IT-GRUNDSCHUTZ-PROFIL

BASIS-ABSICHERUNG KOMMUNALVERWALTUNG

15.10.2019

ARBEITSGRUPPE „MODERNISIERUNG IT-GRUNDSCHUTZ" 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-GS-Kompendium 2019	AG

INHALTSVERZEICHNIS

TABELLENVERZEICHNIS

1 FORMALIEN

Titel	IT-Grundschutz-Profil – Basis-Absicherung Kommunalverwaltung
Autor	Arbeitsgruppe „Modernisierung IT-Grundschutz“
Lizenz	CC-BY-SA 3.0
Version	2.0 (2019)
Status	freigegeben
Revisionszyklus	spätestens alle 3 Jahre
Vertraulichkeit	öffentlich

Tabelle 1: Formalien

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

Dieses Werk ist unter einer Creative Commons Lizenz vom Typ Namensnennung - Weitergabe unter gleichen Bedingungen 3.0 Deutschland (CC-BY-SA 3.0) zugänglich. Um eine Kopie dieser Lizenz einzusehen, konsultieren Sie http://creativecommons.org/licenses/by-sa/3.0/de/ oder wenden Sie sich brieflich an Creative Commons, Postfach 1866, Mountain View, California 94042, USA.

4 AUTORENLISTE

4.1 Version 1.0 (2018)

An der Erarbeitung dieses Profils waren im Rahmen der Arbeitsgruppe „Modernisierung IT-Grundschutz“ die nachfolgend in alphabetischer Reihenfolge aufgelisteten Personen beteiligt:

Markus Albert, Stadt Frankfurt am Main
Thorsten Breer, Städtische Datenverarbeitung Wilhelmshaven
Dr. Lutz Gollan, Behörde für Inneres und Sport Hamburg
Daniel Grimm, VITAKO
Margot Heimfarth, SECURiON Rheinland-Pfalz GmbH
Matthias Hög, Senatsverwaltung für Inneres und Sport Berlin
Gregor Hurtig, Zweckverband Elektronische Verwaltung in Mecklenburg-Vorpommern (eGo-MV)
Christine Jentzsch, Stadt Hennigsdorf
Christopher Johansson, Rhein-Sieg-Kreis
Micha Mark Knierim, Kreis Rendsburg-Eckernförde
Axel Kohl, Landratsamt Konstanz
Nils Körner, Zweckverband Kommunale Datenverarbeitung Oldenburg
David Kottke, Zweckverband Elektronische Verwaltung in Mecklenburg-Vorpommern (eGo-MV)
Norman Kramm, Landeshauptstadt Mainz
Pierre Kustos, Zweckverband Elektronische Verwaltung in Mecklenburg-Vorpommern (eGo-MV)
Jens Lange, Stadt Kassel
Gert Lefèvre, Kreis Bergstraße
Susanne Lenz, Landeshauptstadt München
Ralf Lion, Landeshauptstadt Saarbrücken
Oliver Maas, KomFIT e. V.
Kai Müller, Ministerium des Innern und für Sport Rheinland-Pfalz
Stefan Piotrowski, Landratsamt Schwarzwald-Baar-Kreis
Maik Poburski, Landkreis Osnabrück
Heino Reinartz, Städteregion Aachen
Heino Sauerbrey, Deutscher Landkreistag
Kim Schoen, ITEBO GmbH
Marcus Schröder, SECURiON Rheinland-Pfalz GmbH
Thomas Stasch, civitec
Andreas von Hörde, GEOZENTRUM Hannover
Frank Weidemann, KomFIT e. V.
Stefan Wojciechowski, Landkreis Oberhavel

4.2 Version 2.0 (2019)

An der Überarbeitung des Profils für die Version 2.0, welches das IT-Grundschutz-Kompendium Edition 2019 berücksichtigt, waren die nachfolgend in alphabetischer Reihenfolge aufgelisteten Personen beteiligt:

Markus Albert, Stadt Frankfurt am Main
Margot Heimfarth, SECURiON Rheinland-Pfalz GmbH
Jens Lange, Stadt Kassel
Maik Poburski, Landkreis Osnabrück
Heino Reinartz, Städteregion Aachen
Heino Sauerbrey, Deutscher Landkreistag
Marcus Schröder, SECURiON Rheinland-Pfalz GmbH

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 mindestens die Anforderungen der Basis-Absicherung des BSI-Standards 200-2 [BSI-200-2] abdecken. 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

Mindestens Basis-Absicherung, teilweise Standard-Absicherung.

6.5 ISO27001-Kompatibilität

Mit dieser Basis-Absicherung wird ein nicht zertifizierungsfähiger Basis-Schutz gemäß ISO27001:2015 erreicht.

6.6 Rahmenbedingungen

Die Anwendung des Profils ist nur in Verbindung mit dem jeweils aktuellen IT-Grundschutz-Kompendium 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.

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

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)

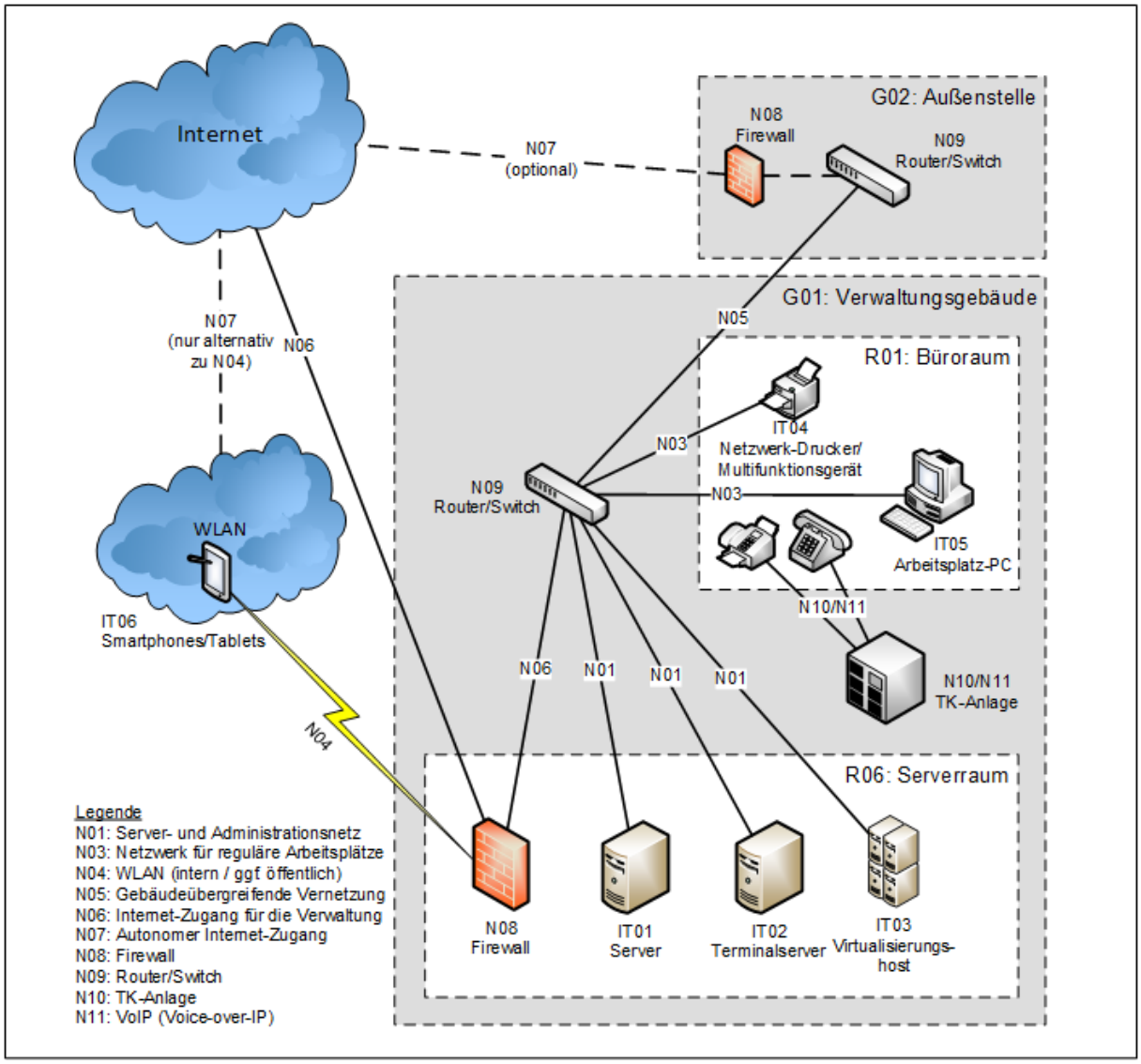
8.1.3 Netze

- 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)

8.2 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 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

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

Anforderungen	**ORP.1.A1 – A5; A6, A9**
Besonderheiten	ORP.1.A1 Von der in den Umsetzungshilfen 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 Umsetzungshilfen 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.A6 Da in Verwaltungen grundsätzlich zeitweise reger Publikumsverkehr herrscht, müssen Mitarbeiter besonders darauf achten, dass sie vertrauliche Informationen Unbefugten nicht (unfreiwillig) zugänglich machen.
	ORP.1.A9

	Die Sorgfaltspflicht der Verwaltung erlischt nicht mit der Entsorgung von Informationen. Aufgrund der Vielzahl von verarbeiteten (personenbezogenen) Informationen ist dafür zu sorgen, dass diese ordnungsgemäß entsorgt werden.

9.1.3 ORP.2 - Personal

Anforderungen	**ORP.2.A1 – A5; A6, A7, A9**
Besonderheiten	ORP.2.A6 Eine genaue Formulierung und Überprüfung der benötigten Qualifikationen und Fähigkeiten ist erforderlich, da ansonsten die Gefahr besteht, dass der Bewerber für die Aufgabe nicht ausreichend geeignet ist.
	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).
	ORP.2.A9 Die regelmäßige Schulung der Mitarbeiter für ihren jeweiligen Aufgabenbereich ist für einen sicheren IT-Betrieb erforderlich.

9.1.4 ORP.3 - Sensibilisierung und Schulung zur Informationssicherheit

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

Anforderungen	**ORP.4.A1 – A9; 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

Anforderungen	**CON.3.A1 – A5**
Besonderheiten	---

9.1.7 CON.4 - Auswahl und Einsatz von Standardsoftware

Anforderungen	**CON.4.A1 – A3; A4, A6 – A8**
Besonderheiten	CON.4.A4 Wird beim Einsatz von Standardsoftware kein Verantwortlicher benannt, kann der interne Betrieb erheblich gestört werden und es kann u. a. zu Vertragsstrafen kommen. Um sicherzustellen, dass alle technischen, rechtlichen und

	organisatorischen Sicherheitsanforderungen erfüllt werden, ist ein Verantwortlicher zu benennen.
	CON.4.A6 Sind im Behördenumfeld verschiedene Softwareprodukte geeignet, kann es erhöhte finanzielle Aufwendungen zur Folge haben, wenn nicht eine verantwortliche Stelle eine Auswahl, Entscheidung und eine rechtssichere Beschaffung nach einem vorher festzulegenden Anforderungskatalog durchführt.
	CON.4.A7 Um die Gefahr von unvollständig oder falsch konfigurierten oder gelieferten Softwareprodukten zu minimieren, sind auch alle Softwareprodukte zu inventarisieren.
	CON.4.A8 Rechtliche Anforderungen sind gerade im Behördenumfeld zwingend zu erfüllen.

9.1.8 CON.6 - Löschen und Vernichten

Anforderungen	**CON.6.A1 – A2; A3, A5 – A6**
Besonderheiten	CON.6.A3 Zu den Datenträgern gehören insbesondere (externe) Festplatten und USB-Sticks, welche in der öffentlichen Verwaltung in nicht unerheblichem Umfang zum Einsatz kommen. Die Daten müssen vor der Weitergabe bzw. dem Austausch des Datenträgers sicher gelöscht werden.
	CON.6.A5 Es muss sichergestellt werden, dass Datenträger (z. B. Festplatten) von IT-Systemen (z. B. Clients, Multifunktionsgeräte) bei Außerbetriebnahme sicher gelöscht werden, da diese zumeist sensible Informationen enthalten. Unter Umständen ist die Vernichtung dauerhafter Speicherelemente sinnvoll.
	CON.6.A6 Um sicherzustellen, dass sensible Informationen sicher gelöscht werden können, müssen die zuständigen Mitarbeiter (insbesondere die des IT-Betriebs) in die hierfür notwendigen Methoden (z. B. Verwendung einer Software) eingewiesen werden.

9.1.9 OPS.1.1.2 - Ordnungsgemäße IT-Administration

Anforderungen	**OPS.1.1.2.A1 – A6; A7 – A9, A12**
Hinweis	Wird die IT von externen Auftragnehmern administriert, müssen diese den Baustein umsetzen.
Besonderheiten	OPS.1.1.2.A7 Vermeidung von 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

Anforderungen	**OPS.1.1.3.A1 – A3**
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	OPS.1.1.3.A1 Die Kritikalität von Patches ist im Test- und Freigabeprozess zu berücksichtigen (so kann es sein, dass manche Patches schneller ausgerollt werden sollten als andere).

9.1.11 OPS.1.1.4 - Schutz vor Schadprogrammen

Anforderungen	**OPS.1.1.4.A1 – A7**
Besonderheiten	---

9.1.12 OPS.1.1.5 - Protokollierung

Anforderungen	**OPS.1.1.5.A1 – 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.1.2.3 - Informations- und Datenträgeraustausch

Anforderungen	**OPS.1.2.3.A1 – A5**
Hinweis	Im Rahmen dieses Profils ist dieser Baustein einmal übergreifend zu behandeln. Dadurch werden grundsätzliche Regelungen geschaffen (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.
Besonderheiten	---

9.1.14 OPS.1.2.4 - Telearbeit

Anforderungen	**OPS.1.2.4.A1 – A5**

Hinweis	Dieser Baustein ist nur zu betrachten, wenn Telearbeit genutzt wird. Es ist dabei unerheblich ob dies von einem mobilen oder einem Heimarbeitsplatz aus erfolgt.
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. Telearbeiter sind genauso in den Kommunikationsfluss der Verwaltung zu integrieren wie alle anderen Mitarbeiter.
	OPS.1.2.4.A4 Wenn von Telearbeitsplätzen aus nur auf Netzlaufwerken gearbeitet wird, lokal also keine sicherungswürdigen Daten anfallen, ist diese Anforderung entbehrlich.

9.1.15 OPS.2.1 - Outsourcing für Kunden

Anforderungen	**OPS.2.1.A1; A3 - A4, A6 - A10, A12**
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.
Besonderheiten	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.
	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.

9.1.16 OPS.2.4 - Fernwartung

Anforderungen	**OPS.2.4.A1 – A5; A7 – A9, A14, A18**
Hinweis	Dieser Baustein ist nur zu beachten, wenn Möglichkeiten zur Fernwartung von Dritten genutzt werden.
Besonderheiten	OPS.2.4.A7 Die Dokumentation der Fernwartung enthält vertrauliche Informationen über Fernzugriffsmöglichkeiten. Der Schutz vor unbefugtem Zugriff muss sichergestellt sein.
	OPS.2.4.A8 Um eine Kompromittierung der Fernwartungssitzung zu verhindern, müssen aktuelle und als sicher eingestufte Kommunikationsprotokolle eingesetzt werden.
	OPS.2.4.A9 Um unkontrollierte Fernzugriffe zu unterbinden, müssen organisatorische Verwaltungsprozesse zum Umgang mit ausgewählten Fernwartungswerkzeugen etabliert werden.
	OPS.2.4.A14 Um administrative Anpassungen, die im Rahmen einer Fernwartung durchgeführt werden, nachweislich zu dokumentieren und um eine lückenlose Betriebsdokumentation vorzuhalten, müssen alle Aktivitäten während einer Administrationssitzung protokolliert werden.
	OPS.2.4.A18 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.

9.1.17 DER.2.1 - Behandlung von Sicherheitsvorfällen

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 APP.1.1 - Office-Produkte

Anforderungen	**APP.1.1.A1 – A4; A7, A9, A12 – 13 & 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.A7 Um Fehlkonfigurationen und das Umgehen von Sicherheitseinstellungen zu unterbinden, muss für die eingesetzten Office-Produkte eine an den Bedarf der Institution angepasste Standardkonfiguration erstellt und genutzt werden.
	APP.1.1.A9 Im Laufe ihrer Bearbeitung können Informationen durch verschiedene Abteilungen gehen. Dabei anfallende Restinformationen oder Metadaten sind vor der Weitergabe zu bereinigen. Dies beugt vor allem der versehentlichen Veröffentlichung von Informationen vor.
	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.

9.2.1.2 SYS.3.4 - Mobile Datenträger

Anforderungen	**SYS.3.4.A1 – A3; A4 – A8**
Hinweis	Der Baustein ist für jeden mobilen Datenträger bzw. für jede Gruppe hiervon anzuwenden.
Besonderheiten	SYS.3.4.A4 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 allem muss unmissverständlich klar sein, welche mobilen Datenträger genutzt werden dürfen.
	SYS.3.4.A5 Mobile Datenträger können sehr schnell mit Schadprogrammen infiziert werden. Dies gilt vor allem in fremden IT-Umgebungen. Deshalb muss klar geregelt werden, wie mit mobilen Datenträgern außerhalb der Kommunalverwaltung umzugehen ist.
	SYS.3.4.A6 Um sicherzustellen, dass nur zugelassene mobile Datenträger eingesetzt werden, sind diese geregelt zu verwalten.
	SYS.3.4.A7 Die Löschung vor und nach der Nutzung ist notwendig, um stets „saubere“ mobile Datenträger bereitstellen zu können.
	SYS.3.4.A8 Versehentliche Infektionen der eigenen IT-Infrastruktur aufgrund von unsachgemäßer Nutzung von mobilen Datenträgern können am zuverlässigsten durch die Absicherung der dazu notwendigen Schnittstellen verhindert werden. Des Weiteren werden Anwender dadurch noch zusätzlich sensibilisiert.

9.2.1.3 NET.1.1 - Netzarchitektur und -design

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.

9.2.1.4 NET.2.2 - WLAN-Nutzung

Anforderungen	**NET.2.1.A1 – A3**
Besonderheiten	---

9.2.2 Infrastruktur

9.2.2.1 Verwaltungsgebäude (Objekt G01)

9.2.2.1.1 INF.1 - Allgemeines Gebäude

Anforderungen	**INF.1.A1 – A8; A9**
Besonderheiten	INF.1.A3 Die Erstellung eines Brandschutzkonzeptes für ein Gebäude ist nur dann notwendig, wenn es baurechtlich erforderlich ist. Unabhängig davon sind IT-bezogene Anforderungen an den Brandschutz zu beachten.
	INF.1.A4 Eine Brandmeldeanlage oder Komponenten einer Brandmeldeanlage (wie z. B. Rauchmelder) sind nur notwendig, wenn sie baurechtlich gefordert sind. Das gleiche gilt für Alarmierungsanlagen.
	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.3 - Elektrotechnische Verkabelung

Anforderungen	**INF.3.A1 – A3**
Besonderheiten	---

9.2.2.1.3 INF.4 - IT-Verkabelung

Anforderungen	**INF.4.A1 – A3; A9**
Besonderheiten	INF.4.A9 Die Anforderung ist umzusetzen, um den Betrieb effizient planen zu können und um die zukünftige Weiterentwicklung der IT-Netze bestmöglich zu unterstützen. Zur Umsetzung reicht es aus, wenn die folgenden Punkte beachtet werden: Die Anschlüsse (Ports) von Rangierfeldern (Panels) in IT-Verteilerschränken und die Anschlussdosen (Ports) für die Endgeräte müssen durchgängig, einheitlich, gut lesbar und dauerhaft beschriftet sein. Alle IT-Kabelstrecken (Lichtwellenleiter und Kupfer) sind auf der Grundlage der festgelegten Link-Klassifizierungen zu messen und die Messprotokolle dem Auftraggeber zu übergeben.

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

9.2.2.2.1 INF.1 - Allgemeines Gebäude

Anforderungen	**INF.1.A1 – A8; A9**
Besonderheiten	INF.1.A3 Die Erstellung eines Brandschutzkonzeptes für ein Gebäude ist nur dann notwendig, wenn es baurechtlich erforderlich ist. Unabhängig davon sind IT-bezogene Anforderungen an den Brandschutz zu beachten.
	INF.1.A4 Eine Brandmeldeanlage oder Komponenten einer Brandmeldeanlage (wie z. B. Rauchmelder) sind nur notwendig, wenn sie baurechtlich gefordert sind. Gleiches gilt für Alarmierungsanlagen.
	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.3 - Elektrotechnische Verkabelung

Anforderungen	**INF.3.A1 – A3**
Besonderheiten	---

9.2.2.2.3 INF.4 - IT-Verkabelung

Anforderungen	**INF.4.A1 – A3; A9**
Besonderheiten	INF.4.A9 Die Anforderung ist umzusetzen, um den Betrieb effizient planen zu können und um die zukünftige Weiterentwicklung der IT-Netze bestmöglich zu unterstützen. Zur Umsetzung reicht es aus, wenn die folgenden Punkte beachtet werden: Die Anschlüsse (Ports) von Rangierfeldern (Panels) in IT-Verteilerschränken und die Anschlussdosen (Ports) für die Endgeräte müssen durchgängig, einheitlich, gut lesbar und dauerhaft beschriftet sein. Alle IT-Kabelstrecken (Lichtwellenleiter und Kupfer) sind auf der Grundlage der festgelegten Link-Klassifizierungen zu messen und die Messprotokolle dem Auftraggeber zu übergeben.

9.2.2.3 Büroraum (Objekt R01)

9.2.2.3.1 INF.7 - Büroarbeitsplatz

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.
	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

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-, Schulungsraum

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

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

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.
	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

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

Anforderungen	**INF.2.A1 – A11; A15**
Hinweis	Der Baustein ist pro selbst betriebenem Serverraum anzuwenden. Wenn die IT extern gehostet wird (z. B. in einem Rechenzentrum), ist der jeweilige Dienstleister auf die Umsetzung dieses Bausteins zu verpflichten.
Besonderheiten	INF.2.A15 Aufgrund der zentralen Bedeutung für das Verwaltungshandeln und um die Arbeitssicherheit zu gewährleisten, müssen Serverräume über einen ausreichenden Blitz- und Überspannungsschutz verfügen.

9.2.2.9 Raum für technische Infrastruktur (Objekt R07)

[Die Veröffentlichung des Bausteins INF.5 Raum sowie Schrank für technische Infrastruktur ist vom BSI geplant. Der Baustein wird in das Profil integriert, sobald er verfügbar ist.]

9.2.2.10 Archivraum (Objekt R08)

9.2.2.10.1INF.6 - Datenträgerarchiv

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 (siehe hierzu Baustein "INF.5 Raum oder Schrank für technische Infrastruktur" des IT-Grundschutz-Kompendium).
Besonderheiten	---

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.

9.2.2.11.1SYS.4.1 - Drucker, Kopierer und Multifunktionsgeräte

Anforderungen	**SYS.4.1.A1 – A3; A4, A7, A9, A11, A12, A13**

Hinweis	Der Baustein ist für jeden Drucker, Kopierer oder Multifunktionsgerät im Informationsverbund bzw. in jeder Gruppe hiervon anzuwenden. Als Multifunktionsgeräte werden dabei Geräte bezeichnet, die mehrere verschiedene papierverarbeitende Funktionen bieten, etwa Drucken, Kopieren und Scannen oder auch Fax-Dienste.
Besonderheiten	SYS.4.1.A4 Da die Geräte von verschiedenen Abteilungen genutzt werden, muss deren Einsatz sorgfältig geplant werden. Nur so können Risiken für die Vertraulichkeit von Informationen minimiert werden.
	SYS.4.1.A7 Da die Geräte unbeaufsichtigt genutzt werden, ist es notwendig, die Administrationszugriffe soweit wie möglich einzuschränken, um sicherzustellen, dass abgestimmte Einstellungen nicht geändert werden.
	SYS.4.1.A9 Durch die gemeinschaftliche Nutzung der Geräte können Unstimmigkeiten oder Probleme nur durch eine korrekte Protokollierung nachgehalten und erkannt werden. Um sicherzustellen, dass die dafür geltenden rechtlichen Vorschriften eingehalten werden, ist eine sorgfältige Planung der Protokollierung notwendig.
	SYS.4.1.A12 Die ordnungsgemäße Entsorgung muss für alle schützenswerten Betriebsmittel klar geregelt sein. Vor allem um sicherzustellen, dass für gemeinschaftlich genutzte Ressourcen keine Risiken durch unklare Zuständigkeiten entstehen.
	SYS.4.1.A13 Da die Geräte von verschiedenen Abteilungen genutzt werden, muss speziell auf deren sichere Außerbetriebnahme geachtet werden. Andernfalls könnten nach der Entsorgung Unbefugte Einsicht in nahezu alle Verwaltungsprozesse und -informationen erlangen.

9.2.2.11.2 INF.10 - Besprechungs-, Veranstaltungs-, Schulungsraum

Anforderungen	**INF.10.A1 – A3; A7**
Hinweis	Der Baustein ist auf jeden Drucker- und Kopierraum bzw. jede Gruppe hiervon anzuwenden.
Besonderheiten	INF.10.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.

9.2.3 IT-Systeme

9.2.3.1 Serversystem (Objekt IT01)

9.2.3.1.1 SYS.1.1 - Allgemeiner Server

Anforderungen	**SYS.1.1.A1 – A10; A15, A17, 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.A17 Ein Freigabeverfahren für den Einsatz im Produktivbetrieb ist unabdingbar, da sonst die Gefahr besteht, dass nicht (ausreichend) getestete Server produktiv eingesetzt werden.
	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.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.1.5 - Virtualisierung

Anforderungen	**SYS.1.5.A1 – A7; A12, A18**
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.
	SYS.1.5.A18 Um die korrekte Nutzung und Konfiguration von virtuellen Umgebungen sicherzustellen, müssen die zuständigen Administratoren entsprechend geschult werden.

9.2.3.4 Netzwerk-Drucker / Multifunktionsgerät (Objekt IT04)

Im Gegensatz zum Drucker- und Kopierraum (Objekt R09) wird hier davon ausgegangen, dass eine Aufstellung der Geräte in einem überwachten Bereich erfolgt und somit eine gewisse Kontrolle über das Gerät besteht.

9.2.3.4.1 SYS.4.1 - Drucker, Kopierer und Multifunktionsgeräte

Anforderungen	**SYS.4.1.A1 – A3; A7 – A9, A11 – A12**
Hinweis	Der Baustein ist für jeden Drucker, Kopierer oder Multifunktionsgerät im Informationsverbund bzw. für jede Gruppe hiervon anzuwenden.
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.A8 Die Versorgung als auch die Entsorgung der Verbrauchsgüter muss geregelt sein. Diesbezügliche Verantwortlichkeiten sind zu regeln und zu kommunizieren.
	SYS.4.1.A9 Sicherheitsrelevante Aktivitäten auf Druckern, Kopierern und Multifunktionsgeräten sollten protokolliert werden. Dabei muss abgestimmt sein, was protokolliert wird, wo dies gespeichert wird und wer dies in welchen Zeiträumen auswertet, um insbesondere den gesetzlichen Anforderungen zu entsprechen.
	SYS.4.1.A12 Schutzbedürftige Betriebsmittel, die bei Druckern, Kopierern und Multifunktionsgeräten anfallen, müssen ordnungsgemäß entsorgt werden. Es müssen Regelungen für eine ordnungsgemäße Entsorgung bestehen. Wenn Betriebsmittel erst gesammelt und später entsorgt werden, müssen diese vor einem unberechtigten Zugriff geschützt sein.
	SYS.4.1.A13 Bevor Drucker, Kopierer und Multifunktionsgeräte entsorgt, zurückgegeben oder ausgetauscht werden, müssen alle auf ihnen befindlichen Informationen sicher gelöscht werden.

9.2.3.5 Arbeitsplatz-PC (Objekt IT05)

9.2.3.5.1 SYS.2.1 - Allgemeiner Client

Anforderungen	**SYS.2.1.A1 – A8; A19, A22, A25, A27**
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.A4 Eine Clientsicherung ist entbehrlich, wenn sichergestellt ist, dass eine Datenspeicherung nur auf den Servern erfolgt.
	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.A19 Analog zu A2 ist sicherzustellen, dass Nutzer nur tatsächlich benötigte Rechte erhalten.
	SYS.2.1.A22 Insbesondere in öffentlich zugänglichen Bereichen muss nach Aufgabenerfüllung eine Abmeldung erfolgen.
	SYS.2.1.A25 Wichtige Sicherheitsvorkehrungen, die technisch nicht oder nur unter nicht vertretbarem Aufwand umgesetzt werden können, sind organisatorisch in einer Richtlinie zur sicheren IT-Nutzung zu regeln.
	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 Mobiler Arbeitsplatz

9.2.3.6.1 SYS.2.1 - Allgemeiner Client

Anforderungen	**SYS.2.1.A1 – A8; A19, A22, A25, A27**
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.A4 Eine Clientsicherung ist entbehrlich, wenn sichergestellt ist, dass eine Datenspeicherung nur auf den Servern erfolgt.
	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.A19 Analog zu A2 ist sicherzustellen, dass Nutzer nur tatsächlich benötigte Rechte erhalten.
	SYS.2.1.A22 Insbesondere in öffentlich zugänglichen Bereichen muss nach Aufgabenerfüllung oder bei Arbeitsunterbrechungen eine Abmeldung erfolgen.
	SYS.2.1.A25

	Wichtige Sicherheitsvorkehrungen, die technisch nicht oder nur unter nicht vertretbarem Aufwand umgesetzt werden können, sind organisatorisch in einer Richtlinie zur sicheren IT-Nutzung zu regeln.
	SYS.2.1.A27 Es ist vor der Entsorgung sicherzustellen, dass eine Wiederherstellung der auf den Clients einmal vorhandenen Daten grundsätzlich ausgeschlossen ist.

9.2.3.6.2 SYS.3.1 - Laptop

Anforderungen	**SYS.3.1.A1 – A5; A6, A8 – A10, A12 – A13**
Hinweis	Der Baustein ist auf jeden mobilen Computer (z. B. Laptop, Notebook) bzw. jede Gruppe gleichartiger Computer anzuwenden.
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.
	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.

9.2.3.7 Smartphones und Tablets (inkl. „BYOD“ von Ratsmitgliedern) (Objekt IT06)

9.2.3.7.1 SYS.3.2.1 - Allgemeine Smartphones und Tablets

Anforderungen	**SYS.3.2.1.A1 – A8; A10 – A11, A16, A21**

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.
Besonderheiten	SYS.3.2.1.A10 Um sicherzustellen, dass Benutzer mobile Endgeräte im dienstlichen Einsatz auch nur in erlaubter Weise verwenden, müssen diese Regelungen klar dokumentiert sein und bekannt gemacht werden.
	SYS.3.2.1.A11 Um die Auswirkungen bei Verlusten von mobilen Endgeräten zu minimieren, sollten diese verschlüsselt werden. Gerade im kommunalen Umfeld, wo in nahezu jeder kommunalen Anwendung sensible (Bürger-)Daten verarbeitet werden, sind solche zusätzlichen Absicherungen notwendig.
	SYS.3.2.1.A16 Aktive, nicht benutzte Kommunikationsschnittstellen können von Unbefugten mit vergleichsweise geringem Aufwand gefunden und ausgenutzt werden. Um dieses Risiko zu minimieren, sollten daher stets nur die Kommunikationsschnittstellen aktiviert werden, die auch tatsächlich benötigt werden.
	SYS.3.2.1.A21 Es besteht ein unüberschaubares Angebot an Applikationen für alle möglichen Zwecke. Um vergleichbare Arbeitsvoraussetzungen für Benutzer zu schaffen und das Risiko und die Auswirkungen von ungewollten Datenabflüssen zu minimieren, ist klar zu definieren, welche Informationen auf mobilen Endgeräten gespeichert und verarbeitet werden dürfen.

9.2.4 Anwendungen

9.2.4.1 Internet-Nutzung (Objekt A01)

9.2.4.1.1 APP.1.2 - Web-Browser

Anforderungen	**APP.1.2.A1 – A4; A5**
Hinweis	Der Baustein ist für alle IT-Systeme anzuwenden, auf denen Web-Browser eingesetzt werden.
Besonderheiten	APP.1.2.A4 Nur erforderlich, wenn kein zentrales Softwareverteilungstool vorhanden ist.
	APP.1.2.A5 Erweiterte Rechte würden eine zusätzliche Gefährdung darstellen. Sofern vorhanden sollten daher die Rechte der Browser soweit standardisiert sein, dass nur die für die Benutzung notwendigen Rechte vorhanden sind.

9.2.4.2 Benutzer-Authentifizierung (A02)

9.2.4.2.1 APP.2.1 - Allgemeiner Verzeichnisdienst

Anforderungen	**APP.2.1.A1 - A6; A7 - A15**

Hinweis	Der Baustein sollte, unabhängig vom gewählten Produkt, auf jeden Verzeichnisdienst einmal angewandt werden.
Besonderheiten	Wenn die aufgeführten Standard-Anforderungen (A7 - A15) nicht eingehalten werden können, sollte der eigenverantwortliche Betrieb eines Verzeichnisdienstes überdacht werden.
	APP.2.1.A7 Aufgrund der Komplexität der Sachlage ist die Erstellung eines Sicherheitskonzeptes für den Einsatz von Verzeichnisdiensten notwendig. Darin sollen die relevantesten Informationen dokumentiert werden, um negative Auswirkungen von z. B. Personalwechseln zu minimieren.
	APP.2.1.A8 Eine fehlerhafte oder unzureichende Planung der Partitionierung und der Replizierung des Verzeichnisdienstes kann zu Datenverlusten sowie Inkonsistenzen in der Datenhaltung, zu einer mangelhaften Verfügbarkeit des Verzeichnisdienstes und zu einer insgesamt schlechten Systemperformance bis hin zu Systemausfällen führen.
	APP.2.1.A9 Die vorgesehene Hardware für den Verzeichnisdienst muss entsprechend der Anforderungen des vorgesehenen Verzeichnisdienstes ausreichend dimensioniert sein. Die Netzlast sollte bei Anfragen an den Verzeichnisdienst so verteilt werden, dass die Verfügbarkeit des Dienstes aufrecht erhalten bleibt. Die Software des Verzeichnisdienstes sollte den Anforderungen der administrativen Aufgaben einschließlich der Vergabe von Rollen- / Rechte-Definitionen genügen und ausreichend sichere Authentisierungen der Benutzer gegenüber dem Verzeichnisdienst unterstützen.
	APP.2.1.A10 Zur Gewährleistung eines sicheren Betriebes müssen Administratoren über ein hinreichendes Grundwissen über Verzeichnisdienste aber auch der zugrunde liegenden Betriebssysteme verfügen. Umfang und Tiefe der Schulung sollte den Tätigkeitsmerkmalen in angemessenem Umfang entsprechen.
	APP.2.1.A11 Über den Verzeichnisdienst werden Benutzer und Berechtigungen verwaltet. Der Zugriff auf alle Administrationswerkzeuge muss für normale Benutzer unterbunden werden.
	APP.2.1.A12 Um den Sicherheitszustand des Verzeichnisdienstes nachvollziehen zu können, ist es notwendig, diesen kontinuierlich zu überwachen.
	APP.2.1.A13 Die Kommunikation und Übertragung von Informationen wie Kennwörter muss durch eine ausreichende Verschlüsselung abgesichert sein. Die Zugriffe auf den Verzeichnisdienst sollten eingeschränkt sein, um die unnötige Herausgabe sicherheitssensitiver Informationen zu verhindern.
	APP.2.1.A14

	Bei der Außerbetriebnahme eines Verzeichnisdienstes sollen berechtigte Benutzer weiterhin auf benötigte Ressourcen zugreifen können.
	APP.2.1.A15 Verbesserte Funktionalitäten und erhöhte Sicherheit aber auch der Austausch von Hardwarekomponenten sind Gründe für die Migration eines Verzeichnisdienstes auf eine höhere Version. Während der Migration soll die Verfügbarkeit des Verzeichnisdienstes gewährleistet sein. Migrationen müssen geplant und dokumentiert werden.

9.2.4.3 Dateiablage (A03)

9.2.4.3.1 APP.3.3 - Fileserver

Anforderungen	**APP.3.3.A1 – A5; A8, A10**
Hinweis	Der Baustein ist auf jeden Fileserver anzuwenden.
Besonderheiten	APP.3.3.A8 Die strukturierte Datenhaltung ist eine grundlegende Voraussetzung für die Erstellung eines geeigneten Datensicherungskonzepts.
	APP.3.3.A10 Aufgrund der Gefahr des Datenverlusts durch Schadsoftware (z. B. Verschlüsselungstrojaner) ist ein regelmäßiger Test des Datensicherungs- bzw. Wiederherstellungskonzepts notwendig.

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

9.2.4.4.1 APP.5.1 - Allgemeine Groupware

Anforderungen	**A1 - A4; A5, A13, A19**
Hinweis	Der Baustein ist auf jedes E-Mail-System (intern oder extern) anzuwenden.
Besonderheiten	APP.5.1.A5 Mitarbeiter sollten dafür sensibilisiert sein, dass sie vor der Weitergabe personenbezogener oder vertraulicher Informationen mittels Groupware prüfen, ob diese zulässig ist, das gewählte Übertragungsmedium geeignet ist und ob die Empfänger die notwendigen Berechtigungen zur Weiterverarbeitung dieser Informationen besitzen. Die gesetzlichen Vorschriften (insbesondere Datenschutzgesetze) und interne Regelungen (Dienstanweisungen und Dienstvereinbarungen) müssen eingehalten werden.
	APP.5.1.A13 Vor der Weitergabe von Dateien (beispielsweise Word-, Excel- oder PDF-Dokumente) sollten diese auf verborgene Inhalte, Kommentare, Änderungsmarkierungen, Versionshistorien, interne Verweise sowie sonstige Dateiinformationen (Dateieigenschaften) überprüft werden. Diese zusätzlichen Informationen sind üblicherweise "nicht zur Veröffentlichung" bestimmt und zu entfernen.

	APP.5.1.A19 E-Mails enthalten zusätzlich zu den Inhaltsdaten (d. h. dem Text der Mail und etwaigen Anhängen) auch Metadaten wie Absender und Empfänger, das Datum und den Betreff. Sowohl Inhalts- als auch Metadaten können personenbezogene Daten beinhalten. Daher sind bei der datenschutzrechtlichen Beurteilung beide Datenarten zu berücksichtigen. Siehe hierzu Art. 32 DSGVO, Art. 35 DSGVO sowie "BSI TR-03108-1: Secure E-Mail Transport". Können bei der Übermittlung schutzbedürftiger Daten weder Ende-zu-Ende-Verschlüsselung noch eine Verschlüsselung auf Transportebene gewährleistet werden, sollten alternative Übermittlungsmedien genutzt werden.

9.2.5 Netze

9.2.5.1 Server- und Administrationsnetz (Objekt N01)

9.2.5.1.1 NET.1.2 - Netzmanagement

Anforderungen	**NET.1.2.A1 – 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

Anforderungen	**NET.1.2.A1 – 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

Anforderungen	**NET.1.2.A1 – 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

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

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)

9.2.5.6.1 OPS.3.3 - Internet-Provider

[Die Veröffentlichung des Bausteins OPS.3.3 Internet-Provider ist vom BSI geplant. Der Baustein wird in das Profil integriert, sobald er verfügbar ist.]

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

9.2.5.7.1 OPS.3.3 - Internet-Provider

[Die Veröffentlichung des Bausteins OPS.3.3 Internet-Provider ist vom BSI geplant. Der Baustein wird in das Profil integriert, sobald er verfügbar ist.]

9.2.5.8 Firewall (Objekt N08)

9.2.5.8.1 NET.3.2 - Firewall

Anforderungen	**NET.3.2.A1 – A15; A17 – A20**

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.
	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.A19 Es handelt sich bei den beiden erstgenannten Angriffstechniken um bekannte und zum Teil leicht anzuwendende Angriffsmethoden, die bei richtiger Ausführung zu Systemabstürzen und Netzwerkausfällen führen können. Die Gefahr von Sequence Number Guessing wird durch die zufällige Generierung von Sequenznummern deutlich vermindert, da Angreifer dadurch nicht mehr ohne weiteres in der Lage sind, Sequenznummern zu berechnen.
	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

Anforderungen	**NET.3.1.A1 – A9**
Hinweis	Der Baustein ist für jedes aktive Netz anzuwenden.
Besonderheiten	---

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

9.2.5.10.1 *NET.4.1 – TK-Anlagen*

Anforderungen	**NET.4.1.A1 – A5; A7, A10, A12, A15, A16**

Hinweis	Der Baustein ist für jede TK-Anlage anzuwenden.
Besonderheiten	---

9.2.5.10.2NET.4.3 – Faxgeräte und Faxserver

Anforderungen	**NET.4.3.A1 – A3; A5, A8**
Hinweis	Der Baustein ist für jedes Faxgerät oder Faxserver anzuwenden.
Besonderheiten	---

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

9.2.5.11.1NET.4.2 - VoIP

Anforderungen	**NET.4.2.A1 – A6; A10, 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.2.4 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.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

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.

10.1 Outsourcing

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.

Als Auslagerung zählen auch Aufgabenübertragungen (z. B. an einen Zweckverband).

Von jedem Outsourcing-Auftragnehmer ist ein Sicherheitskonzept pro Outsourcing-Dienstleistung zu verlangen.

10.2 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

Anmerkungen, Rückfragen und Kritik können jederzeit unter folgender E-Mail-Adresse an die AG „Modernisierung IT-Grundschutz" gerichtet werden: kommunalprofile@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 „Modernisierung IT-Grundschutz" vertreten. Das IT-SiBe-Forum ist unter folgender URL zu erreichen: www.it-sibe-forum.de.

14 ANHANG

14.1 Abkürzungen

Abkürzung	Erläuterung
AG	Arbeitsgruppe
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 2019; Bundesamt für Sicherheit in der Informationstechnik; (https://www.bsi.bund.de)

[BSI-IT-GS-UH] Umsetzungshinweise zum IT-Grundschutz-Kompendium Edition 2019; Final Draft; Bundesamt für Sicherheit in der Informationstechnik; (https://www.bsi.bund.de)

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