls.

2. Managementberichte (Zielgruppe: Leitungsebene, Sicherheitsmanagement)

Alle Informationen, die das Management benötigt, um seinen Lenkungs- und Steuerungsaufgaben nachkommen zu können, sind im erforderlichen Detaillierungsgrad aufzuzeichnen (zum Beispiel Ergebnisse von Audits, Effektivitätsmessungen, Berichte über Sicherheitsvorfälle).

3. Aufzeichnung von Managemententscheidungen (Zielgruppe: Leitungsebene)

Die Leitungsebene muss die gewählte Sicherheitsstrategie aufzeichnen und begründen. Zudem müssen auch auf allen anderen Ebenen Entscheidungen, die sicherheitsrelevante Aspekte betreffen, ebenso dokumentiert werden, damit diese jederzeit nachvollziehbar und wiederholbar sind.

In den nachfolgenden Kapiteln wird daher jede Aktion, die angemessen dokumentiert bzw. aufgezichnet werden muss, entsprechend mit „[DOK]“ gekennzeichnet.

Formale Anforderungen an Dokumentationen

Dokumentationen müssen nicht zwingend in Papierform vorliegen. Das Dokumentationsmedium sollte je nach Bedarf gewählt werden. Beispielsweise kann für das Notfallmanagement der Einsatz eines Softwarewerkzeugs hilfreich sein, mittels dessen vorab alle Notfallmaßnahmen und Ansprechpartner erfasst werden und das im Krisenfall mobil eingesetzt werden kann. Dann muss dieses Tool auch im Notfall mit allen erforderlichen Informationen und den benötigten IT-Systemen verfügbar sein, beispielsweise auf einem Laptop. Je nach Notfall kann es aber gegebenenfalls sinnvoller sein, alle Informationen in einem praktischen Handbuch in Papierform griffbereit zu haben.

Es kann gesetzliche oder vertragliche Anforderungen an Dokumentationen geben, die zu beachten sind, z. B. zu Aufbewahrungsfristen und Detaillierungstiefe. Dokumentationen erfüllen nur dann ihren Zweck, wenn sie regelmäßig erstellt und aktuell gehalten werden. Außerdem müssen sie so bezeichnet und abgelegt werden, dass sie im Bedarfsfall nutzbar sind. Es muss klar erkennbar sein, wer wann welche Teile der Dokumentation erstellt hat. Dort, wo auf andere Dokumente verwiesen wird, müssen die Quellen explizit beschrieben sein. Weiterführende Dokumente müssen zudem im Bedarfsfall ebenfalls zur Verfügung stehen.

Sicherheitsrelevante Dokumentationen können schutzbedürftige Informationen enthalten und müssen daher angemessen geschützt werden. Neben dem Schutzbedarf müssen die Aufbewahrungsart und -dauer und Optionen für die Vernichtung von Informationen festgelegt werden. In den Prozessbeschreibungen muss aufgeführt sein, ob und wie Dokumentationen auszuwerten sind, wer diese in welchen Abständen zu bearbeiten hat und wer darauf zugreifen darf.

Nutzung verfügbarer Informationsquellen und Erfahrungen

Informationssicherheit ist ein komplexes Thema, sodass die hierfür Verantwortlichen sich sorgfältig einarbeiten müssen. Es gibt viele verfügbare Informationsquellen, die dazu genutzt werden können. Hierzu gehören bestehende Normen und Standards, Internetveröffentlichungen und sonstige Publikationen. Außerdem sollte die Kooperation mit Verbänden, Partnern, Gremien, anderen Unternehmen oder Behörden sowie CERTs (Computer Emergency Response Teams) zum Erfahrungsaustausch über erfolgreiche Sicherheitsaktionen genutzt werden. Da das Thema Informationssicherheit sehr umfangreich ist, scheint es wichtig, die für die jeweilige Institution und die dort zu verortenden Rahmenbedingungen passenden Informationsquellen und Kooperationspartner zu identifizieren und entsprechend zu dokumentieren.

4.3 Erfolgskontrolle im Sicherheitsprozess

Eine Erfolgskontrolle und Bewertung des Sicherheitsprozesses durch die Leitungsebene sollte regelmäßig stattfinden (Managementbewertung). Bei Bedarf (z. B. bei der Häufung von Sicherheitsvorfällen oder einer deutlichen Änderung der Rahmenbedingungen) müssen entsprechende Kontrollen und Bewertungen auch zwischen den Routineterminen vorgenommen werden. Alle Ergebnisse und Beschlüsse müssen nachvollziehbar dokumentiert werden [DOK].

Bei der Diskussion sollte unter anderem folgenden Fragen nachgegangen werden:

- Haben sich Rahmenbedingungen geändert, die dazu führen, dass das Vorgehen in Bezug auf Informationssicherheit geändert werden muss?

- Sind die Sicherheitsziele noch angemessen?
- Ist die Leitlinie zur Informationssicherheit noch aktuell?

Der Schwerpunkt bei der Erfolgskontrolle des Sicherheitsprozesses liegt dabei nicht auf der Überprüfung einzelner Sicherheitsmaßnahmen oder organisatorischer Regelungen, sondern auf einer Gesamtbetrachtung. Beispielsweise könnte sich der sichere Betrieb eines Internetportals als zu teuer für ein kleines Unternehmen herausstellen. Die Leitungsebene könnte dann als Alternative einen Dienstleister mit der Betreuung des Portals beauftragen.

Hierbei ist es hilfreich, zu prüfen, wie sich das Sicherheitskonzept und die Sicherheitsorganisation bisher bewährt haben. In Kapitel 8 *Sicherheitskonzept* werden verschiedene Aktivitäten für die Erfolgskontrolle einzelner Sicherheitsmaßnahmen beschrieben. Die dort gesammelten Ergebnisse sollten bei der Erfolgskontrolle der Sicherheitsstrategie berücksichtigt werden. Stellt sich z. B. heraus, dass die Sicherheitsmaßnahmen unwirksam oder ausgesprochen teuer sind, kann dies ein Anlass dafür sein, die gesamte Sicherheitsstrategie noch einmal zu überdenken und anzupassen. Dabei sollten sich die Betroffenen die folgenden Fragen stellen:

- Ist die Sicherheitsstrategie noch angemessen?
- Ist das Sicherheitskonzept geeignet, um die gesteckten Ziele zu erreichen? Werden z. B. die gesetzlichen Anforderungen erfüllt?
- Ist die Sicherheitsorganisation geeignet, um die Ziele realisieren zu können? Muss deren Stellung innerhalb der Institution gestärkt oder sie stärker in interne Abläufe eingebunden werden?
- Steht der Aufwand – also Kosten, Personal, Material –, der zur Erreichung der Sicherheitsziele betrieben wird, in einem sinnvollen Verhältnis zu den Geschäftszielen bzw. dem Auftrag der Institution?

4.4 Kontinuierliche Verbesserung des Sicherheitsprozesses

Die Ergebnisse der Erfolgskontrolle müssen konsequent zu angemessenen Korrekturen genutzt werden. Dies kann bedeuten, dass die Sicherheitsziele, die Sicherheitsstrategie und/oder das Sicherheitskonzept geändert werden müssen und die Sicherheitsorganisation den Erfordernissen angepasst werden sollte. Unter Umständen erscheint es sinnvoll, grundlegende Änderungen an Geschäftsprozessen oder der IT-Landschaft vorzunehmen sowie Geschäftsprozesse aufzugeben oder auszulagern, wenn z. B. deren sicherer Betrieb mit den zur Verfügung stehenden Ressourcen nicht länger gewährleistet werden kann. Wenn größere Veränderungen vorgenommen und umfangreiche Verbesserungen umgesetzt werden, schließt sich der Management-Kreislauf wieder durch den erneuten Beginn der Planungsphase.

5 Ressourcen für Informationssicherheit

Die Einhaltung eines bestimmten Sicherheitsniveaus erfordert stets finanzielle, personelle und zeitliche Ressourcen, die von der Leitungsebene ausreichend bereitgestellt werden müssen. Wenn die Zielvorgaben aufgrund fehlender Ressourcen nicht erfüllt werden können, sind hierfür nicht die mit der Umsetzung betrauten Personen verantwortlich, sondern die Vorgesetzten, die unrealistische Ziele gesetzt bzw. die erforderlichen Ressourcen nicht zur Verfügung gestellt haben. Um die gesteckten Ziele nicht zu verfehlen, ist es wichtig, schon bei deren Festlegung eine erste Kosten-Nutzen-Schätzung durchzuführen. Im Laufe des Sicherheitsprozesses sollte dieser Aspekt weiterhin eine entscheidende Rolle spielen, einerseits, um keine Ressourcen zu verschwenden, und andererseits, um die notwendigen Investitionen zur Erreichung des angemessenen Sicherheitsniveaus gewährleisten zu können.

Oft werden mit der IT-Sicherheit ausschließlich technische Lösungen assoziiert. Diese Sichtweise greift jedoch zu kurz. Dies ist ein weiterer Grund, statt IT-Sicherheit besser den Begriff Informationssicherheit zu verwenden. Vor allem erscheint es aber wichtig, darauf hinzuweisen, dass Investitionen in personelle Ressourcen häufig effektiver sind als Investitionen in Sicherheitstechnik. Technik alleine löst somit keine Probleme, sie muss immer in organisatorische Rahmenbedingungen eingebunden sein. Auch die Überprüfung der Wirksamkeit und Eignung von Sicherheitsmaßnahmen muss durch ausreichende Ressourcen sichergestellt werden.

In der Praxis fehlt den institutionseigenen Sicherheitsexperten häufig die Zeit, um alle sicherheitsrelevanten Einflussfaktoren und Rahmenbedingungen (z. B. gesetzliche Anforderungen oder technische Fragen) zu analysieren. Teilweise mangelt es ihnen auch an entsprechenden Grundlagen. Es ist immer dann sinnvoll, auf externe Experten zurückzugreifen, wenn Fragen und Probleme nicht mit eigenen Mitteln zu klären bzw. zu lösen sind. Dies muss von den institutionseigenen Sicherheitsexperten dokumentiert werden, damit die Leitungsebene die erforderlichen Ressourcen bereitstellen kann.

Die Grundvoraussetzung für einen sicheren Betrieb der Informationstechnik ist ein gut funktionierender Betrieb. Für den Betrieb müssen daher ausreichende Ressourcen zur Verfügung gestellt werden. Typische Probleme des Betriebs (knappe Ressourcen, überlastete Administratoren oder eine unstrukturierte und schlecht gewartete IT-Landschaft) müssen in der Regel erst gelöst werden, damit die eigentlichen Sicherheitsmaßnahmen wirksam und effizient umgesetzt werden können.

6 Einbindung der Mitarbeiter in den Sicherheitsprozess

Die Informationssicherheit betrifft ohne Ausnahme alle Mitarbeiter. Jeder Einzelne kann durch ein verantwortungs- und qualitätsbewusstes Handeln Schäden vermeiden und zum Erfolg beitragen. Eine Sensibilisierung für Informationssicherheit und entsprechende Schulungen der Mitarbeiter sowie aller Führungskräfte sind daher eine Grundvoraussetzung für Informationssicherheit. Um Sicherheitsmaßnahmen wie geplant umsetzen zu können, müssen bei den Mitarbeitern die erforderlichen Grundlagen vorhanden sein. Dazu gehört neben den Kenntnissen, wie Sicherheitsmechanismen bedient werden müssen, auch das Wissen über den Sinn und Zweck von Sicherheitsmaßnahmen. Auch das Arbeitsklima, gemeinsame Wertvorstellungen und das Engagement der Mitarbeiter beeinflussen die Informationssicherheit entscheidend.

Werden Mitarbeiter neu eingestellt oder erhalten sie neue Aufgaben, ist eine gründliche Einarbeitung und gegebenenfalls Ausbildung notwendig. Die Vermittlung sicherheitsrelevanter Aspekte des jeweiligen Arbeitsplatzes muss dabei berücksichtigt werden. Wenn Mitarbeiter die Institution verlassen oder sich ihre Zuständigkeiten verändern, muss dieser Prozess durch geeignete Sicherheitsmaßnahmen begleitet werden (z. B. Entzug von Berechtigungen, Rückgabe von Schlüsseln und Ausweisen).

Mitarbeiter müssen zur Einhaltung aller im jeweiligen Umfeld relevanten Gesetze, Vorschriften und Regelungen verpflichtet werden. Dazu ist es natürlich erforderlich, sie mit den bestehenden Regelungen zur Informationssicherheit vertraut zu machen und die gleichzeitig zu deren Einhaltung zu motivieren. Des Weiteren sollten die Mitarbeiter wissen, dass jeder erkannte (oder vermutete) Sicherheitsvorfall dem Sicherheitsmanagement unmittelbar gemeldet werden muss und wie und an wen die Meldung zu erfolgen hat.

7 Der Sicherheitsprozess

Die Leitungsebene muss die Sicherheitsziele in Kenntnis aller relevanten Rahmenbedingungen, der Umfeldanalyse und basierend auf den Geschäftszielen des Unternehmens bzw. dem Auftrag der Behörde festlegen und die Voraussetzungen für deren Umsetzung schaffen. Mit einer Sicherheitsstrategie wird das Vorgehen geplant, um einen kontinuierlichen Sicherheitsprozess zu etablieren. Umgesetzt wird die Strategie mithilfe eines Sicherheitskonzepts und einer Sicherheitsorganisation. Im Folgenden werden daher für jede Lebenszyklusphase die relevanten Managementtätigkeiten beschrieben. Aufgrund des Umfangs und zur besseren Übersicht werden die Tätigkeiten rund um das Sicherheitskonzept jeweils in einem eigenen Kapitel beschrieben.

7.1 Planung des Sicherheitsprozesses

Ermittlung von Rahmenbedingungen

Die Schaffung von Informationssicherheit ist kein Selbstzweck, sondern Informationssicherheit trägt dazu bei, dass die Ziele einer Institution erreicht und Geschäftsprozesse bzw. Aufgaben zuverlässig ausgeführt werden können. Hierzu ist es erforderlich, dass die Institution alle Rahmenbedingungen identifiziert und analysiert, die Sicherheitsziele festlegt und eine Sicherheitsstrategie ausarbeitet, die grundlegende Aussagen darüber enthält, wie die gesetzten Ziele erreicht werden sollen. Die Identifikation der Rahmenbedingungen beinhaltet auch eine Umfeldanalyse, bei der sowohl interne als auch externe Parteien sowie deren Sicherheitsanforderungen, deren Anforderungen an das ISMS und ihre gesetzlichen und regulatorischen Anforderungen berücksichtigt werden.

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. Zudem wird dadurch eine erste Selbsteinschätzung (Self-Assessment) möglich, da bei der Zusammenstellung der Hintergrundinformationen bereits deutlich wird, worin Konfliktpotenzial liegt und wo möglicherweise noch Handlungsbedarf besteht.

Formulierung von Sicherheitszielen und einer Leitlinie zur Informationssicherheit [DOK]

Zu Beginn eines jeden Sicherheitsprozesses sollten die Informationssicherheitsziele sorgfältig festgelegt 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 und strategische Vorgaben gemacht werden, wie diese Sicherheitsziele zur Umsetzung gelangen können. Folgende Themen sollten bei der Entwicklung der Sicherheitsstrategie mindestens berücksichtigt werden:

- Ziele des Unternehmens bzw. Aufgaben der Behörde,
- gesetzliche Anforderungen und Vorschriften, wie z. B. zum Datenschutz,
- Kundenanforderungen und bestehende Verträge,
- interne Rahmenbedingungen (z. B. organisationsweites Risikomanagement), Umfeldanalyse,
- (IT-gestützte) Geschäftsprozesse und Fachaufgaben und
- globale Bedrohungen der Geschäftstätigkeit durch Sicherheitsrisiken (z. B. Imageschäden, Verstöße gegen Gesetze und vertragliche Verpflichtungen, Diebstahl von Forschungsergebnissen).

Die Kernaussagen der Sicherheitsstrategie werden in einer Leitlinie zur Informationssicherheit (englisch: „Information Security Policy“ oder „IT Security Policy“) dokumentiert. Die Sicherheitsleitlinie sollte mindestens Aussagen zu den folgenden Themen enthalten:

- 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 noch folgende Aussagen hinzukommen:

- Zur Motivation können einige, für die Geschäftsprozesse wichtige Gefährdungen diskutiert 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 ISB, die Mitarbeiter und den IT-Betrieb, ausführliche Informationen zu den einzelnen Rollen finden sich in Kapitel 4 *Organisation des Sicherheitsprozesses* des BSI-Standards 200-2 *IT-Grundschutz-Methodik*. 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.

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.

Festlegung des Geltungsbereichs [DOK]

Zunächst muss der Geltungsbereich festgelegt werden, für den das ISMS zuständig sein soll. Der Geltungsbereich umfasst häufig die gesamte Institution, kann sich aber z. B. auch auf eine oder mehrere Fachaufgaben oder Geschäftsprozesse oder eine oder mehrere Organisationseinheiten beziehen. Hierbei ist es wichtig, dass die betrachteten Fachaufgaben und Geschäftsprozesse im gewählten Geltungsbereich vollständig enthalten und inhaltlich abgeschlossen sind, also bei keinem Geschäftsprozess wesentliche Anteile außerhalb des Geltungsbereiches liegen. Im Rahmen des IT-Grundschutzes wird für den Geltungsbereich der Begriff „Informationsverbund“ verwendet. Der Informationsverbund umfasst auch alle infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die der Aufgabenerfüllung in diesem Anwendungsbereich der Informationsverarbeitung dienen.

Während bei der Basis- und Standard-Absicherung der Geltungsbereich häufig die gesamte Institution umfasst, konzentriert man sich bei der Kern-Absicherung auf einige herausragende, besonders geschäftskritische Assets (sogenannte „Kronjuwelen“).

7.2 Aufbau einer Sicherheitsorganisation [DOK]

Zur Planung und Durchsetzung eines Sicherheitsprozesses gehören die Festlegung von Organisationsstrukturen (z. B. Abteilungen, Gruppen, Kompetenzzentren) und die Definition von Rollen und Aufgaben. In Bezug auf die Aufbauorganisation des Informationssicherheitsmanagements bieten sich verschiedene Möglichkeiten an. Dabei richtet sich die personelle Ausgestaltung 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.

Bei der Definition von Rollen im Informationsmanagement sind die nachfolgenden Grundregeln zu beachten:

1. Die Gesamtverantwortung für die Informationssicherheit verbleibt bei der Leitungsebene.
2. Es muss mindestens eine Person benannt werden, die den Informationssicherheitsprozess fördert und koordiniert, typischerweise als Informationssicherheitsbeauftragter (ISB).
3. Jeder Mitarbeiter ist gleichermaßen für seine originäre Aufgabe wie für die Aufrechterhaltung der Informationssicherheit an seinem Arbeitsplatz und in seiner Umgebung verantwortlich.

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

7.3 Umsetzung der Leitlinie zur Informationssicherheit

Um die gesetzten Sicherheitsziele zu erreichen, muss zunächst ein Sicherheitskonzept erstellt werden. Zur besseren Übersichtlichkeit wird in einem eigenen Kapitel dargestellt, wie ein Sicherheitskonzept geplant, umgesetzt und das Informationssicherheitsniveau aufrechterhalten und verbessert werden kann. Die Ergebnisse der Überprüfung der Sicherheitsmaßnahmen gehen dann in die Erfolgskontrolle des Sicherheitsprozesses ein und werden von der Leitungsebene bewertet.

7.4 Aufrechterhaltung der Informationssicherheit

Die Schaffung von Informationssicherheit ist kein zeitlich begrenztes Projekt, sondern ein kontinuierlicher Prozess. Die Angemessenheit und Wirksamkeit aller Elemente des Managementsystems für die Informationssicherheit müssen regelmäßig überprüft werden. Das bedeutet, dass nicht nur einzelne Sicherheitsmaßnahmen überprüft werden müssen, sondern auch die Sicherheitsstrategie regelmäßig überdacht werden muss.

Die Umsetzung der Sicherheitsmaßnahmen sollte in regelmäßigen Abständen mithilfe von internen Audits ausgewertet werden. Diese dienen auch dazu, die Erfahrungen aus der täglichen Praxis zusammenzutragen und auszuwerten. Neben Audits ist die Durchführung von Übungen und Sensibilisierungsmaßnahmen notwendig, da nur so festgestellt werden kann, ob alle vorgesehenen Abläufe und das Verhalten in Notfallsituationen auch tatsächlich funktionieren. Erkenntnisse über Schwachstellen und Verbesserungsmöglichkeiten müssen ohne Ausnahme zu Konsequenzen in der Sicher-

heitsorganisation führen. Zudem ist es wichtig, zukünftige Entwicklungen sowohl bezüglich der eingesetzten Technik als auch in Geschäftsprozessen und Organisationsstrukturen frühzeitig zu erkennen, um potenzielle Gefährdungen rechtzeitig identifizieren, Vorkehrungen treffen und Sicherheitsmaßnahmen umsetzen zu können. Wenn sich wesentliche Änderungen in Geschäftsprozessen oder Organisationsstrukturen abzeichnen, muss hier das Informationssicherheitsmanagement eingebunden werden. Der ISB muss auch proaktiv tätig werden: Auch wenn die Einbindung des Informationssicherheitsmanagements in den Organisationsverfügungen vorgesehen ist, sollte dieses nicht darauf warten, dass es wie geplant involviert wird, sondern sich rechtzeitig eigenständig in die entsprechenden Prozesse einmischen.

Bei allen Audits sollte darauf geachtet werden, dass sie nicht von denjenigen durchgeführt werden, die an der Planung oder Konzeption von Sicherheitsvorgaben beteiligt waren, da es schwierig ist, eigene Fehler zu finden. Je nach Größe der Institution kann es hilfreich sein, für Audits Externe hinzuzuziehen, um eine gewisse Betriebsblindheit zu vermeiden.

Auch für kleine und mittlere Institutionen ist die Aufrechterhaltung der Informationssicherheit ein wichtiger Punkt. Die Audits werden zwar weniger umfangreich als in großen Institutionen sein, dürfen aber auf keinen Fall unterbleiben. Im Rahmen der jährlichen Managementbewertung muss von der obersten Leitungsebene auch überprüft werden, ob es neue gesetzliche Vorgaben gibt, die beachtet werden müssen, oder ob sich sonstige Rahmenbedingungen geändert haben.

7.5 Kontinuierliche Verbesserung der Informationssicherheit

Die Überprüfung des Sicherheitsprozesses dient letztendlich dessen Verbesserung. Die Ergebnisse sollten vor diesem Hintergrund dazu genutzt werden, die Wirksamkeit und Effizienz der gewählten Sicherheitsstrategie zu beurteilen und eventuell anzupassen. Auch bei Veränderungen der Sicherheitsziele oder der Rahmenbedingungen muss die Sicherheitsstrategie überarbeitet werden.

8 Sicherheitskonzept

8.1 Erstellung des Sicherheitskonzepts

Um die Informationssicherheitsziele zu erfüllen und das angestrebte Sicherheitsniveau zu erreichen, muss zunächst verstanden werden, wie die Erfüllung von Aufgaben und Geschäftsprozessen von der Vertraulichkeit, Integrität und Verfügbarkeit der Informationen abhängt. Dazu muss man auch berücksichtigen, durch welche Schadensursachen, wie zum Beispiel höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen oder auch Cyberrisiken, Geschäftsprozesse bedroht werden. Danach muss eine Entscheidung erfolgen, wie mit diesen Risiken umgegangen werden soll. Im Einzelnen sind nachfolgende Teilschritte notwendig:

Auswahl einer Methode zur Risikoanalyse [DOK]

Die Risiken, die durch Schäden für die Geschäftstätigkeit und Aufgaben einer Institution durch Sicherheitsvorfälle entstehen können, müssen analysiert werden. Eine Methode zur Risikoanalyse ist daher Bestandteil jedes Managementsystems für Informationssicherheit. Um ein Risiko bestimmen zu können, müssen die Bedrohungen ermittelt, deren Schadenspotenzial und Eintrittswahrscheinlichkeit eingeschätzt und diese der Risikoakzeptanz der Institution gegenübergestellt werden. Je nach Anwendungsfall, organisatorischen Randbedingungen, Branchenzugehörigkeit sowie angestrebtem Sicherheitsniveau kommen unterschiedliche Methoden zur Risikoanalyse infrage. Das Informationssicherheitsmanagement muss eine Methode auswählen, die für die Art und Größe der Institution angemessen ist. Die Methodenwahl beeinflusst den Arbeitsaufwand für die Erstellung des Sicherheitskonzepts entscheidend.

Verschiedene Arten der Risikobeurteilung sind in den Standards ISO/IEC 31010 und ISO/IEC 27005 beschrieben. Das BSI hat hieraus abgeleitet ein zweistufiges Verfahren entwickelt. In der Vorgehensweise nach IT-Grundschutz wird bei der Erstellung der IT-Grundschutz-Bausteine implizit eine Risikobewertung für typische Einsatzbereiche mit normalem Schutzbedarf durchgeführt. Hierbei werden nur solche Gefährdungen betrachtet, die nach sorgfältiger Analyse eine so hohe Eintrittshäufigkeit oder so einschneidende Auswirkungen haben, dass Sicherheitsmaßnahmen ergriffen werden müssen. Typische Gefährdungen, gegen die sich jeder schützen muss, sind z. B. Schäden durch Feuer, Wasser, 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 vorab vom BSI 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.

Daher wird das weiter oben beschriebene Vorgehen bei normalem Schutzbedarf durch den im BSI-Standard 200-3 *Risikoanalyse auf der Basis von IT-Grundschutz* (siehe [BSI3]) beschriebenen Ansatz ergänzt.

Die Anwendung des IT-Grundschatzes hat den Vorteil, dass der eigene Arbeitsaufwand deutlich reduziert wird, weil im Rahmen des IT-Grundschatzes bereits eine konkrete Methode beschrieben wird und geeignete Sicherheitsanforderungen sowie Sicherheitsmaßnahmen vorgeschlagen werden.



Abbildung 6: Überblick über den Lebenszyklus eines Sicherheitskonzepts

Klassifikation von Risiken bzw. Schäden [DOK]

Das Informationssicherheitsmanagement muss in Abhängigkeit von der gewählten Methode zur Risikoanalyse festlegen, wie Bedrohungen, Schadenspotenziale, Eintrittshäufigkeiten eingeschätzt und die daraus resultierenden Risiken bewertet werden. Allerdings ist es schwierig, aufwendig und zudem fehleranfällig, für Schäden und Eintrittshäufigkeiten individuelle Werte zu ermitteln. Es empfiehlt sich, nicht zu viel Zeit in die exakte Bestimmung von Eintrittshäufigkeiten und mögliche Schäden zu stecken. In den meisten Fällen ist es sowohl für die Eintrittshäufigkeit als auch für die potenzielle Schadenshöhe praktikabler, mit qualitativen Kategorien zu arbeiten. Hierbei sollten pro Dimension nicht mehr als fünf Kategorien gewählt werden, z. B.

- Eintrittswahrscheinlichkeit: selten, mittel, häufig, sehr häufig
- Potenzielle Schadenshöhe: vernachlässigbar, begrenzt, beträchtlich, existenzbedrohend

Nachdem solche Kategorien in geeigneter Art und Weise innerhalb der Institution definiert wurden, können diese als Grundlage für eine qualitative Risikobetrachtung verwendet werden.

Risikoanalyse [DOK]

Jede Risikoanalyse muss die folgenden Schritte umfassen:

- Die zu schützenden Informationen und Geschäftsprozesse müssen identifiziert werden.
- Alle relevanten Bedrohungen für die zu schützenden Informationen und Geschäftsprozesse müssen ermittelt werden.
- Schwachstellen, durch welche die Bedrohungen wirken könnten, müssen analysiert werden.
- Die möglichen Schäden durch den Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit müssen benannt und eingeschätzt werden.
- Die anzunehmenden Auswirkungen auf die Geschäftstätigkeit oder die Aufgabenerfüllung durch Sicherheitsvorfälle müssen untersucht werden.
- Das Risiko, durch Sicherheitsvorfälle Schäden zu erleiden, muss bewertet werden.

Die hier verwendeten Begriffe „Bedrohung“, „Schwachstelle“ und „Risiko“ werden im Glossar näher definiert und sind dort entsprechend nachzuschlagen.

Entwicklung einer Strategie zur Behandlung von Risiken [DOK]

Die oberste Leitungsebene muss vorgeben, wie die erkannten Risiken behandelt werden sollen. Abhängig vom Risikoappetit einer Institution sind jeweils unterschiedliche Risikoakzeptanzkriterien möglich. „Risikoappetit“ bezeichnet die durch kulturelle, interne, externe oder wirtschaftliche Einflüsse entstandene Neigung einer Institution im Hinblick darauf, wie diese Risiken bewertet und mit ihnen umgeht. Die erkannten Risiken müssen vom Informationssicherheitsmanagement entsprechend aufbereitet werden. Dazu gibt es folgende Optionen: Risiken können

- vermieden werden, beispielsweise indem die Risikoursache ausgeschlossen wird,
- reduziert werden, indem die Rahmenbedingungen, die zur Risikoeinstufung beigetragen haben, modifiziert werden,
- transferiert werden, indem die Risiken mit anderen Parteien geteilt werden, z. B. durch Outsourcing oder Versicherungen,
- akzeptiert werden (auf Basis einer nachvollziehbaren Faktenlage), beispielsweise weil die mit dem Risiko einhergehenden Chancen wahrgenommen werden sollen.

Die Art des Umgangs mit Risiken muss dokumentiert, einem Risikoeigentümer zugeordnet und von der obersten Leitungsebene genehmigt werden. Die notwendigen Ressourcen zur Umsetzung der Strategie müssen geplant und zur Verfügung gestellt werden.

Bei der Ausgestaltung der Strategie ist neben den Kosten das verbleibende Restrisiko ein wesentliches Entscheidungskriterium, das von der Leitungsebene berücksichtigt werden muss.

In der Praxis werden die Schritte der Risikoeinstufung und Risikobehandlung 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 („**Risiko-Akzeptanz**“) vorgelegt werden. Damit wird nachvollziehbar dokumentiert, dass die Institution sich des Restrisikos bewusst ist.

Im Rahmen der Risikobewertung ergeben sich meist Risiken, die oberhalb der Risikoakzeptanzlinie (siehe BSI-Standard 200-3) liegen und daher behandelt werden müssen. Im Folgenden wird die Risikobehandlungsoption „Reduktion durch Umsetzung von Sicherheitsmaßnahmen“ näher betrachtet.

Auswahl von Sicherheitsmaßnahmen [DOK]

Aus den allgemeinen Sicherheitszielen und Sicherheitsanforderungen, die die Leitungsebene vorgegeben hat, leiten sich konkrete Sicherheitsmaßnahmen ab. Bei der Auswahl von Sicherheitsmaßnahmen sind neben den Auswirkungen auf das Sicherheitsniveau auch Kosten-Nutzen-Aspekte und die Praxistauglichkeit zu beachten.

Neben technischen Sicherheitsmaßnahmen müssen auch organisatorische Abläufe und Prozesse (wie Benutzerrichtlinien, Rechtevergaben, Sicherheitsschulungen, Test- und Freigabeverfahren) eingerichtet werden. Es müssen dabei unter anderem die folgenden Themen geregelt werden:

- Organisation (inklusive Festlegung von Zuständigkeiten, Aufgabenverteilung und Funktionstrennung, Regelung des Umgangs mit Informationen, Anwendungen und IT-Komponenten, Hard- und Software-Management, Änderungsmanagement usw.),
- Personal (z. B. Einweisung neuer Mitarbeiter, Vertretungsregelungen usw.),
- Schulung und Sensibilisierung zur Informationssicherheit,
- Identitäts- und Berechtigungsmanagement,
- Datensicherung (für alle Informationen, Anwendungen und IT-Komponenten),
- Compliance und Datenschutz,
- Schutz vor Schadprogrammen,
- Schutz von Informationen bei Verarbeitung, Übertragung und Speicherung (z. B. durch Einsatz von Kryptografie),
- Hard- und Softwareentwicklung,
- Detektion von Sicherheitsvorfällen,
- Verhalten bei Sicherheitsvorfällen (englisch: „incident handling“),
- Sicherheitsüberprüfungen (Audits und Revisionen, Penetrationstests usw.),
- Notfallvorsorge und Aufrechterhaltung der Geschäftstätigkeit im Notfall (englisch: „business continuity“),
- Löschen und Vernichten von Daten und
- Outsourcing bzw. Cloud Computing.

Es muss nachvollziehbar dokumentiert werden, warum die ausgewählten Maßnahmen geeignet sind, die Sicherheitsziele und -anforderungen zu erreichen.

8.2 Umsetzung des Sicherheitskonzepts

Nach der Auswahl von Sicherheitsmaßnahmen müssen diese nach einem Realisierungsplan umgesetzt werden. Bei der Umsetzung sollten die folgenden Schritte eingehalten werden:

Erstellung eines Realisierungsplans für das Sicherheitskonzept [DOK]

Ein Realisierungsplan muss folgende Themen enthalten:

- Festlegung von Prioritäten (Umsetzungsreihenfolge),
- Festlegung von Verantwortlichkeiten für Initiierung,
- Bereitstellung von Ressourcen durch das Management und
- Umsetzungsplanung einzelner Maßnahmen (Festlegung von Terminen und Kosten, Festlegung von Verantwortlichen für die Realisierung sowie von Verantwortlichen für die Kontrolle der Umsetzung bzw. der Effektivität von Maßnahmen).

Umsetzung der Sicherheitsmaßnahmen

Die geplanten Sicherheitsmaßnahmen müssen gemäß dem Realisierungsplan umgesetzt werden. Informationssicherheit muss dabei in die organisationsweiten Abläufe und Prozesse integriert werden. Falls sich bei der Umsetzung Schwierigkeiten ergeben, sollten diese sofort kommuniziert werden, damit überlegt werden kann, wie diese behoben werden können. Als typische Lösungswege könnten beispielsweise sowohl Kommunikationswege oder Rechtezuweisungen geändert als auch technische Verfahren angepasst werden.

Steuerung und Kontrolle der Umsetzung [DOK]

Die Einhaltung der Zielvorgaben muss regelmäßig überprüft werden. Falls Zielvorgaben nicht eingehalten sind, ist das für die Informationssicherheit zuständige Mitglied der Leitungsebene zu informieren, um auf Probleme rechtzeitig reagieren zu können.

8.3 Erfolgskontrolle des Sicherheitskonzepts

Zur Aufrechterhaltung des Sicherheitsniveaus müssen einerseits die als angemessen identifizierten Sicherheitsmaßnahmen korrekt angewendet und andererseits muss das Sicherheitskonzept fortlaufend aktualisiert werden. Darüber hinaus ist es wichtig, Sicherheitsvorfälle rechtzeitig zu entdecken und schnell und adäquat auf diese zu reagieren. Es muss regelmäßig eine Erfolgskontrolle des Sicherheitskonzepts durchgeführt werden. Die Analyse der Effektivität und Effizienz der umgesetzten Maßnahmen sollte im Rahmen von internen Audits erfolgen. Wenn nicht genügend Ressourcen zur Verfügung stehen, um solche Audits von erfahrenen internen Mitarbeitern durchführen zu lassen, sollten externe Experten mit der Durchführung von Prüfungsaktivitäten beauftragt werden.

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

Im Einzelnen sollten die folgenden Aktivitäten durchgeführt werden:

Reaktion auf Änderungen im laufenden Betrieb

Bei Änderungen im laufenden Betrieb (z. B. Einführung neuer Geschäftsprozesse, Organisationsänderungen oder Einsatz neuer IT-Systeme) müssen das Sicherheitskonzept sowie die damit verbundenen Dokumente (wie auch die Liste der Zuständigkeiten oder der IT-Systeme) aktualisiert werden.

Detektion von Sicherheitsvorfällen im laufenden Betrieb [DOK]

Es müssen bestimmte Maßnahmen umgesetzt werden, um Fehler in der Informationsverarbeitung, welche die Vertraulichkeit, Verfügbarkeit oder Integrität beeinträchtigen können, sicherheitskritische Fehlhandlungen und Sicherheitsvorfälle möglichst zu verhindern, in ihrer Auswirkung zu begrenzen oder zumindest frühzeitig zu bemerken. Die Behandlung von Fehlern muss dokumentiert werden. Dazu gehört, dass die ergriffenen Maßnahmen, die Auswirkungen und möglicherweise resultierende Folgemaßnahmen festgehalten werden. Zur frühzeitigen Erkennung von Sicherheitsproblemen können beispielsweise Tools zu System- und Netzüberwachungen, Integritätsprüfungen, die Protokollierung von Zugriffen, Aktionen oder Fehlern, die Kontrolle des Zutritts zu Gebäuden und Räumen oder Brand-, Wasser- bzw. Klimasensoren beitragen.

Die Aufzeichnungen und Protokolle der Detektionsmaßnahmen müssen regelmäßig ausgewertet werden.

Überprüfung der Einhaltung von Vorgaben [DOK]

Es muss eine regelmäßige Prüfung stattfinden, ob alle Sicherheitsmaßnahmen wie im Sicherheitskonzept vorgesehen angewendet und durchgeführt werden. Hierbei muss sowohl die Einhaltung der technischen Sicherheitsmaßnahmen (z. B. hinsichtlich der Konfiguration) als auch die der organisatorischen Regelungen (z. B. Prozesse, Verfahren und Abläufe) kontrolliert werden. Es sollte auch eine Überprüfung erfolgen, ob die notwendigen Ressourcen zur korrekten Umsetzung der Maßnahmen zur Verfügung stehen und alle Personen, denen bestimmte Rollen zur Umsetzung von Sicherheitsmaßnahmen zugewiesen wurden, ihren Verpflichtungen nachkommen.

Überprüfung der Eignung und Wirksamkeit von Sicherheitsmaßnahmen [DOK]

Es muss regelmäßig geprüft werden, ob die Sicherheitsmaßnahmen geeignet sind, die gesetzten Sicherheitsziele zu erreichen. Zur Überprüfung auf ihre Eignung können z. B. zurückliegende Sicherheitsvorfälle ausgewertet, Mitarbeiter befragt oder Penetrationstests durchgeführt werden. Dazu gehört es auch, relevante Entwicklungen im Umfeld der Geschäftsprozesse oder Fachaufgaben der Institution zu verfolgen. Beispielsweise könnten sich technische oder regulatorische Rahmenbedingungen geändert haben. Um sich auf dem aktuellen Stand zu halten, sollten die Sicherheitsverantwortlichen beispielsweise externe Wissensquellen nutzen, Fachkonferenzen besuchen sowie Standards, Fachliteratur und Informationen aus dem Internet auswerten. Wenn intern nicht das erforderliche Wissen oder die Zeit dazu vorhanden ist, sollten externe Experten hinzugezogen werden.

In diesem Zusammenhang erscheint es zudem sinnvoll, kritisch zu hinterfragen, ob die eingesetzten Sicherheitsmaßnahmen effizient sind oder die Sicherheitsziele mit anderen Maßnahmen ressourcenschonender erreicht werden könnten. Dabei ist auch zu prüfen, ob Prozesse und organisatorische Regelungen praxistauglich und effizient sind. Häufig ergibt sich hieraus die Gelegenheit, notwendige Organisationsverbesserungen und Restrukturierungen vorzunehmen.

Managementbewertungen [DOK]

Die Leitungsebene muss vom Informationssicherheitsmanagement regelmäßig in angemessener Form Ergebnisse der Überprüfungen erhalten. Dabei sollten Probleme, Erfolge und Verbesserungsmöglichkeiten aufgezeigt werden.

Die Managementberichte müssen alle für die Leitungsebene notwendigen Informationen zur Steuerung des Sicherheitsprozesses beinhalten. Solche Informationen sind beispielsweise:

- Übersicht über den aktuellen Status im Sicherheitsprozess,
- Begutachtung von Folgemaßnahmen vorangegangener Managementbewertungen,
- Rückmeldungen von Kunden und Mitarbeitern sowie
- Überblick über neu aufgetretene Bedrohungen und Sicherheitslücken.

Die Leitungsebene nimmt die Managementberichte zur Kenntnis und trifft die notwendigen Entscheidungen, wie beispielsweise zur Verbesserung des Sicherheitsprozesses, zum Ressourcenbedarf sowie zu den Ergebnissen von Sicherheitsanalysen (z. B. Reduzierung oder Akzeptanz von Risiken).

8.4 Kontinuierliche Verbesserung des Sicherheitskonzepts

Die regelmäßige Überprüfung des Sicherheitskonzepts dient dazu, erkannte Fehler und Schwachstellen abzustellen und die Sicherheitsmaßnahmen in Bezug auf Effizienz zu optimieren.

Ein wichtiger Punkt ist die Verbesserung der Praxistauglichkeit von technischen Maßnahmen und organisatorischen Abläufen, um die Akzeptanz der Sicherheitsmaßnahmen zu erhöhen. Ebenso sollten die Formulierungen geeigneter Sicherheitsmaßnahmen immer wieder auch hinsichtlich ihrer Nachvollziehbarkeit und Verständlichkeit beurteilt und gegebenenfalls modifiziert werden.

9 Zertifizierung des ISMS

Der erfolgreiche Aufbau und Betrieb eines ISMS ist keine einfache Aufgabe. Wenn diese erfolgreich durchgeführt wurde, bietet es sich an, dies auch nach innen und außen zu dokumentieren und die erfolgreichen Bemühungen um Informationssicherheit transparent zu machen. Dies kann sowohl gegenüber Kunden als auch gegenüber Geschäftspartnern als Qualitätsmerkmal dienen und somit durchaus auch zu einem Wettbewerbsvorteil führen. Aber auch Behörden können diesen Mechanismus nutzen, um das Vertrauen der Bürger in die Sicherheit ihrer Geschäftsprozesse und die zugehörige IT – insbesondere im Bereich E-Government – zu verbessern. Ein weiterer Grund, um eine Zertifizierung anzustreben, kann sich aus Compliance-Gründen ergeben, also um nachzuweisen, dass einschlägige Gesetze oder vertragliche Anforderungen erfüllt werden. Darüber hinaus ergibt sich häufig ein „passiver“ Nutzen, da andere Institutionen ein ISMS-Zertifikat heranziehen können, um sich über den Sicherheitszustand bei potenziellen Partnern zu informieren.

Die ISO/IEC 27001 ist die grundlegende Norm, auf deren Basis ein ISMS zertifiziert werden kann. Sie sieht ein zweistufiges Zertifizierungsverfahren vor: Hierbei werden die Zertifikate durch unabhängige Zertifizierungsstellen erteilt. Der Erteilung eines Zertifikates geht eine Überprüfung durch einen qualifizierten Auditor voraus.

Damit die Ergebnisse der Zertifizierungsaudits wiederholbar und reproduzierbar sind, werden erfahrene und geschulte Auditoren benötigt. Daher müssen Auditoren nachweisen, dass sie über das erforderliche Fachwissen verfügen und das vorgegebene Schema kennen und einhalten. All dies erfolgt auf der Basis weiterer ISO-Normen, um die hohe Qualität und Nachvollziehbarkeit von Zertifikaten sicherzustellen.

Die Standard- und die Kern-Absicherung des IT-Grundschutzes bilden die Anforderungen der ISO/IEC 27001 ab. Daher besteht auch die Möglichkeit, sich die erfolgreiche Umsetzung des IT-Grundschutzes mit dem Aufbau eines ISMS durch das BSI zertifizieren zu lassen. Das BSI hat ein Zertifizierungsschema für Informationssicherheit entwickelt, das die Anforderungen an Managementsysteme für die Informationssicherheit aus der ISO/IEC 27001 berücksichtigt. Das IT-Grundschutz-Kompendium bildet den Prüfkatalog für die Zertifizierung nach ISO/IEC 27001. Diese wird deshalb als ISO 27001-Zertifizierung auf der Basis des IT-Grundschutzes bezeichnet. Das IT-Grundschutz-Kompendium als Prüfkatalog wird vom BSI (im Gegensatz zu anderen Zertifizierungsstellen) kostenfrei zur Verfügung gestellt.

Grundlage für die Vergabe eines ISO 27001-Zertifikats auf der Basis des IT-Grundschutzes 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 dann wiederum über die Vergabe des ISO 27001-Zertifikats auf der Basis des IT-Grundschutzes entscheidet.

Weitere Informationen zur Zertifizierung nach ISO/IEC 27001 finden sich auf der Website des BSI (siehe [ZERT]).

10 Das ISMS auf Basis von BSI IT-Grundschutz

10.1 IT-Grundschutz-Methodik

Die Beschreibungen eines Managementsystems für Informationssicherheit sind in diesem Dokument und auch in den ISO-Normen 27000, 27001 und 27002 sehr generisch gehalten und geben lediglich einen Rahmen vor. In der Praxis besteht daher ein großer Gestaltungsspielraum bei der praktischen Umsetzung der generischen Vorgaben. Die große Herausforderung besteht darin, in der eigenen Institution ein ISMS zu etablieren, das nicht nur hilft, die gesteckten Sicherheitsziele zu erreichen, sondern auch noch kostengünstig und somit wirtschaftlich ist.

Dabei ist die Frage, wie ein Sicherheitskonzept für die Institution zu erstellen ist, meist am schwierigsten zu lösen. Die zentralen Arbeitsschritte bei der Erstellung eines Sicherheitskonzepts sind dabei die Risikobeurteilung und die Auswahl der richtigen Sicherheitsmaßnahmen. Der Wahl der Methode zur Risikoanalyse kommt dabei eine besondere Bedeutung zu, da die Methodenwahl den Arbeitsaufwand für die Erstellung des Sicherheitskonzepts entscheidend beeinflusst. Die IT-Grundschutz-Methodik beschreibt unterschiedliche Vorgehensweisen, die für die meisten Anwendungsfälle geeignet sind. Abhängig vom angestrebtem Sicherheitsniveau und der zu sichernden Informationen ist ein abgestufter Einstieg in ein Sicherheitsmanagement möglich. Der IT-Grundschutz ist dabei im Vergleich zur klassischen quantitativen Risikoanalyse weitaus kostengünstiger sowie seit vielen Jahren praxiserprobt. Als Mehrwert wird in der IT-Grundschutz-Methodik nicht nur beschrieben, wie ein ISMS grundsätzlich funktioniert, sondern zusammen mit dem IT-Grundschutz-Kompendium wird auch geschildert, welche Sicherheitsanforderungen in der Praxis erfüllt werden sollten. Praktische Erläuterungen, wie die Anforderungen der Bausteine des IT-Grundschutz-Kompendiums erfüllt werden können, sind in den entsprechenden Umsetzungshinweisen zum IT-Grundschutz zu finden.

Wie bereits weiter oben erwähnt, umfasst die IT-Grundschutz-Methodik verschiedene Vorgehensweisen zur Ausgestaltung der Informationssicherheit. Die Anwendung der Vorgehensweise der Basis-Absicherung bietet speziell für kleine und mittelständische Institutionen einen ersten Einstieg in die Informationssicherheit und hilft, ein schlankes ISMS („Bonsai-ISMS“) aufzubauen. Anders als bei der Standard-Absicherung bilden die Aktionsfelder bei der Basis-Absicherung keinen geschlossenen Zyklus, sondern sind eine Einstiegsvorgehensweise, die mit der Standard-Absicherung fortgeführt werden kann.

Dieses Kapitel gibt eine Einführung in die wesentlichen Elemente der IT-Grundschutz-Methodik und zeigt auf, dass ein Vorgehen nach IT-Grundschutz vollständig kompatibel zum Standard ISO/IEC 27001 (siehe [27001]) ist. Eine ausführliche Darstellung der Vorgehensweisen nach dem IT-Grundschutz kann dem BSI-Standard 200-2 *IT-Grundschutz-Methodik* (siehe [BSI2]) entnommen werden.

Die IT-Grundschutz-Methodik beschreibt einen Anwendungsansatz für die Etablierung und Aufrechterhaltung eines Managementsystems für Informationssicherheit, basierend auf den IT-Grundschutz-Vorgehensweisen und dem IT-Grundschutz-Kompendium. Dort werden die hier erwähnten Themen ausführlicher und praxisbezogener dargestellt als im vorliegenden Dokument.

10.2 Der Sicherheitsprozess nach IT-Grundschutz

Alle gängigen Methoden, Best Practices und Standards zum Management von Informationssicherheit unterscheiden sich kaum in den Ausführungen, die sich mit dem Sicherheitsprozess oder den Aufgaben des leitenden Managements beschäftigen. Die größten Unterschiede bestehen in der Art und

Weise, wie ein Sicherheitskonzept konkret erstellt wird, also bei der Ausgestaltung der Risikobeurteilung und der Auswahl der Sicherheitsmaßnahmen. Aus diesem Grund wird an dieser Stelle das grundsätzliche Vorgehen bei der Erstellung eines Sicherheitskonzepts nach IT-Grundschutz dargestellt.

10.2.1 Integrierte Risikobewertung im IT-Grundschutz

Eine Risikoanalyse in der Informationssicherheit unterscheidet sich in wesentlichen Punkten von klassischen Methoden der Versicherungsmathematik oder des Controllings. Die exakte Berechnung von Schadenshöhen und Eintrittswahrscheinlichkeiten bei einer „klassischen“ oder quantitativen Risikoanalyse ist meistens nicht möglich, da geeignetes Zahlenmaterial fehlt. Selbst wenn eine Berechnung möglich ist, bleibt die Interpretation der Ergebnisse sehr schwierig.

Beispiel:



Bei der klassischen Risikoanalyse berechnet sich das Risiko aus der Schadenshöhe multipliziert mit der Eintrittswahrscheinlichkeit. Wenn also die Zerstörung eines Rechenzentrums durch einen Flugzeugabsturz 20 Millionen € kostet und statistisch ein einziges Mal in 20.000 Jahren passiert, beträgt das theoretische Risiko 1.000,- € pro Jahr. Das gleiche Risiko ergibt sich, wenn der Schaden beim Diebstahl eines Notebooks (ohne Datenverlust) mit 2.000,- € angesetzt wird und dieser rechnerisch ein einziges Mal in zwei Jahren eintritt. Obwohl das Risiko rein rechnerisch im Wert übereinstimmt, müssen diese beiden Schadensszenarien im Rahmen des Risikomanagements völlig unterschiedlich behandelt werden.

In der IT-Grundschutz-Methodik ist daher bereits ein qualitatives Verfahren zur Risikobewertung enthalten, das die notwendigen Informationen zur Beurteilung von geschäftsschädigenden Sicherheitsvorfällen liefert und, im Vergleich zum quantitativen Verfahren, leichter im Umgang sowie für alle betrachteten Fälle ausreichend ist. Im IT-Grundschutz wird davon ausgegangen, dass unabhängig von der Art und Ausrichtung einer Institution überall geschäftsrelevante Informationen sicher verarbeitet werden müssen, gängige und damit vergleichbare IT-Systeme eingesetzt werden und vergleichbare Umfeldbedingungen existieren. Damit liegen meistens vergleichbare Bedrohungen vor. Die Sicherheitsanforderungen der Geschäftsprozesse und Fachanwendungen sind zwar individuell und können unterschiedlich sein, in der Praxis führen sie jedoch meist zu ähnlichen und vergleichbaren Sicherheitsanforderungen.

Das BSI analysiert für die IT-Grundschutz-Methodik im IT-Grundschutz-Kompendium Bedrohungen und Schwachstellen für typische Einsatzfelder und Komponenten und ermittelt daraus die resultierenden Gefährdungen. Dabei werden nur solche Gefährdungen betrachtet, die nach 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, Schadprogramme oder Hardware-Defekte. Dieser Ansatz hat den Vorteil, dass Anwender des IT-Grundschutzes für einen Großteil des Informationsverbundes keine Bedrohungs- und Schwachstellenanalyse durchführen oder Eintrittswahrscheinlichkeiten berechnen müssen, weil ihnen das BSI diese Arbeit bereits abgenommen hat.

Auf Basis der elementaren Gefährdungen sowie der ermittelten spezifischen Gefährdungen beschreibt das IT-Grundschutz-Kompendium bewährte technische, infrastrukturelle, personelle und organisatorische Basis- und Standard-Anforderungen sowie Anforderungen bei erhöhtem Schutzbedarf zur Absicherung typischer Objekte.

Für Informationen und Geschäftsprozesse mit einem hohen oder sehr hohen Schutzbedarf oder für Einsatzumgebungen, die im IT-Grundschutz nicht behandelt werden, muss eine Risikoanalyse durchgeführt werden. Eine vereinfachte Risikoanalyse nach der IT-Grundschutz-Methodik wird im BSI-Standard 200-3 *Risikoanalyse auf der Basis von IT-Grundschutz* (siehe [BSI3]) beschrieben.

Sowohl die Risikobewertung nach IT-Grundschutz als auch die in [BSI3] dargestellte Risikoanalyse sind deutlich einfacher und kostengünstiger als eine quantitative Risikoanalyse. Die Risikobewertung nach IT-Grundschutz bietet zudem den Vorteil, dass auch Institutionen aus den verschiedensten Branchen, die nach dieser Methode vorgehen, eine gemeinsame und klar definierte Grundlage für ihre Risikobewertung vorweisen können.

Klassifikation von Risiken

Die allgemeine Anforderung, Risiken zu klassifizieren, wird im IT-Grundschutz in folgenden Schritten durchgeführt:

1. Orientierung an Schadensszenarien

Um Schäden und negative Auswirkungen von Sicherheitsvorfällen möglichst anschaulich zu beschreiben, sollten verschiedene Schadensszenarien betrachtet werden, z. B. die nachfolgenden:

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

Beim Durchspielen der Szenarien sollte dabei untersucht werden, welche Schäden beim Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit entstehen können.

Beispielsweise sollte für das Szenario „Verstoß gegen Gesetze“ unter anderem erörtert werden, welche Daten aufgrund gesetzlicher Auflagen vertraulich behandelt werden müssen und welche Konsequenzen ein fahrlässiger Verstoß gegen diese Auflagen hätte.

2. Klassifizierung von Schäden: Definition von Schutzbedarfskategorien

Meist ist eine exakte Berechnung von potenziellen Schäden nicht sinnvoll oder sogar unmöglich und für die Auswahl geeigneter Sicherheitsmaßnahmen auch nicht nötig. Daher empfiehlt sich eine Einteilung von Schäden in wenige Klassen. Der Versuch einer „exakten“ Schadensberechnung gefährdet in vielen Fällen sogar die Sicherheit, da eine nicht zutreffende Genauigkeit suggeriert wird und die Verantwortlichen dadurch nur von einer „Scheinsicherheit“ ausgehen.

Ausgehend von möglichen Schäden, werden im Rahmen des IT-Grundschutzes drei Schutzbedarfskategorien vorgeschlagen, in die später die Schutzobjekte (z. B. IT-Systeme) eingeordnet werden:

„normaler Schutzbedarf“: Die Schadensauswirkungen sind begrenzt und überschaubar.

„hoher Schutzbedarf“: Die Schadensauswirkungen können beträchtlich sein.


„sehr hoher Schutzbedarf“: Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Jede Institution muss für jedes Schadensszenario individuell festlegen, wie „normal“, „hoch“ und „sehr hoch“ im Einzelfall zu interpretieren sind, welche Rahmenbedingungen für die Einteilung in

die Schutzbedarfskategorien also zugrunde zu legen sind. Da dies unmittelbare Auswirkungen auf den Umgang mit Risiken und den Bedarf an Ressourcen hat, muss diese Festlegung durch die oberste Leitungsebene der Institution erfolgen. Die Festlegung der Schutzbedarfskategorien kann je nach Art und Größe der Institution sehr unterschiedlich sein und nur die oberste Leitungsebene kann diese in Zusammenarbeit mit dem Sicherheitsmanagement konkret bestimmen. Das BSI kann daher nur Beispiele für entsprechende Werte nennen, die an die jeweiligen Bedingungen anzupassen sind.

Institutionen können auch andere Schutzbedarfskategorien verwenden. Um dann weiter mit dem IT-Grundschutz arbeiten zu können, muss überlegt werden, wie die individuellen Schutzbedarfskategorien auf die des IT-Grundschutzes abgebildet werden können. Dies kann auch dazu führen, dass Anforderungen aus den IT-Grundschutz-Bausteinen in andere Kategorien fallen.

Beispiel für die Klassifizierung finanzieller Schäden:

 *Ein normaler Schutzbedarf ist gegeben, wenn ein finanzieller Schaden für die Institution tolerabel ist. Bei einem kleinen Betrieb kann dies beispielsweise bedeuten, dass durch Sicherheitsvorfälle keine Schäden über 10.000,- € entstehen dürfen. Ein hoher Schutzbedarf besteht, wenn ein Schaden beachtliche finanzielle Verluste nach sich zieht, jedoch nicht existenzbedrohend ist. Bei einem kleinen Betrieb kann dies Summen zwischen 10.000,- € und 100.000,- € bedeuten. Ein sehr hoher Schutzbedarf liegt dann vor, wenn der finanzielle Schaden für die Institution existenzbedrohend ist. Bei einem kleinen Betrieb könnte dies bereits bei einem Schadenspotenzial von über 100.000,- € gegeben sein. Bei einer großen Geschäftsbank ergeben sich hier natürlich ganz andere Werte.*


10.2.2 Sicherheitskonzeption

Der IT-Grundschutz bietet neben der Standard-Absicherung zwei weitere Vorgehensweisen zum Einstieg in die Informationssicherheit an (Basis- und Kern-Absicherung). Die Vorgehensweise nach IT-Grundschutz ermöglicht eine Hilfestellung beim Aufbau und Betrieb sowie der Aufrechterhaltung und Verbesserung des Prozesses der Informationssicherheit in einer Institution, indem Wege und Methoden für das generelle Vorgehen, aber auch für die Lösung spezieller Probleme aufgezeigt werden. Für die Erstellung einer Sicherheitskonzeption nach IT-Grundschutz sind die folgenden Schritte zu durchlaufen:

- **Definition des Informationsverbundes:** Festlegung des Geltungsbereichs
Zu Beginn muss der Geltungsbereich festgelegt werden, für den die Sicherheitskonzeption erstellt und umgesetzt werden soll. Dies können beispielsweise bestimmte Organisationseinheiten einer Institution sein. Es könnten aber auch Bereiche sein, die definierte Geschäftsprozesse oder Fachaufgaben bearbeiten, inklusive der dafür notwendigen Infrastruktur. Im IT-Grundschutz wird der Geltungsbereich für die Sicherheitskonzeption auch als „Informationsverbund“ bezeichnet. Die Bestandteile des betrachteten Informationsverbunds sind die mit den passenden Bausteinen des IT-Grundschutz-Kompendiums abzusichernden Komponenten.
- **Strukturanalyse:** Identifikation von Schutzobjekten
Im Rahmen der Strukturanalyse werden die für den betrachteten Informationsverbund, also Geltungsbereich oder Geschäftsprozess relevanten Schutzobjekte wie Informationen, Anwendungen, IT-, ICS-, oder IoT-Systeme, Netze, Räume und Gebäude, aber auch zuständige Mitarbeiter ermittelt.

Bei der Strukturanalyse müssen zusätzlich die Beziehungen und Abhängigkeiten zwischen den einzelnen Schutzobjekten dargestellt werden. Die Erfassung von Abhängigkeiten dient vor allem dazu, die Auswirkungen von Sicherheitsvorfällen auf die Geschäftstätigkeit zu erkennen, um dann angemessen reagieren zu können.

Beispiel:

 *Wenn der „Server xy“ von einem Sicherheitsvorfall betroffen ist, muss schnell erkannt werden, welche Anwendungen oder Geschäftsprozesse davon betroffen sind.*

- Schutzbedarfsfeststellung: Analyse der Auswirkungen von Sicherheitsvorfällen auf die betrachteten Geschäftsprozesse
Für jeden bei der Strukturanalyse ermittelten Wert wird das Maß an Schutzbedürftigkeit bestimmt.


Beispiel:

 *Kann der Ausfall eines IT-Systems einen hohen Schaden verursachen, ist der ermittelte Wert hoch, da das IT-System einen dementsprechend hohen Schutzbedarf hat.*

Zuerst muss dazu der Schutzbedarf der Geschäftsprozesse ermittelt werden. Anschließend kann darauf aufbauend der Schutzbedarf der Anwendungen bestimmt werden, die bei der Strukturanalyse erfasst wurden. Dabei muss berücksichtigt werden, welche Informationen mit diesen Anwendungen verarbeitet werden. In den allermeisten Institutionen reicht es an dieser Stelle aus, sehr wenige Informationsgruppen zu betrachten. Beispiele hierfür sind Kundendaten, öffentlich zugängliche Informationen (z. B. Adressen, Öffnungszeiten) oder strategische Daten für die Geschäftsführung. Danach wird betrachtet, welche Informationen wo und mit welchen IT-Systemen verarbeitet werden.

Der Schutzbedarf der Anwendungen überträgt sich auf die IT-Systeme, die die jeweiligen Anwendungen unterstützen. Der Schutzbedarf der Räume leitet sich aus dem Schutzbedarf der Anwendungen und IT-Systeme, die dort betrieben werden, ab.]

Beispiel:

 *Der Geschäftsprozess „Kundendatenverwaltung“ ist essenziell für die Aufrechterhaltung des Geschäftsbetriebs. Dieser Geschäftsprozess läuft auf dem „Server xy“, der damit einen hohen Schutzbedarf hat. Der Raum, in dem der Server untergebracht ist, beinhaltet daher auch mindestens einen hohen Schutzbedarf.*

- Modellierung: Auswahl der Sicherheitsanforderungen
In den Bausteinen des IT-Grundschutz-Kompodiums werden für typische Aufgaben des Informationssicherheitsmanagements und Bereiche des IT-Einsatzes spezifische Gefährdungen sowie Basis-, Standard- und Anforderungen für einen erhöhten Schutzbedarf beschrieben. Dabei werden jeweils organisatorische, personelle, infrastrukturelle und technische Aspekte der Informationssicherheit betrachtet.
Das IT-Grundschutz-Kompodium enthält Prozessbausteine aus den folgenden Bereichen bzw. Schichten:
 - ISMS: Management von Informationssicherheit,
 - ORP: Organisation und Personal,

- CON: Konzepte und Vorgehensweisen (z. B. Kryptokonzept, Softwareentwicklung),
- OPS: Betrieb (z. B. Schutz vor Schadprogrammen, Cloud Computing) und
- DER: Detektion und Reaktion (Behandlung von Sicherheitsvorfällen, Notfallmanagement).

Darüber hinaus enthält das IT-Grundschutz-Kompendium Systembausteine zur

- INF: Infrastruktur (z. B. Gebäude, Rechenzentrum),
- SYS: IT-Systemen (z. B. Servern, Clients),
- NET: Netzen und Kommunikation (z. B. Netzarchitektur und -design),
- APP: Anwendungen (z. B. E-Mail und Browser) und
- IND: Industrieller IT (z. B. Betriebs- und Steuerungstechnik sowie Leitstand).

Nach der Strukturanalyse kann der Geschäftsbetrieb mithilfe dieser Bausteine modelliert werden. Dabei wird dem betrachteten Geltungsbereich eine Sammlung von relevanten IT-Grundschutz-Bausteinen (Informationsverbund) zugeordnet. Daraus resultiert eine Sammlung an Sicherheitsanforderungen, die als Grundlage für die Erstellung der Sicherheitskonzeption dienen kann. Die im IT-Grundschutz-Kompendium enthaltenen Basis- und Standard-Anforderungen sowie Anforderungen bei erhöhtem Schutzbedarf konkretisieren die generischen Anforderungen aus ISO/IEC 27001 bzw. ISO/IEC 27002. Darüber hinaus enthalten die Umsetzungshinweise, die für zahlreiche IT-Grundschutz-Bausteine des IT-Grundschutz-Kompendiums veröffentlicht sind, konkrete Implementierungshilfen sowie zahlreiche technische Maßnahmen für den sicheren Betrieb von typischen IT-, ICS-, oder IoT-Systemen und Anwendungen. Eine genaue Anleitung zur Auswahl der Bausteine (Modellierung nach IT-Grundschutz) hilft dabei, alle sicherheitsrelevanten Aspekte zu berücksichtigen. Mit dieser Hilfe ist es Institutionen möglich, die angestrebten Sicherheitsziele ohne oder mit deutlich weniger Hilfe von externen Beratern zu erreichen.

- IT-Grundschutz-Check: Durchführung eines Soll-Ist-Vergleichs
Der IT-Grundschutz-Check ist ein Organisationsinstrument, das einen schnellen Überblick über das vorhandene Sicherheitsniveau bietet. Mithilfe 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.
- Risikoanalyse
Die Anwendung der IT-Grundschutz-Methodik ermöglicht es, ein Sicherheitsniveau zu schaffen, das für den normalen Schutzbedarf ausreichend und angemessen ist. Wenn der Schutzbedarf für einen bestimmten Bereich (beispielsweise eine Anwendung oder ein IT-System) höher ist oder wenn für einen Bereich keine IT-Grundschutz-Bausteine existieren, sollte nach der Umsetzung von IT-Grundschutz eine Risikoanalyse durchgeführt werden.
Das BSI hat eine eigene Methode zur Risikoanalyse entwickelt, die auf der Umsetzung von IT-Grundschutz aufbaut. Sie wird im BSI-Standard 200-3 *Risikoanalyse auf der Basis von IT-Grundschutz* (siehe [BSI3]) beschrieben. Als Methode kann aber auch eine klassische quantitative Risikoanalyse für die betroffenen Bereiche gewählt werden. Wenn nur ein kleiner Bereich der Informationsverarbeitung betroffen ist, kann der Aufwand für eine zusätzliche Risikoanalyse meistens als gering eingestuft werden. Ist z. B. nur ein spezielles IT-System betroffen, für das kein IT-Grundschutz-Baustein vorliegt, kann die hierauf beschränkte Beratung durch den Hersteller oder unab-

hängige Sicherheitsberater in der Regel schon helfen, um das Risiko abzuschätzen und geeignete Sicherheitsmaßnahmen auszuwählen.

Die Kombination aus Standard-Sicherheitsmaßnahmen und Risikoanalyse für die Bereiche, deren Schutzbedürftigkeit über den normalen Schutzbedarf hinausgeht, ist wesentlich effizienter als eine vollständige quantitative Risikoanalyse. Anschließend müssen dann die jeweils identifizierten Maßnahmen wieder in den restlichen Sicherheitsprozess eingebracht und konsolidiert werden.

- **Umsetzung der Maßnahmen**

Die identifizierten Sicherheitsmaßnahmen müssen geplant, durchgeführt, begleitet und überwacht werden. Hierfür sollte festgelegt werden, in welcher Reihenfolge die Maßnahmen umgesetzt werden und auch wer bis wann welche Maßnahmen realisieren muss. Alle Mitarbeiter, die Sicherheitsmaßnahmen ein- und umsetzen müssen, sollten geschult werden, um zu erfahren, was deren Zweck ist und was bei der Nutzung zu beachten ist.

11 Anhang

11.1 Literaturverzeichnis

- [20000] ISO/IEC 20000, IT Service-Management; bestehend unter anderem aus ISO/IEC 20000-1:2011, Service management – Part 1: Service management system requirements und ISO/IEC 20000-2:2012, Part 2: Guidance on the application of service management systems, International Organization of Standardization (ISO), ISO/IEC JTC 1/SC 40, 2011/2012
- [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
- [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
- [27006] ISO/IEC 27006:2015, International Organization for Standardization (Hrsg.), Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems, ISO/IEC JTC 1/SC 27, 2015
- [27031] ISO/IEC 27031:2011, International Organization for Standardization (Hrsg.), Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity, ISO/IEC JTC 1/SC 27, 2011
- [31000] ISO/IEC 31000:2009, International Organization for Standardization (Hrsg.), Risk management – Principles and guidelines, ISO/TC 262, 2009
- [BSI2] IT-Grundschutz-Methodik, BSI-Standard 200-2, 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>
- [BSI4] Notfallmanagement, BSI-Standard 100-4, Version 1.0, November 2008, <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>
- [COBIT] COBIT (Control Objectives for Information and Related Technology), Version 5, ISACA, <http://www.isaca.org/cobit>
- [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-standardinformation-security>

- [ITIL] IT Infrastructure Library (ITIL), IT-Service Management (ITSM), März 2017, <https://www.axelos.com/best-practice-solutions/itil>
- [NIST80053] 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>
- [PCI] Payment Card Industry Data Security Standard (PCI DSS), Version 3.2, PCI Security Standards Council (Hrsg.), April 2016, <https://www.pcisecuritystandards.org>
- [ZERT] Informationen zur Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz, BSI, <https://www.bsi.bund.de/iso27001-zertifikate>