

IT-Grundschutz-Profil für Leitstellen

Herausgeber: Fachverband Leitstellen e.V.

Version: 2.0

Revisionszyklus: jährlich

Version IT-Grundschutz-Kompendium 2023

Inhaltsverzeichnis

Vorwort.....	1
1 Management Summary.....	2
2 Festlegung des Geltungsbereichs.....	2
3 Abgrenzung des Informationsverbundes	3
3.1 Bestandteile des Informationsverbundes.....	3
3.2 Nicht berücksichtigte Teile.....	3
4 Referenzarchitektur	4
4.1 Prozesse	4
4.2 Anwendungen.....	5
4.3 IT-Systeme.....	6
4.4 Netze und Netzkomponenten	6
4.4.1. Netzplan.....	7
4.5 Gebäude und Räume	7
4.6 Umgang mit Abweichungen.....	8
5 Zu erfüllende Anforderungen und umzusetzende Maßnahmen.....	8
5.1 Feststellung des Schutzbedarfs.....	8
5.1.1. Schutzbedarfsfeststellung für Prozesse	12
5.1.2. Schutzbedarfsfeststellung für Anwendungen	14
5.1.3. Schutzbedarfsfeststellung für IT-Systeme	15
5.1.4. Schutzbedarfsfeststellung für Netzwerke.....	17
5.1.5. Schutzbedarfsfeststellung für Räume	17
5.2 Auswahl relevanter Bausteine	18
5.3 Anforderungen übergreifend gültiger Prozessbausteine	25
5.4 Anforderungen spezifisch gültiger Prozessbausteine.....	29
5.5 Anforderungen für spezifische Objekte	33
6 Restrisiko	34
7 Anwendungshinweise	34
8 Notfallmanagement (BCM).....	34
9 Unterstützende Informationen	35

Versionshistorie

Datum	Version	Änderung
12.02.2024	2.0	<ul style="list-style-type: none">- Hinweise zu BCM auf BSI Standard 200-4 aktualisiert- Vorwort aktualisiert- Bausteine an IT-Grundschutz-Kompendium Version 2023 angepasst
01.02.2021	1.0	Erstveröffentlichung

Vorwort

Moderne Leitstellenarbeit ist ohne eine sicher funktionierende und performante IT Infrastruktur nicht vorstellbar. Dabei ist für die zunehmende Digitalisierung der Arbeitsprozesse die Sicherung der Verfügbarkeit, der Datenintegrität sowie der Vertraulichkeit stets sicherzustellen. Die digitalisierten Arbeitsprozesse erstrecken sich vom Notrufeingang, über die Ermittlung des Einsatzortes, die Erarbeitung eines Meldebildes, die Alarmierung, die Datenübermittlung an die Einsatzkräfte bis hin zur automatisierten Anmeldung von Patient*innen in den Kliniken. Allein der Notruf wird sich daher immer mehr von der reinen sprachlichen Kommunikation hinzu automatisierten Notrufen entwickeln. Mobile Produkte aus dem Bereich ehealth können Herzrhythmusstörungen erkennen, Stürze detektieren und mit Angabe des genauen Standorts einen Notruf auslösen. Fahrzeuge melden automatisiert über das ecall-System Unfälle und liefern wichtige Zusatzinformationen für die Feuerwehr. An der Schnittstelle zwischen Leitstelle und Stabsarbeit werden bei Großschadenslagen Daten aus dem Einsatzleitsystem an nachgeordnete Stabsinformationssysteme übergeben. Die Digitalisierung hält in alle Bereiche der Gefahrenabwehr Einzug, die Leitstelle als Steuerungselement in der Gefahrenabwehr ist hier natürlich besonders involviert. Durch die zunehmende Vernetzung von Leitstellen wird zudem die gebietsübergreifende Zusammenarbeit leichter und die Prozesse insgesamt effizienter.

Die Nutzung internetbasierte Anwendungen und Informationssysteme mit Anbindung an die kritische Infrastruktur Leitstelle bietet viele Chancen aber auch Risiken. Die Gefahr des manipulierenden Zugriffs von außen oder der „Angriff“ von innen, durch unsachgemäße Handlungen oder sogar vorsätzliche Manipulation stellt eine Gefahr für die Betriebssicherheit dar. BOS-Leitstellen stellen hier durchaus ein lohnendes Ziel für Cyberangriffe dar, sind sie doch ein Symbol für eine funktionierende Notfallversorgung und damit für eine gesicherte Daseinsvorsorge.

IT-Sicherheit ist jedoch nicht nur technisch zu sehen, sondern auch aus der prozessualen Sicht. Dazu gibt das vorliegende Dokument ebenfalls Hinweise für die praktische Umsetzung in den Leitstellen.

Neben dem IT-Grundschutz des BSI liegt nun in einer aktuellen Version ein detailliertes Grundschutzprofil für BOS-Leitstellen vor, das den Verantwortlichen eine wichtige Hilfestellung bei der Umsetzung der IT-Sicherheit bietet.

Gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) haben der Fachverband Leitstellen e.V. mit einer eigenen Arbeitsgruppe „Informationssicherheit“, der Bundesverband Professioneller Mobilfunk e.V. (PMeV) mit vertretenen Mitgliedern sowie weiteren engagierten Mitstreitern aus Leitstellen und Fachfirmen in mehreren Workshops das vorliegende Grundschutzprofil erarbeitet und aktualisiert. Aus der Praxis – für die Praxis.

Unser Dank gilt allen Beteiligten aus Leitstellen, Landesbehörden, BSI und Firmenvertretern, die sich hier mit Ihrer Expertise eingebracht haben.

Fachverband Leitstellen e.V.

1 Management Summary

Das IT-Grundschutz-Profil für Leitstellen richtet sich an die für Informationstechnik verantwortlichen Entscheidungsträger aus dem Bereich der Leitstellen. Ebenso soll es aber auch Herstellern von Leitstellentechnik und mit der technischen Planung von Leitstellen beauftragten Fachplanern als Handlungsleitfaden für die Informationssicherheitskonzeption in Leitstellen dienen.

Dieses IT-Grundschutz-Profil soll den Anwendern helfen, einen Informationssicherheitsprozess in einer Leitstelle zu installieren und diesen an deren Bedürfnisse anzupassen. Es soll als Schablone dienen, den IT-Grundschutz des BSI in geeigneter Weise zu implementieren.

2 Festlegung des Geltungsbereichs

Zielgruppe

Das IT-Grundschutz-Profil für Leitstellen richtet sich an die für Informationstechnik verantwortlichen Entscheidungsträger aus diesem Bereich. Gleichzeitig soll es auch Herstellern und Lieferanten von Leitstellentechnik als Grundlage für Aufbau und Entwicklung ihrer Systeme und Anwendungen dienen. Auch Fachplaner für Leitstellen sind Zielgruppe des IT-Grundschutz-Profils.

Beschreibung des Schutzbedarfs

Die Betriebsbereitschaft von Leitstellen muss ständig gegeben sein. Ebenso muss auf die Korrektheit und Vertraulichkeit der verarbeiteten Daten großen Wert gelegt werden. Die Informationssicherheitsziele Vertraulichkeit, Verfügbarkeit und Integrität müssen daher über das übliche Maß hinaus erreicht werden. Infolgedessen wird in diesem IT-Grundschutz-Profil ein Schutzniveau mit mindestens der Standard-Absicherung der IT-Grundschutz-Vorgehensweise angestrebt.

IT-Grundschutz Vorgehensweise

Der IT-Grundschutz des BSI bietet die Vorgehensweisen Basis-, Standard oder Kern-Absicherung an. Abhängig von der gewählten Vorgehensweise müssen die in den Bausteinen beschriebenen Anforderungen umgesetzt werden. Die beschriebenen Anforderungen in diesem IT-Grundschutz-Profil entsprechen mindestens der Standard-Absicherung des BSI-Standards 200-2. Zudem wird empfohlen, einzelne Anforderungen aus dem erhöhten Schutzbedarf umzusetzen.

Kompatibilität zu anderen Standards

Durch eine Umsetzung der Standard-Absicherung besteht Kompatibilität zu ISO 27001.¹

Berücksichtigte Rahmenbedingungen

Vorgaben aus der DSGVO und dem BSI-Gesetz werden in diesem IT-Grundschutz-Profil berücksichtigt.

1 <https://www.beuth.de/de/norm/din-en-iso-iec-27001/269670716> (aufgerufen am 12.02.2024)

3 Abgrenzung des Informationsverbundes

Die zusammenhängenden Komponenten einer Institution oder eines speziellen Anwendungsbereichs werden als Informationsverbund bezeichnet. Im nächsten Abschnitt werden die für das IT-Grundschutz-Profil relevanten Bestandteile des Informationsverbunds Leitstelle definiert. Anschließend werden die Teile des Informationsverbundes aufgeführt, die in diesem IT-Grundschutz-Profil nicht berücksichtigt werden.

3.1 Bestandteile des Informationsverbundes

Die folgende Tabelle zeigt die technischen Bestandteile des Informationsverbundes, die Prozesse und Verfahren in Leitstellen unterstützen und in diesem IT-Grundschutz-Profil berücksichtigt werden.

Identifikator	Objekt des Informationsverbundes
IV1	Prozesse
IV2	Anwendungen
IV3	Gebäude und Räume
IV4	IT-Systeme
IV5	Netzwerke

Tabelle 1: Bestandteile des Informationsverbundes, die Prozesse und Verfahren in Leitstellen unterstützen.

3.2 Nicht berücksichtigte Teile

Der auf den TETRA-Standard basierende digitale Funk der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) wird im IT-Grundschutz-Profil für Leitstellen nicht vollständig berücksichtigt, weil dieser ein eigenständiges System darstellt, das lediglich Schnittstellen zu den Leitstellen bereitstellt.

Die technische Sicherheit der Daten- und Telefonanschlüsse liegt in Verantwortung der Netzbetreiber. Eine Berücksichtigung im IT-Grundschutz-Profil für Leitstellen ist daher nicht notwendig.

Immer mehr Hersteller bieten Notruf-Apps für Smartphones an, über die eine Notfallmeldung an die Leitstelle abgesetzt werden kann. Die offizielle Notruf-App des Bundes ist im Jahr 2020 erschienen. Diese Form von Apps stellen ein eigenständiges System dar. Die Schnittstelle zu Leitstellen besteht in der Regel aus einer Web-Applikation, die über den Web-Browser abgerufen werden kann. Notruf-Apps müssen daher im IT-Grundschutz-Profil für Leitstellen nicht berücksichtigt werden.

Neben der Alarmierung über das Funknetz der BOS nutzen viele Feuerwehren und Hilfsorganisationen Alarmierungs-Apps für Smartphones. Auf eine sichere Implementierung dieser Apps hat die Leitstelle keinen Einfluss. Auch hier muss daher lediglich die Schnittstelle zwischen den Anwendungen in der Leitstelle und der Alarmierungs-App betrachtet werden. Deshalb findet eine Berücksichtigung der Alarmierungs-App im IT-Grundschutz-Profil nicht statt.

4 Referenzarchitektur

Die Referenzarchitektur beinhaltet neben Gebäuden und Räumen, in denen die Leitstelle betrieben wird, die Kommunikationsverbindungen, Netzwerke und die dafür benötigten Komponenten. Außerdem werden alle beteiligten IT-Systeme, die verwendeten Anwendungen und die in der Leitstelle durchgeführten Prozesse in der Referenzarchitektur aufgeführt.

Es ist möglich, dass sich die Referenzarchitektur von der tatsächlich vorhandenen Architektur einer Leitstelle unterscheidet. Der Umgang mit solchen Abweichungen ist in Abschnitt 4.6 beschrieben.

4.1 Prozesse

Der Betrieb einer Leitstelle gliedert sich in unterschiedliche Prozesse, die für das IT-Grundschutz-Profil relevant sind und in diesem Abschnitt definiert werden. Die Kernprozesse sind die Annahme, das Verteilen und das Begleiten eines Einsatzes. Abbildung 1 zeigt die Ablauffolge der Prozesse:

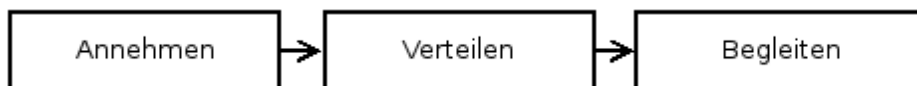


Abbildung 1: Kernprozesse in einer Leitstelle

In der folgenden Tabelle werden die in der Leitstelle durchgeführten Prozesse in Unterprozesse gegliedert und mit einem Identifikator versehen.

Identifikator	Prozesse der Einsatzannahme
P1.1	Meldung priorisieren
P1.2	Meldung annehmen
P1.3	Einsatzort lokalisieren
P1.4	Sachverhalt klären/bewerten

Tabelle 2: Prozesse in der Leitstelle bei Einsatzannahme.

Identifikator	Prozesse der Einsatzverteilung
P2.1	Disposition
P2.2	Alarmierung/Benachrichtigung
P2.3	Überwachung

Tabelle 3: Prozesse in der Leitstelle bei Einsatzverteilung.

Identifikator	Prozesse der Einsatzbegleitung
P3.1	Dokumentation
P3.2	Unterstützung der Einsatzkräfte
P3.3	Abschließen/Nachbereiten

Tabelle 4: Prozesse in der Leitstelle bei Einsatzbegleitung.

Ein weiterer wichtiger Unterstützungsprozess ist in vielen Leitstellen die Stammdatenpflege. Dieser wird in diesem Profil nicht separat berücksichtigt. Sofern die Stammdatenpflege nicht zentral, sondern von Leitstellenpersonal durchgeführt wird, muss auch diese betrachtet und bewertet werden.

4.2 Anwendungen

Zum Informationsverbund gehören neben den Prozessen auch die Anwendungen, die eine optimale Bearbeitung der Prozesse unterstützen sollen. Dies sind in einer Leitstelle insbesondere das Einsatzleit- und das Notrufabfragesystem. Auch Gefahrenmeldesysteme und Internetanwendungen stellen wichtige Komponenten dar. Alle Anwendungen sind in der folgenden Tabelle mit einem Identifikator aufgeführt. In der rechten Spalte ist angegeben, welche Prozesse von den Anwendungen unterstützt werden.

Identifikator	Anwendungen des Informationsverbundes	Unterstützte Prozesse
A1	Einsatzleitsystem	P1.2, P1.3, P1.4, P2.1, P2.2, P2.3, P3.1, P3.2
A2	Notrufabfragesystem	P1.1, P1.2
A3	Internetanwendungen	P1.3, P1.4, P2.1, P2.3, P3.2, P3.3
A4	Gefahrenmeldesystem	P1.2
A5	Funkanschaltung	P2.1, P2.2
A6	Telefonie/Fax	P1.2, P2.2
A7	Geoinformationssystem	P1.3, P2.1, P2.3
A8	Standardisiertes Abfragesystem	P1.4
A9	Sprachdokumentation	P1.2
A10	Modulares Warnsystem (MoWaS)	P3.2
A11	Einsatznachbearbeitungssystem	P3.3

Tabelle 5: Anwendungen des Informationsverbundes, die in einer Leitstelle verwendet werden.

4.3 IT-Systeme

Identifikator	IT-Systeme des Informationsverbundes	Abhängige Anwendungen/Prozesse
S1	Clients [Win10, 7, Linux]	A1, A2, A3, A6, A8, A9, A11
S2	Server [Win 2016, Linux, Win 2019]	A1, A2, A3, A4, A5, A6, A7, A8, A9, A11
S3	Virtualisierungs-Host	A1, A2, A3, A4, A5, A6, A7, A8, A9
S4	Active Directory	A1
S5	Datenbankserver [Win/Linux]	A1, A2, A4, A8, A9, A11
S6	Dateiserver [Win, Linux]	A1
S7	Kommunikationsserver [Win, Linux]	A1, A2, A6
S8	TK-Anlage	A6
S9	Schnittstellenserver [Win, Linux]	A1, A4
S10	WMS [Win, Linux]	A7
S11	Störmeldeserver [Win, Linux]	A1, A2
S12	Backup-Server	A1, A2, A9
S13	Alarmierungsserver [Win, Linux]	A1
S14	Alarm-Drucker/Fax	A1, A6

Tabelle 6: IT-Systeme des Informationsverbundes, die in einer Leitstelle verwendet werden.

4.4 Netze und Netzkomponenten

Anwendungen und IT-Systeme der Leitstelle sind in verschiedene Netzwerke eingebunden. Auch wenn sich Anzahl und Aufbau der Netze nicht im Detail verallgemeinern lassen, wird davon ausgegangen, dass die Architektur in vielen Leitstellen zumindest ähnlich ist. Zum Betrieb der Netze sind aktive und passive Netzkomponenten erforderlich.

Identifikator	Objekt des Informationsverbundes	Abhängige Objekte
N1	Netze (Router, Switches, Firewall...)	A1, A2, A3, A6, A8, A9, A11
N2	Session Border Controller	A2, A6, S8

Tabelle 7: Netzkomponenten und Netze des Informationsverbundes.

4.4.1. Netzplan

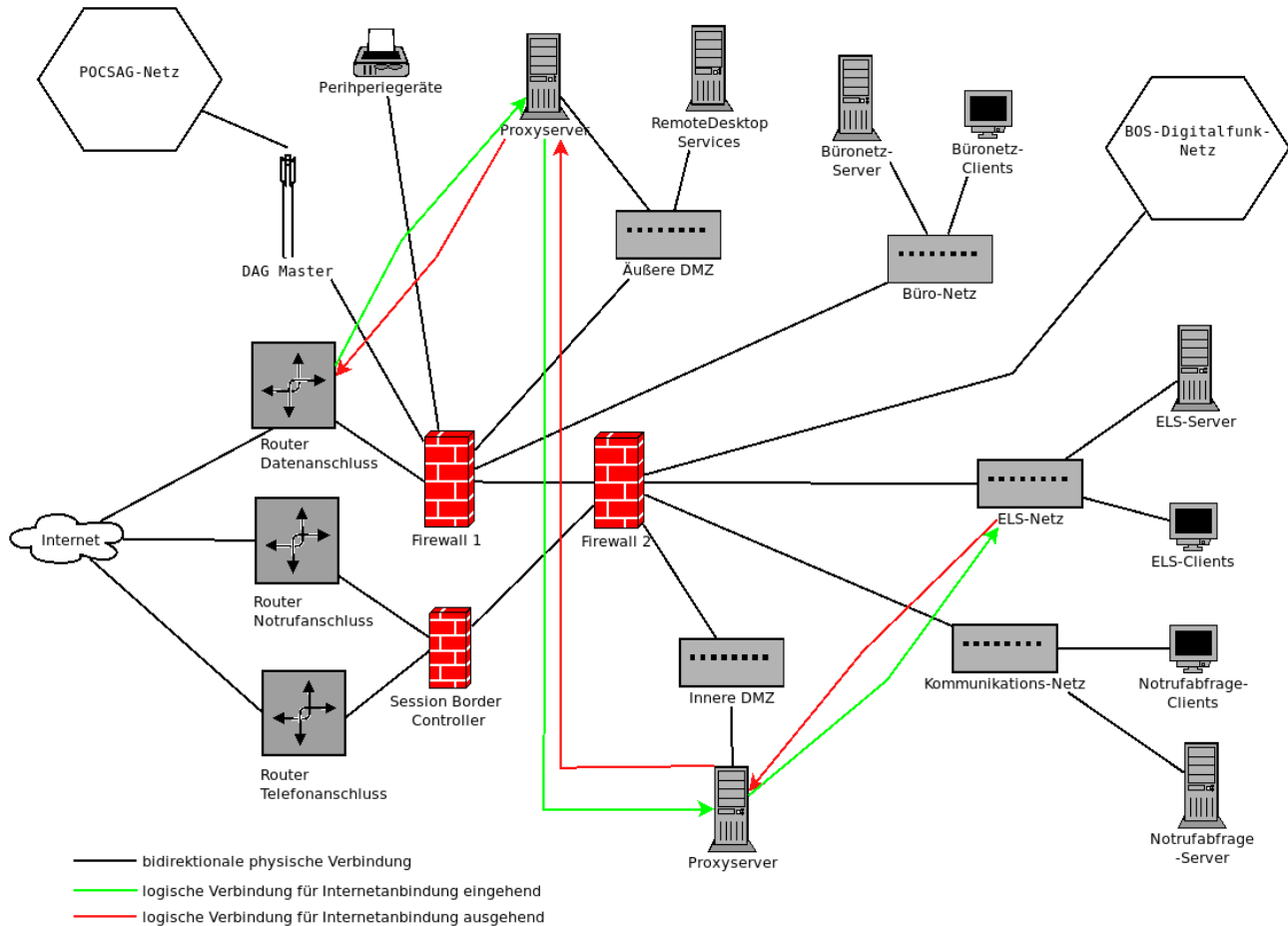


Abbildung 2: Muster-Netzplan für eine gedachte Musterleitstelle, die Grundlage dieses Profils ist. Auf die Darstellung von Redundanzen wurde zugunsten einer besseren Übersichtlichkeit verzichtet.

4.5 Gebäude und Räume

Nicht nur die informationstechnischen Komponenten spielen bei der Informationssicherheit eine große Rolle. Auch die Sicherheit der Gebäude und Räume in denen die Leitstelle betrieben wird muss in einem IT-Grundschutz-Profil berücksichtigt werden. Dies betrifft nicht nur den Einsatzleitraum, in denen die Notfallmeldungen entgegengenommen und die Rettungsmittel zu den Einsätzen disponiert werden. Die Räume, in denen die Server und andere Technik untergebracht sind müssen ebenso betrachtet werden wie die Büroräume für Verwaltungsmitarbeiter. R2 bezeichnet ein externes Rechenzentrum, das sich nicht in den Räumen der Leitstelle befindet, von dieser aber genutzt wird.

Identifikator	Räume des Informationsverbundes	In den Räumen installierte IT-Systeme oder durchgeführte Prozesse
R1	Leitstelle	P1, P2, P3, S1, N1
R1.1	Einsatzleitraum	P1, P2, P3, S1, N1
R1.2	Technikraum/Serverraum	S2, S3, S4, S5, S6, S7, S8, S9, S11, S12, S13, N1, N2
R1.3	Büro	S1
R1.4	Administratorbüro	S1
R1.5	Stabs-/Führungsraum	S1
R1.6	Not-Abfrageplätze	S1

Tabelle 8: Räume des Informationsverbundes.

4.6 Umgang mit Abweichungen

Weicht der zu schützende Informationsverbund von der hier dargestellten Referenzarchitektur ab, müssen die zusätzlichen oder nicht vorhandenen Objekte dokumentiert werden. Die Objekte sollten passenden Komponenten des IT-Grundschatz Kompendium zugeordnet werden. Die abgeleiteten Anforderungen müssen an den jeweiligen Schutzbedarf angepasst werden.

5 Zu erfüllende Anforderungen und umzusetzende Maßnahmen

Das IT-Grundschatz-Kompendium des BSI stellt Bausteine bereit, die anwendungsbezogene Empfehlungen zur Umsetzung des IT-Grundschatzes geben. Hierzu muss zunächst der Schutzbedarf der Prozesse, Anwendungen, IT-Systeme und Kommunikationsverbindungen festgelegt werden. Anschließend müssen die relevanten Bausteine identifiziert und eine Anpassung der Anforderungen an die entsprechende Zielgruppe durchgeführt werden. Das Resultat der Anpassung der Anforderungen kann bedeuten, dass alle oder nur bestimmte Anforderungen des Bausteins für die Informationssicherheit in Leitstellen relevant sind. Ebenso können Anforderungen als komplett irrelevant eingestuft werden. Auch die Relevanz der in den Anforderungen aufgeführten Maßnahmen muss identifiziert werden.

5.1 Feststellung des Schutzbedarfs

Grundlegend zur Festlegung des Schutzbedarfs sind die Auswirkungen, die eine Verletzung der Grundziele der Informationssicherheit, Vertraulichkeit, Integrität oder Verfügbarkeit hätten. Diese Effekte werden im Folgenden betrachtet. Das BSI benennt verschiedene Szenarien, auf die sich ein Schaden beziehen kann. Diese sind in Tabelle 9 aufgeführt.

Verstöße gegen Gesetze, Vorschriften oder Verträge (SZ1) können zum Beispiel vorliegen, wenn die Leitstelle nicht betriebsbereit ist und somit ihre Aufgaben nicht erfüllen kann (SZ4). Gleichzeitig kann es hierdurch zu Beeinträchtigungen der persönlichen Unversehrtheit von Notrufenden kommen

(SZ3), wenn diesen nicht rechtzeitig geholfen wird. Verstöße gegen Datenschutzgesetze fallen ebenfalls unter Schadensszenario 1. Die Übermittlung vertraulicher Informationen, über Anrufer oder Patienten an Unbefugte, stellt zudem eine Beeinträchtigung des informationellen Selbstbestimmungsrechts der Hilfesuchenden dar (SZ2). Alle diese Fälle können aufgrund von Schadensersatzforderungen der Betroffenen auch finanzielle Auswirkungen auf die Leitstelle haben (SZ6).

Für die Bürger ist ein hohes Vertrauen in die Arbeit der Leitstelle elementar. Dass ihnen im Notfall geholfen werden kann, gibt den Menschen ein sicheres Gefühl. Durch eine negative Außenwirkung (SZ5) kann diese Gewissheit abhandenkommen. Gleiches gilt für das eigene Personal der Leitstelle oder der angebundenen Hilfsorganisationen bei einer negativen Innenwirkung. Diese Effekte können zum Beispiel aufgrund von Ausfällen und damit verbundener negativer Berichterstattung in den Medien auftreten.

Identifikator	Schadensszenario
SZ1	Verstöße gegen Gesetze, Vorschriften oder Verträge
SZ2	Beeinträchtigungen des informationellen Selbstbestimmungsrechts
SZ3	Beeinträchtigungen der persönlichen Unversehrtheit
SZ4	Beeinträchtigungen der Aufgabenerfüllung
SZ5	negative Innen- oder Außenwirkung
SZ6	finanzielle Auswirkungen

Tabelle 9: Potentielle Schadensszenarien.

Die Schadensszenarien werden in den folgenden Abschnitten für jedes der Grundziele der Informationssicherheit einzeln betrachtet. Die Schadensauswirkung kann dabei im Voraus normalerweise nicht detailgenau festgelegt werden. Aus diesem Grund empfiehlt die IT-Grundschutz-Methodik des BSI drei Kategorien zu bestimmen, die den Schutzbedarf einstufen. Die drei Kategorien sind *normal*, *hoch* oder *sehr hoch*. Tabelle 10 führt die Kategorien auf, ergänzt um die Schadensauswirkungen. Die Schadensauswirkung kann sich dabei immer auf die Leitstelle selbst oder auf die hilfesuchenden Bürger beziehen.

Kategorie	Schadensauswirkung
normal	Die Schadensauswirkungen für die Leitstelle oder die hilfesuchenden Bürger sind begrenzt und überschaubar.
hoch	Die Schadensauswirkungen können den Betrieb der Leitstelle erheblich einschränken. Für die hilfesuchenden Bürger können die Konsequenzen beträchtlich sein.
sehr hoch	Die Schadensauswirkungen können den Betrieb der Leitstelle stilllegen. Für Hilfesuchende kann es zu existenziell- oder lebensbedrohlichen Konsequenzen kommen.

Tabelle 10: Vom BSI empfohlene Schutzbedarfskategorien.

In den folgenden drei Tabellen werden die Schutzbedarfskategorien mit den potentiellen Schadensszenarien verknüpft.

Schutzbedarfskategorie: Normal

Schadensszenario	Eigenschaft
SZ1	Verstöße gegen Vorschriften und Landesgesetze (RD-G, FW-G, KatS-G, LS-G), sowie Ausführungsverordnungen und Dienstanweisungen, die zu arbeitsrechtlichen und / oder zivilrechtlichen Folgen für das Leitstellenpersonal führen können.
SZ2	Es handelt sich hierbei um die Offenlegung personenbezogener Daten, bei deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann. In diese Kategorie fallen alle öffentlich zugänglichen Daten, wie Name, Adresse, Telefonnummer, sowie besondere personenbezogene Daten für die eine Freigabe nach dem BDSG vorliegen.
SZ3	Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht ausgeschlossen werden. Es ist mit leichten Gesundheitsschäden zu rechnen.
SZ4	Der Schaden ist durch Ersatzsysteme oder Ausweichlösungen weitgehend kompensierbar. Die Beeinträchtigung würde von den Betroffenen weitgehend als tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit des IT-Systems ist größer als 24 und kleiner als 72 Stunden (SLA-2).
SZ5	Der Schadensfall wird nur innerhalb der Leitstelle und den angegliederten Einsatzkräften wahrgenommen. Es kommt zu keiner Offenlegung innerhalb der Bevölkerung.
SZ6	Der finanzielle Schaden ist durch Versicherungen abgedeckt oder kann durch das Leitstellenbudget aufgefangen werden.

Tabelle 11: Schadensszenarien bei Schutzbedarfskategorie normal.

Schutzbedarfskategorie: Hoch

Schadensszenario	Eigenschaft
SZ1	Verstöße gegen Vorschriften und Landesgesetze (RD-G, FW-G, KatS-G, LS-G), sowie allgemeingültigem Recht (BGB, Strafrecht), die zu strafrechtlichen und zivilrechtlichen Folgen für das Leitstellenpersonal, sowie zu Haftungsschäden beim Leitstellenträger führen können.
SZ2	Es handelt sich hierbei um die Offenlegung personenbezogener Daten, bei deren unkontrollierter Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden wird. In diese Kategorie fallen alle besonders schutzbedürftigen Daten nach dem BDSG, beispielsweise persönliche medizinische Daten.
SZ3	Eine Beeinträchtigung der persönlichen Unversehrtheit ist wahrscheinlich. Es ist mit erheblichen Gesundheitsschäden einzelner Personen zu rechnen und/oder mit irreparablen Folgen ohne die Möglichkeit einer vollständigen Genesung.
SZ4	Die Schadenshöhe in der Leitstelle führt zu Ausfällen in der polizeilichen / nichtpolizeilichen Gefahrenabwehr. Die Reaktionszeiten und sonstige Leistungsmerkmale sind stark eingeschränkt. Der Schaden ist durch Ersatzsysteme oder Ausweichlösungen nur teilweise kompensierbar. Der Ausfall muss innerhalb von 24 Stunden behoben werden (SLA-1).
SZ5	Der Schaden ist öffentlich sichtbar. Regionale Presseeinrichtungen berichten über das Schadensausmaß. Es müssen öffentliche Durchsagen ausgestrahlt werden.
SZ6	Der finanzielle Schaden ist nur durch den Betreiber (Organisation, Stadt, Landkreis, Bundesland) insgesamt, aber nicht durch das Einzelbudget der Leitstelle tragbar.

Tabelle 12: Schadensszenarien bei Schutzbedarfskategorie hoch.

Schutzbedarfskategorie: Sehr hoch

Scha- dens- sze- nario	Eigenschaft
SZ1	Verstöße gegen Vorschriften und Landesgesetze (RD-G, FW-G, KatS-G, LS-G), sowie allgemeingültigem Recht (BGB, Strafrecht), die zu erheblichen strafrechtlichen und zivilrechtlichen Folgen für das Leitstellenpersonal, sowie zu umfangreichen (über 1 Million Euro) Haftungsschäden beim Leitstellenträger führen können.
SZ2	Es handelt sich um die Verarbeitung besonderer personenbezogener Daten, bei deren Offenlegung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen ERHEBLICH beeinträchtigt wird und möglicherweise eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist.
SZ3	Es ist mit sehr hoher Wahrscheinlichkeit mit dem Tode einzelner oder mehrerer Personen zu rechnen.
SZ4	Die polizeiliche / nichtpolizeiliche Gefahrenabwehr ist erheblich eingeschränkt. Externe Notfallpläne müssen eingesetzt werden. Der Schaden kann nicht kompensiert werden. Die Beeinträchtigung wird von allen Betroffenen als nicht tolerabel eingeschätzt. Der Ausfall muss innerhalb von 4 Stunden behoben werden (SLA-0).
SZ5	Es kommt zur Berichterstattung in überregionalen Presseorganen, mit hohem Vertrauensverlust in der Bevölkerung und den handelnden Personen in die eingesetzte Technik ist zu rechnen.
SZ6	Der finanzielle Schaden ist durch den Betreiber nicht mehr kompensierbar. Der Schaden führt zum Ruin des Betreibers und hinterlässt offene Forderungen.

Tabelle 13: Schadensszenarien bei Schutzbedarfskategorie sehr hoch.

Bei der Bestimmung des Schutzbedarfs eines in Abschnitt 4 bestimmten Objekts müssen immer auch die Prozesse oder andere Objekte betrachtet werden, für die dieses Objekt benötigt wird. Wird zum Beispiel ein Objekt für einen Prozess verwendet, dessen Schutzbedarf sehr hoch ist, so ist auch der Schutzbedarf des betrachteten Objekts als sehr hoch einzustufen.

5.1.1. Schutzbedarfsfeststellung für Prozesse

Für die Schutzbedarfsfeststellung der Prozesse muss das Ausmaß eines Schadens auf den jeweiligen Prozess ermittelt werden. Zunächst wird jeder in Abschnitt 4.1 definierte Prozess hinsichtlich der Vertraulichkeit untersucht. Anschließend findet eine Untersuchung bezüglich der Integrität statt. Zuletzt wird der Schutzbedarf für die Verfügbarkeit der einzelnen Prozesse ermittelt.

Schutzbedarfsfeststellung der Vertraulichkeit für Prozesse des Informationsverbundes

Objekt	Schutzbedarf	Begründung
P1.1	hoch	Verarbeitung personenbezogener Daten mit medizinischen Diagnosen, die vertraulich behandelt werden müssen (SZ1, SZ2, SZ5, SZ6).
P1.2	hoch	Verarbeitung personenbezogener Daten mit medizinischen Diagnosen, die vertraulich behandelt werden müssen (SZ1, SZ2, SZ5, SZ6).
P1.3	normal	Der Einsatzort enthält im Normalfall keine personenbezogenen Daten.
P1.4	hoch	Verarbeitung personenbezogener Daten mit medizinischen Diagnosen, die vertraulich behandelt werden müssen (SZ1, SZ2, SZ5, SZ6).
P2.1	hoch	Verarbeitung personenbezogener Daten mit medizinischen Diagnosen, die vertraulich behandelt werden müssen (SZ1, SZ2, SZ5, SZ6).
P2.2	hoch	Verarbeitung personenbezogener Daten mit medizinischen Diagnosen, die vertraulich behandelt werden müssen (SZ1, SZ2, SZ5, SZ6).
P2.3	normal	Der Einsatzort enthält im Normalfall keine personenbezogenen Daten.
P3.1	hoch	Verarbeitung personenbezogener Daten mit medizinischen Diagnosen, die vertraulich behandelt werden müssen (SZ1, SZ2, SZ5, SZ6).
P3.2	hoch	Verarbeitung personenbezogener Daten mit medizinischen Diagnosen, die vertraulich behandelt werden müssen (SZ1, SZ2, SZ5, SZ6).
P3.3	hoch	Verarbeitung personenbezogener Daten mit medizinischen Diagnosen, die vertraulich behandelt werden müssen (SZ1, SZ2, SZ5, SZ6).

Tabelle 14: Schutzbedarfsfeststellung der Vertraulichkeit für Prozesse in der Leitstelle.

Schutzbedarfsfeststellung der Integrität für Prozesse des Informationsverbundes

Objekt	Schutzbedarf	Begründung
P1, P2, P3.2	sehr hoch	Lebensbedrohliche Folgen bei Verarbeitung inkorrektur Daten oder fehlerhaftem Verhalten (SZ1, SZ3, SZ4, SZ5, SZ6).
P3.1, P3.3	normal	Die Schadensauswirkungen der Prozesse (Einsatzdokumentation und Abschließen/Nachbereiten) sind begrenzt und überschaubar.

Tabelle 15: Schutzbedarfsfeststellung der Integrität für Prozesse in der Leitstelle.

Schutzbedarfsfeststellung der Verfügbarkeit für Prozesse des Informationsverbundes

Objekt	Schutzbedarf	Begründung
P1, P2, P3.2	sehr hoch	Lebensbedrohliche Folgen bei Verarbeitung inkorrektur Daten oder fehlerhaftem Verhalten (SZ1, SZ3, SZ4, SZ5, SZ6).
P3.1, P3.3	normal	Die Schadensauswirkungen der Prozesse (Einsatzdokumentation und Abschließen/Nachbereiten) sind begrenzt und überschaubar.

Tabelle 16: Schutzbedarfsfeststellung der Verfügbarkeit für Prozesse in der Leitstelle.

5.1.2. Schutzbedarfsfeststellung für Anwendungen

Die Schutzbedarfsfeststellung für Anwendungen richtet sich nach dem Schutzbedarf der Prozesse, die durch die Verwendung der jeweiligen Anwendung unterstützt werden. Dabei wird das Maximumprinzip berücksichtigt und der jeweils höchste Schutzbedarf durch die Anwendung geerbt. Ist der Schutzbedarf nur für einen Teil, der von den Anwendungen unterstützten Prozesse als sehr hoch eingestuft, so ist der Schutzbedarf der gesamten Anwendung als sehr hoch einzustufen.

Schutzbedarfsfeststellung der Vertraulichkeit für Anwendungen

Objekt	Schutzbedarf	Begründung
A1	hoch	hoher Schutzbedarf für Prozesse P1.2, P1.4, P2.1, P2.2, P3.1, P3.2
A2	hoch	hoher Schutzbedarf für Prozesse P1.1, P1.2
A3	hoch	hoher Schutzbedarf für Prozesse P1.4, P2.1, P3.2, P3.3
A4	hoch	hoher Schutzbedarf für Prozess P1.2
A5	hoch	hoher Schutzbedarf für Prozesse P2.1, P2.2
A6	hoch	hoher Schutzbedarf für Prozesse P1.2, P2.2
A7	hoch	hoher Schutzbedarf für Prozess P2.1
A8	hoch	hoher Schutzbedarf für Prozess P1.4
A9	hoch	hoher Schutzbedarf für Prozess P1.2
A10	hoch	hoher Schutzbedarf für Prozess P3.2
A11	hoch	hoher Schutzbedarf für Prozess P3.3

Tabelle 17: Schutzbedarfsfeststellung der Vertraulichkeit für Anwendungen.

Schutzbedarfsfeststellung der Integrität für Anwendungen

Objekt	Schutzbedarf	Begründung
A1	sehr hoch	sehr hoher Schutzbedarf für Prozesse P1, P2, P3.2
A2	sehr hoch	sehr hoher Schutzbedarf für Prozess P1
A3	sehr hoch	sehr hoher Schutzbedarf für Prozesse P1, P2, P3.2
A4	sehr hoch	sehr hoher Schutzbedarf für Prozess P1
A5	sehr hoch	sehr hoher Schutzbedarf für Prozess P2
A6	sehr hoch	sehr hoher Schutzbedarf für Prozesse P1, P2
A7	sehr hoch	sehr hoher Schutzbedarf für Prozesse P1, P2
A8	sehr hoch	sehr hoher Schutzbedarf für Prozess P1
A9	sehr hoch	sehr hoher Schutzbedarf für Prozess P1
A10	sehr hoch	sehr hoher Schutzbedarf für Prozess P3.2
A11	normal	normaler Schutzbedarf für Prozess P3.3

Tabelle 18: Schutzbedarfsfeststellung der Integrität für Anwendungen.

Schutzbedarfsfeststellung der Verfügbarkeit für Anwendungen

Objekt	Schutzbedarf	Begründung
A1	sehr hoch	sehr hoher Schutzbedarf für Prozesse P1, P2, P3.2
A2	sehr hoch	sehr hoher Schutzbedarf für Prozess P1
A3	sehr hoch	sehr hoher Schutzbedarf für Prozesse P1, P2, P3.2
A4	sehr hoch	sehr hoher Schutzbedarf für Prozess P1
A5	sehr hoch	sehr hoher Schutzbedarf für Prozess P2
A6	sehr hoch	sehr hoher Schutzbedarf für Prozesse P1, P2
A7	sehr hoch	sehr hoher Schutzbedarf für Prozesse P1, P2
A8	sehr hoch	sehr hoher Schutzbedarf für Prozess P1
A9	sehr hoch	sehr hoher Schutzbedarf für Prozess P1
A10	sehr hoch	sehr hoher Schutzbedarf für Prozess P3.2
A11	normal	Normaler Schutzbedarf für Prozess P3.3

Tabelle 19: Schutzbedarfsfeststellung der Verfügbarkeit für Anwendungen.

5.1.3. Schutzbedarfsfeststellung für IT-Systeme

Der Schutzbedarf für die IT-Systeme einer Leitstelle richtet sich nach den Anwendungen, die auf den IT-Systemen installiert sind oder mit diesen verbunden sind. Nach dem Maximumprinzip muss der Schutzbedarf auch wieder mindestens so hoch angesetzt werden, wie für diese Anwendungen.

Schutzbedarfsfeststellung der Vertraulichkeit für IT-Systeme

Objekt	Schutzbedarf	Begründung
S1	hoch	hoher Schutzbedarf für Anwendungen A1, A2, A3, A6, A8, A9, A11
S2	hoch	hoher Schutzbedarf für Anwendungen A1, A2, A3, A4, A5, A6, A7, A8, A9, A11
S3	hoch	hoher Schutzbedarf für Anwendungen A1, A2, A3, A4, A5, A6, A7, A8, A9
S4	hoch	hoher Schutzbedarf für Anwendung A1
S5	hoch	hoher Schutzbedarf für Anwendungen A1, A2, A4, A8, A9, A11
S6	hoch	hoher Schutzbedarf für Anwendung A1
S7	hoch	hoher Schutzbedarf für Anwendungen A1, A2, A6
S8	hoch	hoher Schutzbedarf für Anwendung A6
S9	hoch	hoher Schutzbedarf für Anwendungen A1, A4
S10	hoch	hoher Schutzbedarf für Anwendung A7
S11	hoch	hoher Schutzbedarf für Anwendungen A1, A2
S12	hoch	hoher Schutzbedarf für Anwendungen A1, A2, A9
S13	hoch	hoher Schutzbedarf für Anwendung A1
S14	hoch	hoher Schutzbedarf für Anwendungen A1, A6

Tabelle 20: Schutzbedarfsfeststellung der Vertraulichkeit für IT-Systeme.

Schutzbedarfsfeststellung der Integrität für IT-Systeme

Objekt	Schutzbedarf	Begründung
S1	sehr hoch	sehr hoher Schutzbedarf für Anwendungen A1, A2, A3, A6, A8, A9
S2	sehr hoch	sehr hoher Schutzbedarf für Anwendungen A1, A2, A3, A4, A5, A6, A7, A8, A9
S3	sehr hoch	sehr hoher Schutzbedarf für Anwendungen A1, A2, A3, A4, A5, A6, A7, A8, A9
S4	sehr hoch	sehr hoher Schutzbedarf für Anwendung A1
S5	sehr hoch	sehr hoher Schutzbedarf für Anwendungen A1, A2, A4, A8, A9
S6	sehr hoch	sehr hoher Schutzbedarf für Anwendung A1
S7	sehr hoch	sehr hoher Schutzbedarf für Anwendungen A1, A2, A6
S8	sehr hoch	sehr hoher Schutzbedarf für Anwendung A6
S9	sehr hoch	sehr hoher Schutzbedarf für Anwendungen A1, A4
S10	sehr hoch	sehr hoher Schutzbedarf für Anwendung A7
S11	sehr hoch	sehr hoher Schutzbedarf für Anwendungen A1, A2
S12	sehr hoch	sehr hoher Schutzbedarf für Anwendungen A1, A2, A9
S13	sehr hoch	sehr hoher Schutzbedarf für Anwendung A1
S14	sehr hoch	sehr hoher Schutzbedarf für Anwendungen A1, A6

*Tabelle 21: Schutzbedarfsfeststellung der Integrität für IT-Systeme.***Schutzbedarfsfeststellung der Verfügbarkeit für IT-Systeme**

Objekt	Schutzbedarf	Begründung
S1	sehr hoch	sehr hoher Schutzbedarf für Anwendungen A1, A2, A3, A6, A8, A9
S2	sehr hoch	sehr hoher Schutzbedarf für Anwendungen A1, A2, A3, A4, A5, A6, A7, A8, A9
S3	sehr hoch	sehr hoher Schutzbedarf für Anwendungen A1, A2, A3, A4, A5, A6, A7, A8, A9
S4	sehr hoch	sehr hoher Schutzbedarf für Anwendung A1
S5	sehr hoch	sehr hoher Schutzbedarf für Anwendungen A1, A2, A4, A8, A9
S6	sehr hoch	sehr hoher Schutzbedarf für Anwendung A1
S7	sehr hoch	sehr hoher Schutzbedarf für Anwendungen A1, A2, A6
S8	sehr hoch	sehr hoher Schutzbedarf für Anwendung A6
S9	sehr hoch	sehr hoher Schutzbedarf für Anwendungen A1, A4
S10	sehr hoch	sehr hoher Schutzbedarf für Anwendung A7
S11	sehr hoch	sehr hoher Schutzbedarf für Anwendungen A1, A2
S12	sehr hoch	sehr hoher Schutzbedarf für Anwendungen A1, A2, A9
S13	sehr hoch	sehr hoher Schutzbedarf für Anwendung A1
S14	sehr hoch	sehr hoher Schutzbedarf für Anwendungen A1, A6

Tabelle 22: Schutzbedarfsfeststellung der Verfügbarkeit für IT-Systeme.

5.1.4. Schutzbedarfsfeststellung für Netzwerke

Viele Anwendungen und IT-Systeme, die in der Leitstelle verwendet werden, übermitteln und empfangen Daten über die in Abschnitt 4.4 definierten Netze und Netzkomponenten. Der Schutzbedarf der Netze und Netzkomponenten ist somit abhängig vom Schutzbedarf der Anwendungen und IT-Systeme, die über diese Netze Daten übermitteln und empfangen.

Schutzbedarfsfeststellung der Vertraulichkeit für Netzwerke

Objekt	Schutzbedarf	Begründung
N1	hoch	hoher Schutzbedarf für A1, A2, A3, A6, A8, A9, A11
N2	hoch	hoher Schutzbedarf für A2, A6, S8

Tabelle 23: Schutzbedarfsfeststellung der Vertraulichkeit für Netzwerke.

Schutzbedarfsfeststellung der Integrität für Netzwerke

Objekt	Schutzbedarf	Begründung
N1	sehr hoch	sehr hoher Schutzbedarf für A1, A2, A3, A6, A8, A9
N2	sehr hoch	sehr hoher Schutzbedarf für A2, A6, S8

Tabelle 24: Schutzbedarfsfeststellung der Integrität für Netzwerke.

Schutzbedarfsfeststellung der Verfügbarkeit für Netzwerke

Objekt	Schutzbedarf	Begründung
N1	sehr hoch	sehr hoher Schutzbedarf für A1, A2, A3, A6, A8, A9
N2	sehr hoch	sehr hoher Schutzbedarf für A2, A6, S8

Tabelle 25: Schutzbedarfsfeststellung der Verfügbarkeit für Netzwerke.

5.1.5. Schutzbedarfsfeststellung für Räume

Die Schutzbedarfsfeststellung für Räume richtet sich nach den IT-Systemen, die in dem betrachteten Raum installiert sind und den Prozessen, die in diesen Räumen durchgeführt werden. Je höher deren Schutzbedarf ist, desto höher ist auch der Schutzbedarf für den Raum einzustufen. Dabei ist bei der Festlegung des Schutzbedarfs auch die Menge an Systemen zu berücksichtigen, die in dem Raum installiert sind.

Schutzbedarfsfeststellung der Vertraulichkeit für Räume

Objekt	Schutzbedarf	Begründung
R1	hoch	hoher Schutzbedarf für die durchgeführten Prozesse, betriebenen Systeme und Netzwerke

Tabelle 26: Schutzbedarfsfeststellung der Vertraulichkeit für Räume.

Schutzbedarfsfeststellung der Integrität für Räume

Objekt	Schutzbedarf	Begründung
R1	sehr hoch	sehr hoher Schutzbedarf für die durchgeführten Prozesse, betriebenen Systeme und Netzwerke

Tabelle 27: Schutzbedarfsfeststellung der Integrität für Räume.

Schutzbedarfsfeststellung der Verfügbarkeit für Räume

Objekt	Schutzbedarf	Begründung
R1	sehr hoch	sehr hoher Schutzbedarf für die durchgeführten Prozesse, betriebenen Systeme und Netzwerke

Tabelle 28: Schutzbedarfsfeststellung der Verfügbarkeit für Räume.

5.2 Auswahl relevanter Bausteine

Das IT-Grundschutz-Kompendium wird jährlich aktualisiert. Die jeweils aktuelle Fassung veröffentlicht das BSI auf ihrer Homepage.² In den Tabellen 29 bis Tabelle 37 wird jeder Baustein aus dem **Kompendium 2023** aufgelistet und auf Relevanz im vorliegenden IT-Grundschutz-Profil überprüft. Sofern ein Baustein nicht relevant ist, wird dies begründet. Dabei kommt das Mindestprinzip zur Anwendung: Es werden nur diejenigen Bausteine modelliert, die für eine Mehrheit der Leitstellen bedeutend sind. Diese Vorgehensweise fokussiert das IT-Grundschutz-Profil auf die wesentlichen und wiederverwendbaren Aspekte. Dies vereinfacht die spätere Umsetzung für die Leitstellen. Unabhängig davon, muss von den Leitstellen untersucht werden, inwiefern der eigene Informationsverbund vom Profil abweicht. Gegebenenfalls sind bei der späteren Umsetzung weitere Bausteine als relevant einzustufen.

Die Bausteine aus der Rubrik Industrielle IT werden mangels Relevanz für den Betrieb von Leitstellen von vornherein nicht aufgeführt.

Die nachfolgenden Tabelle 29 bis Tabelle 33 beinhalten die Prozessbausteine. Diese behandeln ganzheitliche Anforderungen und gelten für sämtliche Teile des Informationsverbundes. Dagegen führen

die Tabelle 34 bis Tabelle 37 die Systembausteine auf. Systembausteine behandeln die Facetten bestimmter Komponenten. Hier ist entscheidend, ob der Baustein für eine spezifische, in Abschnitt 4 bestimmte, Komponente relevant ist.

ISMS: Sicherheitsmanagement

ID	Baustein	Relevant?	Hinweis
ISMS.1	Sicherheitsmanagement	Ja	

Tabelle 29: Relevanz der Bausteine aus der Schicht ISMS: Sicherheitsmanagement.

² https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html (abgerufen am 13.02.2024)

ORP: Organisation und Personal

ID	Baustein	Relevant?	Hinweis
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	

Tabelle 30: Relevanz der Bausteine aus der Schicht ORP: Organisation und Personal

CON: Konzeption und Vorgehensweise

ID	Baustein	Relevant?	Hinweis
CON.1	Kryptokonzept	Ja	Leitstelle ist in der Regel nur Nutzer von Systemen die kryptografische Verfahren benötigen (z.B. Digitalfunk). Siehe auch Punkt 1.3 im Baustein.
CON.2	Datenschutz	Ja	
CON.3	Datensicherungskonzept	Ja	
CON.6	Löschen und Vernichten	Ja	
CON.7	Informationssicherheit auf Auslandsreisen	Nein	Leitstellen arbeiten üblicherweise ausschließlich lokal.
CON.8	Software-Entwicklung	Nein	Leitstellen entwickeln üblicherweise keine Software.
CON.9	Informationsaustausch	Ja	
CON.10	Entwicklung von Webanwendungen	Nein	Leitstellen entwickeln üblicherweise keine Webanwendungen.
CON.11.1	Geheimchutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NFD)	Nein	Dieser Baustein richtet sich an Bundesbehörden oder bundesunmittelbare öffentlich-rechtliche Einrichtungen, die der VSA unterliegen. Dies ist bei Leitstellen nicht der Fall.

Tabelle 31: Relevanz der Bausteine aus der Schicht CON: Konzeption und Vorgehensweise

OPS: Betrieb

ID	Baustein	Relevant?	Hinweis
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	Ja	
OPS.1.2.2	Archivierung	Ja	
OPS.1.2.4	Telearbeit	Ja	Sofern im üblichen Dienstbetrieb, insbesondere in der Administration, genutzt.
OPS.1.2.5	Fernwartung	Ja	
OPS.1.2.6	NTP-Zeitsynchronisation	Ja	
OPS.2.2	Cloud-Nutzung	Nein	Der Betrieb der IT-Systeme findet in Leitstellen üblicherweise lokal statt. Das BSI definiert Cloud als die Nutzung dynamisch anpassbarer und abzurechnender Systeme über ein Netz.
OPS.2.3	Nutzung von Outsourcing	Ja	Relevant sobald Dienstleister/Hersteller von Leitstellensystemen Fernwartung nutzen.
OPS.3.2	Anbieten von Outsourcing	Nein	Leitstellen übernehmen üblicherweise keine ausgelagerten Dienstleistungen für andere Institutionen.

Tabelle 32: Relevanz der Bausteine aus der Schicht OPS: Betrieb

DER: Detektion und Reaktion

ID	Baustein	Relevant?	Hinweis
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	Revision auf Basis des Leitfadens IS-Revision	Nein	Gilt nur für Bundesbehörden.
DER.4	Notfallmanagement	Ja	

Tabelle 33: Relevanz der Bausteine aus der Schicht DER: Detektion und Reaktion

In den folgenden Tabellen werden die Systembausteine aufgeführt. Hier ist entscheidend, ob der Baustein für eine spezifische, in Abschnitt 4 bestimmte, Komponente relevant ist.

APP: Anwendungen

ID	Baustein	Relevant?	Hinweis
APP.1.1	Office-Produkte	Ja	
APP.1.2	Web-Browser	Ja	
APP.1.4	Mobile Anwendung (Apps)	Nein	Für Apps zur Alarmierung der angebundenen Organisationen oder Notruf-Apps liegt die Verantwortung bei den jeweiligen Betreibern und Nutzern. Werden Apps innerhalb der Leitstelle verwendet, z.B. auf Tablets zur Bedienung der Medientechnik, wird der Baustein relevant.
APP.2.1	Allgemeiner Verzeichnisdienst	Ja	
APP.2.2	Active Directory Domain Services	Ja	
APP.2.3	OpenLDAP	Nein	
APP.3.1	Webanwendungen und Webservices	Ja	
APP.3.2	Webserver	Ja	Sofern eigene Webserver betrieben werden.

Fortsetzung der Tabelle nächste Seite

ID	Baustein	Relevant?	Hinweis
APP.3.3	Fileserver	Ja	
APP.3.4	Samba	Nein	
APP.3.6	DNS-Server	Ja	Gilt auch, wenn der DNS kann als Teilprozess auf Router oder Firewall betrieben wird.
APP.4.2	SAP-ERP-System	Nein	In Leitstellen üblicherweise nicht vorhanden.
APP.4.3	Relationale Datenbanksysteme	Ja	
APP.4.4	Kubernetes	Ja	Ist immer mit dem Baustein SYS.1.6 Containerisierung anzuwenden
APP.4.6	SAP ABAP-Programmierung	Nein	In Leitstellen üblicherweise nicht vorhanden.
APP.5.2	Microsoft Exchange und Outlook	Nein	Nicht zwingend erforderlich, sofern kein Exchange/Outlook eingesetzt wird.
APP.5.3	Allgemeiner E-Mail-Client und -Server	Ja	
APP.5.4	Unified Communications und Collaboration (UCC)	Nein	UCC umfasst Kommunikationsdienste wie z.B. Videokonferenzsysteme. Auch das KMS könnte darunterfallen. NET.1.1 und NET.3.2 sind zu beachten.
APP.6	Allgemeine Software	Ja	
APP.7	Entwicklung von Individualsoftware	Nein	Normalerweise keine Entwicklung von Individualsoftware in den Leitstellen.

Tabelle 34: Relevanz der Bausteine aus der Schicht APP: Anwendungen

SYS: IT-Systeme

ID	Baustein	Relevant?	Hinweis
SYS.1.1	Allgemeiner Server	Ja	
SYS.1.2.2	Windows Server 2012	Ja	
SYS.1.2.3	Windows Server	Ja	
SYS.1.3	Server unter Linux und Unix	Ja	
SYS.1.5	Virtualisierung	Ja	

Fortsetzung der Tabelle nächste Seite

ID	Baustein	Relevant?	Hinweis
SYS.1.6	Containerisierung	Ja	
SYS.1.7	IBM Z-System	Nein	In Leitstellen üblicherweise nicht vorhanden.
SYS.1.8	Speicherlösungen	Ja	
SYS.1.9	Terminalserver	Nein	In Leitstellen nicht zwingend benötigt.
SYS.2.1	Allgemeiner Client	Ja	
SYS.2.2.3	Clients unter Windows	Ja	
SYS.2.3	Clients unter Linux und Unix	Ja	Kann auch relevant werden bei Nutzung von Anzeigesystemen (z.B. durch Raspberry Pi)
SYS.2.4	Clients unter macOS	Nein	Üblicherweise nicht vorhanden, weil Leitstellensysteme in Deutschland meistens Windows/Linux benötigen.
SYS.2.5	Client-Virtualisierung	Ja	
SYS.2.6	Virtual Desktop Infrastructure	Nein	In Leitstellen nicht zwingend vorhanden.
SYS.3.1	Laptops	Ja	
SYS.3.2.1	Allgemeine Smartphones und Tablets	Nein	Kann für Bedienung für Peripheriesysteme (z.B. Steuerung Haustechnik/Medientechnik) relevant sein.
SYS.3.2.2	Mobile Device Management (MDM)	Nein	Für Betrieb der Leitstelle nicht erforderlich.
SYS.3.2.3	iOS (for Enterprise)	Nein	In Leitstellen üblicherweise nicht vorhanden.
SYS.3.2.4	Android	Nein	In Leitstellen üblicherweise nicht vorhanden.
SYS.3.3	Mobiltelefon	Nein	In Leitstellen üblicherweise nicht vorhanden.
SYS.4.1	Drucker, Kopierer und Multifunktionsgeräte	Ja	
SYS.4.3	Eingebettete Systeme	Nein	In Leitstellen üblicherweise nicht vorhanden.
SYS.4.4	Allgemeines IoT-Gerät	Nein	In Leitstellen üblicherweise nicht vorhanden.
SYS.4.5	Wechseldatenträger	Ja	SYS.4.5A12: Durch das Verwenden einer Datenschluse mit Antivirensoftware kann die Sicherheit erhöht werden.

Tabelle 35: Relevanz der Bausteine aus der Schicht SYS: IT-Systeme

NET: Netze und Kommunikation

ID	Baustein	Relevant?	Hinweis
NET.1.1	Netzwerkarchitektur und -design	Ja	
NET.1.2	Netzmanagement	Ja	
NET.2.1	WLAN-Betrieb	Ja	Auf strikte Trennung zu den kritischen Systemen ist zu achten!
NET.2.2	WLAN-Nutzung	Ja	
NET.3.1	Router und Switches	Ja	
NET.3.2	Firewall	Ja	
NET.3.3	VPN	Ja	
NET.3.4	Network Access Control	Nein	Ist in Leitstellen noch nicht stark verbreitet. Z.B. bei Nutzung von RADIUS-Server relevant.
NET.4.1	TK-Anlagen	Ja	
NET.4.2	VoIP	Ja	
NET.4.3	Faxgeräte und Faxserver	Ja	Solange noch in Benutzung.

Tabelle 36: Relevanz der Bausteine aus der Schicht NET: Netze und Kommunikation

INF: Infrastruktur

ID	Baustein	Relevant?	Hinweis
INF.1	Allgemeines Gebäude	Ja	
INF.2	Rechenzentrum sowie Serverraum	Ja	
INF.5	Raum sowie Schrank für technische Infrastruktur	Ja	
INF.6	Datenträgerarchiv	Ja	
INF.7	Büroarbeitsplatz	Ja	
INF.8	Häuslicher Arbeitsplatz	Ja	Siehe Baustein OPS.1.2.4 Telearbeit
INF.9	Mobiler Arbeitsplatz	Nein	Abweichend kann es in einigen Leitstellen mobile Arbeitsplätze z.B. im ELW oder in der IT-Administration geben.
INF.10	Besprechungs-, Veranstaltungs- und Schulungsraum	Ja	
INF.11	Allgemeines Fahrzeug	Nein	Wird relevant, wenn organisationseigene Fahrzeuge zum Informationsverbund gehören
INF.12	Verkabelung	Ja	
INF.13	Technisches Gebäudemanagement	Ja	
INF.14	Gebäudeautomation	Ja	

Tabelle 37: Relevanz der Bausteine aus der Schicht INF: Infrastruktur

5.3 Anforderungen übergreifend gültiger Prozessbausteine

Nachdem die Bausteine bezüglich der Informationssicherheit in Leitstellen auf Relevanz untersucht wurden, werden im nächsten Schritt die Anforderungen der relevanten Bausteine geprüft. Sofern notwendig werden sie an die Rahmenbedingungen in Leitstellen angepasst. Die Bausteine sind im Folgenden tabellarisch dargestellt. Aufgeführt sind Basis- und Standard-Anforderungen. Dabei müssen die aufgeführten Anforderungen auf geeignete Weise erfüllt werden: Sind bei einzelnen Bausteinen auch die Anforderungen für erhöhten Schutzbedarf zu erfüllen, werden diese extra benannt:

Baustein	Hinweise
ISMS.1 Sicherheits-manage-ment	<p>ISMS.1.A4: Der Informationssicherheitsbeauftragte kann je nach Größenordnung der Leitstelle auch weitere Funktionen in Personalunion ausüben.</p> <p>ISMS.1.A5: Der externe Informationssicherheitsbeauftragte sollte über die notwendigen Qualifikationen verfügen, dies kann bspw. durch eine Zertifizierung zum Informationssicherheitsbeauftragten sichergestellt werden.</p> <p>ISMS.1.A10: Bei der Erstellung eines Sicherheitskonzepts empfiehlt es sich mit den Bereichen der Leitstelle zu beginnen, die das höchste Schutzniveau erfordern. Anschließend kann das Sicherheitskonzept um weitere Bereiche ergänzt werden</p> <p>ISMS.1.A12: Bei der Erstellung der Management-Berichte empfiehlt es sich, die zugehörigen Vorgaben der Norm ISO 27001 zu berücksichtigen.</p>
ORP.1 Organisa-tion	<p>Sofern eine Beeinträchtigung des Betriebs der Leitstelle unvermeidbar ist, sind Wartungs- und Reparaturarbeiten, sofern möglich, zu Tageszeiten durchzuführen, in denen mit weniger Einsätzen gerechnet werden kann (z.B. nachts).</p> <p>ORP.1.A8: Mit der Implementierung eines Überwachungs- und Audit-Programms kann sichergestellt werden, dass Geräte und Betriebsmittel ordnungsgemäß verwaltet werden und den Sicherheitsanforderungen entsprechen.</p> <p>ORP.1.A16: Die Richtlinie zur sicheren IT-Nutzung sollte auch den Meldeweg für die Mitarbeiter zur Meldung von Sicherheitsvorfällen berücksichtigen (z.B. Online-Formulare, E-Mail-Adressen oder Hotlines).</p>
ORP.2 Personal	<p>ORP.2.A1: Die Mitarbeiter sollten nach der initialen Einarbeitung kontinuierlich über neue / geänderte Regelungen zur Informationssicherheit informiert werden (z.B. Intranet-News, Update-Schulungen).</p> <p>ORP.2.A3: Die Vertretenden sollten in einer für alle Mitarbeiter leicht und schnell zugänglichen Liste festgehalten werden, um im Bedarfsfall schnell darauf zurückgreifen zu können.</p> <p>ORP.2.A7: Je nach Position und Verantwortung / Zugriffsberechtigungen können Sicherheitsüberprüfungen sinnvoll sein.</p> <p>ORP.2.A14: Neben Verordnungen zum Datenschutz (Datenschutz Grundverordnung und Ländergesetze) umfasst dies für das Personal der Leitstelle auch Teile der Ländergesetze zur Gefahrenabwehr und des Strafgesetzbuches. Aufgaben und Zuständigkeiten von Mitarbeitenden sollten in Rollen- / Stellenbeschreibungen dokumentiert werden.</p>
ORP.3 Sensibili-sierung und Schulung zur In-formationssicher-heit	<p>ORP.3.A4: Die Landesschulen für Feuerwehr und Rettungsdienst können im Rahmen der Aus- und Fortbildungen für Leitstellendisponenten mit einbezogen werden.</p>

ORP.4 Identitäts- und Berechtigungsmanagement	<p>ORP.4.A12: Es ist ratsam eine Multifaktor-Authentisierung (MFA), insbesondere für Systeme und Anwendungen, die besonders Schützenswerte Informationen verarbeiten zu implementieren. MFAs bieten eine zusätzliche Sicherheits-ebene, indem mehrere Authentisierungsfaktoren erforderlich sind.</p> <p>ORP.4.A23: Es ist essenziell ein sicheres Passwort für alle Konten zu besitzen. Grundsätzlich gilt: „Je länger, desto besser“. Deswegen sollte ein sicheres Passwort mindestens acht Zeichen lang sein und weitere Sicherheitsvorgaben der Organisation beinhalten (z.B. Sonderzeichen, Zahlen).</p>
ORP.5 Compliance Management (Anforderungsmanagement)	<p>ORP.5.A1: Das Personal der Leitstelle muss auf die Dokumentation der Vorgaben schnellen Zugriff haben.</p> <p>ORP.5.A4: Eine regelmäßige Risikoanalyse kann dabei unterstützen, sicherheitsrelevante Anforderungen in geeignete Sicherheitsmaßnahmen zu überführen. Die Umsetzung der Maßnahmen kann bspw. über interne Audits kontrolliert werden.</p> <p>ORP.5.A5: Die Implementierung eines Prozesses zur regelmäßigen Überprüfung stellt sicher, dass die gewährten Ausnahmegenehmigungen weiterhin gerechtfertigt sind. Ändern sich die Umstände, sollten die Ausnahmen entsprechend angepasst und aufgehoben werden.</p>
CON.1 Kryptokonzept	-
CON.2 Datenschutz	-
CON.3 Datensicherungskonzept	<p>CON3.A.3: Die Regelungen zur Speicherdauer von Notrufen in den Gesetzen der Länder sind zu beachten.</p> <p>CON.3.A4: Der Datensicherungsplan sollte je IT-System aufgestellt werden. Eine prozess- oder anwendungsbezogene Sicherung ist im begründeten Fall auch denkbar. Mindestanforderung muss eine tägliche Sicherung der notwendigen Daten sein. Hierbei ist das Generationenprinzip anzuwenden.</p> <p>CON.3.A9: Von einer Online-Datensicherung sollte abgesehen werden. Diese ist zumindest kritisch zu prüfen.</p> <p>CON.3.A12: Als geografisch entfernter Aufbewahrungsort kann zum Beispiel eine definierte Ersatznotrufabfragestelle bestimmt werden.</p> <p>CON.3.A13: Im Umfeld der Leitstellen normalerweise entbehrlich, sofern die Datensicherung lokal oder an einem vergleichbaren Ort aufbewahrt wird.</p>
CON.6 Löschen und Vernichten	CON.6.A14: Diese erhöhte Anforderung sollte im Umfeld der Leitstellen auch umgesetzt werden.
CON.9 Informationsaustausch	CON.9.A9: Diese erhöhte Anforderung sollte im Umfeld der Leitstellen auch umgesetzt werden.

OPS.1.1.1 Allgemeiner IT-Betrieb	OPS.1.1.1.A3: Auf Grund vielfältiger Systemtechnik in einer Leitstelle sollte es für alle relevanten IT-Komponenten entsprechende Betriebshandbücher geben. Diese Unterlagen sollten regelmäßig überprüft und bei Bedarf entsprechend aktualisiert werden.
OPS.1.1.2 Ordnungsgemäße IT-Administration	<p>OPS.1.1.2.A22: Auch wenn die Tätigkeiten der Administration durch Disponenten in Personalunion durchgeführt werden, ist auf Rollentrennung zu achten. Der Disponent sollte nicht mit Administrationsrechten eingeloggt sein</p> <p>OPS.1.1.2.A25: Sofern eine Beeinträchtigung des Betriebs der Leitstelle unvermeidbar ist, sind Wartungs- und Reparaturarbeiten, sofern möglich, zu Tageszeiten durchzuführen, in denen mit weniger Einsätzen gerechnet werden kann (z.B. nachts).</p>
OPS.1.1.3 Patch- und Änderungsmanagement	<p>OPS.1.1.3.A1: Nach Möglichkeit können Änderungen zunächst an einem Schulungssystem getestet werden, bevor sie in das Produktivsystem übernommen werden.</p> <p>OPS.1.1.3.A7: Die Erreichbarkeit des Supports sollte bei und unmittelbar nach der Installation von Patches gewährleistet sein. Eine Installation vor Wochenenden, Feiertagen oder Terminen, die eine hohe Einsatzanzahl erwarten lassen, sollte vermieden werden.</p>
OPS.1.1.4 Schutz vor Schadprogrammen	OPS.1.1.4.A5: Um Funktionseinschränkungen zu vermeiden, sollte der Betrieb und die Konfiguration des Viren-Schutzprogramms mit den Herstellern von Leitstellensystemen abgestimmt werden.
OPS.1.1.5 Protokollierung	OPS.1.1.5.A6/A9: Protokollierungsdaten sind wichtig sowohl zur präventiven Fehlererkennung und -vermeidung als auch zur Feststellung von Anomalien, die mit einem gerade stattfindenden Cyberangriff im Zusammenhang stehen. Deshalb sollten Protokolldaten zentral gesammelt und fortlaufend – sinnvollerweise automatisiert – ausgewertet werden.
OPS.1.1.6 Software-Tests und -Freigaben	OPS.1.1.6.A13: Neue und aktualisierte Software (z. B. Service Packs oder Hot Fixes) sollten zunächst in einem separaten Test- bzw. Schulungssystem überprüft werden, bevor sie dann ins Produktivsystem übernommen werden. Bei Synchronisierung sollte darauf geachtet werden, keine datenschutzrelevanten Daten in das Testsystem zu übernehmen (Patientendaten).
OPS.1.1.7 Systemmanagement	OPS.1.1.7.A18: Da es in Leitstellen meist auch zur Verwendung von OT-Systemen kommt oder noch sog. Legacy-Systeme im Einsatz sind, sollte der tatsächliche Systemzustand solcher Systeme regelmäßig überprüft werden. Denn bei Aktualisierungen, bei welchen auch die Management-Schnittstellen verändert werden, besteht ein erhöhtes Risiko für plötzliche Inkompatibilitäten und folglich unbemerkten Fehlerzuständen bzw. Fehlfunktionen.
OPS.1.2.2 Archivierung	OPS.1.2.2.A9: Bei einem Wechsel des Leitstellensystems muss darauf geachtet werden, den Zugriff auf die Einsatzdaten des alten Systems zu Dokumentationszwecken temporär zu behalten.

OPS.1.2.5 Fernwartung	Der Baustein ist relevant, wenn externe IT-Dienstleister oder die Hersteller von Einsatzleitsystemen Wartungsarbeiten per Fernwartung in der Leitstelle durchführen.
OPS.1.2.6 NTP-Zeitsynchronisation	
DER.1 Detektion von sicherheitsrelevanten Ereignissen	-
DER.2.1 Behandlung von Sicherheitsvorfällen	DER.2.1.A6: Eine Inbetriebnahme der Ersatznotrufabfragestelle kann in Betracht gezogen werden.
DER.2.2 Vorsorge für die IT-Forensik	-
DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle	-
DER.3.1 Audits und Revisionen	-
DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision	-
DER.4 Notfallmanagement	Siehe hierzu Kapitel 8.

Tabelle 38: Anforderungen und Hinweise übergreifend gültiger Prozessbausteine

5.4 Anforderungen spezifisch gültiger Prozessbausteine

Die folgenden aufgeführten Bausteine betreffen nur die jeweils angegebenen Zielobjekte. Erfüllt werden müssen in der Regel die Basis- und Standard-Anforderungen. Dabei müssen die aufgeführten Anforderungen auf geeignete Weise erfüllt werden. Sind bei einzelnen Bausteinen zusätzlich die Anforderungen für erhöhten Schutzbedarf zu erfüllen, werden diese extra benannt:

Baustein	Ziel- objekt	Hinweise
APP.1.1 Office-Produkte	S1	APP.1.1.A9: Ein geeignetes Format für die Weitergabe von Dokumenten, die vom Empfänger nicht bearbeitet werden müssen, ist zum Beispiel das PDF-Format.
APP.1.2 Web-Browser	S1	Zu den Basis- und Standardanforderungen ist zusätzlich APP.1.2.A12 zu erfüllen
APP.2.1 Allgemeiner Verzeichnis-dienst	S2	-
APP.2.2 Active Directory	S2, S4	-
APP.2.3 Open-LDAP	S2	-
APP.3.3 Fileserver	S6	-
APP.3.4 Samba	S6	-
APP.3.6 DNS-Server	S2, N1	-
APP.4.3 Relationale Datenbanksysteme	S5	<p>Datenbanksysteme und deren Daten sind die Grundlage der Einsatzleitsysteme. Es besteht ein hoher bis sehr hoher Schutzbedarf für die vorgehaltenen Daten. Die folgenden Bausteine aus dem erhöhtem Schutzbedarf sollten daher zusätzlich angewendet werden:</p> <p>APP.4.3.A21 Einsatz von Datenbank Security Tools (H) APP.4.3.A22 Notfallvorsorge (H) APP.4.3.A23 Archivierung (H) APP.4.3.A25 Sicherheitsprüfungen von Datenbanksystemen (H)</p> <p>Sofern die Datenhaltung nicht lokal erfolgt ist noch APP.4.3.A24 (Datenverschlüsselung in der Datenbank) zu beachten.</p>
APP.4.4 Kubernetes	A1,A2	
APP.5.3 Allgemeine E-Mail-Client und -Server	A3, S1	<p>Durch Schnittstellen mit Einsatzleitsystemen ist hier ein Einfallstor für Angriffsszenarien, ebenso könnten vertrauliche Daten aus Einsatzleitsystemen durch Mails abfließen.</p> <p>APP.5.3.A10 Ende-zu-Ende-Verschlüsselung und Signatur (H) APP.5.3.A11 Einsatz redundanter E-Mail-Server (H) APP.5.3.A12 Überwachung öffentlicher Block-Listen (H)</p>
APP.5.4 Unified Communications und Collaboration	A2,A3	Durch Einbindung von neuen Kommunikationswegen in den Notruf und deren Einbindung in Einsatzleitsysteme entstehen neue Risiken die beachtet werden müssen.
APP.6 Allgemeine Software	Alle A	

SYS.1.1 Allgemeiner Server	S2	-
SYS.1.2.3 Windows Server	S2	
SYS.1.3 Server unter Linux und Unix	S2	
SYS.1.5 Virtualisierung	S3	Einsatzleitsysteme und weitere Leitstellensysteme werden vielfach auf Virtualisierungssystemen betrieben.
SYS.1.6 Containerisierung	A1,A2	
SYS.1.8 Speicherlösungen	S3,S6	
SYS.2.1 Allgemeiner Client	S1	-
SYS.2.2.3 Clients unter Windows	S1	SYS.2.2.3.A4: Gesperrt werden können diese Verbindungen z.B. in der Firewall.
SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte	P2.2	-
SYS.4.5 Wechseldatenträger	P3.3	SYS.3.4.A4: Durch das Verwenden einer Datenschleuse mit Antivirensoftware kann die Sicherheit erhöht werden.
NET.1.1 Netzarchitektur und -design	N1	<p>NET.1.1.A4: Die Aufteilung in Sicherheitszonen (Schalenmodell) ermöglicht die Erstellung mehrerer zu überwindender Sicherheitsgrenzen und erschwert dadurch das Eindringen in relevante Bereiche. ELS und KMS müssen im internen Netz betrieben werden.</p> <p>NET.1.1.A5: Durch eine Client-Server-Segmentierung mit unterschiedlichen Netzsegmenten werden besonders sensible Bereiche wie ELS und KMS geschützt.</p> <p>NET.1.1.A18: Die Absicherung sollte mittels einer NG-Firewall mit P-A-P-Struktur (Paketfilter – Application-Level-Gateway – Paketfilter) erfolgen mit eng definierten Zugangskanälen.</p> <p>NET.1.1.A23 Die Trennung von Einsatzleitsystem- und anderen Netzen erhöht das Sicherheitsniveau.</p> <p>NET.1.1.A28: HA-(High Availability) -Strukturen sind zwingend vorzusehen mit mindestens 99,99 % Verfügbarkeit (gemäß Verfügbarkeitsklasse 3, Handreichung Leitstellenplanung des Fachverbands Leitstellen)</p>

NET.1.2 Netzmanagement	N1	Inkl. NET.1.2.A31 bis NET.1.2.A38 Anforderungen für den erhöhten Schutzbedarf
NET 2.1 WLAN-Betrieb	N1	NET.2.1.A1: Eine Festlegung einer Strategie für den Einsatz von WLANs mit Beachtung der erhöhten Vulnerabilität und der dadurch besonders notwendigen Sicherheitsbetrachtung ist hier erforderlich!
NET 2.2 WLAN-Nutzung	N1	
NET.3.1 Router und Switches	N1	
NET.3.2 Firewall	N1, N2	NET.3.2.A27 aus erhöhtem Schutzbedarf ist zu beachten!
NET.3.3 VPN	N1	Für VPN-Zugänge sind zwingend Multifaktor-Authentifizierungen (MFA) vorzusehen.
NET.3.4 Network Access Control	N1	Der Einsatz von NAC ist eine Organisationsentscheidung und nicht zwingend vorausgesetzt, muss dann aber Anforderungskonform erfolgen.
NET.4.1 TK-Anlagen	A6, S8, N2	NET.4.1.A19: Redundanter Anschluss insbesondere für Notruf-Leitungen ist zwingend vorzusehen.
NET.4.2 VoIP	A6, S7, N2	NET.4.2.A1: Die Erfüllung der technischen Richtlinie Notruf ist bei der Planung des VoIP-Einsatzes zu beachten.
NET.4.3 Faxgeräte und Faxserver	A6	Prüfen ob Fax durch andere Transportmedien ersetzt werden kann!
INF.1 Allgemeines Gebäude	R1	-
INF.2 Rechenzentrum sowie Serverraum	R1.2	INF.2.A26: Redundante Auslegung von Netzersatzanlagen in Form kurzzeitig verfügbarer mobiler Einheiten vorsehen.
INF.5 Raum sowie Schrank für technische Infrastruktur	R1.2	Sollte in separater Räumlichkeit vorhanden sein und nicht in anderweitig genutzten Räumen integriert.
INF.6 Datenträgerarchiv	R1	
INF.7 Büroarbeitsplatz	R1.3, R1.4	Administrationsbüros unterliegen einem erhöhten Sicherheitsniveau und sind vor jeglichem Besucherverkehr abzusichern.
INF.8 Häuslicher Arbeitsplatz	extern	Es ist immer INF.8.A6 aus dem erhöhten Schutzbedarf zu beachten!

INF.9 Mobiler Arbeitsplatz	extern	Nutzung im ELW oder in externer Befehlsständen bzw. angeschlossenen Wachen. Insbesondere die erhöhten Anforderungen INF.9.A10 Einsatz von Diebstahlsicherungen und INF.9.A11 Verbot der Nutzung unsicherer Umgebungen sind zu beachten.
INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume	R1.5	Es sind unterschiedliche Schutzbedarfe vorhanden zwischen rein intern genutzten Räumlichkeiten und denen, die öffentlich zugänglich sind. Interne Räume sind in besonders Zugangsgesicherten Bereichen einzurichten. INF.10.A3: Es empfiehlt sich, den Verschluss von Fenster und Türen organisatorisch zu regeln (z.B. über eine Richtlinie oder Arbeitsanweisung).
INF.12 Verkabelung	Alle R	INF.12.A1: Es sollte ein angemessener Kabelschutz berücksichtigt werden, um vor physischen Schäden oder Umwelteinflüssen geschützt zu sein. INF.12.A2: Der Bedarf an Kabelkapazität und Kabelwegen sollte zukünftige Erweiterungen / Änderungen aufgrund bspw. technischer Anforderungen berücksichtigen. Vor allem die steigenden Anforderungen an Bandbreite und Datenübertragungsgeschwindigkeiten sind wichtig.
INF.13 Technisches Gebäudemanagement	Alle R	INF.13.A4: Bei der Erstellung der Sicherheitsrichtlinie sollten Meinungen und Empfehlungen von Experten eingeholt werden, insbesondere Fachleute für Gebäudetechnik und Sicherheit.
INF.14 Gebäudeautomation	Alle R	INF.14.A6: Basierend auf der Art und dem Grad der Sicherheitsanforderungen sollte die Segmentierung des Netzwerkes entsprechend eingeteilt werden. Sicherheitskritische Systeme sollten in stärker abgeschotteten Segmenten platziert werden. INF.14.A11: Damit keine unbefugten Verbindungen aufgebaut werden, müssen notwendige offene Ports überwacht werden. Außerdem sollten Standard-Ports möglichst vermieden werden.

Tabelle 39: Anforderungen und Hinweise spezifisch gültiger Prozessbausteine

5.5 Anforderungen für spezifische Objekte

Es gibt für Leitstellen spezifische Objekte, die mit den vorhandenen Bausteinen des IT-Grundschutz nicht hinreichend modelliert werden. Diese müssen gesondert betrachtet werden und einer Risikoanalyse unterzogen werden. Daraus sind dann gemäß der IT-Grundschutzmethode Anforderungen abzuleiten, um das angestrebte Schutzniveau zu erreichen.

6 Restrisiko

Auch bei Umsetzung aller Anforderungen ist keine hundertprozentige Sicherheit zu erreichen. Dies muss sowohl den Anwendern des IT-Grundschutz-Profils, als auch den Entscheidungsträgern bewusst sein. Ein Restrisiko bleibt bestehen.

Durch die Zusammenarbeit mit anderen Organisationen werden vertrauliche Informationen an Institutionen übertragen, auf deren Sicherheitsmanagement eine Leitstelle nur beschränkt Einfluss nehmen kann. Auch eigene Mitarbeiter können trotz Dienstanweisungen und Schulungen, absichtlich oder unbewusst, solche Informationen an Unbefugte weitergeben.

Gezielte Angriffe auf die Informationstechnik einer Institution nehmen zu. Bekannt gewordene Sicherheitslücken in den Systemen werden immer schneller ausgenutzt. Eine rechtzeitige Behebung durch entsprechende Updates ist nicht immer möglich. Dies betrifft insbesondere Systeme, bei denen der Schwerpunkt bei der Entwicklung nicht auf die Informationssicherheit gelegt wurde.

Ein Restrisiko bleibt auch beim Bezug von Dienstleistungen Dritter. Trotz redundanter Internetanschlüsse kann es zum Beispiel zu Störungen an großen Netzknotenpunkten kommen, wodurch mehrere ISP betroffen sein können.

7 Anwendungshinweise

Die ermittelten Anforderungen sind in das Gesamtsicherheitskonzept zu integrieren und im Zuge der geplanten Realisierung umzusetzen.

Das BSI empfiehlt die Anforderungen der Bausteine in einer festgelegten Reihenfolge durchzuführen. Dadurch wird gewährleistet, dass die grundlegenden Risiken frühzeitig abgedeckt sind. Folgende Bausteine sollten als erstes umgesetzt werden:

- ISMS Sicherheitsmanagement
- ORP.1 bis ORP.4 aus ORP Organisation und Personal
- CON.3 und CON.6 aus CON Konzepte und Vorgehensweisen
- alle Bausteine aus OPS.1.1 Kern-IT-Betrieb

8 Notfallmanagement (BCM)

Trotz eines hohen Sicherheitsniveaus kann eine Beeinträchtigung der Betriebsbereitschaft der Leitstelle nicht ausgeschlossen werden. Aus diesem Grund müssen weitere Vorbereitungen getroffen werden, um auch bei einem Ausfall, der Aufgabenerfüllung in einer Leitstelle nachkommen zu können. Die Planung des Umgangs mit Krisen in einem kontinuierlichen Zyklus wird als Notfallmanagement oder mit dem englischen Begriff Business Continuity Management (BCM) bezeichnet. Ein standardisiertes Vorgehen ist im BSI Standard 200-4 und in der DIN EN ISO 22301:2014³ spezifiziert.

3 <https://www.beuth.de/de/norm/din-en-iso-22301/215741063> (abgerufen am 13.02.2024).

Das BSI beschreibt im Standard 200-4⁴ einen Notfallmanagement-Prozess. Dieser besteht aus fünf Phasen, die nach einer Initiierung kontinuierlich durchlaufen werden müssen: Konzeption, Umsetzung des Notfallvorsorgekonzepts, Notfallbewältigung, Tests und Übungen, Aufrechterhaltung und Verbesserung.

9 Unterstützende Informationen

Detailliertere Informationen zu den einzelnen Anforderungen finden sich in den Umsetzungshinweisen die für ausgewählte Bausteine des IT-Grundschutzes formuliert und zur Verfügung gestellt worden sind. Außerdem gibt es ein Dokument der European Emergency Number Association (EENA) zum Thema IT-Sicherheit in Leitstellen.⁵

4 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html (abgerufen am 13.02.2024).

5 <https://eena.org/our-work/eena-special-focus/cybersecurity/> (abgerufen am 13.02.2024).