A. IT-Grundschutz-Profil

A.1. Formale Aspekte

Titel:	IT-Grundschutz-Profil für einen großen IT-Dienstleister
Autor:	Christoph Möhring
Herausgeber:	Christoph Möhring
Registrierungsnummer:	zu vergeben
Versionsstand:	Working Draft, Version 0.1 vom 14. März 2018
Revisionszyklus:	jährlich
Vertraulichkeit:	öffentlich
Anerkennung durch BSI:	in Diskussion

A.2. Management Summary

A.2.1. Zielgruppe

Dieses Profil richtet sich an große IT-Dienstleister[1] die charakterisiert sind durch

- einen erwirtschafteten Jahresumsatz von mindestens 50 Millionen Euro (brutto) oder
- einen Mitarbeiterstamm von mindestens 250 Mitarbeitern oder
- eine Verteilung über mindestens 5 verschiedene Standorte

sowie zu erbringende Dienstleistungen für mehrere unterschiedliche Kunden und die Realisierung der damit verbundenen Anforderungen bezüglich sicherheitsrelevanter Aspekte.

A.2.2. Zielsetzung

Das Profil definiert Mindest-Vorgaben an ein stabiles und nachhaltiges Informationssicherheits-Management sowie einen IT-Betrieb im Rahmen der anforderungsgerechten Realisierung der Schutzziele **Verfügbarkeit**, **Vertraulichkeit** und **Integrität** unter besonderer Berücksichtigung der auf den Systemen des IT-Dienstleisters gespeicherten und verarbeiteten Kundendaten. Mit der Umsetzung erfolgt eine Realisierung der BSI-IT-Grundschutz-Vorgehensweise hin zu einer

[1] Die Begrifflichkeiten „IT-Service-Provider“ und „IT-Dienstleister“ werden synonym gebraucht.

Basis-Absicherung.

Aufgrund der anzunehmenden komplexen Strukturen und vielschichtigen Ausprägungen innerhalb einzelner Organisationen ist zwingend eine Reduktion auf einen zu definierenden Ausschnitt des Informationsverbundes notwendig. Durch diese Maßnahme wird es ermöglicht, die gegebenen Anforderungen vielfach umsetzbar darzustellen. Es wird empfohlen, dieses Profil im Rahmen der initialen Realisierung einer Sicherheitskonzeption anzuwenden.

Grundsätzlich richten sich die Anforderungen dieses Profils nur an die IT-Dienstleister/IT-Service-Provider. Die nachfolgenden Vorgaben decken dabei ausschließlich den jeweiligen eigenen Informationsverbund ab. Eine direkte Auswirkung auf die betreuten Kunden ist nicht vorgesehen. Allerdings sind die IT-Dienstleister im Rahmen ihrer vertraglichen Vereinbarungen und Pflichten verantwortlich für die sichere und korrekte Verarbeitung der ihnen überantworteten Kundendaten innerhalb ihrer Informationsverbünde und ihrer jeweiligen Zuständigkeit.

A.3. Geltungsbereich (Scope)

A.3.1. Zielgruppe

Das Profil richtet sich sowohl an Organisationen der öffentlichen Hand als auch der freien Wirtschaft, die ihren Geschäftszweck in der Bereitstellung von IT-Dienstleistungen für Dritte haben. Hierbei werden insbesondere die Institutionen angesprochen, die die nachfolgenden Kriterien erfüllen:

- Erwirtschaftung eines einen Jahresumsatzes von mindestens 50 Millionen Euro (brutto) oder
- Mitarbeiterstamm von mindestens 250 Mitarbeitern oder
- Verteilung über mindestens 5 verschiedene Standorte.

Die Auswahlkriterien wurden aufgrund der festzustellenden Unterschiede innerhalb der Zielgruppe selbst so festgelegt, um möglichst Organisationen aus allen Bereichen der Wirtschaft und der öffentlichen Hand adressieren zu können. Weiterhin relevant ist für die Zielgruppe dieses Profils die Betreuung (vieler) verschiedener Kunden mit unterschiedlichen Anforderungen.

A.3.2. Schutzbedarf

Bei dem im Rahmen der Umsetzung dieses Profils realisierbaren Schutzbedarfes, handelt es sich um den Standard-Schutzbedarf „**NORMAL**“ für Systeme und Netzwerk-Topologien. Dabei

werden ausschließlich Daten mit **normalen** Anforderungen an die o. g. Schutzziele verarbeitet[2]. Das umgesetzte Profil erlaubt im Rahmen dieser Anforderung eine Grund-Sicherheit als umgesetzt zu betrachten. Jegliche darüber hinausgehende Anforderungen an Aspekte der Informationssicherheit oder des Geheimschutzes etc. müssen gesondert betrachtet und das Delta mit ergänzenden Maßnahmen behandelt werden.

A.3.3. IT-Grundschutz-Vorgehensweise

Die im Rahmen dieses Profils dargestellten Anforderungen sind Empfehlungen für große IT-Dienstleister. Sie decken die Anforderungen der **Basis-Absicherungen** des BSI-Standards 200-1[3] und der entsprechenden Vorgehensweise gemäß IT-Grundschutz ab. Unter Berücksichtigung der gegenwärtigen Überarbeitung des BSI-IT-Grundschutzes wird für die Entwicklung dieses Profils bereits auf die Bausteine des IT-Grundschutz-Kompendiums zurückgegriffen. Mit der Veröffentlichung weiterer Regelungsaspekte in diesem Zusammenhang erfolgt, sofern sinnvoll und geboten, deren Einarbeitung.

Aufgrund der vorhandenen Komplexität größerer Informationsverbünde können im Rahmen dieses Profils lediglich grundsätzliche Anforderungen an die Sicherheit berücksichtigt werden. Damit einhergehend ist die bewusste Auswahl der **Basis-Absicherung** als Vorgehensweise. Für die Abbildung darüber hinausgehender Anforderungen, beispielsweise die Umsetzung einer Standard-Absicherung und einer sich daran anknüpfenden Zertifizierung, müssen durch die Verantwortlichen weiterführende Schutzmaßnahmen realisiert werden. Die Umsetzung des hier vorliegenden Profils allein genügt nicht für eine Verbund-Zertifizierung „ISO27001 auf Basis IT-Grundschutz“. Entsprechende Audits sind jedoch möglich.

Es ist vorzusehen, dass im Rahmen der Absicherung des Informationsverbundes das weitere Vorgehen festgelegt wird. Hieraus sollten sich belastbare Planungen, bezogen auf die Überführung hin zu einer Standard-Absicherung, ableiten. In Vorbereitung darauf und unter Berücksichtigung der Verantwortung der Zielgruppe gegenüber ihren Kunden, werden im Rahmen dieses Profils, neben den zwingend umzusetzenden Basis-Anforderungen, bereits für verschiedene Aspekte die weiterführenden Standard-Anforderungen verbindlich vorgegeben. Den aufgeführten zusätzlichen Anforderungen liegt die Überlegung zugrunde, dass einer sinnvollen Abbildung der organisatorisch und technischen Umsetzung notwendiger Regelungen und Abläufe Rechnung getragen wird.

Abdeckung Vorgehensweise:	Basis
ISO 27001-Kompatibilität:	ja
Rahmenbedingungen:	Anwendung des IT-Grundschutz-Kompendiums

[2] Jeweils für die Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität.

[3] Vgl.https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_2.pdf?___blob=publicationFile&v=5, S. 61-67, 13.01.2018

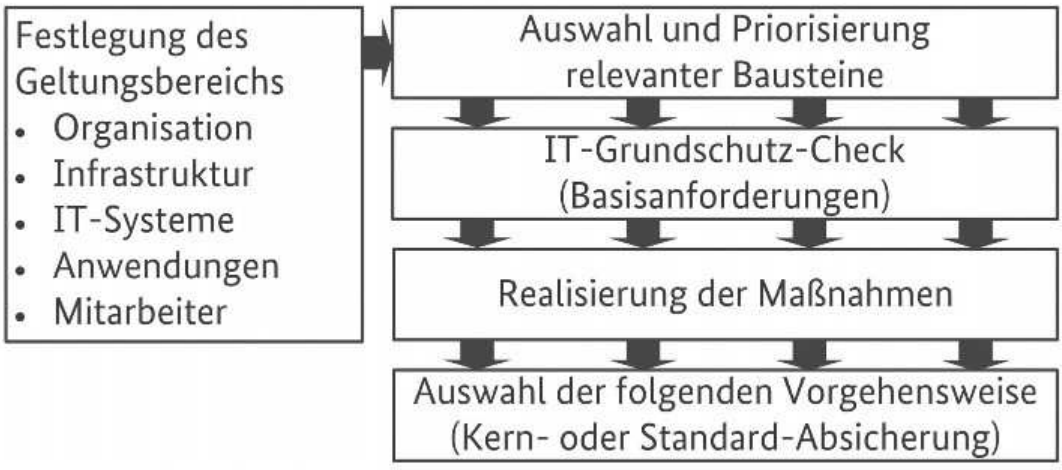

Abbildung : Basis-Absicherung [1]

A.4. Relevante Bausteine, Anforderungen und Maßnahmen

A.4.1. Bestandteile des Informationsverbundes

Die Idee eines generischen IT-Grundschutz-Profils ist es, dieses möglichst pauschal auf gleichartige Organisationen anzuwenden. Im Rahmen der betrachteten Ausprägung „**großer IT-Dienstleister**“ wird daher davon ausgegangen, dass die relevanten Organisationen ähn- liche Rahmenbedingungen erfüllen und in ihren Grundstrukturen vergleichbar sind. Gestützt wird diese Annahme auf den Fakt, dass sie vergleichbaren gesetzlichen Regelungen (IT- Sicherheitsgesetz, Datenschutz-Gesetze) und sonstigen normativen Vorgaben unterliegen. Weiterhin ist davon auszugehen, dass alle diese Organisationen ihren IT-Betrieb in gleichar- tiger Weise, beispielsweise durch einen Rückgriff auf ITIL, organisieren. Ferner benötigen sie Ablauf-Prozesse, die zur Optimierung des Betriebes kontinuierlich angepasst werden und stetig in ihren Abläufen reifen. Selbiges gilt für den Aufbau eines stabilen und nachhaltig wirksamen Informationssicherheits-Managements.

A.4.2. Nicht berücksichtige Objekte

Irrelevant bei der Betrachtung sind die jeweils konkreten Details innerhalb der Einzel- Organisation an sich. Um das Profil anzuwenden, ist daher eine gewisse Abstraktion notwendig. Diese stellt sicher, dass die benötigte Betrachtungsmenge erhalten werden kann. Für die Be-wertung des jeweiligen Deltas wird folglich eine gesonderte Bewertung der Institution, außerhalb des Regelungsbereiches des Profils, notwendig. Nicht berücksichtigt werden weiterhin konkrete organisatorische Ausprägungen, Details-Fragen der technischen Ausstattung des einzelnen Mitarbeiters/der einzelnen Mitarbeiterin,

[1] Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_2.pdf?__blob=publicationFile&v=5 ; Seite 61, 14.03.2018

konkrete technische Fragen des Betriebes und der Netztechnik, Anwendungen etc. Ebenfalls nicht berücksichtigt

werden die technischen und organisatorischen Aspekte auf Seiten der Kunden sowie Anforderungen, die über eine Basis- Absicherung hinausgehen.

A.4.3. Verweis auf andere IT-Grundschutz-Profile

Entfällt aktuell.

Es ist denkbar, für die innerhalb dieses Profils nicht berücksichtigten Aspekte weitere, eigenständige Profile zu erarbeiten. Diese könnten dann das hier vorliegende Profil ergänzen und den betrachteten Informationsverbund vervollständigen. Es ist weiterhin zu prüfen, ob die Testierung der Profil-Umsetzung durch eine dritte Stelle möglich ist.

A.5. Referenzarchitektur / Untersuchungsverbund

Das vorliegende IT-Grundschutz-Profil betrachtet innerhalb des zu untersuchenden Infor-ma tionsverbundes alle wesentlichen Objekte, wie unter Bestandteile des Informationsverbundes dargestellt. Eine Reduktion des Betrachtungsumfanges erfolgt aufgrund der für die gebotene Generalität notwendigen Eingrenzung. Der Betrachtung zugrundegelegt wird folgendes gene- risches Netzwerkdiagramm:

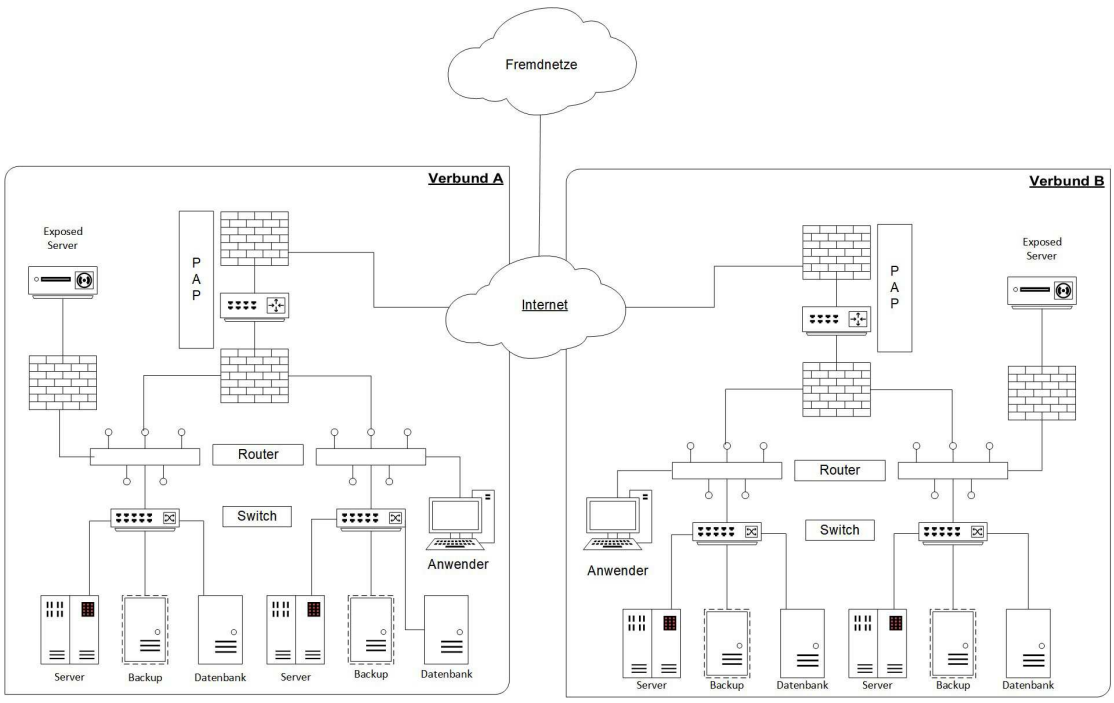

Abbildung: Generischer Netzplan

Die Abbildung ist hierbei bewusst abstrakt gehalten, um ein möglichst großes Spektrum an Aus-

prägung zu gewährleisten. Im Rahmen der Profilumsetzung erfolgt eine konkrete Betrachtung der nachfolgend aufgezählten Bausteinschichten. Die innerhalb der Einzel-Bausteine aufgeführten **Basis-Anforderungen** (**MUSS**) sind grundsätzlich umzusetzen. Die zusätzlich dazu definierten Standard-Anforderungen (**SOLL**) sind ebenfalls wie vorgegeben zu realisieren. Anmerkungen zu einzelnen Bausteinen werden explizit ausgeführt und deren Umsetzung kurz erläutert. Sofern im Einzelfall bereits eine höhere Absicherungsnotwendigkeit besteht, sind die diesbezüglich zusätzlichen Anforderungen des höheren Schutzbedarfes ebenfalls umzusetzen.

A.5.1. Untersuchungsrelevante Aspekte der ISMS-Schicht

Baustein	Basis-Anforderungen (MUSS)	Standard-Anforderungen (SOLL)
ISMS.1 Sicherheitsmanagement	ja	mit Anmerkungen

Tabelle A.1.: Untersuchungsrelevante Bausteine Bereich ISMS

Anmerkungen:

ISMS.1.A15 - Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit

Die Forderung ist unter Umständen für Einzel-Organisationen schwierig bezifferbar. Trotzdem müssen Maßnahmen hinsichtlich der Umsetzung einer wirksamen Informationssicherheit in einem wirtschaftlichen Verhältnis stehen. Da dies jedoch in einem Gesamt-Kontext der sonstigen wirtschaftlichen Ausprägung der jeweiligen Organisation steht, sind die entsprechenden Rahmenbedingungen zu berücksichtigen.

A.5.2. Untersuchungsrelevante Aspekte der Prozess-Schicht

Baustein	Basis-Anforderungen (MUSS)	Standard-Anforderungen (SOLL)
ORP.1 Organisation	ja	mit Anmerkungen
ORP.2 Personal	ja	mit Anmerkungen
ORP.3 Sensibilisierung und Schulung	ja	mit Anmerkungen
ORP.4 Identitäts- und Berechtigungsmanagement	ja	ja
ORP.5 Compliance Management (Anforderungs-Management)	ja	ja

Tabelle A.2.: Untersuchungsrelevante Bausteine Bereich ORP

Anmerkungen:

ORP.1.A6 - Der aufgeräumte Arbeitsplatz

Unbestritten ist die gebotene Notwendigkeit einer solchen Forderung im Rahmen der Umsetzung einer gebotenen Sorgfaltspflicht. Im Rahmen einer Initialerstellung eines grundsätzlichen Sicherheitsniveaus ist dies nachrangig regelungsrelevant, da andere Maßnahmen zu einer deutlich intensiveren Sicherheitsentfaltung führen.

ORP.1.A8 - Betriebsmittelverwaltung

Eine Regelung bezüglich der zum Einsatz kommenden Betriebsmittel ist nachrangig zu betrachten. Insbesondere das Fehlen von Betriebsmitteln in ausreichender Menge ist sicherlich für einen stabilen Betrieb nicht zielführend, grenzt die Gesamtsicherheit allerdings nur marginal ein.

ORP.2.A10 - Vermeidung von Störungen des Betriebsklimas

Diese Forderung ist insgesamt nachvollziehbar, allerdings in ihrer Umsetzung subjektiv geprägt. Daher scheint eine nachrangige Berücksichtigung aus Sicht der Informationssicherheit vertretbar. Dies insbesondere unter dem Aspekt der erfolgreichen Umsetzung der anderen Vorgaben des Bausteins ORP.2.

ORP.3.A8 - Messung und Auswertung des Lernerfolgs

Im Kontext des Aufbaus einer funktionsfähigen und sicheren Umgebung scheint es wichtiger, die Maßnahmen zu realisieren, die das System als Startbedingungen benötigt. Maßnahmen mit eher messendem Charakter sind für eine iterative Verbesserung unabdingbar, in der Realisierungsphase jedoch noch nicht zwingend notwendig in ihrer Umsetzung.

Baustein	Basis-Anforderungen (MUSS)	Standard-Anforderungen (SOLL)
CON.1 Kryptokonzept	ja	ja
CON.2 Datenschutz	ja	ja
CON.3 Datensicherungskonzept	ja	mit Anmerkungen
CON.4 Auswahl und Einsatz von Standardsoftware	ja	ja
CON.5 Entwicklung und Einsatz von Fachanwendungen	ja	ja
CON.6 Löschen und Vernichten	ja	ja

Tabelle A.3.: Untersuchungsrelevante Bausteine Bereich CON

Anmerkungen:

CON.3.A10 - Verpflichtung der Mitarbeiter zur Datensicherung

Datensicherung kann nur dann funktionieren, wenn diese im Rahmen automatisierter Prozesse abläuft. Eine manuelle Sicherung mag im Einzelfall funktionieren und sollte auch möglich sein, kann allerdings nicht die Grundlage für die Umsetzung diesbezüglicher Anforderungen im Rahmen der Diensteerbringung durch einen IT-Dienstleister sein. Von daher sollte die Maßnahme inhaltlich automatisiert werden. Natürlich stellt dies den/die einzelne/n Mitarbeiter/in nicht von der Pflicht frei, die ihm/ihr obliegenden Sorgfaltspflichten wahrzunehmen.

Baustein	Basis-Anforderungen (MUSS)	Standard-Anforderungen (SOLL)
OPS.1.1.2 Ordnungsgemäße IT-Administration	ja	teilweise
OPS.1.1.3 Patch- und Änderungsmanagement	ja	ja
OPS.1.1.4 Schutz vor Schadprogrammen	ja	ja
OPS.3.1 Outsourcing für Dienstleister	ja	Mit Anmerkungen

Tabelle A.4.: Untersuchungsrelevante Bausteine Bereich OPS

Anmerkungen:

OPS.1.1.2.A9 - Ausreichende Ressourcen für den IT-Betrieb

Natürlich kann ohne die Bereitstellung von qualifiziertem Personal kein Informationsverbund fach- und sachgerecht betrieben werden. Jedoch ist die hier vorgelegte Forderung nicht

bezifferbar und damit nicht messbar umzusetzen. Weiterhin verändern sich mit Betriebsverlauf die Anforderungen an die Quantität des Personals, so dass die Maßnahme kaum nachweisbar erfolgreich umsetzbar scheint. Unter Berücksichtigung dieser Feststellung scheint es angezeigt, die Umsetzung der Maßnahme zeitlich dahingehend nachrangig zu realisieren, um eine Berechnungsmatrix aufzubauen.

OPS.1.1.2.A13 - Absicherung von Fernwartung

Die Forderung, Fernwartung nur von lokalen Systemen aus zu initiieren, ist dahingehend umzusetzen, dass Fernwartungszugriffe nur von IT-Systemen des jeweiligen Informationsverbundes erfolgen. Das bedeutet, dass bei verteilten Systemen eines IT-Dienstleisters, auch über mehrere Standorte hinweg, der Zugriff erfolgen kann, sofern die Übertragung gesichert ist. Ausgeschlossen ist jedoch die Fernwartung unter Nutzung Verbund-fremder Systeme, die nicht unter der eigenen Kontrolle stehen (z. B. bereitgestellte Jump-Hosts im Internet). Der Charakter einer Fernwartung ist gerade die Möglichkeit des abgesetzten Zugriffs und damit eben nicht von lokaler Stelle.

OPS.3.1.A6 - Regelungen für den Einsatz von Fremdpersonal

Der Umstand, ob der IT-Dienstleister im Rahmen der Leistungserbringung weiteres Fremdpersonal zum Einsatz bringen darf, muss Gegenstand der vertraglichen Vereinbarungen zwischen Dienstleister und Kunde zu sein.

A.5.3. Untersuchungsrelevante Aspekte der System-Schicht

Baustein	Basis-Anforderungen (MUSS)	Standard-Anforderungen (SOLL)
INF.1 Allgemeines Gebäude	ja	ja
INF.2 Rechenzentrum sowie Serverraum	ja	ja
INF.3 Elektrotechnische Verkabelung	ja	ja
INF.4 IT-Verkabelung	ja	ja
INF.7 Büroarbeitsplatz	ja	ja

Tabelle A.5.: Untersuchungsrelevante Bausteine Bereich INF

Anmerkungen:

Keine.

Baustein	Basis-Anforderungen (MUSS)	Standard-Anforderungen (SOLL)
NET.1.1 Netzarchitektur und -design	ja	ja
NET.1.2 Netzmanagement	ja	ja
NET.3.1 Router und Switches	ja	ja
NET.3.2 Firewall	ja	ja
NET.3.3 VPN	ja	ja

Tabelle A.6.: Untersuchungsrelevante Bausteine Bereich NET

Anmerkungen:

Keine.

A.5.4. Untersuchungsrelevante Aspekte der DER-Schicht

Baustein	Basis-Anforderungen (MUSS)	Standard-Anforderungen (SOLL)
DER.1 Detektion von sicherheitsrelevanten Ereignissen	ja	ja
DER.2.1 Behandlung von Sicherheitsvorfällen	ja	ja
DER.4 Notfallmanagement	ja	ja

Tabelle A.7.: Untersuchungsrelevante Bausteine Bereich DER

Anmerkungen:

DER.1.A10 - Einsatz von TLS/SSH-Proxies

Der Mehrwert dieser Geräte ist hinsichtlich ihrer Arbeitsweise umstritten, da vorhandene Mängel dieser Geräte zu einer Reduktion der kompletten Umgebung führen. Unter diesem Aspekt sollte der Einsatz sehr genau geprüft und bewertet werden. Unbedingt ist auf eine korrekte Konfiguration dieser Geräte zu achten. Weiterhin sollten im Falle des Einsatzes derartiger Geräte geeignete Ausgleichsmaßnahmen geschaffen werden.

A.6. Umgang mit Abweichungen

Die vorgenannten Aspekte sind grundsätzlich im Rahmen der Profilumsetzung zu betrachten und die diesbezüglich bestehenden Anforderungen umzusetzen. Sollte jedoch im Einzelfall eine

Realisierung unmöglich oder nicht zielführend sein, erfolgt eine entsprechende Risikobetrachtung, wie in Kapitel A.7 dargestellt. Gleiches gilt für Abweichungen innerhalb der einzelnen Schutzbedarfe über normal hinaus.

A.7. Restrisikobetrachtung / Risikobehandlung

Die umzusetzenden Maßnahmen und zu berücksichtigenden Aspekte bilden die Grundlage für den Aufbau und Betrieb eines Informationsverbundes zur Bereitstellung von IT-Dienstleistungen mit normalen Anforderungen an die Schutzziele der Informationssicherheit. Jegliche Abweichung davon ist im Einzelfall detailliert hinsichtlich der zusätzlichen Risiken zu bewerten und durch geeignete weitere eigene Maßnahmen zu ergänzen.

A.8. Anwendungshinweise

Die festgelegten Anforderungen sind im Rahmen des Gesamtsicherheitskonzeptes zu integrieren und geeignet umzusetzen. Im Zuge der festzulegenden Revisionszyklen sind die getroffenen Entscheidungen und Maßnahmen regelmäßig auf ihre Aktualität und Geeignetheit zu überprüfen und ggf. anzupassen.

A.9. Unterstützende Informationen

Zur Vereinfachung und zur Einordnung wird davon ausgegangen, dass das Schichtenmodell des bisherigen Grundschutzes als bekannt vorausgesetzt werden kann:

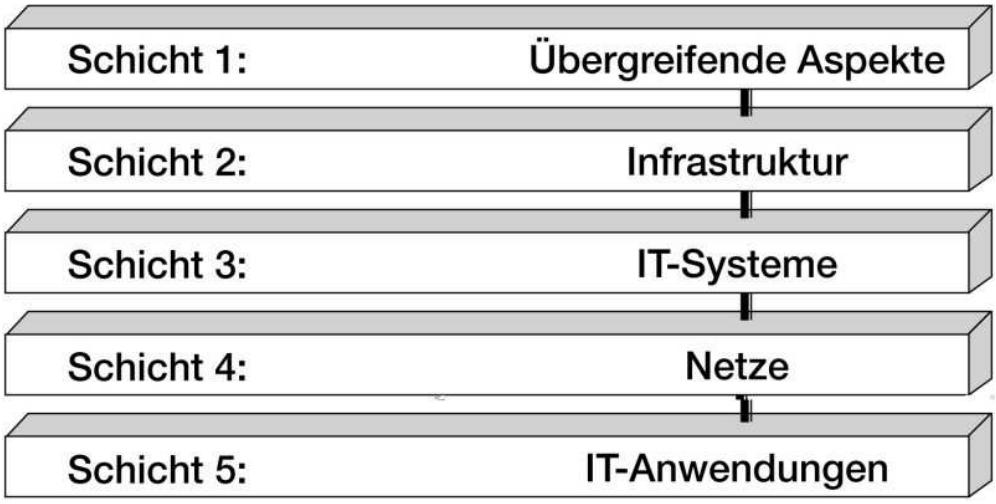

Abbildung A.3.: Schichtenmodell alter BSI-Grundschutz (Quelle: Schicht.2016, S. 2)

Aufgrund der getroffenen Festlegungen und notwendigen Einschränkungen deckt das Profil gedanklich die Schichten 1 und 2, und damit die Grundstruktur eines IT-Dienstleisters, ab.

Die Betrachtungsgrenze verläuft zwischen den Schichten 2 und 3. Es müssen jedoch aufgrund bestehender logischer und technisch notwendiger Einzel-Aspekte auch Anforderungen der anderen Schichten berücksichtigt werden. Zu dem betrachteten Teil-Informationsverbund gehören somit die wesentlichen Funktionalitäten der organisationsübergreifenden Regelungen, des Informationssicherheits-Managements und der Infrastruktur. Mit der erweiterten **Basis-Absicherung** der elementaren Strukturen – als Grundlage der zu erbringenden IT-Dienstleistungen – kann der sichere und nachhaltig stabile IT-Betrieb sowie die gesicherte Umsetzungsgrundlage der Anforderungen an die Verfügbarkeit, Vertraulichkeit und Integrität der Daten initial sichergestellt werden.

Wie bereits beschrieben, orientiert sich das vorliegende Profil allerdings ausschließlich an dem überarbeiteten und im Oktober 2017 freigegebenen BSI-Grundschutz-Kompendium. Daher ist eine entsprechende Transformation des Bisherigen hin zu den nunmehr gültigen Regelungen notwendig. Insbesondere orientiert sich der aktualisierte IT-Grundschutz mehr an einem Prozess- und Service-Gedanken und lässt sich deutlich agiler im Kontext der ISO27001ff. einsetzen.
In diesem Kontext erfuhr auch das Schichtenmodell eine Überarbeitung mit entsprechender Gliederung:

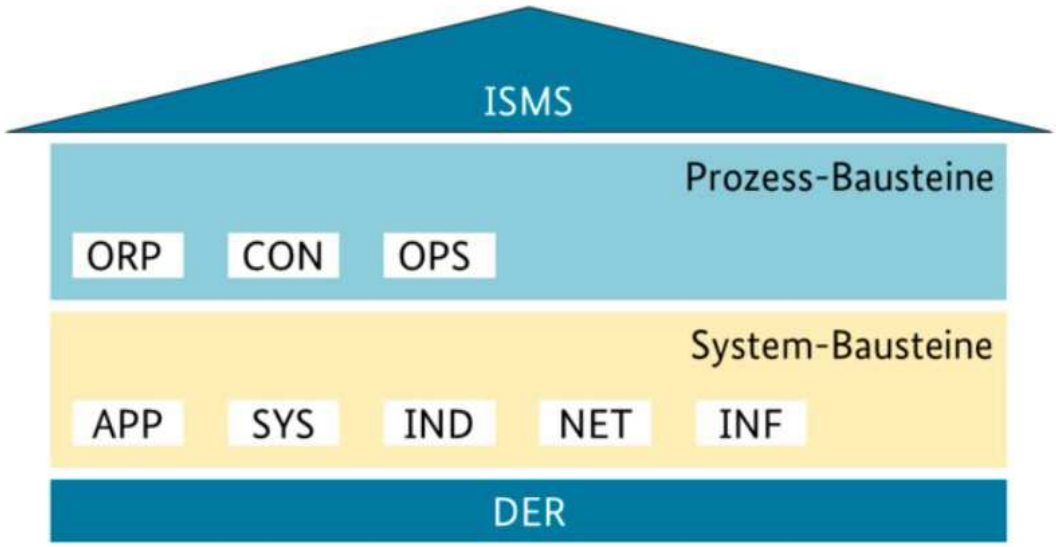

Abbildung A.4.: Schichten-Modell neuer BSI-Grundschutz (Quelle: SchichtenM.2017, S. 2)

Ferner wurden die bisherigen IT-Grundschutz-Bausteine umbenannt, neu strukturiert und teilweise ergänzt. Diese gliedern sich innerhalb des aktualisierten Grundschutzes in die nachfolgenden Bereiche

- ISMS - Sicherheitsmanagement
- ORP - Organisation und Personal

- CON - Konzeption und Personal
- OPS - Betrieb
- APP - Anwendungen
- SYS - IT-Systeme
- IND - Industrielle IT
- NET - Netze und Kommunikation
- INF - Infrastruktur
- DER - Detektion und Reaktion.

Wie oben dargestellt, sind zum heutigen Zeitpunkt im Rahmen der IT-Grundschutz-Profil-Umsetzung nicht alle Baustein-Schichten sowie aus den relevanten Schichten nicht alle Bausteine bzw. Maßnahmen für eine Initialisierung des Sicherheitsniveaus relevant. Es sei allerdings angemerkt, dass es im Interesse des Anwenders liegt, im Zuge der Realisierung regelmäßig zu prüfen, ob es Neuerungen und/oder Anpassungen der Anforderungen gab. Als Quelle für aktuelle Informationen sei daher die Webseite des BSI empfohlen[4]. Jederzeit können die dort aufgeführten Forderungen bei Bedarf um eigene, speziell auf den jeweiligen Informationsverbund angepasste Maßnahmen ergänzt werden.

[4]https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html, 06.01.2018