Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Anforderungskatalog zur Informationssicherheit bei der Ermittlung des vorläufigen Wahlergebnisses bundesweiter parlamentarischer Wahlen

Informationssicherheit bei Schnellmeldungen

An der Erstellung waren folgende Mitarbeiter des BSI (Bundesamt für Sicherheit in der Informationstechnik) beteiligt: René Paegelow, René Costa, Philipp Gauer und Thomas Kock.

Weiterhin haben Alexander Busse und Andrea Schmitt von der PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft maßgeblich an der Erstellung mitgewirkt.

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: bsi@bsi.bund.de
Internet: https://www.bsi.bund.de
© Bundesamt für Sicherheit in der Informationstechnik 2020

Danksagung

Auf Bitten des Bundeswahlleiters hat das Bundesamt für Sicherheit in der Informationstechnik den vorliegenden Anforderungskatalog erstellt.

In mehreren Feedback-Runden wurde der Anforderungskatalog mit Vertretern der Zielgruppen Bund, Länder, Kommunen und kommunale Spitzenverbände gemeinschaftlich erarbeitet und abgestimmt.

An dieser Stelle sei allen Beteiligten für ihr Engagement gedankt.

Inhalt

1 Formale Aspekte

Titel	Anforderungskatalog zur Informationssicherheit bei der Ermittlung des vorläufigen Wahlergebnisses bundesweiter parlamentarischer Wahlen
Untertitel	Informationssicherheit bei Schnellmeldungen
Version	1.0
Status	Final
Revisionszyklus	Der Anforderungskatalog wird in Anlehnung an das IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ alle drei Jahre, spätestens aber ein Jahr vor der nächsten planmäßigen Bundestagswahl gesichtet und bei Bedarf angepasst.
Anmerkung	In diesem Dokument wird aus Gründen der besseren Lesbarkeit das generische Maskulinum verwendet. Weibliche und anderweitige Geschlechteridentitäten werden dabei ausdrücklich mitgemeint, soweit es für die Aussage erforderlich ist.

2 Haftungsausschluss

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

3 Management Summary

3.1 Hintergrund

Bei bundesweiten parlamentarischen Wahlen ermitteln die Wahlorgane ein vorläufiges Wahlergebnis, das noch in der Wahlnacht bekannt gegeben wird. Sobald die Wahlergebnisse in den Wahlbezirken festgestellt wurden, sind sie auf schnellstem Wege über die Gemeindebehörden, die Kreiswahlleitungen und die Landeswahlleitungen an den Bundeswahlleiter zu melden. Die Ermittlung der jeweiligen Teilergebnisse und die Übermittlung werden in der Praxis überwiegend durch IT unterstützt. Damit sind vielfältige Gefährdungen verbunden.

Im Prozess der Übermittlung der vorläufigen Wahlergebnisse spielen neben sicherer Software eine geschützte IT-Umgebung mit robuster Hardware sowie reibungsfreie organisatorische Abläufe und geschultes, sensibilisiertes Personal eine wichtige Rolle für die gesamte Informationssicherheit. Bei der Betrachtung der Informationssicherheit ist ein ganzheitlicher Ansatz von besonderer Bedeutung. So kann bspw. eine als „sicher“ geltende Software in einer „unsicheren“ IT-Umgebung eine Gefährdung darstellen.

Von den beteiligten Wahlorganen und in den Wahlbehörden werden unterschiedliche Hardware und Software zur Unterstützung bei den Schnellmeldungen eingesetzt. Für einschlägige Software-Lösungen zur Datenauswertung oder Datenaufbereitung für die Schnellmeldungen hat sich ein Markt mit verschiedenen Anbietern gebildet. Darüber hinaus haben Gemeinden, Statistische Landesämter und Landeswahlleitungen teilweise selbst Software-Lösungen entwickelt.

In der Vergangenheit kam es jedoch bei Wahlen zu verschiedenen technischen Schwierigkeiten oder Ausfällen. Es wurden diverse, für Angreifer ausnutzbare, Schwachstellen entdeckt.[1] Aufgrund der hohen Bedeutung von korrekten und schnell verfügbaren vorläufigen Wahlergebnissen, ist es unbedingt notwendig, die Integrität und Verfügbarkeit dieser eingehend und umfassend zu schützen.

3.2 Zielgruppe

Dieser Anforderungskatalog richtet sich an die Wahlorgane und -behörden aller Ebenen von Wahlbezirk bis Bund, welche in den Prozess der Schnellmeldungen nach § 71 Bundeswahlordnung (BWO) eingebunden sind.

3.3 Zielsetzung

Der Anforderungskatalog stellt Sicherheitsanforderungen für die Ermittlung des vorläufigen Wahlergebnisses bei bundesweiten parlamentarischen Wahlen dar. Anhand des Anforderungskatalogs soll die Informationssicherheit im Rahmen der Ermittlung des vorläufigen Wahlergebnisses erhöht werden. Das Ziel ist es, mit den enthaltenen Anforderungen insbesondere die Verfügbarkeit und Integrität bei der Ermittlung der vorläufigen Ergebnisse zu gewährleisten. Des Weiteren ist im Kontext der Integrität die Sicherstellung der Authentizität von wichtiger Bedeutung im Prozess der Schnellmeldungen. Zudem soll die Evaluierung der Sicherheit der genutzten Verfahren sowie der eingesetzten, den Wahlverlauf unterstützenden IT-Systeme, erleichtert werden.

[1] Vgl. Eckert, 2019; Schröder et al., 2017; Zawatzka-Gerlach, 2016

4 Festlegung des Geltungsbereichs

4.1 Beschreibung der Zielgruppe

Dieser Anforderungskatalog richtet sich an die in den Prozess zur Ermittlung der vorläufigen Wahlergebnisse eingebundenen Einheiten. Dazu gehören:

- Wahlbezirke,
- Gemeinden,
- Landkreise / kreisfreie Städte / Wahlkreise,
- Länder und
- Bund.

Im Zuge der Analyse des Informationsverbunds wurden hierbei die folgenden relevanten Rollen identifiziert:

- Wahlvorsteher,
- Gemeindebehörde,
- Kreiswahlleiter,
- Verwaltungsbehörde des Kreises,
- Landeswahlleiter (LWL),
- Bundeswahlleiter (BWL) sowie
- Mitglieder bzw. Beschäftigte in Kommunen, Ländern und Bund, die am Dateneingang, an der Datenzusammenfassung oder am Datenausgang der vorläufigen Wahlergebnisse beteiligt sind. Hierzu zählen auch interne oder externe IT-Dienstleister (Administration / Support).

4.2 Beschreibung des Prozesses der Schnellmeldungen

Gemäß § 71 BWO wird mittels Schnellmeldungen ein vorläufiges Wahlergebnis ermittelt. Nach der Feststellung des Wahlergebnisses in einem Wahlbezirk, wird das Ergebnis von dem Wahlvorsteher an die Gemeindebehörde übermittelt. Diese fasst die Ergebnisse aller Wahlbezirke der Gemeinde zusammen und meldet sie dem Kreiswahlleiter. Sollte in einer Gemeinde nur ein Wahlbezirk vorhanden sein, erfolgt die Meldung aus dem Wahlbezirk direkt an den Kreiswahlleiter. Von dem Landeswahlleiter kann angeordnet werden, dass die Wahlergebnisse in den kreisangehörigen Gemeinden über die Verwaltungsbehörde des Kreises zu melden sind.

Der Kreiswahlleiter ermittelt aus den Schnellmeldungen und unter Einbeziehung der Ergebnisse der Briefwahl, das vorläufige Wahlergebnis im Wahlkreis. Dieses Wahlergebnis wird auf dem schnellsten Wege dem Landeswahlleiter mitgeteilt. Die eingehenden Wahlkreisergebnisse werden durch den Landeswahlleiter dem Bundeswahlleiter schnellstmöglich und laufend gemeldet. Nach den Schnellmeldungen durch die Kreiswahlleiter ermittelt der Landeswahlleiter das vorläufige zahlenmäßige Wahlergebnis im Land und meldet dieses auf schnellstem Wege dem Bundeswahlleiter. Anschließend wird nach den Schnellmeldungen der Landeswahlleiter entsprechend § 78 BWO das vorläufige Wahlergebnis im Wahlgebiet durch den Bundeswahlleiter ermittelt.

Für die Durchführung der Schnellmeldungen bis zur Bekanntgabe der vorläufigen Wahlergebnisse sind zahlreiche Anforderungen zu erfüllen, um die Informationssicherheit entlang des Prozesses zu erhöhen.

Explizit **nicht** Teil des betrachteten Prozesses sind die Abgabe der Stimmen durch die Bürger in einem Wahlraum oder per Briefwahl, die manuelle Zählung der Stimmen im Wahlraum sowie die sichere Aufbewahrung der ausgefüllten Stimmzettel bis zum Zeitpunkt der Bekanntgabe der Ergebnisse. Die Prozesse zur Präsentation bzw. Veröffentlichung der Ergebnisse durch Gemeinden, Länder oder Bund gehören nicht zum Geltungsbereich. Ebenfalls nicht Bestandteil ist die Ermittlung der endgültigen Wahlergebnisse.

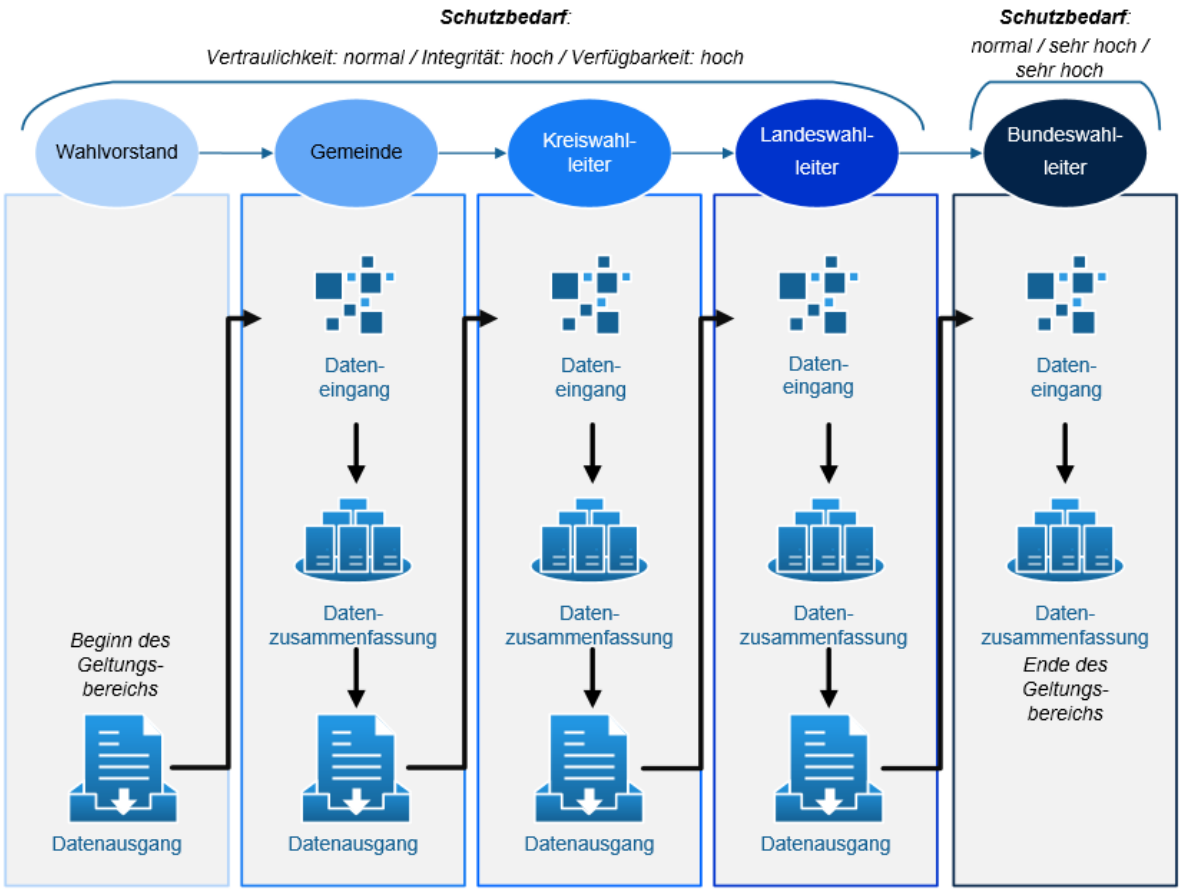

Abb. 1 Relevante Bestandteile des Prozesses der Schnellmeldungen

Die hier dargestellte Grafik visualisiert den betrachteten Teil des Prozesses der Schnellmeldungen, für welchen die Sicherheitsanforderungen ermittelt wurden. Zusätzlich gibt die Abbildung bereits einen Überblick über den Schutzbedarf, welcher im nächsten Kapitel erläutert wird.

4.3 Schutzbedarf

Die drei Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ wurden für die Bewertung der Schnellmeldungen verwendet. Diese drei Kategorien sind gemäß dem BSI-Standard 200-2 „IT-Grundschutz-Methodik“ folgendermaßen definiert:

- „normal“: Die Schadensauswirkungen sind begrenzt und überschaubar.
- „hoch“: Die Schadensauswirkungen können beträchtlich sein.
- „sehr hoch“: Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Eine ausführlichere Definition und Erläuterungen zum Schutzbedarf sind im Anhang A enthalten.

Es gilt anzumerken, dass ein Wahlorgan bzw. eine Wahlbehörde die Kategorien anpassen, umbenennen oder weitere Kategorien definieren kann.

Mit Blick auf § 71 BWO enthalten Schnellmeldungen die Zahlen der:

- Wahlberechtigten,
- Wähler,
- gültigen und ungültigen Erststimmen,
- gültigen und ungültigen Zweitstimmen,
- für jeden Bewerber abgegebenen gültigen Erststimmen,
- für jede Landesliste abgegebenen gültigen Zweitstimmen.

Die Zahlen werden auf dem schnellsten Weg, beispielsweise telefonisch oder auf einem sonstigen elektronischen Weg, gemeldet.

Der Schutzbedarf dieser verarbeiteten Daten wird in den Wahlbezirken, Kommunen, Landkreisen / kreisfreien Städten und Ländern hinsichtlich der

- Vertraulichkeit als „normal“,
- Integrität als „hoch“ und
- Verfügbarkeit als „hoch“ bewertet.[2]

In der Instanz des Bundes bzw. für den Bundeswahlleiter wird der Schutzbedarf der verarbeiteten Daten hinsichtlich der

- Vertraulichkeit als „normal“,
- Integrität als „sehr hoch“ und der
- Verfügbarkeit als „sehr hoch“ bewertet.[3]

4.4 Vorgehensweise nach IT-Grundschutz

Die in diesem Anforderungskatalog aufgeführten Anforderungen sind Empfehlungen des BSI für Bund, Länder und Kommunen zur Verbesserung der Informationssicherheit in dem Prozess der Schnellmeldungen der vorläufigen Wahlergebnisse nach § 71 BWO.

Die Auswahl der IT-Grundschutz-Bausteine wurde unter Abwägung der Relevanz für die Erhöhung der Informationssicherheit bei den Schnellmeldungen getroffen. Um ein ganzheitliches Informationssicherheitsmanagementsystem (ISMS) aufzubauen, sind jedoch langfristig auch unter anderem folgende Bausteine umzusetzen:

- ORP.5 – Compliance Management (Anforderungsmanagement),
- CON.3 – Datensicherungskonzept,
- CON.6 – Löschen und Vernichten,
- DER.2.2 – Vorsorge für die IT-Forensik,
- DER.3.1 – Audits und Revisionen,
- DER.3.2 – Revisionen auf Basis des Leitfadens IS-Revision.

Aus den relevanten Bausteinen im IT-Grundschutz-Kompendium wurden die zur Absicherung der Schnellmeldungen passenden Basis- oder Standard-Anforderungen ermittelt. Darüber hinaus wurden für

[2] Vgl. Bund-Länder-Arbeitsgruppe, 2018
[3] Vgl. ebd.

einige Bausteine und für einzelne Adressaten spezielle Anforderungen für den erhöhten Schutzbedarf ausgewählt. Des Weiteren wurden bei Bedarf zusätzliche Anforderungen formuliert, welche für den Informationsverbund zu beachten sind. Kapitel 7.1 „Methodik" enthält die Erläuterungen hierzu.

Das IT-Grundschutz-Kompendium Edition 2020 des BSI stellt die Grundlage für die Umsetzung der Anforderungen dar. Die im IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ (15.10.2019) genannten Anforderungen werden als Voraussetzung betrachtet. Außerdem wurden die Vorgaben aus § 71 BWO berücksichtigt.

Ferner ist anzumerken, dass eine ISO 27001-Kompatibilität gegeben ist.

4.4.1 Formulierung der Anforderungen

Gemäß IT-Grundschutz-Kompendium wurden die Anforderungen in den entsprechenden Bausteinen mit den Modalverben formuliert, die im Folgenden kurz erläutert werden.

- muss / darf nur: Dieser Ausdruck bedeutet, dass es sich um eine Anforderung handelt, die unbedingt erfüllt werden muss (uneingeschränkte Anforderung).
- darf nicht / darf kein: Dieser Ausdruck bedeutet, dass etwas in keinem Fall getan werden darf (uneingeschränktes Verbot).
- sollte: Dieser Ausdruck bedeutet, dass eine Anforderung normalerweise erfüllt werden muss, es aber Gründe geben kann, dies doch nicht zu tun. Dies muss aber sorgfältig abgewogen und stichhaltig begründet werden.
- sollte nicht / sollte kein: Dieser Ausdruck bedeutet, dass etwas normalerweise nicht getan werden sollte, es aber Gründe gibt, dies doch zu tun. Dies muss aber sorgfältig abgewogen und stichhaltig begründet werden.

4.4.2 Reihenfolge der Anforderungen

Die IT-Grundschutz-Bausteine wurden zur Priorisierung mit einer Umsetzungsreihenfolge gekennzeichnet. Hierbei wurde die im IT-Grundschutz-Kompendium vorgeschlagene Reihenfolge berücksichtigt und für den Geltungsbereich entsprechend teilweise angepasst. Gemäß IT-Grundschutz wurden die Kennzeichnungen „R1“, „R2“ und „R3“ gewählt. Diese drei Kategorien sind wie folgt definiert:

- R1: Diese Bausteine sollten vorrangig umgesetzt werden, da sie die Grundlage für einen effektiven Sicherheitsprozess bei den Schnellmeldungen bilden.
- R2: Diese Bausteine sollten als nächstes umgesetzt werden, da sie in wesentlichen Teilen des Informationsverbunds für die Sicherheit bei den Schnellmeldungen erforderlich sind.
- R3: Diese Bausteine werden zur Erreichung des angestrebten Sicherheitsniveaus ebenfalls benötigt und müssen umgesetzt werden, insofern sie für Wahlorgan oder -behörde von Relevanz sind. Es wird empfohlen, diese erst nach den anderen Bausteinen zu betrachten.

Diese Kennzeichnung zeigt eine mögliche zeitliche Reihenfolge für die Umsetzung der Anforderungen des jeweiligen Bausteins auf und stellt keine Gewichtung der Bausteine untereinander dar. Grundsätzlich müssen alle für den jeweiligen Informationsverbund relevanten Bausteine des IT-Grundschutz-Kompendiums umgesetzt werden.[4]

[4] Vgl. Bundesamt für Sicherheit in der Informationstechnik, 2020, S. 6

5 Abgrenzung des Informationsverbunds

5.1 Bestandteile des Informationsverbunds

Zum Informationsverbund gehören alle Systeme, Verfahren und Objekte, die nach der öffentlichen Ermittlung der vorläufigen Ergebnisse in den Wahlbezirken bis hin zur Zusammenfassung der Daten auf Bundesebene notwendig sind. Auf technischer Ebene sind hierfür in der Regel Client-Server-Systeme, Faxgeräte, (Mobil-)Telefone sowie Smartphones und Tablets in die entsprechende Netzinfrastruktur einzubeziehen. Das manuelle Verfahren und das zentrale Fachverfahren sind für die Datenzusammenfassung in Gemeinden und in Landkreisen / kreisfreien Städten relevant. Des Weiteren gehören Eingabe-, Ausgabe- und Freigabeschnittstellen dazu. Darüber hinaus sind auch Boten für die Übermittlung von Daten zu berücksichtigen. Im Kapitel 6 „Referenzarchitektur" ist die komplette Auflistung der als relevant eingestuften Objekte enthalten.

5.2 Nicht berücksichtige Objekte

Objekte, die im betrachteten Prozess der vorläufigen Wahlergebnisermittlung keine direkte Relevanz besitzen oder eine Nutzung explizit nicht vorgesehen sein sollte, wurden nicht berücksichtigt bzw. für diese wurden keine Anforderungen gelistet. Dazu zählen beispielsweise:

- Clients, die für die Bürokommunikation genutzt werden, die nicht dem Zweck der vorläufigen Wahlergebnismeldung dienen,
- Server, die nicht die vorläufige Wahlergebnismeldung unterstützen.

Eine Auflistung und Bewertung aller von den Wahlorganen und -behörden verwendeten Anwendungen oder Dienste ist an dieser Stelle aufgrund der Heterogenität nicht zielführend, um die angestrebte Sicherheit zu erreichen. Darüber hinaus soll an dieser Stelle auch auf die kurze Zeitperiode der Schnellmeldungen hingewiesen werden. Es handelt sich somit um einen temporär genutzten Informationsverbund.

5.3 Verweis auf andere IT-Grundschutz-Profile und Leitlinien

Die folgenden Dokumente stellen (entsprechend der Zielgruppe) eine wichtige Grundlage dar:

- IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ (15.10.2019),
- IT-Grundschutz-Profil für die obersten Landesbehörden Deutschlands (31.05.2019),
- Umsetzungsplan Bund 2017 – Leitlinie für Informationssicherheit in der Bundesverwaltung (Juli 2017).

6 Referenzarchitektur

Der vom Anforderungskatalog betrachtete Informationsverbund beinhaltet die Objekte, welche für die Ergebniszusammenstellung und -übermittlung ab dem Wahlraum nach der Stimmzettelauszählung essenziell sind. Der Untersuchungsgegenstand wird im folgenden Unterkapitel in vier Kategorien unterteilt und dazu werden die einzelnen Zielobjekte gelistet. Hierbei ist anzumerken, dass auch externe Systeme, Anwendungen oder extern unterstützte Geschäftsprozesse (Outsourcing), eine Rolle spielen und entsprechende Informationssicherheitsanforderungen für diese gelten.

6.1 Untersuchungsgegenstand

6.1.1 Infrastruktur

- Verwaltungsgebäude
- Elektrotechnische Verkabelung
- IT-Verkabelung
- Serverraum / Rechenzentrum
- Raum sowie Schrank für technische Infrastruktur
- Büroraum
- Mobiler Arbeitsplatz
- Häuslicher Arbeitsplatz
- Drucker- und Kopierraum

6.1.2 IT-Systeme

- Server
- Arbeitsplatz-PC / Laptop
- Mobiltelefon
- Smartphone und Tablet
- Netzwerk-Drucker, Drucksysteme und Multifunktionsgerät
- Virtualisierungshost
- Cloud Computing
- IBM Z-System
- Speicherlösungen
- Wechseldatenträger

6.1.3 Netze

- Behördennetzwerk
- Server- und Administrationsnetz

- Demilitarisierte Zone (DMZ)
- Netzwerk für reguläre Arbeitsplätze
- WLAN
- Gebäudeübergreifende Vernetzung
- Router
- Switch
- Firewall
- TK-Anlage und Voice-over-IP (VoIP)
- Faxgerät

6.1.4 Anwendungen / Geschäftsprozesse

- Groupware und E-Mail
- Dateiablage
- Relationale Datenbanken
- Office-Produkte
- Webbrowser
- Webanwendungen
- Mobile Anwendungen
- Benutzer-Authentifizierung
- Standardsoftware
- Individualsoftware
- Datenausgang
- Dateneingang
- Datenzusammenfassung

6.2 Netzplan

Die folgende Darstellung stellt beispielhaft die wesentlichen Objekte in vereinfachter Form schematisch dar.

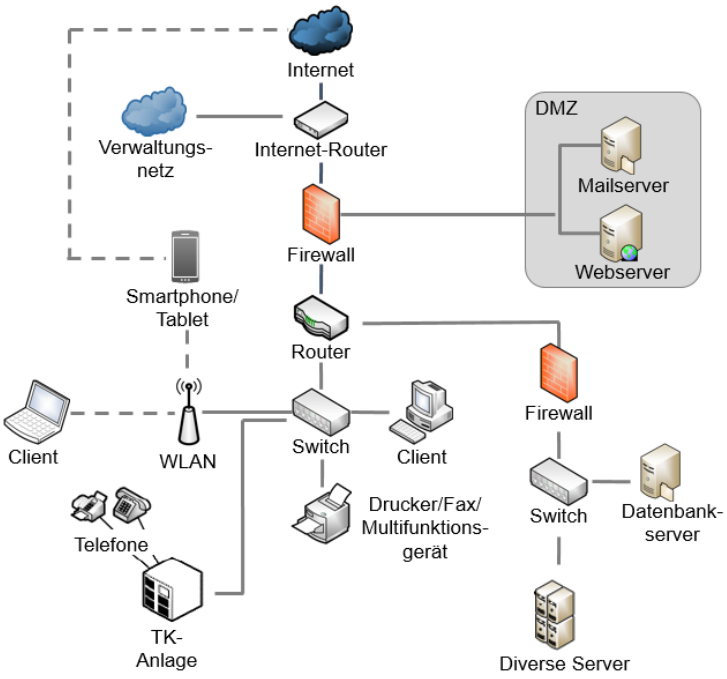

Abb. 2 Vereinfachter Netzplan

Aufgrund unterschiedlicher Modelle bei den Wahlorganen und -behörden wird auf die Darstellung von ausgelagerten Anteilen (outgesourcte Objekte) des Informationsverbunds verzichtet.

6.3 Umgang mit Abweichungen und Risiken

Die Anforderungen zu Technologien, Verfahren oder Systemen, welche das jeweilige Wahlorgan oder die jeweilige Wahlbehörde nicht bei den Schnellmeldungen einsetzen, müssen nicht beachtet werden.

Es ist stets durch die Anwender zu prüfen, ob zusätzliche Objekte zu berücksichtigen sind, welche über die Auflistung in diesem Dokument hinausgehen. Weicht der zu schützende Informationsverbund von der Referenzarchitektur ab, sind die Differenzen im Sinne weiterer eingesetzter Objekte von den Anwendern zu dokumentieren. Den zusätzlichen Objekten sind geeignete Bausteine des IT-Grundschutz-Kompendiums zuzuordnen. Existieren für ein zusätzliches Objekt keine geeigneten Bausteine, so können individuelle Bausteine mit Anforderungen erstellt werden. Das entsprechende Vorgehen wird im BSI-Standard 200-2 geschildert.

Die im Anforderungskatalog aufgeführten Anforderungen stehen in Abhängigkeit zu dem festgelegten Schutzbedarf. Insbesondere bei Abweichungen vom Modell-Informationsverbund und von dem festgelegten Schutzbedarf sind die Anwender in der Verantwortung Risikoanalysen durchzuführen. Im Rahmen der Risikoanalysen können Risiken identifiziert werden und die Anwender können diesen mit zusätzlichen risikospezifischen Anforderungen oder mit der Anpassung vorhandener Anforderungen begegnen. Letztlich sind verbleibende Risiken (Restrisiken) zu ermitteln und zu dokumentieren. In dem BSI-Standard 200-3 „Risikoanalyse auf der Basis von IT-Grundschutz“ werden die hierfür notwendigen Schritte ausführlich beschrieben. Abschließend soll angemerkt werden, dass auch wenn die dargestellten Anforderungen umgesetzt sind, gegebenenfalls Restrisiken verbleiben, die nicht mit vertretbarem Aufwand abgemildert werden können. Die Restrisiken müssen der verantwortlichen Instanz bekannt sein und von dieser akzeptiert werden.

7 Anforderungen

7.1 Methodik

Im Folgenden Teil werden die für den Informationsverbund geltenden Anforderungen tabellarisch dargestellt. Die Darstellung wurde in Anlehnung an das Schema des IT-Grundschutz-Profils „Basis-Absicherung Kommunalverwaltung“[5] erarbeitet. Zunächst werden in Kapitel 7 und Kapitel 8 die relevanten Anforderungen der Prozess-Bausteine genannt. Im jeweils nächsten Unterkapitel werden die Anforderungen der System-Bausteine zum entsprechenden Zielobjekt gemäß Referenzarchitektur aufgeführt. Darüber hinaus werden zusätzliche Anforderungen an den Bund in Kapitel 8 gelistet.

Unter Anwendung des IT-Grundschutz-Kompendiums Edition 2020 werden die IDs und die Titel der relevanten Anforderungen aufgeführt. Die „Vorausgesetzten Anforderungen“ beziehen sich auf die bereits im IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ enthaltenen Anforderungen. Diese „Vorausgesetzten Anforderungen“ werden für die Zielgruppe dieses Anforderungskatalogs als bereits umgesetzt angenommen. Jeweils in der Zeile „Weitere relevante Anforderungen“ werden die für den Informationsverbund wichtigen Anforderungen gemäß IT-Grundschutz-Methodik aufgeführt. Bei den Prozess- oder System-Bausteinen, welche für den Informationsverbund benötigt werden und die im IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ noch nicht enthalten waren, wurden die jeweiligen Zeilen in den Bausteinen bzw. Tabellen mit „Anforderungen“ bezeichnet. In jeweils dieser Zeile wurden die notwendigen Anforderungen aus dem Baustein aufgeführt. Anforderungen, welche nicht als relevant für den Geltungsbereich bewertet wurden, sind nicht gelistet worden. Bei Bedarf bzw. in Anbetracht des erhöhten Schutzbedarfs bei den Schnellmeldungen, wurden die ausgewählten Basis- oder Standard-Anforderungen um die darüber hinaus zu erfüllenden Anforderungen bei erhöhtem Schutzbedarf erweitert. Bei dem Übergang der Listung von Basis-Anforderungen zu Standard-Anforderungen und von diesen zu Anforderungen bei erhöhtem Schutzbedarf, sind die Grenzen zur jeweils nächsten Gruppe mit einem Semikolon kenntlich gemacht. Gelten zu den Aspekten in der Zeile „Vorausgesetzte Anforderungen“ keine weiteren Anforderungen, so sind in der Zelle jeweils drei Striche („---") vermerkt.

Es ist darauf hinzuweisen, dass für die Umsetzung der Anforderungen jeweils die gesamte Beschreibung der Anforderung aus dem IT-Grundschutz-Kompendium hinzuzuziehen und zu berücksichtigen ist.

In vielen Bausteinen wurden Hinweise zur Abgrenzung und Anwendung gegeben. Unter „Besonderheiten“ werden die für die Zielgruppe und den Informationsverbund spezifischen Aspekte aufgeführt. Dabei wurden die im IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ enthaltenen Besonderheiten nicht nochmals aufgeführt, sondern die nennenswerten Aspekte mit Blick auf den Prozess der Schnellmeldungen aufgeführt. Die formulierten Besonderheiten in den IT-Grundschutz-Bausteinen dieses Anforderungskatalogs sind als Spezifizierung bzw. Konkretisierung zu verstehen. Existieren keine nennenswerten Spezifizierungen, so sind in der Zelle jeweils drei Striche („---") vermerkt.

Zum erleichterten Verständnis ist das Schema mit Erläuterungen nachfolgend dargestellt.

Umsetzungs-reihenfolge	Die für die Umsetzung der Anforderungen empfohlene Reihenfolge (Definitionen hierzu in Kapitel 4.4.2 „Reihenfolge der Anforderungen")
Vorausgesetzte Anforderungen	Anforderungen aus dem IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ (2019)
Weitere relevante Anforderungen	Die für Schnellmeldungen als relevant eingeschätzten Anforderungen (welche noch nicht im IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ aus 2019 enthalten waren)
Hinweis	Abgrenzungen, Empfehlungen, Anwendungsbereich

[5] Hinweis: Das IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ bezieht sich auf das IT-Grundschutz-Kompendium 2019.

Umsetzungs-reihenfolge	Die für die Umsetzung der Anforderungen empfohlene Reihenfolge (Definitionen hierzu in Kapitel 4.4.2 „Reihenfolge der Anforderungen")
Besonderheiten	Zum Prozess der Schnellmeldungen spezifische Anmerkungen und Erläuterungen für die Adressaten zu ausgewählten Anforderungen

Gemäß Formatvorlage wird bei Tabellen, welche über mehrere Seiten gehen, jeweils die Kopfzeile auf der Folgeseite wiederholt.

Das nächste Beispiel soll den Fall veranschaulichen, wenn es keine Anforderungen zu einem Objekt im IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ gab und somit die Zeile „Vorausgesetzte Anforderungen“ nicht aufgeführt wurde. Die neu ausgewählten Aspekte wurden mit „Anforderungen“ bezeichnet.

Umsetzungs-reihenfolge	Die für die Umsetzung der Anforderungen empfohlene Reihenfolge (Definitionen hierzu in Kapitel 4.4.2 „Reihenfolge der Anforderungen“)
Anforderungen	Die für Schnellmeldungen als relevant eingeschätzten Anforderungen (welche noch nicht im IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ aus 2019 enthalten waren)
Hinweis	Abgrenzungen, Empfehlungen, Anwendungsbereich
Besonderheiten	Zum Prozess der Schnellmeldungen spezifische Anmerkungen und Erläuterungen für die Adressaten zu ausgewählten Anforderungen

Wie im obigen Abschnitt beschrieben, wurde diese Form dem Fall entsprechend angepasst. Falls bspw. keine Bemerkung notwendig war, wurde die Zeile „Hinweis“ nicht abgebildet.

Übergreifend ist anzumerken, dass die relevanten Anforderungen bei externen Systemen, Anwendungen oder extern unterstützten Geschäftsprozessen (Outsourcing), auch an die entsprechenden Dienstleister gestellt werden müssen.

In mehreren Bausteinen ist eine Sicherheitsrevision Bestandteil der Anforderungen. Die Durchführung dieser Sicherheitsrevisionen liegt in der Verantwortung der Wahlleiter, während der Informationssicherheitsbeauftragte (ISB), sofern vorhanden, dazu an den Wahlleiter berichtet.

7.2 Prozess-Bausteine

Die folgenden Prozess-Bausteine sind, wenn nicht anders angegeben, einmal auf den gesamten Informationsverbund anzuwenden.

ISMS.1 – Sicherheitsmanagement

Umsetzungs-reihenfolge	R1
Vorausgesetzte Anforderungen	ISMS.1.A1: Gesamtverantwortung für Informationssicherheit durch die Leitungsebene ISMS.1.A2: Sicherheitsziele und -strategie ISMS.1.A3: Erstellung einer Leitlinie zur Informationssicherheit ISMS.1.A4: Benennung eines Informationssicherheitsbeauftragten ISMS.1.A5: Vertragsgestaltung bei Bestellung eines externen ISBs ISMS.1.A6: Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit ISMS.1.A7: Festlegung von Sicherheitsmaßnahmen ISMS.1.A8: Integration der Mitarbeiter in den Sicherheitsprozess ISMS.1.A9: Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse
Weitere relevante Anforderungen	ISMS.1.A10: Erstellung eines Sicherheitskonzepts ISMS.1.A11: Aufrechterhaltung der Informationssicherheit ISMS.1.A13: Dokumentation des Sicherheitsprozesses ISMS.1.A14: Sensibilisierung zur Informationssicherheit ISMS.1.A16: Erstellung von zielgruppengerechten Sicherheitsrichtlinien
Besonderheiten	ISMS.1.A10 Als Mindestanforderung sollte ein Sicherheitskonzept erstellt werden, welches die Ermittlung des vorläufigen Wahlergebnisses adressiert. ISMS.1.A11 Bei der regelmäßigen Durchführung der Sicherheitsrevisionen sollte eine Orientierung am Sicherheitskonzept mit dem entsprechenden Fokus der Schnellmeldungen erfolgen. ISMS.1.A13 Bei dieser Anforderung liegt der Fokus auf der Dokumentation des Sicherheitsprozesses für das vorläufige Wahlergebnis. ISMS.1.A15 Für die Schnellmeldungen sollte eine Planung der personellen und technischen Ressourcen für die Informationssicherheit erfolgen. ISMS.1.A16 Für den Prozess der Schnellmeldungen sollten für die Beteiligten zielgruppengerechte Richtlinien oder sonstige dokumentierte Arbeitsanweisungen zur Verfügung gestellt werden.

ORP.1 – Organisation

Umsetzungs-reihenfolge	R1
Vorausgesetzte Anforderungen	ORP.1.A1: Festlegung von Verantwortlichkeiten und Regelungen ORP.1.A2: Zuweisung der Verantwortung ORP.1.A3: Beaufsichtigung oder Begleitung von Fremdpersonen ORP.1.A4: Funktionstrennung zwischen unvereinbaren Aufgaben ORP.1.A5: Vergabe von Berechtigungen; ORP.1.A6: Schutz von sensiblen Informationen am Arbeitsplatz
Weitere relevante Anforderungen	ORP.1.A8: Betriebsmittelverwaltung ORP.1.A10: Reaktion auf Verletzungen der Sicherheitsvorgaben ORP.1.A12: Regelungen für Wartungs- und Reparaturarbeiten ORP.1.A13: Sicherheit bei Umzügen
Hinweis	Der Baustein behandelt übergreifende Aspekte zur Umsetzung von Informationssicherheit. ORP.1 ist auf den gesamten Informationsverbund mindestens einmal anzuwenden. Wenn Teile des Informationsverbunds einer anderen Organisationseinheit zugeordnet sind und daher anderen Rahmenbedingungen unterliegen, sollte der Baustein auf jede Einheit separat angewandt werden.
Besonderheiten	ORP.1.A8 Für den Wahlabend sollte ausreichend Hardware (z.B. Ersatzgeräte) bereitgestellt werden, sodass auch bei Ausfall eines Client-PCs bspw., die Aufbereitung und Übermittlung der vorläufigen Ergebnisse möglichst nur geringfügig verzögert werden. ORP.1.A10 Es sollte festgelegt sein, welche Reaktionen bei Verdacht auf Verletzungen der Sicherheitsvorgaben erfolgen. Fehlende Regelungen können zu massiven Sicherheitslücken führen, wenn bspw. die Mitglieder bzw. Beschäftigten nicht wissen, wie sie bei Vorfällen reagieren sollen. ORP.1.A12 Wartungs- und Reparaturarbeiten sollten geregelt sein. Hierbei sollten Verantwortlichkeiten geklärt werden, denn bei externen Reparaturen oder Wartungen von Geräten können diese manipuliert werden. Anfallende Wartungen sollten zudem zeitlich sinnvoll organisiert werden, um die Schnellmeldungen nicht zu gefährden. ORP.1.A13 Sofern in größerem Ausmaß IT zum Zwecke der Schnellmeldungen verlagert wird (z.B. ganze Serverracks), sollten dazu entsprechende Sicherheitsrichtlinien zum Umzug erarbeitet werden.

ORP.2 - Personal

Umsetzungs-reihenfolge	R1
Vorausgesetzte Anforderungen	ORP.2.A1: Geregelte Einarbeitung neuer Mitarbeiter ORP.2.A2: Geregelte Verfahrensweise beim Weggang von Mitarbeitern ORP.2.A3: Festlegung von Vertretungsregelungen ORP.2.A4: Festlegung von Regelungen für den Einsatz von Fremdpersonal ORP.2.A5: Vertraulichkeitsvereinbarungen für den Einsatz von Fremdpersonal; ORP.2.A6: Überprüfung von Kandidaten bei der Auswahl von Personal ORP.2.A7: Überprüfung der Vertrauenswürdigkeit von Mitarbeitern ORP.2.A9: Schulung von Mitarbeitern
Weitere relevante Anforderungen	ORP.2.A8: Aufgaben und Zuständigkeiten von Mitarbeitern Zusätzliche Anforderung zu personellen Änderungen am Wahlabend
Hinweis	Der Baustein ist für das bei der Ermittlung des vorläufigen Wahlergebnisses eingebundene Personal anzuwenden.
Besonderheiten	ORP.2.A8 Die Verantwortlichkeiten des an den Schnellmeldungen beteiligten Personals sollten klar dokumentiert sein. Die festgelegten Zuständigkeiten und Aufgaben sollten rechtzeitig vor dem Wahltag allen Beteiligten bekannt sein. Personelle Änderungen am Wahlabend Im Falle von Personalausfall sind die aufgrund der Abgabe oder des Empfangs von Meldungen direkt beteiligten Stellen umgehend über die Änderungen zu informieren. Auf Seiten der meldenden Gemeinden ist der Kreiswahlleiter in Kenntnis zu setzen. Bei der Landeswahlleitung ist die Bundeswahlleitung in Kenntnis zu setzen.

ORP.3 - Sensibilisierung und Schulung

Umsetzungs-reihenfolge	R1
Vorausgesetzte Anforderungen	ORP.3.A1: Sensibilisierung der Institutionsleitung für Informationssicherheit ORP.3.A2: Ansprechpartner zu Sicherheitsfragen ORP.3.A3: Einweisung des Personals in den sicheren Umgang mit IT; ORP.3.A6: Planung und Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit; ORP.3.A9: Spezielle Schulung von exponierten Personen und Institutionen
Weitere relevante Anforderungen	ORP.3.A4: Konzeption eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit ORP.3.A5: Analyse der Zielgruppen für Sensibilisierungs- und Schulungsprogramme

Umsetzungs-reihenfolge	R1
Besonderheiten	ORP.3.A4 Für die Sensibilisierung zu wichtigen Informationssicherheitsthemen im Rahmen der Schnellmeldungen sollte ein Schulungsprogramm für die Mitarbeiter erstellt werden. ORP.3.A6 Alle Beteiligten, die bei der Ermittlung der vorläufigen Wahlergebnisse mitwirken, sollten vor ihrem Einsatz ihren Funktionen gemäß in geeigneter Weise informiert oder geschult werden. (Zu den Beteiligten gehören auch ehrenamtliche Wahlhelfer.) ORP.3.A9 Das beteiligte Personal sollte zu möglichen Gefährdungen sowie geeigneten Verhaltensweisen unterrichtet werden.

ORP.4 - Identitäts- und Berechtigungsmanagement

Umsetzungs-reihenfolge	R1
Vorausgesetzte Anforderungen	ORP.4.A1: Regelung für die Einrichtung und Löschung von Benutzern und Benutzergruppen ORP.4.A2: Regelung für Einrichtung, Änderung und Entzug von Berechtigungen ORP.4.A3: Dokumentation der Benutzerkennungen und Rechteprofile ORP.4.A4: Aufgabenverteilung und Funktionstrennung ORP.4.A5: Vergabe von Zutrittsberechtigungen ORP.4.A6: Vergabe von Zugangsberechtigungen ORP.4.A7: Vergabe von Zugriffsrechten ORP.4.A8: Regelung des Passwortgebrauchs ORP.4.A9: Identifikation und Authentisierung; ORP.4.A19: Einweisung aller Mitarbeiter in den Umgang mit Authentisierungsverfahren und -mechanismen
Weitere relevante Anforderungen	ORP.4.A22: Regelung zur Passwortqualität ORP.4.A23: Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme; ORP.4.A10: Schutz von Benutzerkennungen mit weitreichenden Berechtigungen ORP.4.A11: Zurücksetzen von Passwörtern ORP.4.A12: Entwicklung eines Authentisierungskonzeptes für IT-Systeme und Anwendungen ORP.4.A13: Geeignete Auswahl von Authentisierungsmechanismen ORP.4.A14: Kontrolle der Wirksamkeit der Benutzertrennung am IT-System bzw. Anwendung ORP.4.A15: Vorgehensweise und Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement ORP.4.A16: Richtlinien für die Zugriffs- und Zugangskontrolle ORP.4.A17: Geeignete Auswahl von Identitäts- und Berechtigungsmanagement-Systemen ORP.4.A18: Einsatz eines zentralen Authentisierungsdienstes
Hinweis	Die Anwendung dieses Bausteins gilt für die Systeme, welche im Kontext der Schnellmeldungen ein Risiko für Integrität und Verfügbarkeit der Daten bergen.

Umsetzungs-reihenfolge	R1
Besonderheiten	ORP.4.A23 Um die Integrität der zu verarbeitenden Wahldaten zu gewährleisten, müssen Standardpasswörter durch ausreichend starke Passwörter ersetzt und vordefinierte Kennungen geändert werden. Zudem müssen Passwörter sicher gespeichert werden. Sie sollten nur verschlüsselt übertragen werden. ORP.4.A12 Das Authentisierungskonzept sollte für die relevanten Systeme zu den Schnellmeldungen erstellt werden. ORP.4.A14 Es sollte kontrolliert werden, dass nicht mehrere Benutzer unter der gleichen Kennung arbeiten, um Prävention zu betreiben vor fälschlichen Meldungen der Ergebnisse durch Unbefugte. ORP.4.A16 Eine schriftliche Zugriffsregelung im Sinne einer Richtlinie für die Zugriffs- und Zugangskontrollen der betroffenen Systeme bei den Schnellmeldungen sollte erstellt werden. ORP.4.A.17 Diese Anforderung ist relevant, wenn die Wahlsoftware ein eigenes komplexes Rechteverwaltungssystem besitzt. ORP.4.A18 Mindestens für die IT-Systeme, welche für die Schnellmeldungen genutzt werden, sollte der Einsatz eines zentralen Authentisierungsdienstes, bspw. File Share, geplant und dieser genutzt werden.

CON.1 – Kryptokonzept

Umsetzungs-reihenfolge	R2
Anforderungen	CON.1.A1: Auswahl geeigneter kryptografischer Verfahren; CON.1.A3: Verschlüsselung der Kommunikationsverbindungen CON.1.A4: Geeignetes Schlüsselmanagement; CON.1.A9: Auswahl eines geeigneten kryptografischen Produkts CON.1.A10: Entwicklung eines Kryptokonzepts CON.1.A11: Sichere Konfiguration der Kryptomodule
Hinweis	Dieser Baustein enthält Anforderungen an kryptografische Verfahren für den Einsatz bei den Schnellmeldungen und ist auf den gesamten Informationsverbund einmal anzuwenden.
Besonderheiten	---

CON.4 – Auswahl und Einsatz von Standardsoftware

Umsetzungs-reihenfolge	R1
Vorausgesetzte Anforderungen	CON.4.A1: Sicherstellen der Integrität von Standardsoftware CON.4.A2: Entwicklung der Installationsanweisung für Standardsoftware CON.4.A3: Sichere Installation und Konfiguration von Standardsoftware; CON.4.A4: Festlegung der Verantwortlichkeiten im Bereich Standardsoftware CON.4.A6: Auswahl einer geeigneten Standardsoftware CON.4.A7: Überprüfung der Lieferung von Standardsoftware CON.4.A8: Lizenzverwaltung und Versionskontrolle von Standardsoftware
Weitere relevante Anforderungen	CON.4.A5: Erstellung eines Anforderungskatalogs für Standardsoftware; CON.4.A10: Implementierung zusätzlicher Sicherheitsfunktionen CON.4.A11: Nutzung zertifizierter Standardsoftware CON.4.A12: Einsatz von Verschlüsselung, Checksummen oder digitalen Signaturen
Hinweis	CON.4 ist für den gesamten Informationsverbund einmal anzuwenden, wenn Standardsoftware beschafft, deren Betrieb geregelt oder diese ausgesondert werden soll. Dieser Baustein befasst sich ausschließlich mit standardisierten Programmen, die von Anwendern selbstständig für die Ermittlung des vorläufigen Wahlergebnisses eingesetzt und angepasst werden können, ohne Unterstützung durch Hersteller oder externe Dienstleister.
Besonderheiten	CON.4.A5 Die relevanten Inhalte dieses Dokuments sollten für die Erstellung eines Anforderungskatalogs für Standardsoftware berücksichtigt werden. CON.4.A6 Auf cloudbasierte Software und deren Funktionen sollte verzichtet werden, sofern diese nicht unter vollständiger Kontrolle der Anwender läuft. CON.4.A7 Alle Software-Lizenzen sollten in Listen oder Programmen dokumentiert und gepflegt werden.

CON.5 – Entwicklung und Einsatz von Individualsoftware

Umsetzungs-reihenfolge	R1
Anforderungen	CON.5.A1: Festlegung benötigter Sicherheitsfunktionen der Individualsoftware CON.5.A3: Sichere Installation von Individualsoftware CON.5.A4: Heranführen von Benutzerinnen und Benutzern an Individualsoftware; CON.5.A6: Dokumentation der Anforderungen an die Individualsoftware CON.5.A8: Geeignete Steuerung der Anwendungsentwicklung CON.5.A11: Geeignete und rechtskonforme Beschaffung; CON.5.A12: Treuhänderische Hinterlegung CON.5.A13: Entwicklung eines Redundanzkonzeptes für Anwendungen
Hinweis	Dieser Baustein ist für einzelne, individuell entwickelte Anwendungen zu nutzen, welche bei der Ermittlung des vorläufigen Wahlergebnisses eingesetzt werden.

Umsetzungs-reihenfolge	R1
Besonderheiten	CON.5.A1 Die Sicherheitsfunktionen für die Individualsoftware müssen unter Berücksichtigung verbundener Prozesse und des Schutzbedarfs der verarbeiteten Informationen dokumentiert werden. CON.5.A4 Mittels Einweisungen und Handbüchern müssen sowohl Nutzer als auch Administratoren zum sicheren Umgang mit der Software geschult werden. CON.5.A11 Aufgrund von unzureichenden vertraglichen Regelungen mit externen Dienstleistern können schwerwiegende Sicherheitsprobleme bei der Erstellung, Implementierung, Unterstützung und bei der Wartung der Anwendung auftreten. Daher sollten auch wichtige Sicherheitsaspekte in den Verträgen behandelt werden.

CON.8 - Software-Entwicklung

Umsetzungs-reihenfolge	R1
Anforderungen	CON.8.A1: Definition von Rollen und Verantwortlichkeiten CON.8.A2: Auswahl eines Vorgehensmodells CON.8.A3: Auswahl einer Entwicklungsumgebung CON.8.A4: Einhaltung einer sicheren Vorgehensweise CON.8.A5: Sicheres Systemdesign CON.8.A6: Verwendung von Bibliotheken aus vertrauenswürdigen Quellen CON.8.A7: Anwendung von Testverfahren CON.8.A8: Bereitstellung von Patches, Updates und Änderungen CON.8.A9: Berücksichtigung von Compliance-Anforderungen CON.8.A10: Versionsverwaltung des Quellcodes; CON.8.A11: Erstellung einer Richtlinie für die Software-Entwicklung CON.8.A12: Ausführliche Dokumentation CON.8.A13: Beschaffung von Werkzeugen CON.8.A14: Schulung des Projektteams zur Informationssicherheit CON.8.A15: Sicherer Einsatz der Test- und Entwicklungsumgebungen CON.8.A16: Geeignete Steuerung der Software-Entwicklung; CON.8.A17: Auswahl vertrauenswürdiger Entwicklungswerkzeuge CON.8.A18: Regelmäßige Sicherheitsaudits für die Entwicklungsumgebung Zusätzliche Anforderungen zu Individueller Datenverarbeitung (IDV)
Hinweis	Der Baustein CON.8 ist für den gesamten Informationsverbund einmal anzuwenden, wenn Software für die Unterstützung der Ermittlung des vorläufigen Wahlergebnisses entwickelt werden soll. Zudem werden Anforderungen an IDV[6] beschrieben.

[6] IDV sind von den Fachbereichen selbst entwickelte Anwendungen, bei der Benutzer eine Arbeitstätigkeit definieren und ausführen. IDV umfasst Änderungen von Daten und Inhalten oder die Verarbeitung von Daten, die als Dateneingabe für andere betriebliche Prozesse verwendet werden. Dies geschieht durch den Einsatz individuell definierter Funktionalitäten auf der Basis von Standardsoftware, typischerweise Büro-Desktop-Anwendungen oder Anwendungen für statistische Auswertungen.

Umsetzungs-reihenfolge	R1
Besonderheiten	CON.8.A5 Bei der Entwicklung von Software zum Einsatz im Prozess der Schnellmeldungen müssen die Grundregeln des sicheren Systemdesigns eingehalten werden. CON.8.A12 Eine sorgfältige Dokumentation der Programmierung ist notwendig, um beispielsweise falsche Arbeitsergebnisse, Störungen des IT-Betriebs oder Verzögerungen des Arbeitsablaufs zu vermeiden. CON.8.A15 Wenn die Entwicklungsumgebung unzureichend gesichert eingesetzt wird, kann die zu produzierende Anwendung manipuliert werden. Die Test- und Entwicklungsumgebungen sollten getrennt von der Produktionsumgebung betrieben werden. CON.8.A16 Wenn nicht geprüft wird, ob die eigenentwickelte Software sicher implementiert wird, drohen Schwachstellen in der ausgelieferten Software. Daher sollten die Qualitätssicherung und das Risikomanagement in den Entwicklungsprozess verankert werden.

Umsetzungs-reihenfolge	R1
Besonderheiten IDV	Folgende weitere Anforderungen sind bei der Entwicklung von Individueller Datenverarbeitung (IDV) zu berücksichtigen: Einheitlicher Prozess für IDV Es sollte ein einheitlicher Prozess zur Identifizierung und Nutzung von IDV innerhalb der Wahlbehörde festgelegt werden. Nachvollziehbare Dokumentation für IDV Der Entwicklungsprozess der betroffenen IDV sollte nachvollziehbar dokumentiert sein. Versionsverwaltung für IDV Es sollte eine geeignete Versionsverwaltung für IDV durchgeführt werden. Zudem sollte den Anwendern stets die aktuellste Version zur Verfügung gestellt werden, sobald sie für den Produktionsbetrieb abgenommen ist. Es sollte ein geschützter und robuster Update-Pfad eingerichtet werden. Datensicherung bei IDV Die IDV müssen die in der Wahlbehörde geltenden Vorgaben zur Datenverarbeitung und -sicherung erfüllen. Testen und Qualitätsprüfung bei IDV Bei der Entwicklung für die Anwendungen zur IDV sollte nach einem definierten Testverfahren getestet werden und eine Qualitätssicherung durchgeführt sowie dokumentiert werden. Trennung von Umgebungen Die Test-, Entwicklungs- und Produktionsumgebungen sollten getrennt sein. Im Kontext von IDV muss eine Umgebung nicht eine physisch getrennte Umgebung sein, geeignete logische Zugriffsbeschränkungen können ebenfalls eingesetzt werden. IDV-Inventar Abteilung soll ein zentrales Inventar für kritische IDV führen, in dem alle relevanten IDV-Instanzen inventarisiert werden. Dieses Inventar soll die wesentlichen Informationen zu der IDV enthalten.

CON.9 – Informationsaustausch

Umsetzungs-reihenfolge	R1
Anforderungen	CON.9.A1: Festlegung zulässiger Empfänger CON.9.A2: Regelung des Informationsaustausches CON.9.A3: Unterweisung des Personals zum Informationsaustausch; CON.9.A4: Vereinbarungen zum Informationsaustausch mit Externen CON.9.A5: Beseitigung von Restinformationen in Dateien vor Weitergabe CON.9.A6: Kompatibilitätsprüfung des Sender- und Empfängersystems CON.9.A8: Verschlüsselung und Signatur Zusätzliche Anforderung zur Authentisierung bei Übermittlung per Bote, Fax oder Telefon

Umsetzungs-reihenfolge	R1
Hinweis	Dieser Baustein ist einmal auf den gesamten Informationsverbund anzuwenden, wenn Informationen mit Stellen außerhalb der eigenen Wahlbehörde ausgetauscht werden sollen und dabei nicht das interne Datennetz verwendet wird. Bei komplexen Informationsverbünden ist CON.9 auch für jeden Informationsaustausch zwischen Standorten anzuwenden. Insbesondere wenn neue Transportwege aufgebaut werden, wie z. B. mit neuen Kommunikationspartnern, über neue Medien oder neue Datennetze, sind diese Anforderungen relevant.
Besonderheiten	CON.9.A1 Zwischen den Beteiligten sowie in den Wahlbehörden selbst, muss festgelegt werden, welche Empfänger die vorläufigen Wahlergebnisse erhalten und weitergeben dürfen, um zu vermeiden, dass vertrauliche Informationen in unbefugte Hände gelangen oder das gewünschte Ziel nicht rechtzeitig erreicht wird. CON.9.A3 Das Personal, welches bei Dateneingang, -zusammenfassung oder -ausgang zu den Schnellmeldungen eingesetzt wird, muss über die Regeln für einen sicheren Informationsaustausch rechtzeitig vor Tätigkeitsbeginn unterwiesen werden. CON.9.A6 Auch eine Kompatibilitätsprüfung sollte im Rahmen des Testens von unterstützender Software zur Wahlergebnisermittlung stattfinden. Authentisierung bei Übermittlung per Bote, Fax oder Telefon Bei der Übermittlung von Wahlergebnissen per Bote, Fax oder Telefon muss eine sichere Authentisierung erfolgen. Die Verifizierung der übergebenen Wahlergebnisse sollte ab der Gemeindeebene durch einen authentisierten zweiten Kanal oder durch Einsatz von Plausibilisierungsregeln durchgeführt werden.

Bring Your Own Device

Umsetzungs-reihenfolge	R2
Anforderungen	[Neue Anforderungen zu „Bring Your Own Device“ (BYOD)]
Hinweis	Dieser zusätzlich konzipierte Baustein ist relevant, wenn private Geräte der Mitglieder bzw. Beschäftigten, die nicht im Einfluss des Arbeitgebers stehen, bei der Ermittlung der vorläufigen Wahlergebnisse eingesetzt werden. Hervorzuheben ist hierbei die Empfehlung zur kritischen Prüfung, ob private Geräte prinzipiell zugelassen oder zumindest für die Schnellmeldungen untersagt werden sollten.

Umsetzungs-reihenfolge	R2
Besonderheiten	Konzept für BYOD Wahlorgane und -behörden müssen festlegen, ob BYOD ein zulässiges Betriebsszenario ist und in welcher Form der Einsatz von BYOD für die Schnellmeldungen sinnvoll sowie akzeptabel ist. Dazu sollte analysiert und bewertet werden, ob und für wen BYOD zur Ermittlung des vorläufigen Wahlergebnisses zur Verfügung stehen sollte. Absicherung des Geräts vor fremdem Zugriff Das Gerät muss ausreichend vor fremden Zugriffen abgesichert sein. Sichere Kommunikationsverbindung Die Nutzung der Datendienste sollte über eine abgesicherte Kommunikationsverbindung erfolgen. Angemessene Schnittstellen sowie eine entsprechende Dokumentation sollten hierbei sichergestellt werden. Liste unterstützter Geräte und Plattformen Es sollte eine verbindliche Aufstellung zugelassener Geräte und empfohlener bzw. kompatibler Plattformen zur Verfügung gestellt und regelmäßig aktualisiert werden. Geräte, die nicht mehr mit Sicherheitsupdates vom Hersteller versorgt werden, müssen von der Nutzung ausgeschlossen werden. Aktivierung automatischer Updates Zur Einschränkung möglicher Sicherheitslücken sollte die automatische Installation von Updates auf den genutzten Geräten aktiviert sein. Die Geräte müssen auf dem aktuellen Update-Stand sein. Die Sicherheitsmechanismen von mobilen Endgeräten dürfen nicht deaktiviert sein oder umgangen werden. Sensibilisierung für BYOD Der Einsatz von BYOD ändert die Gefährdungslage der Nutzer. Diese sollten auf die Nutzung im Wahlprozess angemessen sensibilisiert sein. Insbesondere Gefährdungen am Wahltag und entsprechende Vorsichtsmaßnahmen sollten hierbei den Betroffenen aufgezeigt werden. Ein Leitfaden für die sichere Nutzung sollte zur Verfügung gestellt werden. Einschränkung der Nutzung von Software Der Einsatz bestimmter Anwendungen kann zu Risiken führen. Es sollte eine Ausschlussliste risikobehafteter Software geführt werden. Systemabsicherung Antivirus-Programme sowie Firewalls bieten eine technische Grundlage für den sicheren Systembetrieb. Genutzte Privatgeräte müssen daher durch Firewalls geschützt sein. Verschlüsselung tragbarer IT-Systeme Mobile Geräte sollten verschlüsselt werden, um unbefugte Zugriffe auf die Daten des Geräts zu vermeiden.

OPS.1.1.2 - Ordnungsgemäße IT-Administration

Umsetzungs-reihenfolge	R1
Vorausgesetzte Anforderungen	OPS.1.1.2.A1: Personalauswahl für administrative Tätigkeiten OPS.1.1.2.A2: Vertretungsregelungen und Notfallvorsorge OPS.1.1.2.A3: Geregelte Einstellung von IT-Administratoren OPS.1.1.2.A4: Beendigung der Tätigkeit als IT-Administrator OPS.1.1.2.A5: Nachweisbarkeit von administrativen Tätigkeiten OPS.1.1.2.A6: Schutz administrativer Tätigkeiten; OPS.1.1.2.A7: Regelung der IT-Administrationstätigkeit OPS.1.1.2.A8: Administration von Fachanwendungen OPS.1.1.2.A9: Ausreichende Ressourcen für den IT-Betrieb OPS.1.1.2.A12: Regelungen für Wartungs- und Reparaturarbeiten; OPS.1.1.2.A18: Durchgängige Protokollierung administrativer Tätigkeiten
Weitere relevante Anforderungen	OPS.1.1.2.A11: Dokumentation von IT-Administrationstätigkeiten
Hinweis	OPS.1.1.2 ist auf den Informationsverbund anzuwenden, wenn die IT von der Wahlbehörde selbst administriert wird.
Besonderheiten	OPS.1.1.2.A18 Für die Ebenen Land und Bund sollten alle administrativen Zugriffe bei besonders sicherheitskritischen IT-Systemen durchgängig und vollständig protokolliert werden.

OPS.1.1.3 - Patch- und Änderungsmanagement

Umsetzungs-reihenfolge	R1
Vorausgesetzte Anforderungen	OPS.1.1.3.A1: Konzept für das Patch- und Änderungsmanagement OPS.1.1.3.A2: Festlegung der Verantwortlichkeiten OPS.1.1.3.A3: Konfiguration von Autoupdate-Mechanismen
Weitere relevante Anforderungen	OPS.1.1.3.A4: Planung des Änderungsmanagementprozesses OPS.1.1.3.A5: Umgang mit Änderungsanforderungen OPS.1.1.3.A6: Abstimmung von Änderungsanforderungen OPS.1.1.3.A8: Sicherer Einsatz von Werkzeugen für das Patch- und Änderungsmanagement OPS.1.1.3.A9: Test- und Abnahmeverfahren für neue Hard- und Software OPS.1.1.3.A10: Sicherstellung der Integrität und Authentizität von Softwarepaketen OPS.1.1.3.A11: Kontinuierliche Dokumentation der Informationsverarbeitung OPS.1.1.3.A.14: Synchronisierung innerhalb des Änderungsmanagements Zusätzliche Anforderung zu einer Frozen Zone
Hinweis	Das Patchmanagement stellt einen speziellen Prozess innerhalb des Änderungsmanagements dar, der auf die Aktualisierung von Software abzielt und auf den gesamten Informationsverbund anzuwenden ist.

Umsetzungs-reihenfolge	R1
Besonderheiten	OPS.1.1.3.A1 Das Konzept für das Patch- und Änderungsmanagement sollte insbesondere regeln, welche Arten von Patches eingespielt werden dürfen. Hierbei sollte eine Klassifizierung nach Wichtigkeit und Dringlichkeit vorgenommen werden. Der Erhalt des (angestrebten) Sicherheitsniveaus muss während und nach dem Patchen gewährleistet werden. OPS.1.1.3.A5 Änderungsanträge sollten nach einem definierten Verfahren eingereicht und bearbeitet werden. Werden Änderungen falsch priorisiert und wichtige Patches zu spät installiert, bleiben Sicherheitslücken länger bestehen. OPS.1.1.3.A6 Für die Schnellmeldungen sollte es ein festgelegtes Verfahren geben, um die Bewertung dringend notwendiger Änderungsanforderungen beschleunigen zu können. OPS.1.1.3.A11 Diese Anforderung gilt für die relevanten Programme im Prozess der Schnellmeldung. OPS.1.1.3.A14 Cold-Stand-By-Systeme sollten den gleichen Patch-Stand wie die Produktivsysteme haben. Frozen Zone Vor dem Wahltag sollte mit einem ausreichenden zeitlichen Abstand eine „Frozen Zone“[7] eingerichtet werden, um zu vermeiden, dass Konfigurationen, unter denen z.B. Tests erfolgreich gelaufen sind, nachträglich und damit kurzfristig vor dem Wahltag wieder verändert werden.

[7] Frozen Zone bezeichnet den Zeitraum, in dem Änderungen nicht zugelassen sind.

OPS.1.1.4 - Schutz vor Schadprogrammen

Umsetzungs-reihenfolge	R1
Vorausgesetzte Anforderungen	OPS.1.1.4.A1: Erstellung eines Konzepts für den Schutz vor Schadprogrammen OPS.1.1.4.A2: Nutzung systemspezifischer Schutzmechanismen OPS.1.1.4.A3: Auswahl eines Virenschutzprogrammes für Endgeräte OPS.1.1.4.A4: Auswahl eines Virenschutzprogrammes zum Datenaustausch OPS.1.1.4.A5: Betrieb und Konfiguration von Virenschutzprogrammen OPS.1.1.4.A6: Regelmäßige Aktualisierung eingesetzter Virenschutzprogramme und Signaturen OPS.1.1.4.A7: Sensibilisierung und Verpflichtung der Benutzer
Weitere relevante Anforderungen	OPS.1.1.4.A8: Nutzung von Cloud-Diensten zur Detektionsverbesserung OPS.1.1.4.A9: Meldung von Infektionen mit Schadprogrammen; OPS.1.1.4.A10: Nutzung spezieller Analyseumgebungen OPS.1.1.4.A11: Einsatz mehrerer Scan-Engines OPS.1.1.4.A13: Umgang mit nicht vertrauenswürdigen Dateien OPS.1.1.4.A14: Auswahl und Einsatz von Cyber-Sicherheitsprodukten gegen gezielte Angriffe
Besonderheiten	OPS.1.1.4.A1 Es muss ein Konzept erstellt werden, das beschreibt, welche IT-Systeme vor Schadprogrammen geschützt werden müssen. Sollten im Kontext der Schnellmeldungen Systeme genutzt werden, die nachweislich falsche Warnungen in der verwendeten Softwarelösung gegen Schadprogramme auslösen, können diese unter Anwendung anderer kompensierender Maßnahmen von dieser Anforderung ausgenommen werden. OPS.1.1.4.A3 Klassische Virenschutzprogramme ermitteln Bedrohungen aufgrund von fortlaufend aktualisierten Signaturen und können vor bekannten Viren und Schadsoftware schützen. Die Wirksamkeit gegen individualisierte Angriffe ist jedoch gering. Für die konkreten Einsatzzwecke müssen entsprechende Schutzprogramme ausgewählt und installiert werden. OPS.1.1.4.A8 Zur Verbesserung der Detektionsleistung von Virenschutzprogrammen sollten Cloud-Dienste genutzt werden. Der Einsatz dieser Lösungen sollte mit großer Sorgfalt geprüft und Risiken abgewogen werden. OPS.1.1.A10 Eine automatisierte Analyse in einer gesicherten Testumgebung (Sandbox) sollte zur Prüfung von Anhängen in E-Mails vor der internen Auslieferung genutzt werden. OPS.1.1.A14 Neben den klassischen Virenschutzlösungen bieten sogenannte Endpoint Protection Produkte zusätzlich zu dem Schutz vor Viren, Schadsoftware und Spionagesoftware, auch zum Beispiel Schutz gegen Phishing, Interprozesskommunikation im Speicher oder Rechteerwerb durch Overflows. Mit Hilfe von statistischen Methoden und maschinellem Lernen können auch unbekannte Angriffsszenarien erkannt und potenziell gefährliche Vorgänge verhindert werden. Daher sollten geeignete Sicherheitsprodukte gegen gezielte Angriffe ausgewählt und eingesetzt werden.

OPS.1.1.5 - Protokollierung

Umsetzungs-reihenfolge	R1
Vorausgesetzte Anforderungen	OPS.1.1.5.A1: Erstellung einer Sicherheitsrichtlinie für die Protokollierung OPS.1.1.5.A2: Festlegung von Rollen und Verantwortlichkeiten OPS.1.1.5.A3: Konfiguration der Protokollierung auf System- und Netzebene OPS.1.1.5.A4: Zeitsynchronisation der IT-Systeme OPS.1.1.5.A5: Einhaltung rechtlicher Rahmenbedingungen; OPS.1.1.5.A10: Zugriffsschutz für Protokollierungsdaten
Weitere relevante Anforderungen	OPS.1.1.5.A6: Aufbau einer zentralen Protokollierungsinfrastruktur OPS.1.1.5.A7: Sichere Administration von Protokollierungsservern OPS.1.1.5.A8: Archivierung von Protokollierungsdaten OPS.1.1.5.A9: Bereitstellung von Protokollierungsdaten für die Auswertung OPS.1.1.5.A11: Zugriffsschutz für Protokollierungsdaten OPS.1.1.5.A12: Verschlüsselung der Protokollierungsdaten OPS.1.1.5.A13: Hochverfügbare Protokollierungssysteme
Hinweis	Der Baustein enthält übergreifende Anforderungen, welche zu erfüllen sind, damit die Protokollierung der sicherheitsrelevanten Ereignisse umgesetzt werden kann. OPS.1.1.5 Protokollierung ist für den gesamten Informationsverbund einmal anzuwenden.

Umsetzungs-reihenfolge	R1
Besonderheiten	OPS.1.1.5.A6 Eine zentrale Protokollierungsinfrastruktur dient zur Identifikation und Rückverfolgung von Fehlern. Diese Anforderung sollte in größeren Informationsverbünden umgesetzt werden, wie beispielsweise auf Landesebene, da hier eine höhere Menge an Daten verarbeitet und übermittelt wird. OPS.1.1.5.A7 Für den Protokollierungsserver sollte eine sichere Administration über ein separates Managementnetz (Out-of-Band-Management) erfolgen, so dass nur ein berechtigter IT-Administrator über die Administrationsschnittstelle Zugriff erlangen kann. OPS.1.1.5.A8 Die Protokolldateien sind mindestens bis zur Feststellung des endgültigen Wahlergebnisses revisionssicher zu archivieren. OPS.1.1.5.A10 Einige generierte Protokollierungsdaten können Personen zugeordnet werden. Um zu vermeiden, dass die Informationen manipuliert werden, sollten sie verschlüsselt übertragen und sicher gespeichert werden. OPS.1.1.5.A11 Für die an den Schnellmeldungen beteiligten Systeme ist für den Zeitraum der Zusammenfassung und Übertragung der Daten eine erweiterte Protokollierung durchzuführen, welche Sicherheitsvorfälle in Bezug auf das Verändern oder Löschen der Daten erkennbar macht. OPS.1.1.5.A12 Wenn aufgrund der Systemarchitektur das Risiko besteht, dass Protokollierungsdaten bei der Übertragung manipuliert werden können, sollte diese Übertragung durch eine Verschlüsselung gesichert werden. OPS.1.1.5.A13 Sind die Systeme für Erhalt, Zusammenfassung und Übermittlung der Daten bei den Schnellmeldungen als hochverfügbar ausgelegt, so sollte auch die Protokollierung die Vorgaben zur Hochverfügbarkeit erfüllen, um Sicherheitsvorfälle zu erkennen.

OPS.1.1.6 - Software-Tests und -Freigaben

Umsetzungs-reihenfolge	R1
Anforderungen	OPS.1.1.6.A1: Planung der Software-Tests OPS.1.1.6.A2: Durchführung von funktionalen Software-Tests OPS.1.1.6.A3: Auswertung der Testergebnisse OPS.1.1.6.A4: Freigabe der Software OPS.1.1.6.A5: Durchführung nicht-funktionaler Software-Tests; OPS.1.1.6.A6: Geordnete Einweisung der Software-Tester OPS.1.1.6.A7: Personalauswahl der Software-Tester OPS.1.1.6.A11: Verwendung von anonymisierten oder pseudonymisierten Testdaten OPS.1.1.6.A12: Durchführung von Regressionstests OPS.1.1.6.A13: Trennung von Test- und Qualitätsmanagement-Umgebung von der Produktivumgebung; OPS.1.1.6.A14: Durchführung von Penetrationstests
Besonderheiten	OPS.1.1.6.A5 Bevor Software zur Verarbeitung von Daten zur Ermittlung des Wahlergebnisses eingesetzt wird, müssen sicherheitsspezifische Software-Tests durchgeführt werden. Die Testfälle und -ergebnisse müssen dokumentiert werden. OPS.1.1.6.A7 Ausschließlich geeignetes Personal mit ausreichenden Kenntnissen sollte die Software-Tests durchführen. OPS.1.1.6.A11 Bei der Erstellung von Testdaten sollte darauf geachtet werden, dass die Daten nicht mit Echtdaten verwechselt werden können. OPS.1.1.6.A14 Je nach Risikoprofil der eingesetzten Anwendung (z.B. unbeschränkt im Internet erreichbar), sollte ein Penetrationstest durchgeführt werden.

OPS.1.2.4 - Telearbeit

Umsetzungs-reihenfolge	R3
Vorausgesetzte Anforderungen	OPS.1.2.4.A1: Regelungen für Telearbeit OPS.1.2.4.A2: Sicherheitstechnische Anforderungen an den Telearbeitsrechner OPS.1.2.4.A3: Sicherheitstechnische Anforderungen an die Kommunikationsverbindung OPS.1.2.4.A4: Datensicherung bei der Telearbeit OPS.1.2.4.A5: Sensibilisierung und Schulung der Telearbeiter
Weitere relevante Anforderungen	OPS.1.2.4.A6: Erstellen eines Sicherheitskonzeptes für Telearbeit OPS.1.2.4.A7: Regelung der Nutzung von Kommunikationsmöglichkeiten bei Telearbeit OPS.1.2.4.A8: Informationsfluss zwischen Telearbeiter und Institution
Hinweis	Die Anwendung von OPS.1.2.4 ist für jeden Telearbeitsplatz vorgesehen. Der Baustein ist zu beachten, wenn für den Erhalt, die Zusammenfassung oder Übermittlung der vorläufigen Wahlergebnisse, aufgrund von Notfällen oder Krisen, Telearbeit unbedingt notwendig ist.
Besonderheiten	---

OPS.1.2.5 - Fernwartung

Umsetzungs-reihenfolge	R1
Vorausgesetzte Anforderungen	OPS.1.2.5.A1: Planung des Einsatzes der Fernwartung OPS.1.2.5.A2: Sicherer Verbindungsaufbau bei der Fernwartung von Clients OPS.1.2.5.A3: Absicherung der Schnittstellen zur Fernwartung OPS.1.2.5.A4: Regelungen zu Kommunikationsverbindungen; OPS.1.2.5.A5: Einsatz von Online-Diensten OPS.1.2.5.A7: Dokumentation bei der Fernwartung OPS.1.2.5.A8: Sichere Protokolle bei der Fernwartung OPS.1.2.5.A9: Auswahl und Beschaffung geeigneter Fernwartungswerkzeuge; OPS.1.2.5.A14: Dedizierte Systeme bei der Fernwartung
Weitere relevante Anforderungen	OPS.1.2.5.A17: Authentisierungsmechanismen bei der Fernwartung OPS.1.2.5.A19: Fernwartung durch Dritte OPS.1.2.5.A20: Betrieb der Fernwartung OPS.1.2.5.A24: Absicherung integrierter Fernwartungssysteme
Hinweis	Für den Zeitraum der Schnellmeldungen sollten Fernwartungen nicht zugelassen werden. Wenn Fernwartungen dennoch durchgeführt werden müssen aufgrund von dringenden Problemen im Zusammenhang mit der Wahl, ist dieser Baustein auf die entsprechenden Zielobjekte des Informationsverbunds anzuwenden. (Im IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung" waren die aus dem IT-Grundschutz-Kompendium 2019 in OPS.2.4, welcher urspr. die Fernwartung behandelte, enthaltenen Anforderungen OPS.2.4.A1 – A5; A7 – A9, A14, A18 gelistet. A18 ist mittlerweile entfallen.)
Besonderheiten	OPS.1.2.5.A1 Speziell für den betrachteten Zeitraum der Ergebniszusammenstellung und -übermittlung der Wahldaten müssen Fernwartungszugänge grundsätzlich deaktiviert sein. Bei unbedingt notwendigen Fernwartungen sollten die verantwortlichen Wahlleiter und Informationssicherheitsbeauftragten informiert werden. OPS.1.2.5.A6 Die Regelungen zur Fernwartung sollten dokumentiert und für die Mitarbeiter verfügbar sein.

OPS.2.1 - Outsourcing für Kunden

Umsetzungs-reihenfolge	R2
Vorausgesetzte Anforderungen	OPS.2.1.A1: Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben; OPS.2.1.A3: Auswahl eines geeigneten Outsourcing-Dienstleisters OPS.2.1.A4: Vertragsgestaltung mit dem Outsourcing-Dienstleister OPS.2.1.A6: Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben OPS.2.1.A7: Festlegung der möglichen Kommunikationspartner OPS.2.1.A8: Regelungen für den Einsatz des Personals des Outsourcing-Dienstleiters OPS.2.1.A9: Vereinbarung über die Anbindung an Netze der Outsourcing-Partner OPS.2.1.A10: Vereinbarung über Datenaustausch zwischen den Outsourcing-Partnern OPS.2.1.A12: Änderungsmanagement

Umsetzungs-reihenfolge	R2
Weitere relevante Anforderungen	OPS.2.1.A5: Festlegung einer Strategie zum Outsourcing OPS.2.1.A11: Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb OPS.2.1.A14: Notfallvorsorge beim Outsourcing; OPS.2.1.A16: Sicherheitsüberprüfung von Mitarbeitern
Hinweis	Der Baustein OPS.2.1 ist für jeden Outsourcing-Dienstleister, der Dienstleistungen für ein Zielobjekt im Informationsverbund erbringt, aus Sicht des Anwenders separat einzusetzen.
Besonderheiten	OPS.2.1.A4 Da die Wahlen sonntags stattfinden sollten entsprechende Servicezeiten bzw. eine entsprechende Rufbereitschaft mit den Dienstleistern vereinbart werden. Des Weiteren sollten relevante Anforderungen aus diesem Katalog in Bezug auf die Dienstleistung gestellt werden. OPS.2.1.A8 Die Beschäftigten des Outsourcing-Dienstleisters sollten auch in ihre Aufgaben im Rahmen des Wahlprozesses und in die Informationssicherheitsregelungen eingewiesen werden. OPS.2.1.A14 Vor dem Wahlabend sollte rechtzeitig ein Notfallvorsorgekonzept erstellt und mit den Dienstleistern abgestimmt werden. Hierzu sollten die Abläufe und Zuständigkeiten geregelt sein.

DER.1 - Detektion von sicherheitsrelevanten Ereignissen

Umsetzungs-reihenfolge	R1
Anforderungen	DER.1.A1: Erstellung einer Sicherheitsrichtlinie für die Detektion von sicherheitsrelevanten Ereignissen DER.1.A2: Einhaltung rechtlicher Bedingungen bei der Auswertung von Protokolldaten DER.1.A3: Festlegung von Meldewegen für sicherheitsrelevante Ereignisse DER.1.A4: Sensibilisierung der Mitarbeiter DER.1.A5: Einsatz von mitgelieferten Systemfunktionen zur Detektion; DER.1.A6: Kontinuierliche Überwachung und Auswertung von Protokolldaten DER.1.A8: Festlegung von zu schützenden Segmenten DER.1.A9: Einsatz zusätzlicher Detektionssysteme
Besonderheiten	DER.1.A3 Sicherheitsrelevante Ereignisse, welche im Zusammenhang mit den Schnellmeldungen auftreten, müssen schnellstmöglich der nächsten Instanz entlang des Prozesses der Schnellmeldungen gemeldet werden. Die Instanz muss anhand der Dringlichkeit des sicherheitsrelevanten Ereignisses entscheiden über den Umgang und die weitere Meldung, ggf. bis zum Bundeswahlleiter. DER.1.A9 Diese Anforderung zum Einsatz zusätzlicher Detektionssysteme sollte in den Wahlorganen und -behörden zur Anwendung kommen, wenn durch die Kumulierung von Wahlergebnissen mit einer signifikanten Auswirkung ein größeres Risiko entsteht.

DER.2.1 – Behandlung von Sicherheitsvorfällen

Umsetzungs-reihenfolge	R1
Vorausgesetzte Anforderungen	DER.2.1.A1: Definition eines Sicherheitsvorfalls DER.2.1.A2: Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen DER.2.1.A3: Festlegung von Verantwortlichkeiten und Ansprechpartnern bei Sicherheitsvorfällen DER.2.1.A4: Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen DER.2.1.A5: Behebung von Sicherheitsvorfällen DER.2.1.A6: Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen
Weitere relevante Anforderungen	DER.2.1.A7: Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen DER.2.1.A8: Aufbau von Organisationsstrukturen zur Behandlung von Sicherheitsvorfällen DER.2.1.A9: Festlegung von Meldewegen für Sicherheitsvorfälle DER.2.1.A10: Eindämmen der Auswirkung von Sicherheitsvorfällen DER.2.1.A11: Einstufung von Sicherheitsvorfällen DER.2.1.A12: Festlegung der Schnittstellen der Sicherheitsvorfallbehandlung zur Störungs- und Fehlerbehebung DER.2.1.A14: Eskalationsstrategie für Sicherheitsvorfälle DER.2.1.A16: Dokumentation der Behandlung von Sicherheitsvorfällen DER.2.1.A17: Nachbereitung von Sicherheitsvorfällen
Besonderheiten	DER.2.1.A7 Durch einen ungeeigneten Umgang mit Sicherheitsvorfällen können große Schäden entstehen, wenn bspw. Sicherheitslücken in den verwendeten IT-Systemen bekannt werden. Beschaffen sich Wahlorgane und -behörden diese Informationen nicht rechtzeitig und leitet sie die notwendigen Gegenmaßnahmen verzögert ein, können Sicherheitslücken von Angreifern ausgenutzt werden. Gerade aufgrund der brisanten Situation hinsichtlich festgestellter Mängel in Wahlsoftware, sollte eine Vorgehensweise zur Behandlung von Sicherheitsvorfällen etabliert werden. DER.2.1.A12 Um sicherzugehen, dass Störungsmeldungen auch hinsichtlich Sicherheitsgefahren bei den Schnellmeldungen untersucht und entsprechend behandelt werden, sollte eine Analyse der Schnittstellen der Sicherheitsvorfallbehandlung zur Störungs- und Fehlerbehebung durchgeführt werden. DER.2.1.A17 Anhand der Nachbereitung von relevanten Sicherheitsvorfällen in Bezug auf die Schnellmeldungen sollten Handlungsanweisungen generiert werden, um bei der nächsten Wahl bessere Vorkehrungen gegen Angriffe treffen zu können.

DER.4 – Notfallmanagement

Umsetzungs-reihenfolge	R1
Anforderungen	DER.4.A1: Erstellung eines Notfallhandbuchs DER.4.A2: Integration von Notfallmanagement und Informationssicherheitsmanagement; DER.4.A3: Festlegung des Geltungsbereichs und der Notfallmanagementstrategie DER.4.A5: Aufbau einer geeigneten Organisationsstruktur für das Notfallmanagement DER.4.A8: Integration der Mitarbeiter in den Notfallmanagement-Prozess DER.4.A10: Tests und Notfallübungen DER.4.A16: Notfallvorsorge- und Notfallreaktionsplanung für ausgelagerte Komponenten
Besonderheiten	DER.4.A1 Vor dem Wahlabend sollte ein Notfallplan konzipiert werden, der das Vorgehen in Notfällen genau beschreibt und die Zuständigkeiten sowie Notrufnummern enthält. Diese Unterlage sollte allen Beteiligten rechtzeitig vor dem Wahlabend in ausgedruckter Form zur Verfügung gestellt werden. DER.4.A10 Wesentliche Sofortmaßnahmen und Notfallpläne sollten auch unter Berücksichtigung der besonderen Bedingungen, wie sie an einem Wahlsonntag vorherrschen, getestet werden. DER.4.A16 Die bei den Schnellmeldungen eingesetzten, an Dritte ausgelagerte Komponenten, sollten in die Notfallplanung und in die Notfallübungen miteinbezogen werden.

7.3 System-Bausteine

Nachfolgend sind die Zielobjekte (gemäß gelisteter Referenzarchitektur) mit den entsprechenden Bausteinen aufgeführt.

7.3.1 Infrastruktur

7.3.1.1 Verwaltungsgebäude

INF.1 – Allgemeines Gebäude

Umsetzungs-reihenfolge	R2
Vorausgesetzte Anforderungen	INF.1.A1: Planung der Gebäudeabsicherung INF.1.A2: Angepasste Aufteilung der Stromkreise INF.1.A3: Einhaltung von Brandschutzvorschriften INF.1.A4: Branderkennung in Gebäuden INF.1.A5: Handfeuerlöscher INF.1.A6: Geschlossene Fenster und Türen INF.1.A7: Zutrittsregelung und -kontrolle INF.1.A8: Rauchverbot; INF.1.A9: Sicherheitskonzept für die Gebäudenutzung
Weitere relevante Anforderungen	INF.1.A11: Abgeschlossene Türen INF.1.A23: Bildung von Sicherheitszonen Zusätzliche Anforderung zur Vermeidung der Reinigung im Zeitraum der Schnellmeldung

Umsetzungs-reihenfolge	R2
Hinweis	Die Anforderungen dieses Bausteins gelten für die Gebäude, welche von Kommunen, Bund und Ländern für die vorläufige Wahlergebnisermittlung genutzt werden. Sofern in Amtshilfe Räumlichkeiten anderer Gebietskörperschaften, Ressorts oder Einrichtungen mitgenutzt werden (sollen) und formal notwendige Vereinbarungen (z.B. Staatsverträge) nicht zeit- und situationsgerecht abgeschlossen werden können, sollte die Einhaltung der Anforderungen mit dem Gastgeber besprochen bzw. kompensatorische eigene Maßnahmen vorgesehen werden.
Besonderheiten	INF.1.A23 Für die Instanzen Länder und Bund sollten Räume ähnlichen Schutzbedarfs in Sicherheitszonen zusammengefasst werden. Es sollte ein Sicherheitszonenkonzept für das jeweilige Gebäude entwickelt und dokumentiert werden. Zusätzliche Anforderung zur Vermeidung der Reinigung Am Tag der Wahl bzw. während den Arbeiten für die Schnellmeldungen sollte keine Gebäudereinigung stattfinden, um mögliche Störungen oder Manipulationen der Daten zu vermeiden.

INF.3 – Elektrotechnische Verkabelung

Umsetzungs-reihenfolge	R3
Vorausgesetzte Anforderungen	INF.3.A1: Auswahl geeigneter Kabeltypen INF.3.A2: Planung der Kabelführung INF.3.A3: Fachgerechte Installation
Weitere relevante Anforderungen	INF.3.A5: Abnahme der elektrotechnischen Verkabelung
Hinweis	Bei Wahlen wird wegen dem temporären Aufbau von Technik häufig auch eine temporäre Elektroinstallation durchgeführt. Für diesen Fall ist der Baustein INF.3 zu berücksichtigen.
Besonderheiten	INF.3.A5 Wird für die Schnellwahl eine temporäre Verkabelung eingerichtet, sollte diese vorab geprüft und abgenommen werden.

INF.4 – IT-Verkabelung

Umsetzungs-reihenfolge	R3
Vorausgesetzte Anforderungen	INF.4.A1: Auswahl geeigneter Kabeltypen INF.4.A2: Planung der Kabelführung INF.4.A3: Fachgerechte Installation; INF.4.A9: Dokumentation und Kennzeichnung der IT-Verkabelung
Weitere relevante Anforderungen	INF.4.A5: Abnahme der IT-Verkabelung
Hinweis	Bei Wahlen ist wegen dem temporären Aufbau von Technik häufig auch eine temporäre Netzwerkinstallation vorzufinden. Für diesen Fall ist der Baustein INF.4 zu berücksichtigen.

Umsetzungs-reihenfolge	R3
Besonderheiten	INF.3.A5 Die für die Schnellwahlen eingerichtete IT-Verkabelung sollte vorab geprüft und abgenommen werden.

7.3.1.2 Serverraum / Rechenzentrum

INF.2 – Rechenzentrum sowie Serverraum

Umsetzungs-reihenfolge	R2
Vorausgesetzte Anforderungen	INF.2.A1: Festlegung von Anforderungen INF.2.A2: Bildung von Brandabschnitten INF.2.A3: Einsatz einer unterbrechungsfreien Stromversorgung INF.2.A4: Notabschaltung der Stromversorgung INF.2.A5: Einhaltung der Lufttemperatur und -feuchtigkeit INF.2.A6: Zutrittskontrolle INF.2.A7: Verschließen und Sichern INF.2.A8: Einsatz einer Brandmeldeanlage INF.2.A9: Einsatz einer Lösch- oder Brandvermeidungsanlage INF.2.A10: Inspektion und Wartung der Infrastruktur INF.2.A11: Automatische Überwachung der Infrastruktur; INF.2.A15: Überspannungsschutzeinrichtung
Weitere relevante Anforderungen	INF.2.A17: Brandfrüherkennung; INF.2.A12: Perimeterschutz für das Rechenzentrum INF.2.A13: Planung und Installation von Gefahrenmeldeanlagen INF.2.A14: Einsatz einer Netzersatzanlage INF.2.A16: Klimatisierung im Rechenzentrum INF.2.A30: Anlagen zur Erkennung, Löschung oder Vermeidung von Bränden
Hinweis	Bei relativ kleinen Wahlbehörden mit wenigen IT-Arbeitsplätzen und einem Server, der in einem separaten Raum steht, ist INF.5 anzuwenden. Bei größeren Informationsverbünden ist INF.2 auf jeden selbst betriebenen Serverraum anzuwenden. Insofern die IT extern gehostet wird, ist der jeweilige Dienstleister auf die Umsetzung dieses Bausteins zu verpflichten (vertragliche Vereinbarung der notwendigen Leistungen).
Besonderheiten	---

7.3.1.3 Raum für technische Infrastruktur

INF.5 – Raum sowie Schrank für technische Infrastruktur

Umsetzungs-reihenfolge	R2
Anforderungen	INF.5.A1: Planung der Raumabsicherung INF.5.A2: Lage und Größe des Raumes für technische Infrastruktur INF.5.A3: Zutrittsregelung und -kontrolle [Informationssicherheitsbeauftragter INF.5.A4: Schutz vor Einbruch INF.5.A5: Vermeidung sowie Schutz vor elektromagnetischen Störfeldern INF.5.A6: Minimierung von Brandlasten INF.5.A7: Verhinderung von Zweckentfremdung; INF.5.A8: Vermeidung von unkontrollierter elektrostatischer Entladung INF.5.A9: Stromversorgung INF.5.A10: Einhaltung der Lufttemperatur und -feuchtigkeit INF.5.A11: Vermeidung von Leitungen mit gefährdenden Flüssigkeiten und Gasen INF.5.A12: Schutz vor versehentlicher Beschädigung von Zuleitungen INF.5.A13: Schutz vor Schädigung durch Brand und Rauchgase INF.5.A14: Minimierung von Brandgefahren aus Nachbarbereichen INF.5.A15: Blitz- und Überspannungsschutz INF.5.A16: Einsatz einer unterbrechungsfreien Stromversorgung INF.5.A17: Inspektion und Wartung der Infrastruktur
Hinweis	Der Baustein INF.5 ist für Räume anzuwenden, in denen die technische Infrastruktur betrieben wird. Der Baustein ist ebenfalls anzuwenden, wenn stationäre Container, im Sinne eines großen Schranks, betrieben werden. Für Wahlorgane und -behörden mit wenigen IT-Arbeitsplätzen und einem Server, der in einem separaten Raum betrieben wird, genügt es oft, die Anforderungen des vorliegenden Bausteins anstatt des Bausteins INF.2 zu erfüllen.
Besonderheiten	INF.5.A10 Für die Ebenen Länder und Bund sollte sichergestellt werden, dass die Lufttemperatur und Luftfeuchtigkeit im Raum für technische Infrastruktur innerhalb der für die darin befindlichen Geräte angemessen sind.

7.3.1.4 Büroraum

INF.7 – Büroarbeitsplatz

Umsetzungs-reihenfolge	R1
Vorausgesetzte Anforderungen	INF.7.A1: Geeignete Auswahl und Nutzung eines Büroraumes INF.7.A2: Geschlossene Fenster und abgeschlossene Türen; INF.7.A5: Ergonomischer Arbeitsplatz INF.7.A6: Aufgeräumter Arbeitsplatz INF.7.A7: Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger
Weitere relevante Anforderungen	INF.7.A4: Zutrittsregelungen und -kontrolle; INF.7.A8: Einsatz von Diebstahlsicherungen
Hinweis	Dieser Baustein ist auf jeden Büroraum (innerhalb der Verwaltungsgebäude oder sonstiger Gebäude von Bund und Ländern) anzuwenden, in denen sich Beschäftigte bzw. Mitglieder aufhalten, um dort ihre Aufgaben innerhalb des Informationsverbunds zu erledigen.
Besonderheiten	INF.7.A2 Es ist sicherzustellen, dass während der Zusammenfassung der Wahlergebnisse schädliche Einflüsse, z.B. durch Handlungen unbefugter Personen im Raum oder negative Einflüsse aufgrund offener Türen oder Fenster, weitestgehend minimiert werden. INF.7.A4 Da in Verwaltungen zeitweise Publikumsverkehr herrscht, sollten Vorkehrungen getroffen werden, damit Unbefugte die Büroräume, in welchen die Wahldaten konsolidiert oder kurzfristig aufbewahrt werden, nicht betreten können. INF.7.A8 Insbesondere in den Wahlräumen sollten Diebstahlsicherungen zum Schutz der Geräte und Daten eingesetzt werden. Damit soll einem Missbrauch der Geräte vorgebeugt werden. (Eine Diebstahlsicherung kann entbehrlich sein, wenn eine lückenlose Anwesenheit oder Beaufsichtigung durch Befugte sichergestellt werden kann.)

7.3.1.5 Mobiler Arbeitsplatz

INF.9 – Mobiler Arbeitsplatz

Umsetzungs-reihenfolge	R1
Vorausgesetzte Anforderungen	INF.9.A1: Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes INF.9.A2: Regelungen für mobile Arbeitsplätze INF.9.A3: Zutritts- und Zugriffsschutz INF.9.A4: Arbeiten mit fremden IT-Systemen; INF.9.A5: Zeitnahe Verlustmeldung INF.9.A6: Entsorgung von vertraulichen Informationen
Weitere relevante Anforderungen	INF.9.A8: Sicherheitsrichtlinie für mobile Arbeitsplätze INF.9.A9: Verschlüsselung tragbarer IT-Systeme und Datenträger
Hinweis	Der Baustein ist hinzuzuziehen, wenn aufgrund von besonderen Umständen die Erledigung der Aufgaben bei der Ermittlung der Schnellmeldungen nur an einem mobilen Arbeitsplatz möglich ist. INF.9 ist dabei für alle Räumlichkeiten anzuwenden, in welchen mobil gearbeitet wird.
Besonderheiten	---

7.3.1.6 Häuslicher Arbeitsplatz

INF.8 – Häuslicher Arbeitsplatz

Umsetzungs-reihenfolge	R1
Vorausgesetzte Anforderungen	INF.8.A1: Sichern von dienstlichen Unterlagen am häuslichen Arbeitsplatz INF.8.A2: Transport von Arbeitsmaterial zum häuslichen Arbeitsplatz INF.8.A3: Schutz vor unbefugtem Zutritt am häuslichen Arbeitsplatz; INF.8.A5: Entsorgung von vertraulichen Informationen am häuslichen Arbeitsplatz
Weitere relevante Anforderungen	---
Hinweis	Dieser Baustein ist relevant, wenn aufgrund von Notfällen oder Krisen die Erledigung der Aufgaben für die Schnellmeldungen nur an einem häuslichen Arbeitsplatz möglich ist. Er hat dann für die Räume zu gelten, die als Telearbeitsplatz genutzt werden.
Besonderheiten	---

7.3.1.7 Drucker- und Kopierraum

INF.10 – Besprechungs-, Veranstaltungs-, Schulungsraum

Umsetzungs-reihenfolge	R2
Vorausgesetzte Anforderungen	INF.10.A1: Sichere Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen INF.10.A2: Beaufsichtigung von Besuchern INF.10.A3: Geschlossene Fenster und Türen; INF.10.A7: Sichere Konfiguration von Schulungs- und Präsentationsrechnern

Umsetzungs-reihenfolge	R2
Weitere relevante Anforderungen	INF.10.A6: Einrichtung sicherer Netzzugänge
Hinweis	Im kommunalen Bereich befinden sich Drucker, Kopierer oder Multifunktionsgeräte häufig in nicht zutrittsgesicherten Bereichen. Da Bürger in der Regel einen ungehinderten Zutritt in das Rathaus bzw. Kreishaus haben, ist somit auch der freie Zugang zu den Druckern und Kopierern möglich. Aufgrund dieser Gegebenheit eignet sich der Baustein INF.10 für entsprechende Anforderungen.
Besonderheiten	---

7.3.2 IT-Systeme

7.3.2.1 Server

SYS.1.1 – Allgemeiner Server

Umsetzungs-reihenfolge	R2
Vorausgesetzte Anforderungen	SYS.1.1.A1: Geeignete Aufstellung SYS.1.1.A2: Benutzerauthentisierung an Servern SYS.1.1.A3: Restriktive Rechtevergabe SYS.1.1.A4: Rollentrennung SYS.1.1.A5: Schutz der Administrationsschnittstellen SYS.1.1.A6: Deaktivierung nicht benötigter Dienste und Kennungen SYS.1.1.A7: Updates und Patches für Firmware, Betriebssystem und Anwendungen SYS.1.1.A8: Regelmäßige Datensicherung SYS.1.1.A9: Einsatz von Virenschutz-Programmen SYS.1.1.A10: Protokollierung; SYS.1.1.A15: Unterbrechungsfreie und stabile Stromversorgung SYS.1.1.A17: Einsatzfreigabe für Server SYS.1.1.A21: Betriebsdokumentation für Server SYS.1.1.A25: Geregelte Außerbetriebnahme eines Servers
Weitere relevante Anforderungen	SYS.1.1.A11: Festlegung einer Sicherheitsrichtlinie für Server SYS.1.1.A12: Planung des Server-Einsatzes SYS.1.1.A14: Erstellung eines Benutzer- und Administrationskonzepts SYS.1.1.A16: Sichere Installation und Grundkonfiguration von Servern SYS.1.1.A18: Verschlüsselung der Kommunikationsverbindungen SYS.1.1.A19: Einrichtung lokaler Paketfilter SYS.1.1.A20: Beschränkung des Zugangs über Netze SYS.1.1.A22: Einbindung in die Notfallplanung SYS.1.1.A23: Systemüberwachung und Monitoring von Servern SYS.1.1.A24: Sicherheitsprüfungen; SYS.1.1.A26: Verwendung von Mehr-Faktor-Authentisierung SYS.1.1.A28: Steigerung der Verfügbarkeit durch Redundanz SYS.1.1.A31: Application Whitelisting
Hinweis	Dieser Baustein ist für alle allgemeinen Server-Systeme mit beliebigem Betriebssystem anzuwenden, die eine Rolle spielen bei der Ermittlung der vorläufigen Wahlergebnisse.

Umsetzungs-reihenfolge	R2
Besonderheiten	SYS.1.1.A26 Insofern eine Multi-Faktor-Authentisierung notwendig ist, sollte diese von der empfangenden Instanz implementiert und verwendet werden. SYS.1.1.A28 Für die Server der Länder und des Bundes sollten für die Schnellmeldungen geeignete Redundanzen verfügbar sein, um Ausfälle zu vermeiden. SYS.1.1.A31 Auf den Ebenen der Länder und des Bundes sollte über Application Whitelisting sichergestellt werden, dass nur erlaubte Programme ausgeführt werden.

SYS.1.2.2 – Windows Server 2012

Umsetzungs-reihenfolge	R2
Anforderungen	SYS.1.2.2.A2: Sichere Installation von Windows Server 2012 SYS.1.2.2.A3: Sichere Administration von Windows Server 2012 SYS.1.2.2.A4: Sichere Konfiguration von Windows Server 2012 SYS.1.2.2.A5: Schutz vor Schadsoftware auf Windows Server 2012 SYS.1.2.2.A6: Sichere Authentisierung und Autorisierung in Windows Server 2012 SYS.1.2.2.A8: Schutz der Systemintegrität SYS.1.2.2.A9: Lokale Kommunikationsfilterung
Hinweis	Dieser Baustein ist für alle Server-Systeme anzuwenden, auf denen das Betriebssystem Microsoft Windows Server 2012 eingesetzt wird und die eine Rolle spielen bei der Ermittlung der vorläufigen Wahlergebnisse. (Im IT-Grundschutz-Kompendium 2021 wird der neue Baustein SYS.1.2.3 für Windows Server 2019 enthalten sein.)
Besonderheiten	---

SYS.1.3 – Server unter Linux und Unix

Umsetzungs-reihenfolge	R2
Anforderungen	SYS.1.3.A1: Authentisierung von Administratoren und Benutzern SYS.1.3.A2: Sorgfältige Vergabe von IDs SYS.1.3.A3: Kein automatisches Einbinden von Wechsellaufwerken SYS.1.3.A4: Schutz vor Ausnutzung von Schwachstellen in Anwendungen SYS.1.3.A5: Sichere Installation von Software-Paketen; SYS.1.3.A6: Verwaltung von Benutzern und Gruppen SYS.1.3.A8: Verschlüsselter Zugriff über Secure Shell SYS.1.3.A9: Absicherung des Bootvorgangs SYS.1.3.A10: Verhinderung der Ausbreitung bei der Ausnutzung von Schwachstellen SYS.1.3.A11: Einsatz der Sicherheitsmechanismen von NFS SYS.1.3.A12: Einsatz der Sicherheitsmechanismen von NIS
Hinweis	Der Baustein SYS.1.3 ist für alle Server-Systeme anzuwenden, auf denen Linux- oder Unix-basierte Betriebssysteme eingesetzt werden und die eine Rolle spielen bei der Ermittlung der vorläufigen Wahlergebnisse.

Umsetzungs-reihenfolge	R2
Besonderheiten	SYS.1.3.A11 Werden über das Network File System (NFS) Verzeichnisse exportiert, sollte dies nur für unbedingt notwendige Verzeichnisse durchgeführt werden. SYS.1.3.A12 Wird ein Network Information Service (NIS) eingesetzt, so sollte dieser nur in einer sicheren Betriebsumgebung zum Einsatz kommen.

APP.3.2 – Webserver

Umsetzungs-reihenfolge	R2
Anforderungen	APP.3.2.A1: Sichere Konfiguration eines Webservers APP.3.2.A2: Schutz der Webserver-Dateien APP.3.2.A3: Absicherung von Datei-Uploads und -Downloads APP.3.2.A4: Protokollierung von Ereignissen APP.3.2.A5: Authentisierung APP.3.2.A7: Rechtliche Rahmenbedingungen für Webangebote APP.3.2.A11: Verschlüsselung über TLS; APP.3.2.A8: Planung des Einsatzes eines Webservers APP.3.2.A9: Festlegung einer Sicherheitsrichtlinie für den Webserver APP.3.2.A12: Geeigneter Umgang mit Fehlern und Fehlermeldungen APP.3.2.A14: Integritätsprüfungen und Schutz vor Schadsoftware APP.3.2.A16: Penetrationstest und Revision; APP.3.2.A15: Redundanz APP.3.2.A17: Einsatz erweiterter Authentisierungsmethoden für Webserver APP.3.2.A18: Schutz vor Denial-of-Service-Angriffen
Hinweis	Der Baustein ist nur relevant, wenn der Webserver Teil der Software-Lösung ist, mit der die Schnellmeldungen verarbeitet werden. (Dies gilt insbesondere nicht für die Web-Präsenz der Gemeinde, da diese nicht zum Geltungsbereich gehört.)
Besonderheiten	APP.3.2.A2 Die Dateien auf dem Webserver müssen vor unberechtigtem Zugriff und Modifikation geschützt werden, um zu vermeiden, dass Angreifer sich Zugriff auf einen Webserver verschaffen und dessen Inhalte, wie Wahldaten, manipulieren. APP.3.2.A16 Ist im Szenario der Schnellmeldungen ein Webserver Teil der notwendigen Systemarchitektur, sollten regelmäßige Revisionen sowie Penetrationstests durchgeführt werden. Die Revisionen und Penetrationstests sollten rechtzeitig vor dem Wahltag erfolgen und nicht im Zeitraum der Schnellmeldungen. APP.3.2.A18 Um die Verfügbarkeit der Daten für die Schnellmeldungen zu gewährleisten, sollte der Webserver überwacht werden, um Distributed Denial of Service-Angriffe (DDOS) abzuschwächen oder sogar zu verhindern.

APP.3.6 – DNS-Server

Umsetzungs-reihenfolge	R2
Anforderungen	APP.3.6.A2: Einsatz redundanter DNS-Server APP.3.6.A3: Verwendung von separaten DNS-Servern für interne und externe Anfragen APP.3.6.A4: Sichere Grundkonfiguration eines DNS-Servers APP.3.6.A6: Absicherung von dynamischen DNS-Updates APP.3.6.A7: Überwachung von DNS-Servern APP.3.6.A9: Erstellen eines Notfallplans für DNS-Server; APP.3.6.A11: Ausreichende Dimensionierung der DNS-Server APP.3.6.A12: Schulung der Verantwortlichen APP.3.6.A16: Integration eines DNS-Servers in eine „P-A-P“-Struktur APP.3.6.A17: Einsatz von DNSSEC
Hinweis	Der Baustein ist zu beachten, wenn im betrachteten Informationsverbund DNS-Server, die auch für externe Anfragen genutzt werden, zum Einsatz kommen.
Besonderheiten	APP.3.6.A12 Eine spezielle Schulung ist nicht unbedingt notwendig, es sollte jedoch qualifiziertes Personal bei dem Einsatz von DNS-Servern unterstützen. Die Verantwortlichen sollten mit den Konfigurationsmöglichkeiten und sicherheitsrelevanten Aspekten der DNS-Server vertraut sein. APP.3.6.A16 Bei dem eigenen Betrieb von DNS-Servern sollte die Integration dieser in eine „Paketfilter – Application-Level-Gateway – Paketfilter“-Struktur („P-A-P“-Struktur) vorgenommen werden.

7.3.2.2 Arbeitsplatz-PC / Laptop

SYS.2.1 – Allgemeiner Client

Umsetzungs-reihenfolge	R2
Vorausgesetzte Anforderungen	SYS.2.1.A1: Sichere Benutzerauthentisierung SYS.2.1.A2: Rollentrennung SYS.2.1.A3: Aktivieren von Autoupdate-Mechanismen SYS.2.1.A4: Regelmäßige Datensicherung SYS.2.1.A5: Verwendung einer Bildschirmsperre SYS.2.1.A6: Einsatz von Viren-Schutzprogrammen SYS.2.1.A7: Protokollierung auf Clients SYS.2.1.A8: Absicherung des Bootvorgangs; SYS.2.1.A19: Restriktive Rechtevergabe SYS.2.1.A22: Abmelden nach Aufgabenerfüllung SYS.2.1.A25: Mitarbeiterrichtlinie zur sicheren IT-Nutzung SYS.2.1.A27: Geregelte Außerbetriebnahme eines Clients

Umsetzungs-reihenfolge	R2
Weitere relevante Anforderungen	SYS.2.1.A9: Festlegung einer Sicherheitsrichtlinie für Clients SYS.2.1.A12: Kompatibilitätsprüfung von Software SYS.2.1.A13: Zugriff auf Ausführungsumgebungen mit unbeobachtbarer Codeausführung SYS.2.1.A14: Updates und Patches für Firmware, Betriebssystem und Anwendungen SYS.2.1.A15: Sichere Installation und Konfiguration von Clients SYS.2.1.A16: Deaktivierung und Deinstallation nicht benötigter Komponenten und Kennungen SYS.2.1.A17: Einsatzfreigabe für Clients SYS.2.1.A18: Nutzung von TLS SYS.2.1.A20: Schutz der Administrationsschnittstellen SYS.2.1.A23: Bevorzugung von Client-Server-Diensten SYS.2.1.A24: Umgang mit externen Medien und Wechseldatenträgern SYS.2.1.A26: Schutz vor Ausnutzung von Schwachstellen in Anwendungen
Hinweis	SYS.2.1 ist für Client-IT-Systeme mit beliebigem Betriebssystem anzuwenden, in welchen Informationen für die vorläufige Wahlergebnisermittlung erstellt, gelesen, bearbeitet, gespeichert oder versendet werden.
Besonderheiten	SYS.2.1.A4 Diese Anforderung ist zu beachten, insofern Daten auf dem Standalone-Client gespeichert werden. Wo möglich, sollten Daten im Netzwerk oder auf Servern gespeichert werden. SYS.2.1.A12 Bevor Wahlsoftware beschafft wird, sollte geprüft werden, ob die Software mit dem eingesetzten Betriebssystem in der vorliegenden Konfiguration kompatibel ist.

SYS.2.2.2 – Clients unter Windows 8.1

Umsetzungs-reihenfolge	R2
Anforderungen	SYS.2.2.2.A2: Festlegung eines Anmeldeverfahrens für Windows 8.1 SYS.2.2.2.A5: Lokale Sicherheitsrichtlinien für Windows 8.1; SYS.2.2.2.A6: Datei- und Freigabeberechtigungen unter Windows 8.1 SYS.2.2.2.A7: Einsatz der Windows-Benutzerkontensteuerung UAC SYS.2.2.2.A8: Keine Verwendung der Heimnetzgruppen-Funktion SYS.2.2.2.A10: Integration von Online-Konten in das Betriebssystem SYS.2.2.2.A11: Konfiguration von Synchronisationsmechanismen in Windows 8.1 SYS.2.2.2.A12: Sichere zentrale Authentisierung in Windows-Netzen; SYS.2.2.2.A20: Sicherheit beim Fernzugriff über RDP
Hinweis	Dieser Baustein SYS.2.2.2 ist für alle Client-Systeme anzuwenden, auf denen das Betriebssystem Microsoft Windows 8.1 eingesetzt wird und die für die Ermittlung der vorläufigen Wahlergebnisse relevant sind. Der reguläre Support für Windows 8.x endetet am 8. Januar 2018. Seitdem gibt es nur noch kostenpflichtigen Support. Der erweiterte Support für Windows 8.x endet am 10. Januar 2023. Microsoft liefert für Windows 8.x bis dahin nur noch Sicherheits-Updates. Empfohlene, optionale oder wichtige Updates entfallen. Daher sollte ein Umstieg auf Windows 10 rechtzeitig durchgeführt werden.
Besonderheiten	---

SYS.2.2.3 – Clients unter Windows 10

Umsetzungs-reihenfolge	R2
Anforderungen	SYS.2.2.3.A6: Integration von Online-Konten in das Betriebssystem SYS.2.2.3.A8: Zentrale Verwaltung der Sicherheitsrichtlinien von Clients SYS.2.2.3.A9: Sichere zentrale Authentisierung in Windows-Netzen SYS.2.2.3.A10: Konfiguration zum Schutz von Anwendungen unter Windows 10 SYS.2.2.3.A11: Schutz der Anmeldeinformationen unter Windows 10 SYS.2.2.3.A12: Datei- und Freigabeberechtigungen unter Windows 10 SYS.2.2.3.A13: Einsatz der SmartScreen-Funktion SYS.2.2.3.A14: Einsatz des Sprachassistenten Cortana SYS.2.2.3.A15: Einsatz der Synchronisationsmechanismen unter Windows 10; SYS.2.2.3.A17: Keine Speicherung von Daten zur automatischen Anmeldung SYS.2.2.3.A18: Einsatz der Windows-Remoteunterstützung SYS.2.2.3.A19: Sicherheit beim Fernzugriff über RDP SYS.2.2.3.A20: Einsatz der Benutzerkontensteuerung UAC für privilegierte Konten
Hinweis	Der Baustein SYS.2.2.3 ist für alle Client-Systeme im Informationsverbund anzuwenden, auf denen das Betriebssystem Microsoft Windows 10 eingesetzt wird.
Besonderheiten	---

SYS.2.3 – Clients unter Linux und Unix

Umsetzungs-reihenfolge	R2
Anforderungen	SYS.2.3.A1: Authentisierung von Administratoren und Benutzern SYS.2.3.A2: Auswahl einer geeigneten Distribution SYS.2.3.A3: Nutzung von Cloud- und Online-Funktionen SYS.2.3.A4: Einspielen von Updates und Patches auf unixartigen Systemen SYS.2.3.A5: Sichere Installation von Software-Paketen; SYS.2.3.A7 Restriktive Rechtevergabe auf Dateien und Verzeichnisse SYS.2.3.A8: Einsatz von Techniken zur Rechtebeschränkung von Anwendungen SYS.2.3.A9: Sichere Verwendung von Passwörtern auf der Kommandozeile
Hinweis	Der Baustein SYS.2.3 ist für alle Client-Systeme anzuwenden, auf denen Linux- oder Unix-basierte Betriebssysteme eingesetzt werden für die Ermittlung der vorläufigen Wahlergebnisse.
Besonderheiten	---

SYS.2.4 – Clients unter macOS

Umsetzungs-reihenfolge	R2
Anforderungen	SYS.2.4.A2: Nutzung der integrierten Sicherheitsfunktionen von macOS SYS.2.4.A3: Verwendung geeigneter Benutzerkonten; SYS.2.4.A5: Deaktivierung sicherheitskritischer Funktionen von macOS SYS.2.4.A10: Aktivierung der Personal Firewall unter macOS
Hinweis	Dieser Baustein ist für alle Client-Systeme anzuwenden, auf denen das Betriebssystem Apple macOS eingesetzt wird für die Ermittlung der vorläufigen Wahlergebnisse.
Besonderheiten	---

SYS.3.1 – Laptops

Umsetzungs-reihenfolge	R2
Vorausgesetzte Anforderungen	SYS.3.1.A1: Regelungen zur mobilen Nutzung von Laptops SYS.3.1.A2: Zugriffsschutz am Laptop SYS.3.1.A3: Einsatz von Personal Firewalls SYS.3.1.A4: Einsatz von Antivirenprogrammen; SYS.3.1.A6: Sicherheitsrichtlinien für Laptops SYS.3.1.A8: Sicherer Anschluss von Laptops an Datennetze SYS.3.1.A9: Sicherer Fernzugriff SYS.3.1.A10: Abgleich der Datenbestände von Laptops SYS.3.1.A11: Sicherstellung der Energieversorgung
Weitere relevante Anforderungen	---
Hinweis	Der Baustein SYS.3.1 ist für alle Laptops anzuwenden, die mobil oder stationär für die Ermittlung der vorläufigen Wahlergebnisse genutzt werden.
Besonderheiten	---

7.3.2.3 Mobiltelefon

SYS.3.3 – Mobiltelefon

Umsetzungs-reihenfolge	R2
Anforderungen	SYS.3.3.A1: Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung; SYS.3.3.A5: Nutzung der Sicherheitsmechanismen von Mobiltelefonen SYS.3.3.A6: Updates von Mobiltelefonen SYS.3.3.A9: Sicherstellung der Energieversorgung von Mobiltelefonen
Hinweis	Dieser Baustein ist auf alle Mobiltelefone anzuwenden, welche zu der Ermittlung der vorläufigen Wahlergebnisse genutzt werden.
Besonderheiten	---

7.3.2.4 Smartphone und Tablet

SYS.3.2.1 – Allgemeine Smartphones und Tablets

Umsetzungs-reihenfolge	R2
Vorausgesetzte Anforderungen	SYS.3.2.1.A1: Festlegung einer Richtlinie für den Einsatz von Smartphones und Tablets SYS.3.2.1.A2: Festlegung einer Strategie für die Cloud-Nutzung SYS.3.2.1.A3: Sichere Grundkonfiguration für mobile Geräte SYS.3.2.1.A4: Verwendung eines Zugriffschutzes SYS.3.2.1.A5: Updates von Betriebssystem und Apps SYS.3.2.1.A6: Datenschutzeinstellungen SYS.3.2.1.A7: Verhaltensregeln bei Sicherheitsvorfällen SYS.3.2.1.A8: Keine Installation von Apps aus unsicheren Quellen; SYS.3.2.1.A10: Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten SYS.3.2.1.A11: Verschlüsselung des Speichers SYS.3.2.1.A16: Verwendung nicht personalisierter Gerätenamen SYS.3.2.1.A21: Definition der erlaubten Informationen und Applikationen auf mobilen Geräten
Weitere relevante Anforderungen	SYS.3.2.1.A9: Restriktive Nutzung von funktionalen Erweiterungen SYS.3.2.1.A12: Verwendung nicht personalisierter Gerätenamen SYS.3.2.1.A13: Regelungen zum Screensharing und Casting SYS.3.2.1.A14: Schutz vor Phishing und Schadprogrammen im Browser SYS.3.2.1.A15: Deaktivierung von Download-Boostern SYS.3.2.1.A17: Verwendung der SIM-Karten-PIN SYS.3.2.1.A19: Verwendung von Sprachassistenten SYS.3.2.1.A20: Auswahl und Freigabe von Apps SYS.3.2.1.A22: Einbindung mobiler Geräte in die interne Infrastruktur via VPN SYS.3.2.1.A28: Verwendung der Filteroption für Webseiten
Hinweis	Dieser Baustein ist für alle Smartphones und Tablets anzuwenden, welche zu der Ermittlung der vorläufigen Wahlergebnisse genutzt werden.
Besonderheiten	---

SYS.3.2.2 – Mobile Device Management (MDM)

Umsetzungs-reihenfolge	R2
Anforderungen	SYS.3.2.2.A1: Festlegung einer Strategie für das Mobile Device Management SYS.3.2.2.A2: Festlegung erlaubter mobiler Endgeräte SYS.3.2.2.A3: Auswahl eines MDM-Produkts SYS.3.2.2.A4: Verteilung der Grundkonfiguration auf mobile Endgeräte SYS.3.2.2.A5: Sichere Grundkonfiguration für mobile Endgeräte SYS.3.2.2.A6: Protokollierung und Gerätestatus SYS.3.2.2.A20: Regelmäßige Überprüfung des MDM; SYS.3.2.2.A7: Auswahl und Freigabe von Apps SYS.3.2.2.A8: Festlegung erlaubter Informationen auf mobilen Endgeräten SYS.3.2.2.A9: Auswahl und Installation von Sicherheits-Apps SYS.3.2.2.A10: Sichere Anbindung der mobilen Endgeräte an die Institution SYS.3.2.2.A11: Berechtigungsmanagement im MDM SYS.3.2.2.A12: Absicherung der MDM-Betriebsumgebung SYS.3.2.2.A21: Verwaltung von Zertifikaten
Hinweis	Der Baustein SYS.3.2.2 ist für den Informationsverbund einzusetzen, wenn die bei den Schnellmeldungen genutzten mobilen Endgeräte durch ein Mobile Device Management (MDM) verwaltet werden.
Besonderheiten	---

SYS.3.2.3 – iOS (for Enterprise)

Umsetzungs-reihenfolge	R3
Anforderungen	SYS.3.2.3.A1: Strategie für die iOS-Nutzung SYS.3.2.3.A7: Verhinderung des unautorisierten Löschens von Konfigurationsprofilen; SYS.3.2.3.A10: Verwendung biometrischer Authentisierung SYS.3.2.3.A13: Verwendung der Konfigurationsoption „Einschränkungen unter iOS“ SYS.3.2.3.A18: Verwendung der Konfigurationsoption für den Browser Safari SYS.3.2.3.A20: Einbindung der Geräte in die interne Infrastruktur via VPN SYS.3.2.3.A21: Freigabe von Apps und Einbindung des Apple App Stores; SYS.3.2.3.A26: Keine Verbindung mit Host-Systemen
Hinweis	Der Baustein SYS.3.2.3 ist für alle dienstlich verwendeten Smartphones und Tablets mit dem Betriebssystem Apple iOS anzuwenden, welche bei der Ermittlung der vorläufigen Wahlergebnisse genutzt werden.
Besonderheiten	---

SYS.3.2.4 – Android

Umsetzungs-reihenfolge	R3
Anforderungen	SYS.3.2.4.A1: Auswahl von Android-basierten SYS.3.2.4.A2: Deaktivieren der Entwickler-Optionen SYS.3.2.4.A3: Einsatz des Multi-User- und Gäste-Modus SYS.3.2.4.A5: Erweiterte Sicherheitseinstellungen
Hinweis	Dieser Baustein ist für alle dienstlich verwendeten Smartphones und Tablets mit dem Betriebssystem Google Android anzuwenden, welche bei der Ermittlung der vorläufigen Wahlergebnisse genutzt werden.
Besonderheiten	---

7.3.2.5 Netzwerk-Drucker, Drucksysteme und Multifunktionsgerät

SYS.4.1 – Drucker, Kopierer und Multifunktionsgeräte

Umsetzungs-reihenfolge	R3
Vorausgesetzte Anforderungen	SYS.4.1.A1: Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten SYS.4.1.A2: Geeignete Aufstellung und Zugriff auf Drucker, Kopierer und Multifunktionsgeräte SYS.4.1.A12: Ordnungsgemäße Entsorgung von Geräten und schützenswerten Betriebsmitteln; SYS.4.1.A4: Erstellung eines Sicherheitskonzeptes für den Einsatz von Druckern, Kopieren und Multifunktionsgeräten SYS.4.1.A7: Beschränkung der administrativen Fernzugriffe auf Drucker, Kopierer und Multifunktionsgeräte SYS.4.1.A11: Einschränkung der Anbindung von Druckern, Kopierern und Multifunktionsgeräten SYS.4.1.A12: Ordnungsgemäße Entsorgung von Geräten und schützenswerten Betriebsmitteln
Weitere relevante Anforderungen	SYS.4.1.A5: Erstellung von Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten SYS.4.1.A7: Beschränkung der administrativen Fernzugriffe auf Drucker, Kopierer und Multifunktionsgeräte SYS.4.1.A15: Verschlüsselung von Informationen bei Druckern, Kopierern und Multifunktionsgeräten SYS.4.1.A17: Schutz von Nutz- und Metadaten SYS.4.1.A18: Konfiguration von Druckern, Kopierern und Multifunktionsgeräten SYS.4.1.A19: Sicheres Löschen von Informationen bei Druckern, Kopierern und Multifunktionsgeräten; SYS.4.1.A14: Authentisierung und Autorisierung bei Druckern, Kopierern und Multifunktionsgeräten SYS.4.1.A16: Notfallvorsorge bei Druckern, Kopierern und Multifunktionsgeräten SYS.4.1.A20: Erweiterter Schutz von Informationen bei Druckern, Kopierern und Multifunktionsgeräten SYS.4.1.A21: Erweiterte Absicherung von Druckern, Kopierern und Multifunktionsgeräten Zusätzliche Anforderung zum Schutz vor Diebstahl von Informationen
Hinweis	Der Baustein SYS.4.1 ist für jeden Drucker, Kopierer oder jedes Multifunktionsgerät im Informationsverbund bzw. für jede Gruppe der genannten Geräte anzuwenden.
Besonderheiten	SYS.4.1.A5 Rechtzeitig vor der Übermittlung des vorläufigen Wahlergebnisses sollten Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten erstellt und den Benutzern bekannt gemacht werden. Schutz vor Diebstahl von Informationen Gerade wenn Drucker oder Multifunktionsgeräte in Räumen stehen, die für die Öffentlichkeit zugänglich sind, sollten Vorkehrungen gegen den Diebstahl von Dokumenten eingerichtet werden. Damit sollen die Integrität und Verfügbarkeit der zu übermittelnden Information gewährleistet werden.

7.3.2.6 Virtualisierungshost

SYS.1.5 – Virtualisierung

Umsetzungs-reihenfolge	R2
Vorausgesetzte Anforderungen	SYS.1.5.A1: Einspielen von Aktualisierungen und Sicherheitsupdates SYS.1.5.A2: Sicherer Einsatz virtueller IT-Systeme SYS.1.5.A3: Sichere Konfiguration virtueller IT-Systeme SYS.1.5.A4: Sichere Konfiguration eines Netzes für virtuelle Infrastrukturen SYS.1.5.A5: Schutz der Administrationsschnittstellen SYS.1.5.A6: Protokollierung in der virtuellen Infrastruktur SYS.1.5.A7: Zeitsynchronisation in virtuellen IT-Systemen; SYS.1.5.A12: Rechte- und Rollenkonzept für die Administration einer virtuellen Infrastruktur SYS.1.5.A18: Schulung der Administratoren virtueller Umgebungen
Weitere relevante Anforderungen	SYS.1.5.A11: Administration der Virtualisierungsinfrastruktur über ein gesondertes Managementnetz SYS.1.5.A13: Auswahl geeigneter Hardware für Virtualisierungsumgebungen; SYS.1.5.A20: Verwendung von hochverfügbaren Architekturen SYS.1.5.A22: Härtung des Virtualisierungsservers SYS.1.5.A23: Rechte-Einschränkung der virtuellen Maschinen
Hinweis	Dieser Baustein kommt nur zur Anwendung, wenn auf dem Virtualisierungshost für den Prozess der Schnellmeldungen relevante Systeme betrieben werden.
Besonderheiten	SYS.1.5.A20 Im Zeitraum zur Übermittlung der Wahlergebnisse sollte die Hochverfügbarkeit bei den Virtualisierungslösungen gegeben sein.

7.3.2.7 Cloud Computing

OPS.2.2 – Cloud-Nutzung

Umsetzungs-reihenfolge	R2
Anforderungen	OPS.2.2.A1: Erstellung einer Cloud-Nutzungs-Strategie OPS.2.2.A2: Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung OPS.2.2.A3: Service-Definition für Cloud-Dienste durch den Cloud-Kunden OPS.2.2.A4: Festlegung von Verantwortungsbereichen und Schnittstellen; OPS.2.2.A6: Planung der sicheren Einbindung von Cloud-Diensten OPS.2.2.A7: Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung OPS.2.2.A9: Vertragsgestaltung mit dem Cloud-Diensteanbieter OPS.2.2.A11: Erstellung eines Notfallkonzeptes für einen Cloud-Dienst OPS.2.2.A13: Nachweis einer ausreichenden Informationssicherheit bei der Cloud-Nutzung OPS.2.2.A17: Einsatz von Verschlüsselung bei Cloud-Nutzung
Hinweis	Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software. Der Einsatz von Cloudlösungen sollte mit großer Sorgfalt geprüft und die Risiken abgewogen werden. Daher ist individuell zu untersuchen, wo im Rahmen der Schnellmeldungen Komponenten im Rahmen von Cloud Computing abgebildet wurden. Organisatorisch und technisch muss das festgelegte Schutzniveau für den Cloud-Dienst hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit sichergestellt werden. OPS.2.2 ist immer auf eine konkrete Cloud-Dienstleistung anzuwenden, welche zum Einsatz kommt bei der Ermittlung der vorläufigen Wahlergebnisse. Nutzen Wahlorgane oder -behörden unterschiedliche Cloud-Provider, so ist der Baustein für jeden Cloud-Diensteanbieter einmal anzuwenden.
Besonderheiten	---

7.3.2.8 IBM Z-System

SYS.1.7 – IBM Z-System

Umsetzungs-reihenfolge	R3
Anforderungen	SYS.1.7.A1: Einsatz restriktiver z/OS-Kennungen SYS.1.7.A2: Absicherung sicherheitskritischer z/OS-Dienstprogramme SYS.1.7.A3: Wartung von Z-Systemen SYS.1.7.A5: Einsatz und Sicherung systemnaher z/OS-Terminals SYS.1.7.A6: Einsatz und Sicherung der Remote Support Facility SYS.1.7.A7: Restriktive Autorisierung unter z/OS SYS.1.7.A8: Einsatz des z/OS-Sicherheitssystems RACF SYS.1.7.A10: Absichern des Login-Vorgangs unter z/OS SYS.1.7.A11: Schutz der Session-Daten; SYS.1.7.A13: Erstellung von Sicherheitsrichtlinien für z/OS-Systeme SYS.1.7.A15: Überprüfungen zum sicheren Betrieb von z/OS SYS.1.7.A16: Überwachung von z/OS-Systemen SYS.1.7.A18: Rollenkonzept für z/OS-Systeme SYS.1.7.A22: Absicherung der Betriebsfunktionen von z/OS SYS.1.7.A23: Absicherung von z/VM SYS.1.7.A24: Datenträgerverwaltung unter z/OS-Systemen SYS.1.7.A26: WorkLoad Management für z/OS-Systeme SYS.1.7.A27: Zeichensatzkonvertierung bei z/OS-Systemen SYS.1.7.A29: Absicherung von Unix System Services bei z/OS-Systemen SYS.1.7.A30: Absicherung der z/OS-Trace-Funktionen SYS.1.7.A31: Notfallvorsorge für z/OS-Systeme; SYS.1.7.A33: Trennung von Test- und Produktionssystemen unter z/OS SYS.1.7.A34: Batch-Job-Planung für z/OS-Systeme SYS.1.7.A35: Einsatz von RACF-Exits SYS.1.7.A36: Interne Kommunikation von Betriebssystemen SYS.1.7.A37: Parallel Sysplex unter z/OS SYS.1.7.A38: Einsatz des VTAM Session Management Exit unter z/OS
Hinweis	Der Baustein SYS.1.7 ist lediglich zu beachten, wenn IBM-Z-Systeme eine Rolle spielen bei der Ermittlung der vorläufigen Wahlergebnisse, bspw. wenn die Wahlsoftware über das IBM-Z-System läuft.
Besonderheiten	---

7.3.2.9 Speicherlösungen

SYS.1.8 – Speicherlösungen

Umsetzungs-reihenfolge	R2
Anforderungen	SYS.1.8.A1: Geeignete Aufstellung von Speichersystemen SYS.1.8.A2: Sichere Grundkonfiguration von Speicherlösungen SYS.1.8.A3: Restriktive Rechtevergabe SYS.1.8.A4: Schutz der Administrationsschnittstellen SYS.1.8.A5: Protokollierung bei Speichersystemen; SYS.1.8.A11: Sicherer Betrieb einer Speicherlösung SYS.1.8.A17: Dokumentation der Systemeinstellungen von Speichersystemen SYS.1.8.A18: Sicherheitsaudits und Berichtswesen bei Speichersystemen SYS.1.8.A20: Notfallvorsorge und Notfallreaktion für Speicherlösungen SYS.1.8.A22: Einsatz einer hochverfügbaren SAN-Lösung SYS.1.8.A24: Sicherstellung der Integrität der SAN-Fabric
Hinweis	SYS.1.8 ist relevant, wenn während der Schnellmeldungen zentrale Speicherlösungen, bestehend aus einem oder mehreren Speichernetzen sowie mindestens einem Speichersystem, hinzugezogen werden.
Besonderheiten	SYS.1.8.A22 Wenn eine hochverfügbare Speicherlösung im Rahmen der vorläufigen Wahlergebnisermittlung genutzt wird und Teil der Notfallplanung ist, sollten die Aspekte aus A22 erfüllt werden. SYS.1.8.A24 Wenn die Bedingungen für A22 erfüllt sind und zusätzlich die technische Notwendigkeit besteht, sollte A24 ebenfalls umgesetzt werden.

7.3.2.10 Wechseldatenträger

SYS.4.5 – Wechseldatenträger

Umsetzungs-reihenfolge	R3
Anforderungen	SYS.4.5.A1: Sensibilisierung der Mitarbeiter zum sicheren Umgang mit Wechseldatenträgern SYS.4.5.A2: Verlust- bzw. Manipulationsmeldung SYS.4.5.A12: Schutz vor Schadsoftware; SYS.4.5.A4: Erstellung einer Richtlinie zum sicheren Umgang mit Wechseldatenträgern SYS.4.5.A5: Regelung zur Mitnahme von Wechseldatenträgern SYS.4.5.A6: Datenträgerverwaltung SYS.4.5.A13: Angemessene Kennzeichnung der Datenträger beim Versand
Hinweis	Dieser Baustein ist auf alle Wechseldatenträger anzuwenden, welche bei der Übermittlung der vorläufigen Wahlergebnisse zum Einsatz kommen. Der Datentransport mittels Wechseldatenträger sollte nur in Notfällen, bspw. bei einem IT-Ausfall, erfolgen.
Besonderheiten	---

7.3.3 Netze

7.3.3.1 Behördennetzwerk

NET.1.1 – Netzarchitektur und -design

Umsetzungs-reihenfolge	R2
Vorausgesetzte Anforderungen	NET.1.1.A1: Sicherheitsrichtlinie für das Netz NET.1.1.A2: Dokumentation des Netzes NET.1.1.A3: Anforderungsspezifikation für das Netz NET.1.1.A4: Netztrennung in Sicherheitszonen NET.1.1.A5: Client-Server-Segmentierung NET.1.1.A6: Endgeräte-Segmentierung im internen Netz NET.1.1.A7: Absicherung von schützenswerten Informationen NET.1.1.A8: Grundlegende Absicherung des Internetzugangs NET.1.1.A9: Grundlegende Absicherung der Kommunikation mit nicht vertrauenswürdigen Netzen NET.1.1.A10: DMZ-Segmentierung für Zugriffe aus dem Internet NET.1.1.A11: Absicherung eingehender Kommunikation vom Internet in das interne Netz NET.1.1.A12: Absicherung ausgehender interner Kommunikation zum Internet NET.1.1.A13: Netzplanung NET.1.1.A14: Umsetzung der Netzplanung NET.1.1.A15: Regelmäßiger Soll-Ist-Vergleich [Informationssicherheitsbeauftragter; NET.1.1.A21: Separierung des Management-Bereichs
Weitere relevante Anforderungen	NET.1.1.A16: Spezifikation der Netzarchitektur NET.1.1.A17: Spezifikation des Netzdesigns NET.1.1.A18: P-A-P-Struktur für die Internet-Anbindung NET.1.1.A19: Separierung der Infrastrukturdienste NET.1.1.A20: Zuweisung dedizierter Subnetze für IPv4/IPv6-Endgerätegruppen
Hinweis	Der Baustein ist auf das Gesamtnetz der Behörde und auf ihre Teilnetze anzuwenden.
Besonderheiten	NET.1.1.A16 Falls möglich, sollten für die Übertragung der vorläufigen Wahlergebnisse sichere Netze und Netzübergänge eingesetzt werden.

7.3.3.2 Server- und Administrationsnetz inkl. Demilitarisierte Zone (DMZ) und Netzwerk für reguläre Arbeitsplätze

NET.1.2 – Netzmanagement

Umsetzungs-reihenfolge	R2
Vorausgesetzte Anforderungen	NET.1.2.A1: Planung des Netzmanagements NET.1.2.A2: Anforderungsspezifikation für das Netzmanagement NET.1.2.A3: Rollen- und Berechtigungskonzept für das Netzmanagement NET.1.2.A4: Grundlegende Authentisierung für den Netzmanagement-Zugriff NET.1.2.A5: Einspielen von Updates und Patches NET.1.2.A6: Regelmäßige Datensicherung NET.1.2.A7: Grundlegende Protokollierung von Ereignissen NET.1.2.A8: Zeit-Synchronisation NET.1.2.A9: Absicherung der Netzmanagement-Kommunikation NET.1.2.A10: Beschränkung der SNMP-Kommunikation; NET.1.2.A18: Schulungen für Management-Lösungen
Weitere relevante Anforderungen	NET.1.2.A11: Festlegung einer Sicherheitsrichtlinie für das Netzmanagement NET.1.2.A12: Ist-Aufnahme und Dokumentation des Netzmanagements NET.1.2.A13: Erstellung eines Netzmanagement-Konzepts NET.1.2.A15: Konzept für den sicheren Betrieb der Netzmanagement-Infrastruktur NET.1.2.A16: Einrichtung und Konfiguration von Netzmanagement-Lösungen NET.1.2.A19: Starke Authentisierung des Management-Zugriffs NET.1.2.A20: Absicherung des Zugangs zu Netzmanagement-Lösungen NET.1.2.A21: Entkopplung der Netzmanagement-Kommunikation NET.1.2.A23: Protokollierung der administrativen Zugriffe NET.1.2.A24: Zentrale Konfigurationsverwaltung für Netzkomponenten NET.1.2.A25: Statusüberwachung der Netzkomponenten NET.1.2.A26: Umfassende Protokollierung, Alarmierung und Logging von Ereignissen NET.1.2.A27: Einbindung des Netzmanagements in die Notfallplanung
Hinweis	Der Baustein ist auf jedes Netzmanagement-System (Management-System und zu verwaltendes IT-System) anzuwenden, das im Informationsverbund eingesetzt wird.
Besonderheiten	---

7.3.3.3 WLAN

NET.2.1 – WLAN-Betrieb

Umsetzungs-reihenfolge	R2
Vorausgesetzte Anforderungen	NET.2.1.A1: Festlegung einer Strategie für den Einsatz von WLANs NET.2.1.A2: Auswahl eines geeigneten WLAN-Standards NET.2.1.A3: Auswahl geeigneter Kryptoverfahren für WLAN

Umsetzungs-reihenfolge	R2
Weitere relevante Anforderungen	NET.2.1.A4: Geeignete Aufstellung von Access Points NET.2.1.A5: Sichere Basis-Konfiguration der Access Points NET.2.1.A6: Sichere Konfiguration der WLAN-Clients NET.2.1.A7: Aufbau eines Distribution Systems NET.2.1.A8: Verhaltensregeln bei WLAN-Sicherheitsvorfällen NET.2.1.A9: Sichere Anbindung von WLANs an ein LAN NET.2.1.A10: Erstellung einer Sicherheitsrichtlinie für den Betrieb von WLANs NET.2.1.A13: Regelmäßige Sicherheitschecks in WLANs NET.2.1.A14: Regelmäßige Audits der WLAN-Komponenten
Hinweis	Der Baustein enthält grundsätzliche Anforderungen, die erfüllt werden sollten, wenn WLANs aufgebaut sowie betrieben und nicht lediglich als (ersetzbarer) Träger für ein VPN verwendet werden. (Diese Anforderungen für das WLAN gelten nicht, wenn eine VPN-Verbindung für die Übertragung der Daten genutzt wird.)
Besonderheiten	---

NET.2.2 – WLAN-Nutzung

Umsetzungs-reihenfolge	R2
Anforderungen	NET.2.2.A1: Erstellung einer Benutzerrichtlinie für WLAN NET.2.2.A2: Sensibilisierung und Schulung der WLAN-Benutzer NET.2.2.A3: Absicherung der WLAN-Nutzung in unsicheren Umgebungen; NET.2.2.A4: Verhaltensregeln bei WLAN-Sicherheitsvorfällen
Hinweis	Dieser Baustein ist auf alle IT-Systeme (WLAN-Clients) im Informationsverbund anzuwenden, die zur Nutzung von WLANs verwendet werden. (Diese Anforderungen für das WLAN gelten nicht, wenn eine VPN-Verbindung für die Übertragung der Daten genutzt wird.)
Besonderheiten	---

7.3.3.4 Gebäudeübergreifende Vernetzung

NET.3.3 – VPN

Umsetzungs-reihenfolge	R2
Vorausgesetzte Anforderungen	NET.3.3.A1: Planung des VPN-Einsatzes NET.3.3.A2: Auswahl eines VPN-Dienstleisters NET.3.3.A3: Sichere Installation von VPN-Endgeräten NET.3.3.A4: Sichere Konfiguration eines VPN NET.3.3.A5: Sperrung nicht mehr benötigter VPN-Zugänge; NET.3.3.A7: Planung der technischen VPN-Realisierung NET.3.3.A11: Sichere Anbindung eines externen Netzes
Weitere relevante Anforderungen	NET.3.3.A6: Durchführung einer VPN-Anforderungsanalyse NET.3.3.A10: Sicherer Betrieb eines VPN NET.3.3.A13: Integration von VPN-Komponenten in eine Firewall
Hinweis	NET.3.3 ist für Fernzugriffe auf den Informationsverbund auf jeden VPN-Endpunkt anzuwenden.

Umsetzungs-reihenfolge	R2
Besonderheiten	NET.3.3.A6 Die Anforderungsanalyse für VPN sollte aufzeigen, wer mit wem kommunizieren wird. Gerade bei der Ermittlung von vorläufigen Wahlergebnissen, die zahlreiche Ressourcen benötigt, kann dies wichtig sein zur Prävention von Engpässen.

7.3.3.5 Router und Switches

NET.3.1 – Router und Switches

Umsetzungs-reihenfolge	R2
Vorausgesetzte Anforderungen	NET.3.1.A1: Sichere Grundkonfiguration eines Routers oder Switches NET.3.1.A2: Einspielen von Updates und Patches NET.3.1.A3: Restriktive Rechtevergabe NET.3.1.A4: Schutz der Administrationsschnittstellen NET.3.1.A5: Schutz vor Fragmentierungsangriffen NET.3.1.A6: Notfallzugriff auf Router und Switches NET.3.1.A7: Protokollierung bei Routern und Switches NET.3.1.A8: Regelmäßige Datensicherung NET.3.1.A9: Betriebsdokumentationen
Weitere relevante Anforderungen	NET.3.1.A10: Erstellung einer Sicherheitsrichtlinie NET.3.1.A18: Einrichtung von Access Control Lists
Hinweis	Der Baustein NET.3.1 Router und Switches ist auf jeden im Informationsverbund eingesetzten Router und Switch bzw. auf jede Gruppe hiervon anzuwenden.
Besonderheiten	---

7.3.3.6 Firewall

NET.3.2 – Firewall

Umsetzungs-reihenfolge	R2
Vorausgesetzte Anforderungen	NET.3.2.A1: Erstellung einer Sicherheitsrichtlinie NET.3.2.A2: Festlegen der Firewall-Regeln NET.3.2.A3: Einrichten geeigneter Filterregeln am Paketfilter NET.3.2.A4: Sichere Konfiguration der Firewall NET.3.2.A5: Restriktive Rechtevergabe NET.3.2.A6: Schutz der Administrationsschnittstellen NET.3.2.A7: Notfallzugriff auf die Firewall NET.3.2.A8: Unterbindung von dynamischem Routing NET.3.2.A9: Protokollierung NET.3.2.A10: Abwehr von Fragmentierungsangriffen am Paketfilter NET.3.2.A11: Einspielen von Updates und Patches NET.3.2.A12: Vorgehen bei Sicherheitsvorfällen NET.3.2.A13: Regelmäßige Datensicherung NET.3.2.A14: Betriebsdokumentationen NET.3.2.A15: Beschaffung einer Firewall; NET.3.2.A17: Deaktivierung von IPv4 oder IPv6 NET.3.2.A18: Administration über ein gesondertes Managementnetz NET.3.2.A19: Schutz vor TCP SYN Flooding, UDP Paket Storm und Sequence Number Guessing am Paketfilter NET.3.2.A20: Absicherung von grundlegenden Internetprotokollen
Weitere relevante Anforderungen	NET.3.2.A16: Aufbau einer „P-A-P“-Struktur NET.3.2.A23: Systemüberwachung und -Auswertung NET.3.2.A29: Einsatz von Hochverfügbarkeitslösungen
Hinweis	Der Baustein NET.3.2 ist immer auf jede Firewall des Informationsverbunds anzuwenden.
Besonderheiten	NET.3.2.A16 Für die Ebenen Länder und Bund sollte eine P-A-P-Struktur aus mehreren Komponenten aufgebaut werden. NET.3.2.A23 Firewalls sollten im Rahmen des Monitorings überwacht und Protokolldaten sollten ausgewertet werden. Damit können rechtzeitig Manipulationsversuche erkannt werden.

7.3.3.7 Telekommunikationsanlage

NET.4.1 – TK-Anlage und

NET.4.2 – VoIP

Umsetzungs-reihenfolge	R2
Vorausgesetzte Anforderungen	NET.4.1.A1: Anforderungsanalyse und Planung für TK-Anlagen NET.4.1.A2: Auswahl von TK-Diensteanbietern NET.4.1.A3: Änderung voreingestellter Passwörter NET.4.1.A4: Absicherung von Remote-Zugängen NET.4.1.A5: Protokollierung bei TK-Anlagen; NET.4.1.A7: Aufstellung der TK-Anlage NET.4.1.A10: Dokumentation und Revision der TK-Anlagenkonfiguration NET.4.1.A12: Datensicherung der Konfigurationsdateien NET.4.1.A15: Notrufe bei einem Ausfall der TK-Anlage NET.4.1.A16: Sicherung von Telefonie-Endgeräten in frei zugänglichen Räumen NET.4.2.A1: Planung des VoIP-Einsatzes NET.4.2.A2: Sichere Administration der VoIP-Middleware NET.4.2.A3: Sichere Administration und Konfiguration von VoIP-Endgeräten NET.4.2.A4: Einschränkung der Erreichbarkeit über VoIP NET.4.2.A5: Sichere Konfiguration der VoIP-Middleware NET.4.2.A6: Protokollierung bei VoIP; NET.4.2.A10: Schulung der Administratoren für die Nutzung von VoIP NET.4.2.A11: Sicherer Umgang mit VoIP-Endgeräten NET.4.2.A13: Anforderungen an eine Firewall für den Einsatz von VoIP; NET.4.2.A16: Trennung des Daten- und VoIP-Netzes
Weitere relevante Anforderungen	NET.4.1.A14: Notfallvorsorge für TK-Anlagen NET.4.1.A17: Wartung von TK-Anlagen NET.4.1.A18: Erhöhter Zugangsschutz NET.4.2.A8: Verschlüsselung von VoIP
Hinweis	Der Baustein ist für jede TK-Anlage anzuwenden, die entlang des Prozesses zur Ermittlung der Schnellmeldungen eingesetzt wird. Wenn die Kommunikation im Rahmen des Informationsverbunds per VoIP erfolgt, wird der hier ebenfalls gelistete Baustein NET.4.2 relevant.
Besonderheiten	---

7.3.3.8 Faxgerät

NET.4.3 – Faxgeräte und Faxserver

Umsetzungs-reihenfolge	R3
Vorausgesetzte Anforderungen	NET.4.3.A1: Geeignete Aufstellung eines Faxgerätes NET.4.3.A2: Informationen für Mitarbeiter über die Faxnutzung NET.4.3.A3: Sicherer Betrieb eines Faxservers; NET.4.3.A8: Geeignete Entsorgung von Fax-Verbrauchsgütern und -Ersatzteilen
Weitere relevante Anforderungen	NET.4.3.A7: Geeignete Kennzeichnung ausgehender Faxsendungen NET.4.3.A9: Nutzung von Sende- und Empfangsprotokollen NET.4.3.A10: Kontrolle programmierbarer Zieladressen, Protokolle und Verteilerlisten; NET.4.3.A12: Sperren bestimmter Empfänger- und Absender-Faxnummern NET.4.3.A13: Festlegung berechtigter Faxbediener NET.4.3.A15: Ankündigung und Rückversicherung im Umgang mit Faxsendungen
Hinweis	Der Baustein ist für jedes im Informationsverbund eingesetzte Faxgerät oder für jeden eingesetzten Faxserver anzuwenden.
Besonderheiten	NET.4.3.A7 Zur Sicherstellung der Authentizität sollten Absender und gewünschter Empfänger mit jeweils dem Namen, der Funktion und Telefonnummer auf allen ausgehenden Faxsendungen ersichtlich sein. NET.4.3.A10 Es sollte eine regelmäßige Kontrolle der im Faxgerät programmierten Zieladressen erfolgen, um eine mögliche Manipulation von Adressbüchern und Verteilerlisten vor dem Datenausgang festzustellen.

7.3.4 Anwendungen / Geschäftsprozesse

7.3.4.1 Groupware und E-Mail

APP.5.1 – Allgemeine Groupware

Umsetzungs-reihenfolge	R2
Vorausgesetzte Anforderungen	APP.5.1.A1: Sichere Installation von Groupware-Systemen APP.5.1.A2: Sichere Konfiguration der Groupware-Clients APP.5.1.A3: Sicherer Betrieb von Groupware-Systemen APP.5.1.A4: Datensicherung und Archivierung bei Groupware
Weitere relevante Anforderungen	APP.5.1.A22: Spam- und Virenschutz auf dem E-Mailserver; APP.5.1.A6: Festlegung von Vertretungsregelungen bei E-Mail-Nutzung APP.5.1.A8: Festlegung einer Sicherheitsrichtlinie für Groupware APP.5.1.A12: Schulung zu Sicherheitsmechanismen von Groupware-Clients für Benutzer APP.5.1.A16: Umgang mit SPAM durch Benutzer APP.5.1.A17: Auswahl eines Groupware- oder E-Mail-Providers APP.5.1.A18: Erweiterter Spamschutz auf dem E-Mailserver; APP.5.1.A21: Ende-zu-Ende-Verschlüsselung
Hinweis	Der Baustein muss auf jedes Groupware-System im Informationsverbund angewendet werden.

Umsetzungs-reihenfolge	R2
Besonderheiten	APP.5.1.A8 In Behörden kann der Verlust oder die Verfälschung von Daten zur Wahl die internen Fachaufgaben verzögern oder sogar unmöglich machen. Die Wahlorgane und -behörden sollten jeweils prüfen, ob die Sicherheitsrichtlinien korrekt angewendet werden. APP.5.1.A12 In vielen Tools und Anwendungen gibt es Programmierschnittstellen die es ermöglichen, den Funktionsumfang zu erweitern. Damit kann Groupware jedoch dazu missbraucht werden, Schadsoftware zu verbreiten. Administratoren sollten daher zu Sicherheitsmechanismen von Groupware-Clients geschult werden. Zudem sollten die Benutzer zu Angriffsmöglichkeiten über E-Mails sensibilisiert werden.

APP.5.2 – Microsoft Exchange und Outlook

Umsetzungs-reihenfolge	R2
Anforderungen	APP.5.2.A1: Planung des Einsatzes von Microsoft Exchange und Outlook APP.5.2.A2: Auswahl einer geeigneten Microsoft Exchange-Infrastruktur APP.5.2.A3: Berechtigungsmanagement und Zugriffsrechte APP.5.2.A5: Datensicherung von Microsoft Exchange; APP.5.2.A9: Sichere Konfiguration von Microsoft Exchange-Servern APP.5.2.A11: Absicherung der Kommunikation zwischen Microsoft Exchange-Systemen APP.5.2.A12: Einsatz von Outlook Anywhere, MAPI over HTTP und Outlook Web App APP.5.2.A19: Erstellung einer Sicherheitsrichtlinie für Microsoft Exchange Zusätzliche Anforderung zum Versand der Wahlergebnisdaten mit Microsoft Exchange und Outlook
Hinweis	Zusätzlich zum Baustein für Allgemeine Groupware ist APP.5.2 auf jedes Groupware- oder E-Mail-System anzuwenden, das auf Microsoft Exchange bzw. Outlook basiert, insofern dieses bei den Schnellmeldungen genutzt wird.
Besonderheiten	Versand der Wahlergebnisdaten mit Microsoft Exchange und Outlook Zusätzlich zu der in APP.5.1 geforderten Verschlüsselung ist auch an dieser Stelle zu erwähnen, dass Wahlergebnisdaten verschlüsselt und signiert per Microsoft Exchange und Outlook zu versenden sind. Es sollte darauf geachtet werden, dass die Schlüssel / Zertifikate gültig sind. Der Versand verschlüsselter und signierter E-Mails sollte vorab mit den beteiligten Partnern getestet werden.

7.3.4.2 Dateiablage

APP.3.3 – Fileserver

Umsetzungs-reihenfolge	R2
Vorausgesetzte Anforderungen	APP.3.3.A2: Einsatz von RAID-Systemen APP.3.3.A3: Einsatz von Viren-Schutzprogrammen APP.3.3.A5: Restriktive Rechtevergabe
Weitere relevante Anforderungen	APP.3.3.A15: Planung von Fileservern; APP.3.3.A8: Strukturierte Datenhaltung

Umsetzungs-reihenfolge	R2
Hinweis	Der Baustein ist anzuwenden, wenn im Rahmen der Schnellmeldungen Fileserver eingesetzt werden.
Besonderheiten	---

APP.3.4 – Samba

Umsetzungs-reihenfolge	R2
Anforderungen	APP.3.4.A1: Planung des Einsatzes eines Samba-Servers APP.3.4.A2: Sichere Grundkonfiguration eines Samba-Servers; APP.3.4.A3: Sichere Konfiguration des Samba-Servers APP.3.4.A4: Vermeidung der NTFS-Eigenschaften auf einem Samba-Server APP.3.4.A5: Sichere Konfiguration der Zugriffssteuerung bei einem Samba-Server APP.3.4.A6: Sichere Konfiguration von Winbind unter Samba APP.3.4.A7: Sichere Konfiguration von DNS unter Samba APP.3.4.A8: Sichere Konfiguration von LDAP unter Samba APP.3.4.A9: Sichere Konfiguration von Kerberos unter Samba APP.3.4.A10: Sicherer Einsatz externer Programme auf einem Samba-Server APP.3.4.A11: Sicherer Einsatz von Kommunikationsprotokollen beim Einsatz eines Samba-Servers APP.3.4.A12: Schulung der Administratoren eines Samba-Servers
Hinweis	Der Baustein APP.3.4 ist auf jeden Samba-Server des betrachteten Informationsverbunds anzuwenden.
Besonderheiten	---

7.3.4.3 Relationale Datenbanken

APP.4.3 – Relationale Datenbanksysteme

Umsetzungs-reihenfolge	R2
Anforderungen	APP.4.3.A1: Erstellung einer Sicherheitsrichtlinie für Datenbanksysteme APP.4.3.A2: Installation des Datenbankmanagementsystems APP.4.3.A3: Basishärtung des Datenbankmanagementsystems APP.4.3.A4: Geregeltes Anlegen neuer Datenbanken APP.4.3.A5: Benutzer- und Berechtigungskonzept APP.4.3.A6: Passwortänderung APP.4.3.A7: Zeitnahes Einspielen von Sicherheitsupdates APP.4.3.A8: Datenbank-Protokollierung APP.4.3.A9: Datensicherung eines Datenbanksystems; APP.4.3.A11: Ausreichende Dimensionierung der Hardware APP.4.3.A18: Überwachung des Datenbankmanagementsystems APP.4.3.A19: Schutz vor schädlichen Datenbank-Skripten; APP.4.3.A22: Notfallvorsorge
Hinweis	Diese Anforderungen aus APP.4.3 sind auf jedes relationale Datenbanksystem bzw. auf jede Gruppe von relationalen Datenbanksystemen einmal anzuwenden, insofern diese im Informationsverbund eingesetzt werden.
Besonderheiten	---

7.3.4.4 Office-Produkte

APP.1.1 – Office-Produkte

Umsetzungs-reihenfolge	R2
Vorausgesetzte Anforderungen	APP.1.1.A1: Sicherstellen der Integrität von Office-Produkten APP.1.1.A2: Einschränken von Aktiven Inhalten APP.1.1.A3: Sicheres Öffnen von Dokumenten aus externen Quellen APP.1.1.A4: Absichern des laufenden Betriebs von Office-Produkten; APP.1.1.A7: Installation und sichere Standardkonfiguration von Office-Produkten APP.1.1.A9: Beseitigung von Restinformationen vor Weitergabe von Dokumenten APP.1.1.A12: Verzicht auf Cloud-Speicherung APP.1.1.A13: Verwendung von Viewer-Funktionen Zusätzliche Anforderung zur Beschaffung kommunaler Anwendungen mit Schnittstellen zu Office-Produkten
Weitere relevante Anforderungen	APP.1.1.A5: Auswahl geeigneter Office-Produkte APP.1.1.A6: Testen neuer Versionen von Office-Produkten APP.1.1.A10: Regelung der Software-Entwicklung durch Endbenutzer APP.1.1.A11: Geregelter Einsatz von Erweiterungen für Office-Produkte APP.1.1.A14: Schutz gegen nachträgliche Veränderungen von Dokumenten APP.1.1.A15: Einsatz von Verschlüsselung und Digitalen Signaturen APP.1.1.A16: Integritätsprüfung von Dokumenten
Hinweis	APP.1.1 ist auf alle Office-Produkte anzuwenden, mit denen Dokumente zum Zwecke der Ermittlung des vorläufigen Wahlergebnisses betrachtet, bearbeitet oder erstellt werden.
Besonderheiten	APP.1.1.A14 Um für die Schnellmeldungen erstellte Dateien zu schützen, sollten die in den Anwendungsprogrammen vorhandenen Sicherheitsmechanismen genutzt werden.

7.3.4.5 Webbrowser

APP.1.2 – Webbrowser

Umsetzungs-reihenfolge	R2
Vorausgesetzte Anforderungen	APP.1.2.A1: Verwendung von Sandboxing APP.1.2.A2: Unterstützung sicherer Verschlüsselung der Kommunikation APP.1.2.A3: Verwendung von vertrauenswürdigen Zertifikaten APP.1.2.A4: Versionsprüfung und Aktualisierung des Webbrowsers; APP.1.2.A5: Verwendung einer zentralen Basiskonfiguration
Weitere relevante Anforderungen	APP.1.2.A8: Verwendung von Plug-ins und Erweiterungen; APP.1.2.A11: Überprüfung auf schädliche Inhalte APP.1.2.A12: Zwei-Browser-Strategie Zusätzliche Anforderung zur Kompatibilität des Webbrowsers
Hinweis	Der Baustein gilt für alle Webbrowser, die auf den Client-Systemen im Informationsverbund eingesetzt werden.

Umsetzungs-reihenfolge	R2
Besonderheiten	APP.1.2.A8 Über Webbrowser kann Schadcode aus kompromittierten Quellen geladen werden, z.B. über Plug-ins. Schadcode stellt eine Gefahr für die Daten bei den Schnellmeldungen dar. Plug-ins sollten deshalb ausschließlich aus vertrauenswürdigen Quellen bezogen werden. Der Webbrowser sollte die Möglichkeit bieten, Erweiterungen zu konfigurieren und zu deaktivieren. Kompatibilität des Webbrowsers Bevor Wahlsoftware beschafft wird, sollte die Kompatibilität mit gängigen Browsern und -versionen geprüft werden.

7.3.4.6 Webanwendungen

APP.3.1 – Webanwendungen

Umsetzungs-reihenfolge	R2
Anforderungen	APP.3.1.A1: Authentisierung bei Webanwendungen APP.3.1.A2: Zugriffskontrolle bei Webanwendungen APP.3.1.A3: Sicheres Session-Management APP.3.1.A4: Kontrolliertes Einbinden von Daten und Inhalten bei Webanwendungen APP.3.1.A5: Protokollierung sicherheitsrelevanter Ereignisse von Webanwendungen APP.3.1.A7: Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen; APP.3.1.A14: Schutz vertraulicher Daten APP.3.1.A16: Umfassende Eingabevalidierung und Ausgabekodierung APP.3.1.A19: Schutz vor SQL-Injection; APP.3.1.A8: Systemarchitektur einer Webanwendung; APP.3.1.A9: Beschaffung, Entwicklung und Erweiterung von Webanwendungen APP.3.1.A11: Sichere Anbindung von Hintergrundsystemen APP.3.1.A12: Sichere Konfiguration von Webanwendungen APP.3.1.A13: Restriktive Herausgabe sicherheitsrelevanter Informationen APP.3.1.A15: Verifikation essenzieller Änderungen APP.3.1.A17: Fehlerbehandlung APP.3.1.A21: Sichere HTTP-Konfiguration bei Webanwendungen APP.3.1.A22: Überprüfung von Webanwendungen APP.3.1.A23: Verhinderung von Cross-Site-Request-Forgery; APP.3.1.A20: Einsatz von Web Application Firewalls APP.3.1.A24: Verhinderung der Blockade von Ressourcen APP.3.1.A25: Kryptografische Sicherung vertraulicher Daten
Hinweis	Der Baustein ist auf alle Webanwendungen anzuwenden, welche zur Ermittlung des vorläufigen Wahlergebnisses eingesetzt werden.
Besonderheiten	---

7.3.4.7 Mobile Anwendungen

APP.1.4 – Mobile Anwendungen (Apps)

Umsetzungs-reihenfolge	R2
Anforderungen	APP.1.4.A1: Anforderungsanalyse für die Nutzung von Apps APP.1.4.A2: Regelungen für die Verwendung von mobilen Endgeräten und Apps APP.1.4.A3: Verwendung sicherer Quellen für Apps APP.1.4.A4: Test und Freigabe von Apps APP.1.4.A5: Minimierung und Kontrolle von App-Berechtigungen APP.1.4.A6: Patchmanagement für Apps; APP.1.4.A9: Sichere Anbindung an Backend-Systeme APP.1.4.A10: Sichere Authentisierung von Apps APP.1.4.A11: Zentrales Management von Apps; APP.1.4.A15: Durchführung von Penetrationstests für Apps
Hinweis	Dieser Baustein APP.1.4 ist anzuwenden, wenn Apps auf mobilen Endgeräten für die Ermittlung der vorläufigen Wahlergebnisse eingesetzt werden.
Besonderheiten	APP.1.4.A11 Über Prüfmechanismen eines MDM sollte sichergestellt werden, dass bei dienstlichen mobilen Endgeräten nur geprüfte und freigegebene Apps für die Ermittlung der vorläufigen Wahlergebnisse verwendet werden.

7.3.4.8 Benutzer-Authentifizierung

APP.2.1 – Allgemeiner Verzeichnisdienst

Umsetzungs-reihenfolge	R2
Vorausgesetzte Anforderungen	APP.2.1.A1: Erstellung einer Sicherheitsrichtlinie für Verzeichnisdienste APP.2.1.A2: Planung des Einsatzes von Verzeichnisdiensten APP.2.1.A3: Einrichtung von Zugriffsberechtigungen auf Verzeichnisdienste APP.2.1.A4: Sichere Installation von Verzeichnisdiensten APP.2.1.A5: Sichere Konfiguration und Konfigurationsänderungen von Verzeichnisdiensten APP.2.1.A6: Sicherer Betrieb von Verzeichnisdiensten; APP.2.1.A7: Erstellung eines Sicherheitskonzepts für den Einsatz von Verzeichnisdiensten APP.2.1.A8: Planung einer Partitionierung und Replikation im Verzeichnisdienst APP.2.1.A9: Geeignete Auswahl von Komponenten für Verzeichnisdienste APP.2.1.A10: Schulung zu Administration und Betrieb von Verzeichnisdiensten APP.2.1.A11: Einrichtung des Zugriffs auf Verzeichnisdienste APP.2.1.A12: Überwachung von Verzeichnisdiensten APP.2.1.A14: Geregelte Außerbetriebnahme eines Verzeichnisdienstes APP.2.1.A15: Migration von Verzeichnisdiensten
Weitere relevante Anforderungen	APP.2.1.A16: Erstellung eines Notfallplans für den Ausfall eines Verzeichnisdienstes
Hinweis	Der Baustein APP.2.1 ist für alle verwendeten Verzeichnisdienste im Informationsverbund anzuwenden.
Besonderheiten	---

APP.2.2 – Active Directory

Umsetzungs-reihenfolge	R2
Anforderungen	APP.2.2.A3: Planung der Gruppenrichtlinien unter Windows APP.2.2.A4: Schulung zur Active-Directory-Verwaltung APP.2.2.A5: Härtung des Active Directory APP.2.2.A7: Umsetzung sicherer Verwaltungsmethoden für Active Directory; APP.2.2.A8: Konfiguration des „Sicheren Kanals“ unter Windows APP.2.2.A9: Schutz der Authentisierung beim Einsatz von Active Directory APP.2.2.A10: Sicherer Einsatz von DNS für Active Directory
Hinweis	Der Baustein ist für alle verwendeten Verzeichnisdienste anzuwenden, die auf Microsoft Active Directory basieren, insofern diese bei der Ermittlung der vorläufigen Wahlergebnisse eine Rolle spielen.
Besonderheiten	---

APP.2.3 – OpenLDAP

Umsetzungs-reihenfolge	R2
Anforderungen	APP.2.3.A3: Sichere Konfiguration von OpenLDAP APP.2.3.A4: Konfiguration der durch OpenLDAP verwendeten Datenbank APP.2.3.A5: Sichere Vergabe von Zugriffsrechten auf dem OpenLDAP APP.2.3.A6: Sichere Authentisierung gegenüber OpenLDAP; APP.2.3.A7: Schulung von Administratoren von OpenLDAP APP.2.3.A10: Sichere Aktualisierung von OpenLDAP
Hinweis	Der Baustein ist auf jedes OpenLDAP-Verzeichnis anzuwenden, welches bei den Schnellmeldungen eine Rolle spielt.
Besonderheiten	---

8 Weitere Anforderungen an den Bund

Aufgrund des bewerteten Schutzbedarfs für die Integrität als „sehr hoch“ und die Verfügbarkeit als „sehr hoch“ sowie der Position im Prozess der Schnellmeldungen und den damit einhergehenden Risiken wurden weitere Anforderungen für den Bund als relevant identifiziert.

8.1 Prozess-Bausteine

Die folgenden Prozess-Bausteine sind, wenn nicht anders angegeben, einmal auf den gesamten Informationsverbund anzuwenden.

ORP.4 - Identitäts- und Berechtigungsmanagement

Umsetzungs-reihenfolge	R1
Anforderungen Bund	ORP.4.A20: Notfallvorsorge für das Identitäts- und Berechtigungsmanagement-System
Besonderheiten	---

OPS.1.1.2 - Ordnungsgemäße IT-Administration

Umsetzungs-reihenfolge	R1
Anforderungen Bund	OPS.1.1.2.A16: Zugangsbeschränkungen für administrative Zugänge OPS.1.1.2.A19: Berücksichtigung von Hochverfügbarkeitsanforderungen
Besonderheiten	---

OPS.1.1.4 - Schutz vor Schadprogrammen

Umsetzungs-reihenfolge	R1
Anforderungen Bund	OPS.1.1.4.A12: Einsatz von Datenträgerschleusen
Besonderheiten	---

DER.2.1 - Behandlung von Sicherheitsvorfällen

Umsetzungs-reihenfolge	R1
Anforderungen Bund	DER.2.1.A19: Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen DER.2.1.A20: Einrichtung einer internen Meldestelle für Sicherheitsvorfälle
Besonderheiten	DER.2.1.A19 Für die Behandlung von Sicherheitsvorfällen entlang des Prozesses der Schnellmeldungen sollten Prioritäten vorab festgelegt werden. DER.2.1.A20 Eine interne Meldestelle für Sicherheitsvorfälle sollte eingerichtet werden und im Zeitraum der Schnellmeldungen zur Verfügung stehen.

8.2 System-Bausteine

Nachfolgend sind die Zielobjekte (gemäß gelisteter Referenzarchitektur) mit den entsprechenden Bausteinen aufgeführt.

8.2.1 Infrastruktur

8.2.1.1 Verwaltungsgebäude

INF.1 – Allgemeines Gebäude

Umsetzungs-reihenfolge	R2
Anforderungen Bund	INF.1.A22: Sichere Türen und Fenster
Hinweis	Die Anforderungen dieses Bausteins gelten auch für die Gebäude, welche gemeinsam von Kommunen, Ländern und Bund für die vorläufige Wahlergebnisermittlung genutzt werden.
Besonderheiten	---

8.2.1.2 Serverraum / Rechenzentrum

INF.2 – Rechenzentrum sowie Serverraum

Umsetzungs-reihenfolge	R2
Anforderungen Bund	INF.2.A23: Sicher strukturierte Verkabelung im Rechenzentrum
Hinweis	INF.2 ist auf jeden selbst betriebenen Serverraum und auf jedes Rechenzentrum anzuwenden. Insofern die IT extern gehostet wird, ist mit dem jeweiligen Dienstleister die Umsetzung dieses Bausteins zu vereinbaren.
Besonderheiten	---

8.2.1.3 Raum für technische Infrastruktur

INF.5 – Raum sowie Schrank für technische Infrastruktur

Umsetzungs-reihenfolge	R2
Anforderungen Bund	INF.5.A18: Lage des Raumes für technische Infrastruktur INF.5.A19: Redundanz des Raumes für technische Infrastruktur INF.5.A20: Schutz vor Einbruch und Sabotage INF.5.A21: Redundante Leitungstrassen INF.5.A22: Redundante Auslegung der Stromversorgung INF.5.A23: Netzersatzanlage INF.5.A24: Lüftung und Kühlung INF.5.A25: Erhöhter Schutz vor Schädigung durch Brand und Rauchgase INF.5.A26: Überwachung der Energieversorgung
Hinweis	Der Baustein INF.5 ist für Räume anzuwenden, in denen technische Infrastruktur betrieben wird. Der Baustein ist ebenfalls anzuwenden, wenn stationäre Container, im Sinne eines großen Schranks, betrieben werden.
Besonderheiten	INF.5.A18 – A26 Diese Anforderungen an die physische Sicherheit dienen zur Gewährleistung der Verfügbarkeit der übermittelten Wahldaten.

8.2.2 IT-Systeme

8.2.2.1 Arbeitsplatz-PC

SYS.2.1 – Allgemeiner Client

Umsetzungs-reihenfolge	R2
Anforderungen Bund	SYS.2.1.A29: Systemüberwachung und Monitoring der Clients SYS.2.1.A31: Einrichtung lokaler Paketfilter SYS.2.1.A32: Einsatz zusätzlicher Maßnahmen zum Schutz vor Exploits SYS.2.1.A33: Application Whitelisting SYS.2.1.A34: Einsatz von Anwendungsisolation SYS.2.1.A36: Selbstverwalteter Einsatz von SecureBoot und TPM SYS.2.1.A38: Einbindung in die Notfallplanung SYS.2.1.A39: Unterbrechungsfreie und stabile Stromversorgung
Hinweis	SYS.2.1 ist für IT-Systeme mit beliebigem Betriebssystem anzuwenden, in welchen Informationen für die vorläufige Wahlergebnisermittlung erstellt, gelesen, bearbeitet, gespeichert oder versendet werden.
Besonderheiten	---

8.2.3 Netze

8.2.3.1 Router und Switches

NET.3.1 – Router und Switches

Umsetzungs-reihenfolge	R2
Anforderungen Bund	NET.3.1.A12: Erstellung einer Konfigurations-Checkliste für Router und Switches NET.3.1.A13: Administration über ein gesondertes Managementnetz NET.3.1.A14: Schutz vor Missbrauch von ICMP-Nachrichten NET.3.1.A15: Bogon- und Spoofing-Filterung NET.3.1.A16: Schutz vor „IPv6 Routing Header Type-0“-Angriffen NET.3.1.A17: Schutz vor DoS- und DDoS-Angriffen NET.3.1.A19: Sicherung von Switch-Ports NET.3.1.A20: Sicherheitsaspekte von Routing-Protokollen NET.3.1.A22: Notfallvorsorge bei Routern und Switches; NET.3.1.A25: Erweiterter Integritätsschutz für die Konfigurationsdateien NET.3.1.A26: Hochverfügbarkeit NET.3.1.A28: Einsatz von zertifizierten Produkten
Hinweis	Diese Anforderungen aus NET.3.1 sind auf jeden im Informationsverbund eingesetzten Router und Switch bzw. auf jede Gruppe hiervon anzuwenden.
Besonderheiten	---

8.2.3.2 Firewall

NET.3.2 – Firewall

Umsetzungs-reihenfolge	R2
Anforderungen Bund	NET.3.2.A24: Revision und Penetrationstests
Hinweis	Der Baustein NET.3.2 ist immer auf jede Firewall des Informationsverbunds anzuwenden.
Besonderheiten	---

8.2.4 Anwendungen / Geschäftsprozesse

8.2.4.1 Relationale Datenbanken

APP.4.3 – Relationale Datenbanksysteme

Umsetzungs-reihenfolge	R2
Anforderungen Bund	APP.4.3.A13: Restriktive Handhabung von Datenbank-Links APP.4.3.A14: Überprüfung der Datensicherung eines Datenbanksystems APP.4.3.A15: Schulung der Datenbankadministratoren; APP.4.3.A21: Einsatz von Datenbank Security Tools APP.4.3.A25: Sicherheitsüberprüfungen von Datenbanksystemen
Hinweis	Diese Anforderungen sind auf jedes relationale Datenbanksystem bzw. auf jede Gruppe von relationalen Datenbanksystemen einmal anzuwenden, insofern diese eingesetzt werden im Informationsverbund.
Besonderheiten	---

9 Anwendungshinweise

Die in Kapitel 7 und Kapitel 8 definierten Anforderungen sind, sofern vorhanden, in das Gesamtsicherheitskonzept der Wahlbehörde zu integrieren. Es sollte zeitnah entschieden werden, wann mit dem Umsetzungsprozess der Anforderungen zur Informationssicherheit begonnen wird. Die Umsetzung sollte nach einem Realisierungsplan erfolgen. Der BSI-Standard 200-1 „Managementsysteme für Informationssicherheit“ beschreibt in Kapitel 8 „Sicherheitskonzept“ ausführlich die Schritte dazu.

Für einige Bausteine des IT-Grundschutz-Kompendiums stehen Umsetzungshinweise zur Verfügung, welche detaillierte Informationen zu einzelnen Anforderungen liefern. Diese Umsetzungshinweise sind auf der Website des BSI frei zugänglich. Für eine effiziente Umsetzung können durchaus sinnvolle Clusterungen der Anforderungen vorgenommen werden. So können bspw. die in zahlreichen Bausteinen geforderten spezifischen Richtlinien für die jeweiligen IT-Systeme in wenigen, thematisch passenden Richtlinien zusammengefasst werden.

Des Weiteren ist nochmals auf die in der Praxis existierenden Differenzen zu dem in diesem Dokument vereinfacht dargestellten Informationsverbund hinzuweisen. Bei Abweichungen der genutzten Objekte der Wahlorgane und -behörden sind die Erläuterungen in Kapitel 6.3 „Umgang mit Abweichungen und Risiken" zu berücksichtigen.

In den festgelegten Revisionszyklen sind die getroffenen Entscheidungen regelmäßig auf ihre Aktualität und Angemessenheit zu überprüfen und bei Bedarf anzupassen.

Literaturverzeichnis

Arbeitsgruppe „Modernisierung IT-Grundschutz“. 2019. *IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung*. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunalverwaltung.html.

Bundesministerium des Innern. 2017. *Umsetzungsplan Bund 2017 – Leitlinie für Informationssicherheit in der Bundesverwaltung.* URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/up-bund-2017.html.

Bundesamt für Sicherheit in der Informationstechnik. 2017. *BSI-Standard 200-1, Managementsysteme für Informationssicherheit (ISMS)*. URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard201/ITGStandard201_node.html.

Bundesamt für Sicherheit in der Informationstechnik. 2017. *BSI-Standard 200-2 – IT-Grundschutz-Methodik.* URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard202/ITGStandard202_node.html.

Bundesamt für Sicherheit in der Informationstechnik. 2017. *BSI-Standard 200-3. Risikoanalyse auf der Basis von IT-Grundschutz.* URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard203/ITGStandard203_node.html.

Bundesamt für Sicherheit in der Informationstechnik. 2020. *IT-Grundschutz-Kompendium.* URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html.

Bundesamt für Sicherheit in der Informationstechnik, Referat BL 11. 2019. *Darstellung Wahlverlauf – Diskussionsgrundlage für die TR: Erweitertes Modell „5w“ aus der Bund-Länder-Arbeitsgruppe 2018 zur EU-Wahl.* Bonn.

Bundesamt für Sicherheit in der Informationstechnik, Referat BL 11. 2019. *Definition von Schutzbedarfskategorien.* Bonn.

Bund-Länder-Arbeitsgruppe. 2018. *Schutzbedarfsfeststellung für Aggregationsstufen.*

Eckert, Till. 2019. *Wahlsoftware in Deutschland vor EU-Wahl: Intransparent, unkontrolliert – und möglicherweise manipulierbar.* URL: https://correctiv.org/faktencheck/hintergrund/2019/05/25/wahlsoftware-in-deutschland-vor-eu-wahl-intransparent-unkontrolliert-und-moeglicherweise-manipulierbar.

Grieger, Raphael. 2019. *IT-Grundschutz-Profil für die obersten Landesbehörden Deutschlands.* URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Profil_oberste_landesbehoerden.pdf?__blob=publicationFile&v=4.

Schröder, Thorsten; Neumann, Linus; Tschirsich, Martin. 2017. *Analyse einer Wahlsoftware*. URL: https://linus-neumann.de/2017/09/damit-es-der-russetm-nicht-macht-ccc-hackt-die-bundestagswahl/

Zawatzka-Gerlach. 2016. *Probleme durch Meldestau und Wahlsoftware – Wahlen in Berlin akut gefährdet.* URL: https://www.tagesspiegel.de/berlin/probleme-durch-meldestau-und-wahlsoftware-wahlen-in-berlin-akut-gefaehrdet/13719090.html

Abbildungsverzeichnis

Anhang

A: Schutzbedarfskategorien

Im Folgenden sind die Beschreibungen von Schadensszenarien der drei Schutzbedarfskategorien in Anlehnung an den BSI-Standard 200-2 dargestellt. Die Tabellen dienen der Orientierung und sollten von den jeweiligen Wahlorganen und -behörden auf die eigenen Gegebenheiten angepasst werden.

Schadensszenarien	**Erläuterungen in der Schutzbedarfskategorie „normal“**
Verstoß gegen Gesetze / Vorschriften / Verträge	Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen.
Beeinträchtigung des informationellen Selbstbestimmungsrechtes	Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann. Der Schaden ist reparabel.
Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung erscheint nicht möglich.
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit liegt zwischen 24 und 72 Stunden.
Negative Außen- oder Innenwirkung	Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
Finanzielle Auswirkungen	Der finanzielle Schaden bleibt für die Institution tolerabel und kann aus dem laufenden Haushalt (Behörde, Ressort) gedeckt werden.

Tab. 1 Erläuterungen zur Schutzbedarfskategorie "normal"

Schadensszenarien	Erläuterungen in der Schutzbedarfskategorie „hoch“
Verstoß gegen Gesetze / Vorschriften / Verträge	Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen.
Beeinträchtigung des informationellen Selbstbestimmungsrechtes	Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann. Der Schaden ist irreparabel.
Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung kann nicht absolut ausgeschlossen werden.
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit liegt zwischen 1 und 24 Stunden.
Negative Außen- oder Innenwirkung	Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
Finanzielle Auswirkungen	Der Schaden bewirkt beachtliche finanzielle Verluste und muss durch über- oder außerplanmäßige Ausgaben gedeckt werden.

Tab. 2 Erläuterungen zur Schutzbedarfskategorie "hoch"

Schadensszenarien	Erläuterungen in der Schutzbedarfskategorie „sehr hoch“
Verstoß gegen Gesetze / Vorschriften / Verträge	Verstöße gegen Vorschriften und Gesetze mit fundamentalen Konsequenzen.
Beeinträchtigung des informationellen Selbstbestimmungsrechtes	Es handelt sich um personenbezogene Daten, durch deren Verarbeitung eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist.
Beeinträchtigung der persönlichen Unversehrtheit	Eine gravierende Beeinträchtigung ist möglich. Es besteht eine Gefahr für Leib und Leben.
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.
Negative Außen- oder Innenwirkung	Eine bundesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, ist denkbar.
Finanzielle Auswirkungen	Der finanzielle Schaden ist für die Institution existenzbedrohend und muss durch einen Nachtragshaushalt gedeckt werden.

Tab. 3 Erläuterungen zur Schutzbedarfskategorie "sehr hoch"

Für detaillierte Informationen und Beispiele zu den Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ kann auf den BSI-Standard 200-2, Kapitel 8.2.1 referenziert werden.