IT-GRUNDSCHUTZ-PROFIL

BASIS-ABSICHERUNG KOMMUNALVERWALTUNG

31.03.2022

ARBEITSGRUPPE KOMMUNALE BASIS-ABSICHERUNG (AG KOBA) mit Unterstützung durch

Deutscher Städtetag

Deutscher Landkreistag

Deutscher Städte- und Gemeindebund

DOKUMENTENHISTORIE

Datum	Version	Änderungsgrund	Bearbeiter
08.05.2018	1.0	Erstellung	AG
15.10.2019	2.0	Anpassung an IT-Grundschutz-Kompendium 2019	AG
31.03.2022	3.0	Anpassung an IT-Grundschutz-Kompendium 2022	AG koBa

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

1 FORMALIEN

Titel:	IT-Grundschutz-Profil – Basis-Absicherung Kommunalverwaltung
Autor:	Arbeitsgruppe kommunale Basis-Absicherung (AG koBa)
Lizenz:	CC-BY-SA 3.0
Version:	3.0 (2022)
Status:	freigegeben
Revisionszyklus:	spätestens alle 3 Jahre
Vertraulichkeit:	öffentlich

2 HAFTUNGSAUSCHLUSS

Dieses Dokument wurde mit größter Sorgfalt erstellt, erhebt aber keinen Anspruch auf Vollständigkeit und Richtigkeit. Die Mitwirkenden an diesem Dokument haben keinen Einfluss auf dessen weitere Nutzung durch die einzelnen Anwender und können daher naturgemäß für die Auswirkungen auf die Rechtsposition der Parteien keine Haftung übernehmen.

3 URHEBERRECHT

4 AUTORENLISTE

An der Erarbeitung und Überarbeitung dieses Profils waren im Rahmen der Arbeitsgruppen „Modernisierung IT-Grundschutz" und „Arbeitsgruppe kommunale Basis-Absicherung (AG koBa)" die nachfolgend in alphabetischer Reihenfolge aufgelisteten Personen beteiligt:

Name	Version 1.0	Version 2.0	Version 3.0
Albert, Markus, Stadt Frankfurt am Main	X	X	X
Breer, Thorsten, Städtische Datenverarbeitung Wilhelmshaven	X		
Dr. Gollan, Lutz, Behörde für Inneres und Sport Hamburg	X		
Euler, Stefanie, Bundesamt für Sicherheit in der Informationstechnik (BSI, Referat BL12)			X
Früchtnicht, Thorsten, Zweckverband Kommunale Datenverarbeitung Oldenburg (KDO)			X
Grimm, Daniel, VITAKO	X		
Hansert, Michaela, Bundesamt für Sicherheit in der Informationstechnik (BSI, Referat BL12)			X
Heimfarth, Margot, SECURiON Rheinland-Pfalz GmbH	X	X	X
Hög, Matthias, Senatsverwaltung für Inneres und Sport Berlin	X		
Hurtig, Gregor, Zweckverband Elektronische Verwaltung in Mecklenburg-Vorpommern	X		X
Jacob, Martin, Zweckverband Kommunale Datenverarbeitung Oldenburg (KDO)			X
Jentzsch, Christine, Stadt Hennigsdorf	X		
Johansson, Christopher, Rhein-Sieg-Kreis	X		
Knierim, Micha Mark, Kreis Rendsburg-Eckernförde	X		
Kohl, Axel, Landratsamt Konstanz	X		
Körner, Nils, Zweckverband Kommunale Datenverarbeitung Oldenburg (KDO)	X		X
Kottke, David, Zweckverband Elektronische Verwaltung in Mecklenburg-Vorpommern (eGo-MV)	X		
Kramm, Norman, Landeshauptstadt Mainz	X		
Kustos, Pierre, Zweckverband Elektronische Verwaltung in Mecklenburg-Vorpommern (eGo-MV)	X		
Lange, Jens, Stadt Kassel	X	X	X
Lefèvre, Gert, Kreis Bergstraße	X		
Lenz, Susanne, Landeshauptstadt München	X		
Lion, Ralf, Landeshauptstadt Saarbrücken	X		
Maas, Oliver, KomFIT e. V.	X		
Mattauch, Sven, Bundesamt für Sicherheit in der Informationstechnik (BSI, Referat BL12)			X
Müller, Kai, Ministerium des Innern und für Sport Rheinland-Pfalz	X		
Novicov, Eugeniu, SECURiON Rheinland-Pfalz GmbH			X
Piotrowski,Stefan, Landratsamt Schwarzwald-Baar-Kreis	X		
Poburski, Maik, Landkreis Osnabrück	X	X	X
Reinartz, Heino, Städteregion Aachen	X	X	X
Sauerbrey, Heino, Deutscher Landkreistag	X	X	
Schoen, Kim, ITEBO GmbH	X		X
Schreckenberg, Roland, ML Consulting Köln			X
Schröder, Marcus, SECURiON Rheinland-Pfalz GmbH	X	X	
Stasch, Thomas, civitec	X		
von Hörde, Andreas, GEOZENTRUM Hannover	X		
Weidemann, Frank, IT-Verbund Schleswig-Holstein	X		X
Wojciechowski, Stefan, Landkreis Oberhavel	X		X

Tabelle 1: Beteiligte Personen

5 MANAGEMENT SUMMARY

5.1 Zielgruppe

Dieses IT-Grundschutz-Profil richtet sich an Kommunalverwaltungen, die einen systematischen Einstieg in die Informationssicherheit suchen.

Es ist adressiert an die Verantwortlichen in der Verwaltung, welche für die Umsetzung und Aufrechterhaltung der Informationssicherheit zuständig sind. Dies sind typischerweise die Hauptverwaltungsbeamtinnen und -beamten, welche die Ressourcen bereitstellen und das angestrebte Sicherheitsniveau einschließlich der Risiken verantworten, sowie die für die Steuerung und Koordination des Informationssicherheitsprozesses zuständigen Informationssicherheitsbeauftragten.

5.2 Zielsetzung

Dieses Profil basiert auf dem BSI-Standard 200-2 „IT-Grundschutz-Methodik" [BSI-200-2] und definiert die Mindestsicherheitsmaßnahmen, die in einer Kommunalverwaltung umzusetzen sind, um sich nach hiesiger Einschätzung nicht der groben Fahrlässigkeit schuldig zu machen. Das Profil erleichtert den Einstieg in die Informationssicherheit und hilft, die gröbsten Schwachstellen aufzudecken, die es zu beseitigen gilt, um möglichst schnell das Sicherheitsniveau in der Breite anzuheben. Um ein dem Stand der Technik angemessenes Sicherheitsniveau zu erreichen, müssen darauf aufbauend in einem weiteren Schritt jedoch zusätzliche Anforderungen erfüllt werden.

5.3 Hintergrund

Kommunalverwaltungen sind verpflichtet, ihre IT-Systeme und Verwaltungsvorgänge durch technische und organisatorische Maßnahmen ausreichend abzusichern, auch wenn keine unmittelbare Verpflichtung zur Umsetzung speziell des IT-Grundschutzes aus einer Rechtsnorm abgeleitet werden kann. Diese Verpflichtungen ergeben sich z. B. aus datenschutzrechtlichen Anforderungen (u. a. EU-Datenschutz-Grundverordnung) und dem Grundsatz des rechtmäßigen Verwaltungshandelns (Rechtsstaatsprinzip Art. 20 Abs. 3 Grundgesetz).

Darüber hinaus sind die erheblichen Investitionen der Kommunalverwaltungen in ihre IT-Ausstattungen über angemessene Sicherheitsvorkehrungen zu schützen. Im Hinblick auf die Grundsätze der Wirtschaftlichkeit umfasst das hier beschriebene Profil die Mindestanforderungen, um hohe materielle und immaterielle Schäden (z. B. Rufschäden

bzw. Vertrauensverlust) abzuwenden, die der Kommunalverwaltung durch den Bruch der Vertraulichkeit, Datenmanipulation oder Nichtverfügbarkeit der IT-Unterstützung entstehen können.

5.4 Handlungsempfehlung

Die Anwendung des kommunalen IT-Grundschutz-Profils ist ein wichtiger Schritt beim Aufbau systematischer Informationssicherheit in Kommunalverwaltungen.

Ziel muss es sein, darauf aufbauend mittelfristig ein Sicherheitskonzept gemäß der Standard-Absicherung (definiert in [BSI-200-2]) zu erstellen, da nur dies dem Schutzbedarf der Daten und Prozesse einer Kommunalverwaltung gerecht wird. Darüber hinaus sind kritische Verfahrensbereiche und Verfahren, für die bereits eindeutige rechtliche Vorgaben gelten (z. B. Waffenwesen oder Personenstandswesen), gemäß ihres höheren Schutzbedarfes mit zusätzlichen Maßnahmen abzusichern.

6 FESTLEGUNG DES GELTUNGSBEREICHS

6.1 Zielgruppe

Dieses IT-Grundschutz-Profil richtet sich an alle Kommunalverwaltungen und kommunalen Gebietskörperschaften in der Bundesrepublik Deutschland, unabhängig von ihrer Art oder Größe, die einen systematischen Einstieg in die Informationssicherheit suchen.

6.2 Schutzbedarf

Hinsichtlich des Schutzniveaus definiert das vorliegende Profil ein Niveau, das mindestens der Basis-Absicherung entspricht und unter dem der Standard-Absicherung der IT-Grundschutz-Vorgehensweise liegt.

Der Schutzbedarf der Daten und Geschäftsprozesse in einer Kommunalverwaltung ist in der Regel höher, insbesondere bei der Verarbeitung personenbezogener Daten. Um diese Verarbeitung abzusichern und ein dem Stand der Technik angemessenes Sicherheitsniveau zu erreichen, ist die Umsetzung zusätzlicher Anforderungen obligat.

6.3 Vorgehensweise nach IT-Grundschutz

Die in diesem Profil aufgeführten Anforderungen sind Empfehlungen, die sich an den Anforderungen der Basis-Absicherung des BSI-Standards 200-2 [BSI-200-2] orientieren. Teilweise wurden die Anforderungen um zusätzlich zu erfüllende Standard-Anforderungen

erweitert. Diese Ergänzungen sind notwendig, da Kommunalverwaltungen routinemäßig personenbezogene oder sonstige schützenswerte Informationen von Bürgerinnen und Bürgern und Unternehmen in teilweise öffentlich zugänglichen Räumlichkeiten verarbeiten.

6.4 Abdeckung Vorgehensweise

Für eine vollständige Basis-Absicherung aus der Sicht des BSI sind zusätzlich die Basis-Anforderungen der folgenden Bausteine umzusetzen.

- ORP.5 Compliance Management (Anforderungsmanagement)
- CON.1 Kryptokonzept
- CON.2 Datenschutz
- OPS.1.1.6 Software-Tests und -Freigaben
- DER.1 Detektion von sicherheitsrelevanten Ereignissen
- DER.2.2 Vorsorge für die IT-Forensik
- DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle
- DER.3.1 Audits und Revisionen
- DER.4 Notfallmanagement
- APP.1.4 Mobile Anwendung (Apps)
- APP.2.1 Allgemeiner Verzeichnisdienst
- Ggf. spezifische Server-Bausteine
- Ggf. spezifische Client-Bausteine

6.5 Testat der Basis-Absicherung

Mit einer Basis-Absicherung wird kein zertifizierungsfähiger Schutz gemäß ISO 27001 erreicht. Die Umsetzung des IT-Grundschutzes gemäß der Basis-Absicherung kann durch ein Testat nach der Basis-Absicherung durch einen BSI-zertifizierten IT-Grundschutz-Auditor nachgewiesen werden.

6.6 Rahmenbedingungen

Die Anwendung des Profils ist nur in Verbindung mit dem IT-Grundschutz-Kompendium Edition 2022 des BSI möglich.

Das Profil stellt eine Ergänzung zur Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen [HR-ISLL-KV] dar, kann aber auch unabhängig davon genutzt werden. Die Handreichung beschreibt den Einstieg in Entwicklung und Gestaltung von Informationssicherheitsleitlinien (ISLL) sowie Wege zum Aufbau und Betrieb kommunaler Informationssicherheitsmanagementsysteme (ISMS). Das Profil ist eine Unterstützung für den zweiten Schritt, da hier die Mindestanforderungen an ein kommunales ISMS definiert werden.

7 ABGRENZUNG DES INFORMATIONSVERBUNDES

7.1 Bestandteile des Informationsverbundes

Zum Informationsverbund „Basis-Absicherung Kommunalverwaltung" gehören jene Objekte, die typischerweise in jeder Kommunalverwaltung, unabhängig z. B. von deren Art und Größe, relevant sind (z. B. Büroraum oder Firewall). Damit wird der Großteil der vorkommenden Objekte abgedeckt.

7.2 Nicht berücksichtigte Objekte

In diesem Profil werden keine Fachprozesse oder Fachverfahren betrachtet. Im Rahmen der Ersterfassung müssen aber ausgehend von den wesentlichen Geschäftsprozessen und Fachverfahren auch die Fachaufgaben und Anwendungen identifiziert und in einer Übersicht erfasst werden. Ausgangspunkt kann hierfür ein vorhandener Aufgabengliederungsplan der Verwaltung sein.

Datenschutzspezifische Anforderungen werden in diesem Profil nicht speziell betrachtet. Jedoch unterstützt die Anwendung dieses Profils die Umsetzung der im Datenschutz geforderten technischen und organisatorischen Maßnahmen (TOMs). Inwiefern dann noch zusätzliche Anforderungen umzusetzen sind, entscheidet der Verantwortliche.

Des Weiteren ist stets zu prüfen, ob zusätzliche Sicherheitsanforderungen für die eigene Verwaltung zu beachten sind, welche über den Anspruch dieses Profils hinausgehen.

7.3 Verweis auf andere IT-Grundschutz-Profile

Entfällt.

8 REFERENZARCHITEKTUR

Der vom IT-Grundschutz-Profil betrachtete Informationsverbund beinhaltet alle essentiellen Objekte einer Kommunalverwaltung und wird im folgenden Unterkapitel „Untersuchungsgegenstand" beschrieben.

8.1 Untersuchungsgegenstand

8.1.1 Infrastruktur

- G01 Verwaltungsgebäude
- G02 Außenstelle (z. B. Bauhof, Kindergarten)
- R01 Büroraum
- R02 Bürgerbüro (Arbeitsplatz mit Publikumsverkehr)
- R03 Besprechungsraum
- R04 Häuslicher Arbeitsplatz
- R05 Mobiler Arbeitsplatz
- R06 Serverraum
- R07 Raum für technische Infrastruktur
- R08 Archivraum
- R09 Drucker- und Kopierraum
- F01 Dienst-Fahrzeuge

8.1.2 IT-Systeme

- IT01 Server (z. B. Datenbankserver, Managementserver)
- IT02 Terminal-Server
- IT03 Virtualisierungshost
- IT04 Netzwerk-Drucker / Multifunktionsgerät
- IT05 Arbeitsplatz-PC
- IT06 Smartphones und Tablets (inkl. „BYOD" von z. B. Ratsmitgliedern)
- IT07 Mobiler Arbeitsplatz-Rechner

8.1.3 Netze

- N01 Server- und Administrationsnetz
- N02 Demilitarisierte Zone (DMZ)
- N03 Netzwerk für reguläre Arbeitsplätze
- N04 WLAN (intern / ggf. öffentlich)
- N05 Gebäudeübergreifende Vernetzung
- N06 Internet-Zugang für die Verwaltung
- N07 Autonomer Internet-Zugang (z. B. einer Außenstelle)
- N08 Firewall
- N09 Router / Switch
- N10 TK-Anlage (inkl. Fax)
- N11 VoIP (Voice-over-IP)

8.1.4 Anwendungen

- A01 Internet-Nutzung
- A02 Benutzer-Authentifizierung
- A03 Dateiablage
- A04 Bürokommunikation (Groupware und E-Mail)
- A05 Office-Produkte

8.2 Netzplan

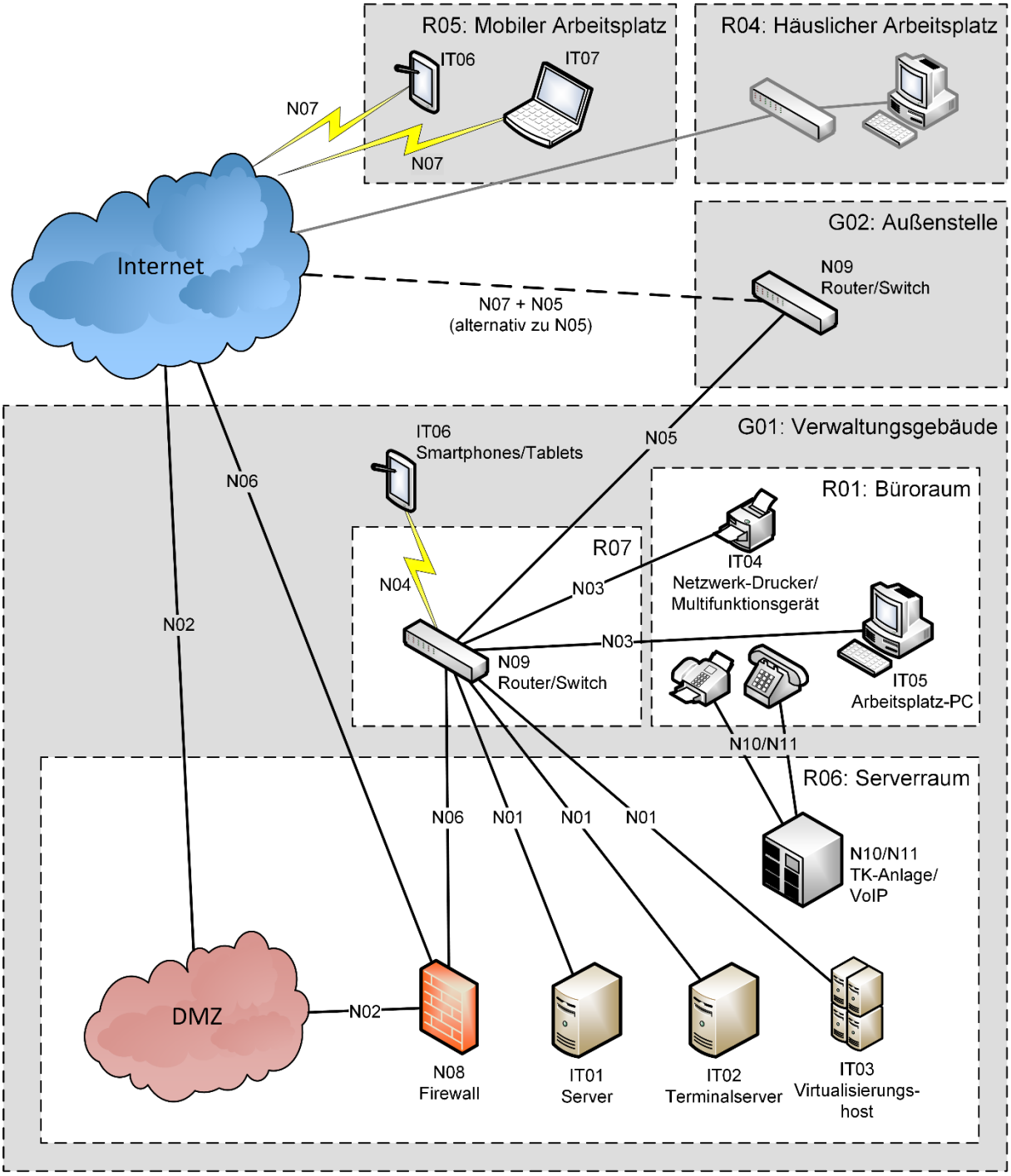

Abbildung 1: Vereinfachter Netzplan

8.3 Umgang mit Abweichungen

Weicht der zu schützende Informationsverbund von der Referenzarchitektur ab, sind die zusätzlichen oder nicht vorhandenen Objekte zu dokumentieren. Diesen sind geeignete Bausteine des IT-Grundschutz-Kompendiums zuzuordnen. Die aus den Bausteinen abgeleiteten Anforderungen müssen in Abhängigkeit des angestrebten Schutzniveaus angepasst werden.

9 ANFORDERUNGEN

9.1 Prozess-Bausteine

Die folgenden Prozess-Bausteine sind einmal auf den gesamten Informationsverbund anzuwenden. Wenn nicht anders angegeben, müssen alle Basis-Anforderungen der Bausteine durch Umsetzung der zugehörigen Maßnahmen der Umsetzungshinweise auf geeignete Weise erfüllt werden. Wenn zur Erreichung der Basis-Absicherung in einer Kommunalverwaltung zusätzlich Standard-Anforderungen und Anforderungen für den erhöhten Schutzbedarf erforderlich sind, werden diese durch ein Semikolon getrennt ebenfalls benannt. Hinweise für die kommunale Umsetzung sind unter „Besonderheiten" aufgeführt, entweder anforderungsspezifisch oder für den gesamten Baustein geltend.

9.1.1 ISMS.1 - Sicherheitsmanagement

Baustein	**ISMS.1**
Anforderungen	**ISMS.1.A1 – A9**
Besonderheiten	Die in der Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen [HR-ISLL-KV] enthaltenen Hilfestellungen können für die Umsetzung dieses Bausteins ebenfalls hilfreich sein.
	ISMS.1.A4 Von zentraler Bedeutung ist es, dass ein Verantwortlicher benannt wird, der die Thematik Informationssicherheit vorantreibt.

9.1.2 ORP.1 - Organisation

Baustein	**ORP.1**
Anforderungen	**ORP.1.A1 – A4, A15**

Baustein	**ORP.1**
Besonderheiten	ORP.1.A1 Von der in den Umsetzungshinweisen geforderten Organisationsstruktur kann abgewichen werden, solange gewährleistet ist, dass die notwendigen Verantwortlichkeiten definiert sind. Dies gilt auch dann, wenn es z. B. wirtschaftlich notwendig ist, dass eine Person mehrere Verantwortlichkeiten auf sich vereint.
	ORP.1.A4 Von der in den Umsetzungshinweisen geforderten Organisationsstruktur kann abgewichen werden, solange gewährleistet ist, dass diejenigen, die sowohl operative als auch kontrollierende Aufgaben wahrnehmen, sich der damit verbundenen Problematik bewusst sind und dementsprechend handeln.
	ORP.1.A15 Der Ansprechpartner für komplexe technische Sicherheitsfragen kann auch ein externer Dienstleister sein.

9.1.3 ORP.2 - Personal

Baustein	**ORP.2**
Anforderungen	**ORP.2.A1 – A5, A7, A14 – A15**
Besonderheiten	ORP.2.A7 Die Anforderung „Überprüfung der Vertrauenswürdigkeit von Mitarbeitern" ist nur zu erfüllen, wenn Positionen zu besetzen sind, deren Kandidaten besonders vertrauenswürdig sein müssen (z. B. Leiter IT).

9.1.4 ORP.3 - Sensibilisierung und Schulung zur Informationssicherheit

Baustein	**ORP.3**
Anforderungen	**ORP.3.A1, A3; A6**
Besonderheiten	ORP.3.A6 Um sicherzustellen, dass Sicherheitsmaßnahmen nicht versehentlich falsch umgesetzt oder unwissentlich ignoriert werden, müssen Mitarbeiter strukturiert und fortlaufend sensibilisiert werden.

9.1.5 ORP.4 - Identitäts- und Berechtigungsmanagement

Baustein	**ORP.4**
Anforderungen	**ORP.4.A1 – A9, A22 – A23; A19**
Besonderheiten	ORP.4.A19 Um die Gefahr versehentlicher Anwendungsfehler zu minimieren, sollten alle Mitarbeiter in den korrekten Umgang der Authentisierungsverfahren eingewiesen werden.

9.1.6 CON.3 - Datensicherungskonzept

Baustein	**CON.3**
Anforderungen	**CON.3.A1, A2, A4, A5; A12, A14 – A15**
Besonderheiten	CON.3.A12 Bei der Auswahl eines geeigneten Aufbewahrungsortes muss die lokale Gefahrenlage der Standorte (z. B. Hochwasser) berücksichtigt werden.

9.1.7 CON.6 - Löschen und Vernichten

Baustein	**CON.6**
Anforderungen	**CON.6.A1 – A2, A11 – A12; A13**
Besonderheiten	---

9.1.8 CON.9 - Informationsaustausch

Baustein	**CON.9**
Anforderungen	**CON.9.A1 – A3**
Hinweis	Es müssen grundsätzliche Regelungen geschaffen werden; z. B. wie zulässige Kommunikationspartner generell festgelegt werden. Die individuelle Ausgestaltung dieser Grundsätze in einzelnen Abteilungen (z. B. wer genau die zulässigen Kommunikationspartner im Meldewesen sind) wird hier nicht betrachtet. Wenn der Informationsaustausch über Datenträger erfolgt, sind die Anforderungen aus Baustein SYS.4.5 Wechseldatenträger anzuwenden.
Besonderheiten	---

9.1.9 OPS.1.1.2 - Ordnungsgemäße IT-Administration

Baustein	**OPS.1.1.2**
Anforderungen	**OPS.1.1.2.A2 – A6; A7 – A10, A12**
Hinweis	Wird die IT von externen Auftragnehmern administriert, müssen diese den Baustein umsetzen.
Besonderheiten	OPS.1.1.2.A7 Administrationslücken sowie eigenmächtige unbefugte Änderungen gefährden den Betrieb sicherer IT; daher sind entsprechende Regelungen zu treffen.
	OPS.1.1.2.A8 Aufgabenteilung zwischen Anwendungs- und Systemadministration ist für den sicheren IT-Betrieb unerlässlich.
	OPS.1.1.2.A9 Ohne ausreichende Ressourcen ist der Betrieb sicherer IT nicht gewährleistet.
	OPS.1.1.2.A12 Es müssen zumindest Regelungen zur Dokumentation durchgeführter Wartungsarbeiten sowie zur Beaufsichtigungspflicht von Wartungspersonal geben.

9.1.10 OPS.1.1.3 - Patch- und Änderungsmanagement

Baustein	**OPS.1.1.3**
Anforderungen	**OPS.1.1.3.A1 – A3, A15 – A16**
Hinweis	Das Patchmanagement stellt einen Teilbereich bzw. speziellen Prozess innerhalb des Änderungsmanagements dar, der auf die Aktualisierung von Software und Hardware zielt und in jedem Fall anzuwenden ist. Aspekte des Änderungsmanagements sind den lokalen Gegebenheiten entsprechend zu betrachten.
Besonderheiten	---

9.1.11 OPS.1.1.4 - Schutz vor Schadprogrammen

Baustein	**OPS.1.1.4**
Anforderungen	**OPS.1.1.4.A1 – A3, A5 – A7**
Besonderheiten	OPS.1.1.4.A5 Es muss gesichert sein, dass Benutzer keine sicherheitsrelevanten Änderungen am Antiviren-Programm vornehmen können.
	OPS.1.1.4.A7 Die Nutzer müssen Ansprechpartner kennen, an die sie sich im Falle des Verdachts auf eine Infektion mit einem Schadprogramm wenden können. Dies sollte in den Prozessen „Behandlung von Sicherheitsvorfällen" geregelt werden (siehe DER.2.1.A4).

9.1.12 OPS.1.1.5 - Protokollierung

Baustein	**OPS.1.1.5**
Anforderungen	**OPS.1.1.5.A1, A3 – A5; A10**
Besonderheiten	OPS.1.1.5.A10 Der Schutz von Protokollierungsdaten vor unbefugtem Zugriff ist unbedingt erforderlich, um deren Vertraulichkeit zu gewährleistet.

9.1.13 OPS.1.2.4 - Telearbeit

Baustein	**OPS.1.2.4**
Anforderungen	**OPS.1.2.4.A1 – A2, A5**
Hinweis	Dieser Baustein ist nur zu betrachten, wenn Telearbeit genutzt wird. Hilfestellung gibt die "Empfehlung zum sicheren mobilen Arbeiten im Homeoffice" des BSI.
Besonderheiten	OPS.1.2.4.A1 Es muss technisch und organisatorisch geprüft und entschieden werden, welche Aufgaben für Telearbeit in Betracht kommen. Für die Telearbeit sollten dieselben Nutzungsrechte für Internet-Dienste gelten wie bei allen anderen Arbeitsplätzen.

Baustein	**OPS.1.2.4**
	Telearbeiter sind genauso in den Kommunikationsfluss der Verwaltung zu integrieren wie alle anderen Mitarbeiter.

9.1.14 OPS.1.2.5 - Fernwartung

Baustein	**OPS.1.2.5**
Anforderungen	**OPS.1.2.5.A1 – A3; A5, A7 – A9, A19**
Hinweis	Dieser Baustein ist zu beachten, wenn Möglichkeiten zur Fernwartung von internen Administratoren oder externen Dritten genutzt werden.
Besonderheiten	OPS.1.2.5 A7 Die Dokumentation der Fernwartung enthält vertrauliche Informationen über Fernzugriffsmöglichkeiten. Der Schutz vor unbefugtem Zugriff muss sichergestellt sein.
	OPS.1.2.5. A8 Um eine Kompromittierung der Fernwartungssitzung zu verhindern, müssen aktuelle und als sicher eingestufte Kommunikationsprotokolle eingesetzt werden.
	OPS.1.2.5. A9 Um unkontrollierte Fernzugriffe zu unterbinden, müssen organisatorische Verwaltungsprozesse zum Umgang mit ausgewählten Fernwartungswerkzeugen etabliert werden.
	OPS.1.2.5.A19 Um administrative Anpassungen, die im Rahmen einer Fernwartung durch Dritte erfolgen, nachweislich zu dokumentieren, müssen auch alle Fernwartungsvorgänge durch Dritte aufgezeichnet werden. Mit Dritten, die Fernwartung durchführen, müssen vertragliche Regelungen getroffen werden, die vor allem der Sicherheit der betroffenen IT-Systeme und Informationen sowie den gesetzlichen Anforderungen entsprechen.

9.1.15 OPS.2.1 - Outsourcing für Kunden

Baustein	**OPS.2.1**
Anforderungen	**OPS.2.1.A1; A2 – A4, A6 – A10, A12, A15**
Hinweis	Dieser Baustein ist nur zu beachten, wenn Dienstleistungen ausgelagert werden. Dann ist er für jede Outsourcing-Dienstleistung aus Sicht der anwendenden Kommunalverwaltung separat anzuwenden. Die Sicherheitsanforderungen der Basisanforderungen referenzieren auf die Standardanforderungen OPS.2.1.A4 (Vertragsgestaltung), OPS.2.1.A5 (Strategie). Die Beschreibung gibt Beispiele für die Formulierung. Unter anderem sind in der Betrachtung aller Schnittstellen, ein individuelles Rollen- und Berechtigungskonzept in einem IT-Sicherheitskonzept (OPS.2.1.A6) zu berücksichtigen. Es wird auf weitere Anwendungshinweise in Abschnitt 10.2 verwiesen.
Besonderheiten	OPS.2.1.A2 Die rechtzeitige Beteiligung der Personalvertretung ergibt sich unter anderem aus den jeweiligen gesetzlichen Regelungen.
	OPS.2.1.A3 Anforderungen an Outsourcing-Dienstleister sind vor der Auftragsvergabe in einem Anforderungsprofil sorgfältig zu definieren und zu dokumentieren. Dies erhöht auch die Transparenz des Entscheidungsfindungsprozesses.
	OPS.2.1.A4 Die Vertragsgestaltung ist eine Grundvoraussetzung für erfolgreiche Outsourcing-Vorhaben, da dort Leistungsmerkmale, Rollen und Verantwortlichkeiten schriftlich fixiert werden. Dies ist vor allem wichtig, um im Streitfall entsprechende Ansprüche geltend machen zu können. In den Verträgen ist bereits eine geordnete Vertragsbeendigung vorzusehen (siehe OPS.2.1.A15).

Baustein	**OPS.2.1**
	OPS.2.1.A6 Von jedem Outsourcing-Auftragnehmer ist ein Sicherheitskonzept pro Outsourcing-Dienstleistung zu verlangen, auch um die Aufsichts- und Kontrollpflicht des Auftraggebers sicherstellen zu können.
	OPS.2.1.A7 Kommunikationswege und Ansprechpartner müssen klar definiert sein, um sicherzustellen, dass die Vertraulichkeit von Verwaltungsinformationen nicht verletzt wird.
	OPS.2.1.A8 Die jeweiligen Befugnisse des Personals von Dienstleistern müssen auf das Notwendigste beschränkt sein.
	OPS.2.1.A9 Um Möglichkeiten und Auswirkungen von missbräuchlicher Nutzung der Verwaltungsnetze zu minimieren, muss die Anbindung von Outsourcing-Partnern daran im Vorfeld klar geregelt werden.
	OPS.2.1.A10 Um die Vertraulichkeit und die Einhaltung möglicher Fristen sicherzustellen, muss genau vereinbart werden, wie Daten zwischen den Outsourcing-Partnern ausgetauscht werden.
	OPS.2.1.A12 Änderungen müssen rechtzeitig kommuniziert werden, um sicherzustellen, dass alle Abhängigkeiten in der Kommunalverwaltung beachtet und entsprechend vorbereitet werden können.
	OPS.2.1.A15 Die geordnete Beendigung eines Outsourcing-Verhältnisses ist bereits beim Vertragsbeginn (siehe OPS.2.1.A4) zu regeln.

9.1.16 OPS.2.2 - Cloud-Nutzung

Baustein	**OPS.2.2**
Anforderungen	**OPS.2.2.A1 – A4; A6, A8, A9, A13, A14**
Hinweis	Dieser Baustein ist nur anzuwenden, wenn Cloud-Dienste genutzt werden. Der Baustein muss auf jede konkrete Cloud-Dienstleistung angewendet werden. Typischerweise werden Cloud-Dienste über den Web-Browser genutzt. Sofern dies zutrifft ist der Baustein APP 1.2 Webbrowser zu berücksichtigen. Cloud-Nutzung hat ggf. Auswirkungen auf weitere Prozesse oder Systembausteine. Die Auswirkungen sind im Einzelfall zu prüfen und zu berücksichtigen. Es wird auf weitere Anwendungshinweise in Abschnitt 10.2 verwiesen.
Besonderheiten	OPS.2.2.A2 Neben den Sicherheitsvorgaben sind insbesondere die datenschutzrechtlichen Vorgaben zu berücksichtigen und der behördliche Datenschutzbeauftragte ist frühzeitig einzubinden.
	OPS.2.2.A6 Um Möglichkeiten und Auswirkungen von missbräuchlicher Nutzung der Verwaltungsnetze zu minimieren, muss die Anbindung von Cloud-Diensten im Vorfeld geprüft und klar geregelt werden.
	OPS.2.2.A8 Anforderungen an Cloud-Dienstleister sind vor der Auftragsvergabe in einem Anforderungsprofil sorgfältig zu definieren und zu dokumentieren. Dies erhöht auch die Transparenz des Entscheidungsfindungsprozesses.
	OPS.2.2.A9 Die Vertragsgestaltung ist eine Grundvoraussetzung für sichere Cloud-Nutzung, da dort Leistungsmerkmale, Verantwortliche, Art und Ort der Verarbeitung schriftlich fixiert werden. Dies ist vor allem wichtig, um im Streitfall entsprechende Ansprüche geltend machen zu können.

Baustein	**OPS.2.2**
	OPS.2.2.A13 Die unter OPS.2.2.A2 und OPS.2.2.A8 definierten Sicherheitsanforderungen an den Dienst und den Dienstanbieter müssen regelmäßig anhand aktueller Nachweise kontrolliert werden.
	OPS.2.2.A14 Die geordnete Beendigung eines Dienstleistungs-Verhältnisses ist bereits beim Vertragsbeginn zu regeln.

9.1.17 DER.2.1 - Behandlung von Sicherheitsvorfällen

Baustein	**DER.2.1**
Anforderungen	**DER.2.1.A1 – A6**
Besonderheiten	---

9.2 System-Bausteine

Die folgenden System-Bausteine sind auf die verwiesenen Zielobjekte (gemäß Referenzarchitektur) anzuwenden. Wenn nicht anders angegeben, müssen alle Basis-Anforderungen der Bausteine durch Umsetzung der zugehörigen Maßnahmen der Umsetzungshinweise *auf geeignete Weise* erfüllt werden. Zusätzlich zu erfüllende Standard-Anforderungen sind gesondert aufgeführt.

Manche Anforderungen des BSI sind zusätzlich kommentiert, wenn kommunale Besonderheiten bei der Umsetzung zu berücksichtigen sind.

9.2.1 Allgemein

9.2.1.1 SYS.4.5 - Wechseldatenträger

Baustein	**SYS.4.5**
Anforderungen	**SYS.4.5.A1 – A2, A10, A12; A4 – A7**
Hinweis	Die Nutzung von mobilen Datenträgern erfolgt zumeist, um Datentransfers zu vereinfachen. Die damit verbunden möglichen Risiken müssen berücksichtigt werden. Nutzungsgebote müssen klar dokumentiert und den Mitarbeitern kommuniziert werden, da sie ansonsten umgangen oder ignoriert werden. Vor

Baustein	**SYS.4.5**
	allem muss unmissverständlich klar sein, welche mobilen Datenträger genutzt werden dürfen. Es muss klar geregelt werden, wie mit mobilen Datenträgern außerhalb der Kommunalverwaltung umzugehen ist. Außerdem ist sicherzustellen, dass nur zugelassene mobile Datenträger eingesetzt und diese nach Gebrauch in geeigneter Weise gelöscht werden.
Besonderheiten	---

9.2.1.2 NET.1.1 - Netzarchitektur und -design

Baustein	**NET.1.1**
Anforderungen	**NET.1.1.A1 – A15; A21**
Hinweis	Dieser Baustein ist auf das Gesamtnetz einer Verwaltung (inklusive Teilnetze) anzuwenden.
Besonderheiten	NET.1.1.A21 Aufgrund der Art der verarbeiteten Informationen sehen sich Kommunalverwaltungen einem erhöhten Risiko von externen Angriffen ausgesetzt. Um die Anfälligkeit der Netze dafür zu verringern, ist die Managementkommunikation (z. B. die Administration der IT-Systeme) über ein vom normalen Betrieb getrenntes Netz durchzuführen.

9.2.1.3 NET.2.2 - WLAN-Nutzung

Baustein	**NET.2.2**
Anforderungen	**NET.2.2.A1 – A3; A4**
Besonderheiten	NET.2.2.A4 Die Verhaltensregeln bei WLAN-Sicherheitsvorfällen müssen in einer Dienstvereinbarung geregelt sein.

9.2.2 Infrastruktur

9.2.2.1 Verwaltungsgebäude (Objekt G01)

9.2.2.1.1 INF.1 - Allgemeines Gebäude

Baustein	**INF.1**
Anforderungen	**INF.1.A1 – A8; A9**
Besonderheiten	INF.1.A3 Um die unbestimmte Anforderung eines „IT-bezogenen Brandschutzkonzeptes" zu erfüllen, sollten sich Informationssicherheitsbeauftragte, Brandschutzbeauftragte, Haustechnik und Planer über die erforderlichen Maßnahmen abstimmen.
	INF.1.A9 Bei der Planung der Gebäudenutzung ist aufgrund des regen Publikumsverkehrs in Verwaltungsgebäuden darauf zu achten, schützenswerte Räume oder Gebäudeteile nicht in exponierten oder besonders gefährdeten Bereichen unterzubringen.

9.2.2.1.2 INF.12 - Verkabelung

Baustein	**INF.12**
Anforderungen	**INF.12.A1 – A4**
Besonderheiten	Als fachverantwortlich für Verkabelungen sind im Regelfall die Rollen ‚Haustechnik' und ‚Planer' zu sehen. Die Rolle ‚IT-Betrieb' sollte bei den Anforderungen für die IT-Verkabelung mit einbezogen werden.

9.2.2.2 Außenstelle (z. B. Bauhöfe, Kindergärten) (Objekt G02)

9.2.2.2.1 INF.1 - Allgemeines Gebäude

Baustein	**INF.1**
Anforderungen	**INF.1.A1 – A8; A9**
Besonderheiten	INF.1.A3 Um die unbestimmte Anforderung eines „IT-bezogenen Brandschutzkonzeptes" zu erfüllen, sollten sich

Baustein	**INF.1**
	Informationssicherheitsbeauftragte, Brandschutzbeauftragte, Haustechnik und Planer über die erforderlichen Maßnahmen abstimmen.
	INF.1.A9 Bei der Planung der Gebäudenutzung ist aufgrund des regen Publikumsverkehrs in Verwaltungsgebäuden darauf zu achten, schützenswerte Räume oder Gebäudeteile nicht in exponierten oder besonders gefährdeten Bereichen unterzubringen.

9.2.2.2.2 INF.12 - Verkabelung

Baustein	**INF.12**
Anforderungen	**INF.12.A1 – A4**
Besonderheiten	Als fachverantwortlich für Verkabelungen sind im Regelfall die Rollen ‚Haustechnik' und ‚Planer' zu sehen. Die Rolle ‚IT-Betrieb' sollte bei den Anforderungen für die IT-Verkabelung mit einbezogen werden.

9.2.2.3 Büroraum (Objekt R01)

9.2.2.3.1 INF.7 - Büroarbeitsplatz

Baustein	**INF.7**
Anforderungen	**INF.7.A1 – A2; A5 – A7**
Hinweis	Der Baustein ist auf jeden Raum bzw. jede Gruppe von Räumen anzuwenden, in denen sich Mitarbeiter aufhalten, um dort ihre Aufgaben zu erledigen.
Besonderheiten	INF.7.A5 Es ist vor allem relevant, Bildschirme so aufzustellen, dass sie nicht von Unbefugten eingesehen werden können.
	INF.7.A6 Da in Verwaltungen grundsätzlich reger Publikumsverkehr herrscht, müssen Mitarbeiter besonders darauf achten, dass sie vertrauliche Informationen Unbefugten nicht (unfreiwillig) zugänglich machen.

Baustein	**INF.7**
	INF.7.A7 Aufgrund des Publikumsverkehrs in der Kommunalverwaltung müssen vertrauliche Informationen und Datenträger sicher aufbewahrt werden.

9.2.2.4 Bürgerbüro (Arbeitsplatz mit Publikumsverkehr) (Objekt R02)

Ein Bürgerbüro ist im IT-Grundschutz-Kompendium nicht als Baustein beschrieben. Da es sich hierbei im Wesentlichen um Büroarbeitsplätze handelt, wird der entsprechende Baustein als Grundlage für die Modellierung herangezogen. Bürgerbüros zeichnen sich im Gegensatz zu regulären Büroarbeitsplätzen jedoch durch ungehinderte Zutrittsmöglichkeiten aus, weswegen die entsprechenden Maßnahmen aus dem Baustein Besprechungs-, Veranstaltungs-, Schulungsraum ebenfalls berücksichtigt werden.

Hierbei überschneiden sich die Anforderungen INF.7.A2 und INF.10.A3 (beide behandeln „Geschlossene Türen und Fenster"), in der Anwendung reicht die Bearbeitung einer dieser beiden Anforderungen aus.

9.2.2.4.1 INF.7 - Büroarbeitsplatz

Baustein	**INF.7**
Anforderungen	**INF.7.A1 – A2; A6 – A7**
Besonderheiten	INF.7.A6 Da im Bürgerbüro reger Publikumsverkehr herrscht, müssen Mitarbeiter besonders darauf achten, dass sie vertrauliche Informationen Unbefugten nicht (unfreiwillig) zugänglich machen.
	INF.7.A7 Da stets (unbekannte) Besucher im Bürgerbüro zu Gast sind, müssen vertrauliche Informationen und Datenträger sicher aufbewahrt werden.

9.2.2.4.2 INF.10 - Besprechungs-, Veranstaltungs- und Schulungsräume

Baustein	**INF.10**
Anforderungen	**INF.10.A1, A3; A6**
Hinweis	Der Baustein ist auf jeden solchen Raum bzw. jede Gruppe hiervon anzuwenden.

Baustein	**INF.10**
Besonderheiten	INF.10.A6 Da im Bürgerbüro reger Publikumsverkehr herrscht, muss sichergestellt werden, dass Verbindungen ins interne Netz der Kommunalverwaltung nur von dafür vorgesehenen Arbeitsplätzen und nur im notwendigen Maße möglich sind.

9.2.2.5 Besprechungsraum (Objekt R03)

9.2.2.5.1 INF.10 - Besprechungs-, Veranstaltungs- und Schulungsräume

Baustein	**INF.10**
Anforderungen	**INF.10.A1, A3; A6**
Hinweis	Der Baustein ist auf jeden solchen Raum bzw. jede Gruppe hiervon anzuwenden.
Besonderheiten	INF.10.A6 Da in Kommunalverwaltungen Publikumsverkehr herrscht und Externe sich ohne Aufsicht in Besprechungsräumen aufhalten können, muss sichergestellt werden, dass Verbindungen ins interne Netz der Kommunalverwaltung von diesen Räumen aus nur von dafür vorgesehenen Arbeitsplätzen und nur im notwendigen Maße möglich sind, wenn überhaupt.

9.2.2.6 Häuslicher Arbeitsplatz (Objekt R04)

9.2.2.6.1 INF.8 - Häuslicher Arbeitsplatz

Baustein	**INF.8**
Anforderungen	**INF.8.A1 – A3; A5**
Hinweis	Der Baustein ist auf jeden häuslichen Arbeitsplatz bzw. jede Gruppe hiervon einmal anzuwenden.
Besonderheiten	INF.8.A2 Von der in den Umsetzungshilfen geforderten Verschlüsselung der Datenträger kann abgewichen werden, sofern keine schützenswerten Informationen transportiert werden.

Baustein	**INF.8**
	INF.8.A5 Die Entsorgung von vertraulichen Informationen ist genauso wichtig wie das Sichern und der Transport von dienstlichem Arbeitsmaterial. Die Entsorgung muss daher für den häuslichen Arbeitsplatz geregelt sein.

9.2.2.7 Mobiler Arbeitsplatz (Objekt R05)

9.2.2.7.1 INF.9 - Mobiler Arbeitsplatz

Baustein	**INF.9**
Anforderungen	**INF.9.A1 – A4; A5 – A6**
Hinweis	Der Baustein ist immer dann anzuwenden, wenn Mitarbeiter häufig nicht mehr nur innerhalb der Räumlichkeiten der Institution arbeiten, sondern an wechselnden (mobilen) Arbeitsplätzen außerhalb.
Besonderheiten	INF.9.A5 Eine zeitnahe Verlustmeldung ist notwendig, um schnell effektive Gegenmaßnahmen und andere Schritte (z. B. datenschutzrechtliche Informationspflichten) einleiten zu können. Diese könnte und sollte effizient zusammen mit der Basis-Anforderung INF.9.A2 Regelungen für mobile Arbeitsplätze festgelegt werden.
	INF.9.A6 Die korrekte Entsorgung von vertraulichen Informationen ist notwendig, um z. B. datenschutzrechtliche Gefährdungen zu minimieren. Diese könnte und sollte effizient zusammen mit der Basis-Anforderung INF.9.A2 Regelungen für mobile Arbeitsplätze festgelegt werden.

9.2.2.8 Serverraum (Objekt R06)

9.2.2.8.1 INF.2 - Rechenzentrum sowie Serverraum

Baustein	**INF.2**
Anforderungen	**INF.2.A1 – A11, A17, A29**
Hinweis	Als „Rechenzentrum" können bereits IT-Bereiche bezeichnet werden, in denen wenige Server oder IT-Systeme betrieben werden (siehe Definition in der

Baustein	**INF.2**
	Einleitung des Bausteins). Der Baustein ist pro selbst betriebenem Rechenzentrum sowie Serverraum anzuwenden. Wenn die IT extern gehostet wird (z. B. in einem Rechenzentrum eines kommunalen Dienstleisters), ist der jeweilige Dienstleister auf die Umsetzung dieses Bausteins zu verpflichten.
Besonderheiten	INF.2.A8 – A9 Der Einsatz von Brandschutzmaßnahmen sollte mit einem Fachplaner abgestimmt und wenn möglich als Teil eines ganzheitlichen Brandschutzkonzeptes für das Objekt integriert werden.

9.2.2.9 Raum für technische Infrastruktur (Objekt R07)

9.2.2.9.1 INF.5 - Raum sowie Schrank für technische Infrastruktur

Baustein	**INF.5**
Anforderungen	**INF.5.A1 – A7, A9**
Hinweis	Die Anforderungen des Bausteins sind nicht immer auf Schränke übertragbar.
Besonderheiten	INF.5.A3 Von der individuellen Erfassung aller Zutritte zum Raum bzw. Zugriffe bei Schränken, kann im Regelfall abgesehen werden.

9.2.2.10 Archivraum (Objekt R08)

9.2.2.10.1 INF.6 - Datenträgerarchiv

Baustein	**INF.6**
Anforderungen	**INF.6.A1 – A4**
Hinweis	Die Datenträger und Medien können statt in abgeschlossenen Räumlichkeiten nach dem Baustein INF.6 Datenträgerarchiv auch in geeigneten und dem Schutzbedarf entsprechenden Schutzschränken gelagert werden.
Besonderheiten	INF.6.A1 Bei der Umsetzung eines Datenträgerarchivs als Schutzschrank, MUSS am Aufstellort ein geeigneter Handfeuerlöscher leicht erreichbar sein.

Baustein	**INF.6**
	INF.6.A2 Bei der Umsetzung eines Datenträgerarchivs als Schutzschrank, sind entsprechende Zugriffsregelungen und -kontrollen umzusetzen.
	INF.6.A4 Bei der Umsetzung eines Datenträgerarchivs als Schutzschrank, MÜSSEN Fenster und Türen beim Verlassen des Raumes, in dem sich der Schutzschrank befindet, verschlossen werden.

9.2.2.11 Drucker- und Kopierraum (Objekt R09)

Zentral aufgestellte Drucker und Kopierer finden sich im kommunalen Bereich häufig in nicht zutrittsgesicherten Bereichen. Da eine Kommune zudem ihren Bürgern in der Regel einen ungehinderten Zutritt in das Rathaus ermöglicht, ist somit auch der freie Zutritt zu den Druckern und Kopierern möglich. Da die Bausteine des IT-Grundschutz-Kompendiums die beschriebene Situation nur ungenügend abbilden, werden die Maßnahmen des Bausteins Besprechungs-, Veranstaltungs-, Schulungsraum ebenfalls für die Modellierung herangezogen.

9.2.2.11.1 INF.10 - Besprechungs-, Veranstaltungs- und Schulungsräume

Baustein	**INF.10**
Anforderungen	**INF.10.A1, A3; A6 – A7**
Hinweis	Der Baustein ist auf jeden Drucker- und Kopierraum bzw. jede Gruppe hiervon anzuwenden, wenn der Raum öffentlich zugänglich ist.
Besonderheiten	INF.10.A6 – A7 Da Drucker- und Kopierräume nicht ständig besetzt, aber von allen Abteilungen erreichbar sind, ist sicherzustellen, dass sich Unbefugte nicht von dort aus unbemerkt Zugang zum internen Verwaltungsnetz verschaffen können.

9.2.2.12 Dienst-Fahrzeug (Objekt F01)

9.2.2.12.1 INF.11 – Allgemeines Fahrzeug

Baustein	**INF.11**
Anforderungen	**INF.11.A1 – A3; A10**
Hinweis	Dieser Baustein ist nur zu betrachten, wenn Dienstfahrzeuge zur Verfügung gestellt werden.
Besonderheiten	INF.11.A10 Bei der Aussonderung eines Fahrzeugs sind zumindest Regelungen zu treffen, dass keine vertraulichen Informationen in den Fahrzeugen verbleiben.

9.2.3 IT-Systeme

9.2.3.1 Serversystem (Objekt IT01)

9.2.3.1.1 SYS.1.1 - Allgemeiner Server

Baustein	**SYS.1.1**
Anforderungen	**SYS.1.1.A1, A2, A5, A6, A9, A10; A15, A21, A25**
Hinweis	Der Baustein ist auf jeden Server anzuwenden.
Besonderheiten	SYS.1.1.A15 Der Einsatz einer USV erhöht die Verfügbarkeit und sei es nur um ein geregeltes Herunterfahren der Server zu ermöglichen.
	SYS.1.1.A21 Nicht dokumentierte Änderungen erschweren z. B. das Beheben von Fehlern. Daher ist im ersten Schritt alles zu dokumentieren, was automatisiert dokumentiert werden kann.
	SYS.1.1.A25 Bei der Außerbetriebnahme eines Servers sind zumindest Regelungen zum sicheren Löschen sensitiver Daten erforderlich. Andernfalls besteht die Gefahr, dass die Daten von Unbefugten ausgelesen werden können.

9.2.3.2 Terminal-Server (Objekt IT02)

9.2.3.2.1 SYS.1.1 - Allgemeiner Server

Baustein	**SYS.1.1**
Anforderungen	**SYS.1.1.A1, A2, A5, A6, A9, A10; A15, A21, A25**
Hinweis	Der Baustein ist auf jeden Server anzuwenden.
Besonderheiten	SYS.1.1.A15 Der Einsatz einer USV erhöht die Verfügbarkeit und sei es nur um ein geregeltes Herunterfahren der Server zu ermöglichen.
	SYS.1.1.A21 Nicht dokumentierte Änderungen erschweren z. B. das Beheben von Fehlern. Daher ist im ersten Schritt alles zu dokumentieren, was automatisiert dokumentiert werden kann.
	SYS.1.1.A25 Bei der Außerbetriebnahme eines Servers sind zumindest Regelungen zum sicheren Löschen sensitiver Daten erforderlich. Andernfalls besteht die Gefahr, dass die Daten von Unbefugten ausgelesen werden können.

9.2.3.2.2 SYS.1.x - Terminal-Server

[Die Veröffentlichung des Bausteins SYS.1.x Terminal-Server ist vom BSI geplant. Der Baustein wird in das Profil integriert, sobald er verfügbar ist.]

9.2.3.3 Virtualisierungshost (Objekt IT03)

9.2.3.3.1 SYS.1.1 - Allgemeiner Server

Baustein	**SYS.1.1**
Anforderungen	**SYS.1.1.A1, A2, A5, A6, A9, A10; A15, A21, A25**
Hinweis	Der Baustein ist auf jeden Server anzuwenden.
Besonderheiten	SYS.1.1.A15 Der Einsatz einer USV erhöht die Verfügbarkeit und sei es nur um ein geregeltes Herunterfahren der Server zu ermöglichen.

Baustein	**SYS.1.1**
	SYS.1.1.A21 Nicht dokumentierte Änderungen erschweren z. B. das Beheben von Fehlern. Daher ist im ersten Schritt alles zu dokumentieren, was automatisiert dokumentiert werden kann.
	SYS.1.1.A25 Bei der Außerbetriebnahme eines Servers sind zumindest Regelungen zum sicheren Löschen sensitiver Daten erforderlich. Andernfalls besteht die Gefahr, dass die Daten von Unbefugten ausgelesen werden können.

9.2.3.3.2 SYS.1.5 - Virtualisierung

Baustein	**SYS.1.5**
Anforderungen	**SYS.1.5.A2 – A5, A7; A12**
Hinweis	Der Baustein ist auf jeden Virtualisierungshost bzw. auf jede Gruppe hiervon anzuwenden.
Besonderheiten	SYS.1.5.A12 Es sollten stets nur diejenigen Zugriffsrechte vergeben werden, die für die aktuelle Aufgabe benötigt werden. Dies gilt umso mehr für Administratoren, da ihre (versehentlichen) Fehler höhere Auswirkungen haben als von anderen Nutzern.

9.2.3.4 Netzwerk-Drucker / Multifunktionsgerät (Objekt IT04)

9.2.3.4.1 SYS.4.1 - Drucker, Kopierer und Multifunktionsgeräte

Baustein	**SYS.4.1**
Anforderungen	**SYS.4.1.A1, A2, A22; A4, A7, A11, A18; A14**
Hinweis	Der Baustein ist für jeden Drucker, Kopierer oder Multifunktionsgerät im Informationsverbund bzw. für jede Gruppe hiervon anzuwenden. Zentral aufgestellte Drucker und Kopierer finden sich im kommunalen Bereich häufig in nicht zutrittsgesicherten Bereichen. Da eine Kommune zudem ihren Bürgern in der Regel einen ungehinderten Zutritt in das Rathaus ermöglicht, ist somit auch der freie Zutritt zu den Druckern und Kopierern möglich.

Baustein	**SYS.4.1**
	Nur wenn das Gerät in einem überwachten Bereich, z. B in einem Büroraum, aufgestellt ist, können Anforderungen zur Erhöhung der Zugangs- und Zugriffskontrolle zurückgestellt werden.
Besonderheiten	SYS.4.1.A7 Der Zugriff auf die Konfiguration von Druckern, Kopierern und Multifunktionsgeräten muss beschränkt werden. Wenn Administratoren die Geräte mittels Fernzugriff konfigurieren, muss eine Authentisierung erfolgen.
	SYS.4.1.A14 und SYS.4.1.A18 Die Anforderungen sind umzusetzen, wenn die Geräte in öffentlichen Räumen genutzt werden oder die Nutzung nicht unter ständiger Aufsicht erfolgt.
	Bei der Aussonderung von Drucker, Kopierer und Multifunktionsgerät ist CON.6.A2 zu beachten.

9.2.3.5 Arbeitsplatz-PC (Objekt IT05)

9.2.3.5.1 SYS.2.1 - Allgemeiner Client

Baustein	**SYS.2.1**
Anforderungen	**SYS.2.1.A1, A3, A6, A8, A42; A14, A24, A27; A28**
Hinweis	Der Baustein ist auf jeden Client anzuwenden.
Besonderheiten	SYS.2.1.A3 Es sollte sichergestellt werden, dass Administratoren vorab festlegen, welche automatischen Updatefunktionen zugelassen werden.
	SYS.2.1.A8 Clients sind durch ein BIOS-Passwort vor Veränderungen an der Systemkonfiguration und zum Schutz des Bootvorgangs zu schützen.
	SYS.2.1.A27 Datenträger sind vor der Entsorgung so zu zerstören, dass eine Wiederherstellung der enthaltenen Daten grundsätzlich ausgeschlossen ist.

9.2.3.6 Smartphones und Tablets (inkl. „BYOD" von Ratsmitgliedern) (Objekt IT06)

9.2.3.6.1 SYS.3.2.1 - Allgemeine Smartphones und Tablets

Baustein	**SYS.3.2.1**
Anforderungen	**SYS.3.2.1.A1 – A8**
Hinweis	Der Baustein ist immer dann anzuwenden, wenn in der Verwaltung mobile Endgeräte, die auf mobilen Betriebssystemen wie z. B. Android oder iOS basieren, dienstlich eingesetzt werden. Die Erstellung eines Sicherheitskonzeptes wird empfohlen. Dieses Konzept sollte die Anforderungen A9 – A11, A16 berücksichtigen.
Besonderheiten	---

9.2.3.6.2 SYS.3.3 - Mobiltelefon

Baustein	**SYS.3.3**
Anforderungen	**SYS.3.3.A1-A4**
Hinweis	Der Baustein ist mit dem Baustein SYS.3.2.1 Allgemeine Smartphones und Tablets nur für relevante Anforderungen der Mobilfunkfunktionen zu berücksichtigen.
Besonderheiten	---

9.2.3.7 Mobiler Arbeitsplatz-Rechner (Objekt IT07)

9.2.3.7.1 SYS.2.1 - Allgemeiner Client

Baustein	**SYS.2.1**
Anforderungen	**SYS.2.1.A1, A3, A6, A8, A42; A14, A24, A27; A28**
Hinweis	Der Baustein ist auf jeden Client anzuwenden.
Besonderheiten	SYS.2.1.A3 Es sollte sichergestellt werden, dass Administratoren vorab festlegen, welche automatischen Updatefunktionen zugelassen werden.

Baustein	**SYS.2.1**
	SYS.2.1.A8 Clients sind durch ein BIOS-Passwort vor Veränderungen an der Systemkonfiguration und zum Schutz des Bootvorgangs zu schützen.
	SYS.2.1.A27 Es ist vor der Entsorgung sicherzustellen, dass eine Wiederherstellung der auf den Clients einmal vorhandenen Daten grundsätzlich ausgeschlossen ist.

9.2.3.7.2 SYS.3.1 - Laptop

Baustein	**SYS.3.1**
Anforderungen	**SYS.3.1.A1, A3, A9; A6, A8, A10, A12, A13**
Hinweis	Der Baustein ist auf alle Laptops oder Notebooks anzuwenden, die mobil oder stationär genutzt werden.
Besonderheiten	SYS.3.1.A6 Sicherheitsregelungen sind klar zu dokumentieren, damit in der gesamten Kommunalverwaltung ein einheitliches Sicherheitsniveau eingehalten wird.
	SYS.3.1.A8 Ein einzelner mit Schadprogrammen infizierter Rechner kann das gesamte interne Netz der Kommunalverwaltung gefährden. Um diese Infektionsgefahr möglichst zu reduzieren, ist die Nutzung von fremden Datennetzen mit verwaltungseigenen Geräten klar zu definieren.
	SYS.3.1.A9 Um die Gefahr unbefugter Zugriffe auf das interne Netz der Kommunalverwaltung zu minimieren, ist klar zu definieren, wie von außen darauf zugegriffen werden darf.
	SYS.3.1.A10 Um sicherzustellen, dass Verwaltungsdaten auf Laptops nicht „verloren" gehen können, muss geregelt werden, wie die Datenbestände von Laptops mit denen der Kommunalverwaltung synchronisiert werden.

Baustein	**SYS.3.1**
	SYS.3.1.A12 Eine zeitnahe Verlustmeldung ist notwendig, um schnell effektive Gegenmaßnahmen und andere Schritte (z. B. datenschutzrechtliche Informationspflichten) einleiten zu können. Dafür müssen entsprechende Meldewege etabliert werden.
	SYS.3.1.A13 Laptops sind stets zu verschlüsseln, um die Auswirkungen eines Verlustes zu minimieren.

9.2.4 Anwendungen

9.2.4.1 Internet-Nutzung (Objekt A01)

9.2.4.1.1 APP.6 - Allgemeine Software

Baustein	**APP.6**
Anforderungen	**APP.6.A1 – A5**
Hinweis	Der Baustein ist grundsätzlich für jede Software, die im Informationsverbund eingesetzt wird, anzuwenden.
Besonderheiten	---

9.2.4.1.2 APP.1.2 - Web-Browser

Baustein	**APP.1.2**
Anforderungen	**APP.1.2.A1 – A3, A6, A13; A12**
Hinweis	Der Baustein ist auf jeden eingesetzten Web-Browser anzuwenden.
Besonderheiten	APP.1.2.A12 Durch Schwachstellen im Bereich der Browser kann es notwendig sein für bestimmte Zeiten Browser zu deaktivieren. Jede Kommune sollte daher prüfen, ob eine Zwei-Browser-Strategie anzuwenden ist.

9.2.4.2 Benutzer-Authentifizierung (A02)

9.2.4.2.1 APP.6 – Allgemeine Software

Baustein	**APP.6**
Anforderungen	**APP.6.A1 – A5**
Hinweis	Der Baustein ist grundsätzlich für jede Software, die im Informationsverbund eingesetzt wird, anzuwenden.
Besonderheiten	---

9.2.4.2.2 APP.2.1 - Allgemeiner Verzeichnisdienst

Baustein	**APP.2.1**
Anforderungen	**APP.2.1.A1 – A6**
Hinweis	Der Baustein sollte, unabhängig vom gewählten Produkt, auf jeden Verzeichnisdienst einmal angewandt werden.
Besonderheiten	Aufgrund der hohen Kritikalität des Verzeichnisdienstes, muss zeitnah die Anhebung des Sicherheitsniveaus auf die Standard-Absicherung geplant werden. Wenn die Standard-Anforderungen nicht zeitnah umgesetzt werden können, sollte der eigenverantwortliche Betrieb eines Verzeichnisdienstes geprüft werden.

9.2.4.3 Dateiablage (Objekt A03)

9.2.4.3.1 APP.3.3 - Fileserver

Baustein	**APP.3.3**
Anforderungen	**APP.3.3.A2, A3, A15; A8**
Hinweis	Der Baustein ist auf jeden Fileserver anzuwenden. In der Vergangenheit wurden Fileserver oft realisiert, indem Speichermedien direkt an einen Server angeschlossen wurden. Diese sogenannten Direct-Attached-Storage-(DAS)-Systeme können die aktuellen und zukünftigen Anforderungen jedoch oft nicht mehr erfüllen. Sollten das Konzept der Speicherlösungen angewendet werden sind ergänzend die Basis-

Baustein	**APP.3.3**
	Anforderungen SYS 1.8 Speicherlösungen und die Anforderungen A6 und A 7 anzuwenden.
Besonderheiten	APP.3.3.A8 Die strukturierte Datenhaltung ist eine grundlegende Voraussetzung für die Erstellung eines geeigneten Datensicherungskonzepts.

9.2.4.4 Bürokommunikation (Groupware und E-Mail) (Objekt A04)

9.2.4.4.1 APP.6 – Allgemeine Software

Baustein	**APP.6**
Anforderungen	**APP.6.A1 – A5**
Hinweis	Der Baustein ist grundsätzlich für jede Software, die im Informationsverbund eingesetzt wird, anzuwenden.
Besonderheiten	---

9.2.4.4.2 APP.5.3 - Allgemeiner E-Mail-Client und -Server

Baustein	**APP.5.3**
Anforderungen	**APP.5.3.A1 – A4; A5**
Hinweis	Der Baustein ist auf jeden E-Mail-Client und jeden E-Mail Server anzuwenden.
Besonderheiten	APP.5.3.A5 Bei der Weiterleitung von E-Mails müssen datenschutzrechtliche Aspekte berücksichtigt werden.

9.2.4.5 Office-Produkte (Objekt A05)

9.2.4.5.1 APP.6 – Allgemeine Software

Baustein	**APP.6**
Anforderungen	**APP.6.A1 – A5**
Hinweis	Der Baustein ist grundsätzlich für jede Software, die im Informationsverbund eingesetzt wird, anzuwenden.
Besonderheiten	---

9.2.4.5.2 APP.1.1 - Office-Produkte

Baustein	**APP.1.1**
Anforderungen	**APP.1.1.A2, A3, A17; A12, A13 und zusätzliche Anforderung**
Besonderheiten	APP.1.1.A3 Damit sicherheitsrelevante Einstellungen und Vorkommnisse nicht umgangen oder ignoriert werden, müssen Benutzer durch organisatorische Regelungen sensibilisiert und zur Beachtung von Sicherheitsanforderungen belehrt werden, insbesondere wenn eine technische Maßnahme zur Überprüfung von Dokumenten aus externen Quellen nicht möglich ist.
	APP.1.1.A12 Um einen unkontrollierten Datenabfluss als auch eine Kompromittierung der eigenen Infrastruktur zu verhindern, sollten die in einigen Office-Produkten integrierten Cloud-Speicher-Funktionen grundsätzlich deaktiviert werden. Dies betrifft auch den Zugriff auf Cloud-Laufwerke.
	APP.1.1.A13 Kommunalverwaltungen erhalten eine Vielzahl von Nachrichten aus unbekannten und potentiell unsicheren Quellen. Um eine Kompromittierung der IT-Infrastruktur zu verhindern, sollten solche Daten standardmäßig in einem geschützten Modus geöffnet werden.
	Zusätzliche Anforderung: Beschaffung kommunaler Anwendungen mit Schnittstellen zu Office-Produkten. Bei der Ausschreibung und Vergabe von Anwendungen zur Unterstützung der kommunalen Aufgabenerfüllung sollte für den Fall der Interaktion oder Integration mit Office-Produkten der Anforderungskatalog mitgeteilt werden. Die Auftragnehmer sollten darauf hingewiesen werden, welche Sicherheitsmechanismen zu beachten sind.

9.2.5 Netze

9.2.5.1 Server- und Administrationsnetz (Objekt N01)

9.2.5.1.1 NET.1.2 - Netzmanagement

Baustein	**NET.1.2**
Anforderungen	**NET.1.2.A1 – A2, A6 – A10; A18**
Besonderheiten	NET.1.2.A18 Um Bedienfehler zu vermeiden, müssen Mitarbeiter für die Nutzung der eingesetzten Netzmanagement-Lösungen geschult werden.

9.2.5.2 Demilitarisierte Zone (DMZ) (N02)

9.2.5.2.1 NET.1.2 - Netzmanagement

Baustein	**NET.1.2**
Anforderungen	**NET.1.2.A1 – A2, A6 – A10; A18**
Besonderheiten	NET.1.2.A18 Um Bedienfehler zu vermeiden, müssen Mitarbeiter für die Nutzung der eingesetzten Netzmanagement-Lösungen geschult werden.

9.2.5.3 Netzwerk für reguläre Arbeitsplätze (N03)

9.2.5.3.1 NET.1.2 - Netzmanagement

Baustein	**NET.1.2**
Anforderungen	**NET.1.2.A1 – A2, A6 – A10; A18**
Besonderheiten	NET.1.2.A18 Um Bedienfehler zu vermeiden, müssen Mitarbeiter für die Nutzung der eingesetzten Netzmanagement-Lösungen geschult werden.

9.2.5.4 WLAN (intern / ggf. öffentlich) (N04)

9.2.5.4.1 NET.2.1 - WLAN-Betrieb

Baustein	**NET.2.1**
Anforderungen	**NET.2.1.A1 – A8; A13**

Baustein	**NET.2.1**
Hinweis	Der Baustein ist auf alle Kommunikationsnetze anzuwenden, die gemäß der Standardreihe 802.11 und deren Erweiterungen aufgebaut und betrieben werden.
Besonderheiten	NET.2.1.A13 Um der fortlaufenden technischen Entwicklung gerecht zu werden, müssen Prüfungen auf Sicherheitslücken regelmäßig erfolgen. Hierzu kann es genügen, sich auf den Webseiten des Herstellers und einschlägiger Sicherheitsforen zu informieren, ob Lücken bekannt und ggf. Sicherheitspatches verfügbar sind.

9.2.5.5 Gebäudeübergreifende Vernetzung (N05)

9.2.5.5.1 NET.3.3 - VPN

Baustein	**NET.3.3**
Anforderungen	**NET.3.3.A1 – A5; A7, A11**
Hinweis	Der Baustein ist für jede Art von Fernzugriffen einmal anzuwenden.
Besonderheiten	NET.3.3.A2 Die Nutzung von VPN-Dienstleistern muss auf einer soliden vertraglichen Grundlage beruhen, vor allem um sicherzustellen, dass zugesicherte Leistungen auch eingehalten werden.
	NET.3.3.A7 Ohne die sorgfältige Planung des VPN-Einsatzes besteht die Gefahr, dass sicherheitsrelevante Probleme erst im Laufe der Realisierung auftreten, die von Angreifern sofort ausgenutzt werden könnten.
	NET.3.3.A11 Wenn für die Anbindung von externen Netzen nicht sichere Verschlüsselungsverfahren ausgewählt werden bzw. eine nicht ausreichende Schlüssellänge verwendet wird, besteht die Gefahr, dass sich unbefugte Dritte Zugang verschaffen.

9.2.5.6 Internet-Zugang für die Verwaltung (N06)

Für dieses Netz sind die allgemeinen Anforderungen unter 9.2.1.2 NET.1.1 - Netzarchitektur und -design zu beachten. Soweit zutreffend, sind die darin enthaltenen Verweise auf weitere Bausteine mit den Basis-Anforderungen ebenfalls zu beachten. Beim Stand der Erstellung dieser Version des Profils hat das BSI keinen Baustein für die Internetanbindung geplant.

9.2.5.7 Autonome Internet-Zugänge (z. B. einer Außenstelle) (N07)

Für dieses Netz sind die allgemeinen Anforderungen unter 9.2.1.2 NET.1.1 - Netzarchitektur und -design zu beachten. Soweit zutreffend, sind die darin enthaltenen Verweise auf weitere Bausteine mit den Basis-Anforderungen ebenfalls zu beachten. Beim Stand der Erstellung dieser Version des Profils hat das BSI keinen Baustein für die Internetanbindung geplant.

9.2.5.8 Firewall (Objekt N08)

9.2.5.8.1 NET.3.2 - Firewall

Baustein	**NET.3.2**
Anforderungen	**NET.3.2.A1 – A4, A6 – A10, A14 – A15; A17 – A18, A20, A22**
Hinweis	Der Baustein ist immer anzuwenden, wenn unterschiedlich vertrauenswürdige Netze gekoppelt werden.
Besonderheiten	NET.3.2.A1 Es ist notwendig, die Verantwortlichkeiten für Firewalls und essentielle Vorgaben zu dokumentieren. Dies kann in einer eigenen Richtlinie oder als Teil einer allgemeinen IT-Richtlinie geschehen.
	NET.3.2.A15 Die Anforderungen an eine Firewall sind zu dokumentieren. Dies kann bereits in der Richtlinie geschehen (siehe NET.3.2.A1).
	NET.3.2.A17 Bestimmte Firewall-Regeln, die z. B. unter IPv4 festgelegt wurden, können unter IPv6 nicht gültig sein und somit zur Folge haben, dass bestimmte Dienste ungewollt wieder frei zugänglich sind. Um zu verhindern, dass solche Sicherheitslücken von Angreifern ausgenutzt werden, sollte das jeweils nicht benötigte Protokoll deaktiviert werden.

Baustein	**NET.3.2**
	NET.3.2.A18 Werden Zugriffe auf die Managementkonsole der Firewall aus einem anderen als dem Managementnetz zugelassen, besteht die Gefahr, dass Angreifer die Kontrolle über die Firewall übernehmen und erheblichen Schaden anrichten können.
	NET.3.2.A20 Durch die Einrichtung von Sicherheitsproxys können unerwünschte Befehle von potentiellen Angreifern herausgefiltert und so deren Ausführung verhindert werden.

9.2.5.9 Router / Switche (Objekt N09)

9.2.5.9.1 NET.3.1 - Router und Switches

Baustein	**NET.3.1**
Anforderungen	**NET.3.1.A1, A4 – A9**
Hinweis	Der Baustein ist für jedes aktive Netz und alle darin verwendeten Router/Switches anzuwenden.
Besonderheiten	---

9.2.5.10 TK-Anlage (inkl. Fax) (Objekt N10)

9.2.5.10.1 NET.4.1 – TK-Anlagen

Baustein	**NET.4.1**
Anforderungen	**NET.4.1.A1 – A2, A5; A7, A8, A10, A12, A15 – A17; A18**
Hinweis	Der Baustein ist für jede TK-Anlage anzuwenden.
Besonderheiten	NET.4.1.A18 Die TK-Anlage kann ggfls. in einem gesicherten Serverraum untergebracht werden.

9.2.5.10.2 NET.4.3 – Faxgeräte und Faxserver

Baustein	**NET.4.3**
Anforderungen	**NET.4.3.A1 – A3; A8**
Hinweis	Der Baustein ist für jedes Faxgerät oder Faxserver anzuwenden.
Besonderheiten	---

9.2.5.11 VoIP (Voice-over-IP) (Objekt N11)

9.2.5.11.1 NET.4.2 - VoIP

Baustein	**NET.4.2**
Anforderungen	**NET.4.2.A1, A3 – A5; A8, A11, A13, A16**
Hinweis	Dieser Baustein ist nur dann anzuwenden, wenn die TK-Anlage per VoIP kommuniziert. Werden TK-Anlagen über ein Datennetz verwendet, ist der Baustein NET.4.1 TK-Anlage ebenfalls anzuwenden.
Besonderheiten	NET.4.2.A4 Sofern eine Fremdwartung als Fernwartung erfolgt, ist der Baustein OPS.1.2.5 Fernwartung zu beachten. Findet die Wartung vor Ort statt ist die Anforderung ORP1.A3 Beaufsichtigung oder Begleitung von Fremdpersonal zu beachten.
	NET.4.2.A5 Standard-Passwörter der IT-Systeme sind zu ändern. Die Benutzer müssen technisch oder organisatorisch dazu aufgefordert werden, ihre Start-Passwörter oder -PIN für den persönlichen Zugang zu ihren Einstellungen der Servicedienste der VoIP-Middleware, zu ändern (siehe auch NET.4.2.A11 Sicherer Umgang mit VoIP-Endgeräten). Nicht benötigte Dienste und Leistungsmerkmale sind zu deaktivieren.
	NET.4.2.A8 Sofern eine Verschlüsselung erfolgen soll, sind die Anforderungen NET.4.2.A14 Verschlüsselung der Signalisierung und NET.4.2.A15 Sicherer Medientransport mit SRTP ebenfalls umzusetzen.

Baustein	NET.4.2
	NET.4.2.A11 Sofern es technisch nicht erzwungen wird, müssen die Benutzer darüber informiert werden, dass sie ihr Start-Passwort oder -PIN für den persönlichen Zugang zu ihren Einstellungen der Servicedienste der VoIP-Middleware unbedingt ändern sollten.
	NET.4.2.A16 Das VoIP-Netz ist vom Datennetz zu trennen, dabei sind die Basis-Anforderungen des Bausteins NET.1.1 Netzarchitektur und -design zu beachten.

10 ANWENDUNGSHINWEISE

10.1 Umsetzung offene Punkte

Die in Kapitel 9 definierten Anforderungen sind im Zuge der Realisierungsplanung möglichst schnell umzusetzen. Nachdem dies erfolgt ist, sollte zeitnah entschieden werden, wann mit dem notwendigen, sich anschließenden Verbesserungsprozess begonnen wird.

10.2 Outsourcing und Cloud-Nutzung

Outsourcing- und Cloud-Dienstleister sind zu verpflichten, mindestens die dem tatsächlichen Schutzbedarf entsprechenden Anforderungen des IT-Grundschutzes angemessen zu erfüllen. Der zu erfüllende Schutzbedarf kann nicht weniger als „normal" gemäß IT-Grundschutz sein. Das bedeutet, dass Dienstleister höhere Anforderungen zu erfüllen haben, als in diesem Profil formuliert sind. Dies ist bei der Beschaffung zu berücksichtigen und vertraglich zu regeln.

Für jedes Outsourcing Vorhaben ist ein Sicherheitskonzept pro Outsourcing-Dienstleistung zu erstellen.

Abgrenzung Outsourcing und Cloud-Nutzung: Die Nutzung von Cloud-Diensten ist im Wesentlichen ein Teilbereich des IT-Outsourcing. Beim Outsourcing werden komplette Arbeitsprozesse ganz oder teilweise ausgelagert. Beim Cloud-Computing werden skalierbare und anpassungsfähige Applikationen zur Verfügung gestellt. Typisch für Cloud-Computing ist unter anderem, dass mehrere Kunden eine gemeinsame Infrastruktur nutzen.

Dies können Zusammenarbeitsplattformen, Video-Konferenz-Systeme, Cloud-Speicher oder Extranet-Dienstleistungen sein.

Rechtliche Anforderungen, insbesondere datenschutzrechtliche Anforderungen, sind bei Cloud-Diensten besonders zu berücksichtigen.

Die Bausteine OPS.2.1 und OPS.2.2 haben Überschneidungen, sind aber nicht gemeinsam anzuwenden. Das heißt, bei der Nutzung von Cloud-Diensten ist der Baustein OPS.2.1 nicht anzuwenden.

10.3 Neue Projekte

Dieses Profil ist für die Absicherung bereits existierender Objekte verfasst. Neuanschaffungen sind gemäß dem „Stand der Technik" abzusichern, da ansonsten die getätigten Investitionen nicht ausreichend abgesichert werden.

11 RISIKOBEHANDLUNG

Mit der Umsetzung der ausgewählten Sicherheitsanforderungen werden die Risiken elementarer Gefährdungen für eine Basis-Absicherung des hier festgelegten Informationsverbundes angemessen minimiert.

Soweit Basis-Anforderungen bzw. die dazugehörigen Maßnahmen des IT-Grundschutz-Kompendiums nicht die elementaren Gefährdungen einer Kommunalverwaltung abdecken, sind die abweichenden Anforderungen in den Bausteinen im Kapitel 8 *Anforderungen* dokumentiert.

Dieses Profil verfolgt das Ziel, eine breite, grundlegende systematische Erst-Absicherung über alle Geschäftsprozesse bzw. Fachverfahren einer Kommunalverwaltung vorzunehmen. Dafür sind die Anforderungen berücksichtigt worden, die dazu dienen, grundlegende Sicherheitsmaßnahmen umzusetzen und Benutzer dafür zu sensibilisieren. Restrisiken, wie versehentliche oder vorsätzliche Missachtung dieser grundlegenden Absicherungen, egal ob durch Innen- oder Außentäter, verbleiben also auch nach der Umsetzung dieses Profils.

Im Anschluss an die Umsetzung dieses Profils ist das Sicherheitsniveau weiter zu erhöhen, um verbleibende Risiken auf ein akzeptables Maß zu reduzieren. Verantwortlich für die Akzeptanz der verbleibenden Risiken ist die Behördenleitung.

12 UNTERSTÜTZENDE INFORMATIONEN

Detailliertere Informationen zu den einzelnen Anforderungen finden sich in den Umsetzungshinweisen der einzelnen Bausteine des IT-Grundschutz-Kompendiums ([BSI-IT-GSK] und [BSI-IT-GS-UH]).

13 ANMERKUNGEN ZUM PROFIL

Die kommunale Arbeitsgruppe „Modernisierung des IT-Grundschutzes" hat sich mit der Fortschreibung dieses Profils in „Arbeitsgruppe kommunale Basis-Absicherung (AG koBa)" umbenannt. Anmerkungen, Rückfragen und Kritik zum IT-Grundschutz-Profil können jederzeit unter folgender E-Mail-Adresse an die AG koBa gerichtet werden: ag-koba@it-sibe-forum.de

Verbesserungsvorschläge werden gesammelt und im Zuge der regelmäßigen Aktualisierung des Profils integriert. Die neuen Versionen werden sukzessive zur Verfügung gestellt.

Zum Erfahrungsaustausch, zur Diskussion oder dem Teilen von Erlebnisberichten ist die Nutzung des „Internetforums für IT-Sicherheitsbeauftragte der Kommunen und der Länder" (IT-SiBe-Forum) empfohlen. Dort ist auch die AG koBa vertreten. Informationen zum IT-SiBe-Forum sind unter folgender URL zu finden: https://info.it-sibe-forum.de

14 ANHANG

14.1 Abkürzungen

Abkürzung	Erläuterung
AG koBa	Arbeitsgruppe kommunale Basis-Absicherung
BSI	Bundesamt für Sicherheit in der Informationstechnik
ISLL	Informationssicherheitsleitlinie
TOM	Technisch-Organisatorische Maßnahme

Tabelle 2: Abkürzungsverzeichnis

14.2 Referenzen

[BSI-200-1] BSI-Standard 200-1 - Managementsysteme für Informationssicherheit (ISMS); v1.0; 15.11.2017; Bundesamt für Sicherheit in der Informationstechnik; (https://www.bsi.bund.de)

[BSI-200-2] BSI-Standard 200-2 - IT-Grundschutz-Methodik; v1.0; 15.11.2017; Bundesamt für Sicherheit in der Informationstechnik; (https://www.bsi.bund.de)

[BSI-IT-GSK] IT-Grundschutz-Kompendium; Edition 2022; Bundesamt für Sicherheit in der Informationstechnik; (https://www.bsi.bund.de)

[BSI-IT-GS-UH] Umsetzungshinweise zum IT-Grundschutz-Kompendium; Bundesamt für Sicherheit in der Informationstechnik; (https://www.bsi.bund.de)

[CC] Creative Commons Lizenz; (CC-BY-SA 3.0); http://creativecommons.org/licenses/by-sa/3.0/de/

[HR-ISLL-KV] Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen; Februar 2017; Deutscher Städtetag, Deutscher Landkreistag, Deutscher Städte- und Gemeindebund, VITAKO; (http://info.it-sibe-forum.de/)