

# **IT-Grundschatz-Profil für die obersten Landesbehörden Deutschlands**

<b>Autor:</b>	<b>Raphael Grieger</b>
<b>Institution:</b>	<b>FH Hagenberg</b>
<b>Veröffentlichungsstatus:</b>	<b>Final</b>
<b>Version:</b>	<b>1.0</b>
<b>Datum:</b>	<b>31.05.2019</b>

# Inhaltsverzeichnis

<b>Kapitel 1 Management Summary</b>	<b>1</b>
<b>Kapitel 2 Geltungsbereich</b>	<b>2</b>
<b>Kapitel 3 Betrachteter Informationsverbund</b>	<b>3</b>
<b>Kapitel 4 Referenzarchitektur</b>	<b>4</b>
4.1 Geschäftsprozesse .....	4
4.2 Anwendungen .....	4
4.3 IT-Systeme .....	5
4.4 Netze- und Kommunikation .....	5
4.5 Räumliche Infrastruktur .....	5
4.6 Netzplan .....	7
<b>Kapitel 5 Modellierung des Informationsverbunds</b>	<b>8</b>
5.1 Kreuzreferenztafel .....	8
5.2 Prozess-Bausteine .....	9
5.2.1 Schicht ISMS .....	9
5.2.2 Schicht ORP .....	9
5.2.3 Schicht CON .....	10
5.2.4 Schicht OPS .....	10
5.2.5 Schicht DER .....	10
5.3 System Bausteine .....	11
5.3.1 Schicht APP .....	11
5.3.2 Schicht SYS .....	11
5.3.3 Schicht NET .....	12
5.3.4 Schicht INF .....	12
<b>Kapitel 6 Schutzbedarfe</b>	<b>14</b>
6.1 Schutzbedarfskategorien .....	14
6.2 Schutzbedarfsfeststellung .....	15
6.2.1 Schutzziel Vertraulichkeit .....	15
6.2.2 Schutzziel Integrität .....	17
6.2.3 Schutzziel Verfügbarkeit .....	19
6.3 Zielobjekte für die Risikoanalyse .....	22
<b>Kapitel 7 Risikobetrachtung relevanter Zielobjekte</b>	<b>23</b>
7.1 Risikokriterien .....	23
7.2 Risikoappetit einer obersten Landesbehörde .....	23
7.2.1 Risikomatrix .....	24
7.2.2 Bewertungskategorien der Risiken .....	24
7.3 Risikoanalyse .....	24

7.3.1	Gefährdungen für den Dateiserver .....	25
7.3.2	Risikoeinschätzung und Risikobewertung .....	26
7.3.3	Risikobehandlung.....	27
<b>Kapitel 8</b>	<b>Anwendungshinweise</b>	<b>31</b>
8.1	Andere IT-Grundschatz-Profile .....	31
8.2	Internationale ISMS-Standards.....	31
8.3	Weiterentwicklung des IT-Grundschatz-Profls .....	31
<b>Kapitel 9</b>	<b>Literatur</b>	<b>32</b>

# Kapitel 1                      Management Summary

Dieses IT-Grundschatz-Profil bildet die Anforderungen einer Sicherheitskonzeption einer obersten Landesbehörde in Deutschland für die Absicherung des Geschäftsprozesses der „Beteiligung an der Normsetzung des Landes“ nach der Standard-Absicherung ab. Dazu wird die für den Geschäftsprozess benötigte Referenzarchitektur dargestellt und mit den IT-Grundschatz-Bausteinen modelliert. Zudem werden die Schutzbedarfe der Zielobjekte aufgelistet und es wird eine schematische Risikoanalyse und -behandlung des Dateiservers angefertigt. Neben den Anforderungen der IT-Grundschatz-Bausteine werden Anmerkungen von Verantwortlichen für Informationssicherheit aufgeführt, die spezifisches Wissen aus diesem Anwendungsbereich der Informationssicherheit widerspiegeln.

Durch diese schematische Sicherheitskonzeption wird die Umsetzung einer Standard-Absicherung der Beteiligung an der Normsetzung des Landes durch die Vorauswahl passender IT-Grundschatz-Bausteine vereinfacht. Nach der Modellierung wird zudem eine Risikoanalyse des Dateiservers aufgrund eines erhöhten Schutzbedarfes durchgeführt. Diese Risikoanalyse führt zu der Feststellung zusätzlicher Maßnahmen, um dem erhöhten Schutzbedarf des Zielobjektes gerecht zu werden.

Die Anwender dieses IT-Grundschatz-Profiles können die festgestellten Zielobjekte, Schutzbedarfe und Anforderungen als Grundlage für ihre Sicherheitskonzeption verwenden und individuell auf ihre Organisation anpassen. Die Landesrechnungshöfe als oberste Landesbehörden werden aufgrund divergierender Aufgaben und der gesetzlichen Unabhängigkeit von dem IT-Grundschatz-Profil nicht umfasst.

## Kapitel 2                    Geltungsbereich

Gemeinhin stellen die obersten Landesbehörden einen zentralen Teil der Landesverwaltungen dar und werden als Ministerien, Senate oder Staatskanzleien bezeichnet. Diese Behörden bilden in den Ländern, unter der Leitung des Ministerpräsidenten und der jeweiligen Minister\*innen, die höchste Verwaltungsebene [1, S. 50].

Für die Absicherung ihres Informationsverbundes sollen die Verwaltungen des Bundes und der Länder, gemäß der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung vom 06.12.2018 (ISLL-Bund) ein Informationssicherheitsmanagementsystem (ISMS) betreiben und dort insbesondere eine Sicherheitskonzeption erstellen und umsetzen. Dazu wird in der ISLL-Bund die ISO 2700x-Reihe sowie der IT-Grundschutz als Mindeststandard definiert. Ausgenommen sind die Landesrechnungshöfe, die Landesdatenschutzbeauftragten und die Verwaltungen der Landtage. Daher werden diese Institutionen von dem IT-Grundschutz-Profil nicht betrachtet, auch wenn die Landesrechnungshöfe im weiteren Sinne zu den obersten Landesbehörden gezählt werden [2, S. 96].

Dieses IT-Grundschutz-Profil wendet die Methodik der Standard-Absicherung gemäß dem BSI-Standard 200-2 an, um die Umsetzung eines ISMS in einer obersten Landesbehörde durch ein schematische Sicherheitskonzeption zu unterstützen. Wie im Standard 200-2 angeführt, und vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in einer Referenztabelle weiter konkretisiert [3], ist die Standard-Absicherung des IT-Grundschutzes kompatibel zu dem ISO/IEC Standard 27001:2013. Dies trifft daher auch auf die Umsetzung dieses IT-Grundschutz-Profils zu, sofern für die Institution ein entsprechender Anwendungsbereich des ISMS definiert ist und organisationsspezifische Anpassungen getroffen wurden. Weiterhin kann über die Anwendung dieses IT-Grundschutz-Profils der Verpflichtung nach dem Betrieb eines ISMS und der Umsetzung der Sicherheitskonzeption nach der ISLL-Bund nachgekommen werden.

Dieses IT-Grundschutz-Profil verwendet stets die Begrifflichkeiten des IT-Grundschutzes. Selbiges gilt für methodische Angaben, wie die Verwendung der Worte MUSS und SOLL im Bezug zu einer Sicherheitsanforderung. Eine umfassende Begriffsdefinition befindet sich im Glossar des aktuellen IT-Grundschutz-Kompodiums.

## Kapitel 3                      Betrachteter Informationsverbund

Die Zuständigkeiten und Geschäftsbereiche der obersten Landesbehörden weichen auf Grund unterschiedlicher politischer Konstellationen und der grundsätzlichen Souveränität der Länder [4, S. 35] voneinander ab. Daher wird in diesem IT-Grundschutz-Profil keine tiefergehende Definition der Geschäftsprozesse vorgenommen, sondern es wird ein allgemein formulierter Geschäftsprozess betrachtet, der aus den Aufgaben der obersten Landesbehörden hergeleitet wird. Abstrakt formuliert nehmen die obersten Landesbehörden folgende Aufgaben wahr:

1. Das Erlassen von Verordnungen, Erlassen und die Mitarbeit an Gesetzen.
2. Die Ausführung von Bundes- und Landesgesetzen, sofern diese nicht an nachgeordnete Behörden delegiert ist.
3. Die (politische) Unterstützung des Ministers oder der Ministerin durch Informationsbeschaffung und sonstige Tätigkeiten.
4. Die Selbstverwaltung der Behörde durch strategische Planung, Pressearbeit und Personalsachen.
5. Die Aufsicht über nachgeordnete Behörden.
6. Die Wahrnehmung von sonstigen Aufgaben, wie Beantwortung von parlamentarischen Anfragen, Koordination von ressortübergreifenden Aufgaben sowie Öffentlichkeitsarbeit.

Insbesondere aus der ersten Aufgabengruppe wird der generische Geschäftsprozess der **Beteiligung an der Normsetzung des Landes** generiert und in einer Standard-Absicherung betrachtet. Dieser Geschäftsprozess umfasst, nicht abschließend aufgezählt, folgende Tätigkeiten:

- Die Kommunikation mit anderen Behörden, wie Kommunen und obersten Landesbehörden, zur Abstimmung der Inhalte in Gesetzgebungs-, Verordnungs- und Erlassverfahren.
- Wahrnehmung interner Kommunikationswege für die Steuerung der Aufgaben und Tätigkeiten sowie deren Bearbeitung im eigenen Bereich.
- Die fachliche Mitarbeit an den verschiedenen Normtypen, unter anderem durch die Erstellung von Gutachten, Stellungnahmen und Ausarbeitungen von Vorschlägen und Konzepten.

In den Folgekapiteln werden die für diesen Geschäftsprozess benötigten Zielobjekte in einer Referenzarchitektur aufgeführt, mit den IT-Grundschutz-Bausteinen modelliert und einer Schutzbedarfsfeststellung unterzogen. Zunächst wird der Informationsverbund in Form der Zielobjekte für diesen Geschäftsprozess dargestellt. Dabei ist zu bedenken, dass alle Landesverwaltungen Anteile der IT-Infrastruktur an externe IT-Dienstleister ausgelagert haben [5, S. 101]. In diesem IT-Grundschutz-Profil wird aufgrund unterschiedlicher Auslagerungsmodelle grundsätzlich von keiner Auslagerung ausgegangen. Wenn relevante Zielobjekte der Sicherheitskonzeption ausgelagert sind, müssen die entsprechenden Verantwortlichen die Anforderungen der Sicherheitskonzeption angepasst umsetzen. Weiteres dazu lässt sich dem IT-Grundschutz-Baustein OPS.2.1 (Outsourcing für Kunden) entnehmen.

Grundsätzlich werden andere Aufgaben einer obersten Landesbehörde ähnliche IT-Ressourcen benötigen und indirekt mit abgebildet sein. Dem Umfang dieser Ausarbeitung ist es geschuldet, dass an dieser Stelle nicht weiter auf diesen Umstand eingegangen wird. Bei Erstellung der Sicherheitskonzeption besteht allerdings für jeden Anwender die Prüfungsmöglichkeit, ob weitere Geschäftsprozesse so bereits abgedeckt werden oder ohne großen Mehraufwand abgedeckt werden können. Eine Risikoanalyse ist im Kontext der eigenen Organisation stets durchzuführen und wird hier nur beispielhaft für das Zielobjekt des Dateiservers aufgeführt.

## Kapitel 4 Referenzarchitektur

Bei der Darstellung der Referenzarchitektur wird davon ausgegangen, dass von den obersten Landesbehörden für diese „konzeptionelle“ Arbeit [6, S. 15] entweder Anwendungen der oder Bürokommunikation ein Vorgangsbearbeitungs- bzw. Dokumentenmanagementsystem (VBS; DMS) genutzt werden. In diesem IT-Grundschatz-Profil werden die Anwendungen der Bürokommunikation als zentrale Komponente zur Aufgabenerfüllung angenommen. Zusätzlich dazu werden in der Referenzarchitektur die Zielobjekte festgelegt, die zum Betrieb der Anwendungen der Bürokommunikation, der Nutzerverwaltung und der Aufgabenwahrnehmung benötigt werden.

Die Beschreibungen der Zielobjekte sind weitestgehend dem Lexikon der Informatik von Fischer [7] entnommen und sind nur im Bedarfsfall durch den Autor angepasst. Zum Teil enthält diese Aufzählung konkrete Soft- oder Hardwareprodukte (bspw. Windows 10 und Microsoft Exchange). Diese wurden aufgrund ihrer aktuellen Verbreitung in der heutigen IT-Landschaft, insbesondere in den öffentlichen Verwaltungen, ausgewählt (siehe u.a. [8–10]) und sind über die IT-Grundschatz-Bausteine modelliert.

### 4.1 Geschäftsprozesse

ID	Was	Beschreibung
PRO01	Beteiligung an der Normsetzung des Landes	Die oberste Landesbehörde beteiligt sich an dem landesinternen Gesetzgebungsprozess, dem Erlassen von Verordnungen und dem Fertigen von Erlassen.

### 4.2 Anwendungen

ID	Was	Beschreibung
APP01	Betriebssystem Windows 10	Für den Betrieb eines komplexen Rechners notwendiges Programm zur Verwaltung seiner Betriebsmittel, zur Datenkommunikation mit der Peripherie, als Verbindungsglied zwischen Anwender und Applikation. Hier ein weit verbreitetes Produkt der Fa. Microsoft für den Privat- und Geschäftskundenbereich.
APP02	Microsoft Office 2016	Anwendungen für Textverarbeitung, E-Mail-Client, Erstellen von Präsentationen, Tabellenkalkulationen.
APP03	Dateiserver	Ein zentral auf einer Servermaschine ausgeführtes Programmsystem, das alle Teilnehmenden mit Dateien versorgt und als Kollaborationsplattform dienen kann.
APP04	Web-Browser Firefox	Eine die HTML interpretierende Client-Applikation zum Durchsuchen und Präsentieren ausgewählter Bereiche wie FTP, Usenet und des World Wide Web.
APP05	Verzeichnisdienst Active Directory	Zentrale, einheitliche Datenbank über sämtliche menschlichen und maschinellen Ressourcen einer vernetzten Arbeitsumgebung sowie von Metadaten der ganzen IT einer Unternehmung: Namen, Adressen, Telefonnummern, Geräteparameter, Zugriffsrechte, Datenbeschreibungen, Spezifikationen, Routing-Informationen. Ziele eines Verzeichnisdienstes sind u. a. Single Sign-on-Lösungen, die unternehmensweite zentrale Pflege, die einheitliche Notation, ein vereinheitlichter Workflow, die mobile Datenverarbeitung oder die automatische Konfiguration von Komponenten durch Herauslesen von Informationen.
APP06	Microsoft Exchange	Client/Server-Lösung zur Erledigung der Bürokommunikation (Telefax, Stimme, E-Mail, Termine, Kontaktadressen, Aufgaben) in einem Arbeitskollektiv unter zentraler Verwaltung. Der Server heißt Exchange, der Client (bei Microsoft) Outlook.

APP07	Public-Key Infrastruktur	Zuständig für die authentische Übermittlung von Nachrichten und sichere Identifizierung von Sendern und Empfängern.
-------	--------------------------	---

### 4.3 IT-Systeme

ID	Was	Beschreibung
SYS01	Windows-Server 2016	Eine dezidierte, gesicherte und gehärtete Servermaschine, die zentralisiert Dienstleistungsprogramme für die Nutzer der Netzinfrastruktur bereitstellt.
SYS02	Arbeitsplatz-PC	Ein stationäre Datenverarbeitungseinheit, bestehend aus Prozessor, Primärspeicher, Netzwerkanbindung sowie Ein-/Ausgabeeinheit.
SYS03	Mobiler-PC	Eine mobile Datenverarbeitungseinheit, siehe auch Arbeitsplatz-PC.
SYS04	Telefon	Hardwaregerät zur Nutzung eines Fernsprechdienstes über das Telekommunikationsnetz
SYS05	Telefaxgerät	Endgerät zum Versand und Empfang von Telefaxen.
SYS06	Smartphones mit Android-Betriebssystem	Mobiltelefone mit eingebauten E-Mail-Funktionen, Web-Browser, Terminverwaltung und spezifischen Applikationen für Mobile-Betriebssysteme.
SYS07	Netzwerk-Multifunktionsgerät	Kombinationsgerät, zur Erstellung von Papierdokumenten und zur optischen Erfassung von Informationen, die als Kontrastmuster (Druckschrift, Handschrift, Rasterbild, Foto) vorliegen.

### 4.4 Netze- und Kommunikation

ID	Was	Beschreibung
NET01	Gebäudeverkabelung	Multifunktionale, vorwiegend für digitale Telefonie und Daten vorgesehene, Vollverkabelung des Behördengebäudes. Unter anderem zur Herstellung einer LAN-Verbindung.
NET02	Switch	Vermittlungsgerät zur Weiterleitung von Daten in LAN unter der Herstellung von Direktverbindungen unter Verwendung der MAC-Adresse.
NET03	Router	Intelligenter Brückenrechner auf der Vermittlungsschicht (3) von OSI zwischen kompatiblen, aber nicht unbedingt gleichartigen Netzwerken (Unterschiede auf Schichten 1 oder 2) zu deren gegenseitiger Integration, zur Optimierung der Datenwege und zur Komprimierung der Daten vor dem Transfer.
NET04	Firewall	Oberbegriff für Sicherheitskonzepte, welche den Datenverkehr zwischen zwei TCP/IP Netzen mithören oder filtern.
NET05	Internet-Zugang	Anbindung der Behörde an das Internet über eine Netzanbindung eines Providers.
NET06	Telefondienst	Fernsprechdienst über das Telekommunikationsnetz, i.d.R. unter der Nutzung von Voice-over-IP.
NET07	Telefaxdienst	Fernkopierdienst in der Telekommunikation.
NET08	Abgesicherter Netzwerk-Zugang über ein VPN	Durch strenge Authentisierung, Autorisierung und Verschlüsselung gesicherte und deshalb vertrauliche Koppelung zweier geschlossener Netzwerke über eine öffentliche und unsichere Netzwerkinfrastruktur.

### 4.5 Räumliche Infrastruktur

ID	Was	Beschreibung
INF01	Allgemeines Gebäude	Ein oder mehrere Dienstgebäude der Behörde.
INF02	Bürraum	Arbeitsplatz der Mitarbeiter der Behörde, ausgestattet mit einem stationären Telefon und einem Client-PC.



ID	Was	Beschreibung
INF03	Serverraum	Gesondert ausgerüsteter und abgesicherter Raum innerhalb des Gebäudes, der die Serverinfrastruktur enthält und über ein entsprechendes Klima verfügt.
INF04	Präsentations- und Besprechungsraum	Räumlichkeit zur Besprechung mit mehreren (auch externen) Personen.
INF05	Häuslicher Arbeitsplatz	Arbeitsplatz im privaten Bereich von Mitarbeitern, der über einen VPN-Zugriff in das Behördennetzwerk verfügt.
INF06	Drucker- und Kopierraum	Mit einem Multifunktionsgerät ausgestatteter Raum, der Büroaufgaben wie Scans, Ausdrücke, Kopien und dergleichen vorgesehen ist.

## 4.6 Netzplan

Die zuvor aufgelistete Netzinfrastruktur einer obersten Landesbehörde ist nun schematisch übersichtsweise dargestellt. Aufgrund unterschiedlicher Auslagerungsmodelle wird auf die Darstellung von ausgelagerten Anteilen des Informationsverbundes verzichtet. Für eine klare Struktur des Netzplans sind die Kürzel der Zielobjekte hier; soweit möglich, dargestellt. Auf die Hervorhebung der Netztrennung von Systemen mit hohem Schutzbedarf wird in der schematischen Darstellung verzichtet.

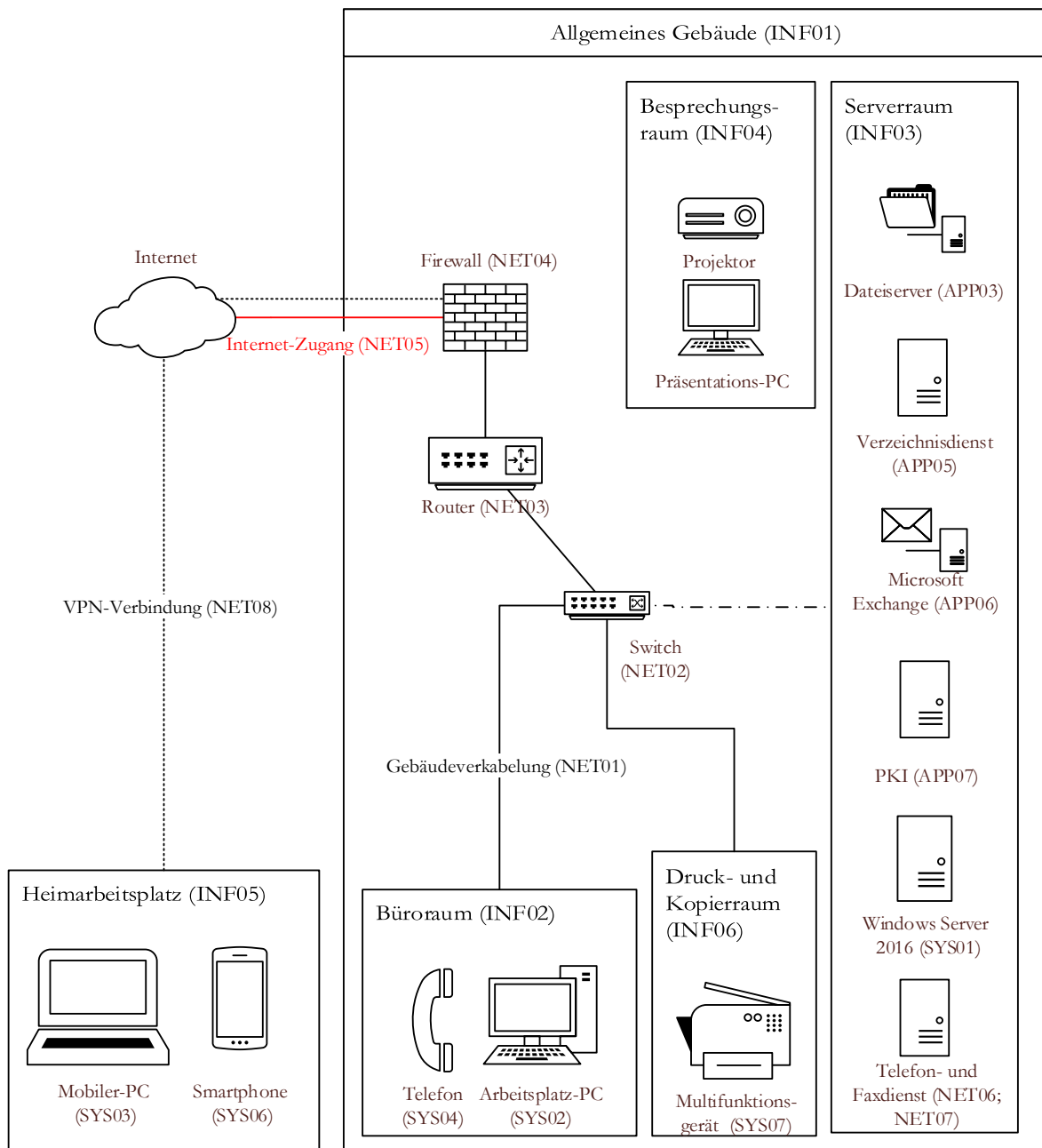


Abbildung 1: Netzplan des Informationsverbundes (eigene Darstellung)

## Kapitel 5 Modellierung des Informationsverbunds

In der Referenzarchitektur der obersten Landesbehörde werden die nachfolgenden IT-Grundschutz-Bausteine für eine Standard-Absicherung empfohlen. Zunächst werden die IT-Grundschutz-Bausteine zu den festgestellten Zielobjekten in einer Kreuzreferenztabelle dargestellt. Daraus ergibt sich in einer Kurzübersicht, welche IT-Grundschutz-Bausteine verwendet werden und welches Zielobjekt über einen IT-Grundschutz-Baustein abgesichert ist.

Anschließend werden die verwendeten IT-Grundschutz-Bausteine gruppiert nach dem IT-Grundschutz-Kompendium aufgezählt. Sofern vorhanden werden Anmerkungen zu bestimmten Bausteinen oder Anforderungen auf der Basis von Expertenmeinungen oder der Fachliteratur unter der jeweiligen Gruppe dargestellt. Neben den Anmerkungen dieser Ausarbeitung können zudem die Anmerkungen des IT-Grundschutz-Profiles für Kommunalverwaltungen beachtet werden.

### 5.1 Kreuzreferenztabelle

In dieser Kreuzreferenztabelle ist dargestellt, welche unter Kapitel 4 aufgezählten Zielobjekte einem IT-Grundschutz-Baustein zugeordnet werden können. Dadurch kann ermittelt werden, ob die Absicherung umfänglich stattfindet. Zudem ist dieser Teilschritt vorbereitend für die Risikoanalyse, da diese zwangsweise Zielobjekte berücksichtigt, denen kein IT-Grundschutz-Baustein zugeordnet ist.

**Kreuzreferenztabelle zwischen Zielobjekten und IT-Grundschutz-Bausteinen**

Anwendungen		
ID	Zielobjekt	Bausteine
PRO01	Allgemeiner Informationsverbund / Beteiligung an der Normsetzung	ISMS.1; OPS.1.1.2; OPS.1.1.3; OPS.1.1.4; OPS.1.1.5; OPS.1.1.6; OPS.1.2.2; OPS.1.2.3; OPS.1.2.4; OPS.2.4 ORP.1; ORP.2; ORP.3; ORP.4; ORP.5 CON.1; CON.3; CON.4; CON.6; DER.1; DER.2.1; DER.2.2; DER.2.3; DER.3.1; DER.3.2; DER.4 SYS.3.2.2;
ID	Zielobjekt	Bausteine
APP01	Betriebssystem Windows 10	SYS.2.1; SYS.2.2.3
APP02	Microsoft Office 2016	APP.1.1
APP03	Dateiserver	APP.3.3
APP04	Web-Browser Firefox	APP.1.2
APP05	Verzeichnisdienst Active Directory	APP.2.1, APP.2.2
APP06	Microsoft Exchange	APP.5.1; APP.5.2
APP07	Public-Key Infrastruktur	Kein spezieller Baustein vorhanden.
IT-Systeme		
SYS01	Windows-Server 2016	SYS.1.1; SYS.1.2.3 (in Erstellung)
SYS02	Arbeitsplatz-PC	SYS.2.1; SYS.2.2.3
SYS03	Mobiler-PC	SYS.2.1; SYS.3.1; SYS.2.2.3
SYS04	Telefon	NET.4.1
SYS05	Telefaxgerät	NET.4.3

SYS06	Smartphones mit Android-Betriebssystem	APP.1.4; SYS.3.2.1; SYS.3.2.4
SYS07	Netzwerk-Multifunktionsgerät	SYS.4.1
<b>Netzwerkkomponenten</b>		
NET01	Gebäudeverkabelung	NET.1.1
NET02	Switch	NET.3.1
NET03	Router	
NET04	Firewall	NET.3.2
NET05	Internet-Zugang	NET.1.1
NET06	Telefondienst	NET.4.2
NET07	Telefaxdienst	NET.4.3
NET08	Abgesicherter Netzwerk-Zugang über ein VPN	NET.3.3
<b>Räumliche Infrastruktur</b>		
INF01	Allgemeines Gebäude	INF.1; INF.3; INF.4
INF02	Bürraum	INF.7
INF03	Serverraum	INF.2
INF04	Präsentations- und Besprechungsraum	INF.10
INF05	Häuslicher Arbeitsplatz	INF.8
INF06	Drucker- und Kopierraum	Kein spezieller Baustein vorhanden.

## 5.2 Prozess-Bausteine

### 5.2.1 Schicht ISMS

Die Basis-Anforderungen des Bausteins ISMS.1 MÜSSEN umgesetzt werden. Zusätzlich dazu SOLLTEN die Vorgaben der Standard-Absicherung dieses Bausteins umgesetzt werden. Wenn von der Umsetzung einer optionalen Anforderung abgesehen wird, so ist dies hinreichend zu begründen und entsprechend zu dokumentieren.

**Zu den Anforderungen bestehen folgende Anmerkungen:**

Anforderung	Titel	Anmerkung	Begründung	Quelle
ISMS.1.A10	Erstellung eines Sicherheitskonzepts	Die Anforderung MUSS umgesetzt werden.	Gemäß der ISLL-Bund müssen die Verwaltungen des Bundes und der Länder Sicherheitskonzeptionen erstellen.	ISLL-Bund
ISMS.1.A12	Management-Berichte zur Informationssicherheit	Die Anforderung MUSS umgesetzt werden.	Diese Anforderungen stellen die erfolgreiche Umsetzung des ISMS in der Behörde sicher.	Expertenbeitrag

### 5.2.2 Schicht ORP

Die Basis-Anforderungen der Bausteine ORP.1-ORP.5 MÜSSEN umgesetzt werden. Zusätzlich dazu SOLLTEN die Vorgaben der Standard-Absicherung dieser Bausteine umgesetzt werden. Wenn von der Umsetzung einer optionalen Anforderung abgesehen wird, so ist dies hinreichend zu begründen und entsprechend zu dokumentieren.

**Folgende Anmerkungen bestehen zu den Anforderungen der Bausteine ORP.1 – ORP.5:**

Anforderung	Titel	Anmerkung	Begründung	Quelle
ORP.4.A8	Regelung des Passwortgebrauchs	Passwörter DÜRFEN NICHT im Klartext elektronisch gespeichert werden. Stattdessen SOLLTE ein Prüfsummenverfahren nach dem Stand der Technik verwendet werden.	Im Klartext abgespeicherte Benutzer-Passwort-Kombinationen können intern zu einem Missbrauch führen oder bei einem Datenabfluss dem Angreifer weitere Möglichkeiten des Missbrauchs einräumen.	Ein entsprechendes Sicherungsvorgehen wird in der ISO 27002:2013 [11, S. 27], der NIST SP 800-63B [12, S. 15] und der PCI DSS [13, S. 72] empfohlen.

**5.2.3 Schicht CON**

Die Basis-Anforderungen der Bausteine CON.1, CON.3, CON.4 und CON.6 MÜSSEN umgesetzt werden. Zusätzlich dazu SOLLTEN die Vorgaben der Standard-Absicherung dieser Bausteine umgesetzt werden. Wenn von der Umsetzung einer optionalen Anforderung abgesehen wird, so ist dies hinreichend zu begründen und entsprechend zu dokumentieren.

**Folgende Anmerkungen bestehen zu den Anforderungen der Bausteine CON.1 – CON.7:**

Anforderung	Titel	Anmerkung	Begründung	Quelle
CON.2.1.1	Einleitung / Standard-Datenschutzmodell	Der Baustein CON.2 ist nicht anzuwenden.	Für die Verwaltungsbehörden gilt bereits das bundesweit etablierte Standard-Datenschutzmodell (SDM) und die entsprechende Datenschutzgesetzgebung. Daher wird der Baustein hier als redundant betrachtet.	IT-Grundschatz Kompendium, Baustein CON.2 – Datenschutz.

**5.2.4 Schicht OPS**

Die Basis-Anforderungen der Bausteine OPS.1.1.2-OPS1.1.6, OPS.1.2.2, OPS.1.2.3, OPS.1.2.4 und OPS.2.4 MÜSSEN umgesetzt werden. Zusätzlich dazu SOLLTEN die Vorgaben der Standard-Absicherung dieser Bausteine umgesetzt werden. Wenn von der Umsetzung einer optionalen Anforderung abgesehen wird, so ist dies hinreichend zu begründen und entsprechend zu dokumentieren.

**Folgende Anmerkungen bestehen zu den Anforderungen der Bausteine OPS.1.1.2 – OPS.4:**

**Keine.**

**5.2.5 Schicht DER**

Die Basis-Anforderungen der Bausteine DER.1, DER.2.1, DER.2.2, DER.2.3, DER.3.1, DER.3.2 und DER.4 MÜSSEN umgesetzt werden. Zusätzlich dazu SOLLTEN die Vorgaben der Standard-Absicherung

dieser Bausteine umgesetzt werden. Wenn von der Umsetzung einer optionalen Anforderung abgesehen wird, so ist dies hinreichend zu begründen und entsprechend zu dokumentieren.

**Folgende Anmerkungen bestehen zu den Anforderungen der Bausteine DER.1 –DER.4:**

**Keine.**

## **5.3 System Bausteine**

### **5.3.1 Schicht APP**

Die Basis-Anforderungen der nachfolgend aufgezählten Bausteine der Schicht APP MÜSSEN umgesetzt werden. Zusätzlich dazu SOLLTEN die Vorgaben der Standard-Absicherung dieser Bausteine umgesetzt werden. Wenn von der Umsetzung einer optionalen Anforderung abgesehen wird, so ist dies hinreichend zu begründen und entsprechend zu dokumentieren.

Folgende Bausteine werden aufgrund der Referenzarchitektur angewandt:

- APP.1.1 – Office Produkte
- APP.1.2 – Web-Browser
- APP.1.4 – Mobile Anwendungen
- APP.2.1 – Allgemeiner Verzeichnisdienst
- APP.2.2 – Active Directory
- APP.3.3 – Dateiserver
- APP.5.1 – Allgemeine Groupware
- APP.5.2 – Microsoft Exchange und Outlook

**Folgende Anmerkungen bestehen zu den Anforderungen der Schicht APP:**

**Keine.**

### **5.3.2 Schicht SYS**

Die Basis-Anforderungen der nachfolgend aufgezählten Bausteine der Schicht SYS MÜSSEN umgesetzt werden. Zusätzlich dazu SOLLTEN die Vorgaben der Standard-Absicherung dieser Bausteine umgesetzt werden. Wenn von der Umsetzung einer optionalen Anforderung abgesehen wird, so ist dies hinreichend zu begründen und entsprechend zu dokumentieren.

Folgende Bausteine werden aufgrund der Referenzarchitektur angewandt:

- SYS.1.1 – Allgemeiner Server
- SYS.1.2.3 – Windows Server 2016 (in Erstellung)
- SYS.1.8 – Speicherlösungen
- SYS.2.1 – Allgemeiner Client
- SYS.2.2.3 – Clients unter Windows 10
- SYS.3.1 – Laptops
- SYS.3.2.1 – Allgemeine Smartphones und Tablets
- SYS.3.2.2 – Mobile Device Management

- SYS.3.2.4 – Android
- SYS.3.3 – Mobiltelefon
- SYS.3.4 – Mobile Datenträger
- SYS.4.1 – Drucker, Kopierer und Multifunktionsgeräte

**Folgende Anmerkungen bestehen zu den Anforderungen der Schicht SYS:**

**Keine.**

### **5.3.3 Schicht NET**

Die Basis-Anforderungen der nachfolgend aufgezählten Bausteine der Schicht NET MÜSSEN umgesetzt werden. Zusätzlich dazu SOLLTEN die Vorgaben der Standard-Absicherung dieser Bausteine umgesetzt werden. Wenn von der Umsetzung einer optionalen Anforderung abgesehen wird, so ist dies hinreichend zu begründen und entsprechend zu dokumentieren.

Folgende Bausteine werden aufgrund der Referenzarchitektur angewandt:

- NET.1.1 – Netzarchitektur und -design
- NET.1.2 – Netzmanagement
- NET.3.1 – Router und Switches
- NET.3.2 – Firewall
- NET.3.3 – VPN
- NET.4.1 – Telekommunikationsanlagen
- NET.4.2 – VoIP
- NET.4.3 – Telefaxgeräte und Telefaxserver

**Folgende Anmerkungen bestehen zu den Anforderungen der Schicht NET:**

**Keine.**

### **5.3.4 Schicht INF**

Die Basis-Anforderungen der nachfolgend aufgezählten Bausteine der Schicht INF MÜSSEN umgesetzt werden. Zusätzlich dazu SOLLTEN die Vorgaben der Standard-Absicherung dieser Bausteine umgesetzt werden. Wenn von der Umsetzung einer optionalen Anforderung abgesehen wird, so ist dies hinreichend zu begründen und entsprechend zu dokumentieren.

Folgende Bausteine werden aufgrund der Referenzarchitektur angewandt:

- INF.1 – Allgemeines Gebäude
- INF.2 – Rechenzentrum sowie Serverraum
- INF.3 – Elektrotechnische Verkabelung
- INF.4 – IT-Verkabelung
- INF.7 – Büroarbeitsplatz
- INF.8 – Häuslicher Arbeitsplatz
- INF.10 – Besprechungs-, Veranstaltungs- und Schulungsräume

**Folgende Anmerkungen bestehen zu den Anforderungen der Schicht SYS:**

**Keine.**



## Kapitel 6 Schutzbedarfe

### 6.1 Schutzbedarfskategorien

Folgende Schutzbedarfskategorien werden für eine erste Schutzbedarfsfeststellung im Rahmen der Standard-Absicherung aus dem BSI-Standard 200-2 herangezogen [14, S. 106-107]:

#### Normaler Schutzbedarf

1. Verstoß gegen Gesetze/Vorschriften/Verträge	<ul style="list-style-type: none"> <li>• Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen.</li> <li>• Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen.</li> </ul>
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	<ul style="list-style-type: none"> <li>• Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann.</li> </ul>
3. Beeinträchtigung der persönlichen Unversehrtheit	<ul style="list-style-type: none"> <li>• Eine Beeinträchtigung erscheint nicht möglich.</li> </ul>
4. Beeinträchtigung der Aufgabenerfüllung	<ul style="list-style-type: none"> <li>• Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden.</li> <li>• Die maximal tolerierbare Ausfallzeit liegt zwischen 24 und 72 Stunden.</li> </ul>
5. Negative Innen- oder Außenwirkung	<ul style="list-style-type: none"> <li>• Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung sind zu erwarten.</li> </ul>
6. Finanzielle Auswirkungen	<ul style="list-style-type: none"> <li>• Der finanzielle Schaden bleibt für die Institution tolerabel.</li> </ul>

#### Hoher Schutzbedarf

1. Verstoß gegen Gesetze/Vorschriften/Verträge	<ul style="list-style-type: none"> <li>• Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen.</li> <li>• Vertragsverletzungen mit hohen Konventionalstrafen.</li> </ul>
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	<ul style="list-style-type: none"> <li>• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann.</li> </ul>
3. Beeinträchtigung der persönlichen Unversehrtheit	<ul style="list-style-type: none"> <li>• Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.</li> </ul>
4. Beeinträchtigung der Aufgabenerfüllung	<ul style="list-style-type: none"> <li>• Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt.</li> <li>• Die maximal tolerierbare Ausfallzeit liegt zwischen drei und 24 Stunden.</li> </ul>
5. Negative Innen- oder Außenwirkung	<ul style="list-style-type: none"> <li>• Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.</li> </ul>
6. Finanzielle Auswirkungen	<ul style="list-style-type: none"> <li>• Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.</li> </ul>

#### Sehr hoher Schutzbedarf

1. Verstoß gegen Gesetze/Vorschriften/Verträge	<ul style="list-style-type: none"> <li>• Fundamentaler Verstoß gegen Vorschriften und Gesetze.</li> <li>• Vertragsverletzungen, deren Haftungsschäden ruinös sind.</li> </ul>
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	<ul style="list-style-type: none"> <li>• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist.</li> </ul>

3. Beeinträchtigung der persönlichen Unversehrtheit	<ul style="list-style-type: none"> <li>• Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich.</li> <li>• Gefahr für Leib und Leben.</li> </ul>
4. Beeinträchtigung der Aufgabenerfüllung	<ul style="list-style-type: none"> <li>• Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden.</li> <li>• Die maximal tolerierbare Ausfallzeit ist kleiner als drei Stunden.</li> </ul>
5. Negative Innen- oder Außenwirkung	<ul style="list-style-type: none"> <li>• Eine landesweite bis bundesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, ist denkbar.</li> </ul>
6. Finanzielle Auswirkungen	<ul style="list-style-type: none"> <li>• Der finanzielle Schaden ist für die Institution existenzbedrohend.</li> </ul>
7. Sonstige Auswirkungen	<ul style="list-style-type: none"> <li>• Der Bestand des Staates oder wesentliche Teile dessen könnten gefährdet werden.</li> </ul>

## 6.2 Schutzbedarfsfeststellung

Nun werden die Schutzbedarfe der Zielobjekte bei der Umsetzung der Basis- und Standard-Anforderungen eingeschätzt und kurz kommentiert. Es wird dabei gemäß dem Standard 200-2 von dem Geschäftsprozess auf die Informationen, Anwendungen und den weiteren Informationsverbund abgeleitet. Für die Anwender dieses IT-Grundschutz-Profiles ist zu beachten, dass es sich bei der Beteiligung an der Normsetzung des Landes um einen Geschäftsprozess handelt, der für gewöhnlich keine herausragenden Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit hat. Im Gegenteil, im Rahmen von Transparenzoffensiven wird dieser Geschäftsprozess in einigen Bundesländern zum größtmöglichen Teil öffentlich gehandhabt – was sich hier auf die Anforderungen der Vertraulichkeit auswirkt.

### 6.2.1 Schutzziel Vertraulichkeit

ID	Was	Vertraulichkeit	Kommentar
PRO01	Beteiligung an der Normsetzung des Landes	Normal	Die verschiedenen Normsetzungsprozesse der obersten Landesbehörden (Beteiligung an Gesetzgebung, Verordnungen und Erlasse) weisen keine herausragenden Anforderungen an die Vertraulichkeit auf. In den vergangenen Jahren haben sich stattdessen weitere Transparenztendenzen durchgesetzt [15, S. 165-166]. Bei einer unberechtigten Kenntnisnahme kommt es zu überschaubaren Konsequenzen.
ID	Was	Vertraulichkeit	Kommentar
APP01	Betriebssystem Windows 10	Normal	Es wird über das Betriebssystem nur auf einen Geschäftsprozess mit einem normalen Schutzbedarf eingewirkt. Die unberechtigte Kenntnisnahme von Daten hat begrenzte Auswirkungen.
APP02	Microsoft Office 2016	Normal	Die Office-Anwendungen speichern lediglich temporär Daten zwischen und sind selbst nicht vertraulich zu behandeln. Es wird nur auf Informationen mit normalem Schutzbedarf zugegriffen.
APP03	Dateiserver	Normal	Auf dem Dateiserver werden Dokumente dauerhaft gespeichert und von berechtigten Personen abgerufen. Die dort abgelegten Dokumente enthalten Informationen, deren unbefugte Kenntnisnahme die Institution und dritte Personen im tolerierbaren Maße schädigen können.
APP04	Web-Browser Firefox	Normal	Ein Web-Browser enthält selbst keine über den normalen Schutzbedarf hinausgehenden Informationen. Besonders schützenswerte Webanwendungen sind nicht vorhanden.

APP05	Verzeichnis- dienst Active Directory	Hoch	Der Verzeichnisdienst speichert Daten und Berechtigungen, die unter anderem für einen ordnungsgemäßen Betrieb der IT und der Rechteverwaltung verantwortlich sind. Eine Verletzung der Vertraulichkeit kann Betriebsausfälle und einen wesentlichen Nachteil für die Institution bedeuten, sodass ein hoher Schutzbedarf besteht.
APP06	Microsoft Exchange	Normal	Microsoft Exchange ergänzt die Office Produkte als Kommunikations- und Planungsressource. Da Informationen mit normalem Schutzbedarf verarbeitet werden, vererbt sich dieser Schutzbedarf auf dieses Zielobjekt.
APP07	Public-Key Infrastruktur	Hoch	Unberechtigte Kenntnisnahmen von spezifischen Informationen der Public-Key Infrastruktur (wie bspw. private Schlüssel) führen zu einer Störung der sicheren Kommunikation der Behörde. Daher liegt ein hoher Schutzbedarf vor.
<b>ID</b>	<b>Was</b>	<b>Vertraulichkeit</b>	<b>Kommentar</b>
SYS01	Windows-Ser- ver 2016	Hoch	Der Server bildet die Grundlage für dezidierte Serveranwendungen wie den Verzeichnisdienst, Microsoft Exchange und den Dateiserver. Es vererbt sich ein hoher Schutzbedarf.
SYS02	Arbeitsplatz- PC	Normal	Von dem Arbeitsplatz-PC wird als Client über das Betriebssystem auf Daten zugegriffen, die einer normalen Vertraulichkeit unterliegen. Daher liegt ein normaler Schutzbedarf vor.
SYS03	Mobile-PCs	Normal	Von dem Mobilien-PCs wird als Client über das Betriebssystem auf Daten zugegriffen, die einer normalen Vertraulichkeit unterliegen. Daher vererbt sich ein normaler Schutzbedarf.
SYS04	Telefon	Normal	Da Informationen mit normalen Schutzbedarf verarbeitet werden, vererbt sich dieser Schutzbedarf des Geschäftsprozesses auf dieses Zielobjekt.
SYS05	Telefaxgerät	Normal	Da Informationen mit normalen Schutzbedarf verarbeitet werden, vererbt sich der normale Schutzbedarf des Geschäftsprozesses auf dieses Zielobjekt.
SYS06	Smartphones mit Android- Betriebssystem	Normal	Da Informationen mit normalen Schutzbedarf verarbeitet werden, vererbt sich der normale Schutzbedarf des Geschäftsprozesses auf dieses Zielobjekt.
SYS07	Netzwerk-Mul- tifunktionsge- rät	Normal	Da Informationen mit normalen Schutzbedarf verarbeitet werden, vererbt sich der normale Schutzbedarf des Geschäftsprozesses auf dieses Zielobjekt.
<b>ID</b>	<b>Was</b>	<b>Vertraulichkeit</b>	<b>Kommentar</b>
NET01	Gebäudeverka- belung	Hoch	Es wird eine hohe Vertraulichkeit durch den Transport von Daten der PKI und des Verzeichnisdienstes vererbt.
NET02	Switch	Hoch	Ähnlich der Gebäudeverkabelung werden über den Switch besonders schützenswerte Daten der PKI und des Verzeichnisdienstes koordiniert. Daraus entsteht ein hoher Schutzbedarf für dieses Objekt.
NET03	Router	Normal	Eine Steuerung vertraulicher Informationen in das Internet ist nicht vorgesehen, sodass ein normaler Schutzbedarf besteht.
NET04	Firewall	Hoch	Die Firewall-Regeln müssen vertraulich behandelt werden, da sonst potenzielle Angreifer Möglichkeiten für eine System-Kompromittierung ausspähen können. Ein darauf basierender Angriff kann die Arbeitsfähigkeit der Behörde entschieden beeinträchtigen.
NET05	Internet-Zu- gang	Normal	Vertrauliche Informationen werden durch den Geschäftsprozess nicht verursacht, weshalb auch die Steuerung zu einem Internet-Provider von normalem Schutzbedarf ist.

NET06	Telefondienst	Normal	Da Informationen mit normalen Schutzbedarf verarbeitet werden, vererbt sich der normale Schutzbedarf des Geschäftsprozesses auch auf dieses Zielobjekt.
NET07	Telefaxdienst	Normal	Da Informationen mit normalen Schutzbedarf verarbeitet werden, vererbt sich hier ein normaler Schutzbedarf.
NET08	Abgesicherter Netzwerk-Zugang über ein VPN	Normal	Unberechtigte Kenntnisnahmen können bei diesem Zielobjekt zu Beeinträchtigungen führen, bei denen gemäß des normalen Schutzbedarfes keine schwerwiegende Folge eintreten sollte. Administrative Prozesse sind von der VPN-Verbindung getrennt.
ID	Was	Vertraulichkeit	Kommentar
INF01	Allgemeines Gebäude	Hoch	Es gilt das Vererbungsprinzip. In dem allgemeinen Gebäude befindet sich auch der Serverraum. Zudem muss eine Akkumulation der Schutzbedarfe in Betracht gezogen werden. Es entsteht ein hoher Schutzbedarf.
INF02	Büroraum	Normal	Im Büroraum werden durch Mitarbeiter Daten mit normalem Schutzbedarf verarbeitet und mitunter in Papierform aufbewahrt.
INF03	Serverraum	Hoch	Physischer Standort des Servers bzw. der Server, daher kommt der Vererbungs- sowie der Kumulationseffekt zum Tragen. Von hier aus werden wesentliche Dienste bereitgestellt.
INF04	Präsentations- und Besprechungsraum	Normal	Es werden hier keine besonders schützenswerten Daten verarbeitet und es stehen nur eingeschränkte IT-Ressourcen zur Verfügung.
INF05	Häuslicher Arbeitsplatz	Normal	Gemäß des Vererbungsprinzips ist von einer normalen Vertraulichkeit der Daten auszugehen, die an einem häuslichen Arbeitsplatz verarbeitet werden.
INF06	Drucker- und Kopierraum	Normal	Vererbung von dem Netzwerk-Multifunktionsgerät auf dem Schutzbedarf „Normal“.

### 6.2.2 Schutzziel Integrität

ID	Was	Integrität	Kommentar
PRO01	Beteiligung an der Normsetzung des Landes	Normal	Der Geschäftsprozess behandelt Informationen, deren unberechtigte Veränderung tolerierbare Beeinträchtigungen nach sich zieht.
ID	Was	Integrität	Kommentar
APP01	Betriebssystem Windows 10	Normal	Auf dem Betriebssystem findet eine Vererbung des normalen Schutzbedarfes des Geschäftsprozesses statt.
APP02	Microsoft Office 2016	Normal	Aufgrund der temporären Datenspeicherung bedarf Microsoft Office selbst keiner Absicherung der Integrität über den normalen Schutzbedarf hinaus.
APP03	Dateiserver	Normal	Die über den Dateiserver verwalteten Daten werden nur durch berechtigte Personen bearbeitet. Die möglichen Auswirkungen unberechtigter oder falscher Änderungen sind im normalen Schutzbereich.
APP04	Web-Browser Firefox	Normal	Der Web-Browser speichert lediglich temporär Daten zwischen und Bedarf selbst keinem Schutz der Integrität über das normale Maß hinaus.
APP05	Verzeichnisdienst Active Directory	Hoch	Der Verzeichnisdienst ist verantwortlich für die sichere Authentifizierung und Bereitstellung von Ressourcen innerhalb der Behörde. Eine unberechtigte Veränderung

			kann unter anderem die Gesamtverfügbarkeit des Informationsverbundes bedeutend einschränken, weshalb ein hoher Schutzbedarf besteht.
APP06	Microsoft Exchange	Normal	Da Informationen mit normalen Schutzbedarf verarbeitet werden, vererbt sich der normale Schutzbedarf des Geschäftsprozesses auf dieses Zielobjekt.
APP07	Public-Key Infrastruktur	Hoch	Nachrichten können unberechtigt von dritten Personen als behördlich autorisiert dargestellt werden, sollte es zu einem Integritätsverlust kommen. Ferner können Datenfehler in der PKI zu unlesbaren Nachrichten führen. Daraus ergibt sich ein hoher Schutzbedarf.
<b>ID</b>	<b>Was</b>	<b>Integrität</b>	<b>Kommentar</b>
SYS01	Windows-Server 2016	Hoch	Es besteht hoher Schutzbedarf durch den Vererbungseffekt, der unter anderem durch den zum Dienstbetrieb benötigten Verzeichnisdienst eintritt. Zudem werden weitere Dienste über den Server bereitgestellt.
SYS02	Arbeitsplatz-PC	Normal	Über den Zugriff des Arbeitsplatz-PCs sind Veränderungen der normal schutzbedürftigen Daten möglich. Da eine Verfälschung dieser Daten tolerierbar ist, besteht ein normaler Schutzbedarf der Integrität.
SYS03	Mobiler-PC	Normal	Der Mobile-PC hält selbst nur Daten vor, die dem normalen Schutzbedarf unterliegen.
SYS04	Telefon	Normal	Das Telefon benötigt keiner weiteren Absicherung und hält keine Daten über den normalen Schutzbereich hinaus vor.
SYS05	Telefaxgerät	Normal	Das Telefaxgerät benötigt keiner weiteren Absicherung und hält keine Daten über den normalen Schutzbereich hinaus vor.
SYS06	Smartphones mit Android-Betriebssystem	Normal	Smartphones und Tablets sind für die Behördenzwecke angepasst und enthalten im Rahmen des Geschäftsprozesses keine Daten, die besonders in der Integrität zu schützen sind.
SYS07	Netzwerk-Multifunktionsgerät	Normal	Das Multifunktionsgerät ist vor unberechtigten Zugriffen abgesichert. Integritätsverletzungen hätten nur Folgen im Rahmen des normalen Schutzbedarfs.
<b>ID</b>	<b>Was</b>	<b>Integrität</b>	<b>Kommentar</b>
NET01	Gebäudeverkabelung	Hoch	Da Informationen mit hohem Schutzbedarf über die Gebäudeverkabelung transportiert werden, liegt ein hoher Schutzbedarf vor.
NET02	Switch	Hoch	Auch besonders schützenswerte Datenverarbeitungsprozesse werden über die Gebäudeverkabelung durchgeführt und durch den Switch im Netzwerk verteilt. Dieser erbt den hohen Schutzbedarf.
NET03	Router	Normal	Über den Router werden nur Informationen geleitet, die einem normalen Schutzbedarf unterliegen.
NET04	Firewall	Hoch	Die Firewall-Regeln dürfen auf keinen Fall unberechtigt verändert werden. Entsprechende Eingriffe oder falsche Daten gefährden die Handlungsfähigkeit der Behörde außerordentlich, weshalb ein hoher Schutzbedarf entsteht.
NET05	Internet-Zugang	Normal	Der Internetzugang ist durch entsprechende Protokolle und Maßnahmen ausreichend abgesichert. Über diesen werden nur Informationen des normalen Schutzbedarfs transportiert.
NET06	Telefondienst	Normal	Es werden Informationen mit normalen Schutzbedarf verarbeitet, für die Integrität vererbt sich der normale Schutzbedarf des Geschäftsprozesses auf dieses Zielobjekt.

NET07	Telefaxdienst	Normal	Es werden Informationen mit normalen Schutzbedarf verarbeitet, für die Integrität vererbt sich der normale Schutzbedarf des Geschäftsprozesses auch auf dieses Zielobjekt.
NET08	Abgesicherter Netzwerk-Zugang über ein VPN	Normal	Unberechtigte Veränderungen können bei diesem Zielobjekt zu Beeinträchtigungen führen, die aufgrund des normalen Schutzbedarfes des zugrunde liegenden Geschäftsprozesses Folgen im Rahmen des normalen Schutzbedarfs haben.
<b>ID</b>	<b>Was</b>	<b>Integrität</b>	<b>Kommentar</b>
INF01	Allgemeines Gebäude	Hoch	In dem Gebäude werden grundsätzlich alle Informationen verarbeitet und es fungiert als Server- und Serverdienststandort. Es kommt zu einer Vererbung des hohen Schutzbedarfes.
INF02	Büroraum	Normal	Normal eingestufte Arbeitsprozesse werden in den Büroräumen als Arbeitsplatz durchgeführt. Daher hat dieser einen normalen Schutzbedarf.
INF03	Serverraum	Hoch	Vererbung des Schutzbedarfes von den dort betriebenen Servermaschinen und den darauf betriebenen Diensten wie dem Verzeichnisdienst.
INF04	Präsentations- und Besprechungsraum	Normal	Im Präsentations- und Besprechungsraum stehen nur eingeschränkte IT-Ressourcen zur Verfügung. Falsche und/oder unberechtigt veränderte Informationen haben nur Auswirkungen in der normalen Schutzbedarfskategorie.
INF05	Häuslicher Arbeitsplatz	Normal	Der häusliche Arbeitsplatz hat im Rahmen des Geschäftsprozesses Zugriff auf Schutzbedarfe im normalen Bereich. Dementsprechend gestaltet sich der Schutzbedarf.
INF06	Drucker- und Kopierraum	Normal	Es findet eine Vererbung des normalen Schutzbedarfs vom Geschäftsprozess sowie von dem Multifunktionsgerät statt.

### 6.2.3 Schutzziel Verfügbarkeit

<b>ID</b>	<b>Was</b>	<b>Verfügbarkeit</b>	<b>Kommentar</b>
PRO01	Beteiligung an der Normsetzung des Landes	Normal	Der Geschäftsprozess behandelt Informationen, bei denen eine Einschränkung der Verfügbarkeit im tolerierbaren Bereich liegt.
<b>ID</b>	<b>Was</b>	<b>Verfügbarkeit</b>	<b>Kommentar</b>
APP01	Betriebssystem Windows 10	Normal	Über eine Internetverbindung oder entsprechend vorbereitete Kopien kann die Software jederzeit neu zur Verfügung gestellt werden. Die Ausfallzeit ist im normalen Schutzbereich
APP02	Microsoft Office 2016	Normal	Über eine Internetverbindung oder entsprechend vorbereitete Kopien kann die Software jederzeit neu zur Verfügung gestellt werden. Längere Ausfallzeiten sind dadurch unwahrscheinlich und hätten nur Auswirkungen im normalen Bereich.
APP03	Dateiserver	Hoch	Ohne die Dateiverwaltung und Kollaborationsmöglichkeiten ist die Arbeitsfähigkeit der Behörde deutlich eingeschränkt, eine längere Ausfallzeit als einen Tag ist nicht akzeptabel. Eine Ausfallzeit von unter einer Stunde ist dabei nicht einzuhalten, existenzbedrohend ist ein Ausfall des



			Dateiservers ebenfalls nicht. Daher liegt ein hoher Schutzbedarf vor.
APP04	Web-Browser Firefox	Normal	Über eine Internetverbindung oder entsprechend vorbereitete Kopien kann die Software jederzeit neu zur Verfügung gestellt werden. Ausfallzeiten sind dadurch reduziert und im Eintrittsfalle von normalem Schutzbedarf.
APP05	Verzeichnisdienst Active Directory	Hoch	Sollte der Verzeichnisdienst nicht verfügbar sein, ist die gesamte Aufgabenwahrnehmung der Behörde gefährdet. Zugriffe auf Systeme, Dateien und andere Ressourcen sind nicht möglich. Dementsprechend ist eine Ausfallzeit von mehr als 24 Stunden nicht akzeptabel.
APP06	Microsoft Exchange	Normal	Ein temporärer Ausfall von Microsoft-Exchange ist tolerierbar, dieser betrifft Informationen mit normalem Schutzbedarf. Andere Kommunikationsmittel stehen bei einem Ausfall gegebenenfalls zur Verfügung.
APP07	Public-Key Infrastruktur	Hoch	Die Public-Key Infrastruktur dient zur verbindlichen Kommunikation und muss dazu nahezu störungsfrei zur Verfügung stehen. Es kann eine Ausfallzeit von bis zu einem Tag toleriert werden, woraus sich ein hoher Schutzbedarf ergibt.
ID	Was	Verfügbarkeit	Kommentar
SYS01	Windows-Server 2016	Hoch	Durch die Vererbung von dem Dateiserver und dem Verzeichnisdienst liegt ein hoher Schutzbedarf der Verfügbarkeit vor.
SYS02	Arbeitsplatz-PC	Normal	Die benötigte Hardware kann als Ersatzteil eingelagert und bei Bedarf zur Verfügung gestellt werden. Es liegt ein normaler Schutzbedarf vor.
SYS03	Mobiler-PC	Normal	Der Mobile-PC fungiert als Client, die benötigte Hardware kann daher als Ersatzteil eingelagert und bei Bedarf zur Verfügung gestellt werden. Es liegt ein normaler Schutzbedarf vor.
SYS04	Telefon	Normal	Das Telefon kann als Ersatzteil bereitgestellt und bei Bedarf zeitnah ersetzt werden. Der Schutzbedarf geht nicht über die Stufe „normal“ hinaus.
SYS05	Telefaxgerät	Normal	Das Telefaxgerät wird als Ersatzteil bereitgestellt und bei Bedarf zeitnah ersetzt.
SYS06	Smartphones mit Android-Betriebssystem	Normal	Das Vorhalten von entsprechenden Ersatzgeräten und die Verarbeitung normaler Informationen führt zu einem normalen Schutzbedarf.
SYS07	Netzwerk-Multifunktionsgerät	Normal	Der Ausfall des Netzwerk-Multifunktionsgeräts ist in die normale Schutzbedarfskategorie einzuordnen.
ID	Was	Verfügbarkeit	Kommentar
NET01	Gebäudeverkabelung	Normal	Eine Reparatur der Verkabelung bei einer Einschränkung kann zeitnah erfolgen und über das Vorhalten von entsprechenden Ersatzteilen und Leitungsplänen sichergestellt werden.
NET02	Switch	Normal	Ein Ersatzgerät wird vorgehalten und notfalls ausgetauscht. Konfigurationen lassen sich auf Datenträgern separat vorhalten und aufspielen. Die Verfügbarkeit liegt daher im normalen Bereich.
NET03	Router	Normal	Ersatzgeräte werden vorgehalten und notfalls ausgetauscht. Konfigurationen lassen sich auf Datenträgern separat vorhalten und aufspielen.

NET04	Firewall	Hoch	Die Firewall schützt jederzeit das Behördennetz gegen unberechtigte Zugriffe und andere sicherheitsrelevante Interaktionen. Eine Ausfallzeit von mehr als 24 Stunden ist nicht tolerabel, da in diesem Falle jegliche betroffene Außenverbindungen unterbrochen werden müssen.
NET05	Internet-Zugang	Normal	Ein Ausfall der Internetverbindung ist für 24 Stunden tolerierbar, die Aufgabenwahrnehmung wird dadurch nur im angemessenen Maße eingeschränkt.
NET06	Telefondienst	Normal	Neben einer telefonischen Erreichbarkeit bestehen weitere Kommunikationskanäle für die Aufgabenwahrnehmung.
NET07	Telefaxdienst	Normal	Neben einer Erreichbarkeit per Telefax bestehen weitere Kommunikationskanäle für die Aufgabenwahrnehmung und verbindliche Kommunikation der Behörde.
NET08	Abgesicherter Netzwerk-Zugang über ein VPN	Normal	Ein Ausfall des externen Netzwerkzugriffes ist für 24 Stunden tolerierbar, die Aufgabenwahrnehmung wird dadurch im angemessenen Maße eingeschränkt
ID	Was	Verfügbarkeit	Kommentar
INF01	Allgemeines Gebäude	Hoch	In dem Gebäude werden grundsätzlich alle Informationen verarbeitet und es fungiert als Serverstandort. Daher kommt es zu einer Vererbung des hohen Schutzbedarfes.
INF02	Büroraum	Normal	Ohne zur Verfügung stehende Büroräumlichkeiten besteht keine Möglichkeit zur Aufgabenwahrnehmung. Allerdings ist eine dadurch verursachte Störung des Geschäftsprozesses im tolerierbaren Bereich.
INF03	Serverraum	Hoch	Der Serverraum ist der zentrale Raum, der für die Erbringung der IT-Dienste im Dienstgebäude verantwortlich ist. Es kommt zu einer Vererbung des hohen Schutzbedarfes von den dort betriebenen Servern und den darauf betriebenen Diensten.
INF04	Präsentations- und Besprechungsraum	Normal	Es sind keine besonderen Schutzbedarfe des Präsentations- und Besprechungsraums hinsichtlich der Verfügbarkeit erkennbar.
INF05	Häuslicher Arbeitsplatz	Normal	Es sind keine Schutzbedarfe des häuslichen Arbeitsplatzes über das normale Maß hinaus hinsichtlich der Verfügbarkeit erkennbar.
INF06	Drucker- und Kopierraum	Normal	Der Schutzbedarf des Drucker- und Kopierraums ist im normalen Bereich.



### 6.3 Zielobjekte für die Risikoanalyse

Übersichtstabelle von Zielobjekten, die in einer Risikoanalyse berücksichtigt werden müssen

ID	Was	Vertraulichkeit	Integrität	Verfügbarkeit
APP03	Dateiserver	Normal	Normal	Hoch
APP05	Verzeichnisdienst Active Directory	Hoch	Hoch	Hoch
APP07	Public-Key Infrastruktur	Hoch	Hoch	Hoch
SYS01	Windows-Server 2016	Hoch	Hoch	Hoch
NET01	Gebäudeverkabelung	Hoch	Hoch	Normal
NET02	Switch	Hoch	Hoch	Normal
NET06	Firewall	Hoch	Hoch	Hoch
INF01	Allgemeines Gebäude	Hoch	Hoch	Hoch
INF03	Serverraum	Hoch	Hoch	Hoch
INF06	Drucker- und Kopierraum	Kein IT-Grundschutz-Baustein vorhanden.		

## Kapitel 7 Risikobetrachtung relevanter Zielobjekte

### 7.1 Risikokriterien

Wie zuvor dargestellt, gibt es in der Referenzarchitektur einer obersten Landesbehörde neun Zielobjekte mit hohem Schutzbedarf und ein Zielobjekt ohne spezifischen IT-Grundschutz-Baustein. Gemäß der IT-Grundschutz-Methodik müssen diese einer Risikoanalyse unterzogen werden. Aufgrund des Umfangs findet dabei im Rahmen dieser Ausarbeitung nur die Analyse eines Zielobjektes statt. Bei dem Zielobjekt handelt es sich um den Dateiserver. Dieser wurde ausgewählt, da er eine zentrale Bedeutung in dem betrachteten Geschäftsprozess hat und über einen erhöhten Schutzbedarf im Bereich der Verfügbarkeit verfügt.

Diese Risikobetrachtung behandelt eine schematisch existierende Organisation, so dass kein existierendes Zielobjekt in seiner tatsächlichen Konfiguration und Nutzung einer Risikoanalyse unterzogen wird. Dementsprechend orientieren sich die festgestellten Risiken nicht an tatsächlichen Gegebenheiten und können so keinen verbindlichen Charakter für die obersten Landesbehörden entwickeln – gemäß den Grundannahmen der ISO 31000:2018 ist die Risikoanalyse durch jede Organisation auf ihren spezifischen internen und externen Kontext anzuwenden [16, S. 3].

Ausgehend davon soll durch eine Organisation keine generische Risikoanalyse genutzt werden, um eine individuelle Betrachtung der eigenen Infrastruktur zu vermeiden. Diese Risikoanalyse hat somit exemplarischen Charakter, kann aber in ihrer Struktur und Formulierung als Leitfaden dienen. So wird neben den Risikokriterien, bei denen ein Rückgriff auf den BSI Standard 200-3 stattfindet, auch eine generische Risikomatrix dargestellt. Bezüglich der Risikokriterien wird auf die allgemeine Empfehlung des Standards 200-3 zurückgegriffen [17, S. 26-27]:

Eintrittshäufigkeit	Beschreibung
selten	Ereignis könnte nach heutigem Kenntnisstand höchstens alle fünf Jahre eintreten.
mittel	Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein.
häufig	Ereignis tritt einmal im Jahr bis einmal pro Monat ein.
sehr häufig	Ereignis tritt mehrmals im Monat ein.

Schadenshöhe/Schadensauswirkungen	Beschreibung
vernachlässigbar	Die Schadensauswirkungen sind gering und können vernachlässigt werden.
begrenzt	Die Schadensauswirkungen sind begrenzt und überschaubar.
beträchtlich	Die Schadensauswirkungen können beträchtlich sein.
existenzbedrohend	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

### 7.2 Risikoappetit einer obersten Landesbehörde

Der Risikoappetit der Behörde beschreibt die Motivation der Institution, Risiken einzugehen. Grundsätzlich steht es dabei jeder Behörde im Rahmen gesetzlicher und politischer Vorgaben und Verpflichtungen frei, den eigenen Risikoappetit festzulegen und Risiken nach eigenem Ermessen in Kauf zu nehmen.

Nichtsdestotrotz sollte in diesem Zusammenhang durch die Verantwortungsträger bedacht werden, dass es sich bei einer obersten Landesbehörde um eine zentrale Institution eines Landes handelt, die weitreichende Entscheidungen auf Landes- und über den Bundesrat – auch auf Bundesebene treffen kann. Daher wird für die hier dargestellte Behörde von einem geringen Risikoappetit ausgegangen.

### 7.2.1 Risikomatrix

Da es sich um eine öffentliche Verwaltung handelt, wird von einer niedrigen Risikoaffinität ausgegangen, da das Eingehen von Risiken keine Vorteile bei einer Institution ohne Gewinnerzielungsabsicht bedeutet. Der Risikoappetit einer obersten Landesbehörde kann in einer Risikomatrix wie folgt dargestellt werden:

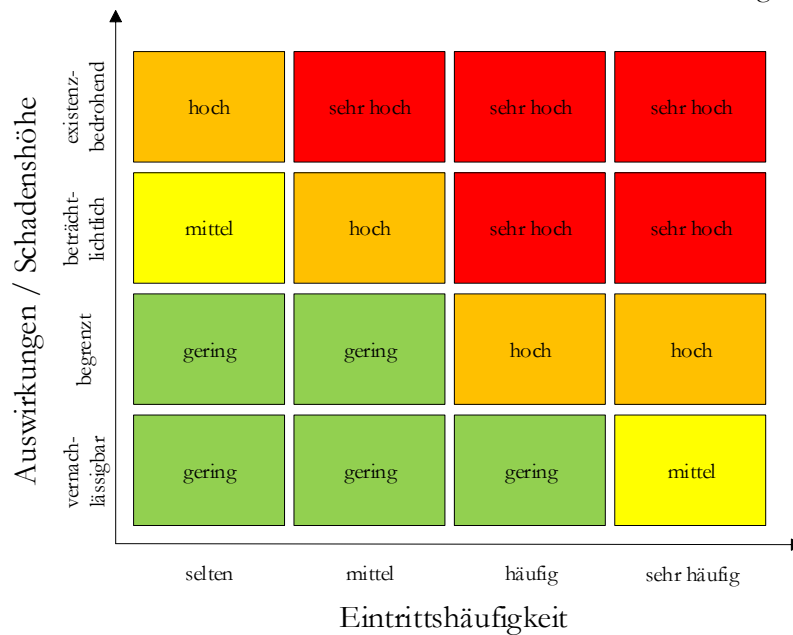


Abbildung 2: Risikomatrix einer obersten Landesbehörde (eigene Darstellung auf Basis des BSI-Standards 200-3 [17, S. 27])

### 7.2.2 Bewertungskategorien der Risiken

Risikokategorien nach Standard 200-3 [17, S. 28]	
gering	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten einen ausreichenden Schutz. In der Praxis ist es üblich, geringe Risiken zu akzeptieren und die Gefährdung dennoch zu beobachten.
mittel	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen reichen möglicherweise nicht aus. In absehbarer Zeit sollten Maßnahmen geplant und umgesetzt werden.
hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung.
sehr hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung. In der Praxis werden sehr hohe Risiken selten akzeptiert.

## 7.3 Risikoanalyse

Nachdem die Rahmenbedingungen für die Einschätzung und Behandlung von Risiken festgelegt sind, folgt nun die Risikoanalyse für schutzbedürftige Zielobjekte aus dem Informationsverbund der obersten Landesbehörde. In diesem IT-Grundschutz-Profil wurden mehrere schutzbedürftige Zielobjekte festgestellt, von

denen der Dateiserver betrachtet wird. Dazu ist in diesem Dokument eine dreiteilige Kapitelstruktur angelegt, die auf die Gefährdungsfeststellung, die Risikoidentifikation und -Einschätzung sowie die Risikobehandlung aufgeteilt ist.

Es ist hervorzuheben, dass eine Risikoanalyse immer individuell auf jede Behörde und ihre dortigen Gegebenheiten durchzuführen ist. Diese hiesige Risikoanalyse dient in diesem Zusammenhang anschaulichen Zwecken und muss von jeder Behörde angepasst aufgegriffen werden. Als Zielobjekt wird dazu der Dateiserver als zentrale Speicher und Kollaborationsplattform abgesichert.

### 7.3.1 Gefährdungen für den Dateiserver

Folgende Gefährdungen bestehen für den Dateiserver [18, APP.3.3 S. 8]

Gefährdung	Titel	Schutzziel	Beispiel
G 0.14	Ausspähen von Informationen (Spionage)	C	Unberechtigte Personen könnten Zugriff auf die abgelegten Daten erhalten und diese für Ihre Zwecke missbrauchen.
G 0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten	C, A	Aus dem Serverraum oder einem anderen Aufstellort für den Dateiserver könnten Festplatten mit sensiblen Daten entnommen werden.
G 0.18	Fehlplanung oder fehlende Anpassung	C, I, A	Der Dateiserver und das darunterliegende Server-Betriebssystem könnten falsch konfiguriert sein und so bspw. schnell überlasten oder unberechtigte Zugriffe zulassen.
G 0.19	Offenlegung schützenswerter Informationen	C	Durch einen berechtigten Benutzer wird die Zugriffsberechtigung falsch eingerichtet und ein unbestimmter Teilnehmerkreis kann schützenswerte Informationen zur Kenntnis nehmen.
G 0.21	Manipulation von Hard- oder Software	C, I, A	Über Schwachstellen könnte der Dateiserver manipuliert werden und so unberechtigte Zugriffe ermöglichen.
G 0.22	Manipulation von Informationen	I	Durch Fehler in den Berechtigungen o.ä. könnten Nutzer wesentliche Informationen manipulieren.
G 0.23	Unbefugtes Eindringen in IT-Systeme	C, I	Jemand könnte sich unberechtigt Zugang zum Dateiserver über fremde Zugangsdaten verschaffen.
G 0.25	Ausfall von Geräten oder Systemen	A	Hardwarefehler, die zum Teil schon in der Produktion entstehen, können zum zeitweiligen Ausfall des Dateiservers führen.
G 0.26	Fehlfunktion von Geräten oder Systemen	C, I, A	Unvorhergesehene Konflikte in den Konfigurationseinstellungen mit anderen IT-Systemen könnten zu einem Ausfall führen.
G 0.27	Ressourcenmangel	A	Es könnte zu Verzögerungen und Ausfällen bei Zugriffen auf den Dateiserver kommen, weil dieser nicht mit ausreichenden Kapazitäten versorgt ist.
G 0.28	Software-Schwachstellen oder -Fehler	C, I, A	Der Dateiserver könnte z.T. unbekannte Sicherheitslücken beinhalten, die die Verletzungen der Sicherheitsziele ermöglichen.

Gefährdung	Titel	Schutzziel	Beispiel
G 0.30	Unberechtigte Nutzung von Geräten und Systemen	C, I, A	Unberechtigte Personen könnten Zugriff auf Administrationskonten erhalten und auf diesem Wege Zugriffe auf den Dateiserver unterbinden oder Daten entwenden.
G 0.31	Fehlerhafte Nutzung von Geräten und Systemen	C, I, A	Durch berechtigte Nutzer und Administratoren könnte der Dateiserver so verändert werden, dass es zu einem Ausfall kommt oder das Daten falsch preisgegeben bzw. verändert werden.
G 0.32	Missbrauch von Berechtigungen	C, I, A	Unberechtigt zugeteilte Berechtigungen könnten von den jeweiligen Mitarbeitern verwendet werden, um nicht für diese bestimmte Daten zu verwenden.
G 0.39	Schadprogramme	C, I, A	Eine Infektion des Dateiservers mit einem Schadprogramm könnte die Sicherstellung der Sicherheitsziele gefährden.
G 0.40	Verhinderung von Diensten (Denial of Service)	A	Der Dateiserver könnte durch eine Vielzahl von missbräuchlich veranlassten Anfragen keine Zugriffe mehr verarbeiten und nicht mehr zur Verfügung stehen.
G 0.43	Einspielen von Nachrichten	C, I	Ein Angreifer könnte die Netzwerkverbindungen des Dateiservers nutzen, um dort vorliegende Daten zu lesen, zu verändern oder unbrauchbar zu machen.
G 0.44	Unbefugtes Eindringen in Räumlichkeiten	C, I, A	Unberechtigte Personen könnten zu dem physischen Standort des Servers vordringen
G 0.45	Datenverlust	A	Durch einen Serverausfall und invalide Datensicherungen könnten Daten unwiederbringlich verloren gehen.
G 0.46	Integritätsverlust schützenswerter Informationen	I	Falsche Konfigurationen seitens des Dateiservers könnten einem Angreifer ermöglichen diverse Daten unberechtigt zu verändern.

### 7.3.2 Risikoeinschätzung und Risikobewertung

Folgend ist das geschätzte Risiko einer obersten Landesbehörde zu den Gefährdungen eines Dateiserver ohne Etablierung eines ISMS. Dabei ist zu beachten, dass jede Institution unterschiedliche Risiken aufgrund der bereits bestehenden Sicherheitsmaßnahmen tragen wird und diese Risiken daher im Rahmen der eigenen Organisation betrachten muss.

#### Risikoeinschätzung und -Bewertung für den Dateiserver

Gefährdung	Titel	Schutzziel	Eintrittshäufigkeit	Auswirkungen	Risiko
G 0.14	Ausspähen von Informationen (Spionage)	C	Mittel	Begrenzt	Gering
G 0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten	C, A	Mittel bis häufig	Beträchtlich	Sehr Hoch
G 0.18	Fehlplanung oder fehlende Anpassung	C, I, A	Mittel	Begrenzt bis beträchtlich	Hoch

Gefährdung	Titel	Schutzziel	Eintrittshäufigkeit	Auswirkungen	Risiko
G 0.19	Offenlegung schützenswerter Informationen	C	Selten	Begrenzt	Gering
G 0.21	Manipulation von Hard- oder Software	C, I, A	Selten	Beträchtlich	Mittel
G 0.22	Manipulation von Informationen	I	Selten	Begrenzt	Gering
G 0.23	Unbefugtes Eindringen in IT-Systeme	C, I	Selten	Beträchtlich	Hoch
G 0.25	Ausfall von Geräten oder Systemen	A	Mittel	Beträchtlich	Hoch
G 0.26	Fehlfunktion von Geräten oder Systemen	C, I, A	Mittel	Beträchtlich	Hoch
G 0.27	Ressourcenmangel	A	Häufig	Beträchtlich	Sehr Hoch
G 0.28	Software-Schwachstellen oder -Fehler	C, I, A	Selten	Beträchtlich	Mittel
G 0.30	Unberechtigte Nutzung von Geräten und Systemen	C, I	Selten	Beträchtlich	Mittel
G 0.31	Fehlerhafte Nutzung von Geräten und Systemen	C, I, A	Häufig	Begrenzt	Hoch
G 0.32	Missbrauch von Berechtigungen	C, I	Häufig	Begrenzt	Hoch
G 0.39	Schadprogramme	C, I, A	Mittel	Beträchtlich	Sehr Hoch
G 0.40	Verhinderung von Diensten (Denial of Service)	A	Mittel	Beträchtlich	Hoch
G 0.43	Einspielen von Nachrichten	I	Selten	Begrenzt	Gering
G 0.44	Unbefugtes Eindringen in Räumlichkeiten	C, I	Mittel	Begrenzt	Gering
G 0.45	Datenverlust	A	Mittel	Beträchtlich	Hoch
G 0.46	Integritätsverlust schützenswerter Informationen	I	Selten	Begrenzt	Gering

### 7.3.3 Risikobehandlung

Aufgrund des erhöhten Schutzbedarfes der Verfügbarkeit sind insbesondere zusätzliche Anforderungen zur Risikoreduktion zu etablieren. Durch den Anspruch an eine hohe Verfügbarkeit des Zielobjekts kommen dabei andere Risikobehandlungen wie eine Risikovermeidung oder ein Risikotransfer nur zum Teil in Frage. In diesem IT-Grundschatz-Profil wird daher zunächst eine Risikobehandlung auf der Basis zusätzlicher Maßnahmen vorgenommen.

In der zusätzlichen Absicherung werden im Sinne der Übersichtlichkeit nur optionale Anforderungen für den erhöhten Schutzbedarf genannt und auf die grundlegenden Bausteine verwiesen. Die zusätzlichen Anforderungen sind in diesem Falle gemäß der Risikohöhe anzuwenden. Dementsprechend genießen sehr hohe Risiken eine die höchste Priorität, für geringe Risiken steht dagegen offen, ob eine Risikoakzeptanz stattfindet.

#### Gefährdungen und deren Risikobehandlung

Gefährdung	Titel	Schutzziel	Risiko	Maßnahmen zur Risikobehandlung
G 0.14	Ausspähen von Informationen (Spionage)	C	Gering	Anforderungen der Bausteine OPR.2 und ORP.4, sowie: <ul style="list-style-type: none"> <li>• ORP.4.A21 (Mehr-Faktor-Authentisierung)</li> <li>• ORP.2.A13 (Sicherheitsüberprüfung)</li> <li>• ORP.5.A10 (Klassifizierung von Informationen)</li> </ul>
G 0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten	C, A	Sehr Hoch	Anforderungen der Bausteine DER.1, OPS.1.2.3, INF.1, INF.2 sowie: <ul style="list-style-type: none"> <li>• CON.1.A10 (Entwicklung eines Kryptokonzepts)</li> <li>• INF.1.A22 (Sichere Türen und Fenster)</li> </ul>
G 0.18	Fehlplanung oder fehlende Anpassung	C, I, A	Hoch	Anforderungen der Bausteine OPS.1.1.2, OPS.1.1.3, OPS.1.1.6, DER.1 sowie: <ul style="list-style-type: none"> <li>• DER.1.A16 (Einsatz von Detektionssystemen nach Schutzbedarfsanforderungen)</li> </ul>
G 0.19	Offenlegung schützenswerter Informationen	C	Gering	Anforderungen der Bausteine ORP.1, ORP.3 sowie: <ul style="list-style-type: none"> <li>• ORP.5.A10 (Klassifizierung von Informationen)</li> <li>• CON.6.A9 (Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Datenträgern bei erhöhtem Schutzbedarf)</li> </ul>
G 0.21	Manipulation von Hard- oder Software	C, I, A	Mittel	Anforderungen der Bausteine OPS.1.1.2, OPS.1.1.3, OPS.1.1.6 sowie: <ul style="list-style-type: none"> <li>• CON.1.A16 (Physische Absicherung von Kryptomodulen)</li> </ul>
G 0.22	Manipulation von Informationen	I	Gering	Anforderungen der Bausteine ORP.4., OPS.1.1.2, OPS.1.1.6, SYS.1.1, APP.3.3.
G 0.23	Unbefugtes Eindringen in IT-Systeme	C, I	Hoch	Anforderungen der Bausteine ORP.4, OPS.1.2.4, DER.1, DER.2.1 sowie: <ul style="list-style-type: none"> <li>• ORP.4.A21 (Mehr-Faktor-Authentisierung)</li> </ul>
G 0.25	Ausfall von Geräten oder Systemen	A	Hoch	Anwendung der Standard-Maßnahmen und Akzeptanz des Restrisikos.
G 0.26	Fehlfunktion von Geräten oder Systemen	C, I, A	Hoch	Anforderungen des Bausteins OPS.1.1.2, OPS.1.1.3, OPS.1.1.5, DER.1, DER.2.1, DER.2.3 sowie: <ul style="list-style-type: none"> <li>• CON.1.A14 (Schulung von Benutzern und Administratoren)</li> </ul>

Gefährdung	Titel	Schutzziel	Risiko	Maßnahmen zur Risikobehandlung
G 0.27	Ressourcenmangel	A	Sehr Hoch	Anforderungen der Bausteine OPS.1.1.2, SYS.1.1, APP.3.3 sowie: <ul style="list-style-type: none"> <li>CON.5.A13 (Entwicklung eines Redundanzkonzeptes für Anwendungen)</li> </ul>
G 0.28	Software-Schwachstellen oder -Fehler	C, I, A	Mittel	Anforderungen der Bausteine OPS.1.1.2, OPS.1.1.3, OPS.1.1.5, DER.1, DER.2.1, DER.2.3, APP.3.3.
G 0.30	Unberechtigte Nutzung von Geräten und Systemen	C, I	Mittel	Anforderungen der Bausteine OPR.4, OPS.1.1.2, DER.1 sowie: <ul style="list-style-type: none"> <li>ORP.4.A21 (Mehr-Faktor-Authentisierung)</li> </ul>
G 0.31	Fehlerhafte Nutzung von Geräten und Systemen	C, I, A	Hoch	Anforderungen der Bausteine ORP.2, OPS.1.1.2 sowie: <ul style="list-style-type: none"> <li>OPS.1.1.2.A17 (IT-Administration im Vier-Augen-Prinzip)</li> </ul>
G 0.32	Missbrauch von Berechtigungen	C, I	Hoch	Anforderungen der Bausteine ORP.2, ORP.4, OPS.1.1.2 sowie: <ul style="list-style-type: none"> <li>ORP.5.A10 (Klassifizierung von Informationen)</li> <li>OPS.1.1.2.A14 (Sicherheitsüberprüfung von Administratoren)</li> <li>OPS.1.1.2.A17 (IT-Administration im Vier-Augen-Prinzip)</li> </ul>
G 0.39	Schadprogramme	C, I, A	Sehr Hoch	Anforderungen der Bausteine OPS.1.1.4, DER.1, DER.2.1, DER.2.3 sowie: <ul style="list-style-type: none"> <li>ORP.3.A9 (Spezielle Schulung von exponierten Personen und Institutionen)</li> <li>DER.1.A16 (Einsatz von Detektionssystemen nach Schutzbedarfsanforderungen)</li> </ul>
G 0.40	Verhinderung von Diensten (Denial of Service)	A	Hoch	Anforderungen der Bausteine CON.5, DER.1, DER.2.1, SYS.1.1, APP.3.3 sowie: <ul style="list-style-type: none"> <li>CON.5.A13 (Entwicklung eines Redundanzkonzeptes für Anwendungen)</li> </ul>
G 0.43	Einspielen von Nachrichten	I	Gering	Anforderungen der Bausteine CON.1, OPS.1.1.5, SYS.1.1, APP.3.3, INF.4 sowie: <ul style="list-style-type: none"> <li>CON.1.A10 (Entwicklung eines Kryptokonzeptes)</li> </ul>
G 0.44	Unbefugtes Eindringen in Räumlichkeiten	C, I	Gering	Anforderungen der Bausteine INF.1, INF.2 sowie: <ul style="list-style-type: none"> <li>INF.2.A24 (Einsatz von Videoüberwachungsanlagen)</li> </ul>
G 0.45	Datenverlust	A	Hoch	Anforderungen der Bausteine CON.3, CON.5, OPS.1.1.6, DER.2.1, DER.4 sowie: <ul style="list-style-type: none"> <li>CON.1.A14 (Schulung von Benutzern und Administratoren)</li> </ul>



Gefährdung	Titel	Schutzziel	Risiko	Maßnahmen zur Risikobehandlung
				<ul style="list-style-type: none"> <li>CON.5.A13 (Entwicklung eines Redundanzkonzeptes für Anwendungen)</li> </ul>
G 0.46	Integritätsverlust schützenswerter Informationen	I	Gering	Anforderungen der Bausteine CON.1, OPS.1.1.5, SYS.1.1, APP.3.3.

# Kapitel 8                    Anwendungshinweise

## 8.1    Andere IT-Grundschutz-Profile

Neben den Anforderungen und Anmerkungen dieses IT-Grundschutz-Profiles können die Anwender ebenfalls auf das IT-Grundschutz-Profil der Basis-Absicherung für Kommunalverwaltungen zurückgreifen. Während eine Kommunalverwaltung über andere Aufgaben und Geschäftsprozesse verfügt, werden diese, abgesehen von spezifischen Fachverfahren, üblicherweise über ähnliche Anwendungen und IT-Systeme bewältigt. Diesem IT-Grundschutz-Profil lassen sich daher nützliche Hinweise bezüglich der hier empfohlenen Anforderungen entnehmen.

Zudem werden weitere IT-Grundschutz-Profile über das BSI veröffentlicht, deren Ansätze und Kommentare auch für das ISMS einer obersten Landesbehörde von Vorteil sein können.

## 8.2    Internationale ISMS-Standards

Neben Publikationen des BSI können zur Umsetzung eines ISMS andere ISMS-Standards herangezogen werden. Dazu empfiehlt sich insbesondere der ISO Standard 27001:2013 sowie der Standard 27002:2013 als Handlungsanleitung zu der ISMS-Umsetzung nach der ISO 27001.

Die Anmerkungen in diesen Dokumenten können für die Anwender der Standard-Absicherung relevant sein, da diese sich das ISMS nach der Standard-Absicherung auch über die ISO 27001:2013 zertifizieren lassen können.

Aus dem gleichen Normenbereich können bei entsprechendem Interesse die Standards 27003:2010 (Leitfaden zu der Umsetzung des ISMS), 27004:2012 (Messbarkeit des ISMS) und 27005:2018 (Informationssicherheits-Risikomanagement) ebenfalls berücksichtigt werden. Allerdings sollte vor einer Anschaffung bedacht werden, dass die Umsetzung der Standard-Absicherung nach IT-Grundschutz die dort formulierten Anforderungen erfüllt.

## 8.3    Weiterentwicklung des IT-Grundschutz-Profiles

Wie das BSI bereits in seinen Publikationen und Veranstaltungen zu dem IT-Grundschutz hervorhebt, profitieren die IT-Grundschutz-Profile besonders durch Beteiligung der betroffenen Institutionen und den dortigen Erfahrungen.

Auch wenn dieses IT-Grundschutz-Profil unter Rücksprache mit mehreren Verantwortlichen der obersten Landesbehörden erstellt wurde, sind zukünftig Verbesserungen zu erwarten. Erst durch die Rückmeldung und Beteiligung von Anwendern können zuvor unbekannte Fehler verbessert und das Profil so effizienter gestaltet werden.

Ebenso besteht die Möglichkeit, auf Basis dieser Ausarbeitung weitere IT-Grundschutz-Profile für spezielle Landesbehörden zu generieren. Diese wären in der Lage, besondere Fachverfahren einer bestimmten Behörde aufzunehmen und gegebenenfalls einen individuellen Baustein dafür abzubilden. Dies würde sich insbesondere bei Ebenen-übergreifenden Fachverfahren anbieten, die gemeinsamen Sicherheitsbestrebungen unterliegen.

## Kapitel 9                      Literatur

- [1] K. Möltgen-Sicking und T. Winter, *Verwaltung und Verwaltungswissenschaft: Eine praxisorientierte Einführung*. Wiesbaden: Springer VS, 2018.
- [2] J. Bogumil und W. Jann, *Verwaltung und Verwaltungswissenschaft in Deutschland: Einführung in die Verwaltungswissenschaft*, 2. Aufl. Wiesbaden: VS Verlag für Sozialwissenschaften, 2009.
- [3] Bundesamt für Sicherheit in der Informationstechnik, „Zuordnung ISO/IEC 27001 sowie ISO/IEC 27002 zum modernisierten IT-Grundschutz“, Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, 2018.
- [4] T. Nentwig und C. Werwath, Hg., *Politik und Regieren in Niedersachsen*. Wiesbaden: Springer VS, 2016.
- [5] R. Heuermann, M. Tomenendal und C. Bressemer, Hg., *Digitalisierung in Bund, Ländern und Gemeinden: IT-Organisation, Management und Empfehlungen*. Berlin, Germany: Springer Gabler, 2018.
- [6] D. Schamburek, „Die Ansiedlung von Aufgaben in der Aufbauorganisation deutscher Landesministerialverwaltungen“. Dissertation, 2016.
- [7] P. Fischer und P. Hofer, *Lexikon der Informatik*, 15. Aufl. Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg, 2011.
- [8] StatCounter, *Global Market Share Held by Operating Systems for Desktop Pcs, from January 2013 to January 2019*. [Online] Verfügbar unter: [www.statista.com/statistics/218089/global-market-share-of-windows-7](http://www.statista.com/statistics/218089/global-market-share-of-windows-7). Zugriff am: 15. Februar 2019.
- [9] ITCandor, *Share of the global server market by operating system in the first half of 2018*. [Online] Verfügbar unter: <https://www.statista.com/statistics/915085/global-server-share-by-os>. Zugriff am: 15. Februar 2019.
- [10] Kantar, *Share of The Leading Smartphone Operating Systems in The Sales Volume of Smartphones in Germany from January 2012 to September 2018*. [Online] Verfügbar unter: [www.statista.com/statistics/461959/smartphone-os-sales-volume-share-germany](http://www.statista.com/statistics/461959/smartphone-os-sales-volume-share-germany). Zugriff am: 15. Februar 2019.
- [11] *ISO/IEC 27002:2013*, 2013.
- [12] *NIST Special Publication 800-63B*, 2017.
- [13] *Data Security Standard*, 2018.
- [14] *BSI-Standard 200-2*, 2017.
- [15] M. Herr, C. E. Müller, B. Engewald und J. Ziekow, „Transparenzgesetzgebung in Deutschland in der Bewährung: Erfahrungen einer Gesetzesevaluation“, *DÖV (Die Öffentliche Verwaltung)*, Jg. 5, S. 165–168, 2018.
- [16] *ISO 31000:2018*, 2018.
- [17] *BSI-Standard 200-3*, 2017.
- [18] Bundesanzeiger Verlag GmbH; Deutschland, *IT-Grundschutz-Kompendium: 2. Edition 2019*. Köln: Bundesanzeiger Verlag, 2019.