Bundesamt
für Sicherheit in der
Informationstechnik

Überblick IT-Grundschutz

Entscheidungshilfe für Manager

Inhaltsverzeichnis

Vorwort 2

1 Warum Informationssicherheit? 4

1.1 Risiken für die Informationssicherheit 4
1.2 Internet-Kriminalität – eine stetig steigende Bedrohung 5
1.3 Informationssicherheit – ein Muss für jede Institution 6
1.4 Ganzheitlicher Ansatz von Informationssicherheit 6

2 Organisation von Informationssicherheit 9

2.1 Sicherheit ist ein Prozess 9
2.2 Die Phase der Planung 9
2.3 Die Phase der Umsetzung 10
2.4 Die Phase der Erfolgskontrolle 11
2.5 Die Phase der Optimierung 11

3 Praktische Unterstützung durch das BSI: Der IT-Grundschutz 13

3.1 Die BSI-Standards 14
3.2 Die IT-Grundschutz-Kataloge 15
3.3 Anwendung des IT-Grundschutzes 16
3.4 Zertifizierung 17
3.5 Hilfsmittel zur Umsetzung IT-Grundschutz 18

4 IT-Grundschutz und andere sicherheitsrelevante Standards 20

5 Literatur 23

Vorwort

Dr. Hartmut Isselhorst

Die Verschlüsselungssoftware Locky war in der jüngsten Vergangenheit ein wichtiger Weckruf für die Informationssicherheit. Der Krypto-Trojaner befiel in Deutschland und weltweit nicht nur private Rechner von Bürgern, sondern auch Unternehmen, Verwaltungseinrichtungen und sogar Kritische Infrastrukturen waren betroffen. Neben der Aufforderung, ein Lösegeld zu bezahlen, sahen sich Unternehmensleitungen plötzlich mit zahlreichen Herausforderungen konfrontiert: Kosten für den Produktivitätsausfall, Kosten für Fehlersuche und -behebung gegebenenfalls auch mit Hilfe externer Sicherheitsexperten, Einnahmeausfälle sowie Reputationsverlust. Dies sind lediglich einige Begleiterscheinungen eines Sicherheitsvorfalls, die allen Beteiligten viel Zeit, Geld und Nerven kosten können.

Wie sicher sind die Informationen in Ihrer Institution? In welchen Bereichen werden in Ihrer Institution bereits fundierte Schutzmaßnahmen umgesetzt, in welchen besteht eventuell dringender Handlungsbedarf? Wie gut sind Ihre sensiblen Firmendaten gegen Ausspähung und Abfischen geschützt?

In einem soliden wie umfassenden Risikomanagement muss der Informationssicherheit heute ein fester Platz eingeräumt werden. Die vorliegende Broschüre liefert Entscheidern aus Wirtschaft und Verwaltung einen ersten Einblick zur Bedeutung eines ganzheitlichen Managementsystems für Informationssicherheit (ISMS). Die bewährte IT-Grundschutz-Methodik stellt ein differenziertes Angebot bereit, das passgenaue Lösungen für individuelle Sicherheitsanforderungen einer Institution liefert. Ein Informationssicherheitsmanagement, das langfristig greifen soll, beinhaltet neben technischen auch personelle, infrastrukturelle und organisatorische Aspekte und wird regelmäßig auf den Prüfstand gestellt. Unternehmensleitung und Behördenleitung nehmen in diesem Prozess eine wichtige Vorbildfunktion ein.

Auch die IT-Grundschutz-Methodik selbst zeichnet sich durch einen starken prozessualen Charakter aus: Das sehr dynamische Themengebiet der Informationssicherheit, neue politische Rahmenbedingungen wie das IT-Sicherheitsgesetz sowie weitere Anforderungen an die Betreiber und Anwender von IT-Systemen haben den Ausschlag gegeben, die bewährte Methodik grundlegend zu modernisieren. Das BSI verfolgt hierbei grundsätzlich das Ziel, auf Bewährtem aufzubauen und zugleich die Nutzungsbreite zu verbessern. Heutige Nutzer werden den modernisierten IT-Grundschutz wiedererkennen und leicht adaptieren können. Neuen Anwendern – besonders kleineren Institutionen – ermöglichen vereinfachte Vorgehensweisen den Einstieg in ein modernes Informationsmanagement. Darüber hinaus werden die IT-Durchdringung von Produktionsstätten berücksichtigt und unterschiedliche Aspekte der Cyber-Sicherheit fokussiert. Der rasanten Entwicklung der Gefährdungslage können dadurch adäquate und praxistaugliche Antworten entgegengesetzt werden. In diesem Sinne wird auch der modernisierte IT-Grundschutz den Stand der Technik widerspiegeln: aktuell, flexibel und praxisnah.

Dr. Hartmut Isselhorst
Abteilungspräsident „Cyber-Sicherheit und Kritische Infrastrukturen“

1 Warum Informationssicherheit?

1 Warum Informationssicherheit?

In den letzten Jahren hat sich die **Bedeutung von Informationssicherheit** für Institutionen stark erhöht, da die Abhängigkeit von modernen Informations- und Kommunikationstechniken gerade im letzten Jahrzehnt enorm gewachsen ist. Verstärkt hat sich diese Entwicklung durch die steigende Vernetzung aufgrund des mobilen Zugriffs auf interne Informationen von einer wachsenden Anzahl von Mitarbeitern mit Smartphones oder Notebooks. Institutionen, unabhängig von ihrer Größe und Art, sind dadurch in immer höherem Maße auf eine funktionierende und sichere IT für ihre Wertschöpfungskette angewiesen. Dem gegenüber stehen stetig wachsende Bedrohungen für eine Institution. Die nachfolgenden Sicherheitsvorfälle sollen exemplarisch zeigen, wie sich Gefährdungen auswirken können, wie professionell Täter heutzutage agieren und welche negativen Folgen durch Ausfälle entstehen können.

1.1 Risiken für die Informationssicherheit

Fall 1: Cyber-Kriminelle verschlüsseln durch die Verbreitung von Erpressungssoftware, so genannter Ransomware, den Datenbestand von Unternehmen und Verwaltungseinrichtungen und fordern anschließend Lösegeld. Eingesetzt werden bekannte Methoden wie mit einem Schadprogramm infizierte E-Mail-Anhänge oder Links zu einer verseuchten Webseite. Den Angreifern reicht es, wenn lediglich ein einzelner Mitarbeiter eine Datei öffnet oder eine Webseite ansurft. Im schlimmsten Fall kann dadurch schnell der produktive IT-Einsatz einer ganzen Institution ausfallen. Neben bekannt gewordenen Fällen bei mehreren Krankenhäusern, einer Forschungseinrichtung sowie hunderten Webseiten zählen tausende Systeme von Unternehmen zu den Opfern der Angriffswelle.

Fall 2: Der Geschäftsführer einer mittelständischen Firma musste auf einer Messe feststellen, dass ein von ihm patentiertes Produkt von einem asiatischen Hersteller angeboten wurde. Da die Firma Luxusgüter produziert, können Umsatzschäden durch Plagiate nicht nur hoch sein, sondern auch die Existenz der Firma gefährden. Nach Aussage des Geschäftsführers ist es jedoch schwierig, ausländische Firmen juristisch zu verfolgen, insbesondere außerhalb der EU. Plagiate des Produkts, die in Deutschland ankamen, wurden vernichtet. Nach diesem Vorfall ließ sich der Geschäftsführer zum Thema Informationssicherheit beraten, wobei diverse Schwachstellen entdeckt

Informationssicherheit muss durch alle Mitarbeiter umgesetzt werden – das Management muss als Vorbild vorangehen.

Wie sicher sind Ihre Unternehmensinformationen?

wurden. Durch die Einführung neuer und die Aktualisierung vorhandener organisatorischer und technischer Sicherheitsmaßnahmen konnte das Risiko für neue Vorfälle minimiert werden.

Fall 3: Durch einen Stromausfall in einem Rechenzentrum der Deutschen Bahn fielen an einem Tag im Jahr 2009 im gesamten Bundesgebiet die über IT-Netze gesteuerten Dienstleistungen aus. Betroffen waren das Fahrkartenbuchungssystem sowie die Kommunikations- und Anzeigesysteme. Daraufhin konnten keine Fahrkarten an den Automaten, im Internet und an den Schaltern gekauft werden. Zusätzlich entstanden massive Beeinträchtigungen und Verspätungen im gesamten Bahnverkehr[1]. Für die Deutsche Bahn kam es durch diesen Vorfall zu einem eklatanten finanziellen Schaden (unter anderem durch Entschädigungen und erhöhten Personaleinsatz) sowie einem (von außen nicht näher bezifferbaren) Imageschaden.

1.2 Internet-Kriminalität – eine stetig steigende Bedrohung

Die alltägliche Realität in der Informationssicherheit verdeutlicht, dass die oben genannten Beispiele keine Einzelfälle sind. Dies spiegelt auch die Medienberichterstattung über Vorfälle wider sowie zahlreiche Studien und Untersuchungen, die regelmäßig zu dem Themenbereich veröffentlicht werden. Unter anderem legt das Bundeskriminalamt jährlich ein „Bundeslagebild Cybercrime“ vor, in dem die aktuellen Cyberdelikte verzeichnet sind. Die gesamte Lage zu erfassen gestaltet sich schwierig, die Dunkelziffer wird weiter sehr hoch eingeschätzt. Das hängt damit zusammen, dass Geschädigte Straftaten oft nicht als solche erkennen oder eine Straftat aus Sorge vor Reputationsverlust nicht zur Anzeige bringen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) informiert im jährlich erscheinenden Bericht „Die Lage der IT-Sicherheit in Deutschland“ über aktuelle IT-Gefährdungen und die daraus resultierenden Risiken. Die Bedrohungen für Informationen und Systeme von Wirtschaft und Staat gehen vor allem von gezielten Spionage-Angriffen wie zum Beispiel Advanced Persistant Threats (APT) und Cyber-Angriffen auf Webseiten aus. Nach Einschätzung des BSI erleichtern es Software-Schwachstellen und ungenügend abgesicherte Internet-Protokolle Angreifern in IT-Systeme einzudringen. Handlungsbedarf besteht darüber hinaus im Bereich Mobilkommunikation, besonders bei der Nutzung von Apps. Auch bei industriellen Steuerungssystemen ist noch häufig festzustellen, dass sie nur unzureichend abgesichert sind.

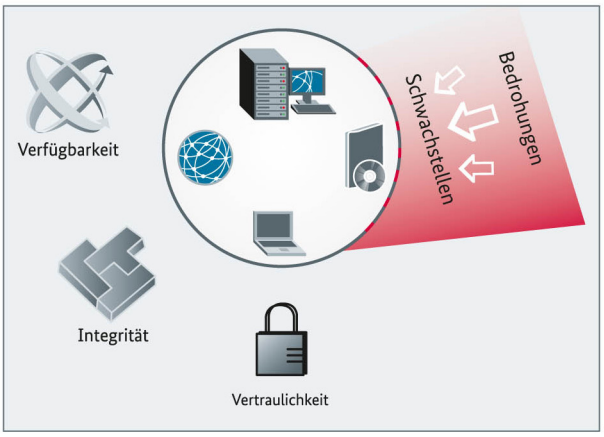
Gefährdung	2014	2015
Cloud Computing		→
Software-Schwachstellen	→	↑
Hardware-Schwachstellen		→
Nutzerverhalten und Herstellerverantwortung		↑
Kryptografie		→
Internet-Protokolle		↑
Mobilkommunikation		↑
Sicherheit von Apps		↑
Sicherheit von Industriellen Steuerungsanlagen		↑
Schadsoftware	↑	↑
Social Engineering	↑	→
Gezielte Angriffe - APT	→	↑
Spam	↑	↑
Botnetze	→	↑
Distributed Denial-of-Service (DDoS)-Angriffe	→	→
Drive-by-Exploits und Exploit-Kits	→	↑
Identitätsdiebstahl	↑	↑

Legende
Gefährdung 2015 (niedrig, durchschnittlich, hoch) ↓ → ↑

Übersicht der Entwicklung von IT-Bedrohungen nach Einschätzung des BSI im Bericht „Die Lage der IT-Sicherheit in Deutschland 2015“[2]

1.3 Informationssicherheit – ein Muss für jede Institution

Um den oben skizzierten **Risiken** entgegenzuwirken, sollte sich eine Institution systematisch dem Management der Risiken sowie der möglichen **Gegenmaßnahmen** aus dem Bereich der Informationssicherheit widmen. Risikoreduzierende (Sicherheits-)Maßnahmen schützen die Assets, also die Unternehmenswerte, vor **Bedrohungen** wie Zerstörung, Enthüllung, Modifizierung und nicht autorisierter Benutzung beziehungsweise stellen deren zeitnahe Wiederherstellung sicher. Damit kann gewährleistet werden, dass **der laufende Geschäftsbetrieb** und die **Erreichung der Geschäftsziele** nicht gefährdet werden. Durch wirtschaftlich angemessene Sicherheitsmaßnahmen kann ein geeigneter Schutz und ein somit **akzeptables Risikoniveau** erreicht werden.



Risikoreduzierende Sicherheitsmaßnahmen schützen Assets.

Positive Nebeneffekte durch Informationssicherheit

Neben dem Hauptzweck, Informationen und Prozesse bezüglich Vertraulichkeit, Verfügbarkeit und Integrität zu schützen, kann Informationssicherheit weiteren Nutzen in anderen Bereichen der Institution bringen:

Betriebswirtschaftlicher Nutzen

» Durch eine nachgewiesene Informationssicherheit ergeben sich Wettbewerbsvorteile, denn sie schafft Vertrauen bei Kunden, Geschäftspartnern und Mitarbeitern und wird zunehmend von diesen auch eingefordert.

» Durch ein ganzheitliches Management der Informationssicherheit werden auch Mängel in internen Abläufen aufgedeckt und so dazu beigetragen, dass Ressourcen effizient und gezielt eingesetzt werden. Dies kann zu einer Kostensenkung beitragen.

Organisatorischer Nutzen

» Eine gelebte und transparente Informationssicherheit fördert eine Unternehmenskultur, in der sicherheitsbewusstes Handeln, Kundenorientierung und die Identifikation mit den Unternehmenszielen fest verankert sind.

» Da sich Informationssicherheit an den Geschäftsprozessen orientiert, werden durch Erfolgskontrollen, zum Beispiel bei Sicherheitsaudits, häufig Verbesserungspotentiale für interne Abläufe und Prozesse aufgezeigt.

» Das Sicherheitsmanagement überprüft regelmäßig organisatorische und technische Änderungen, wodurch die permanente Einhaltung und Gewährleistung eines effizienten und hohen Sicherheitsniveaus nachgewiesen werden kann.

» Mit Hilfe der Informationssicherheit werden gesetzliche, vertragliche oder andere Anforderungen (zum Beispiel der eigenen Revision) umgesetzt und damit Governance und Compliance unterstützt.

Informationssicherheit im Unternehmen: Neben technischen Aspekten müssen auch personelle, organisatorische und infrastrukturelle Aspekte mitbedacht werden.

1.4 Ganzheitlicher Ansatz von Informationssicherheit

Um die eigenen und die externen Anforderungen zu erfüllen (Compliance), ist es wichtig zu wissen, welchen Wert Informationen haben und wie sie vor welchen Risiken geschützt werden müssen. Informationsverarbeitung ist nicht nur mit IT in Zusammenhang zu setzen. Der ganzheitliche Ansatz von Informationssicherheit betrach-

tet Anwendungen und IT-Systeme sowie Personen und Objekte. Es werden alle relevanten Werte einer Institution erfasst, aber dabei nicht jedes einzelne einer gesonderten Prüfung beziehungsweise Risikoanalyse unterzogen. Diese holistische Sichtweise über Geschäftsprozesse und Informationen ist als methodischer Ansatz in diversen nationalen und internationalen Standards mittlerweile etabliert. Durch die Verknüpfung der essentiellen Werte einer Institution (Geschäftsprozesse und Informationen) mit deren unabdingbaren Ressourcen gelingt es dem Informationssicherheitsmanagement Transparenz in die kritischen und risikobehafteten Komplexe zu bringen. Institutionsleitung, Mitarbeiter, Kunden und Stakeholder profitieren so von einem gesenkten Gesamtrisiko, da effiziente, risikoreduzierende Maßnahmen eingeführt werden können.

Compliance umfasst die gesamte Bandbreite der Einhaltung und Umsetzung von internen und externen Anforderungen. Dazu gehören regulatorische Vorgaben durch Gesetze oder Aufsichtsorgane, aber auch Kundenanforderungen.

Originäres Ziel hierbei ist es, negative Auswirkungen oder Strafen zu vermeiden. Gleichzeitig bietet sich so die Chance, Geschäftsprozesse, Fachaufgaben und IT zu optimieren und besser steuern zu können. Eine Optimierung der internen Prozesse führt erfahrungsgemäß zu einem geordneten, effektiven und effizienten IT-Betrieb und reduziert zudem den Aufwand bei Prüfungen.

Was genau Compliance für Informationssicherheit bedeutet, ist von einer Vielzahl von Faktoren abhängig. Dazu gehören beispielsweise die Organisationsform des jeweiligen Unternehmens, die Branche und die Art der Geschäftsprozesse, um die relevanten Kontrollvorgaben identifizieren zu können. Der erste Schritt, um die Einhaltung regulatorischer Vorgaben zu gewährleisten, sollte daher immer die Analyse der Gesetzeslage sein. Es sollte identifiziert werden,

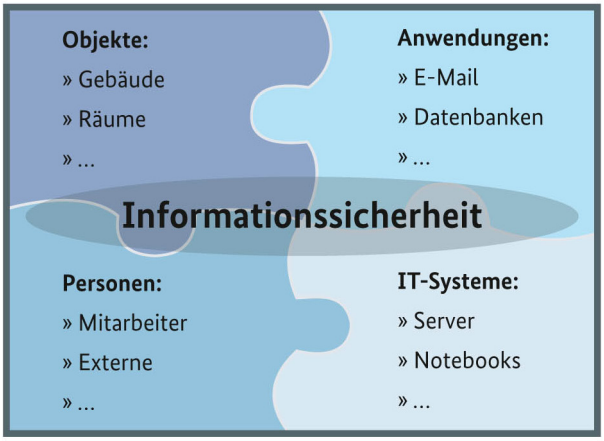
» welche Vorgaben, Gesetzen und Richtlinien in welchen Unternehmensbereichen und für welche Geschäftsfelder relevant sind,

» welche Institutionen deren Einhaltung kontrollieren,

» welche Folgen Verstöße haben können und

» wie die Einhaltung der Vorgaben nachzuweisen ist (beispielsweise über Testate oder Zertifikate oder bestimmte Formen externer oder interner Prüfungen).

Die gesetzlichen Vorschriften können sich häufig bereits auf Landes- und Regionalebene unterscheiden. Ein Unternehmen muss daher nicht nur übergreifend bestimmte Standards einhalten, sondern auch sicherstellen, dass an jedem Standort die dort gültigen Gesetze eingehalten werden. Ebenso können je nach Branche oder Einsatzzweck der IT-Systeme (zum Beispiel Büroumgebung, Prozesssteuerung, Krankenhaus) verschiedene Vorschriften gelten, die im Einzelfall ermittelt werden müssen.
Die meisten regulatorischen Vorgaben sind jedoch nicht so genau abgegrenzt, dass hierfür ein konkret definierter Maßnahmenkatalog vorliegt, der abzuarbeiten ist. Allerdings gibt es Vorgehensweisen, um ein anerkanntes und angemessenes Sicherheitsniveau zu erreichen, bei deren konsequenter Umsetzung auch die verschiedenen Kontrollinstanzen zufrieden gestellt sind.



Ganzheitliche Betrachtung der Informationssicherheit.

In einem soliden wie umfassenden Risikomanagement muss der Informationssicherheit heute ein fester Platz eingeräumt werden. Als Standard gilt inzwischen ein ganzheitlicher Ansatz für ein Managementsystem für Informationssicherheit (ISMS). Ein solches Managementsystem, das langfristig greifen soll, beinhaltet neben technischen auch personelle, infrastrukturelle und organisatorische Aspekte und wird regelmäßig auf den Prüfstand gestellt. Die IT-Grundschutz-Methodik stellt hierzu ein differenziertes Angebot bereit, das passgenaue Lösungen für individuelle Sicherheitsanforderungen einer Institution liefert. Die Unternehmensleitung selbst nimmt in dem ganzen Prozess eine wichtige Vorbildfunktion ein.

2 Organisation von Informationssicherheit

2 Organisation von Informationssicherheit

Wie wichtig und wertvoll die Integration und der Betrieb von Informationssicherheit für Institutionen sein können, wurde im vorherigen Kapitel aufgezeigt. Im Folgenden werden nun die Komponenten dargestellt, die für die **Etablierung eines Managementsystems für Informationssicherheit** notwendig sind.

2.1 Sicherheit ist ein Prozess

Sicherheit ist kein Ziel, das nach einmaligem Erreichen zur Selbstverständlichkeit wird. Auch ist Sicherheit für jede Institution individuell ausgeprägt. Standards zur Informationssicherheit helfen zwar bei der Orientierung, doch müssen beim Aufbau von Organisationsstrukturen für die Informationssicherheit individuelle und dennoch **zentrale Fragen** beachtet werden.

Um ein angemessenes **Sicherheitsniveau** nicht nur zu erreichen, sondern auch kontinuierlich aufrechtzuerhalten, muss Informationssicherheit als ein kontinuierlicher Prozess betrieben und gelebt werden.

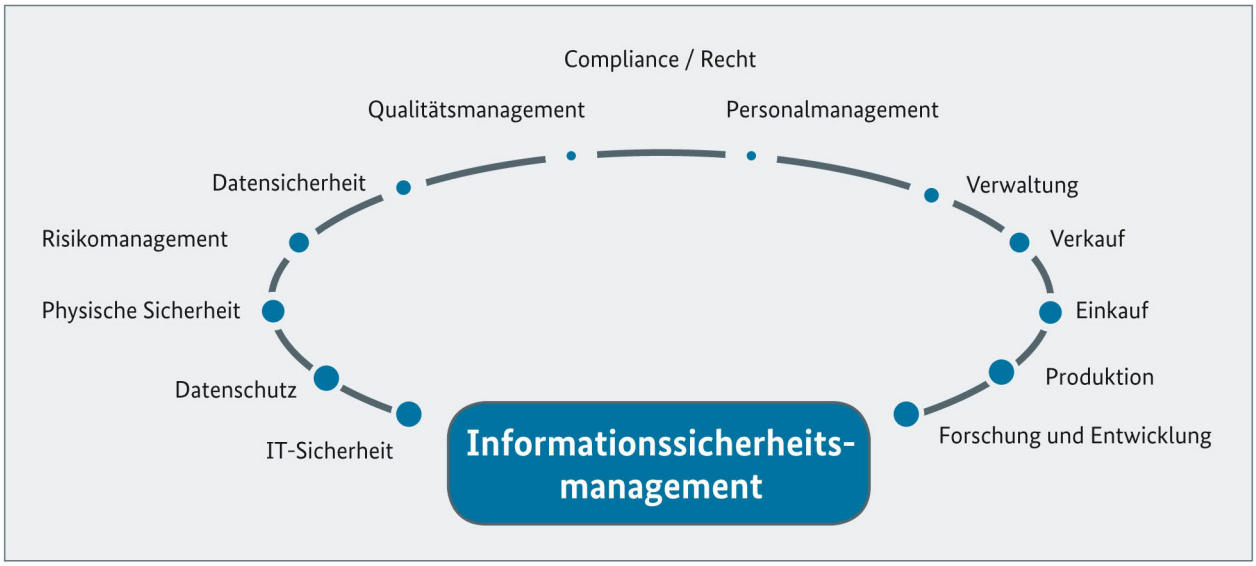
Besonders geeignet erscheint beim Aufbau und Betrieb eines Managementsystems für Informationssicherheit die Orientierung an einem prozessorientierten Problemlösungsansatz. Dieser betrachtet das gesamte betriebliche Handeln als Kombination verschiedener Prozesse beziehungsweise Phasen.

Die folgenden Kapitel skizzieren einen solchen Ansatz, der einen wirtschaftlichen und zielorientierten Aufbau eines Managementsystems für Informationssicherheit erlaubt und der auch in der Praxis einen kontinuierlichen Betrieb auf dem angestrebten Sicherheitsniveau ermöglicht.

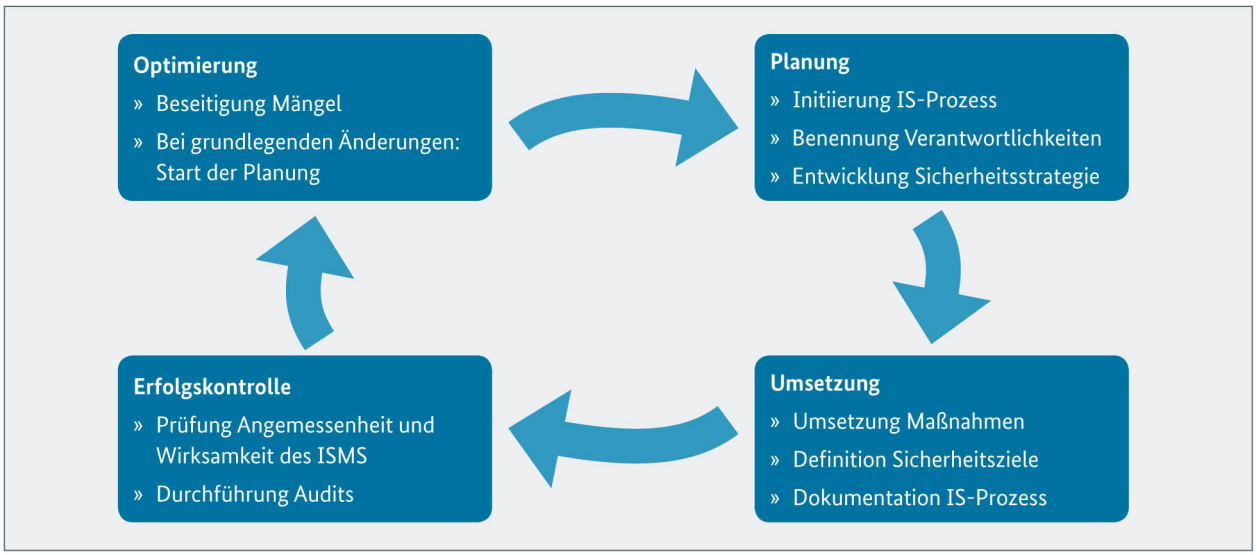
2.2 Die Phase der Planung

Das Managementsystem für Informationssicherheit (oder kurz ISMS) und der Informationssicherheitsprozess haben **Schnittstellen** zu vielen Bereichen und Sicherheitsthemen einer Institution und betreffen alle essentiellen Geschäftsprozesse und Aufgaben.

Nur die Leitungsebene kann für eine reibungslose Integration des Managementsystems für Informationssicherheit in bestehende Organisationsstrukturen und Prozesse sorgen. Deshalb müssen die ersten Schritte zur Einführung eines ISMS in der Institution vor allem durch deren Leitung legitimiert und genehmigt werden. Es muss ein Sicherheitsmanagement etabliert und durch entsprechende finanzielle, personelle und zeitliche Ressourcen unterstützt werden, das sowohl die Kompetenzen als auch die



Schnittstellen des ISMS.



Die vier Phasen eines Managementsystems für Informationssicherheit (ISMS).

Fähigkeiten besitzt, das System aufzubauen und dauerhaft zu steuern.

Für alle Aspekte rund um Informationssicherheit muss ein **Haupt-Ansprechpartner**, ein Informationssicherheitsbeauftragter (ISB) oder Chief Information Security Officer (CISO), ernannt werden, der die Aufgabe „Informationssicherheit" koordiniert und innerhalb der Institution vorantreibt. Ob es neben diesem Haupt-Ansprechpartner weitere Personen mit Sicherheitsaufgaben gibt und wie die Informationssicherheit organisiert ist, hängt von der Art und Größe der Institution ab.

Beim Aufbau und Betrieb des Managementsystems und der Sicherheitsprozesse müssen einige zentrale Fragen beantwortet werden. Dadurch lassen sich sowohl ein angemessenes Sicherheitsniveau als auch eine grundsätzliche **Sicherheitsstrategie** ableiten.

1. Welches sind die zentralen und essentiellen Werte, die für die Institution unabdingbar sind?

2. Welchen realen Risiken ist die Institution ausgesetzt und wie soll darauf reagiert werden?

3. Wie kann strukturiert ein angemessenes und prozessorientiertes Sicherheitsmanagement erreicht werden?

4. Welche technischen und organisatorischen Maßnahmen sind im Hinblick auf den Sicherheitsgewinn notwendig und wirtschaftlich sinnvoll?

5. Welchen sicherheitsrelevanten Veränderungen ist die Institution unterworfen und wie muss darauf reagiert werden?

2.3 Die Phase der Umsetzung

Sind die wesentlichen Fragen beantwortet, ist der organisatorische Grundstein für den Aufbau des Sicherheitsmanagements gelegt und sind die realen Risiken identifiziert, können in der Phase der **Umsetzung** die in der Planungsphase definierten **Maßnahmen** eingeführt werden. Um Institutionen zu unterstützen, geeignete Schutzmaßnahmen festzulegen, haben einige Organisationen – wie die ISO, das BSI und andere – Empfehlungen für Maßnahmen zur Verfügung gestellt.

Diese Empfehlungen sind beispielsweise im Standard ISO 27002 oder in den IT-Grundschutz-Katalogen des BSI zu finden. Es existieren sowohl sehr generisch gehaltene (ISO) wie auch sehr **konkret** formulierte technische und organisatorische Sicherheitsempfehlungen (BSI).

Bei der Auswahl von Maßnahmen sollten die Verantwortlichen immer bedenken, was sie mit deren Umsetzung erreichen möchten. Zu jeder Sicherheitsmaßnahme sollten möglichst **realistische und quantifizierbare Ziele** definiert werden. Nur so kann die Wirkung der Maßnahmen gemessen und optimiert werden.

Es ist notwendig, den Informationssicherheitsprozess zu **dokumentieren**. Nur so können Maßnahmen in die Praxis umgesetzt werden, bleiben Entscheidungen nachvollziehbar und die verschiedenen Prozessschritte wiederholbar.

2.4 Die Phase der Erfolgskontrolle

Die **Angemessenheit und Wirksamkeit** aller Elemente des Managementsystems für Informationssicherheit muss **ständig überprüft** werden. Das bezieht sich nicht nur auf einzelne Sicherheitsmaßnahmen, sondern auch die Sicherheitsstrategie muss regelmäßig überdacht werden.

Die Umsetzung der Sicherheitsmaßnahmen sollte in regelmäßigen Abständen mit Hilfe von internen **Audits** und Erfolgskontrollen ausgewertet werden. So können die Erfahrungen aus der täglichen Praxis zusammengetragen und analysiert werden.

Regelmäßige Erfolgskontrolle des ISMS ist wichtig.

Je nach Größe der Institution und fachlicher Ausrichtung kann es hilfreich sein, für Audits entsprechende externe Spezialisten hinzuzuziehen. Dies vermeidet Betriebsblindheit und unterstützt die eigenen Sicherheitsverantwortlichen bei der Analyse aller sicherheitsrelevanten Einflussfaktoren und Rahmenbedingungen.

2.5 Die Phase der Optimierung

In der Phase der Optimierung wird erkannten Mängeln oder auch Schwächen aus der Ergebniskontrolle entgegengewirkt. Die Optimierung kann dabei auf alle Bestandteile des Sicherheitsmanagements wirken. So sind nicht nur die technischen Maßnahmen betroffen, sondern auch organisatorische oder strategische Aspekte des Managementsystems. Dabei steht die **umgehende Beseitigung kleinerer Mängel** im Vordergrund. Bei grundlegenden oder umfangreichen Veränderungen ist wieder mit der Planungsphase zu beginnen und der gesamte Zyklus zu durchlaufen.

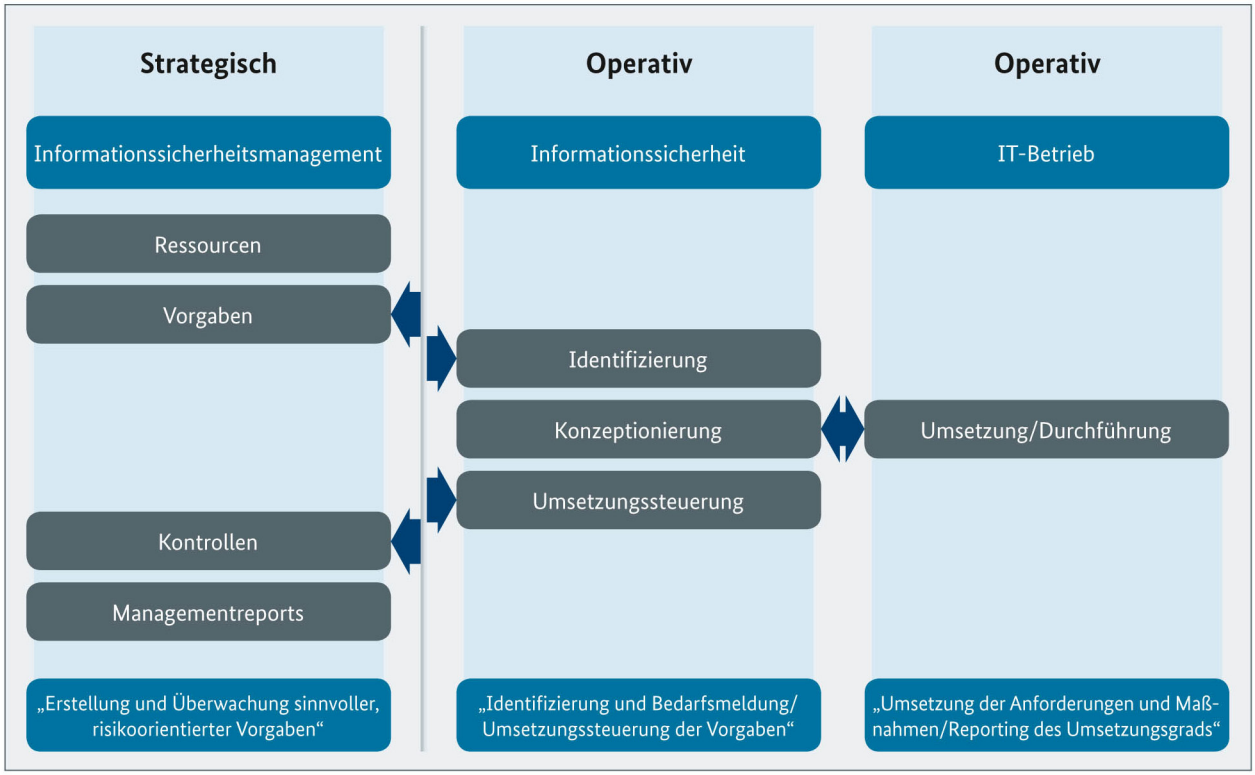
3 Praktische Unterstützung durch das BSI: Der IT-Grundschutz

3 Praktische Unterstützung durch das BSI: Der IT-Grundschutz

Wie bereits in den ersten Kapiteln dargestellt, umfasst Informationssicherheit nicht nur die Absicherung von IT-Systemen und den Schutz von Informationen, sondern auch den Aufbau eines Managementsystems für Informationssicherheit. Vereinfacht gesagt, schützt die Absicherung konkreter Systeme und Infrastrukturen vor den Gefahren von heute, während das Managementsystem die Nachhaltigkeit gewährleistet, dass kommende Gefahren erkannt werden und entsprechend gehandelt wird (zum Beispiel durch zusätzliche Schutzmaßnahmen).

Der IT-Grundschutz bietet eine Methodik für Sicherheitsmanagement mit konkreten Maßnahmenempfehlungen und deckt nicht nur technische, sondern auch organisatorische, personelle und infrastrukturelle Aspekte ab. So kann **schnell und wirtschaftlich** ein für den Normalbedarf angemessenes und ausreichendes Sicherheitsniveau erreicht werden.

Ursprünglich für Behörden konzipiert, hat sich der IT-Grundschutz seit 1994 für alle Branchen als wertvolles



Ebenen eines ISMS.

Für diese beiden Hauptaufgaben bietet das BSI mit dem IT-Grundschutz umfassende Unterstützung, die es einer Institution ermöglicht, schnell auf Basis von **Best Practices** in das Thema einzusteigen und zudem eine Vergleichbarkeit zwischen Institutionen zu erreichen.

Instrument für Informationssicherheit erwiesen und steht Institutionen jeglicher Art und aller Größen kostenlos zur Verfügung.

Seine Vorteile bestehen in der schnellen Vergleichbarkeit durch Soll-Ist-Analysen, der Nutzbarkeit praxiserprobter Maßnahmen und der hohen Akzeptanz durch die staatliche Referenzquelle.

Angebote des IT-Grundschutzes im Hinblick auf den erforderlichen Aufwand.

Daher ist der IT-Grundschutz im deutschsprachigen Raum zu einer Art „offiziellen Messlatte" für Informationssicherheit geworden. Teilweise wird sogar in Regularien, wie etwa den Mindestanforderungen für das Risikomanagement (MaRisk) der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), explizit auf den IT-Grundschutz referenziert. Deutsche Behörden verlangen bei vielen Projekten mit Dienstleistern aus der Privatwirtschaft die Umsetzung des IT-Grundschutzes und richten auch sich selbst danach aus.

Der IT-Grundschutz ist in zwei große Bereiche aufgeteilt: Die **BSI-Standards** und die **IT-Grundschutz-Kataloge**.

3.1 Die BSI-Standards

Derzeit gibt es vier BSI-Standards zur Informationssicherheit:

BSI-Standard 100-1 „Managementsysteme für Informationssicherheit"

Hier werden die allgemeinen Anforderungen an ein Managementsystem für Informationssicherheit (ISMS) definiert. Die Vorgaben sind konkret genug, um eine vollständige Anleitung für den Aufbau und Betrieb eines ISMS zu liefern, aber auch generisch genug, um an die spezifische Situation einzelner Institutionen angepasst werden zu können. Wichtig ist in diesem Zusammenhang, dass der Standard inhaltlich kompatibel zum internationalen Standard ISO 27001 ist (siehe auch Kapitel 4), so dass auch im internationalen Geschäftsverkehr eine Vergleichbarkeit gewährleistet ist.

BSI-Standard 100-2 „IT-Grundschutz-Vorgehensweise"

In diesem Standard zur IT-Grundschutz-Vorgehensweise wird Schritt für Schritt beschrieben, wie ein Managementsystem für Informationssicherheit in der Praxis aufgebaut und betrieben werden kann. Die Aufgaben des Sicherheitsmanagements und der Aufbau von Organisationsstrukturen für Informationssicherheit sind dabei wichtige Themen. Es wird ausführlich darauf eingegangen, wie angemessene Sicherheitsmaßnahmen ausgewählt werden können und was bei der Umsetzung des Sicherheitskonzeptes zu beachten ist. Auch die Frage, wie die Informationssicherheit im laufenden Betrieb aufrechterhalten und verbessert werden kann, wird beantwortet.

BSI-Standard 100-3 „Risikoanalyse auf der Basis von IT-Grundschutz"

In diesem Standard wird eine Methodik für Risikoanalysen vorgestellt, die sich anbietet, wenn in der Institution nach IT-Grundschutz gearbeitet wird. Wird bereits eine andere Risikomanagement-Methode eingesetzt, so kann auch diese verwendet werden.

BSI-Standard 100-4 „Notfallmanagement"

Eine andere Managementdisziplin, die viele Schnittstellen mit dem Sicherheitsmanagement hat, ist das Notfallmanagement. Dieser Standard beschreibt den Aufbau und die Aufgaben eines Notfallmanagementsystems.

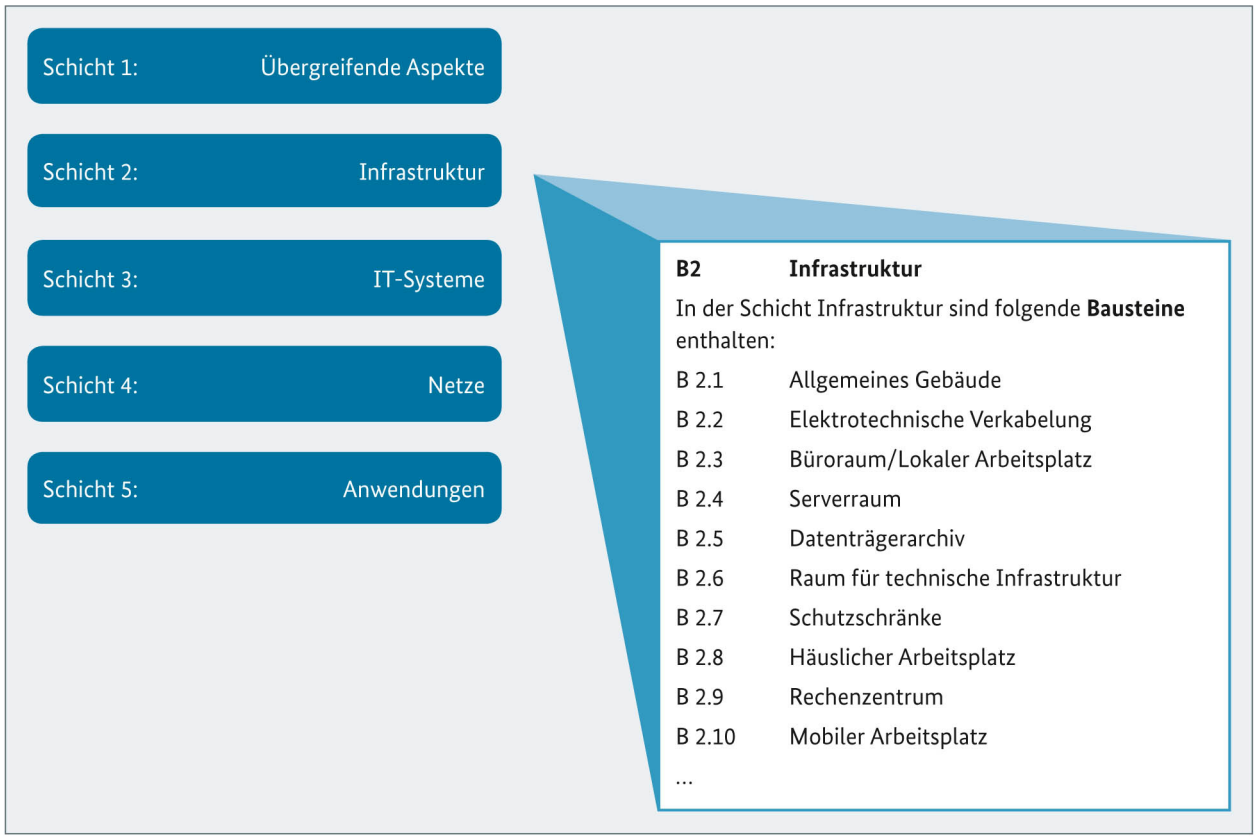
3.2 Die IT-Grundschutz-Kataloge

Die IT-Grundschutz-Kataloge sind in **Bausteine** gegliedert, die jeweils ein spezifisches organisatorisches, technisches oder infrastrukturelles Thema behandeln. Dies können zum Beispiel Schutzmaßnahmen für eine konkrete technische Plattform, Anforderungen an Schulungsmaßnahmen oder Sicherheitsaspekte für einen Serverraum sein. In jedem Baustein wird die Thematik zunächst inhaltlich umrissen, dann Gefährdungen aufgezeigt, die die Sicherheit des betrachteten Objekts beeinträchtigen können und schließlich auf Maßnahmen verwiesen, die diesen Gefährdungen entgegenwirken.

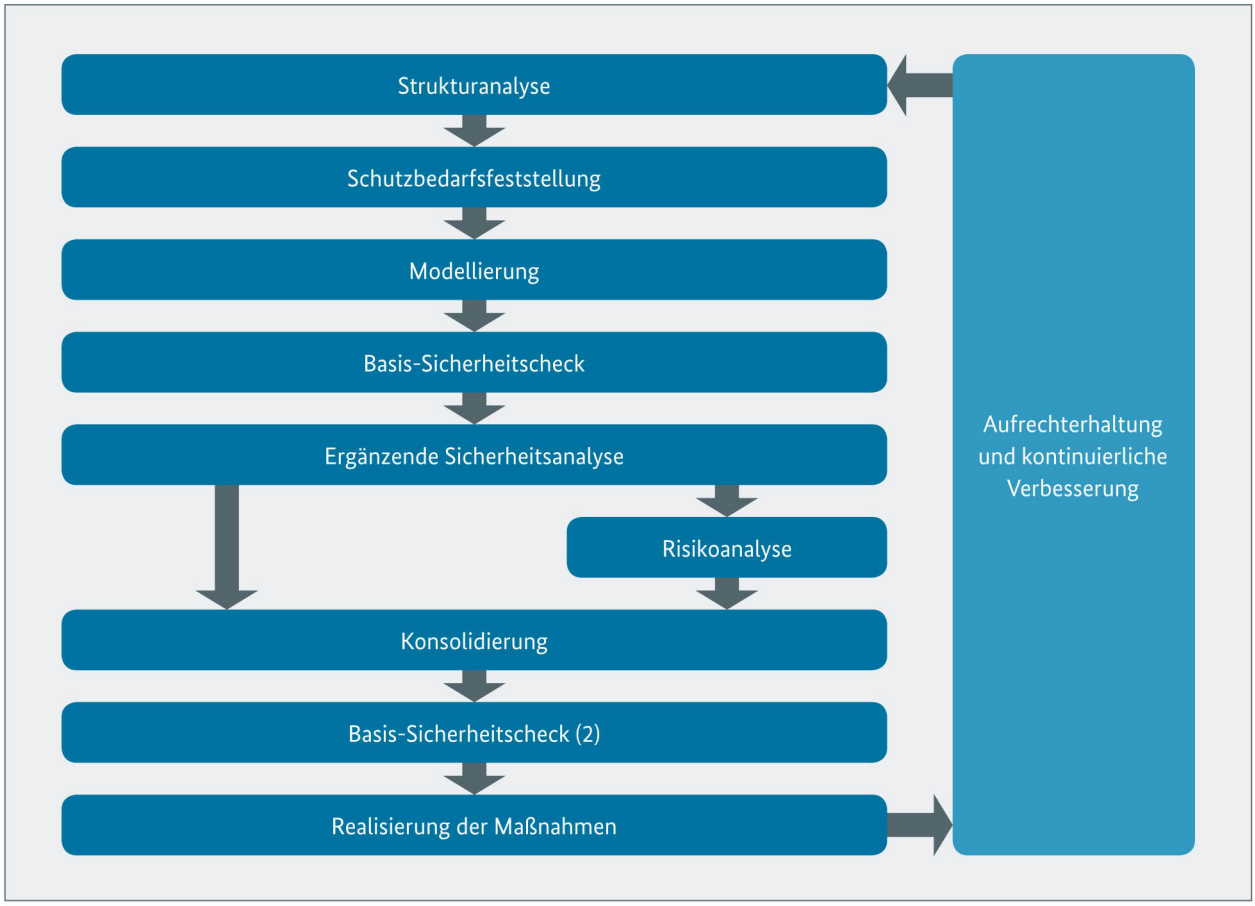
Die Bausteine selbst sind in **fünf Schichten** eingeteilt:

1. **Übergreifende Aspekte:** Hierzu gehören Bausteine wie Sicherheitsmanagement (der BSI-Standard 100-1 beschreibt vereinfacht gesagt, WAS gemacht werden muss, der Baustein konkretisiert das WIE), aber auch Themen wie Patch- und Änderungsmanagement oder Outsourcing. Gerade die beiden letztgenannten Bausteine zeigen auf, dass hier eine enge Anlehnung an klassische IT-Management-Werkzeuge wie ITIL existiert.
2. **Infrastruktur:** In dieser Ebene werden unter anderem Empfehlungen für den Schutz von Gebäuden, Rechenzentren, Büroräumen, mobilen Arbeitsplätzen aber auch an die IT-Verkabelung vorgestellt.
3. **IT-Systeme:** Hier finden sich Anleitungen zur Absicherung von verschiedenen Betriebssystemen, aber auch etwa von Mobiltelefonen, Multifunktionsgeräten oder Router und Switches.
4. **Netze:** Diese Schicht umfasst Sicherheitsvorgaben für heterogene Netze, das Netzmanagement, WLAN (drahtlose Netze), VoIP (Voice over IP, Computer-Telefonie), Bluetooth und andere Netze.
5. **Anwendungen:** In der letzten Schicht werden Maßnahmen zum Beispiel für SAP, Exchange-Server, Active Directory und Internet-Nutzung aufgezeigt.

Die IT-Grundschutz-Kataloge bestehen aktuell aus 88 Bausteinen mit rund 1.600 Empfehlungen für Sicherheitsmaßnahmen auf über 5.000 Seiten. Die IT-Grundschutz-Kataloge sind eine Art fachlich fundiertes



Beispiel für die Struktur eines Bausteins.



Ablauf der Modellierung nach BSI-Standard 100-2.

Kompendium mit konkreten Maßnahmen für die Informationssicherheit.

Trotz des großen Umfangs ist es natürlich nicht möglich, für alle Bereiche und Arten von IT-Systemen eigene IT-Grundschutz-Bausteine zur Verfügung zu stellen. Daher gibt es neben den Bausteinen zu konkreten Produkten auch immer generische Bausteine, die für den Fall, dass ein Produkt eingesetzt wird, für das kein Baustein existiert, genutzt werden können.

3.3 Anwendung des IT-Grundschutzes

IT-Grundschutz basiert auf der Feststellung, dass für normalen Schutzbedarf die Gefährdungen und die zu deren Reduzierung erforderlichen Sicherheitsmaßnahmen bei vielen Institutionen sehr ähnlich sind. Daher beruht das Konzept auf dem Ansatz, dass bestimmte Sicherheitsmaßnahmen unabhängig von der spezifischen Risikosituation umgesetzt sein müssen, um ein angemessenes Sicherheitsniveau zu erreichen.

Die Sicherheitsempfehlungen der IT-Grundschutz-Kataloge basieren auf **generischen Risikoanalysen**, die das BSI für die jeweiligen Bausteine durchgeführt hat. Dadurch kann, im Gegensatz zu anderen Standards (etwa ISO 27001), auf die anfängliche Durchführung einer individuellen Risikoanalyse für jedes Objekt verzichtet werden. Konkrete Schutzmaßnahmen lassen sich so **schneller und wirtschaftlicher** umsetzen.

Außerdem ist es nicht erforderlich, den IT-Grundschutz auf die ganze Institution anzuwenden, sondern es kann zunächst auch nur ein Teil (zum Beispiel ein Rechenzentrum oder die für einen bestimmten Geschäftsprozess erforderliche Infrastruktur) betrachtet werden – der sogenannte **Informationsverbund**.

Bei der Anwendung des IT-Grundschutzes wird im ersten Schritt eine **Strukturanalyse** durchgeführt. Theoretisch sollten die hierzu erforderlichen Informationen (Überblick über die wesentlichen Geschäftsprozesse, Inventarisierung von IT, Netzplan, Raumplan, etc.) im Unternehmen verfügbar sein. Die Praxis hat allerdings gezeigt, dass IT-Grundschutzprojekte oft zum Anlass genommen werden,

mögliche „Versäumnisse“ aus anderen Bereichen aufzuarbeiten. Dies ist aber durchaus „im Sinne des Erfinders“, da es der Anspruch des BSI ist, nicht nur das Eintreten von (Sicherheits-)Vorfällen verhindern zu helfen, sondern auch im Alltag einen Nutzen zu stiften. Ein wesentliches Feedback von Institutionen, die IT-Grundschutz umgesetzt haben, ist, dass dadurch interne Prozesse und Strukturen transparenter werden und dies auch der täglichen Arbeit nutzt.

Herzstück des IT-Grundschutzes ist die sogenannte **Schutzbedarfsfeststellung**, in der der Schutzbedarf der einzelnen Objekte vom Mobiltelefon bis zum Gebäude bestimmt wird. Sie startet bei den Daten und Geschäftsprozessen und wird von dort immer weiter vererbt (Beispiel: „Dieser Prozess benötigt diese Anwendung, die auf diesem Server läuft, der in diesem Raum in diesem Gebäude steht“). Konkrete Ausprägungen und Stufen des Schutzbedarfs werden im IT-Grundschutz vorgeschlagen, sie können aber auch individuell angepasst werden.

Im nächsten Schritt, der sogenannten **Modellierung,** werden nun allen Objekten des Informationsverbunds die passenden Bausteine aus den IT-Grundschutz-Katalogen zugeordnet. Für jedes Objekt gibt es eine Auswahl an Maßnahmen, die im nächsten Schritt einem **Soll-Ist-Vergleich** – dem sogenannten **Basis-Sicherheitscheck** – unterzogen werden. So gibt es nach relativ kurzer Zeit eine konkrete Bewertung des Ist-Standes und eine ebenso konkrete Umsetzungsvorgabe. Um diesen Soll-Ist-Vergleich weiter zu erleichtern, wurden vom BSI konkrete Prüffragen formuliert, so dass für alle Bausteine **detaillierte Fragebögen** zur Verfügung stehen.

Die Maßnahmen basieren immer auf der Annahme, dass ein normaler Schutzbedarf vorliegt. Es hat sich gezeigt, dass dies in der Regel für 80% aller Objekte zutrifft. Besteht ein höherer Schutzbedarf in bestimmten Bereichen, zum Beispiel wenn Schadensauswirkungen dort ein existentiell bedrohliches Ausmaß für die Institution erreichen könnten, so ist zu prüfen, ob zusätzliche Maßnahmen ergriffen werden müssen. In diesem Fall muss die zuvor durch die generische Vorarbeit des BSI eingesparte **Risikoanalyse** für diesen spezifischen Punkt durchgeführt werden. Da aber hierfür schon bei den Bausteinen Gefährdungen als Input geliefert werden, reduziert sich nicht nur – gemäß obiger Annahme – die Anzahl der Risikoanalysen auf ein Fünftel, sondern auch der Aufwand für die verbleibenden Analysen.

3.4 Zertifizierung

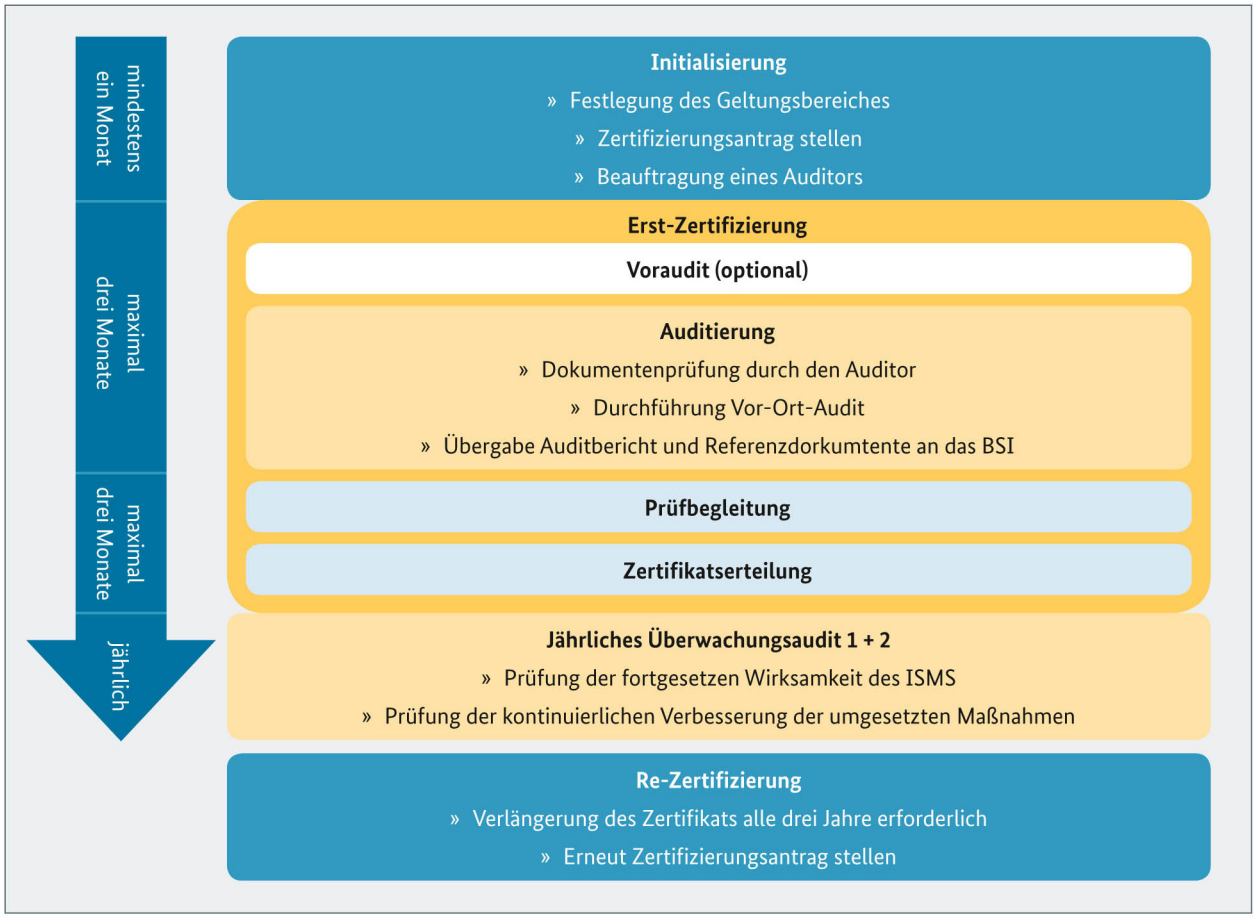
Immer häufiger wird von Geschäftspartnern und Kunden ein Nachweis der eigenen Vorkehrungen gegen IT-Sicherheitsvorfälle verlangt. Eine Zertifizierung nach IT-Grundschutz weist nach, dass in einer Institution ein angemessenes Sicherheitsniveau vorhanden ist.

Dieses Zertifikat deckt auch die internationale Zertifizierungsnorm für Managementsysteme für Informationssicherheit (ISO 27001) mit ab. Um dies zu verdeutlichen, heißt es offiziell **„ISO 27001-Zertifikat auf der Basis von IT-Grundschutz“**. Im Gegensatz zur originären ISO 27001-Zertifizierung umfasst die Prüfung hier aber nicht nur das ISMS, sondern auch die konkrete technische Umsetzung. Dies bedeutet in den meisten Fällen, dank der großen Detailtiefe des IT-Grundschutzes, einen höheren Initialaufwand in der Vorbereitung. Aber im Gegenzug hat es eine deutlich höhere Aussagekraft und Vergleichbarkeit der wirklich vorhandenen Qualität der ergriffenen Schutzmaßnahmen.

Beispiel Zertifikats-Button.

Diese hohe Vergleichbarkeit wird auch durch die Tatsache erreicht, dass alle Auditoren direkt vom BSI ausgebildet und lizenziert werden. Zudem werden alle Zertifizierungen in der letzten Instanz vom BSI entschieden.

Der Auditor nimmt eine Prüfung der eingereichten Unterlagen zum ISMS vor und kontrolliert deren Korrektheit durch Stichproben bei einer Vor-Ort-Prüfung. Entgegen landläufiger Annahmen geht es in dieser Prüfung nicht nur um die konkrete Umsetzung der Maßnahmenkataloge bei technischen Systemen, sondern gerade auch um die Frage, inwieweit das Management seine Verantwortung



Ablauf Zertifizierung nach BSI-Standard 100-2.

wahrnimmt. Es wird beispielsweise nachgefragt, ob das Management ausreichende Ressourcen bereitgestellt hat, um die Managementprozesse für Informationssicherheit nachhaltig zu etablieren.

Der Aufwand für die eigentliche Zertifizierung ist nach Etablierung des ISMS und der Maßnahmenumsetzung vergleichsweise gering. Zudem bietet eine Zertifizierung den zusätzlichen Nutzen, dass viele Nachweis- und Prüfverfahren, wie sie Kunden, Partner oder Wirtschaftsprüfer verlangen, durch Vorlage des Zertifikates in der Regel verkürzt werden können.

Ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz wird für drei Jahre verliehen. Jährlich findet ein Überwachungsaudit statt, um die Aufrechterhaltung des erreichten Sicherheitsniveaus nachzuweisen.

3.5 Hilfsmittel zur Umsetzung IT-Grundschutz

Grundsätzlich ist es möglich, dass die Maßnahmen aus den IT-Grundschutz-Bausteinen in jeder Institution eigenständig umgesetzt werden können. Oftmals hat sich in der Praxis die Einbindung eines Beraters bewährt, der bei der Umsetzung der Maßnahmen durch langjährige Erfahrung unterstützt. Kontaktadressen der durch das BSI lizenzierten Auditoren sind auf der IT-Grundschutz-Webseite zu finden.

Darüber hinaus hat das BSI, insbesondere für Behörden mit höherem Schutzbedarf, eine eigene Zertifizierung von IT-Sicherheitsdienstleistern durchgeführt. Diese zertifizierten Beratungshäuser hat das BSI unter anderem auf ihre fachliche Qualifikation, deren Qualitätsmanagement sowie Informationssicherheit überprüft. Darüber hinaus sind diese Dienstleister geheimschutzbetreut.

Für die technische Unterstützung haben sich in der Praxis vom BSI lizenzierte Tools bewährt. Die Tool-Hersteller und deren Produkte sind ebenfalls auf den Webseiten veröffentlicht. Wichtig beim Einsatz eines Tools ist für jede Institution, dass die besonderen Anforderungen seitens der Institution in die Auswahl eines Tools einfließen. Das Tool sollte sich den Rahmenbedingungen der Institution anpassen, nicht umgekehrt.

4 IT-Grundschutz und andere sicherheitsrelevante Standards

4 IT-Grundschutz und andere sicherheitsrelevante Standards

Der international am weitesten verbreitete Standard für Informationssicherheit ist der ISO-Standard 27001, inklusive der ergänzenden Standards mit den fortlaufenden Nummern 270xx. Während für Bundesbehörden die Anwendung des IT-Grundschutzes obligatorisch ist (und dies seitens der Behörden auch für deren Lieferanten gefordert werden kann), stellt sich für viele privatwirtschaftliche Unternehmen die Frage, welcher der beiden Standards der besser geeignete ist.

Grundsätzlich lässt sich sagen, dass der **IT-Grundschutz deutlich konkreter und tiefgehender** ist. Vereinfacht ausgedrückt, beschreiben die Controls der ISO 27002 WAS gemacht werden muss, der IT-Grundschutz beschreibt darüber hinaus auch, WIE es gemacht werden kann. ISO 27001 fokussiert sich gänzlich auf das Informationsmanagementsystem. Dies entspricht in Umfang und Tiefe dem BSI Standard 100-1. Konkrete technische Fragestellungen beantwortet ergänzend hingegen nur der IT-Grundschutz.

Im Vorgehen gibt es aufgrund der **fehlenden konkreten Handlungsvorschläge seitens der ISO 27001** ebenfalls einen signifikanten Unterschied: da das BSI die IT-Grundschutz-Kataloge auf Basis generischer Risikoanalysen erstellt hat, muss eine Risikoanalyse nur noch für Objekte mit erhöhtem Schutzbedarf durchgeführt werden, während sie bei ISO 27001 grundsätzlich für alle Objekte durchzuführen ist.

ISO 27001 und IT-Grundschutz lassen sich auch gut kombinieren. Entscheidet sich ein Unternehmen dafür, nach ISO 27001 zu arbeiten, müssen die sehr abstrakten Controls der ISO 27001 mit Leben gefüllt werden. Hierbei helfen die umfangreichen Sicherheitsempfehlungen des IT-Grundschutzes, aus denen die Institution die für ihre jeweiligen Rahmenbedingungen geeigneten Sicherheitsempfehlungen auswählen und anpassen kann. IT-Grundschutz ist ein frei zur Verfügung stehendes Angebot des BSI, das auf die jeweiligen Bedürfnisse konfektioniert werden kann.

Auch in der Kombination mit anderen IT-Standards, die wie ITIL/ISO 20000 oder COBIT zum Teil einen Sicherheitsbezug haben, ergeben sich **Synergien** und Überschneidungen, die Doppelarbeiten vermeiden. So gibt es im IT-Grundschutz etwa Bausteine für das Patch- und Änderungsmanagement, die zu den Anforderungen aus **ITIL/ ISO 20000** weitestgehend kompatibel sind. Ein ITIL-konformes IT-Management vereinfacht somit die Einführung des IT-Grundschutzes und dessen Umsetzung liefert eine starke Basis für eine ITIL-/ ISO 20000-Implementierung.

Ähnliches gilt für **COBIT**: Dieses IT-Governance-Framework beschreibt Prozesse und Kontrollziele für Planung, Beschaffung, Betrieb und Überwachung aller IT-Ressourcen. COBIT ist kein IT-Sicherheitsstandard, berücksichtigt jedoch bei der Definition von Anforderungen unter anderem die Sicherheitsziele Vertraulichkeit, Verfügbarkeit und Integrität aus der Informationssicherheit. In den über 300 Kontrollzielen sind zahlreiche Anforderungen an die Informationssicherheit enthalten. Aus den Anforderungen müssen konkrete Maßnahmen abgeleitet und implementiert werden. Analog zur ISO 27001 wird aber nur das WAS und nicht das WIE beschrieben, so dass auch hier der IT-Grundschutz eine sinnvolle Ergänzung darstellt.

Anforderung (Requirement) der ISO 27001

A.9.2 Equipment security		
Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.		
A.9.2.1	Equipment siting and protection	*Control* Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
A.9.2.2	Supporting utilities	*Control* Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
A.9.2.3	Cabling security	*Control* Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

Entsprechendes Control in der ISO 27002

9.2.3 Cabling security

Control

Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.

Implementation guidance

The following guidelines for cabling security should be considered:

a) power and telecommunications lines into information processing facilities should be underground, where possible, or subject to adequate alternative protection;

b) network cabling should be protected from unauthorized interception or damage, for example by using a conduit or by avoiding routes through public areas;

c) power cables should be segregated from communications cables to prevent interference;

d) clearly identifiable cable and equipment markings should be used to minimise handling errors, such as accidental patching of wrong network cables;

e) a documented patch list should be used to reduce the possibility of errors;

f) for sensitive or critical systems further controls to consider include:

1) installation of armoured conduit and locked rooms or boxes at inspection and termination points;

2) use of alternative routings and/or transmission media providing appropriate security;

3) use of fibre optic cabling;

4) use of electromagnetic shielding to protect the cables;

5) initiation of technical sweeps and physical inspections for unauthorized devices being attached to the cables;

6) controlled access to patch panels and cable rooms;

IT-Grundschutzbaustein

Schicht Infrastruktur — B 2.2

B 2.2 Elektrotechnische Verkabelung

Beschreibung

Die elektrotechnische Verkabelung von IT-Systemen und anderen Geräten umfasst alle Kabel und Verteilungen im Gebäude vom Einspeisepunkt des Verteilungsnetzbetreibers bis zu den Elektro-Anschlüssen der Verbraucher.

Die ordnungsgemäße und normgerechte Ausführung der elektrotechnischen Verkabelung ist Grundlage für den sicheren IT-Betrieb. Die IT-Verkabelung zur Kommunikation der IT-Systeme wird in einem separaten Baustein behandelt (siehe Baustein B 2.12 *IT-Verkabelung*). Da häufig gemeinsame Wege und Trassen für beide Arten der Verkabelung genutzt werden, sind die in beiden Bausteinen genannten Maßnahmen gemeinsam umzusetzen.

Gefährdungslage

Für den IT-Grundschutz der elektrotechnischen Verkabelung werden folgende typische Gefährdungen angenommen:

Höhere Gewalt
- G 1.6 *Kabelbrand*

Organisatorische Mängel
- G 2.11 *Unzureichende Trassendimensionierung*
- G 2.12 *Unzureichende Dokumentation der Verkabelung*
- G 2.13 *Unzureichend geschützte Verteiler*

Menschliche Fehlhandlungen
- G 3.5 *Unbeabsichtigte Leitungsbeschädigung*
- G 3.85 *Verletzung von Brandschottungen*

Technisches Versagen
- G 4.6 *Spannungsschwankungen/Überspannung/Unterspannung*
- G 4.62 *Verwendung unzureichender Steckdosenleisten*
- G 4.63 *Verstaubte Lüfter*

Vorsätzliche Handlungen
- G 5.8 *Manipulation an Leitungen*

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für die elektrotechnische Verkabelung sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung über die Umsetzung bis zum Betrieb. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt. Wie beim Gebäude, so ist auch hier zu beachten, dass die Einflussmöglichkeiten beim Einzug in ein schon bestehendes Gebäude auch bei der Absicherung der Verkabelung wesentlich geringer sind als bei der Errichtung eines Neubaus.

Planung und Konzeption

In der Planungsphase werden die Grundlagen für eine leistungsfähige, gut abgesicherte Verkabelung gelegt.

Die mechanischen und elektrischen Eigenschaften der Verkabelung werden durch die Auswahl der einzusetzenden Kabeltypen und durch Kabelführung und -trassen und die Umgebungsbedingungen festgelegt. Durch Auswahl geeigneter Kabeltypen und die typgerechte Verlegung muss die

IT-Grundschutz-Kataloge: 11. EL Stand 2009 — 106

Schicht Infrastruktur — B 2.2

elektrotechnische Installation widerstandsfähig gegen Gefährdungen aus dem Umfeld gemacht werden. Bei der Planung sollte nach Möglichkeit auch darauf geachtet werden, dass Leitungen und Haupt- und Unterverteilungen des Gebäudes gegen Missbrauch in geeigneter Weise physisch abgesichert werden.

Umsetzung

Ein wesentliches Element des Brandschutzes ist die richtige Installation von Kabelkanälen, die durch eine fehlende Brandabschottung erhebliche Risiken verursachen können. Beim Einbau der Verkabelung ist auch auf eine ausführliche und korrekte Dokumentation zu achten, da es im nachhinein meist sehr schwierig oder sogar unmöglich ist, festzustellen, wo Kabel verlaufen und was sie verbinden.

Betrieb

Als Grundlage für einen sicheren und störungsfreien Betrieb müssen die Anlagen und ihre Nutzung regelmäßig geprüft werden (siehe M 2.394 *Prüfung elektrischer Anlagen*). Bei Arbeiten an Trassen ist sicherzustellen, dass der Brandschutzbeauftragte rechtzeitig in Planung und Ausführung mit einbezogen wird (siehe M 2.391 *Frühzeitige Information des Brandschutzbeauftragten*).

Aussonderung

Auch Elektrokabel, die nicht mehr benötigt werden, sind zu entfernen oder fachgerecht außer Betrieb zu nehmen (siehe M 5.1 *Entfernen oder Deaktivieren nicht benötigter Leitungen*).

Notfallvorsorge

Sofern erhöhte Anforderungen an die Verfügbarkeit gestellt werden, sollte die Verkabelung, gegebenenfalls einschließlich der externen Anschlüsse, redundant ausgelegt werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich "elektrotechnische Verkabelung" vorgestellt:

Planung und Konzeption
- M 1.3 (A) *Angepasste Aufteilung der Stromkreise*
- M 1.20 (A) *Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht*
- M 1.21 (A) *Ausreichende Trassendimensionierung*
- M 1.22 (Z) *Materielle Sicherung von Leitungen und Verteilern*
- M 1.25 (B) *Überspannungsschutz*

Umsetzung
- M 1.9 (A) *Brandabschottung von Trassen*
- M 1.64 (A) *Vermeidung elektrischer Zündquellen*
- M 2.19 (B) *Neutrale Dokumentation in den Verteilern*
- M 5.4 (A) *Dokumentation und Kennzeichnung der Verkabelung*
- M 5.5 (A) *Schadensmindernde Kabelführung*

Betrieb
- M 2.391 (B) *Frühzeitige Information des Brandschutzbeauftragten*
- M 2.394 (B) *Prüfung elektrischer Anlagen*

Aussonderung
- M 5.1 (A) *Entfernen oder Deaktivieren nicht benötigter Leitungen*

Notfallvorsorge
- M 6.18 (Z) *Redundante Leitungsführung*

IT-Grundschutz-Kataloge: 11. EL Stand 2009 — 107

ISO 27001 und IT-Grundschutz.

5 Literatur

5 Literatur

Das BSI
https://www.bsi.bund.de

IT-Grundschutz
https://www.bsi.bund.de/grundschutz

IT-Grundschutz-Standards
https://www.bsi.bund.de/standards

IT-Grundschutz-Zertifikat
https://www.bsi.bund.de/iso27001-zertifikate

IT-Grundschutz unterstützende Tools
https://www.bsi.bund.de/gstools

Pressemitteilungen des BSI
https://www.bsi.bund.de/presse

Übersicht BSI-Publikationen
https://www.bsi.bund.de/publikationen

Zertifizierte Auditoren
https://www.bsi.bund.de/auditoren

Endnoten

1 Heise.de: Bahn kämpft mit bundesweitem Netzwerkausfall: http://www.heise.de/netze/meldung/Bahn-kaempft-mit-bundesweitem-Netzwerkausfall-Update-197890.html

2 BSI-Lagebericht „Bericht zur Lage der IT-Sicherheit in Deutschland 2015“: https://www.bsi.bund.de/lageberichte

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185-189
53175 Bonn
E-Mail: bsi@bsi.bund.de
Internet: www.bsi.bund.de
www.bsi-fuer-buerger.de · www.facebook.com/bsi.fuer.buerger

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185-189
53175 Bonn
E-Mail: grundschutz@bsi.bund.de
Telefon: +49 (0) 22899 9582-5369
Telefax: +49 (0) 22899 9582-5400
Internet: www.bsi.bund.de/grundschutz

Stand
August 2016

Druck
Druck- und Verlagshaus Zarbock GmbH & Co. KG
Sontraer Straße 6
63086 Frankfurt am Main
Internet: www.zarbock.de

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik – BSI

Bildnachweis:
Titel: BSI
Graphiken: BSI
S. 4: Contrastwerkstatt/Fotalia
S. 5: Olivier Le Moal/Fotalia
S. 6: Rawpixel/Fotalia
S. 7: asrawolf/Fotolia
S. 19: Bundesanzeiger Verlag

Artikelnummer
BSI-MIBro16/811

Diese Broschüre ist Teil der Öffentlichkeitsarbeit des BSI; sie wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.

www.bsi.bund.de