HOCHSCHULE

FÜR ANGEWANDTE WISSENSCHAFTEN

LANDSHUT

Fakultät Informatik

Bachelorarbeit zum Thema

Migration auf den modernisierten IT-Grundschutz und Entwicklung einer Transformation-Roadmap für das IT-Beratungsunternehmen Capgemini

vorgelegt von
Norbert Kiss

Betreuer: Prof. Dr. rer. nat. Peter Scholz

ERKLÄRUNG ZUR BACHELORARBEIT

Name, Vorname der/des Studierenden:

.....

Hochschule Landshut, Fakultät Informatik

Hiermit erkläre ich, dass ich die Arbeit selbständig verfasst, noch nicht anderweitig für Prüfungszwecke vorgelegt, keine anderen als die angegebenen Quellen oder Hilfsmittel benutzt sowie wörtliche und sinngemäße Zitate als solche gekennzeichnet habe.

....

(Datum) (Unterschrift der/des Studierenden)

Abstract

Das Leben des 21. Jahrhunderts ist von die Informations- und Telekommunikationstechniken geprägt. Informationssicherheit ist aktueller denn je – doch die Informationssicherheit wird häufig nicht ernstgenommen.

Im Zuge der Digitalisierung steigt nicht nur die digitale Datenmenge in Institutionen, sondern auch die Gefahr Informationen zu verlieren oder diese zu missbrauchen. Dabei werden die Informationen von Organisationen nicht nur von externen Einflussfaktoren gefährdet, sondern sie sind ebenfalls internen Gefahrenquellen ausgesetzt. Neue Technologien dürfen nur sicher eingesetzt werden. Daraus resultiert die Pflicht, die Vermögenswerte einer jeden Institution angemessen zu schützen. Das Bundesamt für Sicherheit in der Informationstechnik stellt den IT-Grundschutz kostenfrei zur Verfügung.

Wie gelingt den Institutionen der Umstieg auf den modernen IT-Grundschutz? Wie sieht die Planung für eine Migration von der klassischen auf den modernen IT-Grundschutz aus?

Um die obengenannten Fragen zu beantworten, wird zunächst ein Vergleich der BSI-Standards Reihe 100-x und 200-x durchgeführt. Neben Gemeinsamkeiten werden die Abweichungen mit Schwerpunkt auf die Absicherungsvorgehensweise aufgezeigt. Sobald die Ergebnisse des Vergleichs vorliegen, werden jene Migrationsaspekte betrachtet, mit denen effektiv und effizient der Umstieg auf den modernisierten IT-Grundschutz erfolgen kann. Als eine übersichtliche Darstellung des Vorhabens wird eine Transformation Roadmap entwickelt. Diese soll den Weg von der veralteten auf den modernisierten IT-Grundschutz übersichtlich darstellen.

Inhaltsverzeichnis

Abstract ... III
Inhaltsverzeichnis ... IV
1 Einleitung ... 1
1.1 Motivation ... 1
1.2 Zielsetzung der Arbeit ... 2
1.3 Aufbau der Arbeit ... 3
2 Grundlagen ... 4
2.1 Informationssicherheit ... 4
2.2 Informationssicherheitsmanagementsystem (ISMS) ... 7
2.3 Bundesamt für Sicherheit in der Informationstechnik (BSI) ... 9
2.4 IT-Grundschutz ... 11
3 Vergleich des klassischen und modernisierten IT-Grundschutzes ... 12
3.1 BSI-Standard 200-1: Managementsysteme für die Informationssicherheit ... 12
3.2 BSI-Standard 200-2: IT-Grundschutz-Methodik ... 19
3.2.1 Die Basisabsicherung ... 27
3.2.2 Die Kernabsicherung ... 33
3.2.3 Die Standardabsicherung ... 45
3.3 BSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz ... 50
3.4 BSI-Standard 100-4: Notfallmanagement ... 60
3.5 IT-Grundschutz-Kompendium ... 62
3.6 Absicherungsstrategien ... 73
3.7 Zertifizierung ... 75
4 Migration auf den modernisierten IT-Grundschutz ... 77
4.1 Migrationsvorhaben ... 77
4.2 Migrationstabellen ... 78
4.3 Entwicklung einer Transformation-Roadmap ... 82
4.3.1 Alternative 1 ... 84
4.3.2 Alternative 2 ... 86
4.3.3 Alternative 3 ... 87
5. Fazit ... 93
Literaturverzeichnis ... 95
Abbildungsverzeichnis ... 102
Abkürzungsverzeichnis ... 103
Glossar ... 105
Anhang ... 109

1 Einleitung

Dieses Kapitel verschafft dem Leser einen Überblick über die Motivation der Bachelorarbeit und deren Bedeutung. Es erläutert die Zielsetzung und Forschungsfragen der Arbeit. Der Schluss dieses Kapitels widmet sich dem Aufbau der Arbeit.

1.1 Motivation

Im Zeitalter digitaler Informationen wird die IT immer häufiger zum Angriffsziel von internen und externen Mechanismen. Die Auswirkungen eines erfolgreichen Angriffs können für den Geschäftsbetrieb katastrophal, unter Umständen existenzbedrohlich sein. Die Palette möglicher Schäden ist breit gefächert und die Konsequenzen reichen vom Verlust personenbezogener Daten über ausgefallene Systeme bis hin zu einem Imageschaden in der Öffentlichkeit. Doch das gilt nur für Institutionen, die sich mit der Informationssicherheit nicht beschäftigt haben oder ihre Assets nicht mit adäquaten Maßnahmen geschützt haben.

Im 21. Jahrhundert, der Blütezeit der IT, ist das Vernachlässigen der eigenen Informationssicherheit äußerst kritisch anzusehen. Laut einer Studie aus dem Jahre 2018 hat knapp ein Drittel der befragten Unternehmen ein bereits funktionierendes Managementsystem für Informationssicherheit eingeführt. [1] Dies ist insofern erstaunlich, als jeden Tag mehrere kritische Fehler in IT-Systemen, Informationsverluste großer Unternehmen hohe Wellen durch die Medien schlagen. Informationssicherheit sollte in der Öffentlichkeit ernster genommen werden. Eine Möglichkeit zur Verbesserung der Informationssicherheit ist das Informationssicherheitsmanagementsystem (ISMS).

Die Voraussetzungen für ein erfolgreiches Managementsystem für Informationssicherheit sind klar definiert: Gegenstand und Methode. Viele Unternehmen stellen die Frage: Was kann ich machen, um meine Informationen zu schützen? Wie kann ich es verwirklichen?

Im Jahr 1994 entwickelte das Bundesamt für Sicherheit in der Informationstechnik (BSI) den IT-Grundschutz zum Schutz der eigenen Informationen und stellte ihn anschließend kostenfrei zur Verfügung. [2] IT-Beratungsunternehmen greifen Institutionen unter die Arme und bieten ihre Unterstützung an, z. B. in Form von Beratungen und Umsetzungshilfe bei der Etablierung eines ISMS nach dem IT-Grundschutz. Das ist für Organisationen eine Option gegen die Bedrohung der Informationssicherheit und für den Ausbau eines angemessenen Schutzniveaus.

Aufgrund neu entwickelter Technologien und steigender Komplexität entschloss sich das BSI dazu, einen modernisierten IT-Grundschutz auszuarbeiten. Dieser wurde im Herbst 2017 veröffentlicht und erfüllt die Anforderungen an ein dem aktuellen Stand der Technik angemessenes Sicherheitsniveau. [3]

Am Ende dieser Abschlussarbeit lassen sich folgende Forschungsfragen erfolgreich beantworten:

1. Welche Unterschiede gibt es zwischen dem klassischen und dem modernisierten IT-Grundschutz?
2. Wie wird erkannt, welche bereits umgesetzten Maßnahmen aus dem klassischen IT-Grundschutz sich migrieren lassen?
3. Wie sieht die Transformation Roadmap aus, die einen Überblick über den Weg zum Umstieg auf den modernisierten IT-Grundschutz verschafft?

1.2 Zielsetzung der Arbeit

Aus den obigen Forschungsfragen leiten sich die Ziele dieser Arbeit ab. Zunächst werden die wesentlichen Unterschiede zwischen den IT-Grundschutz-Dokumenten der beiden Versionen herausgearbeitet. Das nächste Ziel ist die generische Analyse des Ist- und Soll-Zustandes in einer Organisation, die ihre Assets bereits nach der klassischen Vorgehensweise des veralteten IT-Grundschutz umgesetzt hat. Das dritte und letzte Ziel soll Auskunft darüber geben, wie der Umstieg von der klassischen auf den modernisierten IT-Grundschutz möglichst effektiv und effizient vollzogen werden kann. Dies soll in Form einer Transformation Roadmap dargestellt werden.

Die Ziele der vorliegenden Arbeit sollen dem IT-Beratungsunternehmen Capgemini bei der Beratung ihrer Kunden zum Thema Anwendung und Umstieg von der veralteten auf den modernisierten IT-Grundschutz des BSI helfen.

1.3 Aufbau der Arbeit

Die vorliegende Arbeit gliedert sich in fünf Kapitel.

Dieser einleitende Teil der Arbeit greift die Problematik auf und dient als Basis für die drei zuvor formulierten Forschungsfragen, die im Laufe der Bachelorarbeit ausgearbeitet und beantwortet werden.

Im zweiten Kapitel findet eine Thematisierung der Grundlagen statt. Hier werden die wesentlichen Begriffe und Definitionen erläutert. Unter anderem lernt der Leser das *Managementsystem für Informationssicherheit* und den vom BSI entwickelten *IT-Grundschutz* kennen.

Im dritten Kapitel wird ein Vergleich zwischen dem klassischen und modernisierten IT-Grundschutz durchgeführt. Dabei wird es insbesondere auf die Darstellung des modernen IT-Grundschutzes eingegangen. Neben der Analyse von Dokumenten des IT-Grundschutzes bildet die neue Methodik bei der Absicherung der Institutionen den Kern des Kapitels.

Im vierten Kapitel beschäftigt sich der Autor mit der Planung der *Migration*. Institutionen, die die Maßnahmen nach dem klassischen IT-Grundschutz umgesetzt haben, möchten wissen, welche Teile sich migrieren lassen und wie viel Aufwand auf sie zukommt, damit sie den Anforderungen des aktualisierten IT-Grundschutzes entsprechen. Die Grundannahme ist, dass bereits erzielte Ergebnisse in den neuen IT-Grundschutz „umgezogen“ werden können.

Im fünften und letzten Kapitel erfolgt eine kurze, präzise Zusammenfassung der Ergebnisse des Hauptteils.

2 Grundlagen

In diesem Kapitel wird der Leser über die Grundlagen der Informationssicherheit aufgeklärt. Zunächst wird der Begriff Informationssicherheit (IS) konkretisiert. Darauf aufbauend erfolgt die Beschreibung eines Managementsystems für die Informationssicherheit (ISMS). Anschließend wird der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) konzeptionierten IT-Grundschutz vorgestellt.

2.1 Informationssicherheit

Die Informationen einer Institution sind heutzutage vielen Gefahren ausgesetzt. Diese stammen nicht nur aus der digitalen Welt, sondern können sowohl materielle als auch immaterielle Informationen als Ziel haben. Die Gesamtheit der Maßnahmen, die den Schutz von technischen (soziotechnischen) und nicht-technischen (nicht-soziotechnischen) Systemen gewährleisten und das Ziel verfolgen, Informationen vor Gefahren oder Manipulationen und den daraus resultierenden wirtschaftlichen Schäden zu schützen, wird als Informationssicherheit bezeichnet. [4]

In der Fachsprache werden mehrere Begriffe unterschieden, die sich mit der Sicherheit der Vermögenswerte von Organisationen beschäftigen. Diese werden oft fälschlicherweise benutzt, da die allgemeine Unterscheidung in der Öffentlichkeit keine große Rolle spielt. Die Abgrenzung benutzen meistens lediglich Fachleute aus dem Bereich Informationssicherheit. So erwähnt auch das BSI, dass der Begriff IT-Sicherheit häufig verwendet wird, da im modernen Sprachgebrauch das Wort „IT“ gerne benutzt wird. [5]

Eine Untersuchung des Zusammenhanges zwischen den Begriffen „Informationssicherheit“, „IT-Sicherheit“ und „Cyber-Sicherheit“ ist daher unerlässlich. Sie alle thematisiert die verschiedenen Dimensionen des Schutzes von Informationen. Unter Informationssicherheit wird der Schutz von technischen und nicht-technischen Systemen verstanden. Dies beinhaltet nicht nur den Schutz der Daten aus technischer Sicht, sondern auch die personellen und organisatorischen Maßnahmen. Der Begriff IT-Sicherheit ist nur ein Teilgebiet der Informationssicherheit. Hier werden explizit jene Informationen geschützt, die durch IT-Systeme verarbeitet werden. Die Form der geschützten Werte ist also digital und elektronisch. Der Begriff Informationssicherheit ist weit umfassender und beinhaltet alle Teilaspekte des sicheren Umgangs mit Informationen. [6] In der deutschen Fachliteratur kann die Unterscheidung beider Begriffe zu Verwirrung führen. Sie werden in der deutschen Sprache oft gleichgesetzt; demgegenüber bietet die englische Fachsprache eine präzisere Definition: Die Funktionssicherheit (engl.: safety) konzentriert sich auf die ordnungsgemäße Funktionalität der Systeme. Hingegen entspricht der deutsche Begriff Informationssicherheit dem englischen Begriff „security“. Letzterer ist durch das Vorbeugen von Sicherheitsvorfällen charakterisiert. [7]

Cyber-Sicherheit (Cyber Security) umfasst das Aktionsfeld der IT-Sicherheit und beinhaltet dabei den gesamten Cyber-Raum. Dazu gehört die Informationstechnik, die mit dem Internet und vergleichbaren Netzen verbunden ist. Dazu zählen unter anderem Kommunikationsnetze, Anwendungen, Prozesse und verarbeitete Informationen. Die Bezeichnung Cyber Security erfreut sich großer Beliebtheit in der Öffentlichkeit. [8]

Folgende Grafik verdeutlicht den Zusammenhang zwischen den verschiedenen Begriffen:

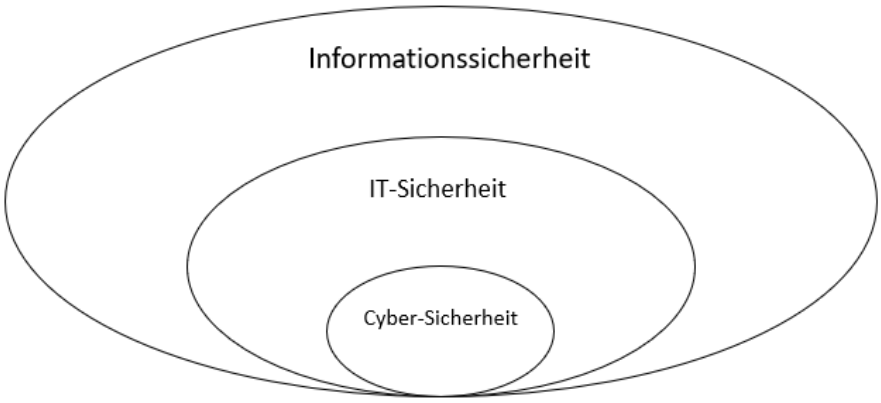

Abbildung 1: Zusammenhang zwischen Sicherheitsbegriffen, eigene Darstellung

Die beliebtesten Methoden für die Sicherstellung von Informationen in Organisationen sind in der internationalen Standardreihe *ISO/IEC-27000* und in dem in Deutschland verbreiteten *IT-Grundschutz* beschrieben. [9] Die umgesetzten Methoden lassen sich zertifizieren. Die umgesetzten Maßnahmen der ISO/IEC-27000-Reihe werden häufig dem Prüfplan *ISO/IEC 15408 (Common Criteria for Information Technology Security Evaluation)* unterzogen. [10] Das BSI bietet für Anwender des IT-Grundschutzes einen eigenen Zertifizierungsprozess.[11]

Gegenstand der Informationssicherheit sind unter anderem Prozesse, Anwendungen, Systeme, Infrastruktur, Kommunikation und Informationen. Informationen können als Daten in digitaler Form abgespeichert werden oder können sich auf das Immaterielle wie z. B. Wissen der Mitarbeiter beziehen.

In der Informationssicherheit werden Sicherheitsziele durch drei Grundwerte bewertet. Diese Sicherheitskriterien werden oft als CIA Prinzipien (CIA Triad) oder Schutzziele bezeichnet. Die Abkürzung setzt sich aus dem Anfangsbuchstaben der Grundwerte in englischer Sprache zusammen.

- *Vertraulichkeit (Confidentiality)*: Vertrauliche Informationen dürfen nur ausgewählten Personenkreisen zugänglich sein.
- *Integrität (Integrity)*: Unbefugte dürfen die Daten nicht verändern.
- *Verfügbarkeit (Availability)*: Die Funktionalität von Diensten und Ressourcen darf nicht beeinträchtigt werden. [7] [12]

Neben den übergeordneten Schutzzielen erwähnt die Literatur davon abgeleitete Schutzziele, die sich mit Anonymität, Unbeobachtbarkeit, Verdecktheit, Zurechenbarkeit, Rechtsverbindlichkeit und Erreichbarkeit beschäftigen. [13]

Die übergeordneten und die abgeleiteten Schutzziele weisen einen Zusammenhang auf. Schutzziele können sich gegenseitig verstärken, schwächen oder andere Grundziele implizieren. Die Wechselwirkung zwischen den Schutzzielen wird durch das folgende Bild verdeutlicht:

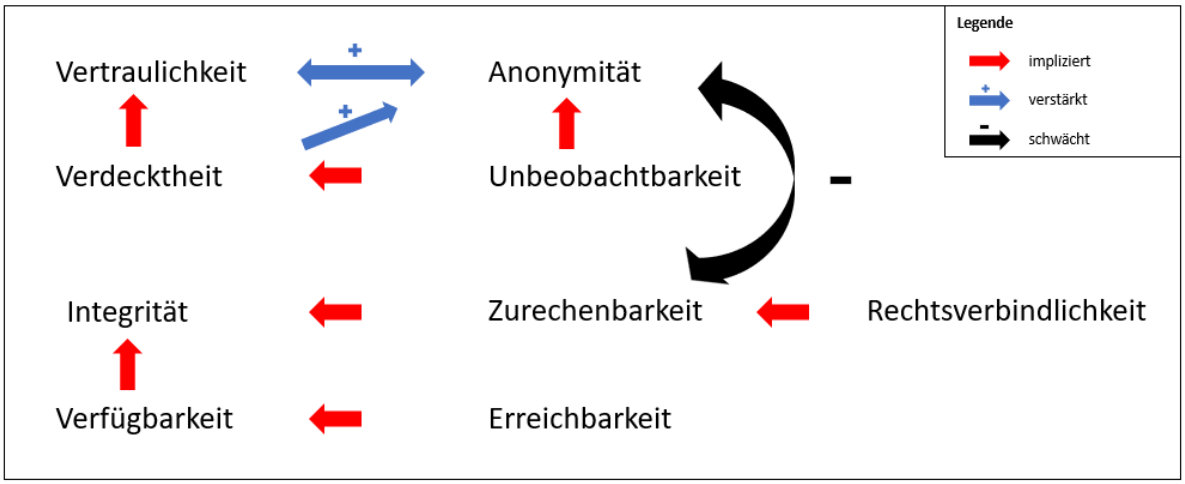

Abbildung 2: Wechselwirkung zwischen Schutzzielen, eigene Darstellung in Anlehnung an [13]

2.2 Informationssicherheitsmanagementsystem (ISMS)

In der heutigen Literatur ist keine eindeutige Begriffsdefinition über ein ISMS zu finden. Doch die meisten Erklärungen liefern dieselben Anforderungen an ein ISMS und dessen Aufgaben. Zunächst wird ein Versuch unternommen, das ISMS zu definieren. Nach Stefan Becks Übersetzung aus der ISO/IEC 27000:2014 wird folgende ISMS-Definition als Ausgangspunkt deklariert:

„Ein ISMS besteht aus Politiken, Verfahren, Richtlinien und den damit in Verbindung stehenden Ressourcen und Aktivitäten, die ganzheitlich von einer Organisation mit dem Ziel gemanagt werden, ihre Informationen zu schützen. Ein ISMS ist ein systematischer Ansatz für Aufbau, Einführung, Betrieb, Überwachung, Überprüfung, Pflege und Verbesserung der Informationssicherheit einer Organisation, um ihre Ziele zu erreichen.“ [14]

Ein Informationssicherheitsmanagementsystem lässt sich am besten durch die an das System gerichtete Anforderungen und Aufgaben charakterisieren. [15]

Folgende Anforderungen werden an das ISMS gestellt:

- Zielvorgabe formulieren
- Chancen und Risiken in Zusammenhang mit den definierten Zielen analysieren
- Rollen und Verantwortlichkeiten definieren
- Methoden zur Zielerreichung angeben
- Regelwerke, Richtlinien in Zusammenhang mit der Informationssicherheit beachten
- Prozessschritte planen, umsetzen
- Zielerreichung evaluieren

Aufgaben:

- Sicherheitsziele formulieren
- Assets der Organisation bestimmen
- Risikomanagement für die Assets durchzuführen
- kontinuierliche Verbesserung

Das Managementsystem hat die Hauptaufgabe Informationen einer Organisation unabhängig von deren Form (z. B. physisch, digital) zu schützen. Der angemessene und effektive Schutz der Assets ist durch die Sicherstellung der drei Grundwerte der Informationssicherheit zu gewährleisten. Die bereits im Kapitel 2.1 erwähnten Schutzziele sind Vertraulichkeit, Integrität und Verfügbarkeit.

Unter Annahme der obigen Definition leitet sich folgende Zusammenfassung ab:

Das ISMS ist eine Sammlung von Verfahren, Richtlinien, Prozessen, die dazu dienen Handlungen bezüglich der Informationssicherheit einer Institution zu steuern, zu überwachen und zu dokumentieren.

Als ISMS wird die systematische Herangehensweise und die Gesamtheit aller eingesetzten Ressourcen bezeichnet, um die wesentlichen Ziele der Informationssicherheit zu ermitteln und zu erreichen. Dies ist jedoch kein permanenter Zustand. Ein effektiver Schutz der Informationen kann ausschließlich durch eine kontinuierliche Verbesserung erreicht werden. Aus diesem Grund ist das ISMS als eine Prozesskette anzusehen. Das System wird nach Bedarf überprüft und gegebenenfalls erweitert und optimiert.

Der Geltungsbereich (engl.: *scope*) des ISMS erstreckt sich meist über die gesamte Organisation. Selten kommt ein ISMS ausschließlich in Teilbereichen zum Einsatz. Hierzu muss ein triftiger Grund vorliegen, denn Aufwandsersparnis durch die Verkleinerung des Geltungsbereichs ist in diesem Fall nicht effektiv.

Beck benennt zusätzliche Effekte, die ein erfolgreiches ISMS charakterisieren können. [16] Neben dem Schutz der Assets der Institution, bietet ein effektives System auch eine *Vertrauensumgebung*. Dies gilt sowohl für die innerbetriebliche Organisation als auch für den Markt. Das ISMS symbolisiert nach außen hin den Aufwand und die Bemühungen der Organisation mit all ihren Vermögenswerten verantwortungsbewusst umzugehen. Interessenkreise können dadurch mehr über die Organisation in Erfahrung bringen und in eine Vertrauensbeziehung mit der Organisation eingehen.

Der zweite Effekt, den Beck erwähnt, ist die *Governance*-Funktion. Damit wird eine Führungs- und Lenkungsform beschrieben, die innerhalb einer Organisation fungiert. Die Vorteile von Governance erstrecken sich von der Rechenschaftspflicht gegenüber Stakeholdern bis zur transparenten Darstellung der Ergebnisse. Dies ist notwendig, denn Unternehmen kommunizieren oft nur Ergebnisse, die ihren Vorstellungen entsprechen und sie in einem besseren Licht darstellen. Die Problematik ist dabei die Geheimhaltung der ungünstigen Ergebnisse vor Interessierten. Ohne Kenntnis aller Ergebnisse kann keine objektive, umfassende Beurteilung der Organisation erfolgen. Durch die Transparenz der Governance-Funktion offenbart die Institution ihre tatsächliche Situation.

Diese Effekte können nach einem erfolgreichen Zertifizierungsprozess einen besonders großen Stellenwert erlangen und als international anerkanntes Zeichen für ein effektives ISMS gelten, auf das sich Geschäftspartner und Kunden verlassen können.

2.3 Bundesamt für Sicherheit in der Informationstechnik (BSI)

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist eine Bundesbehörde der Bundesrepublik Deutschland, die für Fragen der IT-Sicherheit in der öffentlichen Ver-

waltung, in Unternehmen und für Privatanwender zuständig ist. Das im Jahr 1991 gegründete BSI ist dem Geschäftsbereich des Bundesamtes des Innern, für Bau und Heimat untergegliedert. [17]

Das BSI beschäftigt sich mit Themen rund um die IT-Sicherheit in der Informationsgesellschaft. Das BSI hat als sich Ziel gesetzt, den deutschlandweiten, sicheren Einsatz von Informations- und Kommunikationstechnik (IKT) in der heutigen Gesellschaft zu ermöglichen und zu fördern. Zum Adressatenkreis des BSI gehören neben der deutschen Verwaltung, öffentliche und private Institutionen auch Privatanwender. [18]

Ein besonderes Augenmerk legt das BSI auf die präventive Förderung der Informations- und Cybersicherheit in der Öffentlichkeit. Durch die Unterstützung des BSI sind Gesellschaftsmitglieder zum Schutz ihrer Informationen und IT-Systeme motiviert. Darüber hinaus hat die Bundesbehörde zur Aufgabe, ein Bewusstsein für den Schutz der IT-Systeme und Informationen zu wecken. Neben der Sensibilisierung der gesellschaftlichen Akteure für die IT-Sicherheit und die Warnungsfunktion bei gefährlich eingestuften IT-Produkten zählt u. a. die Bundesregierung in IT-bezogenen Fragen zu beraten und deren IT-Systeme zu schützen zu den wichtigsten Aufgabengebieten des BSI. [17]

Neben technischen Aufgaben erfüllt das BSI eine fachliche Funktion. Dies zeichnet sich durch die Entwicklung von Standards und die Zertifizierungsfunktion aus. Das BSI ist ebenfalls eine Zertifizierungsstelle bei sicherheitsbezogenen Themen. Somit können neben IT-Produkten und -Dienstleistungen, Managementsysteme auch Personen mit geeigneter Kompetenz mit einem Zertifikat akkreditiert werden. [19]

Wie erreichen Sie das? Das BSI erreicht sein Ziel, indem es praxisorientierte Standards zum angemessenen und effektiven Schutz von Informationen veröffentlicht. Neben Standards erarbeiten es zielgruppengerechte Handlungsempfehlungen zur IT- und Internet-Sicherheit, um Anwender bei der Vermeidung von Risiken zu unterstützen.

2.4 IT-Grundschutz

Das BSI steht nicht nur mit Rat, sondern auch mit Tat zur Seite, denn einer der Hauptaufgaben ist die Prävention im Bereich Informationssicherheit. Das Konzept sieht vor, Diskrepanzen von Institutionen zu beheben und somit einen negativen Ausgang bei Sicherheitsvorfällen zu vermeiden. Es wird beabsichtigt, dass Institution nicht in eine Notlage geraten. Dies wird realisiert, indem Vorbeugungsmaßnahmen implementiert werden. Der IT-Grundschutz gilt in der Verwaltung und Wirtschaft als Maßstab, wenn es um die Absicherung von Informationen und den Aufbau eines Managementsystems für Informationssicherheit (ISMS) geht.

Der IT-Grundschutz ist eine vom BSI entwickelte Methodik, um das Niveau der Informationssicherheit in Institutionen zu erhöhen. Der IT-Grundschutz vom Bundesamt für Sicherheit in der Informationstechnik enthält verschiedene Standards und Katalogen, die einheitliche Vorgehensmodelle zum Schutz der eingesetzten Informationstechnik in Institutionen beschreiben.

Die Methodik eignet sich für Institutionen jeder Größe, jedoch wurde diese speziell für die Verwaltungsebene konzipiert. Außerdem ist die Vorgehensweise bei kleinen und mittleren Unternehmen (KMU) besonders beliebt. Die Methodik hat sich über die Jahre als Mindeststandard der Absicherung von IT-Systemen bewährt. Der IT-Grundschutz zeichnet sich durch die Kompatibilität mit dem beliebten Standard ISO 27001 aus.

Das BSI hat den IT-Grundschutz mit dem Ziel kreiert, Institutionen ein angemessenes und einheitliches Mindestniveau an Sicherheit in der Informationstechnik zu liefern. Das Konzept sieht vor die Umsetzung der empfohlenen Sicherheitsmaßnahmen, um dieses Ziel zu erreichen. [20]

3 Vergleich des klassischen und modernisierten IT-Grundschutzes

Dieses Kapitel stellt den modernisierten IT-Grundschutz dem klassischen IT-Grundschutz gegenüber. Das Kapitel stellt Bestandteile des modernisierten IT-Grundschutzes vor und geht dabei auf Abweichungen zwischen den Editionen ein.

3.1 BSI-Standard 200-1: Managementsysteme für die Informationssicherheit

Ziel dieses Kapitel ist es, einen groben Überblick über den BSI-Standard 200-1 [21] und das Aufzeigen der Differenzen zwischen den beiden Editionen zu geben.

Die BSI-Standards stellen wesentliche Bestandteile des IT-Grundschutzes dar. Sie beschreiben mehrere Empfehlungen zu Methoden, Vorgehensweisen und Maßnahmen auf verschiedene Abstraktionsebene der Informationssicherheit.

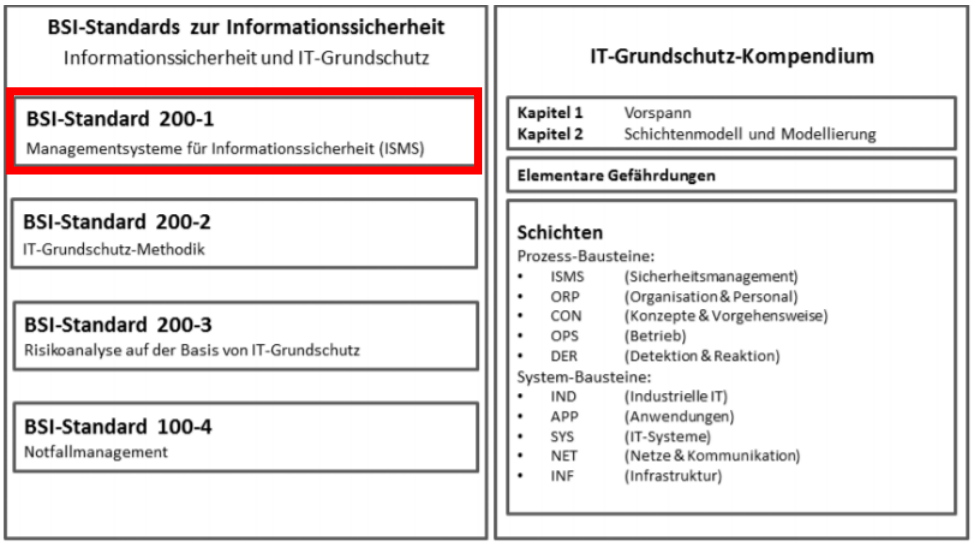

Abbildung 3: Der moderne IT-Grundschutz [21]

Der BSI-Standard 200-1 enthält generisch gehaltene Anforderungen zur Gestaltung eines funktionierenden ISMS. [21] Wie der gesamte IT-Grundschutz, so sind ihre Bestandteile ebenfalls kompatibel zum ISO/IEC 27001. Der BSI-Standard 200-1 gliedert sich in 10 Kapitel und stellt die überarbeitete Edition des BSI-Standards 100-1 aus dem klassischen IT-Grundschutz dar.

Neben inhaltlichen Veränderungen ist der Standard in eine leserfreundlichere Version überführt worden. Der neue Standard setzt viel mehr Wert auf die Gestaltung des Dokuments als sein Vorgänger. Das neue Layout sorgt für eine bessere Handhabung für Anwender. Die neue Struktur und die einheitlichen Formatierungen wirken augenschonend, was – in Anbetracht auf den Umfang des IT-Grundschutzes – sehr erfreulich ist. Eine ausgeprägte Kennzeichnung der Seiten mit den jeweiligen Überschriften schafft Klarheit beim Lesevorgang und informiert den Leser über das aktuelle Kapitel.

Einleitung

Gleich zum Beginn der Einleitung greift die Zielsetzung wichtige Aspekte der Informationssicherheit auf. Die stets zunehmende Abhängigkeit von der IT kann dabei nicht außer Acht gelassen werden. Der steigende Digitalisierungsgrad und neue technologische Entwicklungen ebnen den Weg für die Informationssicherheit in die moderne Welt. Die Breite des IT-Spektrums deckt nahezu alle Bereiche des modernen Lebens ab. Für die Modernisierung des IT-Grundschutzes spricht, dass der klassische IT-Grundschutz Innovationen, wie Internet of Things oder Cloud Computing-Technologien, die während der Lebensspanne des klassischen IT-Grundschutzes teilweise noch nicht existierten, nicht oder nicht genügend abdeckte. Denn letztlich kommen Innovationen zuerst – Bedenken über Sicherheitsaspekte erst danach. Doch der Schutz der Informationen aller Art ist unabdingbar.

Einführung in die Informationssicherheit

Nach der Einleitung führt der Standard den Leser in die informationssicherheitsbezogenen Normen und Standards ein. In der Version 100-2 waren weiterführende Standards enthalten, jedoch ist die Differenzierung zwischen Normen und Standards inzwischen neu formuliert worden. Normen sind die Gesamtheit von Anforderungen an verschiedene Produkte, Dienstleistungen oder Verfahren, die durch Normungsorganisationen veröffentlicht werden. Standards bezeichnen hingegen allgemein anerkannte und angewandte Arten von Leistungen, die sich gegenüber etwas Gleichartigem durchgesetzt hat. Der Standard bezeichnet

Regelwerke der ISO und IEC als ISO-Normen. Im Weiteren erwähnt das Dokument neben allgemeingültigen Werken auch sektorspezifische Normen.

Eine weitere und schärfere Trennung findet zwischen den Begriffen IT-Sicherheit, Informationssicherheit und Cyber-Sicherheit statt, die hier bereits in Kapitel 2.1 erläutert wurden.

Um einen Bezug zu anderen Praktiken und maßgebenden Dokumenten herzustellen, wurden weitere Sicherheitsstandards in das Dokument aufgenommen. So findet sich eine kurze Beschreibung von COBIT 5, ITIL, PCI DSS, NIST und ISF am Ende des Kapitels. Die Erwähnung der Standards zielt darauf ab, Anwender zur weiteren Recherche mit Bezug zur Informationssicherheit zu motivieren.

ISMS-Definition und Prozessbeschreibung

Das dritte Kapitel fasst die Anforderungen an das Informationssicherheitsmanagementsystem zusammen. Der BSI-Standard 200-1 bezeichnet als grundlegende Komponenten eines ISMS die Managementprinzipien, die Mitarbeiter, die zur Verfügung stehenden Ressourcen und den standardisierten Sicherheitsprozess. Grundlagen zum Thema ISMS wurden bereits in Kapitel 2.1 angesprochen. Darüber hinaus wird die Steuerung des ISMS als Managementaufgabe dargestellt, die über Instrumente und Methoden die Informationssicherheit lenken kann. Der Sicherheitsprozess umfasst das Sicherheitskonzept, die Sicherheitsorganisation und die Dokumentation beider Aspekte, d. h. die Leitlinie zur Informationssicherheit. Es wird klar, dass die Sicherheit kein permanenter Zustand sein kann, sondern ein Prozess, der gepflegt und aufrechterhalten werden muss. Das BSI bezieht sich auf den allgemein bekannten Deming Kreislauf (PDCA Zyklus). Im PDCA-Zyklus (Akronym aus dem englischen Anfangsbuchstaben der Phasen) stellen die einzelnen Phasen die Aufgaben des Sicherheitsprozesses in chronologischer Reihenfolge dar. Der Prozess beginnt mit der Planung und Konzeption („Plan“), die als Entwurf der Strategie zur Sicherheit abgebildet werden kann, um anschließend umgesetzt („Do“) zu werden. Um die Zielerreichung zu prüfen, wird die Erfolgskontrolle eingeleitet („Check“). Die Kontinuität und Langlebigkeit des Prozesses zu unterstützen, werden Optimierungen und Verbesserungen („Act“) durchgeführt.

Management-Prinzipien

Kapitel 4 stellt im Wesentlichen die Aufgaben und Pflichten des Managements dar. Die Führungsebene übernimmt die Verantwortung für das Initiieren, Steuern und Kontrollieren der Informationssicherheit in der Organisation. Der Standard bezeichnet die Informationssicherheit als Querschnittsfunktion und nennt konkrete Bereiche (Projektmanagement, Incident Management), deren Einführung sinnvoll ist. Der verantwortungsbewusste Umgang mit Ressourcen ist ebenso Aufgabe des Managements, wie die Vorbildfunktion oder die Ermutigung von Organisationsmitarbeiter, Sicherheitsregeln zu befolgen. Die Managementebene sorgt ebenfalls für den reibungslosen Informationsfluss innerhalb der Organisation. Abschließend initiiert sie die Erfolgskontrolle, mit der die umgesetzten Maßnahmen auf Angemessenheit und Effektivität überprüft werden.

Durch die Neustrukturierung der Themen ergibt sich eine veränderte Reihenfolge, der Inhalt ist jedoch identisch, wie im BSI-Standard 100-1. [22]

Ressourcen für Informationssicherheit

In Kapitel 5 rücken die Ressourcen für die Informationssicherheit in den Vordergrund. Der Schutz von Assets einer Organisation kann mit hohen zeitlichen und finanziellen Aufwänden verbunden sein. Das BSI appelliert an Anwender des IT-Grundschutzes sowie an die Leitungsebene, mit Ressourcen verantwortungsvoll umzugehen. Ein ressourcenverschwenderisches Verhalten kann negative Auswirkungen auf die Organisation, sowie auf die Gesamtbeurteilung des ISMS innerhalb der Institution haben.

Einbindung der Mitarbeiter in den Sicherheitsprozess

Kapitel 6 betont die Notwendigkeit der Einbindung der Mitarbeiter in den Sicherheitsprozess. Um ein ISMS vollständig zu etablieren, ist es notwendig, unter den Beteiligten für ausreichendes Verständnis zu sorgen. Mitarbeiter müssen den Nutzen und die Risiken sowie ihre Aufgaben und Pflichten in Bezug auf das ISMS kennen. Dies kann bspw. durch Sensibilisierungsaktionen oder zusätzlichen Schulungen erreicht werden. Im Fokus steht die allgemeine Akzeptanz bzw. die allgemeine Unterstützung des Managementsystems innerhalb der Organisation.

Der Sicherheitsprozess

Kapitel 7 fasst die detaillierten Phasen des Sicherheitsprozesses zusammen. Um einen erfolgreichen Sicherheitsprozess zu etablieren, sind verschiedene Aspekte zu beachten. Dazu gehört u. a. die Ermittlung der aktuellen Rahmenbedingungen im unternehmenseigenen und regulatorischen Umfeld. Die Leitlinie soll die definierten Sicherheitsziele und weitere Kernaussagen der Sicherheitsstrategie enthalten. Die Auswahl des Informationsverbunds, in dem das ISMS eingesetzt wird, schafft Klarheit, welche Bereiche und Prozesse in der Organisation dadurch abgedeckt sind. Wie bereits erwähnt, trägt das Management die Verantwortung für eine ausreichende Sicherheit. Für die bessere Koordination des Sicherheitsprozesses bietet es sich an, eine Sicherheitsorganisation aufzubauen. Bei kleineren Behörden und Unternehmen besteht diese Organisationsart häufig aus einer Person, typischerweise dem Informationssicherheitsbeauftragten (ISB). Die umgesetzten Maßnahmen für die Informationssicherheit bedeuten keinen dauerhaften Schutz. Ein stetiger Schutz kann ausschließlich durch die Aufrechterhaltung und Pflege des ISMS erzielt werden. Die Gestaltung der Reihenfolge im BSI-Standard 200-1 weicht geringfügig von seinem Vorgänger ab, jedoch nicht der Inhalt.

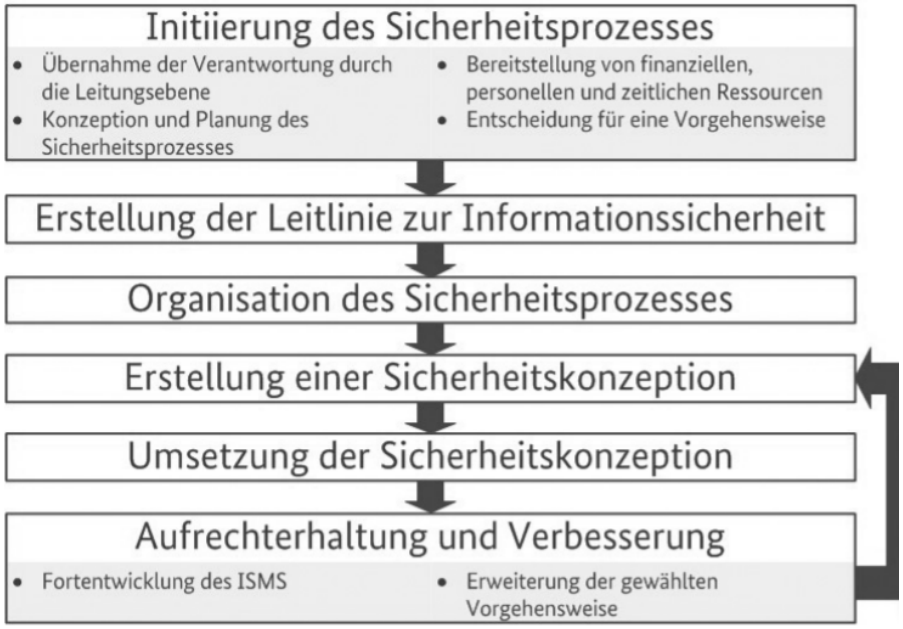

Abbildung 4: Der Sicherheitsprozess gemäß BSI-Standard 200-1 [21]

Sicherheitskonzept

Kapitel 8 beschäftigt sich mit der Erstellung und Umsetzung des Sicherheitskonzepts. Zunächst ist eine Methode zur Risikoanalyse auszuwählen. Analysiert werden Bedrohungen, die Schäden für den Geschäftsbetrieb verursachen können. Die Klassifizierung der Risiken errechnet sich durch die Einflussfaktoren, Schadenspotenzial und Eintrittswahrscheinlichkeit. Um angemessene Maßnahmen dagegen umzusetzen, muss die Institution zunächst wissen, wo die Schwachstellen liegen und wie diese Risiken zu beurteilen sind. Die Auswahl der Risikoanalysemethode soll dabei als Startpunkt fungieren. Nachdem Risiken identifiziert werden, kommt es zur Entscheidung, wie mit diesen umgegangen wird. Unter Berücksichtigung der Risikoakzeptanzkriterien erstellt die Organisation ein strategisches Dokument zum Umgang mit den Risiken, der sich auf mehrere Strategien verteilen kann. Diese können Verhalten vorsehen, um z. B Risiken zu vermeiden (komplette Beseitigung der Bedrohungen), zu reduzieren (Verkleinerung des Schadenspotenzials), zu transferieren (an Dritte übertragen) oder zu akzeptieren. Das Thema wird im BSI-Standard 200-3 Risikoanalyse auf einer tieferen, detaillierten Ebene behandelt.

Die Anzahl und Anforderungen an konkreten Sicherheitsmaßnahmen leiten sich aus den allgemeinen Sicherheitszielen ab. Unter Beachtung der Faktoren zur Wirtschaftlichkeit und Praxistauglichkeit wird die Bestimmung und Auswahl der Maßnahmen durchgeführt, um das vorgestellte Sicherheitsniveau zu erfüllen.

Der Erstellung des Sicherheitskonzepts folgt die Realisierungsphase, in der die Umsetzungsreihenfolge und Verantwortlichkeiten bestimmt sowie Ressourcen bereitgestellt werden. Danach setzt die Institution die geplanten Sicherheitsmaßnahmen um.

Um die Umsetzung der als notwendig erachteten Maßnahmen auf Effektivität und Effizienz zu überprüfen, ist eine Bewertung durchzuführen.

Zertifizierung des ISMS

Kapitel 9 führt nach der Etablierung des Managementsystems für die Informationssicherheit zum Thema Zertifizierung über. Die vorliegende Arbeit beschreibt die ISMS-Zertifizierung im Kapitel 3.7.

Das ISMS auf Basis von BSI IT-Grundschutz

Mit dem letzten Kapitel wird das auf Basis des IT-Grundschutzes etablierte ISMS aufgegriffen und führt das Thema zum nächsten Standard in der BSI-Reihe über.

Die Einführung eines Managementsystems für die Informationssicherheit in eine bestehende Organisation ist eine herausfordernde Aufgabe. Der aktuelle IT-Grundschutz definiert die Anforderungen an das ISMS, so bleibt ein großer Gestaltungsspielraum der Institutionen für die Umsetzung der allgemeingültigen Vorgaben. Die zentrale Herausforderung ist die Entwicklung einer auf die Organisation maßgeschneiderten Sicherheitskonzeption. Nach dem Erstellen des Sicherheitskonzepts stellt sich die Frage, welche Vorgehensweise für die Organisation geeignet ist.

Die IT-Grundschutz-Methodik enthält verschiedene Vorgehensweisen zum Erreichen des gewünschten Sicherheitsniveaus. Die vom BSI vorgeschlagenen Vorgehensweisen beinhalten nicht nur unterschiedliche Aktionsschritte, sondern jede Vorgehensweise ist mit einem abweichenden Aufwand verbunden. Der IT-Grundschutz setzt sich mit dem BSI-Standard 200-2 fort, der die IT-Grundschutz-Methodik beschreibt.

Fazit

Insgesamt weicht der Inhalt des BSI-Standards 200-1 nicht allzu sehr von seinem Vorgänger ab. Der Großteil der Überarbeitung entstand aus Anpassungen und sprachlichen Präzisierungen. Differenzierung zwischen Norm und Standard, Erweiterung der zu schützenden Technologien nach dem aktuellen Stand der Technik und leichte Strukturänderung im Dokument gehören zu den wesentlichen Resultaten des Vergleichs. [21] [22]

3.2 BSI-Standard 200-2: IT-Grundschutz-Methodik

Ziel dieses Kapitels ist es, einen groben Überblick über den BSI-Standard 200-2 zu geben und die Differenzen zwischen den beiden Editionen aufzuzeigen.

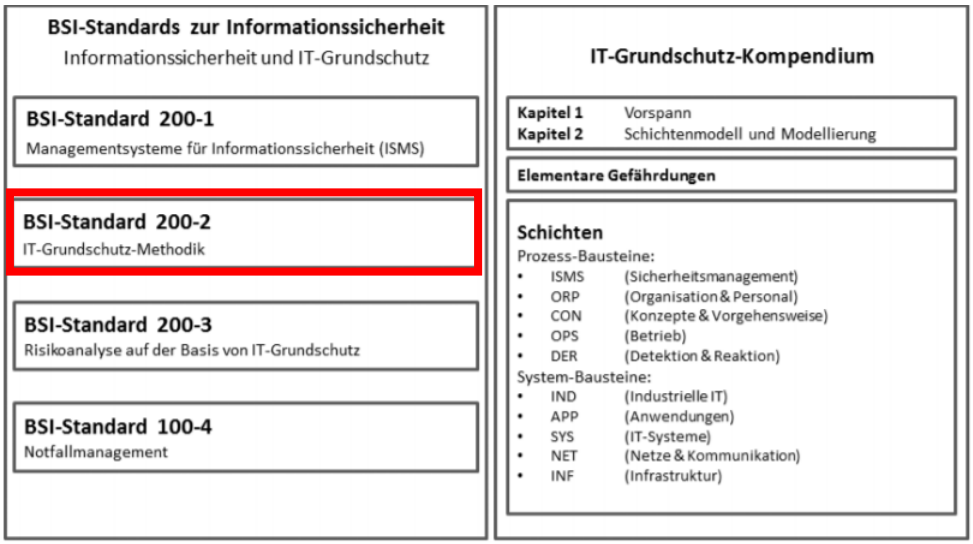

Abbildung 5: Der moderne IT-Grundschutz [21]

Der BSI-Standard 200-2 gliedert sich in 12 Kapitel und bildet eine grundlegende Basis für die bewährte BSI-Methodik zum Aufbau eines soliden ISMS. Der zu beschreibende Standard löst den BSI-Standard 100-2 ab und gilt seit Herbst 2017 als wesentlicher Bestandteil des modernisierten IT-Grundschutzes. Der Standard wurde neu konzipiert; die grundlegende Methodik blieb jedoch aus dem Vorgängerstandard erhalten. Die bewährte Methodik zur Informationssicherheit lässt sich auf Organisationen verschiedener Größe beliebig skalieren und bietet dadurch die Chance zum Einsatz in einem weiten Umfeld. [23] [24]

Einleitung

Kapitel 1 verschafft dem Leser einen kurzen Überblick über die wichtigsten Änderungen und definiert die IT-Grundschutz-Methodik zum Aufbau und zur Aufrechterhaltung eines

angemessenen Managementsystems für die Informationssicherheit. Die im Kapitel 3.1 beschriebenen Layouteänderungen gelten für den ganzen überarbeiteten IT-Grundschutz und somit auch für den BSI-Standard 200-2.

Informationssicherheitsmanagement mit IT-Grundschutz

Kapitel 2 erklärt grundlegende Begrifflichkeiten in Zusammenhang mit dem IT-Grundschutz und stellt die Bestandteile des vom BSI entwickelten IT-Grundschutzes vor.

Initiierung und Organisation des Sicherheitsprozesses

Kapitel 3 und 4 führen den Leser in den Sicherheitsprozess ein und stellen die mit der Initiierung bzw. Organisation zusammenhängenden Schritte vor. Diese Schritte bilden die Grundlage für die Erstellung eines Sicherheitskonzepts und werden im späteren Verlauf in dieser Arbeit als Vorarbeiten bezeichnet. Bereits im Standard 200-1 stellt BSI den Sicherheitsprozess vor (Kapitel 3.1).

Abbildung 6: Initiierung, Organisation und Durchführung des Sicherheitsprozesses [25]

Die Informationssicherheit muss ein essenzieller Teil jeder Organisation sein. Die verantwortungsbewusste Managementebene muss deren Notwendigkeit erkennen und die Rich-

tung vorgeben. Somit trägt die Leitung die Gesamtverantwortung für die Informationssicherheit in der Organisation. In die Ausgestaltung der Informationssicherheit werden in der Regel alle Beschäftigten miteinbezogen. Zur strategischen Ausrichtung gehören dabei die Ermittlung interner und externer Rahmenbedingungen sowie der Faktoren, die einen ausschlaggebenden Einfluss auf die Informationssicherheit ausüben können.

Das Festlegen von Zielen, die durch die Etablierung eines funktionierenden ISMS erreicht werden sollen, und die Erarbeitung einer Leitlinie zur Informationssicherheit runden die ersten Tätigkeiten bei der Einführung des Sicherheitsprozesses ab.

Als Vorbereitung für die Sicherheitskonzeption sollte inmitten des Sicherheitsprozesses eine Ersterfassung aller Assets der Organisation erstellt und deren Sicherheitsniveau grob abgeschätzt werden. Hierzu zählen u. a. Prozesse oder IT-Systeme.

Die expliziten Vorarbeiten sind dadurch abgeschlossen. Es verbleibt die Entscheidung, welche Richtung die Institution bei der Absicherung der Assets einschlägt. Die alte Methodik stellte nur eine Vorgehensweise zur Verfügung. Mit dem neuen IT-Grundschutz stehen Anwender vor der Wahl zwischen drei Vorgehensweisen. Die Vorgehensweisen bilden den Kernpunkt der Modernisierung und werden im Kapitel 3.2 ausführlich erläutert.

Folgende Punkte fassen die Vorarbeiten zur Erstellung einer Sicherheitskonzeption zusammen:

- Initiierung des Informationssicherheitsprozesses
- Definition einer Sicherheitsleitlinie und Informationssicherheitsorganisation
- Erstellung einer Assets-Übersicht
- Wahl einer Vorgehensweise gemäß BSI-Standard 200-2

Die Informationssicherheit besitzt einen übergreifenden Charakter und es gibt keinen Bereich innerhalb einer Organisation, der davon nicht profitieren kann. Der Informationssicherheitsprozess kann deshalb nicht als alleinstehender Prozess ausgeführt werden, sondern muss in die Organisationswelt integriert werden. Die erste Aufgabe, die zu bewältigen ist, ist die Frage, wie der Prozess in die vorhandene Organisationsstruktur eingefädelt werden kann, bzw., ob Änderungen nötig sind, um dies zu tun. Eine Analyse der Struktur soll die

Möglichkeiten aufdecken, wie der Sicherheitsprozess in organisationsweite Abläufe eingeführt werden kann.

Die Integration des Sicherheitsprozesses in die Organisation reicht noch nicht aus. Es ist eine Gruppe zu etablieren, deren Aufgabe die Steuerung des Informationssicherheitsmanagements ist. Wie die Informationssicherheitsorganisation konzipiert werden kann, leistet der Standard große Hilfe durch anschauliche, beispielhafte Grafiken. Die Strukturbeispiele berücksichtigen die Größe der Institution und neuer, erst im modernisierten IT-Grundschutz berücksichtigter Bereiche (z. B. ICS).

Abgesehen von der Struktur muss im Vorfeld definiert werden, welche Kompetenzen die Informationssicherheitsorganisation besitzen soll und welche Aufgaben sie zu verantworten hat. Daraufhin soll durch Festlegung von Rollen und Verantwortlichkeiten die Organisationsstruktur erweitert oder angepasst werden. Aus den verschiedenen Rollen wird ein Managementteam für die Informationssicherheit gebildet. Dieses hat u. a. die Aufgabe Ziele und Strategien zu bestimmen, die Leitlinie zur Informationssicherheit zu pflegen und den ganzheitlichen Informationssicherheitsprozess zu koordinieren.

Der Sicherheitsprozess soll das Zusammenspiel und die Koordination zwischen Informationssicherheit, Datenschutz und IT-Betrieb unterstützen. Aufgrund der hohen Anzahl an Schnittstellen werden die Disziplinen Informationssicherheit und Datenschutz oft zusammen behandelt.

Verfügt die Institution kein ausreichendes Fachwissen, ist es ratsam, externe Fachpersonen in die interne Sicherheitsorganisation (vorläufig) einzubinden.

Der hier beschriebene Sicherheitsprozess entspricht im Wesentlichen dem Sicherheitsprozess aus dem BSI-Standard 100-2.

Dokumentation im Sicherheitsprozess

Kapitel 5 beschäftigt sich mit Anforderungen und Methoden der angemessenen Dokumentation entlang des Sicherheitsprozesses. Es richtet einen Appell an die Anwender des IT-Grundschutzes und mahnt zum verantwortungsbewussten Umgang mit der Vielzahl in diesem Zusammenhang entstandenen Dokumenten. Wichtige Kriterien für die Dokumentation sind die Aussagekraft und der angemessene Dokumentationsaufwand. Die Aussagekraft

soll die Präzision der Erfassung von Tätigkeiten charakterisieren. Der Standard weist darauf hin, dass die Wahl der Vorgehensweise dabei mitberücksichtigt werden soll. So darf der Dokumentationsaufwand der Basisabsicherung sich nicht demjenigen der Standardabsicherung annähern. Eine wichtige Rolle der Dokumentation nimmt das Auswahlschema für die Schutzbedarfsfeststellung ein.

Der Informationsfluss im Prozess ist durch Erstellung und Bereitstellung von Berichten, Konzepten, Richtlinien und Meldungen zu steuern. Die Zielgruppe darf dabei nicht ohne Berücksichtigung bleiben. So gelten für Berichte an die Leitungsebene andere Regeln, als für Meldung an Mitarbeiter. Der Grad an Detailtiefe muss dem Ziel und Zweck angemessen sein.

Erstellung einer Sicherheitskonzeption

Sobald die Voraussetzungen, d. h. die Etablierung des Sicherheitsprozesses, für die Erstellung einer Sicherheitskonzeption erfüllt sind, muss eine geeignete Vorgehensweise ausgewählt werden. Kapitel 6–8 aus dem BSI-Standard 200-2 erläutern einen der wichtigsten Kernpunkte der Modernisierung in der IT-Grundschutz-Methodik. Der BSI-Standard 100-2 hingegen behandelte lediglich eine einzige allgemeine Vorgehensweise, die sogenannte klassische Vorgehensweise.

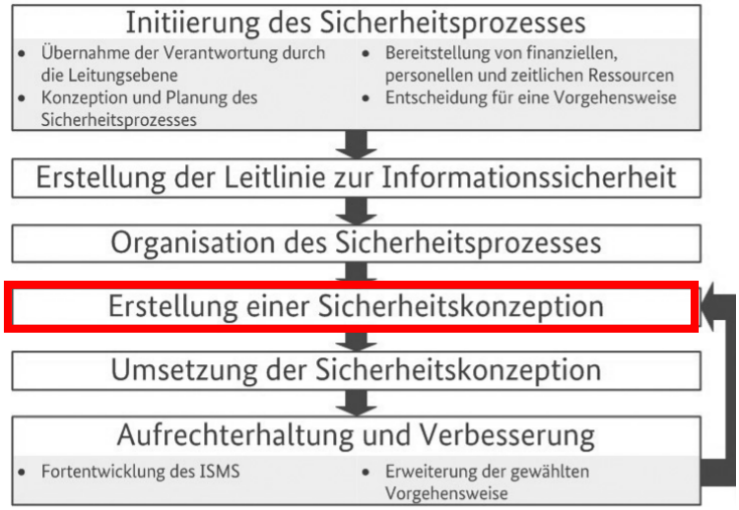

Abbildung 7: Der Informationssicherheitsprozess gemäß BSI-Standard 200-2 [23]

Jede Organisation stellt eine individuelle Form dar, in die der IT-Grundschutz eingeführt werden soll. Dessen Etablierung kann je nach Größe der Organisation zu einer großen Aufgabe heranwachsen. Das BSI hat bei der Entwicklung der neuen Edition die Herausforderungen an Institutionen berücksichtigt und sich für die Etablierung zweier weiterer Vorgehensweisen entschieden. Zu diesen Herausforderungen gehören u. a. der Organisationstyp in Institutionen, die Größe der IT-Abteilung und die Erfahrungen mit Informationssicherheit. Dazu kommt, dass für Sicherheitszwecke oft nur ein begrenztes Budget zur Verfügung steht und dies nicht immer die Ausgaben durch die Einführung der klassischen Vorgehensweise abdeckt. Die Wahl der Vorgehensweise bietet Schritte sowohl für Einsteiger als auch für Fortgeschrittene.

Aus Gründen der Übersichtlichkeit und zur Betonung der Relevanz der Vorgehensweisen widmet sich den drei Vorgehensweisen ein eigenes Unterkapitel.

Umsetzung der Sicherheitskonzeption

In Kapitel 9 des BSI-Standards 200-2 werden verschiedene Aspekte erläutert, die bei der Realisierung von ausgewählten Maßnahmen beachtet werden müssen. Im Wesentlichen basieren folgende Empfehlungen auf Aspekten des Vorgängerstandards und sollen in der Umsetzungsphase unterstützen.

Um einen Überblick über die gesamten Maßnahmen zu erhalten, ist die Zusammenstellung der Ergebnisse des IT-Grundschutz-Checks hilfreich. Durch eine geeignete Dokumentation wird die Nachvollziehbarkeit unterstützt und diese kann auch beim Zertifizierungsprozess vorgelegt werden. Die Priorisierung der umzusetzenden Maßnahmen wurde bereits in Kapitel 3.1 angesprochen. Im Standard werden weitere Anhaltspunkte für die Festlegung der Umsetzungsreihenfolge beschrieben. Dies ist vor allem in Organisationen notwendig, die über knappe Ressourcen verfügen und nicht alle identifizierten Maßnahmen zeitnah umsetzen können. Ebenso sind die Unterteilung der Aufgaben in Teilaufgaben und deren Kontrolle durch einen Maßnahmenverantwortlichen für die Realisierung wichtig. Realisierungsbegleitende Maßnahmen sind Aktionen, die nötig sind oder den Umsetzungsprozess effizienter gestalten. So müssen beispielsweise Sensibilisierungsaktionen umgesetzt werden, um die Wichtigkeit der Informationssicherheit zu betonen und Schulungen für die von den geplanten Sicherheitsmaßnahmen betroffenen Mitarbeiter zu planen.

Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit

In Kapitel 10 wird betont, dass der Informationssicherheitsprozess kontinuierlich erfolgen muss. Neben Anpassungen von Sicherheitsmaßnahmen ist die Überprüfung der Eignung der Strategie für die Informationssicherheit eine Pflicht des Anwenders. Eine regelmäßige Erfolgskontrolle und Bewertung des Prozesses bezüglich Effektivität und Effizienz soll auf verschiedenen Ebenen stattfinden und die Verbesserung des etablierten ISMS bzw. die Aufrechterhaltung des hochwertigen Schutzes von Informationen nach aktuellem Stand der Technik als Ziel haben.

Da durch das BSI viel Wert auf die Umsetzungen gelegt wird, gehören konkrete Empfehlungen zum neuen Standard. Neben automatisiertem Monitoring und Reporting wird die Nutzung eines Reifegradmodells zur Bewertung des ISMS geboten. Somit kann der Fortschritt des ISMS über einen längeren Zeitraum nachvollziehbar dokumentiert werden. Um die geeignete Anzahl und den Ausprägungsgrad der Dimensionen zu finden, können die bei der Durchführung des Sicherheitsprozesses entstandenen Dokumente hilfreich sein.

Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz

In Kapitel 11 werden wesentliche Punkte zum Thema Zertifizierung beschrieben. Die Zertifizierungsmöglichkeiten nach der Erstellung einer Sicherheitskonzeption auf Basis der vom BSI-Standard 200-2 definierten Vorgehensweisen werden in Kapitel 3.7 erläutert.

Anhang

Um eine vollständige Übersicht über den Standard zu erhalten, wird Kapitel 12 erwähnt. Darin werden Anhänge des Standards thematisiert, wie z. B. verschiedene Erläuterungen oder mögliche Fragestellungen zu Schadensszenarien.

Fazit

Das Fundament der Methodik zur Etablierung eines angemessenen ISMS in Institutionen wurde aus dem Vorgängerstandard übernommen. Einer der Kernpunkte der Modernisierung besteht in der Aufspaltung der klassischen Vorgehensweise zur Absicherung von Assets in drei verschiedene Vorgehensweisen. Dadurch wird Organisationen, die den IT-Grundschutz anwenden, mehr Spielraum beim gewählten Schutz der Informationen gegeben. Die Standardabsicherung entspricht der klassischen Vorgehensweise aus dem BSI-Standard 100-2 und bietet umfassenden und angemessenen Schutz der Assets in Organisationen. Um dem technologischen Fortschritt zu entsprechen, werden im neuen Standard auch die Themen Virtualisierung, Cloud-, ICS- und IoT-Absicherung behandelt. Dementsprechend sollen für diese Bereiche neue Rollen eingeführt werden. Die leserfreundliche Layoutgestaltung (beschrieben in Kapitel 3.1) und sprachliche Präzisierungen runden die Änderungen an der IT-Grundschutz-Methodik ab. [23] [24]

3.2.1 Die Basisabsicherung

Dieses Kapitel führt den Leser in die Vorgehensweise Basisabsicherung ein und geht dabei speziell auf die Schritte ein, die nach Wahl dieser Vorgehensweise umzusetzen sind.

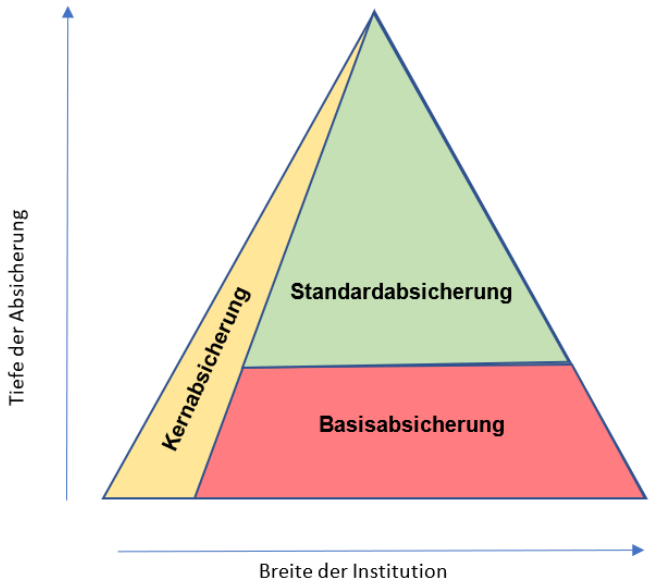

Abbildung 8: Basisabsicherung nach BSI-Standard 200-2, eigene Darstellung in Anlehnung an [26]

Grundlagen

Der Absicherungsprozess kann im modernisierten IT-Grundschutz auch phasenweise eingeführt werden. Die Basisabsicherung stellt eine neue Vorgehensweise bei der Sicherheit von Assets in Organisationen dar. Diese wurde als Einstieg in das Thema Einführung eines ISMS konzipiert. Die Basisabsicherung verfolgt das Ziel, in Form einer schnellen Erstabsicherung der relevanten Geschäftsprozesse, IT-Systeme und weitere wichtige Komponenten einer Institution einen soliden Einstieg in den IT-Grundschutz zu gewährleisten. Die Durchführung der Arbeitsschritte nach der Basisabsicherung strebt ein normales Sicherheitsniveau an. Der ausgewählte Informationsverbund darf Komponenten enthalten, dessen Absicherung durch gewöhnliche Sicherheitsmaßnahmen zufriedenstellend ist. Ist der abzusichernde Informationsverbund geschäftskritisch und stellt dessen Verlust eine Bedrohung der Existenz der Institution dar, empfiehlt sich diese Vorgehensweise nicht. Außerdem eignet sich die Basisabsicherung besonders gut für Unternehmen und Behörden, die den IT-

Grundschutz (frühere oder aktuelle Standards) noch nicht angewendet haben oder erst am Anfang einer Einführung der Informationssicherheit stehen.

Was Organisationen als Informationsverbund auswählen, ist sehr unterschiedlich. Dies kann aus einer Kombination von Geschäftsprozessen, IT-Systemen, Anwendungen usw. bestehen. Grundsätzlich gilt, dass alle möglichen Elemente dadurch abgesichert werden können, jedoch empfiehlt sich bei unternehmenskritischen Assets eine andere Vorgehensweise.

Die realisierten Anforderungen aus dem IT-Grundschutz-Kompendium, die auf der Basisabsicherung beruhen, können zeitnah durchgeführt werden. Die Umsetzung der im Kompendium aufgeführten Basisanforderungen reichen aus, um das Sicherheitsniveau entsprechend der Basisabsicherung zu garantieren.

Die Basisabsicherung dient als Basis für eine weiterführende Vorgehensweise (Kern- oder Standardabsicherung), um das Sicherheitsniveau in einer anderen Phase weiter zu verbessern. Mit der Einführung der Basisabsicherung schaffen Institutionen einen wichtigen Schritt in die Richtung, ihren Assets adäquat zu schützen. Doch das Niveau der Informationssicherheit muss weiterhin gesteigert werden, um alle vielschichtigen Gefahren abzudecken und angemessene Reaktionen darauf bereitzuhalten.

Eine ISO 27001 Zertifizierung für die Basisabsicherung ist nicht möglich, da es sich bei dieser Version um ein Mindestmaß von erfüllten Aspekten der Informationssicherheit handelt. Ein ausgestelltes Testat bestätigt die erbrachten Leistungen, gilt jedoch nicht als Zertifikat. Das Zertifikat ist ausschließlich erst nach der Durchführung der Kern- oder Standardabsicherung für den behandelten Informationsverbund möglich. [27]

Zusätzlich zur Methodik, in der die Vorgehensweise zur Basisabsicherung erläutert wird, hat das BSI einen Leitfaden bereitgestellt. Der Leitfaden liefert einen konsolidierten Überblick zum Aufbau eines ISMS nach der gewählten Vorgehensweise. In drei Schritten zeigt das Dokument die Umsetzungsphasen, die sich sehr stark an den Schritten des Sicherheitsprozesses gemäß BSI-Standard 200-2 IT-Grundschutz-Methodik orientieren.

Insgesamt stellt die Basisabsicherung eine rapide und eine die gesamte Organisation umfassende Vorgehensweise dar. Die Umsetzung ist im Vergleich mit den anderen beiden Vorgehensweisen ressourcenarm und benötigt viel weniger Aufwand. In der Praxis hat es

früher häufig zu Problemen geführt, dass kleine Behörden nicht über ein ausreichendes Budget oder Fachpersonal verfügt haben und deshalb die umfassende klassische Vorgehensweise nicht durchgeführt werden konnte. Um dieses Problem zu lösen, bietet die Basisabsicherung in Form einer Erstabsicherung mit einem normalen Sicherheitsniveau. Die umgesetzten Sicherheitsmaßnahmen nach der Basisanforderungen reichen für eine Erstabsicherung aus, entsprechen aber nicht dem vom BSI empfohlenen Sicherheitsniveau. [23]

Erstellung einer Sicherheitskonzeption nach der Vorgehensweise Basisabsicherung

Der nächste Teil des Kapitels konzentriert auf die Darstellung der Vorgehensweise nach der Basisabsicherung gemäß BSI-Standard 200-2: IT-Grundschutz-Methodik. [23]

Damit die Erstellung der Sicherheitskonzeption begonnen werden kann, müssen wichtige Voraussetzungen erfüllt werden. Diese Vorarbeiten sind Bestandteile des Sicherheitsprozesses und werden im Kapitel 3.1 erläutert. Zur Wiederholung die wesentlichen Schritte:

- Initiierung des Informationssicherheitsprozesses
- Definition einer Sicherheitsleitlinie und Informationssicherheitsorganisation
- Erstellung einer Assets-Übersicht
- Wahl der Basisabsicherung als Vorgehensweise

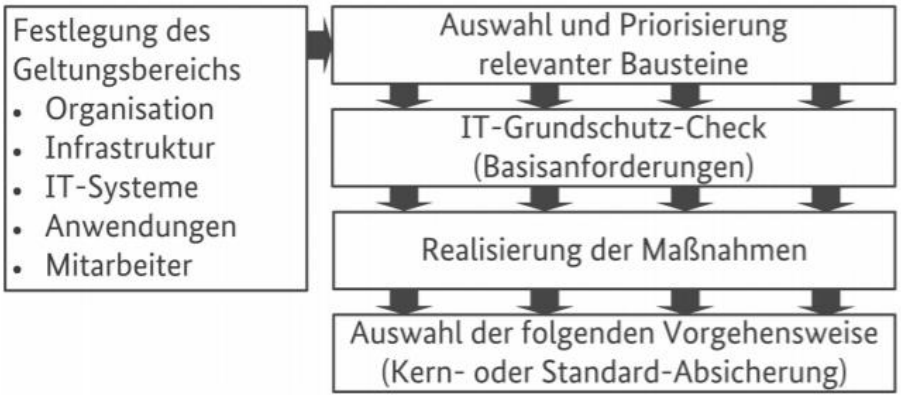

Abbildung 9: Vorgehensweise bei der Basisabsicherung [23]

Zuerst muss der Geltungsbereich definiert werden. Dieser gibt an, welche Bereiche in der Institution geschützt werden sollen. Es gibt keine Vorschriften, wie groß der Geltungsbereich sein oder ob er die ganze Institution abdecken soll. Zum Geltungsbereich zählen alle wesentlichen Komponenten einer Institution, beispielsweise die bestehende Organisationsform, technische Ausstattung und Mitarbeiter. Das BSI empfiehlt die Eingrenzung des Bereichs so eindeutig, dass es keine Rückfragen nötig sind. Der Geltungsbereich muss sinnvoll gewählt sein und die Schnittstellen zu den anderen Komponenten berücksichtigen. Der Geltungsbereich wird in der Phase „Erstellung der Sicherheitskonzeption" als Informationsverbund genannt. Für die weiteren Phasen ist das Ergebnis dieser Phase relevant.

Nachdem der Informationsverbund festgelegt wurde, erfolgt eine Auswahl und Priorisierung relevanter Bausteine. Realisiert wird die Auswahl durch die Modellierung mithilfe des IT-Grundschutz-Kompendiums. Passend zu den Zielobjekten aus dem Informationsverbund müssen die relevanten Bausteine aus dem IT-Grundschutz-Kompendium identifiziert werden. Die Modellierung besteht darin, für die Bausteine jeder Schicht zu entscheiden, ob und wie sie abgebildet werden können. Nachdem alle Bausteine aufgedeckt sind, entsteht eine Liste mit mehreren Elementen. Diese Bausteinliste gibt an, welche Sicherheitsanforderungen umgesetzt werden müssen. Aufgrund der hohen Anzahl der Bausteine muss entschieden werden, welche zuerst behandelt werden. Dieser Schritt wird durch die Priorisierung der Bausteine mit den entsprechenden Anforderungen erreicht. Daher muss die Liste der Bausteine mit einem weiteren Merkmal (Umsetzungsreihenfolge) erweitert werden. Bei der Priorisierung müssen institutionsinterne Kriterien definiert werden.

Liegt die priorisierte Liste mit den wichtigsten Bausteinen vor, müssen die Anforderungen an die Bausteine analysiert werden. Um mit der Basisabsicherung kompatibel zu sein, müssen die Basisanforderungen zu jedem ausgewählten Baustein aus dem Kompendium erfüllt werden. Der Plan steht also fest, jedoch hat das BSI viel Freiheit gelassen, wie dieser umgesetzt werden soll. In der IT-Grundschutz-Methodik gemäß BSI-Standard 100-2 sind sehr konkrete Sicherheitsmaßnahmen definiert. Der modernisierte IT-Grundschutz enthält stattdessen Anforderungen, in denen der Gestaltung der Umsetzung viel Freiheit gelassen ist. Welche und wie viele Maßnahmen umgesetzt werden, ist der Institution überlassen, solange die Anforderungen am Schluss erfüllt sind. Daher müssen für jede relevante Anforderung geeignete Maßnahmen ergriffen und umgesetzt werden. Um die Anwender des IT-Grund-

schutzes zu unterstützen, können Umsetzungshinweise von BSI berücksichtigt werden. Jedoch existieren Umsetzungshinweise nur für ausgewählte Bausteine. Für die Basisabsicherung sollen die Basisanforderungen aus dem Kompendium erfüllt werden.

Nach den umgesetzten Sicherheitsmaßnahmen für jeden Baustein ist die Effektivität und Effizienz zu überprüfen. Die IT-Grundschutz-Methodik nennt dieses Instrument den IT-Grundschutz-Check für die Basisabsicherung. Die Überprüfung hat die Aufgabe, die Frage zu beantworten, ob die herangezogenen Zielobjekte hinreichend geschützt sind.

Der IT-Grundschutz-Check stellt einen Soll-Ist-Vergleich dar, der die identifizierten Anforderungen zu den einzelnen Bausteinen den umgesetzten Sicherheitsmaßnahmen gegenüberstellt. Ergibt die Kontrolle fehlerhafte Umsetzungen oder keine umgesetzten Maßnahmen, so sind diese unverzüglich nachzubessern. Der nächste Schritt kann erst dann gemacht werden, wenn alle umgesetzten Maßnahmen die jeweilige Basisanforderung erfüllen und somit das gewünschte Sicherheitsniveau sichergestellt ist. Bei der Durchführung empfiehlt es sich, einen Umsetzungsstatus, ein Hinweisfeld und ein Feld für die Verantwortlichen in die Liste einzufügen. Die Ausführung unterscheidet sich von Institution zu Institution. Das BSI schlägt zur Beurteilung des Umsetzungsstatus vier Zustände vor: „entbehrlich", „umgesetzt", „teilweise umgesetzt", „noch nicht umgesetzt".

Die Realisierungsphase beschreibt die Umsetzung der identifizierten Sicherheitsmaßnahmen zu den festgestellten Anforderungen. Eine systemische Herangehensweise wird empfohlen. Zur Realisierungsphase gibt das BSI folgende Hinweise:

- Sichtung der Untersuchungsergebnisse
- Konsolidierung der Basisanforderungen
- Kosten- und Aufwandsschätzung
- Festlegung der Umsetzungsreihenfolge der Basisanforderungen
- Festlegung der Aufgaben und der Verantwortung
- Realisierungsbegleitende Basisanforderungen

Der letzte Schritt in der Vorgehensweise nach der Basisabsicherung ist die Auswahl der darauf aufbauenden Vorgehensweisen. Wie bereits in diesem Kapitel erwähnt, stellt die Basisabsicherung eine Erstabsicherung für den Einstieg dar. Die umgesetzten Sicherheits-

maßnahmen sorgen für ein niedriges Sicherheitsniveau, das nicht als Dauerlösung angesehen werden darf. Als Ziel kann die Standardabsicherung, die die klassische Vorgehensweise aus dem früheren BSI-Standard entspricht, herangezogen werden.

Fazit

Die Basisabsicherung stellt eine der drei Vorgehensweisen aus dem BSI-Standard 200-2 dar. Diese Absicherungsart ist für Einsteiger empfohlen, da hier von der Umsetzung grundlegender Sicherheitsmaßnahmen auszugehen ist. Die Basisabsicherung bietet eine schnelle, einfache Absicherung der relevanten Assets. Dabei werden besonders Unternehmen und Behörden berücksichtigt, die über bescheidene Ressourcen verfügen. Nach der Neukonzeption vom IT-Grundschutz, ist diese Absicherungsart ausschließlich als Übergangslösung bis zur Einführung der Standard- oder Kernabsicherung anzusehen. [23] [26]

3.2.2 Die Kernabsicherung

Dieses Kapitel erläutert die Kernabsicherung und deren Rolle, wenn diese Absicherungsart für die Erstellung einer Sicherheitskonzeption gewählt wurde.

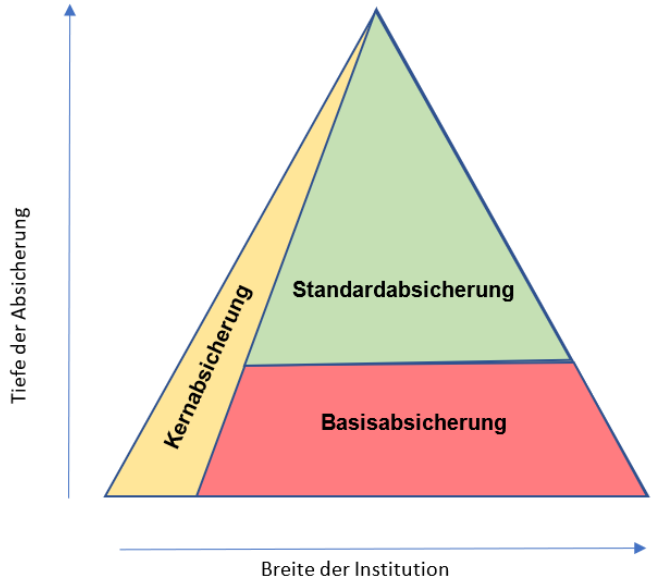

Abbildung 10: Kernabsicherung nach BSI-Standard 200-2, eigene Darstellung in Anlehnung an [26]

Grundlagen

Die Kernabsicherung stellt eine der drei Vorgehensweisen der IT-Grundschutz-Methodik dar. Kritische Assets (sogenannte Kronjuwelen der Institution) sind besonders gefährdet und deren Absicherung genießt Priorität.

Die Kernabsicherung ist als Einstieg in den IT-Grundschutz konzipiert. Die Absicherung umfasst nur einen kleinen, aber sehr essenziellen Teil der Institution. Da es sich um essenzielle Assets handelt, deren Verlust kritische Auswirkungen für den Geschäftsbetrieb verursachen kann, ist eine sofortige Absicherung notwendig. Die Kernabsicherung bietet eine akute Absicherung der wichtigsten Informationen und Geschäftsprozesse. Im Gegensatz zur Basisabsicherung ist die Kernabsicherung keine organisationsumfassende Absicherung mit einem normalen Schutzniveau, sondern genau das Gegenteil. Die Konzentration liegt an sehr wenigen Objekten, die aber mit strikten Sicherheitsmaßnahmen geschützt sind.

Die für Einsteiger gedachte Kernabsicherung bietet keinen umfassenden Schutz. Der Geltungsbereich erstreckt sich nur über die unternehmenskritischen Bereiche. Um den Schutz auf alle Assets der Organisation auszuweiten, müssen die Anforderungen nach der Standardabsicherung durchgesetzt werden.

Eine ISO 27001-Zertifizierung für die Kernabsicherung ist möglich, ist aber nur auf diesen Bereich begrenzt. Ist eine Zertifizierung für eine umfassende Absicherung gewünscht, muss die Standardabsicherung durchgeführt werden, welche eine umfassende und angemessene Absicherung nach dem Stand der Technik entspricht.

Erstellung einer Sicherheitskonzeption nach der Vorgehensweise Kernabsicherung

Dieser Abschnitt konzentriert sich auf die Darstellung der Vorgehensweise der Kernabsicherung gemäß BSI-Standard 200-2: IT-Grundschutz-Methodik. [23]

Um mit der Erstellung der Sicherheitskonzeption begonnen zu können, müssen wichtige Voraussetzungen erfüllt werden. Diese Vorarbeiten sind Bestandteile des Sicherheitsprozesses und werden im Kapitel 3.1 erläutern. Zur Wiederholung sind hier die wesentlichen Schritte zusammengefasst:

- Initiierung des Informationssicherheitsprozesses
- Definition einer Sicherheitsleitlinie und Informationssicherheitsorganisation
- Erstellung einer Assets-Übersicht
- Wahl der Kernabsicherung als Vorgehensweise

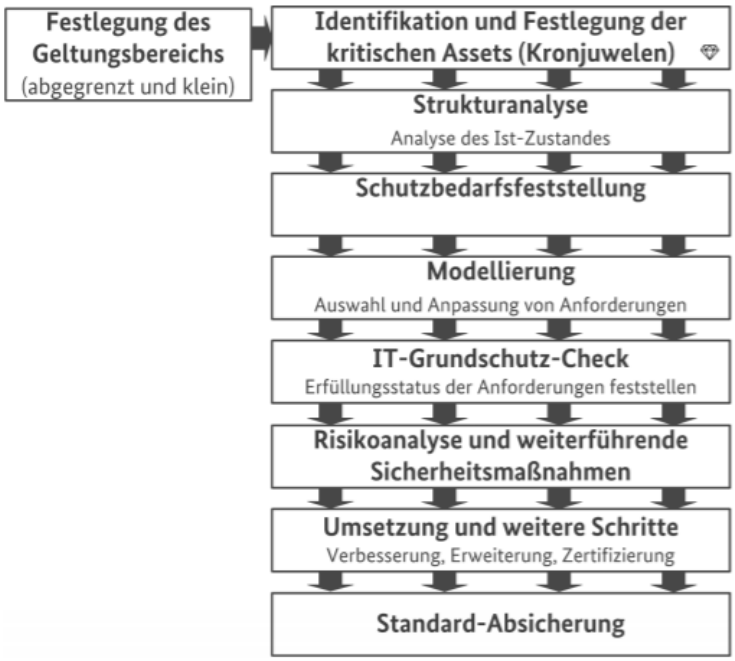

Abbildung 11: Vorgehensweise nach der Kernabsicherung [23]

Die Vorgehensweise nennt die Festlegung des Geltungsbereiches als ersten Schritt. Die Methodik ist nahezu identisch mit der Phase der Basisabsicherung. Der eindeutig abgegrenzte Geltungsbereich gibt an, welche Bereiche durch die Kernabsicherung in der Institution abgedeckt werden sollen. Institutionen sollten den Bereich so klein wie möglich halten, da es sich um die wichtigsten Assets in der Organisation handelt. Der Geltungsbereich wird in der Phase „Erstellung der Sicherheitskonzeption" als Informationsverbund genannt. Für die weiteren Phasen ist das Ergebnis dieser Phase ausschlaggebend.

Die nächste Phase soll die kritischen Assets eingrenzen. Die Identifikation kritischer Assets zählt zu den Aufgaben der Institution. Die endgültige Entscheidung über die Einstufung und die damit verbundene Verantwortung gehört der Leitungsebene. Es ist möglich, externe Quellen mit einzubeziehen, und wird sogar empfohlen, wenn kein geeignetes Fachpersonal in der Organisation vorhanden ist. Kennt eine Institution ihre kritischen Assets, können sie für die Kernabsicherung herangezogen werden. Kennt eine Institution ihre kritischen Assets nicht, müssen diese zuerst aufgespürt werden. Wie die Identifikation durchgeführt wird, steht der Institution zur freien Wahl, da kein einheitliches Schema existiert. Das BSI bietet Unterstützung in Form von Charakterisieren kritischer Assets. Zunächst wird betrachtet,

welche kritischen Objekte in Fragen kommen. Der BSI-Standard 200-2 zählt folgende Objekte auf:

- Informationen, die wesentlich für die erfolgreiche Durchführung essenzieller Geschäftsprozesse sind
- Informationen und Geschäftsprozesse, die ein deutlich erhöhtes Gefährdungspotenzial bezüglich der Informationssicherheit besitzen
- Informationen und Geschäftsprozesse, deren Verlust geschäftskritisch ist

Kritische Assets können wie folgt charakterisiert werden:

- Informationen oder Geschäftsprozesse (auch immateriell), keine Dienstleistungen, Anwendungen, IT-Systeme
- überschaubare Menge der wichtigsten Objekte mit deutlich erhöhtem Schutzbedarf
- Schutzbedarf mindestens hoch

Der Standard weist darauf hin, dass es in der Praxis häufig vorkommt, dass kritische Assets durch die Kumulation wichtiger Objekte mit hohem oder sehr hohem Schutzbedarf zustande kommen.

Strukturanalyse

Die dritte Phase sieht die Durchführung einer Strukturanalyse vor. Sie dient der strukturierten Erfassung der zum Informationsverbund gehörenden Zielobjekte und der Aufbereitung für die nächsten Phasen. Zum Informationsverbund können Geschäftsprozesse, Anwendungen und technische Komponente gehören. [29]

Die Strukturanalyse stellt eine umfangreiche Aufgabe für Institutionen dar und sollte deshalb in Teilaufgaben zerlegt werden. Das BSI macht diesbezüglich folgenden Vorschlag:

1. Erfassung der zum Informationsverbund zugehörigen Zielobjekte
2. Erhebung eines Netzplans
3. Erhebung von IT-Systemen
4. Erfassung der räumlichen Gegebenheiten

Es werden häufig Listen über Objekte und Daten innerhalb einer Organisation geführt. Zunächst sollte die Institution die Existenz einer solchen Liste überprüfen.

Unternehmen und Behörden können eine enorme Menge von Objekten beherbergen. Neben materiellen Gütern müssen auch immaterielle Güter erfasst werden, was für die Organisationen eine herausfordernde Aufgabe sein kann. Oft kann es aufgrund der Datenmenge zu Verwirrungen kommen. Um dies zu vermeiden, sollten Objekte klassifiziert und kategorisiert werden. Eine Komplexitätsreduktion kann erreicht werden, indem Objekte nach Typ, Aufgaben, Rahmenbedingungen oder Schutzbedarf sortiert werden und jene Objekte, die die gleichen Merkmale aufweisen, gruppiert werden. Durch die Gruppenbildung kann davon ausgegangen werden, dass Stichprobentests aus einer Gruppe die gleichen Merkmale (z. B. die Schutzbedarfskategorie) erbringen. [30]

Der BSI-Standard 200-2 erweitert die Strukturanalyse auf neue Konzepte, die der Vorgänger aus unterschiedlichen Gründen nicht behandelt hat. Nennenswerte Beispiele dafür sind Virtualisierung, Cloud Computing, ICS- und IoT-Systeme.

Das BSI unterstützt Anwender des IT-Grundschutzes durch kurze und prägnante Formulierung von Aktionspunkten zu jedem Schritt einer Phase. Darüber hinaus gibt der Standard beispielhafte und detaillierte Ergebnisse einer Erfassung vor. Die Visualisierungen besitzen einen Empfehlungscharakter und dienen als Orientierungshilfe für die Dokumentation der Ergebnisse.

Die Netzplanerhebung stellt eine weitere wichtige Teilaufgabe der Strukturanalyse dar. Um die Analyse der technischen Objekte zu vereinfachen, soll ein Netzplan entworfen werden. Die grafische Übersicht soll die verschiedenen IT-Systeme und ihre Komponenten visualisieren. Dadurch können Schnittstellen und Verbindungen zu anderen Systemen schnell erkannt werden. Durch die automatische Generierung von Netzplänen mithilfe von Softwaretools lässt sich diese Aufgabe ohne großen Aufwand lösen. Folgende Grafik aus der IT-Grundschutz-Schulung zeigt ein Beispiel für einen Netzplan.

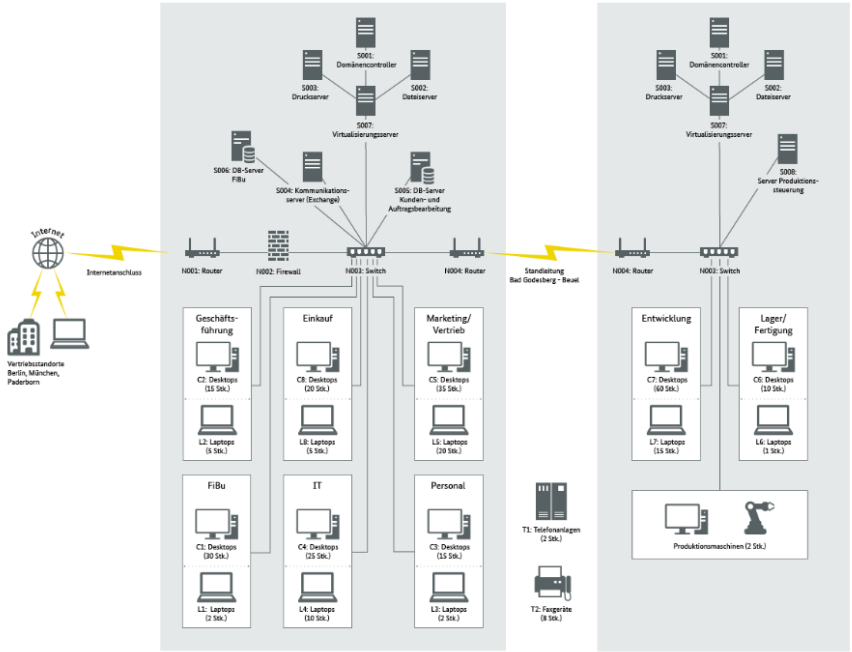

Abbildung 12: Beispiel für einen Netzplan [23]

Informationen zu den einzelnen Objekten sollten im Netzplan abgespeichert werden. Standardinformationen sind beispielsweise eine eindeutige Bezeichnung, Typ, Funktion, Standort, verantwortliche Person und Schnittstellen. Der Netzplan muss stets auf dem aktuellen Stand gehalten werden und Informationen über den Zustand der Objekte liefern. Dies umfasst das Hinzufügen, das Entfernen von Komponenten und das Ändern von Objekteigenschaften. [31]

Als Vorbereitung für die Analyse des Schutzbedarfes der einzelnen Zielobjekte müssen diese vollständig in geordneter Form vorliegen.

IT-Systeme umfassen im Allgemeinen sowohl die im aktualisierten Grundschutz hinzugefügten ICS-Systeme, IoT-Systeme sowie sonstige technische Komponenten als auch die virtuellen Einzeleinheiten von IT-Systemen. Bauteile von IT-Systemen sind als Gesamtheit zu verstehen und müssen deshalb nicht einzeln aufgeführt werden. Objektgruppen, die zusammengefasst wurden, dürfen weiterhin als eine Einheit betrachtet werden. Für die Erfassung der IT-Systeme sollten wichtige Informationen (Bezeichnung, Beschreibung, Status, Standort) erhoben werden. [32]

Die letzte Teilaufgabe beschäftigt sich mit der Erhebung von räumlichen Gegebenheiten. Geschäftsprozesse oder Fachaufgaben aus dem identifizierten Informationsverbund werden nicht nur auf IT-Systemen betrieben, sondern existieren auch in der vorgegebenen räumlichen Infrastruktur der Organisation. Hierzu zählen sowohl Gebäuden als auch Räume. Alle Standorte einer Institution, Aufteilungen von Gebäuden oder Teilung der Ressourcen mit anderen Parteien sind ebenfalls zu berücksichtigen. Durch die Entwicklung der Technologie sind Themen wie Telearbeit und Cloud Computing in den Standard aufgenommen worden. Die Ermittlung des Schutzbedarfes für räumliche Gegebenheiten ist auch Bestandteil der Informationssicherheit. Häufig wird die Schutzbedarfskategorie der gelagerten Objekte an den Raum übertragen. [33]

Schutzbedarfsfeststellung

Ziel der Analyse des Schutzbedarfes von ausgewählten Zielobjekten ist die Einteilung in Schutzbedarfsklassen. Die Klassen bieten eine standardisierte Form des erforderlichen Schutzniveaus für Institutionen und geben an, wie stark die zugeordnete Einheit zu schützen ist. Die Kategorisierung erfolgt anhand der Einteilung der drei Grundwerte aus der Informationssicherheit. Institutionen haben die Aufgabe Auswirkungen einer Verletzung der Vertraulichkeit, Integrität und Verfügbarkeit möglichst korrekt einzuschätzen. Je höher der mögliche Schaden ist, desto höher ist die Schutzbedarfsklasse zu wählen. Abweichungen in der Wahl der Schutzbedarfsklasse zwischen Institutionen sind gewöhnlich, da Schäden abhängig von der Organisationsgröße eingestuft werden können. [34]

In der Kernabsicherung handelt es sich um geschäftskritische Assets. Da sie für den Geschäftsbetrieb unentbehrlich sind, sind sie in einer Klasse mit überdurchschnittlich hohem Schutzbedarf zu finden.

Die Schutzbedarfsanalyse teilt sich in folgenden Teilaufgaben auf:

- Definition der Schutzbedarfskategorien
- Schutzbedarfsfeststellung für Zielobjekte
- Schlussfolgerungen aus den Ergebnissen der Schutzbedarfsfeststellung

Zu Beginn der Schutzbedarfsfeststellung sind Kategorien zur Einteilung von Objekten zu definieren. Der Schutzbedarf stellt eine nicht quantifizierbare Einheit dar, dessen Vergleich

ohne Werte eine schwierige Aufgabe ist. Bei der Auswahl der Klassen ist auf die angemessene Anzahl sowie auf die Aussagekraft zu achten. Organisationen dürfen die Granularität selbst bestimmen, jedoch bietet sich der bewährte Ansatz, Objekte in Klassen mit „normalem", „hohem" oder „sehr hohem" Schutzbedarf einzuteilen. Durch die Wahl geeigneter Kriterien können die Kategorien eindeutig bestimmt und voneinander abgegrenzt werden. [35] [36]

Die zweite Teilaufgabe teilt die Objekte einer Schutzbedarfsklasse zu. Die Zielobjekte sind bereits bei der Festlegung des Geltungsbereichs definiert worden. Mithilfe von Kriterien, beispielsweise finanzielle Auswirkungen oder Störung bei der Aufgabenerfüllung, werden geeignete Klassen für Objekte ermittelt. Die endgültige Entscheidung der Zuordnung ist von der Managementebene zu treffen.

Zielobjekte aus dem Informationsverbund können ihre Schutzbedarfskategorie auf andere Elemente vererben. So kann z. B. das Gebäude, in dem die Infrastruktur für den Serverbetrieb abgelegt ist, die Schutzbedarfsklasse der Infrastruktur erben. Bei gruppierten Objekten ist restriktiv vorzugehen. Die Gruppierung erhält die Schutzbedarfsklasse des Teilobjekts mit der schärfsten Kategorie. Der umgekehrte Effekt kann ebenfalls eintreten, bei dem Teilobjekte nicht die Schutzbedarfsklasse der Gruppierung erhalten, sondern werden einer anderen niedrigeren Kategorie zugeordnet. Der Sinn dahinter liegt darin, dass es Teilobjekte geben kann, die sehr selten benutzt werden oder für unternehmerische Zwecke eine geringe Bedeutung darstellen. [37]

In der letzten Teilaufgabe muss den Zuordnungen eine Bedeutung zugewiesen werden. Die Ergebnisse aus der zweiten Teilaufgabe sind als Anhaltspunkt für die weitere Vorgehensweise der Sicherheitskonzeption zu interpretieren. Der BSI-Standard 200-2 beschreibt die Schutzwirkungen für das bewährte Modell mit drei Schutzkategorien:

- „normal": Die umgesetzten Anforderungen aus dem IT-Grundschutz-Kompendium reichen aus und bieten einen angemessenen Schutz.
- „hoch": Die umgesetzten Anforderungen aus dem IT-Grundschutz-Kompendium liefern eine Kernabsicherung, reichen jedoch nicht immer aus. Eine Risikoanalyse ergibt weitergehende Sicherheitsmaßnahmen.

- „sehr hoch": Die umgesetzten Anforderungen aus dem IT-Grundschutz-Kompendium liefern eine Kernabsicherung, reichen alleine aber nicht aus. Zusätzliche Sicherheitsmaßnahmen sind individuell aus der Risikoanalyse zu entnehmen.

Bei der Kernabsicherung kommt es häufig vor, dass kritischen Assets mit anderen Zielobjekten unterschiedlicher Schutzbedarfsklasse in einem Informationsverbund zusammengefasst werden. Dies kann dazu führen, dass nur die kritischen Assets eine sehr hohe Einstufung haben. Aufgrund starker Vernetzung und Kopplungskomplexität wird das Maximalprinzip angewendet. Der Informationsverbund erhält die am höchsten eingestufte Schutzbedarfsklasse der Teilobjekte.

Modellierung eines Informationsverbunds

Die Struktur und der Schutzbedarf stellen die Voraussetzungen für die Modellierung aus dem IT-Grundschutz-Kompendium dar. Die Modellierung ist die Zuordnung geeigneter Sicherheitsanforderungen für den zugrunde liegenden Informationsverbund. Im Anschluss werden die Bausteine aus dem IT-Grundschutz-Kompendium auf Zielobjekte dargelegt.

Das modular aufgebaute Kompendium enthält elementare Gefährdungen, Bausteine mit drei Anforderungskategorien (Basisanforderungen, Standardanforderungen, Anforderungen mit erhöhtem Schutzbedarf). Kapitel 3.5 erläutert detailliert den Aufbau und die einzelnen Elemente des IT-Grundschutz-Kompendiums. Um die kritischen Assets der Institution durch die Kernabsicherung zu schützen, müssen alle Anforderungen des zutreffenden Bausteins erfüllt werden. Das schließt neben Basisanforderungen auch die Standardanforderungen und die Anforderungen mit erhöhtem Schutzbedarf ein.

Aus dem Vorgängerstandard wurde der Statusansatz für Informationsverbünde in den Standard 200-2 integriert. Der IT-Grundschutz umfasst Informationsverbünde unabhängig von ihrem Status. Sie können bereits realisiert sein oder sich noch in der Planungsphase befinden. Für bereits existierende Informationsverbünde wird das IT-Grundschutz-Modell wie ein Prüfplan verwendet und bezeichnet einen Soll-Ist-Vergleich, um unzureichende oder nicht erfüllte Sicherheitsanforderungen zu identifizieren. Für geplante Informationsverbünde wird das IT-Grundschutz-Modell als Entwicklungsplan herangezogen. [38]

Wesentliche Schritte für die Durchführung der Modellierung:

- Auswahl von Bausteinen
- Reihenfolge der Umsetzung
- Zuordnung von Bausteinen
- Anpassung der Anforderungen

Die IT-Grundschutz-Modellierung besteht darin, dass für die Bausteine einer jeden Schicht zu entscheiden ist, ob und wie sie als sinnvolle Abbildung für den betrachteten Informationsverbund eingesetzt werden können. Da die Auswahl sehr wahrscheinlich mehrere Sicherheitsanforderungen betrifft, kommt es zu einer Entscheidung der Umsetzungsreihenfolge. Die individuelle Priorisierung bestimmt, welche Anforderungen vorrangig und welche nachrangig erfüllt werden müssen. Das BSI empfiehlt zur vorrangigen Umsetzung der ISMS, ORP und OPS Bausteine, da sie die Grundlage der ordnungsgemäßen Sicherheitskonzeption bilden. Die Zuordnung von Bausteinen sollte in übersichtlicher Form dargestellt werden. Am besten eignet sich dafür eine Tabelle mit relevanten Informationen, wie Baustein, Zielobjekt und der Begründung für die Zuordnung. [39]

Zweckdienlich für diese Phase (vor der Umsetzung) ist es, die Anforderungen zu konkretisieren. Die Anforderungen stellen jene Ziele dar, die nach der Umsetzung erreicht werden sollen. Der Weg zum Ziel ist aber unbekannt. Deshalb müssen aus Anforderungen konkrete Maßnahmen gebildet werden, die den Weg vorgeben. Die Maßnahmen beschreiben die Handlungsvorgaben ausführlich genug, so dass diese von Anwendern ohne große Probleme umsetzbar sind.

Der Standard fasst die Tätigkeiten bei der Modellierung in kurze Aktionspunkte zusammen und unterstützt das Verständnis mit geeigneten Grafiken.

IT-Grundschutz-Check

Die sechste Phase nach der Vorgehensweise bei der Kernabsicherung beinhaltet die Überprüfung der umgesetzten Sicherheitsmaßnahmen. Die Kontrolle basiert auf drei Schritten:

- organisatorische Vorarbeiten
- Durchführung des Soll-Ist-Vergleichs
- Dokumentation der Ergebnisse

Für eine schnelle und reibungslose Durchführung des IT-Grundschutz-Checks müssen organisatorische Vorbereitungen getroffen werden. Dazu gehört die Sichtung sicherheitsrelevanter Dokumente, wie zum Beispiel die Dokumentation der umgesetzten Maßnahmen, mit dem Ziel, die Bausteinanforderungen zu erfüllen. Dazu gehört ebenfalls die Person, die die Umsetzung der jeweiligen Anforderung zu verantworten hat. [40]

Basierend auf die Dokumentation der erfüllten Sicherheitsmaßnahmen und Aussagen des Ansprechpartners kann ein Abgleich zwischen dem jetzigen und geplanten Zustand durchgeführt werden. Das Ergebnis des Vergleichs ist der Umsetzungsgrad. Dieser besagt, inwiefern die Umsetzung relevanter Sicherheitsmaßnahmen die gewünschten Anforderungen abdecken. Die Dokumentation der Ergebnisse sieht eine detaillierte Liste mit wesentlichen Informationen zum Vergleich vor. [41]

Risikoanalyse und weiterführende Sicherheitsmaßnahmen

Die Assets, die nach der Kernabsicherung geschützt werden, zeichnen sich durch hohen oder sehr hohen Schutzbedarf aus. Daher müssen bei der Kernabsicherung alle Bausteinanforderungen komplett umgesetzt werden. Ob weitere zusätzliche Sicherheitsmaßnahmen benötigt werden, wird anhand der Risikoanalyse ermittelt. [42] Folgende Punkte bieten eine schnelle Übersicht der Arbeitsschritte, die im Rahmen des BSI-Standards 200-3 durchgeführt werden müssen:

- Etablierung eines Risikomanagementprozesses
- Erstellung einer Gefährdungsübersicht
- Risikoeinstufung
- Risikobehandlung

Kapitel 3.3 beschreibt genauer, in welchen Fällen es zur Durchführung einer Risikoanalyse kommt und wie die Vorgehensweise aussieht.

Umsetzung und weitere Schritte

Da das Ziel des IT-Grundschutzes der umfassende und angemessene Schutz der Informationen einer Institution ist, müssen alle Schlüsselbereiche in einer Behörde oder einem Unternehmen abgedeckt werden. Die beschriebene Vorgehensweise bietet zwar einen effektiven Schutz gegen Bedrohungen, aber nur für einen kleinen Teil der Institution. Eine umfassende Absicherung, was Organisationen als Ziel gesetzt haben sollten, kann ausschließlich durch die Standardabsicherung garantiert werden. [43]

Fazit

Die Kernabsicherung bietet eine tiefgreifende Absicherung geschäftskritischer Assets. Zu dem Geltungsbereich gehören sehr wenige Zielobjekte. Der Umsetzungsaufwand entspricht ungefähr dem Niveau der Basisabsicherung, mit dem Unterschied, dass sich die Maßnahmen auf wenige Assets konzentrieren, die aber mit hohen Sicherheitsvorkehrungen geschützt werden müssen. Der empfohlene Anwenderkreis sind Einsteiger. Die Kernabsicherung kann aber auch als zusätzliche Absicherung von Objekten angewendet werden. Eine umfassende und angemessene Absicherung kann aber nur durch die Standardabsicherung gemäß BSI-Standard 200-2 gewährleistet werden. [23] [28]

3.2.3 Die Standardabsicherung

Dieses Kapitel beschreibt die Standardabsicherung und geht dabei speziell auf die Schritte ein, die nach Wahl dieser Vorgehensweise vorgeschrieben sind.

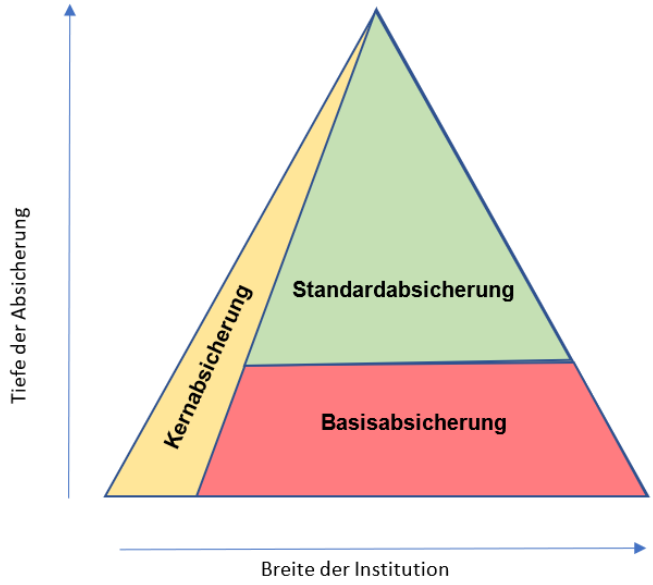

Abbildung 13: Standardabsicherung nach BSI-Standard 200-2, eigene Darstellung nach [23]

Grundlagen

Die umfassende und tiefgehende Standardabsicherung entspricht im Wesentlichen der klassischen Vorgehensweise gemäß BSI-Standard 100-2.

Der pragmatische Ansatz der Standardabsicherung soll als Endziel einen umfassenden und angemessenen Schutz der Informationssicherheit nach dem IT-Grundschutz gewährleisten und sollte deshalb von jeder Institution angestrebt werden. Sollten in der Institution ausreichende Ressourcen zur Verfügung stehen, kann direkt mit dieser Vorgehensweise begonnen werden. Eine andere Möglichkeit zur Einführung stellt die Erweiterung der Basis- und/oder Kernabsicherung dar. Dabei baut die Standardabsicherung auf die Ergebnisse der bereits eingeführten Absicherungsarten auf. Haben Behörden oder Unternehmen die klassische Vorgehensweise gemäß BSI-Standard 100-2 bereits eingeführt, empfiehlt sich eine Migration auf die Standardabsicherung nach dem BSI-Standard 200-2. Kapitel 4 dieser Arbeit behandelt die Migration auf den modernisierten Grundschutz genauer.

Obwohl die Standardabsicherung das Ziel darstellt, können weitere verschärfte Sicherheitsmaßnahmen umgesetzt werden, um Assets zu schützen.

Eine ISO 27001 Zertifizierung für die Standardabsicherung ist möglich und empfohlen. [44]

Erstellung einer Sicherheitskonzeption nach der Vorgehensweise Standardabsicherung

Dieser Abschnitt stellt die als Zielvorgehensweise angestrebte Standardabsicherung gemäß BSI-Standard 200-2: IT-Grundschutz-Methodik vor.

Um mit der Erstellung der Sicherheitskonzeption beginnen zu können, müssen wichtige Voraussetzungen erfüllt werden. Diese Vorarbeiten sind Bestandteile des Sicherheitsprozesses und werden im Kapitel 3.1 erläutert. Zur Wiederholung sind hier die wesentlichen Schritte aufgelistet:

- Initiierung des Informationssicherheitsprozesses
- Definition einer Sicherheitsleitlinie und Informationssicherheitsorganisation
- Erstellung einer Assets-Übersicht
- Wahl der Standardabsicherung als Vorgehensweise

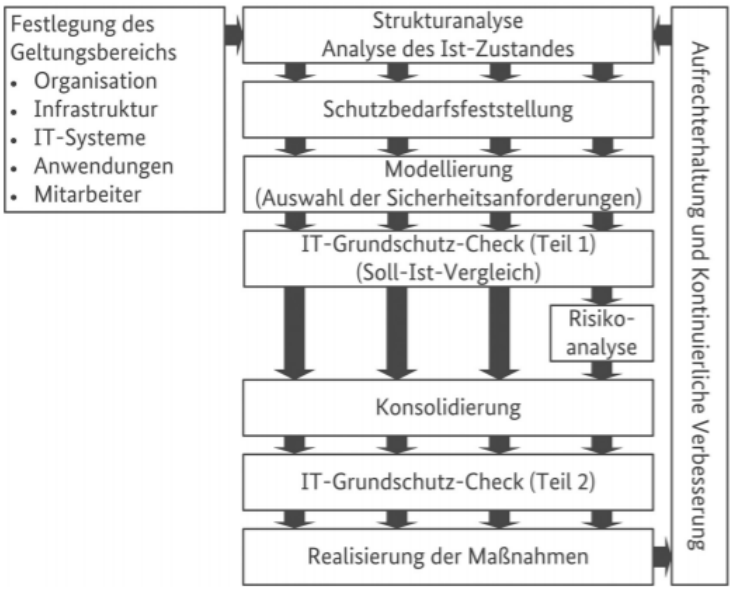

Abbildung 14: Vorgehensweise nach der Standardabsicherung [23]

Die einzelnen Phasen der Standardabsicherung integrieren Schritte aus der Basis- und Kernabsicherung. Eine ausführliche Darstellung ist bei den identischen Phasen der anderen Vorgehensweisen zu finden. Die Reihenfolge der Vorgehensweisen aus der modernisierten IT-Grundschutz-Methodik verfolgt dem Bottom-Up Ansatz, d. h., es in wird zuerst die Variante für den Einstieg und anschließend die Variante vorgestellt, die für eine umfassende und fundierte Absicherung sorgt. Aufgrund identischer Schritte bei den verschiedenen Vorgehensweisen, hat sich das BSI für die redundante Beschreibung dieser Phasen entschieden. Taucht die Phase in einer weiteren Vorgehensweise auf, verweist der Standard auf die detaillierte Beschreibung.

Festlegung des Geltungsbereichs

Die Größe und die möglichen Elemente des Geltungsbereichs entsprechen den Beschreibungen in der Basisabsicherung (siehe Kapitel 3.2.1). Im Gegensatz zur Kernabsicherung müssen die geschäftskritischen Assets nicht ermittelt werden.

Strukturanalyse

Die Strukturanalyse nach der Standardabsicherung ist identisch mit der gleichnamigen Phase nach der Kernabsicherung. Die im Kapitel 3.2.2 beschriebenen Aufgaben gelten somit auch für die Standardabsicherung.

Schutzbedarfsfeststellung

Die Schutzbedarfsfeststellung nach der Standardabsicherung ist identisch mit der gleichnamigen Phase nach der Kernabsicherung. Die im Kapitel 3.2.2 beschriebenen Aufgaben gelten auch für die Standardabsicherung. Die geschäftskritischen Assets der Kernabsicherung sollten ein hohes Schutzbedarfsniveau haben. Hingegen können bei der Standardabsicherung Zielobjekte auch ein normales Sicherheitsniveau besitzen.

Modellierung

Die Modellierung nach der Standardabsicherung ist identisch mit der gleichnamigen Phase nach der Kernabsicherung. Die im Kapitel 3.2.2 beschriebene Aufgaben gelten auch für die

Standardabsicherung. Der Informationsverbund nach der Kernabsicherung muss neben Basis- und Standardanforderungen die Anforderungen mit erhöhtem Schutzbedarf aus dem IT-Grundschutz-Kompendium erfüllen. Ein Informationsverbund, der nach der Standardabsicherung modelliert wird, muss die Basis- und die Standardanforderungen in jedem Fall erfüllen. Zusätzlich sind Objekte mit hohem oder sehr hohem Sicherheitsniveau einer Risikoanalyse zu unterziehen. Das Ergebnis der Risikoanalyse entscheiden, ob weitere Sicherheitsanforderungen erfüllt werden müssen.

IT-Grundschutz-Check 1

Der IT-Grundschutz-Check nach der Standardabsicherung ist identisch mit der gleichnamigen Phase nach der Kernabsicherung. Die im Kapitel 3.2.2 beschriebene Aufgaben gelten auch für die Standardabsicherung.

Ein wesentlicher Unterschied zwischen Kern- und Standardabsicherung stellt die Durchführung der Risikoanalyse dar. Die Kernabsicherung behandelt kritischen Assets, die ein hohes Schutzniveau besitzen. Bei der Standardabsicherung können Assets erfasst werden, die der normalen Schutzkategorie angehören. Die Kernabsicherung sieht die Pflichtdurchführung der Risikoanalyse vor, bei der Standardanalyse hängt es jedoch vom Schutzbedarf des untersuchten Objekts ab.

Konsolidierung

Sind für Zielobjekte mit hoher oder sehr hoher Schutzbedarfseinstufung mittels Risikoanalyse weiterführende Sicherheitsmaßnahmen identifiziert worden, so bedarf es einer Konsolidierung der Maßnahmen zwischen Objekten mit normalem und Objekten mit höherem Schutzbedarf.

IT-Grundschutz-Check 2

Nach der Konsolidierung erfolgt ein erneuter IT-Grundschutz-Check. Dieser beinhaltet die gleiche Methodik, beachtet aber die neu identifizierten und hinzugefügten Sicherheitsmaßnahmen für besonders schützenswerten Assets.

Realisierung

Der letzte Schritt in der Umsetzung der Maßnahmen zur Erfüllung von Bausteinanforderungen ist die Realisierungsphase. In dieser werden die bisher nur theoretischen Schutzmaßnahmen in die Praxis umgesetzt. Die Realisierung ist von der Institution durchzuführen, jedoch mangels Sicherheitskompetenz können externe Quellen herangezogen werden.

Wie bereits einleitend in der Arbeit definiert, umfasst die Sicherheitskonzeption nicht nur die Durchführung der Absicherungsvariante, sondern sie muss innerhalb einer Organisation gelebt werden. Dies beinhaltet die kontinuierliche Verbesserung des Sicherheitsprozesses und die mögliche Anpassung der Sicherheitsmaßnahmen. Die Umsetzung der einzelnen Phasen der Sicherheitskonzeption nach der gewählten Vorgehensweise garantieren im Moment der Durchführung ausreichender Schutz, um jedoch den Schutz aufrechtzuerhalten, müssen Institutionen ihre Maßnahmen stets überprüfen und bei Bedarf aktualisieren.

Fazit

Die im BSI-Standard 100-2 definierte klassische Vorgehensweise entspricht der Standardabsicherung aus dem modernisierten IT-Grundschutz. Ein angemessener Umgang mit Ressourcen sowie die umfassende Absicherung der gewählten Bereiche garantieren hohe Informationssicherheit gemäß dem Stand der Technik. Diese Standardabsicherung ist zwar die aufwendigste der vorgestellten Vorgehensweisen, sie sollte jedoch das Ziel aller Institutionen sein, die ihr Managementsystem für die Informationssicherheit nach der IT-Grundschutz-Methodik nachhaltig schützen möchten. [23] [24] [45]

3.3 BSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz

Ziel dieses Kapitels ist, einen Überblick über den BSI-Standard 200-3 zu geben und Differenzen zwischen beiden Editionen aufzuzeigen.

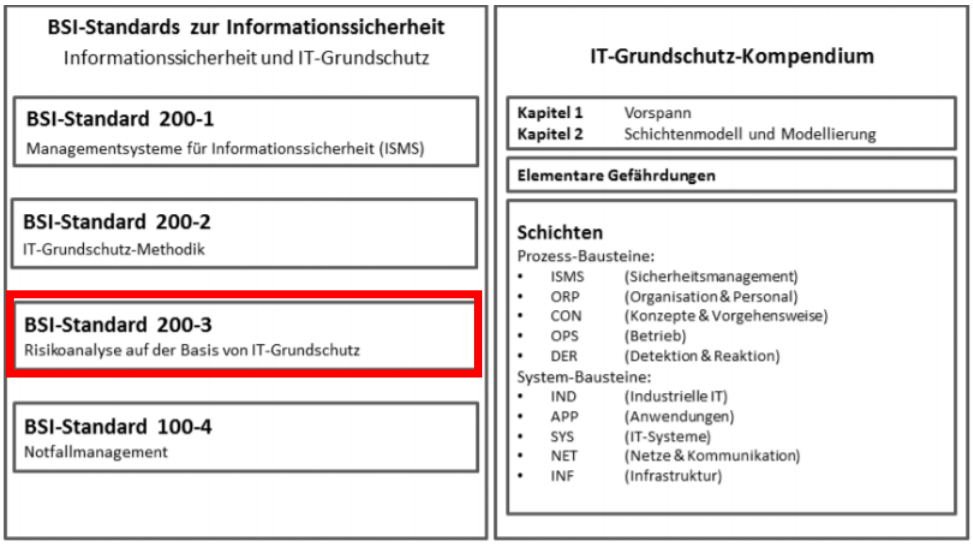

Abbildung 15: Der moderne IT-Grundschutz [21]

Im dritten Standard der modernisierten BSI-Standards-Reihe wird die Risikoanalyse behandelt, die eine vom BSI empfohlene Methodik auf Basis von IT-Grundschutz darstellt.

Das Dokument ist in 9 Kapitel gegliedert.

Einleitung

In der Einleitung werden die Leser informiert, dass der BSI-Standard 200-3 Teil des modernisierten IT-Grundschutzes ist und den Standard mit der Kennzeichnung 100-3 ablöst. Dennoch bildet der Standard 100-3 die Basis der Neukonzeption.

Ziel des Standards ist es, die grundlegende Lenkung und Steuerung der Informationssicherheitsrisiken innerhalb einer Organisation zu vereinheitlichen und diesen Prozess zu unterstützen. Die Vorgehensweise basiert auf elementaren Gefährdungen aus dem IT-Grundschutz-Kompendium. Eine implizierte Risikobewertung ist in der Vorgehensweise nach dem IT-Grundschutz für Informationsverbände mit normalem Schutzbedarf der Bausteinmodellierung inbegriffen.

Jedoch ist eine explizite Durchführung der Risikoanalyse notwendig, wenn innerhalb eines Informationsverbunds Schutzziele eines Objekts in den Kategorien hoch oder sehr hoch eingestuft werden. Mindestens einer der drei Grundwerte muss durch Bedrohung beeinträchtigt werden und dem Schutzbedarf hoch oder sehr hoch zugeordnet sein.

Die Liste der Bausteine deckt nicht alle Objekte einer Institution ab, daher ist ebenfalls eine Risikoanalyse notwendig, wenn Objekte nicht ausreichend modelliert werden können. Ebenso ist das Einsatzgebiet ein relevanter Punkt für die Durchführung der Analyse, wenn Zielobjekte nicht in der vom IT-Grundschutz vorgesehenen Umgebung betrieben werden.

Ziel der Risikoanalyse ist die Identifikation der Gefährdungen von Objekten, die durch die Umsetzung der relevanten IT-Grundschutz-Bausteine weiterhin Gefahren ausgesetzt sind und die Bestimmung, ob individuelle Sicherheitsmaßnahmen notwendig sind, um diese abzusichern.

Vorbereitung der Risikoanalyse

Bevor Unternehmen oder Behörden eine Risikoanalyse durchführen können, sind Vorarbeiten notwendig. Die Risikoanalyse ist ein essenzieller Bestandteil der Sicherheitskonzeption nach der IT-Grundschutz-Methodik. Die Schritte, die vor der Risikoanalyse durchgeführt werden müssen, sind in diesem Werk als Vorarbeiten definiert. In folgende Grafik werden die Schritte der Sicherheitskonzeption nach der Standardabsicherung gemäß IT-Grundschutz-Methodik dargestellt.

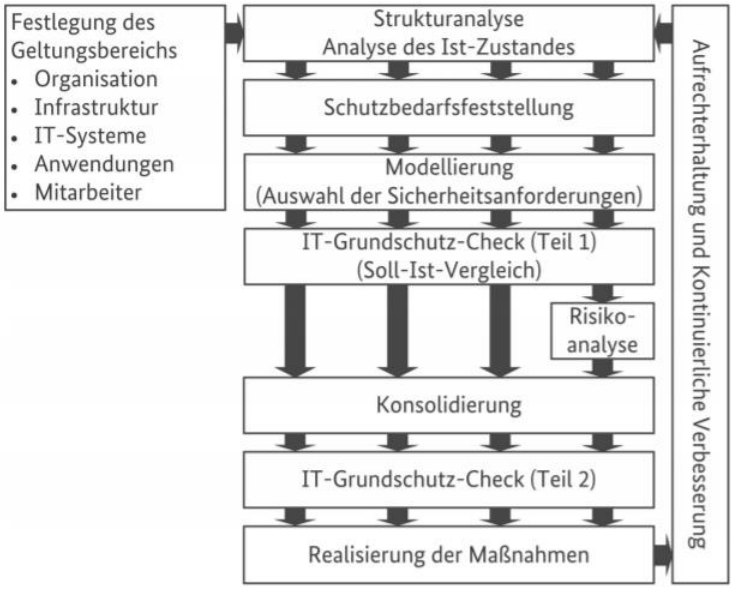

Abbildung 16: Ablauf der Sicherheitskonzeption nach der Standardabsicherung [23]

Die Vorarbeiten sind gemäß BSI-Standard 200-2 definiert und unterstützen das systematische Vorgehen. Eine ausführliche Beschreibung ist in Kapitel 3.2.3 zu finden.

- Initiierung des Sicherheitsprozesses (Vorarbeit für die Sicherheitskonzeption)
- Definition des Geltungsbereichs
- Durchführung einer Strukturanalyse
- Feststellung des Schutzbedarfes für den Geltungsbereich
- Modellierung
- IT-Grundschutz-Check

Sind diese Schritte erledigt, kommt es zu einer Fallunterscheidung, um zu bestimmen, ob eine Risikoanalyse notwendig ist. Die Voraussetzungen sind in diesem Kapitel als explizite Gründe für die Durchführung der Risikoanalyse aufgelistet.

Die Ergebnisse der Vorarbeiten liefern einen Informationsverbund, der für die eventuelle Risikoanalyse (abhängig vom Schutzbedarf) geeignet ist. Ist eine große Menge an Zielobjekten vorhanden, lässt sich eine Priorisierung nicht vermeiden. Für die Basisabsicherung ist üblicherweise keine Risikoanalyse vorgesehen. Ist die gewählte Vorgehensweise die Standardabsicherung, empfiehlt sich eine vorrangige Überprüfung übergeordneter Zielobjekte. Ist die gewählte Vorgehensweise die Kernabsicherung, gilt das *Höchste-Schutzbedarf-Prinzip*, das besagt, dass mit dem Objekt, das den höchsten Schutzbedarf aufweist,

gestartet werden muss. Stehen mehrere Kandidaten zur Auswahl, bleibt es der Organisation überlassen, welche sie präferieren.

Um die Empfehlungen praxisbezogener darstellen zu können, hat das BSI Beispiele entwickelt, die anhand eines fiktiven Unternehmens die Anwendung der Risikoanalyse darstellen. In den Fallbeispielen wird die aktuelle Situation innerhalb des Unternehmens beschrieben und die Objekte, die mit der Risikoanalyse untersucht werden müssen, werden vorgegeben. Diese Beispiele sollen Anwendern helfen und die Nutzung des Standards erleichtern. An den Erkennungsmerkmalen wird deutlich, dass das BSI bei der Modernisierung einen großen Wert auf Anwenderfreundlichkeit gelegt hat.

Übersicht über die elementaren Gefährdungen

Eine wesentliche Änderung stellt die Integration des Kapitels in den BSI-Standard 200-3 dar. Die vorläufige Risikoanalyse wurde im BSI-Standard 100-3 durch Ergänzungen sukzessive erweitert, eine Übersicht der elementaren Gefährdungen wurde aber als Ergänzung zum BSI-Standard 100-3 veröffentlicht. [48]

Das BSI hat es sich zur Aufgabe gemacht, Einzelgefährdungen, die IT-Grundschutz-Bausteine bedrohen, zu sammeln und in einer übersichtlichen Form darzustellen. Bei den 47 elementaren Gefährdungen handelt es sich um erdenkliche Risiken, die sich aus elementaren Gefahren, wie z. B. höhere Gewalt, technisches Versagen oder menschliche Fehlhandlung ergeben. Das BSI hat bei der Erstellung der Tabelle deren leichte Verwendung sowie die Kompatibilität zu anderen informationssicherheitsbezogenen Standards berücksichtigt.

Die Liste der elementaren Gefährdungen wurde vervollständigt und die jeweils betroffenen Grundwerte wurden aktualisiert. In der neuen Ausgabe enthält die Liste – nach dem Hinzufügen des Elements „Schädliche Seiteneffekte IT-gestützter Angriffe“ – 47 Elemente. Die Grundwerte beziehen sich auf die Schutzziele Vertraulichkeit (C: Confidentiality, Integrität (I: Integrity), Verfügbarkeit (A: Availability).

	Gefährdung	Grundwert
G 0.1	Feuer	A
G 0.2	Ungünstige klimatische Bedingungen	I, A
G 0.3	Wasser	I, A
G 0.4	Verschmutzung, Staub, Korrosion	I, A
G 0.5	Naturkatastrophen	A
G 0.6	Katastrophen im Umfeld	A
G 0.7	Großereignisse im Umfeld	C, I, A
G 0.8	Ausfall oder Störung der Stromversorgung	I, A

Abbildung 17: Ausschnitt aus der Tabelle der elementaren Gefährdungen, BSI-Standard 200-3 [46]

Erstellung einer Gefährdungsübersicht

Das BSI hat im Rahmen des vierten Kapitels eine neue Methode für Nutzer des IT-Grundschutzes zur Verfügung gestellt. Im Vergleich zum Vorgänger des Standards ist in der neuen Auflage eine detaillierte Beschreibung der Methode zu finden. Das Ziel ist, anhand der im IT-Grundschutz-Kompendium aufgelisteten elementaren Gefährdungen eine Liste zu erstellen, die den betrachteten Informationsverbund betreffen. Um eine Gefährdungsliste zu erhalten, werden zunächst alle elementaren Gefährdungen mit den ausgewählten Bausteinen in einer Tabelle eingetragen. Die Zuordnung erfolgt anhand der Bewertung, ob Grundwerte der Informationssicherheit durch die jeweilige Gefährdung beeinträchtigt werden können. Sind alle potenziell bedrohten Grundwerte eingetragen, kann eine Komprimierung der Tabelle vorgenommen werden. Die Liste bleibt überschaubar, wenn nicht betroffene Einheiten ausgenommen werden. Zusätzlich wird im BSI-Standard 200-3 die Erweiterung der Tabelle um eine Spalte, in der die Wirkung und Relevanz der Objektgefährdungen beurteilt werden, empfohlen. Die Gefährdungsübersicht kann wie folgt aussehen:

Gefährdung	Grundwerte	Wirkung und Relevanz	Kommentar
G 0.1 Feuer	Verfügbarkeit	**Indirekte Wirkung/ nicht relevant**	Die Gefährdung für ein Betriebssystem durch Feuer ist irrelevant, es würden durch die Betrachtung von G 0.1 *Feuer* keine neuen Aspekte gegenüber G 0.25 *Ausfall von Geräten oder Systemen* abgedeckt.
G 0.9 Ausfall oder Störung von Kommunikationsnetzen	Verfügbarkeit, Integrität	**Indirekte Wirkung/ nicht relevant**	Die Gefährdung für ein Betriebssystem durch *Ausfall oder Störung von Kommunikationsnetzen* ist indirekt, es würden durch die Betrachtung von G 0.9 keine neuen Aspekte gegenüber G 0.26 *Fehlfunktionen von Geräten oder Systemen* entstehen. Ein Betriebssystem bietet keine spezifischen Schutzmaßnahmen gegen G 0.9, die Gefährdung ist somit hier nicht relevant. Es sind keine spezifischen Maßnahmen erforderlich.
G 0.25 Ausfall von Geräten oder Systemen	Verfügbarkeit	**Direkte Wirkung/ relevant**	Die Gefährdung durch G 0.25 *Ausfall von Geräten oder Systemen* wirkt direkt auf ein Betriebssystem ein. Daher sind Maßnahmen gegen G 0.25 *Ausfall von Geräten und Systemen* zu prüfen.
G 0.26 Fehlfunktion von Geräten oder Systemen	Vertraulichkeit, Verfügbarkeit, Integrität	**Direkte Wirkung/ relevant**	Die Gefährdung durch G 0.26 *Fehlfunktionen von Geräten oder Systemen* wirkt direkt auf ein Betriebssystem ein. Daher sind Maßnahmen gegen G 0.26 *Fehlfunktionen von Geräten und Systemen* zu prüfen.

Abbildung 18: Beispiel für die Ermittlung elementarer Gefährdungen [46]

Um das Verständnis zu vertiefen und eine beispielhafte Gestaltung der Listen für die Praxis zu empfehlen, stellt der Autor des Standards weitere Beispiellisten vor, um die Modellierung der Objekte zu erleichtern.

Die finale Version der Gefährdungsübersicht kann wie folgt aussehen:

Virtualisierungsserver S1
Vertraulichkeit: hoch Integrität: hoch Verfügbarkeit: hoch
G 0.14 *Ausspähen von Informationen/Spionage* G 0.15 *Abhören* G 0.18 *Fehlplanung oder fehlende Anpassung* G 0.19 *Offenlegung schützenswerter Informationen* G 0.21 *Manipulation von Hard- oder Software* G 0.22 *Manipulation von Informationen* G 0.23 *Unbefugtes Eindringen in IT-Systeme* G 0.25 *Ausfall von Geräten oder Systemen* G 0.26 *Fehlfunktion von Geräten oder Systemen* G 0.28 *Software-Schwachstellen oder -Fehler* G 0.30 *Unberechtigte Nutzung oder Administration von Geräten und Systemen* G 0.31 *Fehlerhafte Nutzung oder Administration von Geräten und Systemen* G 0.32 *Missbrauch von Berechtigungen* G 0.40 *Verhinderung von Diensten (Denial of Service)* G 0.43 *Einspielen von Nachrichten* G 0.45 *Datenverlust* G 0.46 *Integritätsverlust schützenswerter Informationen*

Abbildung 19: Beispiel für eine Gefährdungsübersicht [46]

Unter zusätzlichen Gefährdungen werden Bedrohungen für Bausteine, die über elementare Gefährdungen hinausgehen und nur in speziellen Umgebungen auftreten, verstanden. Um zu dieser Kategorie zu gehören, gelten nennenswerte Auswirkungen und ein spezielles Einsatzumfeld als Voraussetzung. Die Ermittlung von zusätzlichen Gefährdungen ist besonders von Bedeutung, wenn Zielobjekte mit Hilfe von IT-Grundschutz-Bausteinen nicht ausreichend modelliert werden können.

Risikoeinstufung

In Kapitel 5 wird der nächste Schritt nach der Identifizierung relevanter Gefährdungen erläutert. Um eine genaue Einstufung der Risiken vornehmen zu können, müssen Risiken ermittelt und bewertet werden. Eine Einschätzung des Risikos liefert eine aussagekräftige Beurteilung der Gefahr. Risiken lassen sich durch zwei Einflussfaktoren ermitteln: Eintrittshäufigkeit und potenzielle Schadenshöhe. Zur Einschätzung der Eintrittshäufigkeit empfiehlt das BSI, Experten, Statistiken und Erfahrungen aus der Vergangenheit der Institution heranzuziehen. Institutionen sollten das Bewertungsschema für die Kategorisierung der Schadenshöhe eigenständig erstellen, denn Randbedingungen unterscheiden sich von Organisation zu Organisation. Bei finanziellen Schäden und Imageschäden handelt es sich um subjektive Schäden. Daher eignet sich beispielsweise das Bewertungsschema einer großen Verwaltungsbehörde nicht für ein kleines Unternehmen. Eine Gefahr, die in der Verwaltungsbehörde vorhanden ist und als normal eingestuft wird, kann für das kleine Unternehmen existenzbedrohende Auswirkungen haben. Für die Bewertung von Risiken wird in der Fachliteratur der Matrixansatz empfohlen. In folgender Grafik ist ein Beispiel für eine Risikomatrix mit jeweils vier Einteilungen dargestellt.

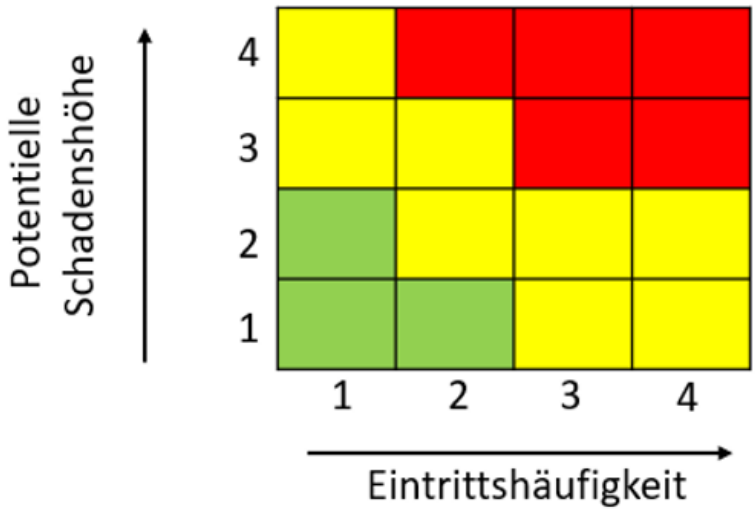

Abbildung 20: Risikomatrix zur Beurteilung von Risiken, eigene Darstellung

Die Empfehlung des BSI ist die Verwendung von aussagekräftigen Risikokategorien mit einer Beschreibung. Die Anzahl der gewählten Kategorien ist unterschiedlich, liegt jedoch überwiegend bei mehr als drei.

Behandlung von Risiken

Nach dem Identifizieren und Bewerten von Risiken muss geklärt werden, wie diese behandelt werden sollen. Die Risikokultur und der Risikoappetit von Institutionen sind individuell, daher gibt es mehrere Möglichkeiten, um Risiken adäquat zu behandeln. Abhängig von der Eintrittshäufigkeit und der potenziellen Schadenshöhe gibt es sinnvolle Strategien, um mit Risiken umzugehen. Risikovermeidung, Risikotransfer und Risikoakzeptanz sind bewährte Ansätze zum Umgang mit Risiken. Die Entscheidung darüber liegt bei der Führungsebene und muss von dieser abgewogen werden. Kapitel 6 aus dem BSI-Standard 200-3 behandelt die genannten Risikoansätze.

In Kapitel 7 und 8 werden die Schritte nach der Durchführung der Risikoanalyse thematisiert.

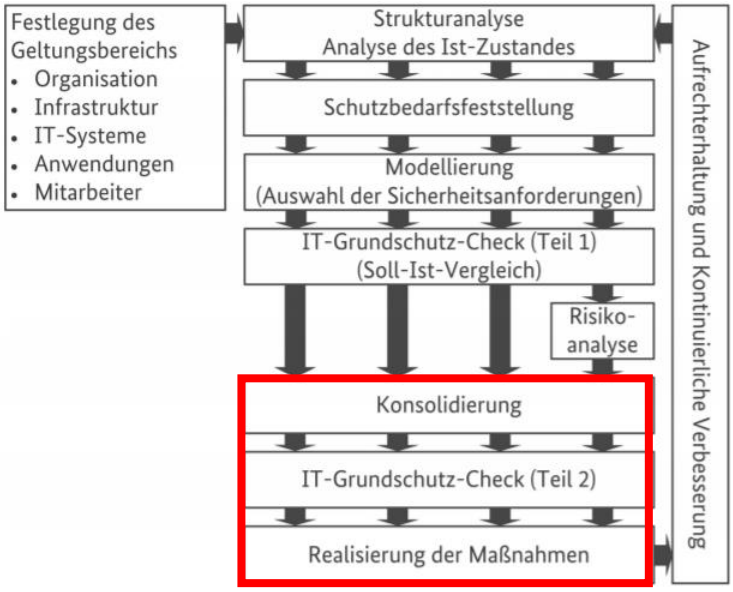

Abbildung 21: Ablauf der Sicherheitskonzeption nach der Standardabsicherung [23]

Wie bereits erwähnt, ergeben sich häufig zusätzliche Gefährdungen, die nicht durch die Gefährdungsliste abgedeckt werden können. Um auf diese Bedrohungen reagieren zu können, sind zusätzliche Sicherheitsmaßnahmen notwendig. Nach dem Hinzufügen spezieller Maßnahmen muss das Sicherheitskonzept vereinheitlicht und konsolidiert werden. Realisiert wird die Konsolidierung anhand folgender vom BSI aufgestellten Kriterien:

- Eignung der Sicherheitsmaßnahmen zur Abwehr der Gefährdungen
- Zusammenwirken der Sicherheitsmaßnahmen
- Benutzerfreundlichkeit der Sicherheitsmaßnahmen
- Angemessenheit/Qualitätssicherung der Sicherheitsmaßnahmen
- Integration der Inhalte

Die Rückführung in den Sicherheitsprozess fasst die Prozessschritte zusammen, die nach der Konsolidierung der Sicherheitsmaßnahmen unternommen werden müssen, um die IT-Grundschutz-Methodik aus dem BSI-Standard 200-2 regelkonform fortzusetzen. Das Sicherheitskonzept nach der Risikoanalyse dient als Basis für folgende Schritte:

- IT-Grundschutz-Check
- Umsetzung der Sicherheitskonzeption
- Überprüfung des Informationssicherheitsprozesses in allen Ebenen
- Informationsfluss im Informationssicherheitsprozess
- ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz

Die Schritte „IT-Grundschutz-Check“, „Umsetzung der Sicherheitskonzeption“ und „Überprüfung des Informationssicherheitsprozesses in allen Ebenen“ werden in Kapitel 3.2 BSI-Standard 200-2 dargestellt. Weitere Informationen über die Zertifizierung sind in Kapitel 3.7 zu finden.

Kapitel 9 enthält diverse Anhänge zum Thema Risikomanagement.

Fazit

Die Änderungen der Neukonzeption des Standards basieren auf dem BSI-Standard 100-3 und der Integration der Ergänzung zum BSI-Standard 100-3 (Version 2.5). Neben sprachlichen Präzisierungen und geringfügigen Strukturänderungen sind der eingeführte Matrix-Ansatz zur Risikobewertung und der unternehmensspezifische Risikoappetit im Standard neu. Im Dokument wird auf die Darstellung der Risikoanalyse in der Sicherheitskonzeption nach der gewählten Vorgehensweise fokussiert. Dies betrifft die Standard- und die Kernabsicherung. [46] [47]

3.4 BSI-Standard 100-4: Notfallmanagement

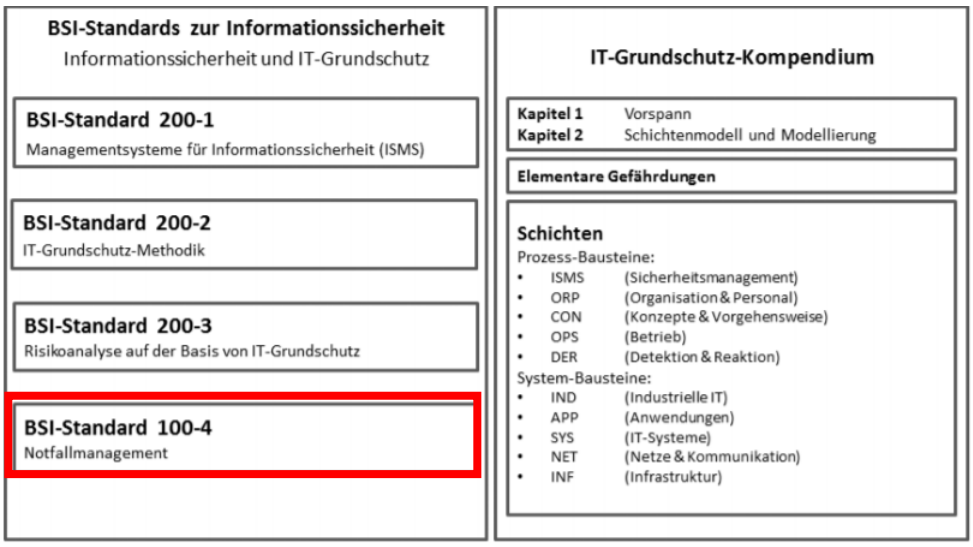

Abbildung 22: Der moderne IT-Grundschutz [21]

Im vierten Teil des IT-Grundschutzes findet eine Beschäftigung mit dem Etablieren und Betrieb des Notfallmanagements statt. Aufgabe des Notfallmanagements ist die Aufrechterhaltung des Geschäftsbetriebs. Diese Aufgabe wird durch die Aufrechterhaltung der kritischen Geschäftsprozesse und durch die Eingrenzung der Auswirkungen möglicher Schadensvorfälle erfüllt.

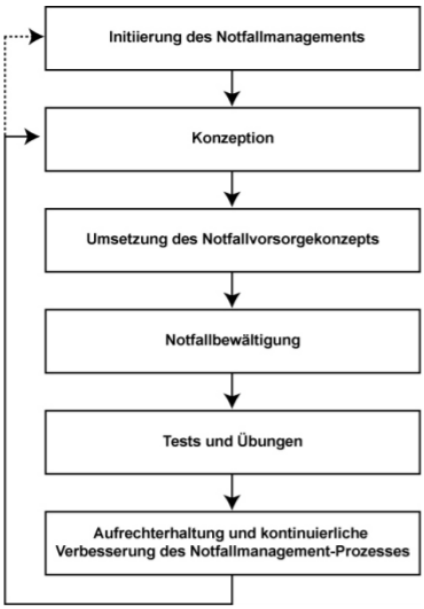

Abbildung 23: Der Notfallmanagementprozess nach BSI-Standard 100-4 [49]

Im Dokument wird der systematische Prozess für die Gestaltung eines Notfallmanagements beschrieben. Der erste Teil des Prozesses beschäftigt sich mit der Initiierung des Notfallmanagements durch das Schaffen optimaler Rahmenbedingungen, wie Aufnahme des Themas in die Unternehmensstrategie und Eingliederung in die Organisationsstruktur.

In der Konzeptionsphase sind Verfügbarkeitsanforderungen bzw. Schwachstellen zu identifizieren, auf die dementsprechend mit Gegenmaßnahmen zu reagieren ist. Des Weiteren beschäftigt sich das Kapitel mit der Erstellung einer Business-Impact-Analyse und einer Risikoanalyse, die als Voraussetzung für das Notfallkonzept gelten. Anschließend wird das Notfallkonzept unter Beachtung wirtschaftlicher Faktoren umgesetzt. Danach wird eine Notfall- und Krisenbewältigung mithilfe geeigneter organisatorischer Strukturen und der Einberufung eines Krisenstabs aufgebaut. Um Effektivität und Effizienz der Notfallvorsorgeplanung zu überprüfen, werden Tests und Übungen durchgeführt und das Ergebnis ausgewertet. Da der Prozess kein einmaliges Vorhaben, sondern eine kontinuierliche Angelegenheit ist, muss stets dafür gesorgt werden, dass jener aufrechterhalten bleibt, der den Geschäftsbetrieb in einer Notfallsituation unterstützt. Ebenfalls ist es Pflicht der Organisation, den Prozess weiterzuentwickeln und zu optimieren.

Dieses Unterkapitel ist aus Übersichtlichkeitsgründen angeführt worden, da das BSI dieses Dokument nicht überarbeitet hat. Das Notfallmanagement ist sowohl Teil des klassischen als auch des modernisierten IT-Grundschutzes. Um Anwender nicht zu verwirren, hat sich das BSI für den Namenserhalt entschieden. Daher trägt das Schreiben den Zusatz 100-4, obwohl es ebenfalls im aktualisierten IT-Grundschutz zu finden ist. [49]

Zukunft

Das BSI arbeitet bereits an der Weiterentwicklung des BSI-Standard 100-4. Unter dem Namen BSI-Standard 200-4 wird das Notfallmanagement neu konzeptioniert. Einem Bericht zufolge liegt der Schwerpunkt auf dem Business-Continuity-Management-System (BCMS) und der Einführung eines Stufenmodells zur Etablierung eines funktionierenden BCMS. [50]

Das Datum der Veröffentlichung der aktualisierten Version ist derzeit noch nicht bekannt.

3.5 IT-Grundschutz-Kompendium

Dieses Kapitel stellt ergänzend zu den BSI-Standards ein umfangreiches Werkzeug, das IT-Grundschutz-Kompendium dar. Das Werk fasst Gefährdungen und Sicherheitsanforderungen zusammen und ist Teil des modernisierten IT-Grundschutzes. Zunächst wird der Vorgänger vorgestellt und darauf folgt die Erläuterung des Aufbaus und der Elemente des Kompendiums.

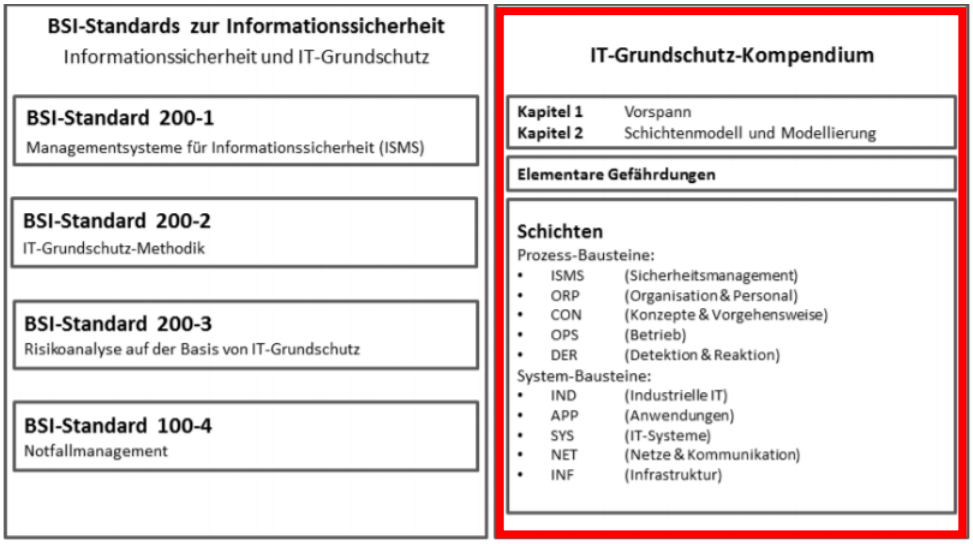

Abbildung 24: Der moderne IT-Grundschutz [21]

IT-Grundschutz-Kataloge

Mit der fünfzehnten und letzten Ergänzungslieferung haben die IT-Grundschutz-Kataloge im Jahr 2016 eine Komplexität erreicht, die nicht mehr zu bewältigen war. Die Aufnahme neuer Bausteine, wie z. B. Cloud Computing, IoT, ICS, die durch die technologische Entwicklung entstanden sind, hätte einen weiteren Verlust der Übersichtlichkeit zur Folge gehabt. Bei einem Dokument mit mehr als 5000 Seiten ist der Einarbeitungsaufwand enorm hoch, was dem Prinzip der Anwenderfreundlichkeit widerspricht. Das BSI beschloss daher, eine neue Struktur für die Kataloge zu finden. Das Ergebnis der Neuausrichtung war das IT-Grundschutz-Kompendium.

Eine detaillierte Beschreibung der IT-Grundschutz-Kataloge ist nicht Gegenstand dieser Arbeit, deshalb wird ausschließlich auf essenzielle Teile eingegangen. Im Dokument wird als Einstieg die Vorgehensweise durch das Hervorheben der Notwendigkeit des Informationssicherheitsmanagements betont.

Den Hauptteil bilden drei unterschiedliche Kataloge. Zunächst die Bausteinkataloge mit fünf Schichten, die verschiedene Sicherheitsaspekte eines Informationsverbunds zusammenfassen. Später wurden diese Schichten in ein neues Schichtenmodell im IT-Grundschutz-Kompendium überführt und durch weitere Bausteingruppen ergänzt. Im zweiten Katalog ist eine pauschal angenommene Gefährdungslage dargestellt. Die bspw. auf höhere Gewalt oder organisatorischen Mängel zurückzuführenden Gefahren werden mit Benotung auf mögliche Auswirkungen, falls diese nicht beachtet werden, beschrieben. Zuletzt folgt ein umfangreicher Maßnahmenkatalog, in dem eine ausführliche Beschreibung der Maßnahmen als Umsetzungshilfe gegeben wird. Neben konkreten Sicherheitsmaßnahmen und der Beschreibung, wie diese umzusetzen sind, werden Sicherheitsdomänen erneut aufgezeigt. Abschließend gibt es für Anwender die Möglichkeit, ihre Ergebnisse zu überprüfen, indem sie Prüffragen durchgehen bzw. beantworten. Ein wichtiger Unterschied zwischen dem Katalog und seinem Nachfolger ist, dass jene Maßnahmen, deren Umsetzung verpflichtend ist, im Kompendium dargestellt werden. Zuvor wurden Anforderungen nur formuliert, dem Anwender blieb jedoch die Entscheidungsfreiheit darüber, auf welchen Weg er diese umsetzt. [51]

IT-Grundschutz-Kompendium

Das vom BSI entwickelte Standardwerk stellt eine der wichtigsten Komponenten des IT-Grundschutzes auf 816 Seiten (Edition 2020) dar. Das modular aufgebaute Dokument enthält standardisierte Sicherheitsanforderungen, die nach Bausteinen gruppiert sind. Das Ziel des IT-Grundschutzes ist der angemessene Schutz der Informationen aller Institutionen. Der ganzheitliche Ansatz der IT-Grundschutz-Methodik sorgt für eine hohe Abdeckung der wichtigsten Sicherheitsanforderungen, um das gewünschte Sicherheitsniveau zu erreichen. Neben den Anforderungen, die für eine akute Basisabsicherung ausreichen, sind die Anforderungen für Standard- und Kernabsicherung ebenfalls aufgelistet. [52]

Anwenderkreis

Anwender des IT-Grundschutz-Kompendiums sollen ein umfassendes Dokument über die technischen, organisatorischen und personellen Aspekte erhalten, die für die Informationssicherheit der Institution bedrohlich sein können.

Aufbau der Überarbeitung

In den im Kompendium formulierten Anforderungen wird beschrieben, was umzusetzen ist, aber nicht, wie es zu erreichen ist. Es handelt sich um eine Zielformulierung und nicht um die Beschreibung der Umsetzungsmittel.

Fortschreibung

Das BSI veröffentlicht jährlich eine aktuelle Version des IT-Grundschutz-Kompendiums. Das aktuelle Kompendium ist die Edition 2020, die im Februar die vorangegangene Auflage aus 2019 ablöste. Für die Erlangung von Zertifizierungen ist das jeweils modernste Kompendium relevant. Die Edition 2020 enthält 96 Bausteine unterschiedlichster informationssicherheitsrelevanter Aspekte, wie z. B. Organisation und Personal oder IT-Systeme. Die Bausteine beziehen sich immer auf den aktuellen Stand der Technik und basieren auf den Kenntnissen zum Veröffentlichungszeitpunkt.

Das BSI stellt die Möglichkeit der branchenübergreifenden Verbesserung des IT-Grundschutz-Kompendiums bereit. Im Kompendium werden allgemeine Aspekte, die nahezu in jedem Unternehmen oder jeder Behörde vorkommen, thematisiert. Darüber hinaus existieren weitere wichtige branchenspezifische bzw. unternehmensspezifische Bausteine. Von der Veröffentlichung der eigenen unternehmensspezifischen Bausteine (selbstverständlich unter Beachtung des Datenschutzes) können Anwender aus der jeweiligen Branche profitieren.

Bei der Überarbeitung des IT-Grundschutz-Kompendiums hat das BSI einen Prozess geschaffen, mit dessen Hilfe Fachexperte ihr Know-how zur Verbesserung des IT-Grundschutzes einbringen können. Das BSI hat die Aufgabe, Arbeitsentwürfe mit vorläufigen Bausteinen zu entwickeln. Erreicht der Arbeitsentwurf den Reifegrad zur Diskussionsveröffentlichung, wird dieser für die Community freigegeben. Nachdem Ideen von Interessierten gesammelt sind, werden die Vorschläge ausgewertet und gegebenenfalls in die finale Version des Bausteins übernommen. Anschließend wird der Baustein nach der Einarbeitung der Community-Hinweise aus dem fachlichen Austausch im Kompendium veröffentlicht. Nach wie vor handelt es sich dabei um einen kontinuierlichen Prozess. Die Überarbeitung eines Bausteins schließt die Unvollständigkeit nicht aus, deshalb kann ein Baustein auch im folgenden Jahr verändert werden.

In der unterstehenden Grafik wird der Arbeitsablauf des BSI deutlich.

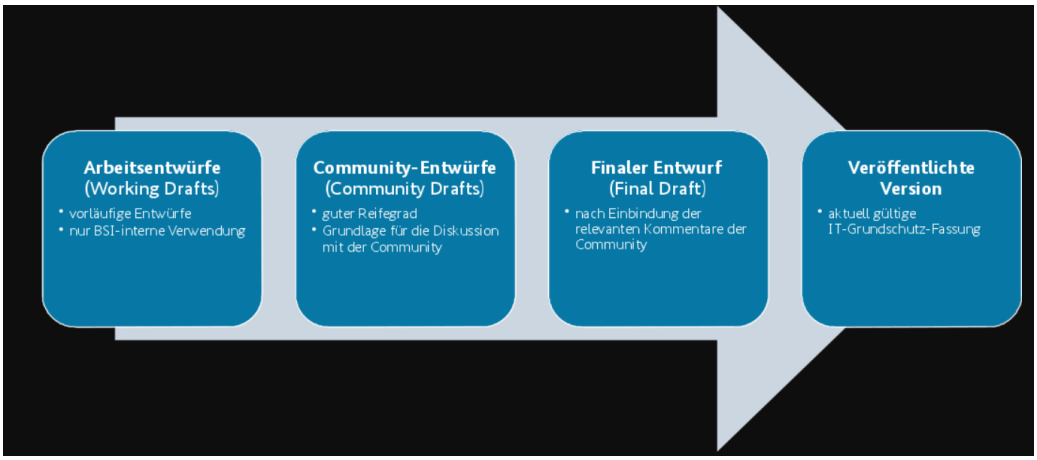

Abbildung 25: Veröffentlichungsworkflow des IT-Grundschutz-Kompendiums [53]

Nicht nur IT-Grundschutz-Anwendern steht die Möglichkeit offen, bei der Entwicklung des IT-Grundschutzes mitzuwirken, sondern auch die Fachöffentlichkeit soll angesprochen werden. Eine Zusammenarbeit mit der Community führt zur Präzisierung der Angaben eines Bausteins und durch Verbesserungsvorschläge aus der Praxis wird der Baustein um weitere essenzielle Punkte erweitert. Dies dient der Optimierung des Endergebnisses (IT-Grundschutz), die somit jedem Anwender zugutekommt. Daher hat das Bundesamt Entwürfe veröffentlicht, die von Interessierten bearbeitet werden können. [53]

Gründe für die Modernisierung

Die Entwickler erklären die Notwendigkeit der Einführung des IT-Grundschutz-Kompendiums und die damit verbundene Ablösung der IT-Grundschutz-Kataloge mit den neuen Anforderungen, die an die Kataloge gestellt wurden. Da die Kataloge nicht effizient an den modernisierten IT-Grundschutz angepasst werden konnten, hat sich das BSI für die Konzeptionierung des IT-Grundschutz-Kompendiums entschieden. Durch dieses sollen sich standardisierte Sicherheitsanforderungen für typische Einsatzszenarien generalisieren lassen, aber keine speziellen Sicherheitsmaßnahmen entwickelt werden. Es werden ausschließlich die zu erreichenden Ziele formuliert und nicht, wie diese zu erfüllen sind. Zuvor hatten Institutionen Schwierigkeiten, da sie die vorgeschriebenen Maßnahmen nicht umsetzen konnten. Sie haben ihre Assets daher mit anderen, oft benutzerdefinierten, Maßnahmen

geschützt. Obwohl das Ergebnis identisch war, entsprach die umgesetzte Maßnahme nicht den Maßnahmen des veralteten IT-Grundschutzes. Deshalb konnte bspw. keine Zertifizierung erlangt werden.

In Kapitel 3.2 wird der neue BSI-Standard 200-2 beschrieben. Der Kern der Modernisierung bildet die Wahl der Absicherungsvorgehensweise. Im klassischen IT-Grundschutz gab es nur eine Vorgehensweise, eine Anpassung des Kompendiums zu den neuen Vorgehensweisen ist unerlässlich.

Ein weiterer wesentlicher Aspekt ist die Reduzierung des Aufwands. Die geänderte Vorgehensweise nach BSI-Standard 200-2 schreibt einen Soll-Ist-Vergleich zwischen den bereits umgesetzten Anforderungen und den neuen Anforderungen aus dem Kompendium vor. Die verbliebenen Anforderungen zeigen Sicherheitsdefizite, die behoben werden müssen. Im neuen IT-Grundschutz wird nur eine individuelle Risikoanalyse für Absicherungsobjekte, die einen signifikant höheren Schutzbedarf aufweisen, verlangt. Aus wirtschaftlicher Sicht war die Durchführung einer Risikoanalyse bei jedem Baustein der Kataloge zuvor als kritisch anzusehen.

Durch die bessere Strukturierung, wie z. B. Zusammenfassung der Bausteine zu Bausteingruppen, Reihenfolgeänderungen sowie einheitliche Struktur der Sicherheitsanforderungen, ist das Finden von gesuchten Inhalten im neuen Kompendium einfacher. Die Komprimierung des Inhalts wird durch die Seitenzahlen deutlich: Die 15. und letzte Auflage der IT-Grundschutz-Kataloge enthielt mehr als 5000 Seiten, durch das Kompendium ist die Seitenanzahl auf 816 (Edition 2020) gesunken, wodurch eine bessere Lesbarkeit und Anwendung in der Praxis gewährleistet wird.

Die Weiterentwicklung des IT-Grundschutz-Kompendiums erlaubt eine kontinuierliche Optimierung des Inhalts. Mit Hilfe der Community arbeitet das BSI an der Verbesserung des Kompendiums unter Beachtung der Meinung der Fachöffentlichkeit. Die Edition 2020 enthält beispielsweise neben zahlreichen Anpassungen zwei zusätzliche Bausteine gegenüber der Edition des Vorjahres. [54][55]

Umsetzungshinweise

Zusätzlich zum IT-Grundschutz-Kompendium sind einige geeignete Maßnahmen aus früheren IT-Grundschutz-Katalogen zu Umsetzungshinweisen geworden. Um Anwender, die an die IT-Grundschutz-Kataloge gewöhnt sind, bei der Umsetzung zu unterstützen,

stellt das BSI kostenlose Umsetzungshinweise zur Verfügung. In diesen sind ausdrückliche Empfehlungen zur Umsetzung der im neuen Kompendium beschriebenen Anforderungen basierend auf langjähriger Erfahrung von Experten und Best Practices enthalten.[Anleitung] Unternehmen und Behörden haben die Möglichkeit, sich daran zu orientieren. Bei Zertifizierungsprozessen werden Organisationen, die benutzerdefinierten Sicherheitsmaßnahmen umgesetzt haben, nicht benachteiligt. Die Hinweise bieten lediglich eine Unterstützungshilfe, die einen Weg aufzeigt, wie die Anforderungen grundschutzgerecht umgesetzt werden können und geben eine Lösungsmöglichkeit zur Erfüllung der Zielvorgaben. Zielvorgaben (Erfüllung von Anforderungen) stehen dabei im Vordergrund und nicht das Mittel oder die Methode zur Erreichung des Ziels. Jedoch ist zu beachten, dass nicht zu jedem Baustein Umsetzungshinweise existieren. [56]

Folgende Abschnitte beschreiben die Elemente des IT-Grundschutz-Kompendiums.

Elementare Gefährdungen

Wie in den Katalogen werden auch im Kompendium elementare Gefährdungen beschrieben, die ein Gefahrpotenzial für die Bausteine darstellen. Die 47 elementaren Gefährdungen stellen Risiken dar, die sich aus grundlegenden Gefahren, wie z. B. höhere Gewalt, technisches Versagen oder menschliche Fehlhandlung, ergeben. Bei der Durchführung einer Risikoanalyse sind elementare Gefährdungen als Gefahrenquellen einzustufen und einzeln zu prüfen. Anhand der zwei Faktoren Eintrittswahrscheinlichkeit und Auswirkung ist die Einstufung der Risiken vorzunehmen. Wurde für ein Zielobjekt noch kein passender Baustein veröffentlicht, werden die elementaren Gefährdungen als Hilfsmittel herangezogen.

IT-Grundschutz-Bausteine

Die Bausteine stehen in der zentralen Rolle im IT-Grundschutz-Kompendium und stellen die Gruppierung von Anforderungen dar. [52]

Da die Struktur aus den Katalogen nicht in das Kompendium übernommen wurde, bedarf es eines grundlegend neuen Aufbaus. Es haben sich nicht nur Namen und Inhalte der Bausteine geändert, sondern auch ihre Ausrichtung. Anstatt konkreter Sicherheitsmaßnahmen

werden im Kompendium Anforderungen zum Schutz der Informationssicherheit formuliert. Die Strukturierung der Bausteine wurde anhand eines neuen Modells festgelegt.

Im neuentworfenen Schichtenmodell werden die Bausteine in prozess- und systemorientierte Bausteingruppen eingeteilt.

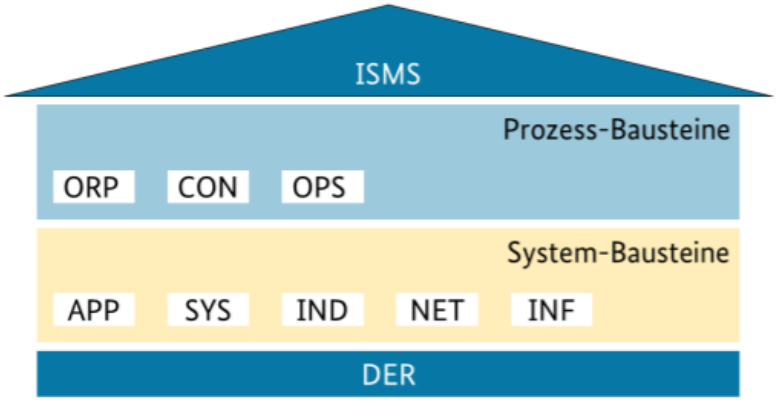

Abbildung 26: Das Schichtenmodell des modernisierten IT-Grundschutzes [52]

Die Gruppierung prozessorientier Bausteine wird folgendermaßen vorgenommen:

- **ISMS**: Managementsysteme für Informationssicherheit; enthält Informationen zu Aufbau und Betrieb eines ISMS im Rahmen des Sicherheitsprozesses
- **ORP**: Organisation und Personal; thematisiert organisatorische und personelle Aspekte bezüglich der Informationssicherheit
- **CON**: Konzepte und Vorgehensweisen; beschreibt Anforderungen zum Thema Konzepte und Vorgehensweisen
- **OPS**: Betrieb; orientiert sich an Sicherheitsaspekten des operativen IT-Betriebs
- **DER**: Detektion und Reaktion; dazu gehören typische Aufgaben von Sicherheitsvorfällen und eine Anforderungsliste angemessener Reaktionen

Zu den systemorientierten Bausteinen gehören folgende Gruppen:

- **APP**: Anwendungen stellen Anforderungen zur Absicherung von Applikationen und Diensten bereit
- **SYS**: IT-Systeme beschäftigen sich mit dem Schutz der eingesetzten IT-Systeme innerhalb der Organisation

- **IND**: Die Industrielle IT ist eine Schicht, die dem modernisierten IT-Grundschutz neu hinzugefügt wurde. Die darunter eingegliederten Bausteine konzentrieren sich auf industrielle Steuerungssysteme (Industrial Control Systems)
- **NET**: Anforderungen aus der Schicht Netze und Kommunikation dienen der Absicherung von Übermittlungswegen und zielen auf sichere Kommunikation zwischen Kommunikationsparteien ab
- **INF**: Die Infrastruktur befasst sich mit den technischen Gegebenheiten und deren sicherem Einsatz

Die Klassifizierung der Bausteine erfolgt danach, ob sie eine Bedeutung für einen Prozess oder ein System haben. Die Bausteine lassen sich in zehn unterschiedliche Bausteingruppen gliedern, die einen für alle Institutionen relevanten Sicherheitsaspekt charakterisieren.

Aufbau von Bausteinen

```
Nummerierung und Name des Bausteins

  • Beschreibung
      o Einleitung
      o Zielsetzung
      o Abgrenzung und Modellierung
  • Gefährdungslage
  • Anforderungen
      o Basisanforderungen
      o Standard-Anforderungen
      o Anforderungen bei erhöhtem Schutzbedarf
  • Weiterführende Informationen
  • Kreuzreferenztabelle zu elementaren Gefährdungen
```

Abbildung 27: Überblick über den Aufbau eines Bausteins aus dem IT-Grundschutz-Kompendium, eigene Darstellung

Die eindeutige Identifikation der Bausteine und eine schnelle Suche werden neben dem Namen des Bausteins durch ein Kürzel aus der Bausteingruppe und einer Nummerierung sichergestellt.

Beschreibung

Im ersten Teil erhält der Leser anhand der Beschreibung des Bausteins grundlegende Informationen zu diesem. Dazu gehören unter anderem eine kurze Einleitung, die Zielsetzung und das Thema Abgrenzung und Modellierung.

Gefährdungslage

Das zweite Kapitel hat zur Aufgabe, spezifische Bedrohungen und bedeutende Schwachstellen des Bausteins aufzuzeigen. Zu jeder Gefahrenquelle gehört eine kurze Erläuterung, in der das Gefahrenpotenzial möglicher Auswirkungen dargelegt wird. Hierbei betont das BSI die Notwendigkeit der Schutzmaßnahmen und appelliert an die Vernunft der Anwender, die genannten Bausteinobjekte angemessen zu schützen, um geschäftskritische Situationen zu vermeiden.

Anforderungen

Im bedeutendsten Teil, Kapitel 3, werden die spezifischen, umzusetzenden Anforderungen an den Baustein beschrieben. Die Anforderungen in drei Kategorien eingeteilt. Die Basisanforderungen stellen grundlegende Aspekte der Sicherheit der Assets zur Problemlösung dar. Sie bieten allein keinen ausreichenden Schutz nach dem IT-Grundschutz. Deshalb werden sie oft in Kombination mit Standardanforderungen oder Anforderungen mit erhöhtem Schutzbedarf angewendet. Basisanforderungen werden durch das Modalverb ‚muss‘ gekennzeichnet und deuten auf die absolute Pflicht deren Umsetzung hin.

Im mittleren Teil des Kapitels werden die Standardanforderungen unter die Lupe genommen. Die Vorgehensweise der Standardabsicherung bietet einen angemessenen und umfassenden Schutz des Informationsverbunds, auf dem diese angewendet wird. Die Erfüllung der Standardanforderungen reicht allein nicht aus. Ein angemessenes Schutzniveau setzt die Umsetzung der Basis- und die darauf aufbauenden Standardanforderungen voraus. Standardanforderungen werden durch das Modalverb ‚soll‘ verdeutlicht.

Die letzte Absicherungsmethode nach dem modernisierten IT-Grundschutz ist die Kernabsicherung. Diese bietet eine tiefgehende Absicherung der ausgewählten geschäftskritischen Objekte. Dazu werden Anforderungen mit erhöhtem Schutzbedarf gezählt. Die Umsetzung

der Anforderungen mit erhöhtem Schutzbedarf keinen organisationsumfassenden Schutz dar. Diese sind ebenfalls in Kombination mit Basis- und/oder Standardanforderungen umzusetzen. Anforderungen mit erhöhtem Schutzbedarf werden durch das Modalverb ‚soll' verdeutlicht.

Darüber hinaus enthält das Kapitel Zuständigkeiten, die als Ansprechpartner fungieren und die Verantwortung für die Umsetzung tragen sollen. Die Ausnahme bildet der Informationssicherheitsbeauftragte (ISB) in der Organisation, der bei allen strategischen Entscheidungen miteinbezogen werden muss und den Umsetzungsgrad überprüft.

Weiterführende Informationen

Im vierten Kapitel findet der Leser weiterführende Informationen zum jeweiligen Baustein. Es existieren weitere Normen und Standards mit engem Bezug zum untersuchten Baustein. Die Analyse weiterer Normen und Standards kann zu einem besseren Schutz beitragen. Nennenswerte Beispiele sind häufig aus ISO/IEC oder NIST gegeben, die weitergehende Anforderungen an den Umgang mit Zielobjekten stellen.

Kreuzreferenztabelle

Im letzten Bereich befindet sich eine Kreuzreferenztabelle zu elementaren Gefährdungen. Die Matrix enthält Zuordnungen relevanter elementarer Gefährdungen zu den Anforderungen. Alle Bausteinanforderungen werden auf relevante elementare Gefährdungen geprüft. Droht der Anforderung eine elementare Gefahr, wird der Zusammenhang mit einem „X" in der Matrix gekennzeichnet. Zusätzlich werden Zusammenhänge auf die Beeinträchtigung der drei Grundwerte der Informationssicherheit geprüft. Ist eines der Schutzziele (Verfügbarkeit, Integrität, Vertraulichkeit) gefährdet, wird es mit der Eintragung des jeweiligen Wertes (C, I, A) in die zugehörige Spalte markiert. Grundsätzlich gilt, dass es Anforderungen gibt, auf die elementare Gefährdungen keine Gefahr bedeuten. Außerdem ist der Tabelle zu entnehmen, dass jeder relevanten elementaren Gefährdung mindestens eine Anforderung zugeordnet wird.

Elementare Gefährdungen Anforderungen	CIA-Werte	G 0.18	G 0.19	G 0.25	G 0.27	G 0.29	G 0.31	G 0.45
CON.5.A1		X						
CON.5.A2								
CON.5.A3		X					X	
CON.5.A4							X	
CON.5.A5								
CON.5.A6		X						
CON.5.A7								
CON.5.A8		X			X			
CON.5.A9		X	X					X
CON.5.A10								
CON.5.A11		X				X		
CON.5.A12	CA							X
CON.5.A13	A			X	X			X

Abbildung 28: Kreuzreferenztabelle zu elementaren Gefährdungen [52]

3.6 Absicherungsstrategien

Im folgenden Abschnitt widmet sich der Autor den unterschiedlichen Wegen, um die Sicherheitskonzeption gemäß BSI-Standard 200-2 in der Institution zu etablieren. Die Basis bildet für die vorliegenden Vorgehensweisen, dass die Institution noch keinen IT-Grundschutz angewendet hat.

Liegt als Basis der bereits eingeführte IT-Grundschutz zugrunde, so soll dieser auf den modernisierten IT-Grundschutz umgestellt werden. Diese Umstellung wird in der Fachsprache als Migration genannt und wird in Kapitel 5 ausführlich behandelt.

Absicherungsstrategien				
Fokus liegt auf der…	Absicherungsphase			Ergebnis
	1. Phase	2. Phase	3. Phase	Nach Abschluss
Basisabsicherung	nur Basis			Basis
	Basis	Standard		Standard
	Basis	Standard	Standard + Kern	Standard + Kern
	Basis + Kern	Standard + Kern		Standard + Kern
Kernabsicherung	nur Kern			Kern
	Kern + Basis	Kern + Standard		Kern + Standard
	Kern + Standard			Kern + Standard
Standardabsicherung	nur Standard			Standard
	Standard + Kern			Standard + Kern

Abbildung 29: Absicherungsstrategien gemäß BSI-Standard 200-2 ohne zuvor angewendeten IT-Grundschutz, eigene Darstellung

Die Grafik zeigt die unterschiedlichen Absicherungsstrategien im Rahmen der Sicherheitskonzeption nach der modernisierten IT-Grundschutz-Methodik. Die Grundlage für die dargestellten Strategien ist, dass die Institution noch keinen IT-Grundschutz eingeführt hat.

Die IT-Grundschutz-Methodik liefert drei Vorgehensweisen (s. Grafik: Spalte 1). Der modernisierte Grundschutz erlaubt Anwendern die phasenweise Einführung der Informationssicherheit (s. Grafik: Spalte 2–4). Das Ziel ist die Absicherung der Informationen nach der Standardabsicherung, die einen umfassenden und tiefgreifenden Schutz der Assets garantiert. Spalte 5 in der Grafik zeigt das Absicherungsergebnis nach der letzten durchgeführten Phase.

Anhand der Basisabsicherung wird die Grafik erläutert:

Nach den Vorarbeiten wurde die Basisabsicherung als Absicherungsvorgehensweise gewählt. Hierbei kommt es zu einer Entscheidung, ob neben der Basisabsicherung noch die Kernabsicherung eingeführt werden soll, um die kritischen Assets abzudecken. Fällt die Entscheidung auf eine Kombination von Basisabsicherung und Kernabsicherung, so sind die kritischen Assets anhand der Kernabsicherung zu schützen und alle anderen ausgewählten Informationsverbünde durch die Basisabsicherung, die ein niedriges Schutzniveau gewährleistet.

Entscheidet sich die Institution anhand der Basisabsicherung eine Erstabsicherung zu etablieren, so wird der ausgewählte Informationsverbund nach der Basisabsicherung geschützt. Es ist möglich, keine weiteren Schritte zu unternehmen; diese Vorgehensweise wird jedoch nicht empfohlen. In der darauffolgenden Phase kann die Basisabsicherung auf die Standardabsicherung heraufgestuft werden. Daraus folgt, dass die ausgewählten Bereiche tiefgehender gesichert werden. So sind die Informationen durch die Standardabsicherung geschützt, was dem Ziel des IT-Grundschutzes entspricht. Stellt die Institution fest, dass es Assets gibt, die noch besser geschützt werden sollen, so bedarf es einer Möglichkeit, diese Bereiche mit zusätzlichen Maßnahmen durch die Kernabsicherung zu schützen.

3.7 Zertifizierung

Wie bereits erwähnt, kann das Erwerben eines Zertifikats eine Menge von Vorteilen mit sich bringen. Das BSI hat gemäß BSI-Errichtungsgesetz die Aufgabe, Sicherheitszertifikate auszustellen. [19]

Für das in der vorliegenden Arbeit behandelte Thema kann eine ISO 27001-Zertifizierung auf Basis des IT-Grundschutzes erteilt werden. Das Zertifikat dient als Nachweis für die Erfüllung der allgemeinen Anforderungen an das Sicherheitsmanagement aus der Norm ISO 27001 und die Umsetzung der konkretisierten Anforderungen aus dem IT-Grundschutz.

Voraussetzung für die Vergabe eines Zertifikats ist eine Überprüfung der umgesetzten Anforderungen nach dem IT-Grundschutz. Die Überprüfung ist von einem BSI-zertifizierten ISO 27001-Grundschutz-Auditor durchzuführen. Zu den Aufgaben gehören u. a. die Sichtung der von der Organisation erstellten Referenzdokumente, eine Vor-Ort-Prüfung und anschließend das Fertigen eines Auditberichts. Auf Basis des Auditberichts entscheidet das BSI über die Ausstellung eines Zertifikats. Die Gültigkeit des Zertifikats beträgt drei Jahre.

Das Erteilen eines ISO 27001-Zertifikats auf Basis des IT-Grundschutzes ist sowohl für die Standardabsicherung als auch für die Kernabsicherung möglich. Diese beiden bieten einen angemessenen Schutz des ausgewählten Informationsverbunds. Da die Basisabsicherung nur grundlegende Sicherheitsmechanismen enthält und als Einstieg konzipiert ist, kann für den Nachweis der Umsetzung ein Testat ausgestellt werden. Folgendes Bild zeigt den zu erlangenden Nachweistyp bei den möglichen Vorgehensweisen nach BSI-Standard 200-2:

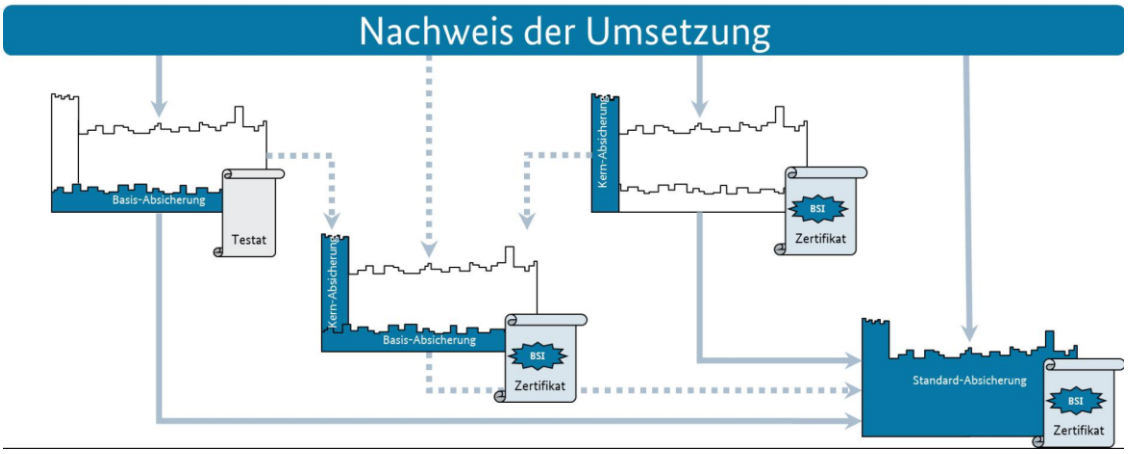

Abbildung 30: Nachweis der Umsetzung für gewählte Absicherungsvorgehensweise [27]

Um das IT-Grundschutz-Zertifikat zu erlangen, stehen drei Audittypen zur Verfügung. Die Erstzertifizierung richtet sich an die Überprüfung des ausgewählten Informationsverbunds, der zum ersten Mal untersucht wird. Die Überwachungsaudits werden nach dem Vergeben eines Zertifikats jährlich durchgeführt, um festzustellen, ob die für die Zertifizierung erbrachte Leistung weiterhin betrieben wird. Rezertifizierungsaudits werden erst nach Ablauf der Zertifizierungslaufzeit durchgeführt, um ein neues, gültiges Zertifikat zu erlangen. Zum großen Teil ist der Ablauf eines Rezertifizierungsaudits mit dem Erstzertifizierungsaudit identisch. [57]

4 Migration auf den modernisierten IT-Grundschutz

Wenn große IT-Projekte bei Unternehmen (wie die Ablösung eines IT-Systems durch ein neues) angesetzt sind, ist der Begriff Migration oft zu hören. Im Allgemeinen bezeichnet die Fachliteratur die IT-Migration als Veränderungsprozess bei der IT-Systemlandschaft. Aus einem bestehenden Zustand werden IT-Systeme in eine neue, veränderte Gestalt umgewandelt. Ein ausschlaggebender Punkt dabei ist, dass bei der Migration Vermögenswerte (gespeicherte Daten, automatisierte Geschäftsprozesse) nicht verfälscht oder verloren gehen dürfen. Zuerst ist die Migration ein strategisches Thema. [58] Ohne ein klares Ziel und gründliche Planung ist das Vorhaben zum Scheitern verurteilt.

4.1 Migrationsvorhaben

Bei der Überführung des klassischen IT-Grundschutzes auf die modernisierte Version schränkt sich der Anwenderkreis ein. Die Migration ist an Institutionen gerichtet, die bereits ein IT-Grundschutz-konformes ISMS nach den BSI-Standards 100-X betreiben und eine Umstellung auf den neuen, modernisierten IT-Grundschutz anstreben. Der Umstieg vom alten auf den neuen IT-Grundschutz ist keine einfache, sondern eine komplexe Aufgabe. Hier gilt der Ansatz: Je größer die Institution ist, die den aktualisierten IT-Grundschutz anwenden will, desto komplexer ist dessen Einführung. Daher wollen Institutionen diese Aufgabe möglichst effizient und effektiv lösen. Institutionen können die dazugehörenden Aufgaben im Alleingang lösen. Schätzen sie aber diese Aufgabenmenge für ihre Ressourcen zu hoch ein, können sie externe Berater beauftragen, um die Herausforderungen des neuen IT-Grundschutzes gemeinsam zu bewältigen.

Das IT-Beratungsunternehmen Capgemini hat Kunden (von staatlichen Behörden bis hin zu privaten Unternehmen) bei der Einführung und Aufrechterhaltung eines wirksamen ISMS unterstützt. Ein umfassender und wirkungsvoller Schutz der Organisationsassets ist ausschließlich durch die aktuelle Version des IT-Grundschutzes gewährleistet. Da diese Kundengruppe bereits ein ISMS betreibt, stellt sich die Frage, inwiefern Maßnahmen auf Anforderungen aus dem neuen IT-Grundschutz abgebildet werden können. Eine Neueinführung ist möglich, jedoch nicht ressourcenschonend. Aufgrund der Reifezeit des neuen IT-Grundschutzes und des verlängerten Zertifizierungszeitraums nach der alten Version hat sich noch kein Service zur Migration des ISMS etabliert.

Diese Arbeit ist als erster Schritt zur Einführung einer neuen Dienstleistung „Migration auf den modernisierten IT-Grundschutz“ bei Capgemini anzusehen.

Ein wesentlicher Punkt vor der Migration ist die Wahl der IT-Grundschutz-Vorgehensweise. In Kapitel 3.2 wurden die Absicherungsarten (Basisabsicherung, Standardabsicherung, Kernabsicherung) dargestellt. Eine Migration bedeutet – wie am Anfang dieses Kapitels erwähnt – einen Veränderungsprozess. Informationsverbünde dürfen entsprechend der klassischen Vorgehensweise aus dem veralteten IT-Grundschutz auf gleichem Niveau oder höher abgebildet werden. Dies hat zu bedeuten, dass die umgesetzte, klassische Vorgehensweise auf die Standardabsicherung oder die Kernabsicherung skaliert werden soll. Der Unterschied zwischen den beiden Migrationszielen ist in der Größe des Geltungsbereichs zu finden.

4.2 Migrationstabellen

Das BSI bietet ein Manko mit den sogenannten Migrationstabellen als Einstieg in die Migration für Institutionen, in denen Unsicherheit über die Vorgehensweise herrscht. Diese Tabellen haben einen Empfehlungscharakter und sollen den Migrationsprozess erleichtern. Sofern sich Institutionen bereits für eine beliebige Migrationsmethodik entschieden haben, können sie die Tabellen außer Acht lassen. Für Institutionen, die sich mit der Migration noch nicht beschäftigt haben, kann dadurch ein Orientierungspunkt geschaffen werden.

Zunächst wird ein Überblick über den Aufbau von Migrationstabellen gegeben. Es bietet sich die Möglichkeit an, den Aufbau von Migrationstabellen anhand einer übersichtlichen,

beschrifteten Grafik zu erläutern. Farbige Hervorhebungen unterstützen den Leser bei den Bereichen.

		B 1.5 Schutz vor Schadprogrammen	M 2.154 (A) Erstellung eines Sicherheitskonzeptes gegen Schadprogramme	M 2.160 (A) Regelungen zum Schutz vor Schadprogrammen	M 3.69 (W) Einführung in die Bedrohung durch Schadprogramme	M 2.157 (A) Auswahl eines geeigneten Viren-Schutzprogramms	M 4.84 (A) Nutzung der BIOS-Sicherheitsmechanismen	M 2.34 (A) Dokumentation der Veränderungen an einem bestehenden System	M 2.158 (A) Meldung von Schadprogramm-Infektionen	M 2.159 (A) Aktualisierung der eingesetzten Viren-Schutzprogramme und Signaturen	M 2.224 (A) Vorbeugung gegen Schadprogramme	M 4.3 (A) Einsatz von Viren-Schutzprogrammen	M 6.23 (A) Verhaltensregeln bei Auftreten von Schadprogrammen	M 6.24 (A) Erstellen eines Notfall-Bootmediums	M 6.32 (A) Regelmäßige Datensicherung	B 3.405 Smartphones, Tablets und PDAs	M 4.466 (C) Einsatz von Viren-Schutzprogrammen auf Tablets und PDAs	B 3.201 Allgemeiner Client	M 4.41 (Z) Einsatz angemessener Sicherheitsprodukte zum IT-Systeme	Bewertung	Kommentar
Basisanforderungen																					
OPS.1.1.4.A1	Erstellung eines Konzepts für den Schutz vor Schadprogrammen		x																	3	Nicht vollständig abgedeckte Soll-Anforderung bzgl. des Falles von nicht vorhandenen verlässlichen Schutzes
OPS.1.1.4.A2	Nutzung systemspezifischer Schutzmechanismen						x													3	Nicht vollständig abgedeckte Muss/Soll-Anforderung bzgl. der Nutzung systemspezifischer Schutzmechanismen
OPS.1.1.4.A3	Auswahl eines Viren-Schutzprogrammes für Endgera					x														3	Nicht vollständig abgedeckte nforderung bzgl. Produkte für den Enterprise-Bereich, Produkte ender sowie Cloud-Funktionen
OPS.1.1.4.A4	Auswahl eines Viren-Schutzprogrammes für Gateway teme zum Datenaustausch					x						x								3	Nicht vollständig abgedeckte nforderung bzgl. Produkte für den Enterprise-Bereich, Produkte ender sowie Cloud-Funktionen
OPS.1.1.4.A5	Betrieb von Viren-Schutzprogrammen											x								3	Nicht vollständig abgedeckte Muss/Soll-Anforderung bzgl. der Erkennungsleistung, der nicht genutzten sicherheitsrelevanten Funktionen sowie der Desktop-Virtualisierung
OPS.1.1.4.A6	Aktualisierung der eingesetzten Viren-Schutzprogramme und Signaturen									x										3	Nicht vollständig abgedeckte Soll-Anforderung bzgl. der
OPS.1.1.4.A7	Sensibilisierung und Verpflichtung der Benutzer			x							x									3	Nicht vollständig abgedeckte Soll-Anforderung bzgl. den grundlegenden Verhaltensregeln
Standard-Anforderungen																					
OPS.1.1.4.A8	Nutzung von Cloud-Diensten					x														3	Nicht vollständig abgedeckte Muss/Soll-Anforderung bzgl. der Nutzung von

Abbildung 31: Aufbau einer Migrationstabelle, eigene Darstellung auf Basis einer Migrationstabelle [59]

In Abschnitt A sind die Anforderungen aus den Bausteinen des modernisierten IT-Grundschutz-Kompendiums aufgelistet. Die Anforderungen sind nach Schutzbedarf kategorisiert. Die Reihenfolge bleibt bei jeder Tabelle konstant. Zuerst werden die Basisanforderungen, danach die Standardanforderungen und zum Schluss die Anforderungen mit erhöhtem Schutzbedarf aufgelistet. Zu jeder Anforderung werden die Nummerierung und der Name angegeben.

Abschnitt B stellt die Maßnahmen aus den alten IT-Grundschutz-Katalogen dar. Die Reihenfolge beginnt immer mit dem Baustein, der den neuen Baustein aus dem IT-Grundschutz-Kompendium bestmöglich abdeckt. In Abschnitt C kommen Maßnahmen aus weiterführenden Bausteinen hinzu. Die Bausteingruppen sind für die bessere Übersicht markiert. Das BSI beachtet an dieser Stelle nur kontextbezogene Bausteine. Im Internet ist der Begriff „15. Ergänzungslieferung“ häufig anzutreffen. Damit ist die 15., letzte Überarbeitung der IT-Grundschutz-Kataloge gemeint, bevor der modernisierte IT-Grundschutz mit dem neustrukturierten IT-Grundschutz-Kompendium eingeführt wurde.

Im mittleren Bereich der Matrix findet sich der Überschneidungsbereich von alten Maßnahmen und neuen Anforderungen. Im Zuordnungsbereich sind inhaltliche Zusammenhänge zwischen einer Anforderung aus dem IT-Grundschutz-Kompendium und einer Maßnahme aus den IT-Grundschutz-Katalogen durch ein „X“ markiert. [59]

Diese Zusammenhänge werden in Abschnitt E klassifiziert. In der Bewertungsspalte sind folgende Werte möglich:

- **1**: Der Wert bedeutet die vollständige Abdeckung der Anforderungen mit den umgesetzten Maßnahmen aus den veralteten IT-Grundschutz-Katalogen. In diesem Fall ist nur noch eine Überprüfung der bestehenden Maßnahmen notwendig. Ergibt sich am Ende eine ordnungsgemäße Funktionsweise der umgesetzten Maßnahmen, ist die Anforderung erfüllt und erfordert somit keine weitere Überarbeitung.

- **2**: Der Wert bedeutet eine partielle Abdeckung der Anforderungen mit den umgesetzten Maßnahmen aus den veralteten IT-Grundschutz-Katalogen. In diesem Fall müssen weitere Sicherheitsmaßnahmen umgesetzt werden, damit die Anforderung erfüllt wird. Eine Überprüfung ist notwendig, da Maßnahmen aus einem anderen Baustein stammen können.

- **3**: Der Wert bedeutet eine unvollständige Abdeckung der Anforderungen mit den umgesetzten Maßnahmen aus den veralteten IT-Grundschutz-Katalogen. Trotz Berücksichtigung weiterer Maßnahmen kann die jeweilige Anforderung nicht in jedem Fall vollständig erfüllt werden. Hierbei wird eine detaillierte Untersuchung angeordnet, wie die Anforderung abgedeckt werden kann.

In Bereich F befindet sich eine Kommentarspalte, in der Hinweise zu weiterführenden Bausteinen gelistet sind.

Rahmenbedingungen

Das BSI stellt Anwendern weitere Informationen zur Nutzung der Migrationstabellen bereit. Es wird darauf hingewiesen, dass alle Anforderungen gleichermaßen behandelt werden

sollen. Die Vollständigkeit der Migrationstabellen bezüglich weiterführender Bausteine kann nicht ausgeschlossen werden. Im Weiteren stellt das BSI einen Hinweis dar, dass bei der Modernisierung marginale Veränderungen an Bausteinen durchgeführt werden könnten und eine 1:1-Zuordnung der Maßnahmen zu Anforderungen, deren Namen gleich sind, ohne weitere Überprüfung nicht übernommen werden soll.

Anwendung

Die Anwendung der Migrationstabelle soll durch drei Anwendungsfälle dargestellt werden:

- **Anwendungsfall 1**: Im Wesentlichen identische Bausteine
  Bausteine sind nicht unbedingt einer großen Veränderung unterzogen worden.
  Es existieren Bausteine, die mit den Bausteinen aus den veralteten IT-Grundschutz-Katalogen im Wesentlichen identisch sind. Der Zuordnungsbereich gibt darüber Auskunft. Je größer der Zusammenhang zwischen Maßnahme und Anforderung ist, desto identischer ist der Baustein. Sind Maßnahmen nach dem klassischen IT-Grundschutz umgesetzt worden, ist eine weitere Änderung nicht mehr nötig, denn die Anforderung kann dadurch vollständig abgedeckt werden (s. Bewertung 1).

- **Anwendungsfall 2**: Inhaltlich veränderte Bausteine
  Bausteine können immer noch denselben Namen besitzen wie zuvor. Jedoch darf dabei keine inhaltliche Überarbeitung ausgeschlossen werden. Dies bedeutet, dass nur ein Teil der Maßnahmen unverändert übernommen werden darf. Eine detaillierte Kontrolle der für die Abdeckung der Anforderungen geeigneten Maßnahmen ist unerlässlich.

- **Anwendungsfall 3**: Neue Bausteine
  Im modernen IT-Grundschutz-Kompendium wurden Bausteine nicht nur verändert, präzisiert oder angepasst, sondern es gibt eine Liste von Bausteinen, die neu hinzugekommen sind. Auslöser dafür sind beispielsweise die technische Entwicklung und neue Ansätze bei der Gruppierung von Bausteinen. Für solche Bausteine sind keine Migrationstabellen zu finden, da diese zuvor nicht existierten. Eine Überprüfung der

individuellen Maßnahmen einer Organisation ist jedoch essenziell, da nicht ausgeschlossen werden kann, dass zum besseren Schutz der Assets solche Maßnahmen zuvor angewendet wurden. [59]

Benutzerspezifische Bausteine

Im IT-Grundschutz-Kompendium listet das BSI allgemeingültige Bausteine auf, die nahezu jede Institution betreffen. Darüber hinaus können Unternehmen zum besseren Schutz ihrer Assets individuelle Maßnahmen umsetzen. Da diese Maßnahmen oft branchenspezifisch sind, empfiehlt das BSI eine Veröffentlichung der Maßnahmen an das BSI. Das Bundesamt reicht diese an die IT-Grundschutz-Community anonymisiert weiter, um neue Bausteine und Anforderungen auszuarbeiten. Dies dient dem Zweck, dass eine vollständige, fehlerfreie Version des IT-Grundschutz-Kompendiums entwickelt werden kann, die allen Organisationen zugutekommt. Trotz aufwendiger Qualitätssicherung kann nicht sichergestellt werden, dass es bei den Migrationstabellen zu Unstimmigkeiten kommt. Auch in diesem Fall dürfen sich Anwender an das BSI wenden.

4.3 Entwicklung einer Transformation-Roadmap

Die Mehrheit der Menschen ist visuell geprägt. Eine übersichtliche Zeichnung prägt sich besser ins Gedächtnis ein. In der IT-Beratung werden häufig Kundenpräsentationen gehalten. Die vorliegende Arbeit wird mit der Erstellung einer managementgerechten Darstellung des Migrationsvorhabens abgerundet.

Die Transformation-Roadmap ist eine visuelle Anleitung – ein sogenannter Fahrplan – zu einem Prozess, wo der Ausgangspunkt und das Ziel meistens vorgegeben sind. Zwischen dem Anfang und dem Ziel steht die inhaltliche Detaillierung der Veränderung. Die Roadmap gehört zu den strategischen Werkzeugen. [60]

Die vorliegende Transformation-Roadmap zeigt den Weg von einer bereits etabliertes ISMS nach der klassischen Vorgehensweise gemäß BSI-Standard 100-2 zum modernisierten IT-Grundschutz. Die grafische Darstellung soll also den aktuellen Stand und den zukünftigen, gewünschten Stand abbilden, wobei unter Transformation der Migrationsprozess verstanden wird.

Die Roadmap soll die signifikanten Änderungen des IT-Grundschutzes aufzeigen und in einer übersichtlichen Form darstellen. Die Roadmap wird von Capgemini bei Kundenpräsentationen verwendet, um den Migrationsweg auf den modernisierten IT-Grundschutz grafisch darzustellen. Zu diesem Zweck ist der klassische IT-Grundschutz als Startpunkt und der modernisierte IT-Grundschutz als Endpunkt vordefiniert.

Um eine geeignete Lösung zu finden, ist das Aufzeigen mehrerer Lösungsvorschläge von großer Relevanz.

Die Alternativvorschläge sind anhand eines Entwicklungsprozesses erarbeitet worden. Zunächst wurden die Ressourcen, die auf der Roadmap vorkommen sollen, bestimmt. Gleichzeitig wurden Ideen generiert, wie die ausgewählten Ressourcen auf einer Präsentationsfolie positioniert werden können. Zudem wurden verschiedene Überlegungen getätigt, in welcher Granularität die Ressourcen dargestellt werden sollen, damit sie möglichst selbsterklärend wirken. Die Ideen führten zur Realisierung von Alternativen. Die umgesetzten Alternativen wurden getestet. Dabei hat sich der Betreuer dieser Arbeit mit langjähriger Expertise als besondere Unterstützung erwiesen. Nach dem Einarbeiten von Feedbacks wurde eine dritte Alternative erstellt, die ein zufriedenstellendes, übersichtliches Ergebnis lieferte.

4.3.1 Alternative 1

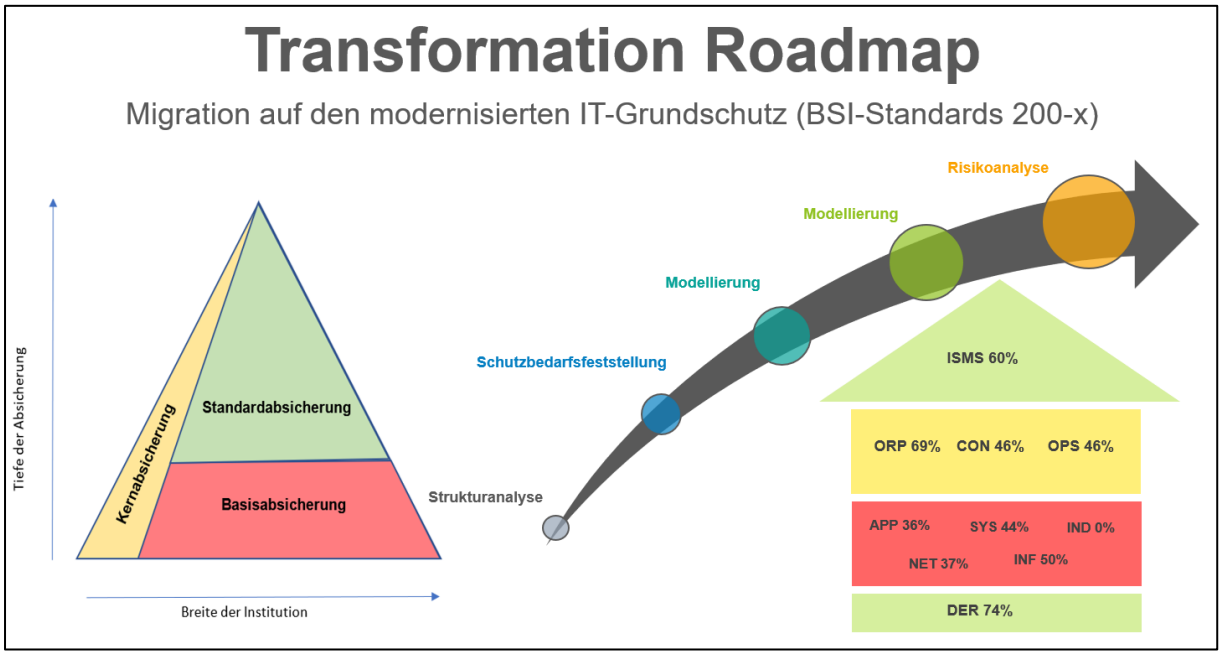

Abbildung 32: Vorschlag für die Transformation-Roadmap (Alternative 1), eigene Darstellung

Für die Transformation-Roadmap (Alternative 1) werden zunächst die benötigten Ressourcen ermittelt. Die drei ausgewählten Darstellungen sind: das Pyramidenmodell der Vorgehensweisen gemäß BSI-Standard 200-2, die Sicherheitskonzeption (ohne Vorstufen) und das Baustein-Hausmodell in Anlehnung an das Schichtenmodell aus dem IT-Grundschutz-Kompendium. Die Überschrift stellt konzise das Ziel dar, das mittels der Roadmap übermittelt wird. Das Pyramidenmodell stellt den Kernpunkt der Modernisierung dar, indem die drei Vorgehensweisen zur Absicherung der Informationsverbünde dargestellt werden. Zudem sind die Phasen der Standardabsicherung als farbige Anhaltspunkte auf einem Pfeil veranschaulicht, der die Abarbeitungsreihenfolge aufzeigt. Für die Transformation-Roadmap sind Vorarbeiten irrelevant. Die Phase der kontinuierlichen Verbesserung wurde ebenfalls weggelassen, da die Migration den Aufbau des ISMS nach dem modernisierten IT-Grundschutz als Ziel hat.

Bei einer Migration ist davon auszugehen, dass die klassische Vorgehensweise des veralteten IT-Grundschutzes in der gleichwertigen Standardabsicherung abgebildet wird. Das Hausmodell stellt die einzelnen Bausteingruppen nach dem IT-Grundschutz-Kompendium

vor, die bei der Migration eine tragende Rolle spielen. Die Bausteine enthalten die Anforderungen, aus denen entsprechende Sicherheitsmaßnahmen abgeleitet werden sollen. Die Prozentzahlen deuten auf den kumulierten Umsetzungsgrad der einzelnen Bausteine hin. Diese bedeuten die bereits abgedeckten Anforderungen (in %) mit Hilfe der bereits umgesetzten klassischen Vorgehensweise aus dem veralteten IT-Grundschutz. Diese Zahlen werden mit Hilfe der Migrationstabellen durch eine generische Aufwandanalyse gebildet. Dabei werden nur die existierenden Migrationstabellen berücksichtigt – oder anders ausgedrückt: Wie viel Prozent der Anforderungen sind bereits durch den Einsatz des klassischen IT-Grundschutzes erfüllt?

4.3.2 Alternative 2

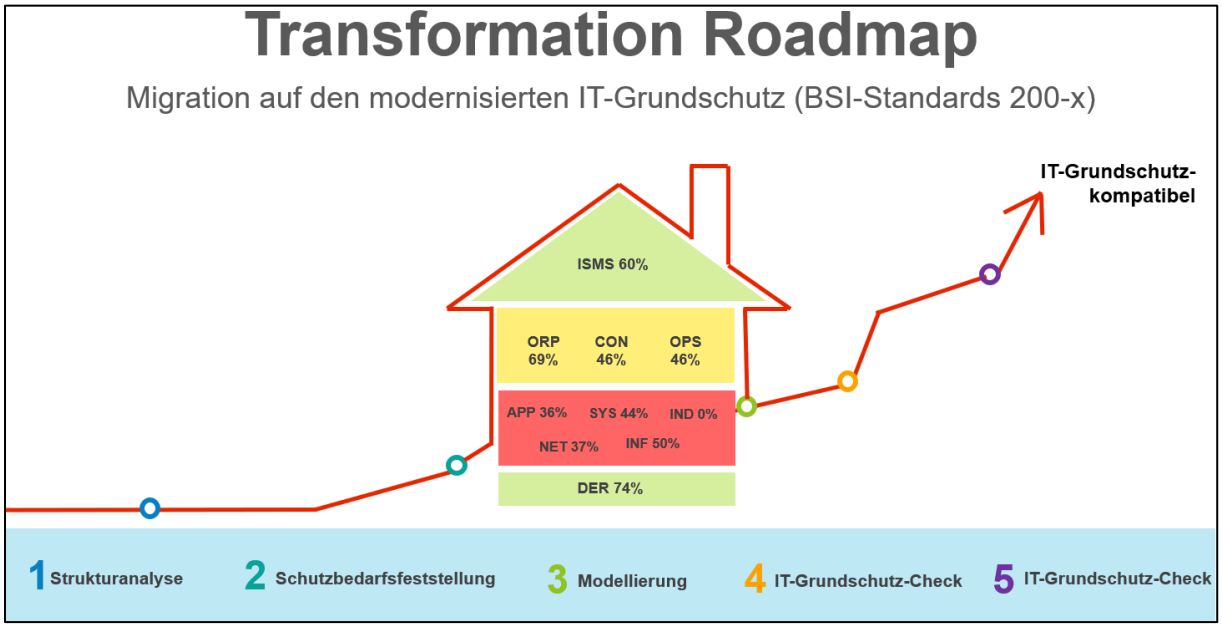

Abbildung 33: Vorschlag für die Transformation-Roadmap (Alternative 2), eigene Darstellung

Parallel zur Alternative 1 wurde Alternative 2 erarbeitet. Auf dem Bild steht das Baustein-Hausmodell im Mittelpunkt. Die Werte bedeuten – wie bei Alternative 1 – die bereits abgedeckten Anforderungen. Die Einzeichnung der Richtung stellt eine Verbesserung dar, indem das Migrationsziel als IT-Grundschutz-kompatibel definiert wird. Die einzelnen Punkte auf dem Weg bedeuten die Phasen bei der Erstellung einer Sicherheitskonzeption. Hierbei gelten die bei Alternative 1 beschriebenen Phasen. Der zugrundeliegende Vorschlag stellt eine schlanke grafische Lösung der Migration dar, indem der Fokus auf die relevanten, durchzulaufenden Phasen und auf den Aufwand gelegt wird, der das Interesse der Kunden weckt: Kunden wollen wissen, wie viel Aufwand auf sie zukommt.

4.3.3 Alternative 3

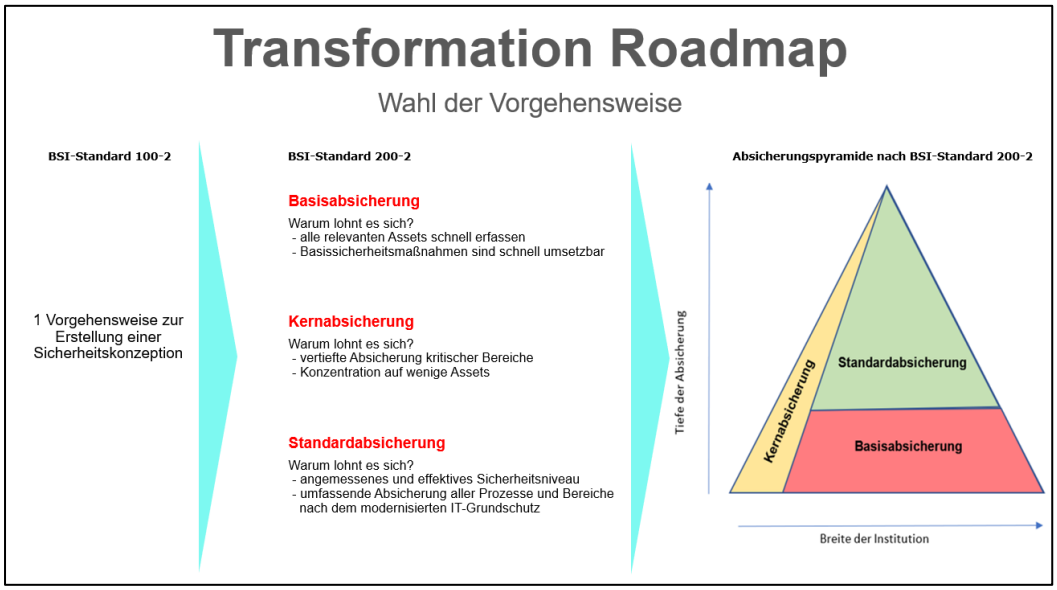

Abbildung 34: Vorschlag für die Transformation-Roadmap I (Alternative 3), eigene Darstellung

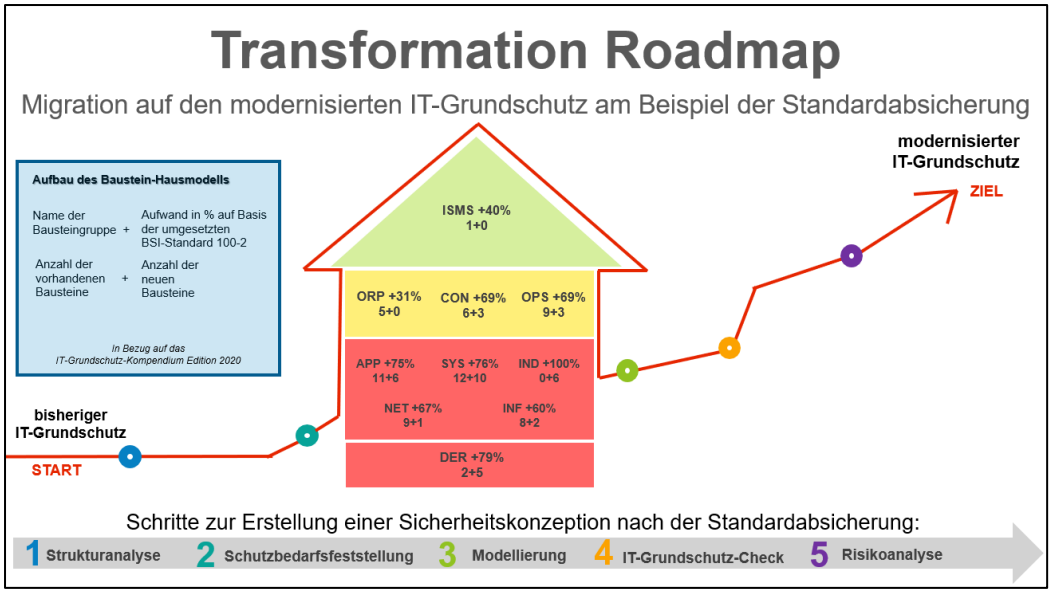

Abbildung 35: Vorschlag für die Transformation-Roadmap II (Alternative 3), eigene Darstellung

Als Testperson wurde aufgrund seiner langjährigen Expertise und Kompetenz in der IT-Beratung der Betreuer der vorliegenden Arbeit und Leiter der Cyber-Security-Abteilung ernannt. Nach der Einarbeitung der Hinweise, die in der Testphase entstanden sind, hat sich der Umfang des Vorschlags auf zwei Präsentationsfolien erweitert. Gewöhnlicherweise

handelt es sich bei Transformation-Roadmaps um einseitige Dokumente. Aufgrund der Anzahl der signifikanten Änderungen im neuen IT-Grundschutz ist die Erweiterung des Umfangs sinnvoll und notwendig. Eine leserfreundliche Gestaltung der Roadmap wird ebenfalls durch zwei nicht mit Grafiken überladene Folien berücksichtigt.

In Teil I ist der Kernpunkt der modernisierten IT-Grundschutz-Methodik dargelegt. Hierbei wurde ein Ansatz gewählt, der die Entwicklung präsentiert. Zunächst wird darauf eingegangen, wie die Methodik nach BSI-Standard 100-2 definiert ist. Durch die Modernisierung ist daraus die Methodik nach BSI-Standard 200-2 entwickelt worden. Anwender stehen drei Vorgehensweisen anstatt einer zur Auswahl. Die Roadmap enthält eine prägnante Beschreibung der drei Vorgehensweisen. Das Pyramidenmodell leistet eine große Hilfe bei schneller Einordnung der Vorgehensweisen in den unternehmerischen Kontext und bei der Erkennung des Zusammenhangs zwischen diesen. Die farbliche Darstellung orientiert sich am Ampelsystem (rot = unterdurchschnittlich, gelb = durchschnittlich, grün = überdurchschnittlich).

In Teil II wird eine allgemeine Migrationsvorgehensweise am Beispiel der Standardabsicherung erläutert. Der Migrationsprozess begleitet Institutionen vom Anfang bis zum Ende. Als Start- und Endpunkt sind die zwei Versionen des IT-Grundschutzes eingezeichnet. Die farbigen Punkte stellen die Phasen der Sicherheitskonzeption nach der Standardabsicherung dar – wie bei Alternative 1. Das Baustein-Hausmodell zeigt die Bausteine aus dem Kompendium. Da Aufwand nicht quantitativ messbar ist, ist eine generische Aufwandsanalyse für jeden Baustein durchgeführt worden. Zudem wird durch eine Legende erklärt, wie die Werte bei jeder Bausteingruppe zu interpretieren sind.

Die erste Zeichenkette ist die Bezeichnung der jeweiligen Bausteingruppe. Auf gleicher Höhe liegt ein Prozentwert. Dieser bedeutet den zusätzlichen Aufwand bei Anforderungen, die nach der Modernisierung zu erfüllen sind. Die Basis (100 %) dafür bildet die Abdeckung durch die klassische Vorgehensweise. Bei der Aufwandsermittlung wurden in dieser Alternative auch Bausteine berücksichtigt, für die keine Migrationstabellen existieren. Ein Prozentwert ist häufig nicht aussagekräftig genug; deshalb sollen konkrete Werte aufgeführt werden. Um Kunden einen groben Überblick zu verschaffen, ist hier die Wahl der Bausteine sinnvoll. Die Bausteine unterteilen sich in alte und neue Bausteine, die aus den IT-Grundschutz-Katalogen bzw. aus dem Kompendium stammen.

Beispiel: IND + 100 %, 0 + 6

IND steht für die Bausteingruppe „Industrielle IT“. Der Grad der Veränderung ist 0 %. Die Anzahl der alten Bausteine beträgt 0, die Anzahl der neuen Bausteine beträgt 6. Als valide Begründung der Werte gilt die Existenz der Bausteine. Der klassische IT-Grundschutz hat diese Bausteingruppe nicht erfasst, erst in der modernisierten Version ist die Gruppe hinzugefügt worden. Die „Industrielle IT“ beschäftigt sich mit Bausteinen, die während der Nutzungszeit des alten IT-Grundschutzes kaum Praxisrelevanz aufzeigten.

Generische Aufwandsanalyse

Anhand folgender Tabelle kann der Aspekt Aufwand bei der Migration bestimmt werden. Im ersten Bereich (1) sind alle IT-Grundschutz-Bausteine, in Bausteingruppen strukturiert, aus dem Kompendium aufgelistet. Farbliche Hervorhebungen in dieser Spalte geben Auskunft über die Existenz der Migrationstabelle. Bausteine beinhalten eine bestimmte Anzahl von Anforderungen (2). Die Gesamtanzahl der Anforderungen teilt sich in Basis-, Standardanforderungen und Anforderungen mit erhöhtem Schutzbedarf auf. Diese werden wiederum in drei Kategorien eingeteilt:

- Die Zahl in der ersten Spalte einer Absicherungsart markiert die Anzahl der Anforderungen, die bei der Migration durch bereits umgesetzte Maßnahmen aus dem klassischen IT-Grundschutz erfüllt sind.
- Die Zahl in der mittleren Spalte markiert die Anzahl der Anforderungen, die bei der Migration durch bereits umgesetzte Maßnahmen aus dem klassischen IT-Grundschutz teilweise erfüllt sind.
- Die Zahl in der letzten Spalte einer Absicherungsart markiert die Anzahl der Anforderungen, die bei der Migration durch bereits umgesetzte Maßnahmen aus dem klassischen IT-Grundschutz nicht erfüllt werden können.

Farbliche Hervorhebungen helfen bei der Abgrenzung zwischen Absicherungsarten.

Prozess-Bausteine		Anzahl Anforderungen	davon Basisanforderungen			davon Standardanforderungen			Anforderungen mit erhöhtem Schutzbedar		
SMS:Sicherheitsmanagement											
SMS.1	Sicherheitsmanage	17	5	1	3	4	0	2	2	0	0
ORP: Organisation und Personal											
ORP.1	Organisation	14	5	0	0	7	0	1	1	0	0
ORP.2	Personal	13	2	1	2	2	0	3	3	0	0
ORP.3	Sensibilisierung un	[illegible]	1	1	1	4	0	1	0	0	1
ORP.4	Identitäts- und Ber	[illegible]	6	0	3	8	0	2	2	0	0
ORP.5	Compliance Manag	[illegible]	2	0	1	4	0	1	1	1	1
CON: Konzepte und Vorgehensweisen											
CON.1	Kryptokonzept	18	1	0	1	2	0	2	8	0	4
CON.2	Datenschutz	1	0	0	1	0	0	0	0	0	0
CON.3	Datensicherungsko	13	5	0	0	5	2	0	0	0	1
CON.4	Auswahl und Einsat	12	2	0	1	2	0	4	0	0	3
CON.5	Entwicklung und Ei	13	1	1	3	4	1	0	2	0	1
CON.6	Löschen und Vernic	11	1	0	1	3	0	3	2	0	1
CON.7	Informationssicher	18			12			2			4
CON.8	Software-Entwickl	19			10			6			3
CON.9	Informationsaustau	8			3			5			0
OPS: Betrieb											
OPS.1											
OPS.1.1											
OPS.1.1.2	Ordnungsgemäße I	18			6			6			6
OPS.1.1.3	Patch- und Änderun	14	1	2	0	8	0	0	3	0	0
OPS.1.1.4	Schutz vor Schadpro	15	0	0	7	0	0	2	0	0	6
OPS.1.1.5	Protokollierung	13	2	0	3	1	1	3	1	0	2
OPS.1.1.6	Software-Tests und	14			5			8			1
OPS.1.2											
OPS.1.2.2	Archivierung	21	8	1	0	6	1	3	0	0	2
OPS.1.2.3	Informations- und D	18	1	1	3	4	2	1	5	0	1
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Abbildung 36: Generische Aufwandsanalyse (Ausschnitt), eigene Darstellung

Um den Aufwand zu ermitteln, ist die Anzahl der erfüllten Anforderungen den nichterfüllten Anforderungen gegenüberzustellen. In dieser Konstellation werden Anforderungen, die nicht erfüllt sind und Anforderungen, die teilweise erfüllt sind, als eine Einheit betrachtet. Maßgebend ist die Anzahl der Anforderungen einer Absicherungsart, die durch bereits umgesetzte Maßnahmen aus den IT-Grundschutz-Katalogen abgedeckt sind.

- Bereich 1 stellt den kumulierten Umsetzungsgrad der erfüllten Anforderungen nach der Basisabsicherung dar. Um die Basisabsicherung umzusetzen, reicht die Erfüllung der Basisanforderungen. Um die Aussagekraft des Prozentwertes zu unterstützen, wird auch eine für Menschen leicht verständliche Darstellung gewählt.
- Bereich 2 stellt den kumulierten Umsetzungsgrad der erfüllten Anforderungen nach der Standardabsicherung dar. Um die Standardabsicherung umzusetzen, sind Basis- und Standardanforderungen zu erfüllen. Um die Aussagekraft des Prozentwertes zu unterstützen, wird auch eine für Menschen leicht verständliche Darstellung gewählt.
- Bereich 3 stellt den kumulierten Umsetzungsgrad der erfüllten Anforderungen nach der Kernabsicherung dar. Um die Kernabsicherung umzusetzen, sind alle drei Arten von Anforderungen zu erfüllen. Um die Aussagekraft des Prozentwertes zu unterstützen, wird auch eine für Menschen leicht verständliche Darstellung gewählt.

Ausgehend von der Annahme, dass die Migration nach der Standardabsicherung erfolgt, ist ein Durchschnitt der Prozentwerte der einzelnen Bausteine einer Gruppe gebildet worden.

Diese repräsentieren die bereits umgesetzten Anforderungen. Auf der Transformation-Roadmap befinden sich die Inverse dieser Zahlen, die den noch zu betreibenden Aufwand bedeuten (Beispiel: Bausteingruppe ISMS: Durchschnitt in der Tabelle 60 %, Roadmap 40 %). Anhand des berechneten Durchschnitts kann eine Priorisierung vorgenommen werden, welche Bausteine zunächst abgesichert werden sollen.

Beispiel: 92 %, 12 aus 13 ist ok, gelb

Die gelbe Markierung steht für die Standardabsicherung. Ist diese Absicherungsart gewählt, so sind die Basis- und Standardanforderungen umzusetzen. Daher wird die Summe der erfüllten Anforderungen (Basis und Standard) den Anforderungen, die nicht oder nur teilweise erfüllt sind (Basis und Standard), gegenübergestellt. In diesem Fall errechnet sich die Prozentzahl 92 %; dies bedeutet, dass aus den insgesamt 13 Basis- und Standardanforderungen 12 durch Maßnahmen aus dem veralteten IT-Grundschutz abgedeckt sind. Bei den verbleibenden 8 % (ein Baustein) müssen Maßnahmen definiert und umgesetzt werden, die diese Anforderung erfüllen, um mit dem modernisierten IT-Grundschutz kompatibel zu sein.

kumulierter Umsetzungsgrad			kumulierter Umsetzungsgrad			kumulierter Umsetzungsgrad		
Gesamt	Anzahl der Anford		Gesamt	Anzahl der Anford		Gesamt	Anzahl der Anford	
56%	5 aus 9 ist ok		60%	9 aus 15 ist ok		65%	11 aus 17 ist ok	
			60%	Durchschnitt				
100%	5 aus 5 ist ok		92%	12 aus 13 ist ok		93%	13 aus 14 ist ok	
40%	2 aus 5 ist ok		40%	4 aus 10 ist ok		54%	7 aus 13 ist ok	
33%	1 aus 3 ist ok	4	63%	5 aus 8 ist ok	5	56%	5 aus 9 ist ok	6
67%	6 aus 9 ist ok		74%	14 aus 19 ist ok		76%	16 aus 21 ist ok	
67%	2 aus 3 ist ok		75%	6 aus 8 ist ok		64%	7 aus 11 ist ok	
			69%	Durchschnitt				
50%	1 aus 2 ist ok		50%	3 aus 6 ist ok		61%	11 aus 18 ist ok	
0%	0 aus 1 ist ok		0%	0 aus 1 ist ok		0%	0 aus 1 ist ok	
100%	5 aus 5 ist ok		83%	10 aus 12 ist ok		77%	10 aus 13 ist ok	
67%	2 aus 3 ist ok		44%	4 aus 9 ist ok		33%	4 aus 12 ist ok	
20%	1 aus 5 ist ok		50%	5 aus 10 ist ok		54%	7 aus 13 ist ok	
50%	1 aus 2 ist ok		50%	4 aus 8 ist ok		55%	6 aus 11 ist ok	
0%	0 aus 12 ist ok		0%	0 aus 14 ist ok		0%	0 aus 18 ist ok	

Abbildung 37: Generische Aufwandsanalyse (Ausschnitt), eigene Darstellung

Nach Feedback und Rücksprache mit dem Betreuer dieser Arbeit seitens Capgemini ist Alternative 3 zur managementgerechten Transformation-Roadmap deklariert worden. Diese

findet später in der Beratung der Kunden bei der Migration vom klassischen IT-Grundschutz auf den modernisierten IT-Grundschutz Anwendung.

Zusätzlich zur generischen Aufwandsanalyse ist die Auflistung der nichterfüllten bzw. nur teilweise erfüllten Anforderungen für eine erfolgreiche Beratung essenziell. Die Tabelle bietet einen Überblick über die Bausteine, die Probleme aufzeigen, und eine Liste der Anforderungen aller drei Kategorien, die nicht erfüllt oder nur teilweise erfüllt sind. Anwender der Liste erkennen auf einen Blick die konkreten Anforderungen, für die noch Maßnahmen definiert werden müssen.

Nicht umgesetzte/nicht vollständig umgesetzte Anforderungen

Bausteinliste		Anforderungsliste nach Absicherungstyp		Bewertung
Prozess-Bausteine				
ISMS:Sicherheitsmanagement				
ISMS.1	Sicherheitsmanagement	**Basis**	Festlegung der Sicherheitsziele und -strategie	2
			Vertragsgestaltung bei Bestellung eines externen Informationssicherheitsbeauftragten	3
			Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit	3
			Integration der Mitarbeiter in den Sicherheitsprozess	3
		Standard	Erstellung eines Sicherheitskonzepts	3
			Management-Berichte zur Informationssicherheit	3
ORP: Organisation und Personal				
ORP.1	Organisation	**Standard**	Geräteverwaltung	3
ORP.2	Personal	**Basis**	Geregelte Einarbeitung neuer Mitarbeiter	2
			Geregelte Verfahrensweise beim Weggang von Mitarbeitern	3
			Regelungen für den Einsatz von Fremdpersonal	3
		Standard	Überprüfung der Vertrauenswürdigkeit von Mitarbeitern	3
			Aufgaben und Zuständigkeiten von Mitarbeitern	3
			Schulung von Mitarbeitern	3
ORP.3	Sensibilisierung und Schulung	**Basis**	Ansprechpartner zu Sicherheitsfragen	2
			Einweisung des Personals in den sicheren Umgang mit IT	3
		Standard	Planung und Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit	3
		erhöhter Schutzbedarf	Spezielle Schulung von exponierten Personen und Institutionen	3
ORP.4	Identitäts- und Berechtigungsmanagement	**Basis**	Vergabe von Zutrittsberechtigungen	3

Abbildung 38: Liste nichterfüllter Anforderungen (Ausschnitt), eigene Darstellung

5. Fazit

Ziel dieser Arbeit war eine Migrationsstrategie für den modernisierten IT-Grundschutz zu bestimmen.

Um dies zu tun, musste zunächst eine Analyse des klassischen und des modernisierten IT-Grundschutzes durchgeführt werden, um die Unterschiede herauszuarbeiten. Der Vergleich erfolgte anhand der Darstellung der Bestandteile des aktuellen IT-Grundschutzes. Insbesondere wurde dabei auf Abweichungen zwischen den beiden Editionen eingegangen. Eine Neueinführung des IT-Grundschutzes in eine Institution ist jederzeit möglich. Doch die Institutionen, die bereits ein Managementsystem für die Informationssicherheit nach dem klassischen IT-Grundschutz etabliert haben, sollen bei der Überführung in den aktuellen IT-Grundschutz Unterstützung erhalten.

Einer der wesentlichen Kernpunkte stellt die Einführung der Wahl der Vorgehensweise, wie Zielobjekte abgesichert werden sollen, dar.

Die Darstellung der Migration und deren Aufwand endete in der Entwicklung einer Transformation-Roadmap. Sie soll Anwendern eine Übersicht über den Kernpunkt der Modernisierung verschaffen und den Weg vom klassischen IT-Grundschutz zum modernisierten aufzeigen. Die größte Veränderung ist die neue IT-Grundschutz-Methodik, die drei Vorgehensweisen zur Erstellung einer Sicherheitskonzeption definiert. Die Basisabsicherung eignet sich für Einsteiger und bietet eine grundlegende und schnelle Erstabsicherung relevanter Assets. Hingegen konzentriert sich die Kernabsicherung auf geschäftskritischen Objekten (sogenannte Kronjuwelen) einer Institution. Da dessen Verlust für Organisationen existenzbedrohlich ist, sollten die wichtigsten Assets mit tiefgreifenden Sicherheitsmaßnahmen geschützt werden. Eine organisationsumfassende und angemessene Absicherung, der für die Informationssicherheit relevanten Objekte ist durch die Standardabsicherung sichergestellt. Diese Absicherung entspricht in Grundzügen der Vorgehensweise aus dem klassischen IT-Grundschutz. Diese Absicherungsmethodik soll das Ziel jeder Organisation sein.

Die Roadmap zeigt die wesentlichen Schritte bei der Sicherheitskonzeption nach der Standardabsicherung. Dabei kann mit Hilfe der Migrationstabellen, ein Zusammenhang zwischen bestehenden Sicherheitsmaßnahmen und Anforderungen nach dem neuen IT-Grundschutz modelliert werden. Durch eine generische Aufwandsanalyse ließ sich die Anzahl der Anforderungen pro Baustein herausarbeiten, die Auskunft über den zu betreibenden Aufwand lieferte.

In der heutigen Zeit ist das Leben ohne IT-Systeme und Informationsaustausch unvorstellbar. Doch sie sind durch unzählige Gefährdungen bedroht. Die Auswirkungen eines mangelhaften Schutzes oder eines ignorierenden Verhaltens können teuer werden. Daher ist die Informationssicherheit ist Pflicht jeder Organisation. Der IT-Grundschutz ist ein effektives und kostenfreies Instrument und die darin formulierten Anforderungen sind angemessen; dies berücksichtigt Institutionen, die zuvor aufgrund Ressourcenmangels keine Maßnahmen im Rahmen der Informationssicherheit umgesetzt haben.

Ein effektiver Schutz nach Stand der Technik ist nur durch den modernen IT-Grundschutz gewährleistet. Daher ist die Migration auf den neuen IT-Grundschutz für Organisationen mit einem funktionierenden ISMS unerlässlich.

Literaturverzeichnis

[1] Statista, „Umfrage zu organisatorischen IT-Sicherheitsmaßnahmen in Unternehmen“, 2018, zuletzt zugegriffen: 05/05/2020. Quelle: https://de.statista.com/statistik/daten/studie/444794/umfrage/umfrage-zu-technischen-it-sicherheitsmassnahmen-in-unternehmen/.

[2] BSI, „Ein Vierteljahrhundert Informationssicherheit: IT-Grundschutz mit Methode“, 2019, zuletzt zugegriffen:18/03/2020. Quelle: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/25-Jahre-IT-Grundschutz_07102019.html.

[3] BSI, „Der neue IT-Grundschutz: Modernisierung erfolgreich abgeschlossen“, 2017, zuletzt zugegriffen: 25/03/2020. Quelle: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/IT-Grundschutz_Modernisierung_11102017.html.

[4] Inge Haschke, Informationssicherheit und Datenschutz systematisch und nachhaltig gestalten, 2020, zuletzt zugegriffen: 01/06/2020. Quelle: https://link.springer.com/content/pdf/10.1007%2F978-3-658-28699-6_1.pdf.

[5] BRANDMAUER IT Security Blog, „Was ist der Unterschied zwischen IT Sicherheit und Informationssicherheit?“, 2018, zuletzt zugegriffen: 04/04/2020. Quelle: https://www.brandmauer.de/blog/it-security/unterschied-it-sicherheit-und-informationssicherheit.

[6] Datenschutzexperte.de, „Was bedeutet Informationssicherheit?“, 2019, zuletzt zugegriffen: 04/04/2020. Quelle: https://www.datenschutzexperte.de/blog/datenschutz-im-alltag/informationssicherheit/.

[7] Tobias Lehner, „Sicherheit mobiler Systeme – Grundlagen der Informationssicherheit“, 2020, zuletzt zugegriffen: 27/03/2020. Quelle: https://moodle.haw-landshut.de/pluginfile.php/213445/mod_resource/content/1/Grundlagen%20der%20Informationsssicherheit.pdf.

[8] BSI, „Cyber-Sicherheit“, 2020, zuletzt zugegriffen: 04/04/2020. Quelle: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html.

[9] Tüv Süd, „ISO/IEC 27001 - ISMS-ZERTIFIZIERUNG“, 2020, zuletzt zugegriffen: 29/03/2020. Quelle: https://www.tuvsud.com/de-de/dienstleistungen/auditierung-und-zertifizierung/cyber-security-zertifizierung/iso-27001.

[10] Wikipedia, „Common Criteria for Information Technology Security Evaluation“, 2019, zuletzt zugegriffen: 30/05/2020. Quelle: https://de.wikipedia.org/wiki/Common_Criteria_for_Information_Technology_Security_Evaluation.

[11] BSI, „ISO 27001 Zertifizierung auf Basis von IT-Grundschutz“, 2020, zuletzt zugegriffen: 15/05/2020. Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzZertifikat/itgrundschutzzertifikat_node.html.

[12] Daniel Heid, Sicherheit in Organisationen: Analysebegriffe und Konzeptionsmethoden, 2008, zuletzt zugegriffen: 15/06/2020. Quelle: https://books.google.de/books?id=5jdoCwAAQBAJ.

[13] G. Wolf, A. Pfitzmann, „Charakteristika von Schutzzielen und Konsequenzen für Benutzungsschnittstellen“, 2000, zuletzt zugegriffen: 20/04/2020. Quelle: https://link.springer.com/content/pdf/10.1007/s002870000101.pdf.

[14] Stefan Beck, Aktualisierung der ISO/IEC 27001 (ISMS) Entstehung, Änderungsbedarf und Handlungsempfehlungen für Unternehmen, 2015, S. 34, zuletzt zugegriffen: 18/06/2020. Quelle: https://books.google.de/books?id=D0YXCgAAQBAJ.

[15] H. Kersten, G. Klett, J. Reuter, K. Schröder, IT-Sicherheitsmanagement nach der neuen ISO 27001, 2019, S. 5, zuletzt zugegriffen: 04/06/2020. Quelle: https://link.springer.com/content/pdf/10.1007%2F978-3-658-27692-8.pdf.

[16] Stefan Beck, Aktualisierung der ISO/IEC 27001 (ISMS) Entstehung, Änderungsbedarf und Handlungsempfehlungen für Unternehmen, 2015, S. 35, zuletzt zugegriffen: 18/06/2020. Quelle: https://books.google.de/books?id=D0YXCgAAQBAJ.

[17] BSI, „Organisationsübersicht des BSI“, 2020, zuletzt zugegriffen: 05/05/2020. Quelle: https://www.bsi.bund.de/DE/DasBSI/Aufgaben/aufgaben_node.html.

[18] Security Insider, „Was ist das BSI?“, 2017, zuletzt zugegriffen: 12/03/2020. Quelle: https://www.security-insider.de/was-ist-das-bsi-a-632838/.

[19] BSI, „Zertifizierung und Anerkennung“, 2020, zuletzt zugegriffen: 07/04/2020. Quelle: https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/zertifizierungnachcc_node.html.

[20] BSI, „IT-Grundschutz“, 2020, zuletzt zugegriffen: 01/03/2020. Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzAbout/itgrundschutzAbout_node.html.

[21] BSI, BSI-Standard 200-1: Managementsysteme für die Informationssicherheit, 2020, zuletzt zugegriffen: 01/07/2020. Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_1.pdf?__blob=publicationFile&v=8.

[22] BSI, BSI-Standard 100-1: Managementsysteme für die Informationssicherheit, 2008, zuletzt zugegriffen: 01/07/2020. Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1001.pdf?__blob=publicationFile&v=2.

[23] BSI, BSI-Standard 200-2: IT-Grundschutz-Methodik, 2020, zuletzt zugegriffen: 01/07/2020. Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_2.pdf?__blob=publicationFile&v=7.

[24] BSI, BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, 2008, zuletzt zugegriffen: 01/07/2020. Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1002.pdf?__blob=publicationFile.

[25] BSI, Leitfaden zur Basis-Absicherung nach IT-Grundschutz, 2017, zuletzt zugegriffen: 16/03/2020. Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.pdf?__blob=publicationFile&v=3.

[26] Holger Schildt, BSI, Vorgehensweisen des neuen IT-Grundschutzes, 2016, zuletzt zugegriffen: 16/03/2020. Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Grundschutz/1GS_Tag_2016/02_Schildt_Vorgehensweise.pdf?__blob=publicationFile&v=1.

[27] BSI, „Testat nach der Basis-Absicherung“, 2019, zuletzt zugegriffen: 27/04/2020. Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzAbout/Testat_Basisabsicherung/Testat_Basisabsicherung_node.html).

[28] BSI, „Lerneinheit 2.9: Wahl der Vorgehensweise“, 2020, zuletzt zugegriffen: 27/03/2020. Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/OnlinekursITGrundschutz2018/Lektion_2_Sicherheitsmanagement/Lektion_2_09/Lektion_2_09_node.html.

[29] BSI, „Lektion 3: Strukturanalyse“, 2020, zuletzt zugegriffen:25/05/2020. Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/OnlinekursITGrundschutz2018/Lektion_3_Strukturanalyse/Lektion_3_node.html.

[30] BSI, „Lerneinheit 3.2: Objekte gruppieren“, 2020, zuletzt zugegriffen: 25/05/2020. Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/OnlinekursITGrundschutz2018/Lektion_3_Strukturanalyse/Lektion_3_02/Lektion_3_02_node.html.

[31] BSI, „Lerneinheit 3.5: Netzplan erheben“, 2020, zuletzt zugegriffen: 25/05/2020. Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/OnlinekursITGrundschutz2018/Lektion_3_Strukturanalyse/Lektion_3_05/Lektion_3_05_node.html.

[32] BSI, „Lerneinheit 3.6: IT-Systeme erheben“, 2020, zuletzt zugegriffen: 25/05/2020. Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/OnlinekursITGrundschutz2018/Lektion_3_Strukturanalyse/Lektion_3_06/Lektion_3_06_node.html.

[33] BSI, „Lerneinheit 3.7: Räume erheben“, 2020, zuletzt zugegriffen: 25/05/2020. Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/OnlinekursITGrundschutz2018/Lektion_3_Strukturanalyse/Lektion_3_07/Lektion_3_07_node.html.

[34] BSI, „Lektion 4: Schutzbedarfsfeststellung“, 2020, zuletzt zugegriffen: 25/05/2020. Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/OnlinekursITGrundschutz2018/Lektion_4_Schutzbedarfsfeststellung/Lektion_4_node.html.

[35] BSI, „Lerneinheit 4.1: Grundlegende Definitionen“, 2020, zuletzt zugegriffen:25/05/2020. Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/OnlinekursITGrundschutz2018/Lektion_4_Schutzbedarfsfeststellung/Lektion_4_01/Lektion_4_01_node.html.

[36] BSI, „Lerneinheit 4.2: Schutzbedarfskategorien“, 2020, zuletzt zugegriffen: 25/05/2020. Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/OnlinekursITGrundschutz2018/Lektion_4_Schutzbedarfsfeststellung/Lektion_4_02/Lektion_4_02_node.html.

[37] BSI, „Lerneinheit 4.3: Vorgehen und Vererbung“, 2020, zuletzt zugegriffen: 25/05/2020. Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/OnlinekursITGrundschutz2018/Lektion_4_Schutzbedarfsfeststellung/Lektion_4_03/Lektion_4_03_node.html.

[38] BSI, „Lektion 5: Modellierung“, 2020, zuletzt zugegriffen: 25/05/2020. Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/OnlinekursITGrundschutz2018/Lektion_5_Modellierung/Lektion_5_node.html.

[39] BSI, „Lerneinheit 5.3: Vorgehen“, 2020, zuletzt zugegriffen: 25/05/2020. Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/OnlinekursITGrundschutz2018/Lektion_5_Modellierung/Lektion_5_03/Lektion_5_03_node.html.

[40] BSI, „Lektion 6: IT-Grundschutz-Check“, 2020, zuletzt zugegriffen: 25/05/2020. Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/OnlinekursITGrundschutz2018/Lektion_6_IT-Grundschutz-Check/Lektion_6_node.html.

[41] BSI, „Lerneinheit 6.2: Vorbereitung und Durchführung“, 2020, zuletzt zugegriffen: 25/05/2020. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/OnlinekursITGrundschutz2018/Lektion_6_IT-Grundschutz-Check/Lektion_6_02/Lektion_6_02_node.html.

[42] BSI, „Lektion 7: Risikoanalyse“, 2020, zuletzt zugegriffen: 25.05.2020. Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/OnlinekursITGrundschutz2018/Lektion_7_Risikoanalyse/Lektion_7_node.html.

[43] BSI, „Lektion 8: Umsetzungsplanung“, 2020, zuletzt zugegriffen: 25/05/2020. Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/OnlinekursITGrundschutz2018/Lektion_8_Umsetzungsplanung/Lektion_8_node.html.

[44] BSI, „ISO 27001 Zertifizierung auf Basis von IT-Grundschutz“, 2020, zuletzt zugegriffen: 18/03/2020. Quelle: https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Managementsystemzertifizierung/Zertifizierung27001/GS_Zertifizierung_node.html.

[45] Heise, „Generalüberholung“, 2017, zuletzt zugegriffen: 07.06.2020. Quelle: https://www.heise.de/select/ix/2017/12/1512149671074410.

[46] BSI, BSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz, 2017, zuletzt zugegriffen: 26/06/2020. Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_3.pdf?__blob=publicationFile&v=7.

[47] BSI, BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz, 2008, zuletzt zugegriffen: 26/06/2020. Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1003.pdf?__blob=publicationFile&v=2.

[48] BSI, Ergänzung zum BSI-Standard 100-3 Version 2.5, 2011, zuletzt zugegriffen: 05/04/2020. Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1003_ergaenzung.pdf?__blob=publicationFile&v=1.

[49] BSI, BSI-Standard 100-4: Notfallmanagement, 2008, zuletzt zugegriffen: 01/03/2020. Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/IT-Grundschutzstandards/BSI-Standard_1004.pdf?__blob=publicationFile&v=2.

[50] BSI, Pressemitteilung „Aktueller Informationsstand zur Weiterentwicklung des BSI-Standards 200-4“, 2019, zuletzt zugegriffen: 01/07/2020. Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BCM/BCM_20190416_Infomail.pdf?__blob=publicationFile&v=2.

[51] BSI, IT-Grundschutz-Kataloge – 15. Ergänzungslieferung, 2016, zuletzt zugegriffen: 04/07/2020. Quelle: https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf.

[52] BSI, IT-Grundschutz-Kompendium, 2020, zuletzt zugegriffen: 04/07/2020. Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.pdf?__blob=publicationFile&v=6.

[53] BSI, Erstellung von Bausteinen: Veröffentlichungsworkflow, 2020, zuletzt zugegriffen: 25/06/2020. Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/GS_Drafts/Workflow/wf_drafts_node.html.

[54] Heise, „IT-Grundschutz: BSI schließt Modernisierung ab“, 2017, zuletzt zugegriffen: 15/06/2020. Quelle: https://www.heise.de/security/meldung/IT-Grundschutz-BSI-schliesst-Modernisierung-ab-3859945.html.

[55] Fokus Datenschutz, Modernisierung des IT-Grundschutzes abgeschlossen, 2017, zuletzt zugegriffen: 15/06/2020. Quelle: https://www.fokus-datenschutz.de/modernisierung-des-it-grundschutzes-abgeschlossen.

[56] BSI, Umsetzungshinweise, 2017, zuletzt zugegriffen:04/03/2020. Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/umsetzungshinweise_node.html.

[57] BSI, Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz Version 2.1, 2019, zuletzt zugegriffen: 07/06/2020. Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/ISO27001/Zertifizierungsschema.pdf?__blob=publicationFile&v=6.

[58] V. Reichenbach, R. Trautloft, Praxishandbuch IT-Projekte in Versicherungsunternehmen, S, 85, 2011, zuletzt zugegriffen: 04/07/2020. Quelle: https://books.google.de/books?id=lH8nB2kTJHcC.

[59] BSI, Anleitung zur Migration von Sicherheitskonzepten, 2018, zuletzt zugegriffen:02/07/2020. Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Anleitung_zur_Migration.pdf?__blob=publicationFile&v=10.

[60] Manymize, DIGITAL TRANSFORMATION ROADMAP: DER WEG ZUM DIGITALEN UNTERNEHMEN (INSIGHT), zuletzt zugegriffen: 27/06/2020. Quelle: https://www.manymize.com/digital-transformation-roadmap.

[61] Refa, PDCA-Zyklus, zuletzt zugegriffen: 27/06/2020. Quelle: https://refa.de/service/refa-lexikon/pdca-zyklus.

Abbildungsverzeichnis

Abbildung 1: Zusammenhang zwischen Sicherheitsbegriffen, eigene Darstellung 5
Abbildung 2: Wechselwirkung zwischen Schutzzielen, eigene Darstellung in Anlehnung an [13] 7
Abbildung 3: Der moderne IT-Grundschutz [21] 12
Abbildung 4: Der Sicherheitsprozess gemäß BSI-Standard 200-1 [21] 16
Abbildung 5: Der moderne IT-Grundschutz [21] 19
Abbildung 6: Initiierung, Organisation und Durchführung des Sicherheitsprozesses [25] 20
Abbildung 7: Der Informationssicherheitsprozess gemäß BSI-Standard 200-2 [23] 23
Abbildung 8: Basisabsicherung nach BSI-Standard 200-2, eigene Darstellung in Anlehnung an [26] 27
Abbildung 9: Vorgehensweise bei der Basisabsicherung [23] 29
Abbildung 10: Kernabsicherung nach BSI-Standard 200-2, eigene Darstellung in Anlehnung an [26] 33
Abbildung 11: Vorgehensweise nach der Kernabsicherung [23] 35
Abbildung 12: Beispiel für einen Netzplan [23] 38
Abbildung 13: Standardabsicherung nach BSI-Standard 200-2, eigene Darstellung nach [23] 45
Abbildung 14: Vorgehensweise nach der Standardabsicherung [23] 46
Abbildung 15: Der moderne IT-Grundschutz [21] 50
Abbildung 16: Ablauf der Sicherheitskonzeption nach der Standardabsicherung [23] 52
Abbildung 17: Ausschnitt aus der Tabelle der elementaren Gefährdungen, BSI-Standard 200-3 [46] 54
Abbildung 18: Beispiel für die Ermittlung elementarer Gefährdungen [46] 55
Abbildung 19: Beispiel für eine Gefährdungsübersicht [46] 55
Abbildung 20: Risikomatrix zur Beurteilung von Risiken, eigene Darstellung 57
Abbildung 21: Ablauf der Sicherheitskonzeption nach der Standardabsicherung [23] 58
Abbildung 22: Der moderne IT-Grundschutz [21] 60
Abbildung 23: Der Notfallmanagementprozess nach BSI-Standard 100-4 [49] 60
Abbildung 24: Der moderne IT-Grundschutz [21] 62
Abbildung 25: Veröffentlichungsworkflow des IT-Grundschutz-Kompendiums [53] 65
Abbildung 26: Das Schichtenmodell des modernisierten IT-Grundschutzes [52] 68
Abbildung 27: Überblick über den Aufbau eines Bausteins aus dem IT-Grundschutz-Kompendium, eigene Darstellung 69
Abbildung 28: Kreuzreferenztabelle zu elementaren Gefährdungen [52] 72
Abbildung 29: Absicherungsstrategien gemäß BSI-Standard 200-2 ohne zuvor angewendeten IT-Grundschutz, eigene Darstellung 73
Abbildung 30: Nachweis der Umsetzung für gewählte Absicherungsvorgehensweise [27] 76
Abbildung 31: Aufbau einer Migrationstabelle, eigene Darstellung auf Basis einer Migrationstabelle [59] 79
Abbildung 32: Vorschlag für die Transformation-Roadmap (Alternative 1), eigene Darstellung 84
Abbildung 33: Vorschlag für die Transformation-Roadmap (Alternative 2), eigene Darstellung 86
Abbildung 34: Vorschlag für die Transformation-Roadmap I (Alternative 3), eigene Darstellung 87
Abbildung 35: Vorschlag für die Transformation-Roadmap II (Alternative 3), eigene Darstellung 87
Abbildung 36: Generische Aufwandsanalyse (Ausschnitt), eigene Darstellung 90
Abbildung 37: Generische Aufwandsanalyse (Ausschnitt), eigene Darstellung 91
Abbildung 38: Liste nichterfüllter Anforderungen (Ausschnitt), eigene Darstellung 92

Abkürzungsverzeichnis

APP	Anwendungen
BCMS	Business Continuity Management System
BSI	Bundesamt für Sicherheit in der Informationstechnik
COBIT	Control Objectives for Information and Related Technology
CON	Konzepte und Vorgehensweisen
DER	Detektion und Reaktion
ICS	Industrial Control System
IEC	International Electrotechnical Commission
IKT	Informations- und Kommunikationstechnik
IND	Industrielle IT
INF	Infrastruktur
IoT	Internet of Things
IS	Informationssicherheit
ISB	Informationssicherheitsbeauftragte
ISF	Information Security Forum
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
IT	Informationstechnik
ITIL	IT Infrastructure Library
KMU	kleine und mittlere Unternehmen
NET	Netze und Kommunikation

NIST	National Institute of Standards and Technology
OPS	Betrieb
ORP	Organisation und Personal
PCDA	Plan-Do-Check-Act
PCI DSS	Payment Card Industry Data Security Standard
SYS	IT-Systeme

Glossar

Anforderung	Forderung, um ein bestimmtes Ziel zu erfüllen.
Asset	Vermögenswert eines Unternehmens.
Audit	Durchführung einer Untersuchung, um die Erfüllung von definierten Anforderungen zu überprüfen.
Basisabsicherung	Grundlegende Erstabsicherung der Zielobjekte im Rahmen des modernisierten IT-Grundschutzes.
BSI-Standard	BSI-Standards sind elementare Bestandteile des IT-Grundschutzes. Die von BSI entwickelten Standards enthalten Empfehlungen zu verschiedenen Aspekten der Informationssicherheit.
Cloud Computing	Bereitstellung von IT-Infrastruktur und IT-Leistungen über das Internet.
Cyber Security	Gesamtheit der Maßnahmen, die Sicherheit im Cyber-Raum als Ziel haben.
Datenschutz	Datenschutz bezieht sich auf den Schutz der personenbezogenen Daten.
Deming Kreis	Ein von William Edwards Deming entwickeltes Modell, das die andauernde Verbesserung symbolisiert. [61]
Gefährdung	Potenzielle Gefahr auf ein Objekt, die Schaden verursachen kann.
Geltungsbereich	s. Informationsverbund
Governance	Steuerung bestimmter Strukturen innerhalb einer Organisation.

Grundwert	s. Schutzziel
Informationssicherheits-managementsystem	Ein ISMS umfasst die Planung, Steuerung und Kontrolle des Prozesses, der die Informationssicherheit in einer Institution betriebt.
Informationssicherheit	Die Gesamtheit der Maßnahmen, die den Schutz von soziotechnischen und nicht-soziotechnischen Systemen gewährleistet.
Informationsverbund	Die Gesamtheit ausgewählter Objekte, die abgesichert werden sollen.
IT-Grundschutz	Von BSI entwickelte Methode, um das Sicherheitsniveau von Institutionen zu erhöhen und ihre Assets zu schützen.
IT-Grundschutz-Baustein	Bündel von Anforderungen aus dem IT-Grundschutz-Kompendium.
IT-Grundschutz-Check	Eine Phase aus dem IT-Grundschutz; prüft, ob die umgesetzten Maßnahmen die definierten Anforderungen erfüllen.
IT-Grundschutz-Kataloge	Vorgänger des IT-Grundschutz-Kompendiums.
IT-Grundschutz-Kompendium	Bestandteil des modernisierten IT-Grundschutzes; enthält Gefährdungen und Anforderungen in Bausteine organisiert.
IT-Grundschutz-Modellierung	Abbildung eines Informationsverbundes mit Hilfe der Bausteine aus dem IT-Grundschutz-Kompendium.
IT-Sicherheit	Teilgebiet der Informationssicherheit; Schutz von Informationen, die durch IT-Systeme verarbeitet werden.
IT-System	Technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden.
Kernabsicherung	Tiefgreifende Absicherung der geschäftskritischen Assets im Rahmen des modernisierten IT-Grundschutzes.

Kronjuwelen	Hier: Kritische Assets einer Organisation.
Leitlinie zur Informationssicherheit	Ein Dokument, das Kernaussagen zum Umgang der Informationssicherheit in einer Organisation definiert.
Maßnahme	Konkrete Handlungsanweisung.
Migration	IT: Ein Umstellungsprozess, der von einem System auf ein anderes System Ressourcen transferiert.
Migrationstabelle	Von BSI entwickelten Tabellen, um die Migration auf den modernisierten IT-Grundschutz zu erleichtern. Die Tabellen definieren einen inhaltlichen Zusammenhang zwischen Sicherheitsmaßnahmen und -anforderungen.
Netzplan	Ein Netzplan bietet eine grafische Übersicht über die Komponenten eines Netzes und ihre Schnittstellen.
Notfallmanagement	Steuerung der Maßnahmen, die der Aufrechterhaltung der Kontinuität des Geschäftsbetriebs dienen.
Risikoanalyse	Identifikation von Risiken, die ein Objekt gefährden.
Schutzbedarf	Eigenschaft von Objekten; bezeichnet die benötigte Sicherheit eines Untersuchungsgegenstandes. Die Bewertung erfolgt anhand der Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit).
Schutzbedarfsfeststellung	Analyse des Schutzbedarfes von Objekten, mit dem Ziel sie einer Schutzbedarfskategorie zuzuordnen.
Schutzziel	Definition über das Schutzniveau eines Objekts. In der Informationssicherheit existieren drei Hauptziele: Vertraulichkeit, Integrität, Verfügbarkeit.
Standardabsicherung	Angemessenes und umfassendes Sicherheitsniveau der Assets im Rahmen des modernisierten IT-Grundschutzes.

Strukturanalyse	Bündel von Analysen und Dokumentationen am zugrundeliegenden Informationsverbund im Rahmen der IT-Grundschutz-Methodik.
Testat	Nachweis für die Erfüllung der Anforderungen der Basisabsicherung.
Transformation Roadmap	Visuelle, managementgerechte Darstellung über eine Veränderung mit Start- und Endpunkten.
Zertifizierung	Ausstellen eines Zertifikats für die Erfüllung definierter Anforderungen an ein Produkt, ein System, einen Prozess oder an Personen.

Anhang

- Generische Aufwandsanalyse und Prioritätsermittlung bei der Umsetzung von Bausteinen (Aufwandsanalyse.xlsx)
- Nicht umgesetzte/nicht vollständig umgesetzte Anforderungen (Aufwandsanalyse.xlsx)
- Transformation-Roadmap (TransformationRoadmap.pptx)