Bundesamt
für Sicherheit in der
Informationstechnik

Anleitung zur Migration von Sicherheitskonzepten

Hilfsmittel zum modernisierten IT-Grundschutz

Änderungshistorie

Version	Datum	Verfasser	Beschreibung
1.0	01.03.18	BSI	1. veröffentlichte Version
1.1	02.10.18	BSI	Sprachliche Anpassungen

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-5369
E-Mail: grundschutz@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung

Seit seiner Einführung im Jahr 1994 wird der IT-Grundschutz des BSI permanent weiterentwickelt. Er gilt als Referenzwerk für Informationssicherheit in Deutschland. 2005 wurde der IT-Grundschutz grundlegend überarbeitet, um ihn an die Bedürfnisse der Anwender und insbesondere auch an die internationale Entwicklung anzupassen. Dabei wurde unter anderem das damalige IT-Grundschutzhandbuch in die BSI-Standards 100-1, 100-2 und 100-3 sowie die IT-Grundschutz-Kataloge aufgeteilt. Letztere wurden seitdem ständig um neue Kapitel und Empfehlungen ergänzt, um mit den vielfältigen und vor allem schnelllebigen Entwicklungen im Bereich der Informationstechnik Schritt halten zu können.

2017 wurde der IT-Grundschutz erneut einer grundlegenden Revision unterzogen. Im Rahmen der Modernisierung des IT-Grundschutzes wurde die bisherige IT-Grundschutz-Vorgehensweise, die nun Standard-Absicherung heißt, um zwei zusätzliche Herangehensweisen erweitert: die Basis- und die Kern-Absicherung. Im Zuge der Modernisierung wurden die BSI-Standards 100-1, 100-2 und 100-3 durch die BSI-Standards 200-1, 200-2 und 200-3 ersetzt. Außerdem wurden die IT-Grundschutz-Bausteine deutlich verschlankt und neu strukturiert. Die IT-Grundschutz-Kataloge wurden hierbei durch das IT-Grundschutz-Kompendium abgelöst. Nähere Informationen und alle aktuellen Veröffentlichungen finden sich unter [GSM].

Die Umstellung auf den modernisierten IT-Grundschutz nach den BSI-Standards 200-1, 200-2 und 200-3 hat auch Auswirkungen auf ein vorhandenes Managementsystem für Informationssicherheit (ISMS), das nach der bisherigen IT-Grundschutz-Methode gemäß den BSI-Standards 100-1, 100-2 und 100-3 sowie den IT-Grundschutz-Katalogen aufgebaut ist. Mit der vorliegenden Anleitung zur Migration unterstützt das BSI die Anwender des IT-Grundschutzes bei der Umstellung vom klassischen auf den modernisierten IT-Grundschutz und ermöglicht somit einen reibungslosen Übergang.

1.1 Adressatenkreis

Diese Anleitung richtet sich ausschließlich an Institutionen, die bereits ein IT-Grundschutz-konformes ISMS nach den BSI-Standards 100-1, 100-2 und 100-3 betreiben und die jetzt eine Umstellung auf den modernisierten IT-Grundschutz nach den BSI-Standards 200-1, 200-2 und 200-3 anstreben. Institutionen, die erst jetzt mit dem Aufbau eines Managementsystems für Informationssicherheit gemäß IT-Grundschutz beginnen, wird direkt der BSI-Standard 200-2 empfohlen.

1.2 Anwendungshinweise

Das vorliegende Dokument beschreibt, wie eine auf dem BSI-Standard 100-2 basierende Sicherheitskonzeption auf den neuen BSI-Standard 200-2 migriert werden kann. Damit ist es zugleich eine Anleitung für den Umstieg von den IT-Grundschutz-Katalogen auf das IT-Grundschutz-Kompendium. Dieses Dokument baut darauf auf, dass die Standard-Absicherung als Vorgehensweise, auf die migriert werden soll, ausgewählt wurde. Institutionen, die ihren Geltungsbereich einschränken und für ihr bisheriges ISMS eine Kern-Absicherung durchführen wollen, können die Anleitung entsprechend adaptieren. Ein Umstieg von der IT-Grundschutz-Vorgehensweise nach 100-2 auf eine Basis-Absicherung wird nicht empfohlen.

Ebenso wie der IT-Grundschutz aktualisiert und modernisiert wurde, haben sich auch andere Rahmenbedingungen geändert, so dass neben der Adaption des modernisierten IT-Grundschutzes auch inhaltliche Änderungen an Sicherheitskonzepten erforderlich sein können.Die Anleitung zur Migration geht nicht näher darauf ein, welche inhaltlichen Veränderungen sich aus der Umstellung der Sicherheitskonzeption ergeben könnten. Es ist möglich, dass zur Erfüllung von Anforderungen weitere Maßnahmen umgesetzt werden müssen.

Die Umstellung auf den modernisierten IT-Grundschutz hat auch Auswirkungen auf zertifizierte Informationsverbünde, die noch auf der vorherigen Grundlage auditiert und zertifiziert wurden. Dazu sind

Übergangsfristen und Möglichkeiten zur Migration im Rahmen der Zertifizierung vorgesehen (siehe [FRIST]).

1.3 Aufbau der Migrationsanleitung

Kapitel 2 gibt zunächst einen Überblick über die BSI-Standards, sowohl zum bisherigen als auch zum modernisierten IT-Grundschutz.

In Kapitel 3 wird schrittweise beschrieben, wie ein bestehendes Sicherheitskonzept auf den modernisierten IT-Grundschutz migriert werden kann. Die Darstellung deckt alle Phasen der IT-Grundschutz-Methodik ab: von der Strukturanalyse über die Schutzbedarfsfeststellung, die Modellierung und den IT-Grundschutz-Check bis hin zur Risikoanalyse.

Kapitel 4 widmet sich dem Thema Hilfsmittel und veranschaulicht, wie diese eingesetzt werden können, um die Migration vom klassischen auf den modernisierten IT-Grundschutz zu vereinfachen. Dabei wird auch ausführlich auf die Migrationstabellen eingegangen.

2 Überblick über die BSI-Standards

Bevor auf das eigentliche Thema – die Migration von Sicherheitskonzepten – eingegangen wird, werden im Folgenden die wesentlichen Prinzipien und Inhalte sowohl der „alten“ als auch „neuen“ Standards dargestellt. Dabei wird kurz insbesondere auf wesentliche Veränderungen eingegangen, die der IT-Grundschutz nach dem BSI-Standard 200-2 gegenüber dem IT-Grundschutz nach dem BSI-Standard 100-2 aufweist. Zudem wird der Fokus auf Aktivitäten gelegt, die bei der Erstellung einer Sicherheitskonzeption nach IT-Grundschutz relevant sind, das heißt, Strukturanalyse, Schutzbedarfsfeststellung, Modellierung, IT-Grundschutz-Check und Risikoanalyse.

2.1 Bisheriger IT-Grundschutz

Der bisherige IT-Grundschutz ist in den folgenden Dokumenten beschrieben:

- BSI-Standard 100-1 – Management-Systeme für Informationssicherheit (ISMS) [BSI1001]
- BSI-Standard 100-2 – IT-Grundschutz-Vorgehensweise [BSI1002]
- BSI-Standard 100-3 – Risikoanalyse auf der Basis von IT-Grundschutz [BSI1003]
- IT-Grundschutz-Kataloge, die über Ergänzungslieferungen regelmäßig aktualisiert wurden

Während der alte BSI-Standard 100-1 im Wesentlichen die Grundprinzipien und den Aufbau eines ISMS beschrieb, wurde die eigentliche IT-Grundschutz-Methode im alten BSI-Standard 100-2 dargestellt. Sie sah die folgenden Phasen vor:

- Strukturanalyse
- Schutzbedarfsfeststellung
- Modellierung
- Basis-Sicherheitscheck
- ergänzende Sicherheitsanalyse
- Risikoanalyse

Anträge auf Zertifizierung eines ISMS auf Basis des BSI-Standard 100-2 können bis zum Stichtag am 30.09.2018 gestellt werden (siehe [FRIST]). Die 15. Ergänzungslieferung der IT-Grundschutz-Kataloge ist dann bis zum 30.09.2021 verwendbar (siehe [PRUEF]).

2.2 Modernisierter IT-Grundschutz

Der 2017 modernisierte IT-Grundschutz ist in den folgenden Dokumenten dargestellt:

- BSI-Standard 200-1 – Managementsysteme für Informationssicherheit (ISMS) [BSI2001]
- BSI-Standard 200-2 – IT-Grundschutz-Methodik [BSI2002]
- BSI-Standard 200-3 – Risikoanalyse auf der Basis von IT-Grundschutz [BSI2003]
- IT-Grundschutz-Kompendium (1. Edition 2018) [GSKO]

Die IT-Grundschutz-Methodik, die im BSI-Standard 200-2 beschrieben ist, sieht nunmehr drei unterschiedliche Vorgehensweisen vor:

- Basis-Absicherung
- Standard-Absicherung

- Kern-Absicherung

Im Fokus dieser Anleitung zur Migration stehen Institutionen, die bereits ein IT-Grundschutz-konformes ISMS etabliert haben und die Standard-Absicherung ausgewählt haben, um ihr Sicherheitskonzept zu aktualisieren. Daher wird im Folgenden ausschließlich die Standard-Absicherung thematisiert. Sie beinhaltet die folgenden Phasen:

- Strukturanalyse
- Schutzbedarfsfeststellung
- Modellierung
- IT-Grundschutz-Check
- Risikoanalyse

2.3 Wesentliche Veränderungen

Im BSI-Standard 200-2 haben sich gegenüber dem BSI-Standard 100-2 die folgenden wesentlichen Veränderungen ergeben. Details zur konkreten Ausführung sind in Kapitel 3 beschrieben.

Strukturanalyse

In der Strukturanalyse muss unverändert der Geltungsbereich exakt festgelegt werden. Neu ist, dass die Geschäftsprozesse, die sich innerhalb des Geltungsbereiches befinden, zentraler Ausgangspunkt der Sicherheitskonzeption sind. Auf Basis des festgelegten Informationsverbunds sind in einem ersten Schritt die dort enthaltenen zentralen Geschäftsprozesse oder Fachaufgaben zu erfassen und zu dokumentieren. Ausgehend von jedem Geschäftsprozess bzw. jeder Fachaufgabe, die im Informationsverbund enthalten ist, müssen in dieser Phase die damit zusammenhängenden Anwendungen und die damit verarbeiteten Informationen identifiziert werden. Darüber hinaus sind in der Strukturanalyse die relevanten Dienstleister anzugeben. Ferner werden IT-Systeme etwas differenzierter betrachtet, so dass jetzt auch Industrielle Steuerungssysteme (ICS) und sonstige Geräte wie z. B. aus dem Bereich Internet of Things (IoT) mit in die Sicherheitskonzeption aufzunehmen sind. Details zur Strukturanalyse finden sich in Kapitel 3.1.

Schutzbedarfsfeststellung

Der Schutzbedarf wird nach der Schutzbedarfsdefinition für die Geschäftsprozesse statt wie bisher für die Anwendungen festgelegt. Dieser Schutzbedarf gilt auch für die übrigen Zielobjekte des Geltungsbereiches wie z. B. Anwendungen oder IT-Systeme. Die Schutzbedarfsfeststellung wird im Detail in Kapitel 3.2 dargestellt.

Modellierung

In der Modellierung werden nach wie vor die relevanten Bausteine des IT-Grundschutz-Kompendiums identifiziert. Dabei ist zu beachten, dass die Bausteine grundlegend überarbeitet und neu strukturiert wurden. Die Bausteine sind jetzt nach einem neuen Schichtenmodell in prozess- und systemorientierte Bausteine organisiert. Die prozessorientierten Bausteine finden sich in den folgenden Schichten:

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

Die systemorientierten Bausteine sind in die folgenden Schichten gruppiert:

- APP: Anwendungen

- SYS: IT-Systeme
- IND: Industrielle IT
- NET: Netze und Kommunikation
- INF: Infrastruktur

Die Bausteine haben sich nicht nur in Namen, Struktur und Inhalten geändert, sondern auch in ihrer grundlegenden Ausrichtung: Während in den Bausteinen vorher Sicherheitsmaßnahmen beschrieben wurden, werden im modernisierten IT-Grundschutz lediglich Anforderungen formuliert. Damit ist eine Institution nun deutlich freier in ihrer Wahl konkreter Maßnahmen, um eine Anforderung zu erfüllen. Dies bedingt zugleich, dass dieser zusätzliche Schritt – von einer Anforderung zu geeigneten Maßnahmen – dokumentiert sein muss. Als Hilfsmittel liegen zu vielen IT-Grundschutz-Bausteinen sogenannte Umsetzungshinweise vor. Diese beschreiben, wie die Anforderungen der Bausteine umgesetzt werden können und erläutern im Detail geeignete Sicherheitsmaßnahmen. Die Umsetzungshinweise sind Best-Practice-Beispiele und nicht verbindlich. Weitere Informationen zur Modellierung finden sich in Kapitel 3.3.

IT-Grundschutz-Check

Im IT-Grundschutz-Check wird pro Baustein und pro Anforderung geprüft, ob eine Anforderung hinreichend erfüllt ist. Aufgrund der oben genannten Änderung ist nun nicht nur die Umsetzung einer konkret vorgegebenen Maßnahme zu prüfen. Zusätzlich muss gewährleistet werden, dass die definierte Maßnahme zur Erfüllung der Anforderung auch angemessen ist. Der IT-Grundschutz-Check wird ausführlich in Kapitel 3.4 erläutert.

Risikoanalyse

Die ergänzende Sicherheitsanalyse entfällt im modernisierten IT-Grundschutz. Stattdessen wird direkt eine Risikoanalyse für Zielobjekte durchgeführt,

- die einen höheren Schutzbedarf aufweisen,
- die mit den bestehenden Bausteinen des IT-Grundschutzes nicht hinreichend abgebildet werden können oder
- die in Einsatzszenarien (Umgebung, Anwendung) betrieben werden, die im Rahmen des IT-Grundschutzes nicht vorgesehen sind.

Eine mögliche Vorgehensweise zur Analyse und Behandlung von Risiken wird im BSI-Standard 200-3 dargestellt. Dieser Standard hat sich gegenüber dem vorherigen Standard 100-3 stark verändert. Neu sind beispielsweise die komplette Umstellung der Risikoanalyse auf die elementaren Gefährdungen, die Einführung eines Matrix-Ansatzes zur Bewertung von Risiken sowie die Einführung von Risikoappetit und Chancenmanagement. Unverändert fließen zusätzliche Sicherheitsmaßnahmen in die Sicherheitskonzeption ein. Weiteres zur Risikoanalyse ist in Kapitel 3.5 dargestellt.

Ein nach BSI-Standard 200-2 etabliertes ISMS kann auditiert und zertifiziert werden. Dazu stehen Auditierungs- und Zertifizierungsschemata (siehe [AUD] und [ZERT]) zur Verfügung.

3 Anleitung zur Migration

Im Nachfolgenden wird Schritt für Schritt beschrieben, wie bestehende Sicherheitskonzepte auf Basis der BSI-Standards 100-1, 100-2 und 100-3 sowie der IT-Grundschutz-Kataloge auf den modernisierten IT-Grundschutz, also gemäß BSI-Standards 200-1, 200-2 und 200-3 sowie dem IT-Grundschutz-Kompendium, migriert werden können. Dabei wird davon ausgegangen, dass ein nach BSI-Standard 100-2 und den IT-Grundschutz-Katalogen aufgebautes Managementsystem für Informationssicherheit (ISMS) vorliegt.

Unverzichtbar ist zunächst, dass sich die Institution mit den neuen BSI-Standards und dem IT-Grundschutz-Kompendium vertraut macht. Die Kenntnis insbesondere des BSI-Standards 200-2 und des IT-Grundschutz-Kompendiums wird vorausgesetzt.

Hinweis: Die Modernisierung des IT-Grundschutzes bietet neben dem zusätzlichen Aufwand auch die Chance, die vorhandene Sicherheitskonzeption einer gründlichen Revision zu unterziehen, die bereits umgesetzten Sicherheitsmaßnahmen kritisch zu hinterfragen und gegebenenfalls im Sinne einer kontinuierlichen Verbesserung zu aktualisieren und zu optimieren.

3.1 Strukturanalyse

Im Vergleich zur bisherigen Strukturanalyse nach BSI-Standard 100-2 hat sich die überarbeitete Strukturanalyse gemäß BSI-Standard 200-2 im Wesentlichen dahingehend verändert, dass die Geschäftsprozesse stärker in den Vordergrund gerückt sind. Die vorhandenen Ergebnisse der Strukturanalyse sind zu ergänzen, bzw. es ist zu prüfen, ob die Geschäftsprozesse, die zum Geltungsbereich gehören, hinreichend präzise in der Strukturanalyse aufgenommen worden sind. Sind die Geschäftsprozesse bisher nicht eindeutig identifiziert und erfasst sowie mit den zugehörigen Anwendungen verknüpft worden, muss dieser Schritt anhand des Geltungsbereichs der Sicherheitskonzeption nachgeholt werden. Darüber hinaus ist es sinnvoll, die identifizierten Anwendungen als Gegenprüfung zu verwenden, da eine Anwendung ohne zugrundeliegenden Geschäftsprozess nicht sinnvoll in die Strukturanalyse aufgenommen werden kann. Schließlich muss die Strukturanalyse um die relevanten Dienstleister sowie Zielobjekte, die in deren Einflussbereich liegen, ergänzt werden (siehe dazu auch Vorgaben zum Outsourcing [OUT]).

Ansonsten kann die vorliegende Strukturanalyse weiterverwendet werden. Hierzu sollten die Anwendungen, Netzpläne sowie IT-Systeme geprüft und die gewonnenen Ergebnisse übernommen werden. Hervorzuheben ist, dass der modernisierte IT-Grundschutz die verschiedenen Arten von IT-Systemen etwas stärker differenziert und etwa Industrielle Steuerungssysteme (ICS) oder sonstige Geräte wie z. B. aus dem Bereich Internet of Things einzeln betrachtet. Wenn sich der Informationsverbund nicht geändert hat, ist zu prüfen, ob es für Zielobjekte, die bisher mit benutzerdefinierten Bausteinen abgedeckt wurden, nun geeignete Bausteine im IT-Grundschutz-Kompendium gibt. Abschließend werden Räume, Gebäude und Standorte erfasst.

Aktionspunkte:

- Identifikation der relevanten Geschäftsprozesse im Geltungsbereich und Aufnahme in die Strukturanalyse
- Abgleich der Geschäftsprozesse mit den bereits aufgeführten Anwendungen und Prüfung, ob alle relevanten Geschäftsprozesse in die Strukturanalyse mit aufgenommen wurden
- Dienstleister sowie alle Zielobjekte in deren Einflussbereich in die Strukturanalyse aufnehmen, sofern diese für den Geltungsbereich relevant sind
- Bereits vorliegende Strukturanalyse kontrollieren und übernehmen
- Bei der Erfassung der IT-Systeme prüfen, ob Industrielle Steuerungssysteme (ICS) und sonstige Geräte mit Bausteinen aus dem IT-Grundschutz-Kompendium abgedeckt werden können

Die exakten Vorgaben und weitere Informationen finden sich in Kapitel 8.1 des BSI-Standards 200-2.

3.2 Schutzbedarfsfeststellung

Die Schutzbedarfsfeststellung hat sich im Wesentlichen dahingehend geändert, dass die Grundlage zur Bestimmung des Schutzbedarfs nunmehr die Geschäftsprozesse und die zugehörigen Informationen .sind Der für diese Elemente ermittelte Schutzbedarf vererbt sich dann auf die für deren Verarbeitung genutzten Zielobjekte, also Anwendungen, IT- und ICS-Systeme sowie sonstige Geräte (IoT-Geräte), Räume und Kommunikationsverbindungen. Häufig wurden in der Vergangenheit die relevanten Anwendungen als Ausgangspunkt der Schutzbedarfsfeststellung genutzt. Der Schutzbedarf der Anwendungen muss sich jetzt konsistent aus dem Schutzbedarf der Geschäftsprozesse ableiten lassen.

Ansonsten kann die bereits vorliegende Schutzbedarfsfeststellung geprüft und übernommen werden. Diese umfasst die Prüfung und Übernahme der Schutzbedarfskategorien sowie die Schutzbedarfsfeststellungen für die IT-Systeme, Räume, Gebäude und Standorte sowie die Kommunikationsverbindungen. Sofern in der Strukturanalyse neben den IT-Systemen auch Industrielle Steuerungssysteme (ICS) und sonstige Geräte wie z. B. IoT-Geräte identifiziert wurden, ist der Schutzbedarf auch für diese Systeme festzulegen. Bei der Festlegung sind unverändert die Abhängigkeiten und Vererbungsregeln mit Maximum-, Kumulations- und Verteilungseffekt zu beachten. Ferner geht der Schutzbedarf auf die relevanten Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit ein. Darüber hinaus gibt Kapitel 8.2.4 des BSI-Standards 200-2 Hinweise zur Schutzbedarfsfeststellung im Kontext von Cloud Computing und virtualisierten Umgebungen.

Aktionspunkte:

- Schutzbedarf der Geschäftsprozesse und zugrundeliegende Informationen bestimmen
- Schutzbedarf der Anwendungen ableiten und begründen
- Schutzbedarf der ICS- oder IoT-Systeme ableiten und begründen (sofern anwendbar ausgeführt, kann der Schutzbedarf für den Bereich ICS gesondert festgelegt werden)
- Schutzbedarf der weiteren Assets inklusive Räume und Gebäude sowie Kommunikationsverbindungen mit Begründungen kontrollieren und übernehmen

Die exakten Vorgaben und weitere Informationen finden sich in Kapitel 8.2 des BSI-Standards 200-2.

3.3 Modellierung

Aufgrund der starken Veränderungen im IT-Grundschutz-Kompendium im Vergleich zu den IT-Grundschutz-Katalogen ist die Modellierung, also die Auswahl von relevanten Bausteinen aus den verschiedenen Schichten, komplett neu durchzuführen. Die Methodik zur Modellierung hat sich allerdings nicht verändert.

Zunächst sind unverändert alle Bausteine in der Modellierung auszuwählen, die für den Informationsverbund relevant sind. Kapitel 8.3 des BSI-Standards 200-2 und das IT-Grundschutz-Kompendium erläutern hierzu die Vorgehensweise, die sich am Schichtenmodell des IT-Grundschutzes orientiert.

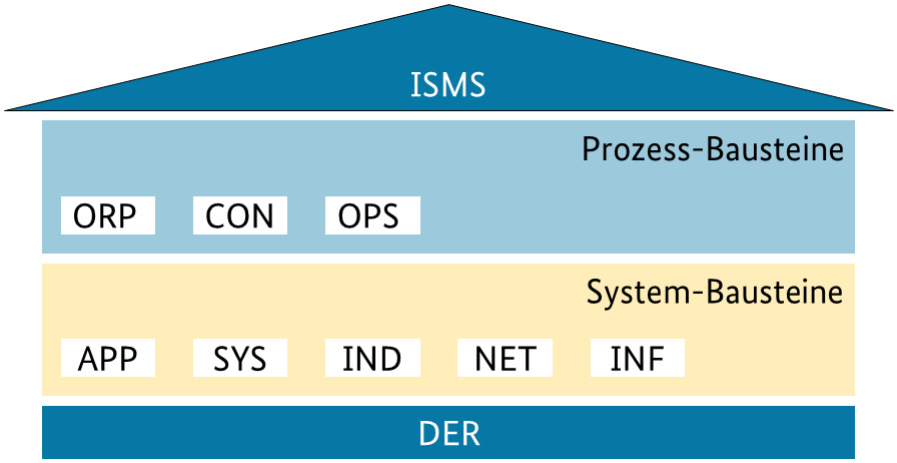

Abbildung 1: Schichtenmodell nach IT-Grundschutz

Danach sind zunächst die Prozess-Bausteine und anschließend die System-Bausteine zu betrachten:

Prozess-Bausteine:

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

System-Bausteine:

- Die Schicht APP beschäftigt sich mit der Absicherung von Anwendungen und Diensten, unter anderem in den Bereichen Kommunikation, Verzeichnisdienste, Netzbasierte Dienste sowie Business- und Client-Anwendungen. Typische Bausteine der Schicht APP sind *Allgemeine Groupware*, *Office-Produkte*, *Webserver* und *Web-Browser*.
- Die Schicht SYS betrifft die einzelnen IT-Systeme des Informationsverbunds, die möglicherweise in Gruppen zusammengefasst wurden. Hier werden Sicherheitsaspekte von Servern, Desktop-Systemen, Mobile Devices und sonstigen IT-Systemen wie Druckern und Telekommunikations-Anlagen behandelt. Zur Schicht SYS gehören beispielsweise Bausteine zu Betriebssystemen, Smartphones und Tablets sowie Drucker, Kopierer und Multifunktionsgeräte.
- Die Schicht IND befasst sich mit Sicherheitsaspekten Industrieller IT (ICS). Zu dieser Schicht zählen beispielsweise die Bausteine *Maschine*, *Sensoren und Aktoren* sowie *Speicherprogrammierbare Steuerung (SPS)*.

- Die Schicht NET betrachtet die Aspekte der Vernetzung, die sich nicht auf bestimmte IT-Systeme, sondern auf die Netzverbindungen und die Kommunikation beziehen. Dazu gehören zum Beispiel die Bausteine *Netzmanagement*, *Firewall* und *WLAN-Betrieb*.
- Die Schicht INF befasst sich mit den baulich-technischen Gegebenheiten. Hier werden Aspekte der infrastrukturellen Sicherheit thematisiert. Dies betrifft unter anderem die Bausteine *Allgemeines Gebäude* und *Rechenzentrum* sowie *Serverraum*.

Das Ergebnis ist eine Modellierung, in der alle Bausteine des Kompendiums aufgeführt sind. Außerdem ist darin für jeden Baustein angegeben, ob bzw. auf welche Zielobjekte er anwendbar ist. Ist ein Baustein nicht anwendbar, muss dies begründet werden.

Kapitel 2.2 im IT-Grundschutz-Kompendium gibt Hinweise dazu, ob ein Baustein lediglich einmal für den ganzen Informationsverbund oder mehrfach für einzelne Bereiche anzuwenden ist. Ferner gibt Kapitel 8.3.5 des BSI-Standards 200-2 Hinweise zur Modellierung im Kontext von Virtualisierung und Cloud-Computing. In Kapitel 8.3.7 des BSI-Standards finden sich zudem Vorgaben zur Einbeziehung von externen Dienstleistern (siehe hierzu auch [OUT]). Die Anforderungen der Bausteine können nach wie vor an spezifische Gegebenheiten angepasst werden.

Aktionspunkte:

- Modellierung gemäß Kapitel 8.3 des BSI-Standards 200-2 durchführen,
- alle Bausteine hinsichtlich Anwendbarkeit prüfen und relevanten Zielobjekten zuordnen und
- Auswahl sowie Nicht-Auswahl begründen.

Die exakten Vorgaben und zusätzliche Informationen finden sich in Kapitel 8.3 des BSI-Standards 200-2 und im IT-Grundschutz-Kompendium.

3.4 IT-Grundschutz-Check

Die umfangreichen inhaltlichen Änderungen im IT-Grundschutz-Kompendium und der vollzogene Paradigmenwechsel – von vorgegebenen Maßnahmen zu Anforderungen, zu denen die Institution selbst passende Maßnahmen definieren muss – machen es erforderlich, den IT-Grundschutz-Check komplett neu durchzuführen.

Als Vorgehensweise wird empfohlen, den Soll-Ist-Vergleich erneut vorzunehmen und pro Schicht, pro ausgewähltem Baustein und für jede Anforderung folgende Informationen zu erfassen:

- Umsetzung der Maßnahme, d. h. Beschreibung, durch welche Maßnahmen die Institution die Anforderung erfüllt
- Umsetzungsstand der definierten Maßnahme

Das BSI unterstützt die Anwender bei diesem umfangreichen Dokumentations-Prozess mit sogenannten Migrationstabellen, die den Zusammenhang zwischen Anforderungen aus den neuen IT-Grundschutz-Bausteinen und vormaligen Maßnahmen aus dem klassischen IT-Grundschutz darstellen. Damit kann eine Institution zunächst feststellen, welche bisherigen Maßnahmen einer Anforderung zugeordnet sind und dann prüfen, ob diese bereits umgesetzten Maßnahmen hinreichend sind, um der jeweils neuen Anforderung zu genügen. Diese Maßnahmen zur Erfüllung einer Anforderung sowie der jeweilige Umsetzungsstand sind zu dokumentieren.

Gerade bei einem bereits etablierten ISMS ist es häufig so, dass die Definition von Maßnahmen zur Erfüllung einer Anforderung einhergeht mit der Beschreibung von bereits umgesetzten Maßnahmen. Dennoch sollte in diesem Prozess auch kritisch hinterfragt werden, ob eine Maßnahme hinreichend ist, um die Anforderung zu erfüllen.

Sofern die bislang realisierten Maßnahmen eine Anforderung nur unzureichend abdecken, sind weitere Maßnahmen zu definieren und deren Umsetzungsstand mit „nein“ oder „teilweise“ zu klassifizieren. Diese

Anforderung und die zugehörigen Maßnahmen sollten dann in den Risikobehandlungsplan überführt und dort bearbeitet werden. Der Umgang mit solchen noch nicht vollständig umgesetzten Maßnahmen ist im Rahmen eines Auditierungs- und Zertifizierungsprozesses geregelt (siehe [BSI2002]).

Institutionen, die bislang schon für jede vorgegebene Maßnahme ausführlich dokumentiert haben, wie diese konkret umgesetzt wird, die also das Feld „Bemerkungen/Begründung für Nicht-Umsetzung“ genutzt haben, werden diesen Umstellungsprozess deutlich einfacher bewerkstelligen können.

Hinsichtlich des Bezugs von Anforderungen zu Maßnahmen sind unterschiedliche Fälle zu betrachten:

- Es gibt Anforderungen, die auf bisherige Maßnahmen abgebildet werden können. In solchen Fällen ist eine Umstellung relativ leicht zu erreichen.
- Daneben gibt es Anforderungen, die nicht nur auf Maßnahmen von einem ursprünglichen Baustein abgebildet werden können, sondern bei denen einzelne Maßnahmen aus weiteren Bausteinen zu betrachten sind. Auch hier ist die Umstellung relativ leicht zu erreichen.
- Schließlich gibt es neue Anforderungen, für die Maßnahmen zunächst definiert werden müssen und danach der Umsetzungsstand dokumentiert werden muss.

Zu den Migrationstabellen finden sich in Kapitel 4.3 dieses Dokuments weiterführende Informationen. Eine weitere Hilfestellung können auch Tools darstellen, mit denen eine Institution ihr ISMS dokumentiert (siehe Kapitel 4.2).

Aktionspunkte:

- Pro Schicht und pro Baustein der Modellierung jede einzelne Anforderung des Bausteins wie folgt bearbeiten:
  - Maßnahmen zur Erfüllung der Anforderung definieren und dokumentieren. Als Hilfsmittel bieten sich die Migrationstabellen an, mit denen sich schnell herausfinden lässt, zu welchen bisherigen Maßnahmen die konkrete Anforderung korrespondiert. Dies kann helfen, den bislang dokumentierten Sachstand schnell abzugleichen.
  - Prüfen, ob durch die Umsetzung solcher Maßnahmen die Anforderung hinreichend erfüllt ist.
  - Umsetzungsstand der definierten Maßnahmen („ja“, „teilweise“, „nein“) prüfen und dokumentieren.
  - Anforderungen und zugehörige Maßnahmen, die nicht oder nur teilweise umgesetzt sind, in den Risikobehandlungsplan überführen.

Die exakten Vorgaben und weitere Informationen finden sich in Kapitel 8.4 des BSI-Standards 200-2.

3.5 Risikoanalyse

Eine Risikoanalyse ist dann erforderlich, wenn es Zielobjekte gibt, die

- einen hohen oder sehr hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit haben oder
- mit den existierenden Bausteinen des IT-Grundschutzes nicht hinreichend abgebildet (modelliert) werden können oder
- in Einsatzszenarien (Umgebung, Anwendung) betrieben werden, die im Rahmen des IT-Grundschutzes nicht vorgesehen sind.

Unter der Annahme, dass eine dieser Voraussetzungen zutrifft, ist gegenüber dem bisherigen IT-Grundschutz relevant, dass die ergänzende Sicherheitsanalyse entfallen ist. Daher ist Folgendes zu beachten:

- Wurde bislang eine ergänzende Sicherheitsanalyse durchgeführt und von der Leitungsebene festgestellt, dass keine Risikoanalyse erforderlich ist, so ist nun immer eine Risikoanalyse durchzuführen. Eine

Migration ist in diesem Fall nicht möglich. Stattdessen ist eine Risikoanalyse z. B. gemäß BSI-Standard 200-3 erforderlich.

- Wurde in der ergänzenden Sicherheitsanalyse festgestellt, dass nur für ausgewählte Zielobjekte eine Risikoanalyse durchzuführen ist, so ist nun auch für die in der ergänzenden Sicherheitsanalyse ausgeschlossenen Zielobjekte eine Risikoanalyse erforderlich.
- Für alle Zielobjekte, für die bereits eine Risikoanalyse nach dem vormaligen BSI-Standard 100-3 durchgeführt wurde, wird empfohlen, die bestehende Risikoanalyse zu aktualisieren.

Um die Risikoanalyse zu aktualisieren, kann eine Risikoanalyse gemäß BSI-Standard 200-3 durchgeführt werden. Dazu kann der nachfolgend beschriebene Migrationsansatz gewählt werden. Institutionen, die ein anderes etabliertes Verfahren (z. B. ISO/IEC 27005, ISO/IEC 31000) oder eine angepasste Methodik für die Analyse von Risiken der Informationssicherheit verwenden, können die folgenden Empfehlungen entsprechend adaptieren.

Migration auf 200-3:

Zunächst ist eine Liste von Zielobjekten vorzulegen, für die eine Risikoanalyse durchgeführt werden muss. Hierfür gelten die oben dargestellten Voraussetzungen. Diese Übersicht stellt den Ausgangspunkt für die Risikoanalyse dar und unterscheidet sich nicht von der Vorgehensweise gemäß BSI-Standard 100-2. Damit diese Aufgabe mit vertretbarem Aufwand durchgeführt werden kann, ist es wichtig, dass die Zielobjekte sinnvoll zu Gruppen zusammengefasst werden. Müssen trotz Gruppenbildung viele Zielobjekte einer Risikoanalyse unterzogen werden, sollte priorisiert werden (siehe Kapitel 2 des BSI-Standards 200-3).

Danach werden für jedes Zielobjekt die relevanten elementaren Gefährdungen zusammengetragen und dem Zielobjekt zugeordnet. Neu ist dabei, dass die Risikoanalyse nach dem BSI-Standard 200-3 komplett auf elementare Gefährdungen umgestellt worden ist. Die spezifischen Gefährdungen aus den IT-Grundschutz-Katalogen (G1 bis G5) spielen bei künftigen Risikoanalysen keine Rolle mehr. Dies bedeutet, dass bei allen Sicherheitskonzepten, die noch auf spezifischen Gefährdungen basieren, die vorhandenen Risikoanalysen darauf überprüft werden müssen, ob sie noch der aktuellen Gefährdungslage entsprechen und ob alle elementaren Gefährdungen betrachtet wurden.

Institutionen, die ihre Sicherheitskonzepte bereits auf die elementaren Gefährdungen umgestellt haben, können ihre bisherigen Betrachtungen nutzen und die Liste von relevanten Gefährdungen aktualisieren. Hierbei sollte besonders darauf geachtet werden, dass die Gefährdungsübersichten aus dem IT-Grundschutz-Kompendium (Listen der relevanten elementaren Gefährdungen in der Kreuzreferenztabelle der modernisierten Bausteine) bei der Aktualisierung mit berücksichtigt werden.

Darüber hinaus können zusätzliche Gefährdungen aufgenommen werden. Dieser Schritt ist von der Vorgehensweise her unverändert, so dass vorherige Informationen für die Betrachtung genutzt werden können.

Nach der Identifikation von Zielobjekten und relevanten Gefährdungen erfolgt die Risikobetrachtung mit den folgenden Schritten:

- Risikoeinschätzung mit Angabe von Eintrittshäufigkeit und Schadenshöhe
- Risikobewertung: Hierzu schlägt der BSI-Standard 200-3 exemplarisch einen Matrix-Ansatz mit diversen Risikokategorien vor. Dieser löst die bisherige Einschätzung anhand der Prüfkriterien Vollständigkeit, Mechanismenstärke und Zuverlässigkeit ab. So kann kontrolliert werden, ob die bereits umgesetzten oder im Sicherheitskonzept vorgesehenen Maßnahmen ausreichend sind („OK=J“ oder „OK=N“).
- Risikobehandlung mit den üblichen Optionen, abhängig vom Risikoappetit der Institution:
  - Risiko-Vermeidung durch Veränderung des Geltungsbereichs
  - Risiko-Reduktion durch Umsetzung weiterer Sicherheitsmaßnahmen
  - Risiko-Transfer durch Abschluss entsprechender Versicherungen

- Risiko-Akzeptanz durch Übernahme des Restrisikos

Unverändert bleibt, dass die Leitungsebene Restrisiken, die akzeptiert werden sollen, abnehmen muss. Gleichfalls unverändert ist der Umgang mit den zusätzlichen Maßnahmen, die in die Sicherheitskonzeption zurückfließen müssen.

Im Ergebnis ist festzustellen, dass sich die Methodik zur Durchführung von Risikoanalysen deutlich verändert hat. Wichtig ist daher, dass die Richtlinie der Institution zur Durchführung der Risikoanalyse angepasst werden muss. Insbesondere müssen im Vorfeld von Risikoanalysen die gewählte Methodik zur Identifizierung, Einschätzung, Bewertung und Behandlung von Risiken sowie die Risikoakzeptanzkriterien festgelegt werden.

Aktionspunkte:

- Zielobjekte, für die eine Risikoanalyse durchgeführt werden muss, identifizieren. Im Weiteren nur solche Zielobjekte betrachten.
- Zielobjekte, bei denen in der ergänzenden Sicherheitsanalyse festgestellt wurde, dass keine weiterführende Risikoanalyse erforderlich ist, identifizieren.
- Für diese Zielobjekte Risikoanalyse gemäß BSI-Standard 200-3 durchführen (eine Migration ist in diesem Fall nicht möglich).
- Eine Migration ist möglich für Zielobjekte, für die bislang schon eine Risikoanalyse durchgeführt wurde:
  - Liste der relevanten Zielobjekte kontrollieren und übernehmen.
  - Die relevanten Gefährdungen entweder zusammentragen und den Zielobjekten zuordnen oder Zuordnung von relevanten Gefährdungen zu Zielobjekten kontrollieren und übernehmen.
  - Risikoeinschätzung pro Zielobjekt unter Berücksichtigung von Eintrittshäufigkeit und Schadenshöhe entweder durchführen oder kontrollieren und übernehmen.
  - Risikobewertung pro Zielobjekt entweder durchführen oder kontrollieren und übernehmen.
  - Risikobehandlung pro Zielobjekt entweder durchführen oder kontrollieren und übernehmen.
  - Übernahme des Restrisikos durch die Leitungsebene
  - Integration von zusätzlichen Sicherheitsmaßnahmen in die Sicherheitskonzeption, eventuell durch Erstellung eines benutzerdefinierten Bausteins

Die exakten Vorgaben und weitere Informationen finden sich im BSI-Standard 200-3.

4 Hilfsmittel

4.1 Umsetzungshinweise

Zu vielen Bausteinen des IT-Grundschutzes existieren Umsetzungshinweise mit beispielhaften Empfehlungen für Sicherheitsmaßnahmen, mittels derer die Anforderungen aus den Bausteinen umgesetzt werden können. Diese basieren auf Best Practices und langjähriger Erfahrung von Experten aus dem Bereich der Informationssicherheit. Die Maßnahmen aus den Umsetzungshinweisen sind jedoch nicht als verbindlich zu betrachten, sondern können und sollten durch eigene Maßnahmen ergänzt oder ersetzt werden.

4.2 Tools

Es gibt eine Reihe von Tools von verschiedenen Anbietern, die eine Sicherheitskonzeption gemäß IT-Grundschutz unterstützen (siehe [GST]). Diese Tools helfen bei der Migration vom bisherigen auf den modernisierten IT-Grundschutz. Welche Funktionen ein konkretes Tool bietet, ist vom jeweiligen Produkt abhängig.

Es sind folgende Hinweise zur „automatisierten“ Umstellung zu beachten:

- Tools mit Migrations-Funktionalität unterstützen den Prozess und entbinden womöglich von lästigen Dokumentationsaufgaben.
- Gleichzeitig gilt: Ein ISMS ist ein Prozess, kein Produkt. So verlockend die Aussicht auch ist, auf Knopfdruck auf den modernisierten IT-Grundschutz umzustellen: Es sollte die Chance genutzt werden, ein ISMS einer gründlichen Überprüfung zu unterziehen und so im Sinne eines PDCA-Zyklus (Plan-Do-Check-Act) fortlaufend weiterzuentwickeln. So können Neuerungen wie neue, aktualisierte Bausteine und neue Freiheitsgrade bei der Auswahl von Maßnahmen im Rahmen des modernisierten IT-Grundschutzes ihre volle Wirkung entfalten.

4.3 Migrationstabellen

Bei der Modernisierung des IT-Grundschutzes wurden die bereits vorhandenen Bausteine der IT-Grundschutz-Kataloge in die neue Form umgewandelt. Hierbei wurde für jeden migrierten Baustein eine sogenannte Migrationstabelle angelegt, welche die Zuordnung der Anforderungen des IT-Grundschutz-Kompendiums zu den Sicherheitsmaßnahmen der IT-Grundschutz-Kataloge abbildet. Mit diesen Migrationstabellen stellt das BSI umfangreiche Informationen zur Verfügung, um einen reibungslosen und effizienten Übergang zu ermöglichen.

Beim IT-Grundschutz-Check lässt sich anhand der Migrationstabellen zu jeder Anforderung leicht feststellen, welche bisherigen Maßnahmen dieser Anforderung entsprechen. Damit kann zumindest bei der Auswahl geeigneter Maßnahmen zur Erfüllung dieser Anforderung kontrolliert werden, welche bisherigen Maßnahmen dazu korrespondieren. Es gibt jedoch oftmals keine 1:1-Beziehung zwischen (neuen) Anforderungen und (bisherigen) Maßnahmen, die eine direkte Übernahme gewährleisten würde. Die Migrationstabellen sind stets wie folgt aufgebaut:

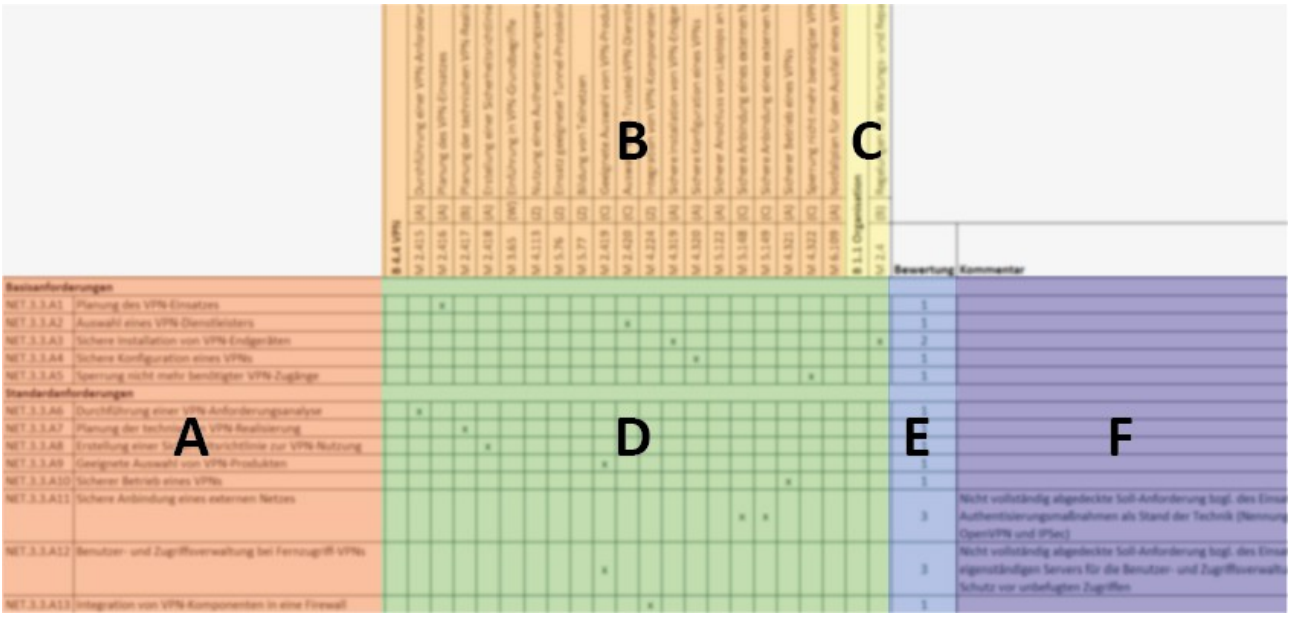

Abbildung 2: Struktur von Migrationstabellen

- Links untereinander sind alle Basis- und Standard-Anforderungen aufgeführt sowie die Anforderungen bei erhöhtem Schutzbedarf aus den (neuen) Bausteinen des IT-Grundschutz-Kompendiums (Abschnitt A in der Abbildung).
- Oben sind die Maßnahmen der (alten) Bausteine aus den IT-Grundschutz-Katalogen dargestellt. Die Auflistung beginnt stets mit dem ursprünglichen Baustein der 15. Ergänzungslieferung, der den neuen Baustein aus dem IT-Grundschutz-Kompendium am besten abdeckt (Abschnitt B). Nachfolgend finden sich gegebenenfalls Maßnahmen aus weiterführenden Bausteinen (Abschnitt C). Hierbei wurden grundsätzlich nur kontextbezogene Bausteine berücksichtigt. Dies bedeutet beispielsweise für den Baustein NET 1.1 *Netzarchitektur und -design*, dass keine Maßnahmen aus dem alten Baustein B 3.101 *Allgemeiner Server* herangezogen wurden, selbst wenn einzelne Abschnitte passen würden.
- Darunter finden sich die Zuordnungen, die durch ein „x“ gekennzeichnet sind. Ein „x“ bedeutet, dass zwischen dieser Anforderung („neu“) und der korrespondierenden Maßnahme („alt“) ein inhaltlicher Zusammenhang besteht (Abschnitt D).
- Über die Art dieses Zusammenhangs gibt die rechts daneben angegebene Bewertung in Form der Ziffern 1, 2 oder 3 Auskunft (Abschnitt E). Dabei sind folgende Fälle zu unterscheiden:
  1. Die Anforderung wird vollständig mit den Maßnahmen aus dem entsprechenden Baustein der 15. Ergänzungslieferung (EL) abgedeckt. Sofern die Maßnahme(n) zuvor vollständig umgesetzt wurde(n), ist eine weitere Überarbeitung der Anforderung nicht zwingend notwendig.
  2. Die Anforderung wird vollständig nur unter Berücksichtigung zusätzlicher Maßnahmen aus weiteren Bausteinen der 15. EL abgedeckt. Eine Kontrolle auf vollständige Abdeckung ist jedoch notwendig, da die Maßnahmen aus einem anderen Kontext (Baustein) stammen. Diese Bewertung wird auch vorgenommen, wenn die Maßnahme aus der 15. EL nur einen empfehlenden oder informierenden Charakter hatte. Im Kommentarfeld findet sich diesbezüglich ein Hinweis.
  3. Die Anforderung wird, auch unter Berücksichtigung weiterer Maßnahmen aus der 15. EL, nicht in jedem Fall vollständig abgedeckt. Hierbei muss im Detail geprüft werden, wie die Anforderung erfüllt werden kann. Im Kommentarfeld findet sich diesbezüglich ein Hinweis auf mögliche, nicht abgedeckte Bereiche der Anforderung.
- Das Kommentarfeld befindet sich rechts neben der Bewertung (Abschnitt F).

Bei der Anwendung sind die folgenden Rahmenbedingungen und Hinweise zu beachten:

- Alle Anforderungen werden gleichermaßen behandelt, da im Zweifelsfall eine Einzelprüfung erfolgen muss.
- Es ist nicht auszuschließen, dass neben den in den Migrationstabellen identifizierten Maßnahmen aus der 15. Ergänzungslieferung weitere Maßnahmen aus anderen Bausteinen passend wären.
- Sofern Anforderungen nicht mit Maßnahmen aus dem ursprünglichen Baustein abgedeckt werden können, werden mögliche Hinweise auf Maßnahmen anderer Bausteine gegeben. Diese sind als Hinweise zu verstehen und müssen manuell durch den Anwender kontrolliert werden.
- Zum Teil wurden bei der Modernisierung die ursprünglichen Maßnahmen bei der Überführung zu den Anforderungen zwar zum großen Teil inhaltlich übernommen, aber marginale Veränderungen (z. B. Verschärfungen) hinzugefügt. So deckt beispielsweise die Maßnahme M 2.322 *Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz* aus dem gleichnamigen Baustein B 3.201 *Allgemeiner Client* die Anforderung SYS.2.1.A9 *Festlegung einer Sicherheitsrichtlinie für Clients* nahezu vollständig ab. Gleichwohl wurde diese ergänzt um die Dokumentationspflicht der regelmäßigen Umsetzungsüberprüfung: „Die Umsetzung der in der Richtlinie geforderten Inhalte SOLLTE regelmäßig überprüft werden. Die Ergebnisse SOLLTEN sinnvoll dokumentiert werden." In diesen Fällen wurde die Bewertung 3 vorgenommen mit einem entsprechenden Hinweis im Kommentarfeld.

Die Anwendung der Migrationstabellen soll durch drei Beispiele verdeutlicht werden.

Beispiel 1: Im Wesentlichen identische Bausteine

Es gibt Bausteine, die im Wesentlichen identisch übernommen wurden, beispielsweise NET.3.3 *VPN*. Der zugehörigen Migrationstabelle ist zu entnehmen, dass die Anforderungen des neuen Bausteins NET.3.3 *VPN* im Wesentlichen durch den alten Baustein B 4.4 *VPN* und B 1.1 *Organisation* erfüllt wurden. Sofern die Maßnahmen zuvor vollständig umgesetzt wurden, ist eine weitere Überarbeitung der Anforderung mit der Bewertung 1 nicht notwendig. Die Anforderung kann damit als umgesetzt gelten und der Text aus dem alten Basis-Sicherheitscheck kann in den neuen IT-Grundschutz-Check übernommen werden. Die Anforderung NET.3.3.A3 *Sichere Installation von VPN-Endgeräten* wird nur vollständig unter Berücksichtigung von M 2.4 *Regelungen für Wartungs- und Reparaturarbeiten* aus dem Baustein B 1.1 *Organisation* umgesetzt, so dass hier auch davon ausgegangen werden kann, dass diese Anforderung umgesetzt ist. Eine Kontrolle ist dabei aber notwendig.

Beispiel 2: Inhaltlich veränderte Bausteine

Es gibt Bausteine, die zwar identisch benannt sind, aber inhaltlich weitgehend überarbeitet wurden, beispielsweise SYS.2.3 *Clients unter Unix*.

Der zugehörigen Migrationstabelle ist zu entnehmen, dass eine Zuordnung zum alten Baustein B 3.204 *Client unter Unix* inhaltlich nur sehr rudimentär möglich ist, da der alte Baustein auf dem Stand von 2009 basierte. Sehr wenige Anforderungen können mit den alten Maßnahmen vollständig abgedeckt werden. Die Bewertung 3 für den Großteil der Anforderungen bedeutet allerdings nicht, dass diese pauschal noch zusätzlich beim Anwender umgesetzt werden müssen. Vielmehr fand sich die konkrete Forderung nicht im bisherigen Baustein. So definiert beispielsweise SYS.2.3.A19 die Anforderung einer Festplattenverschlüsselung mittels bestimmter Methoden beziehungsweise Tools. Dieser Aspekt wurde in den Maßnahmen der 15. EL nicht so detailliert betrachtet. Hier muss der Anwender unter Berücksichtigung der Hinweise zu möglichen Maßnahmen aus der 15. EL im Einzelfall prüfen, ob diese Anforderungen bereits umgesetzt sind.

Beispiel 3: Neue Bausteine

Schließlich gibt es vollkommen neue Bausteine, etwa APP.1.1 *Office-Produkte* oder SYS.3.2.2 *Mobile Device Management (MDM)*. Hierfür sind keine Migrationstabellen vorgesehen. Es sollte allerdings überprüft werden, ob es für diese Themengebiete bisher benutzerdefinierte Bausteine gab. Diese sollten dann mit den neuen Bausteinen abgeglichen werden.

Es wird auch weiterhin Themenbereiche geben, die durch die IT-Grundschutz-Bausteine nicht abgedeckt sind. Wenn dafür in der Institution benutzerdefinierte Bausteine entwickelt wurden, ist es sinnvoll, diese an das BSI weiterzugeben, damit sie der IT-Grundschutz-Community zur Verfügung gestellt werden können. Auf Wunsch anonymisiert das BSI solche Zulieferungen oder hebt die Autoren lobend hervor.

Hinweis: Die Migrationstabellen sind eine komplexe Arbeit, in der viele durchgeführte Änderungen abgebildet wurden. Trotz intensiver Qualitätssicherung können sich darin noch Fehler verstecken. Wenn Sie Unstimmigkeiten finden, informieren Sie uns bitte per E-Mail : grundschutz@bsi.bund.de.

Literaturverzeichnis

[27005] ISO/IEC 27005:2011, Information technology –Security techniques –Information security risk management, ISO/IEC JTC 1/SC 27, 2011

[31000] ISO/IEC 31000:2009, Risk management – Principles and guidelines, ISO/TC 262, 2009

[AUD] Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz, Auditierungsschema, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.0, Oktober 2017

[BSI1001] Managementsysteme für Informationssicherheit (ISMS), BSI-Standard 100-1, Version 1.5, Mai 2008

[BSI1002] IT-Grundschutz-Vorgehensweise, BSI-Standard 100-2, Version 2.0, Mai 2008

[BSI1003] Risikoanalyse auf der Basis von IT-Grundschutz, BSI-Standard 100-3, Version 2.5, Mai 2008

[BSI2001] Managementsysteme für Informationssicherheit (ISMS), BSI-Standard 200-1, Version 1.0, Oktober 2017

[BSI2002] IT-Grundschutz-Methodik, BSI-Standard 200-2, Version 1.0, Oktober2017

[BSI2003] Risikoanalyse auf der Basis von IT-Grundschutz, BSI-Standard 200-3, Version 1.0, Oktober 2017

[FRIST] Übergangsfristen und Migration im Rahmen der Zertifizierung, Bundesamt für Sicherheit in der Informationstechnik (BSI), August 2017

[GSKO] IT-Grundschutz-Kompendium, BSI, jährlich neu, https://www.bsi.bund.de/grundschutz

[GSM] Modernisierung des IT-Grundschutzes, BSI, https://www.bsi.bund.de/gs-modernisierung

[GST] Alternative IT-Grundschutz-Tools, BSI, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/GSTOOL/AndereTools/anderetools_node.html

[OUT] IT-Grundschutz-Methodik im Kontext von Outsourcing, Bundesamt für Sicherheit in der Informationstechnik, Version 1.0, Oktober 2017

[PRUEF] Prüfgrundlage für Zertifizierungen nach ISO 27001 auf der Basis von IT-Grundschutz, Version 3.1, Februar 2018

[ZERT] Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz, Zertifizierungsschema, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.0, September 2017