

IT-Grundschutz-Profil für Ressort-Forschungseinrichtungen

Version: 1.0

Revisionszyklus: 2 Jahre

Version IT-Grundschutz-Kompendium 2023

Inhaltsverzeichnis

1	Einleitung.....	1
2	Formale Aspekte.....	1
3	Haftungsausschluss.....	2
4	Liste der Autorinnen und Autoren.....	2
5	Festlegung des Geltungsbereichs.....	3
6	Abgrenzung des Informationsverbundes	4
7	Referenzarchitektur	4
7.1	Geschäftsprozesse / Fachaufgaben	4
7.2	Anwendungen	5
7.3	IT-Systeme.....	6
7.4	Netze und Netzkomponenten.....	6
7.5	Gebäude und Räume	7
7.5.1.	Netzplan.....	8
7.6	Umgang mit Abweichungen	9
8	Zu erfüllende Anforderungen und umzusetzende Maßnahmen	9
8.1	Feststellung des Schutzbedarfs	9
8.2	Zuordnung der relevanten Bausteine	10
8.3	Relevanz der Anforderungen	13
9	Restrisiko.....	14
10	Anwendungshinweise.....	14
11	Unterstützende Informationen	14

Versionshistorie

Datum	Version	Änderung	Bearbeiter
09.09.2024	1.0	Fertigstellung Version 1.0	Siehe Liste der Autorinnen und Autoren

Tabelle 1: Versionshistorie

1 Einleitung

Die Ressort-Forschungseinrichtungen des Bundes dienen mit ihren Forschungs- und Entwicklungstätigkeiten als Ratgeber für politische Entscheidungen. Sie decken ein breites Aufgabenspektrum mit mannigfaltigen Aufgaben ab. Zusätzlich zu ihren Forschungsprojekten übernehmen sie auch Verwaltungsaufgaben.

Sowohl sensible Forschungstätigkeiten als auch die Verwaltungsaufgaben, bei denen teilweise Informationen im Bereich VS-NfD verarbeitet werden, erfordern ein hohes Sicherheitsniveau. Gleiches gilt für den Informationsaustausch zwischen den beiden Bereichen, der sicher erfolgen muss.

Die Sicherheitsanforderungen aus dem IT-Grundschutz und den Mindeststandards sind nicht immer 1:1 im Forschungsbereich umzusetzen, und so muss das benötigte Sicherheitsniveau in den verschiedenen Bereichen mit angepassten Maßnahmen erreicht werden.

In Ressort-Forschungseinrichtungen besteht daher die Herausforderung, die Anforderungen zur Erreichung eines hohen Sicherheitsniveaus mit den Anforderungen der Forschungsaktivitäten in Einklang zu bringen.

Dieses Profil dient als erste grundlegende Vorlage für Ressort-Forschungseinrichtungen zum Aufbau eines Informationssicherheitsmanagements. In einem weiteren Schritt sollten die Erfahrungen bei der Umsetzung in eine zukünftige Version des Profils eingearbeitet werden, um so das Profil sukzessive fortzuentwickeln und auszubauen.

Sollten Sie bei der Anwendung des IT-Grundschutz-Profiles Anmerkungen oder Ergänzungen haben oder möchten Sie an einer Weiterentwicklung des IT-Grundschutz-Profiles mitarbeiten, wenden Sie sich bitte an sicherheitsberatung@bsi.bund.de

2 Formale Aspekte

Aspekt	Beschreibung
Titel:	IT-Grundschutz-Profil für Ressort-Forschungseinrichtungen
Autoren:	Siehe Liste der Autorinnen und Autoren
Version:	1.0
IT-Grundschutz-Kompodium:	Edition 2023
Revisionszyklus:	2 Jahre
Vertraulichkeit:	-/-

Tabelle 2: Formale Aspekte.

3 Haftungsausschluss

Dieses Dokument wurde mit größter Sorgfalt erstellt, erhebt aber keinen Anspruch auf Vollständigkeit und Richtigkeit. Die Autorinnen und Autoren haben keinen Einfluss auf die Nutzung dieses IT-Grundschutz-Profiles durch Anwenderinnen und Anwender, sodass sie naturgemäß für die Auswirkungen auf die Rechtsposition der Parteien keine Haftung übernehmen können.

4 Liste der Autorinnen und Autoren

Name	Organisation
Fisseler, Daniela	Bundesamt für Naturschutz
Schumann, Beate	Bundesamt für Naturschutz
Weinzettel, Roland	Bundesanstalt für Arbeitsschutz und Arbeitsmedizin
Lehnigk, Carina	Bundesanstalt für Gewässerkunde
Müller, Lukas	Bundesanstalt für Gewässerkunde
Pirke, Herbert	Bundesanstalt für Materialforschung und -prüfung
Wille, Robert	Bundesanstalt für Materialforschung und -prüfung
Schäning, Melanie	Bundesanstalt für Straßenwesen
Stobäus, Patrick	Bundesanstalt für Straßenwesen
Toptas, Ayhan	Bundesanstalt für Straßenwesen
Held, Alexander	Bundesinstitut für Arzneimittel und Medizinprodukte
Lauterbach, Thomas	Bundesinstitut für Arzneimittel und Medizinprodukte
Sibold, Dieter	Physikalisch-Technische Bundesanstalt
Bodurski, Ivaylo	Robert Koch-Institut
Hahn, Sabrina	Robert Koch-Institut
Beule, Bernd	Umweltbundesamt
Blankenburg, Steffi	Umweltbundesamt
Starogardzki, Michael	Umweltbundesamt
Becker, Sylvia	Bundesamt für Sicherheit in der Informationstechnik
Biere, Thomas	Bundesamt für Sicherheit in der Informationstechnik
Brückmann, Andreas	Bundesamt für Sicherheit in der Informationstechnik
Klein, Birger	Bundesamt für Sicherheit in der Informationstechnik
Scharkoff, Jo-Ann	Bundesamt für Sicherheit in der Informationstechnik

Tabelle 3: Liste der Autorinnen und Autoren.

Sollten Sie bei der Anwendung des IT-Grundschutz-Profiles Anmerkungen oder Ergänzungen haben oder möchten Sie an einer Weiterentwicklung des IT-Grundschutz-Profiles mitarbeiten, wenden Sie sich bitte an das GP: sicherheitsberatung@bsi.bund.de.

5 Festlegung des Geltungsbereichs

Zielgruppe

Dieses IT-Grundschutz-Profil richtet sich an die für das Informationssicherheitsmanagement zuständigen Rollen der Ressort-Forschungseinrichtungen und Institutionen.

Beschreibung des Schutzbedarfs

Der Schutzbedarf wird innerhalb des Kreises der Ressort-Forschungseinrichtungen je nach spezifischen Forschungs- und weiteren Aufgabenbereichen variieren. Im Bereich der Forschung, die sich u.a. durch vielfältige nationale und internationale Vernetzung und transparente und offene Kommunikation auszeichnet, wird häufig von einem normalen Schutzbedarf ausgegangen. Gleichzeitig kann es einzelne Forschungsbereiche mit hohem oder sehr hohem Schutzbedarf für einzelne Schutzziele geben. Beispiele sind Labore mit gefährlichen Schadstoffen oder Bereiche, die für die Reputation der Ressort-Forschungseinrichtung in der Öffentlichkeit und der Wirtschaft von besonderer Relevanz sind.

Als Bundesbehörden verfügen Ressort-Forschungseinrichtungen häufig über Netzwerksegmente, die mit den Netzen des Bundes verbunden sind. Über diese Netzwerksegmente werden auch als Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte Informationen innerhalb der Bundesverwaltung ausgetauscht.

Eine allgemeingültige Beschreibung des Schutzbedarfs ist nicht möglich, jede Institution muss den Schutzbedarf individuell bestimmen. In Kapitel 8.1. werden als Hilfestellung Hinweise/Merkmale gegeben, die auf einen erhöhten Schutzbedarf hindeuten können.

IT-Grundschutz Vorgehensweise

Der IT-Grundschutz nach dem BSI-Standard 200-2 bietet grundsätzlich die Optionen der Basis-, Standard- und Kernabsicherung. Da der Umsetzungsplan Bund 2017 in der Bundesverwaltung mindestens die Standard-Absicherung verlangt, wird von dieser Variante bei den hier beschriebenen Anforderungen ausgegangen.

Kompatibilität zu anderen Standards

Für Geschäftsprozesse und Zielobjekte mit normalen Schutzbedarf erfüllt dieses IT-Grundschutz-Profil die Anforderungen der DIN ISO/IEC 27001. In Bereichen mit hohem Schutzbedarf bedarf der Umsetzung einer zum IT-Grundschutz konformen Risikoanalyse, um Konformität zur DIN ISO/IEC 27001 zu erreichen.

Berücksichtigte Rahmenbedingungen

Das IT-Grundschutz-Profil für Ressort-Forschungseinrichtungen und vergleichbare Institutionen berücksichtigt die Vorgaben des BSI-Gesetzes, der DSGVO, des Umsetzungsplanes Bund 2017 und des Mindeststandards Nutzerpflichten NdB. Mit der vorgeschlagenen Referenzarchitektur ist eine rechtskonforme Anbindung an die NdB möglich.

6 Abgrenzung des Informationsverbundes

Der Geltungsbereich einer Sicherheitskonzeption nach BSI-Standard 200-2 wird als Informationsverbund bezeichnet. Da Ressort-Forschungseinrichtungen sehr unterschiedliche Ausprägungen haben, konzentriert sich dieses IT-Grundschutz-Profil weniger auf einzelne Geschäftsprozesse, sondern fokussiert sich auf die dafür benötigte Basis-IT zur Bürokommunikation, die in allen Ressort-Forschungseinrichtungen eingesetzt wird.

Neben dieser Basis-IT eingesetzte Fachverfahren oder Spezialanwendungen werden im Rahmen dieses IT-Grundschutz-Profiles nicht weiter berücksichtigt. Sollten Anwenderinnen und Anwender dieses Profils in ihrem Informationsverbund derartige zusätzliche Dienste einsetzen, müssten diese individuell modelliert werden. Hinweise zum Umgang mit Abweichungen bzw. zur Erweiterung des Informationsverbunds wird unter Punkt 7.6 beschrieben.

7 Referenzarchitektur

7.1 Geschäftsprozesse / Fachaufgaben

Fachaufgabe / Tätigkeit		Beschreibung Fachaufgabe / Tätigkeit
GP01	Basis-IT	Bürokommunikation, Berichtspflichten, Austausch mit anderen Einrichtungen
GP02	VS-Verarbeitung	Austausch und Verarbeitung von VS-Inhalten

Tabelle 4: Geschäftsprozesse / Fachaufgaben

7.2 Anwendungen

Identifikator	Anwendungen	Zuordnung zu Prozessen
A01	Webanwendungen	GP01
A02	Webserver	GP01
A03	Datenbank	GP01
A04	Office-Anwendungen	GP01
A05	Webbrowser	GP01
A06	Active Directory	GP01
A07	Fileserver	GP01
A08	Exchange E-Mail	GP01
A09	Datenbank	GP01
A10	Mobile Anwendungen	GP01
A11	Office-Anwendungen	GP01
A12	Webbrowser	GP01
A13	Datenbank	GP01
A14	Office-Anwendungen	GP02
A15	Webbrowser	GP02
A16	Datenbank	GP02
A17	Video-TK-Anlage VS-NfD	GP02

Tabelle 5: Anwendungen

7.3 IT-Systeme

Identifikator	IT-Systeme	Zuordnung zu Anwendungen
S01	Öffentliche Dienste (Webserver mit Webapplikation, Datenbank)	A01, A02, A03
S02	Büro-Client (Windows mit Office-Anwendungen)	A04, A05
S03	Büro-Notebook (Windows mit Office-Anwendungen)	A04, A05
S04	VK-Anlage	-
S05	Interne Dienste (Fachanwendungen mit Datenbanken usw.)	A06, A07, A08, A09
S06	Mobiler Client (Tablet)	A10
S07	Mobiltelefon	-
S08	Management-Client (Windows)	A11, A12
S09	Management-Dienste (Windows)	A13
S10	VS-NfD Client (Windows)	A14, A15
S11	VS-Nfd Dienste (Fachanwendungen mit Datenbanken)	A16
S12	TK-Anlage VS-NfD	-
S13	Telefon VS-NfD	-
S14	Video-TK-Anlage VS-NfD	A17

Tabelle 6: IT-Systeme

7.4 Netze und Netzkomponenten

Identifikator	Netze und Netzkomponenten	Zuordnung IT-Systeme
N01	Firewall (Internet)	-
N2	Router, Switches, Netze	-
N03	Router, Switches, Netze	-
N04	WLAN	-
N05	Firewall (NdB)	-

Tabelle 7: Netze und Netzkomponenten

7.5 Gebäude und Räume

Identifikator	Gebäude oder Raum	Zuordnung zu IT-Systemen / Netzkomponenten
G01	Gebäude 1	
M01	Unterwegs - Mobil	S06, S07
RZ	Rechenzentrum	S01, S05, S09, S11, N01, N02, N05
R01	Büro-Raum	S02, S03, S08, S10, S13
R02	Besprechungs-Raum	S14
TR	Technik-Raum	S04, S12, N03, N04

Tabelle 8: Gebäude und Räume

7.5.1. Netzplan

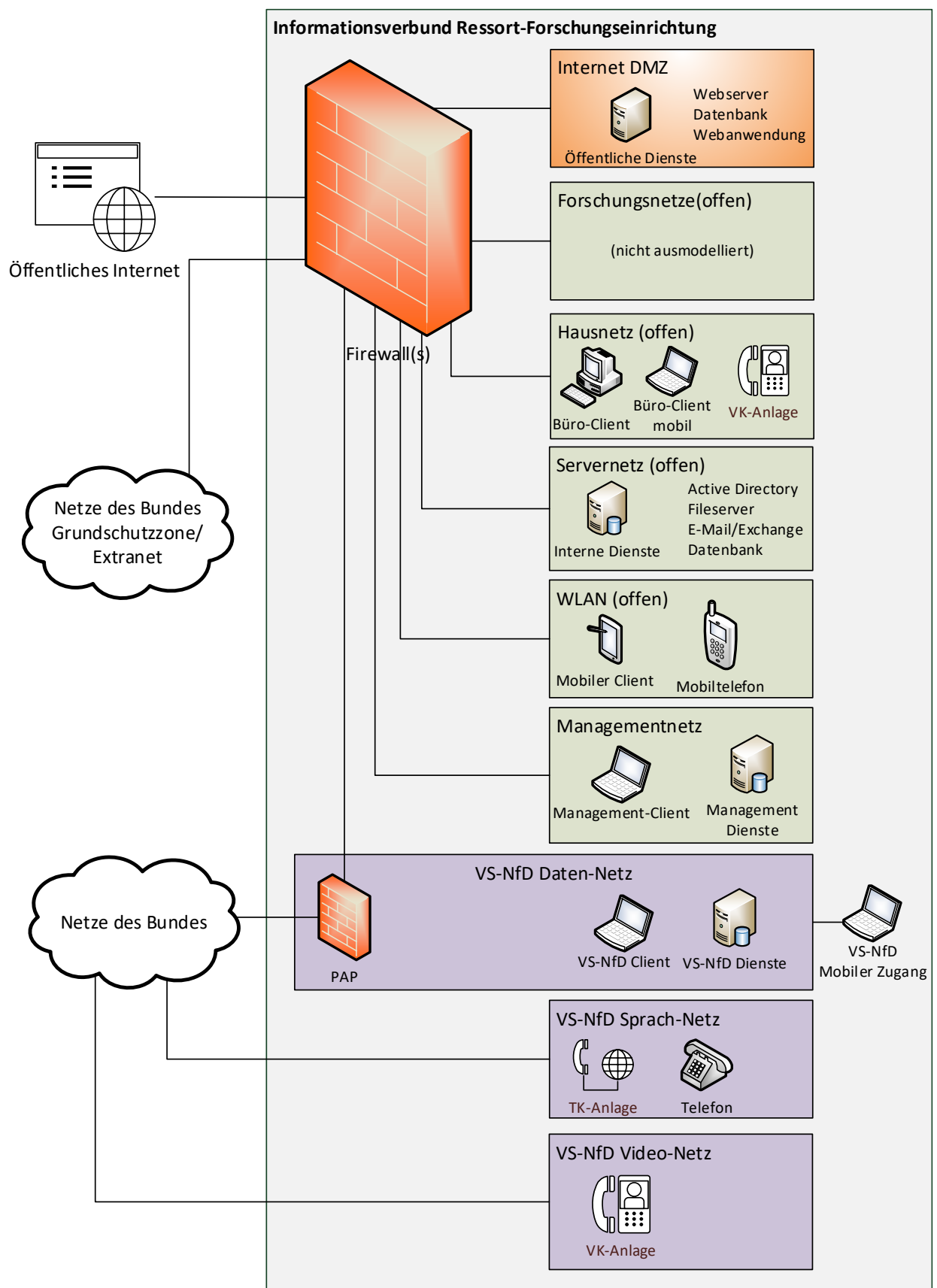


Abbildung 1: Netzplan

7.6 Umgang mit Abweichungen

Weicht der zu schützende Informationsverbund von der Referenzarchitektur ab, sind die zusätzlichen oder nicht vorhandenen Objekte zu ergänzen. Diesen Objekten sind den entsprechenden Bausteine des IT-Grundschutz-Kompends zuzuordnen. Die aus den Bausteinen abgeleiteten Anforderungen müssen in Abhängigkeit des Schutzbedarfs angepasst werden.

8 Zu erfüllende Anforderungen und umzusetzende Maßnahmen

Das IT-Grundschutz-Kompensum ist die grundlegende Veröffentlichung des IT-Grundschutzes. Im Fokus des IT-Grundschutz-Kompends stehen die sogenannten IT-Grundschutz-Bausteine. In den IT-Grundschutz-Bausteinen werden jeweils zu einem Thema alle relevanten Sicherheitsaspekte beleuchtet und Sicherheitsanforderungen zur Absicherung gegeben.

In einem IT-Grundschutz-Profil kann vorgegeben werden, ob alle Anforderungen eines Bausteins oder lediglich eine Auswahl relevant sind. Außerdem können und sollten die ausgewählten Anforderungen konkretisiert werden. Nicht vorhandene Anforderungen aus den IT-Grundschutz-Bausteinen können dem IT-Grundschutz-Profil zugeordnet werden, sowie auch bisher im IT-Grundschutz noch nicht vorhandene Anforderungen. Auf diese Weise kann mit Hilfe der IT-Grundschutz-Profile ein Sicherheitsniveau erreicht werden, das exakt dem Schutzbedarf des betrachteten Anwendungsbereiches entspricht.

Hierzu ist zunächst der Schutzbedarf der Geschäftsprozesse / Fachaufgaben, Anwendungen, IT-Systeme und Kommunikationsverbindungen festzulegen. Anschließend müssen die relevanten Bausteine identifiziert und ggf. eine Anpassung der Anforderungen an die entsprechende Zielgruppe durchgeführt werden.

8.1 Feststellung des Schutzbedarfs

Ziel der Schutzbedarfsfeststellung ist es, für die erfassten Objekte im Geltungsbereich zu entscheiden, welchen Schutzbedarf sie bezüglich Vertraulichkeit, Integrität und Verfügbarkeit besitzen. Dieser Schutzbedarf orientiert sich an den möglichen Schäden, die eintreten können. Die Grundlage zur Bestimmung des Schutzbedarfs verschiedener Objekte ist der Schutzbedarf der Geschäftsprozesse und der zugehörigen Informationen. Der für diese Elemente ermittelte Schutzbedarf vererbt sich auf die für deren Verarbeitung genutzten Objekte, also Anwendungen, IT-Systeme, Gebäude und Räume und Kommunikationsverbindungen. Das Vorgehen ist im Detail im BSI-Standard 200-2 beschrieben. Wenn nicht anders angegeben, werden in diesem IT-Grundschutz-Profil die Schadensszenarien und Schutzbedarfskategorien aus dem BSI-Standard 200-2 verwendet.

Dieses IT-Grundschutz-Profil behandelt die Geschäftsprozesse „Basis-IT“ und „VS-Verarbeitung“, da diese Geschäftsprozesse in allen Ressort-Forschungseinrichtungen vorkommen. Die Informationen, die bei diesen Geschäftsprozessen verarbeitet werden, sind bei den verschiedenen Ressort-Forschungseinrichtungen sehr unterschiedlich. Daher können keine sinnvollen und allgemeingültigen Annahmen getroffen werden, welche Informationen verarbeitet werden, wodurch eine vollständige Schutzbedarfsfeststellung nicht möglich ist.

Aus diesem Grunde wird als Ausgangspunkt der Schutzbedarf „normal“ für Verfügbarkeit, Vertraulichkeit und Integrität angenommen. Es werden im folgenden Hinweise/Merkmale gegeben, die auf einen erhöhten Schutzbedarf hindeuten können. Diese Vorgehensweise bietet Anwenderinnen und Anwendern, die das IT-Grundschutz-Profil umsetzen, für ihre individuelle Schutzbedarfsfeststellung einen Mehrwert.

Schutzziel	Kriterien, die den Schutzbedarf erhöhen können
Vertraulichkeit	<ul style="list-style-type: none"> • Betriebs- und Geschäftsgeheimnisse • besondere personenbezogene Daten/Kategorien, Sozialgeheimnis, Verschlusssachen • Ggf. Anforderungen aus Mindeststandards (z.B. NdB Nutzerpflichten) • Forschungsdaten mit besondere Auswirkung (z.B. auf Leib und Leben)
Integrität	<ul style="list-style-type: none"> • Gesundheitsdaten • Forschungsdaten mit besondere Auswirkung (z.B. auf Leib und Leben) • Publierte Daten (Reputationsschaden)
Verfügbarkeit	<ul style="list-style-type: none"> • Gesundheitsdaten • Aufgrund gesetzlicher oder vertraglicher Vorgaben bezgl. Verfügbarkeit • Betrieb von „kritischer“ Infrastruktur • Forschungsdaten mit besondere Auswirkung (z.B. auf Leib und Leben)

Tabelle 9: Kriterien, die den Schutzbedarf erhöhen können

8.2 Zuordnung der relevanten Bausteine

Nachdem die Referenzarchitektur mit den entsprechenden Zielobjekte definiert ist und die Schutzbedarfsfeststellung durchgeführt wurde, besteht die nächste Aufgabe darin, den betrachteten Informationsverbund (Untersuchungsgegenstand) mit Hilfe des IT-Grundschutz-Modells nachzubilden. Dafür werden im IT-Grundschutz-Kompendium vorhandene Bausteine ausgewählt (siehe auch BSI-Standard 200-2, Kapitel 8.3 Modellierung eines Informationsverbunds oder Kapitel 2 des IT-Grundschutz-Kompendiums).

Modellierung

Baustein	Modellierung
ISMS.1 Sicherheitsmanagement	Ja
ORP.1 Organisation	Ja
ORP.2 Personal	Ja
ORP.3 Sensibilisierung und Schulung zur Informationssicherheit	Ja
ORP.4 Identitäts- und Berechtigungsmanagement	Ja
ORP.5 Compliance Management (Anforderungsmanagement)	Ja
CON.1 Kryptokonzept	Ja
CON.2 Datenschutz	Ja, wenn personenbezogene Daten verarbeitet werden
CON.3 Datensicherungskonzept	Ja
CON.6 Löschen und Vernichten	Ja
CON.7 Informationssicherheit auf Auslandsreisen	Ja, wenn Auslandsreisen stattfinden
CON.8 Software-Entwicklung	Nein, nicht im Einsatz
CON.9 Informationsaustausch	Ja
CON.10 Entwicklung von Webanwendungen	Nein, nicht im Einsatz
CON.11.1 Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)	Ja
OPS.1.1.1 Allgemeiner IT-Betrieb	Ja
OPS.1.1.2 Ordnungsgemäße IT-Administration	Ja
OPS.1.1.3 Patch- und Änderungsmanagement	Ja
OPS.1.1.4 Schutz vor Schadprogrammen	Ja
OPS.1.1.5 Protokollierung	Ja
OPS.1.1.6 Software-Tests und -Freigaben	Ja
OPS.1.1.7 Systemmanagement	Nein, nicht im Einsatz
OPS.1.2.2 Archivierung	Ja, wenn Langzeitspeicherung erforderlich
OPS.1.2.4 Telearbeit	Ja, wenn im Einsatz
OPS.1.2.5 Fernwartung	Ja
OPS.1.2.6 NTP -Zeitsynchronisation	Ja (für alle IT-Systeme, die NTP nutzen)
OPS.2.2 Cloud-Nutzung	Nein, nicht im Einsatz
OPS.2.3 Nutzung von Outsourcing	Nein, nicht im Einsatz
OPS.3.2 Anbieten von Outsourcing	Nein, nicht im Einsatz
DER.1 Detektion von sicherheitsrelevanten Ereignissen	Ja
DER.2.1 Behandlung von Sicherheitsvorfällen	Ja
DER.2.2 Vorsorge für die IT-Forensik	Ja
DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle	Ja
DER.3.1 Audits und Revisionen	Ja
DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision	Ja
DER.4 Notfallmanagement	Ja
APP.1.1 Office-Produkte	A04, A11, A14
APP.1.2 Webbrowser	A05, A12, A15
APP.1.4 Mobile Anwendungen (Apps)	A10
APP.2.1 Allgemeiner Verzeichnisdienst	A06

APP.2.2 Active Directory Domain Services	A06
APP.2.3 OpenLDAP	Nein, nicht im Einsatz
APP.3.1 Webanwendungen und Webservices	A01
APP.3.2 Webserver	A02
APP.3.3 Fileserver	A07
APP.3.4 Samba	Nein, nicht im Einsatz
APP.3.6 DNS-Server	A06
APP.4.2 SAP-ERP-System	Nein, nicht im Einsatz
APP.4.3 Relationale Datenbanken	A03, A09, A13, A16
APP.4.4 Kubernetes	Nein, nicht im Einsatz
APP.4.6 SAP ABAP-Programmierung	Nein, nicht im Einsatz
APP.5.2 Microsoft Exchange und Outlook	A08
APP.5.3 Allgemeiner E-Mail-Client und -Server	A08
APP.5.4 Unified Communications und Collaboration (UCC)	A17
APP.6 Allgemeine Software	A01, A02, A03, A04, A05, A06, A07, A08, A09, A10, A11, A12, A13, A14, A15, A16, A17
APP.7 Entwicklung von Individualsoftware	Nein, nicht im Einsatz
SYS.1.1 Allgemeiner Server	S01, S05, S09, S11
SYS.1.2.2 Windows Server 2012	Nein, nicht im Einsatz
SYS.1.2.3 Windows Server	S01, S05, S09, S11
SYS.1.3 Server unter Linux und Unix	Nein, nicht im Einsatz
SYS.1.5 Virtualisierung	Nein, nicht im Einsatz
SYS.1.6 Containerisierung	Nein, nicht im Einsatz
SYS.1.7 IBM Z	Nein, nicht im Einsatz
SYS.1.8 Speicherlösungen	Nein, nicht im Einsatz
SYS.1.9 Terminalserver	Nein, nicht im Einsatz
SYS.2.1 Allgemeiner Client	S02, S03, S08, S10
SYS.2.2.3 Clients unter Windows	S02, S03, S08, S10
SYS.2.3 Clients unter Linux und Unix	Nein, nicht im Einsatz
SYS.2.4 Clients unter macOS	Nein, nicht im Einsatz
SYS.2.5 Client-Virtualisierung	Nein, nicht im Einsatz
SYS.2.6 Virtual Desktop Infrastructure	Nein, nicht im Einsatz
SYS.3.1 Laptops	S03
SYS.3.2.1 Allgemeine Smartphones und Tablets	S06
SYS.3.2.2 Mobile Device Management (MDM)	Nein, nicht im Einsatz
SYS.3.2.3 iOS (for Enterprise)	Ja, wenn iOS im Einsatz
SYS.3.2.4 Android	Ja, wenn Android im Einsatz
SYS.3.3 Mobiltelefon	S06, S07
SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte	Nein, nicht im Einsatz
SYS.4.3 Eingebettete Systeme	Nein, nicht im Einsatz
SYS.4.4 Allgemeines IoT-Gerät	Nein, nicht im Einsatz
SYS.4.5 Wechseldatenträger	Nein, nicht im Einsatz
NET.1.1 Netzarchitektur und -design	NET
NET.1.2 Netzmanagement	Ja, wenn Netzmanagement-System im Einsatz

NET.2.1 WLAN-Betrieb	NET
NET.2.2 WLAN-Nutzung	NET
NET.3.1 Router und Switches	NET
NET.3.2 Firewall	NET
NET.3.3 VPN	NET
NET.3.4 Network Access Control	Nein, nicht im Einsatz
NET.4.1 TK-Anlagen	S12
NET.4.2 VoIP	Nein, nicht im Einsatz
NET.4.3 Faxgeräte und Faxserver	Nein, nicht im Einsatz
IND.1 Prozessleit- und Automatisierungstechnik	Nein, nicht im Einsatz
IND.2.1 Allgemeine ICS-Komponente	Nein, nicht im Einsatz
IND.2.2 Speicherprogrammierbare Steuerung (SPS)	Nein, nicht im Einsatz
IND.2.3 Sensoren und Aktoren	Nein, nicht im Einsatz
IND.2.4 Maschine	Nein, nicht im Einsatz
IND.2.7 Safety Instrumented Systems	Nein, nicht im Einsatz
IND.3.2 Fernwartung im industriellen Umfeld	Nein, nicht im Einsatz
INF.1 Allgemeines Gebäude	G1
INF.2 Rechenzentrum sowie Serverraum	RZ
INF.5 Raum sowie Schrank für technische Infrastruktur	TR
INF.6 Datenträgerarchiv	Nein, nicht im Einsatz
INF.7 Büroarbeitsplatz	R1
INF.8 Häuslicher Arbeitsplatz	Ja, wenn im Einsatz
INF.9 Mobiler Arbeitsplatz	Ja, wenn im Einsatz
INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume	R2
INF.11 Allgemeines Fahrzeug	Nein, nicht im Einsatz
INF.12 Verkabelung	G1
INF.13 Technisches Gebäudemanagement	Nein, nicht im Einsatz
INF.14 Gebäudeautomatisierung	Nein, nicht im Einsatz

Tabelle 10: Modellierung der Bausteine

8.3 Relevanz der Anforderungen

Nachdem die relevanten Bausteine des IT-Grundschutz-Kompendiums identifiziert worden sind, wird bei der Erstellung von IT-Grundschutz-Profilen im nächsten Schritt eine zielgruppengerechte Anpassung der Anforderungen vorgenommen. In den Bausteinen werden Anforderungen vorgeschlagen, die typischerweise für diese Komponenten geeignet und angemessen sind. Für die Erstellung eines IT-Grundschutz-Profiles müssen die einzelnen Anforderungen durchgearbeitet und, wenn nötig, an die Rahmenbedingungen des IT-Grundschutz-Profiles angepasst werden.

Es kann beispielsweise sinnvoll sein:

- alle Anforderungen eines Bausteins als relevant zu identifizieren,
- nur bestimmte Anforderungen als relevant zu identifizieren (z. B. nur Basis-Anforderungen),

- Anforderungen zu konkretisieren, also zum Beispiel, um weitere Aspekte zu ergänzen, oder
- Anforderungen komplett zu streichen.

Es können nicht nur vorhandene Anforderungen aus den IT-Grundschutz-Bausteinen dem IT-Grundschutz-Profil zugeordnet werden. In der Praxis wird es häufig erforderlich sein, zusätzliche Anforderungen zu identifizieren, die für den betrachteten Informationsverbund von Bedeutung sind. Dies ist beispielsweise dann der Fall, wenn ein erhöhter Schutzbedarf vorliegt. Auch wenn einzelne Zielobjekte der Referenzarchitektur nicht oder nicht hinreichend mit bestehenden Bausteinen aus dem IT-Grundschutz-Kompendium abgebildet werden können, müssen weitere Anforderungen ergänzt werden.

Auf diese Weise kann mit Hilfe der IT-Grundschutz-Profile ein Sicherheitsniveau erreicht werden, das exakt dem Schutzbedarf des betrachteten Anwendungsbereiches entspricht.

9 Restrisiko

Bei der Erstellung von IT-Grundschutz-Profilen werden im Rahmen von Risikoanalysen in der Regel ergänzende Sicherheitsanforderungen identifiziert, die über das IT-Grundschutz-Modell hinausgehen. Dabei werden typischerweise auch Risiken gefunden, die nicht alle durch vorgegebene Anforderungen bzw. dazugehörige Maßnahmen abgedeckt werden können. Solche Restrisiken müssen bewertet und dokumentiert werden. So sollte unter anderem aufgenommen werden, wenn vorhandene (Standard-)Anforderungen eines Bausteins nicht erfüllt werden oder wenn mit zusätzlichen Maßnahmen mehr Risiken abgedeckt werden könnten.

Darüber hinaus können sich im Einzelfall zusätzliche Risiken ergeben, die im Rahmen des Informationssicherheitsmanagements behandelt werden müssen.

10 Anwendungshinweise

Da das IT-Grundschutz-Profil mit der Basis-IT lediglich die kleinste gemeinsame Schnittmenge der IT der Ressort-Forschungseinrichtungen abdeckt, wird den Anwenderinnen und Anwendern dringend empfohlen, das Profil um diejenigen Geschäftsprozesse und damit verknüpften Lösungen anzureichern, die darüber hinaus im betrachteten Informationsverbund anzutreffen sind.

11 Unterstützende Informationen

Da das IT-Grundschutz-Profil der Umsetzung des IT-Grundschutzes in der Bundesverwaltung dient, welche im Umsetzungsplan Bund 2017 als Leitlinie für Informationssicherheit in der Bundesverwaltung festgelegt wurde, sollte dieser insbesondere bei der Ausgestaltung der Anforderungen zum Sicherheitsmanagement ebenfalls konsultiert werden.

Gleiches gilt für die Mindeststandards des BSI nach § 8 Abs.1 BSIG, die ebenso bei der Umsetzung der IT-Grundschutz-Anforderungen, ggf. sogar ergänzend im Sinne einer Verschärfung heranzuziehen sind. Dies gilt insbesondere für den Mindeststandard Nutzerpflichten NdB, sofern ein Anschluss an die NdB vorliegt.