IT-Grundschutzbausteine

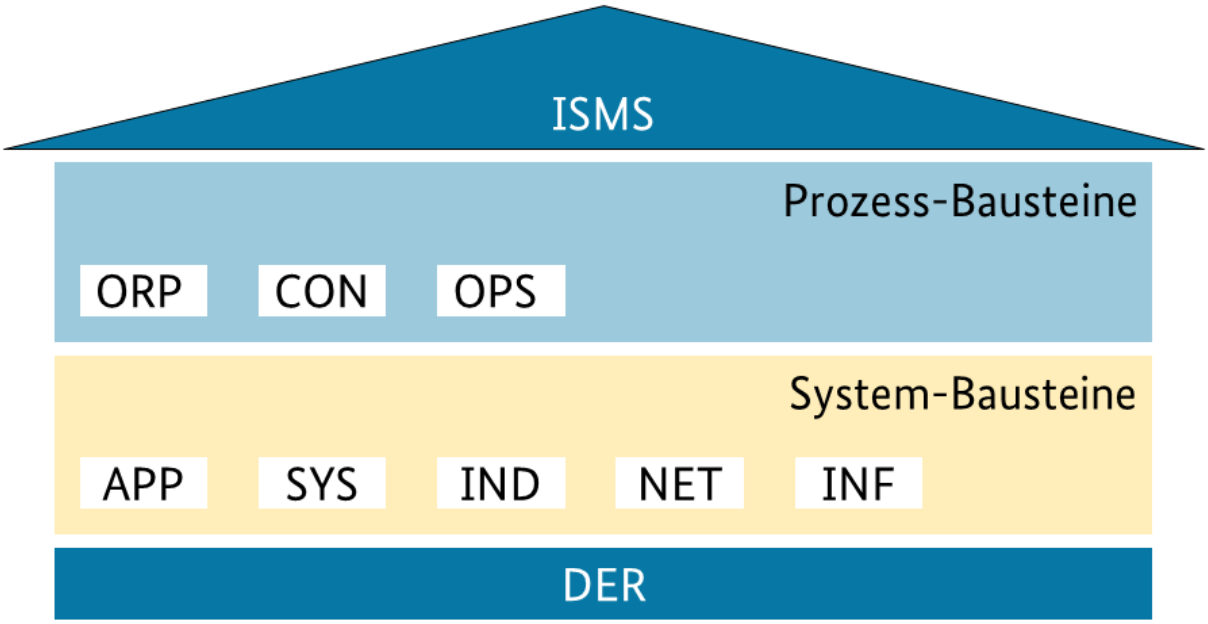
IT-Sicherheit

ITT-Net-IS

20. März 2025

1 1. Einleitung

Die IT-Grundschutzbausteine des Bundesamts für Sicherheit in der Informationstechnik (BSI) bilden einen umfassenden Katalog von Sicherheitsmaßnahmen für verschiedene IT-Umgebungen. In diesem Dokument werden die relevanten Bausteine für einen typischen Arbeitsplatz oder eine HomeOffice-Umgebung identifiziert und analysiert.



- ***ITSMS: Sicherheitsmanagementsystem***
- ***Prozessbausteine***
  - ***ORP: Organisatorische und Personal***
  - ***CON: Konzepte und Vorgehensweisen***
  - ***OPS: Betrieb***

- ***Systembausteine***
  - ***APP: Anwendungen und Dienste***
  - ***SYS: IT-Systeme***
  - ***IND: Industrielle IT***
  - ***NET: Netzwerke und Kommunikation***
  - ***INF: Infrastruktur***
- ***DER: Detektion und Reaktion***

2 ISMS - Sicherheitsmanagement

Informationssicherheitsmanagement (ISMS) umfasst **Planung**, **Lenkung** und **Kontrolle** eines Prozesses zur Herstellung von Informationssicherheit. Es muss in bestehende Managementstrukturen integriert werden und erfordert organisationsspezifische Anpassungen. Ziel ist ein funktionierendes ISMS, wofür der Baustein systematische Schritte und Anleitungen zur Konzepterstellung bietet.

Notes

- `IT_Grundschutzkompendium S. 95 ff`

3 ISMS.1 Sicherheitsmanagement

- **Relevanz**: Fundamentale Basis für die Sicherheit am Arbeitsplatz
- **Anwendung**: Definition von Sicherheitszielen und -strategien
- **Konkrete Maßnahmen**:
  - Festlegung von Sicherheitsrichtlinien für den Arbeitsplatz
  - Regelmäßige Überprüfung der Sicherheitsmaßnahmen
  - Dokumentation von Sicherheitsvorfällen

4 ORP - Organisatorische und personelle Maßnahmen

Der **ORP-Baustein** legt organisatorische Maßnahmen zur Informationssicherheit fest.

Notes

`IT_Grundschutzkompendium S. 105 ff`

4.1 ORP.1 Organisation

- **Relevanz**: Strukturierung der Sicherheitsorganisation
- **Anwendung**: Klare Zuständigkeiten und Verantwortlichkeiten
- **Konkrete Maßnahmen**:

  - Benennung eines Sicherheitsbeauftragten
  - Festlegung von Meldewegen bei Sicherheitsvorfällen

4.2 ORP.2 Personal

- **Relevanz**: Sicherheitsbewusstsein der Mitarbeiter
- **Anwendung**: Schulung und Sensibilisierung
- **Konkrete Maßnahmen**:
  - Regelmäßige Sicherheitsschulungen
  - Unterweisung in sicheres Verhalten im HomeOffice

4.3 ORP.3 Sensibilisierung und Schulung

- **Relevanz**: Kontinuierliche Weiterbildung
- **Anwendung**: Aufbau von Sicherheitskompetenz
- **Konkrete Maßnahmen**:
  - E-Learning-Module zu IT-Sicherheit
  - Regelmäßige Sicherheitstipps per E-Mail

4.4 ORP.4 Identitäts- und Berechtigungsmanagement

- **Relevanz**: Zugriffsschutz für Informationen
- **Anwendung**: Kontrolle der Zugriffsrechte
- **Konkrete Maßnahmen**:
  - Implementierung des Minimalprinzips
  - Regelmäßige Überprüfung der Zugriffsrechte

5 CON - Konzepte und Vorgehensweisen

Die **CON-Bausteine** definieren Konzepte und Vorgehensweisen zur Informationssicherheit in verschiedenen Bereichen.

Notes

```
IT_Grundschutzkompendium S. 133 ff
```

5.1 CON.1 Kryptokonzept

- **Relevanz**: Schutz vertraulicher Daten
- **Anwendung**: Verschlüsselung sensibler Informationen
- **Konkrete Maßnahmen**:
  - Einsatz von Festplattenverschlüsselung
  - Verschlüsselte E-Mail-Kommunikation
  - Sicheres Schlüsselmanagement

  - Einsatz sicherer kryptografischer Algorithmen
  - Regelmäßige Überprüfung der Kryptoverfahren

5.2 CON.2 Datenschutz

- **Relevanz**: Einhaltung datenschutzrechtlicher Vorgaben
- **Anwendung**: Schutz personenbezogener Daten
- **Konkrete Maßnahmen**:
  - Datenschutzkonforme Gestaltung des Arbeitsplatzes
  - Regelmäßige Datenschutz-Folgenabschätzungen
  - Umsetzung des Standard-Datenschutzmodells (SDM)
  - Dokumentation und Nachweise für Datenverarbeitungen

Notes

- **Standard-Datenschutzmodell (SDM)** Das **Standard-Datenschutzmodell (SDM)** ist eine Methodik der deutschen Datenschutzaufsichtsbehörden, um die Anforderungen der **DSGVO** in **technische und organisatorische Maßnahmen (TOMs)** zu überführen. Es dient zur systematischen Bewertung und Umsetzung des Datenschutzes in IT-Systemen.
- **Grundprinzipien (Gewährleistungsziele):** Das SDM übersetzt Datenschutzanforderungen in sieben Schutzziele:
  1. Datenminimierung – Nur notwendige Daten speichern/verarbeiten.
  2. Zweckbindung – Daten nur für festgelegte Zwecke nutzen.
  3. Vertraulichkeit – Schutz vor unbefugtem Zugriff.
  4. Integrität – Schutz vor Manipulation.
  5. Verfügbarkeit – Datenzugriff sicherstellen.
  6. Transparenz – Klare Information über Datenverarbeitung.
  7. Intervenierbarkeit – Rechte der Betroffenen (z. B. Löschung, Widerspruch) ermöglichen.
- **Nutzen des SDM:**
  - Erleichtert die DSGVO-konforme Gestaltung von IT-Systemen.
  - Bietet ein einheitliches Prüfschema für Behörden.
  - Unterstützt Risikoanalysen und Datenschutz-Folgenabschätzungen (DSFA).

5.3 CON.3 Datensicherungskonzept

- **Relevanz**: Schutz vor Datenverlust
- **Anwendung**: Regelmäßige Sicherung wichtiger Daten
- **Konkrete Maßnahmen**:
  - Automatisierte Backups auf externe Medien oder Cloud
  - Regelmäßige Tests der Wiederherstellungsfähigkeit
  - Sichere Aufbewahrung der Backup-Medien
  - Verschlüsselung von Backups zum Schutz der Vertraulichkeit

5.4 CON.6 Löschen und Vernichten

- **Relevanz**: Sicherstellung der vollständigen und irreversiblen Datenlöschung
- **Anwendung**: DSGVO-konforme Löschung von personenbezogenen Daten und anderen sensiblen Informationen
- **Konkrete Maßnahmen**:
  - Einsatz sicherer Löschverfahren (z. B. mehrfaches Überschreiben, physische Zerstörung)
  - Sicheres Löschen vor der Weitergabe oder Entsorgung von IT-Geräten
  - Dokumentation der Lösch- und Vernichtungsvorgänge
  - Regelmäßige Kontrolle der Löschprozesse zur Vermeidung von Datenlecks

5.5 CON.7 Informationssicherheit auf Auslandsreisen

- **Relevanz**: Schutz von Unternehmens- und persönlichen Daten bei Reisen
- **Anwendung**: Maßnahmen zur Minimierung von Sicherheitsrisiken außerhalb der sicheren IT-Umgebung
- **Konkrete Maßnahmen**:
  - Nutzung von VPNs für sichere Verbindungen
  - Verschlüsselung mobiler Datenträger
  - Reduzierung mitgeführter sensibler Daten
  - Sicherstellung von sicheren Kommunikationskanälen

5.6 CON.8 Software-Entwicklung

- **Relevanz**: Gewährleistung von Sicherheit bereits in der Entwicklungsphase
- **Anwendung**: Integration sicherer Programmierpraktiken
- **Konkrete Maßnahmen**:
  - Einsatz sicherer Coding-Praktiken (z. B. OWASP Top 10 beachten)
  - Durchführung regelmäßiger Sicherheitsreviews und Penetrationstests
  - Nutzung von statischen und dynamischen Code-Analysen
  - Sichere Speicherung und Verarbeitung von Benutzerdaten

Notes

- **OWASP (Open Web Application Security Project)**

OWASP ist eine gemeinnützige Organisation, die sich der Sicherheit von Webanwendungen widmet. Sie bietet freie, offene Ressourcen, Tools und Best Practices, um Entwickler, Sicherheitsexperten und Unternehmen dabei zu unterstützen, Sicherheitslücken in Anwendungen zu identifizieren und zu beheben.
OWASP Top 10
Die OWASP Top 10 ist eine regelmäßig aktualisierte Liste der kritischsten Sicherheitsrisiken für Webanwendungen. Diese Liste basiert auf einer umfassenden Analyse realer Sicherheitslücken, die in Webanwendungen weltweit gefunden wurden. Sie dient als grundlegender Leitfaden für Entwickler und Sicherheitsexperten, um Sicherheitsprobleme in ihren Anwendungen zu priorisieren und zu beheben.

- **Die aktuelle OWASP Top 10 (Stand 2021 - Aktualisierung für 2025 geplant)**:
  1. Broken Access Control – Unzureichende Zugriffskontrollen ermöglichen Angreifern unbefugten Zugriff auf Daten oder Funktionen.
  2. Cryptographic Failures – Fehler in der Verschlüsselung oder unsichere Speicherung von Daten führen zu Datenschutzverletzungen.
  3. Injection – Angriffe wie SQL-Injection oder Command-Injection, die durch unsichere Eingabeverarbeitung entstehen.
  4. Insecure Design – Sicherheitsprobleme aufgrund schlechter Architektur und Design-Entscheidungen.
  5. Security Misconfiguration – Unsichere Standardkonfigurationen oder falsch gesetzte Sicherheitsoptionen.
  6. Vulnerable and Outdated Components – Verwendung veralteter oder unsicherer Softwarekomponenten (z. B. Libraries oder Frameworks).
  7. Identification and Authentication Failures – Schwächen in der Authentifizierung, z. B. unsichere Passwörter oder Session-Handling-Probleme.
  8. Software and Data Integrity Failures – Unsichere Software-Updates oder ungeschützte Datenintegrität, z. B. durch fehlende Signaturen.
  9. Security Logging and Monitoring Failures – Unzureichende Protokollierung und Überwachung, die Angriffe schwer erkennbar machen.
  10. Server-Side Request Forgery (SSRF) – Angriffe, bei denen ein Server dazu gebracht wird, ungewollte externe oder interne Anfragen zu senden.

5.7 CON.10 Entwicklung von Webanwendungen

- **Relevanz**: Schutz vor Angriffen auf Webanwendungen
- **Anwendung**: Entwicklung robuster Webanwendungen mit hohen Sicherheitsstandards
- **Konkrete Maßnahmen**:
  - Schutz gegen Cross-Site-Scripting (XSS) und SQL-Injection
  - Nutzung sicherer Authentifizierungsmechanismen
  - Einsatz von Content Security Policies (CSP)
  - Regelmäßige Updates und Patches für eingesetzte Frameworks

Notes

- **XSS (Cross-Site Scripting) Cross-Site Scripting (XSS)** ist eine **Sicherheitslücke** in Webanwendungen, bei der Angreifer schädlichen **JavaScript-Code** in Webseiten einschleusen. Dieser Code wird dann im Browser anderer Nutzer ausgeführt, um Daten zu stehlen, Sitzungen zu kapern oder Schadcode zu verbreiten.
  - **Arten von XSS**
    - **Stored XSS** – Schadcode wird dauerhaft in der Datenbank gespeichert und bei jedem Aufruf der Seite ausgeführt.
    - **Reflected XSS** – Schadcode wird über eine manipulierte URL oder Formularfelder eingeschleust und sofort zurückgesendet.
    - **DOM-based XSS** – Manipulation des DOMs durch unsichere JavaScript-Verarbeitung.
  - **Schutzmaßnahmen gegen XSS**
    - **Input-Validierung:** Eingaben filtern und bereinigen.
    - **Output-Encoding:** HTML, JavaScript und URL-Inhalte korrekt maskieren.
    - **Content Security Policy (CSP):** Skript-Ausführung einschränken.
    - **Escape-Techniken:** Zeichen wie < > & ” ’ maskieren.
- **SQL-Injection (SQLi)** SQL-Injection (SQLi) ist eine kritische Sicherheitslücke, bei der ein Angreifer schädliche SQL-Befehle in eine Datenbank-Abfrage einschleust. Dadurch kann er Daten lesen, manipulieren oder sogar löschen.
  - **Arten von SQL-Injection**
    - **Classic SQLi** – Direkte Manipulation von SQL-Abfragen über Eingabefelder.
    - **Blind SQLi** – Angreifer erhält keine direkte Rückmeldung, kann aber durch Ja/Nein-Antworten Daten exfiltrieren.
    - **Time-based SQLi** – Verzögerungen in der Antwortzeit zeigen an, ob eine Abfrage erfolgreich war.
  - Beispiel für eine unsichere SQL-Abfrage

```
1 SELECT * FROM users WHERE username = '"␣+␣user_input␣+␣"' AND password = '"␣+
    ␣pass_input␣+␣"'";
```

Angriff: admin’ – könnte die Passwortprüfung umgehen.

Notes

- **Schutzmaßnahmen gegen SQL-Injection:**
  - **Prepared Statements & Parameterized Queries** – Ersetzen Benutzereingaben durch sichere Platzhalter.
  - **Eingabevalidierung** – Nur erwartete Werte zulassen.
  - **Least Privilege Prinzip** – Datenbankbenutzer mit minimalen Rechten.
  - **Web Application Firewall (WAF)** – Erkennung und Blockierung von SQLi-Versuchen.
- **Content Security Policy (CSP) Content Security Policy (CSP)** ist eine **Sicherheitsrichtlinie für Webanwendungen**, die den Ladevorgang und die Ausführung von Inhalten im Browser steuert. Sie schützt vor verschiedenen Angriffen, indem sie einschränkt, welche Ressourcen (z. B. Skripte, Styles, Frames) von einer Webseite geladen werden dürfen.
  - **Schutz durch CSP**
    - Verhindert Cross-Site Scripting (XSS) – Blockiert unerlaubte Skripte.
    - Schützt vor Code-Injection – Begrenzung externer Skriptquellen.
    - Reduziert das Risiko von Clickjacking – Kontrolle über eingebettete Inhalte.
    - Erschwert Datendiebstahl durch unsichere Verbindungen – Erzwingt HTTPS.
  - **Wichtige CSP-Regeln:**
    - `default-src 'self'` – Erlaubt Inhalte nur von der eigenen Domain.
    - `script-src 'self' https://trusted.cdn.com` – Kontrolle über erlaubte Skriptquellen.
    - `style-src 'self' 'unsafe-inline'` – Einschränkung von CSS-Quellen.
    - `frame-ancestors 'none'` – Schutz vor Clickjacking durch iFrames.

5.8 CON.11.1 Geheimschutz

- **Relevanz**: Schutz von Verschlusssachen und sensiblen Informationen
- **Anwendung**: Einhaltung spezieller Geheimhaltungsanforderungen
- **Konkrete Maßnahmen**:
  - Einsatz von Verschlusssachentresoren
  - Regelmäßige Sicherheitsüberprüfungen des Personals
  - Strenge Zugangskontrollen zu geheimhaltungsbedürftigen Informationen
  - Einsatz von sicheren Kommunikationswegen für vertrauliche Daten

6 OPS - Betrieb und Organisation

Die **OPS-Bausteine** definieren Anforderungen an einen sicheren IT-Betrieb und die organisatorischen Prozesse in Institutionen. Dabei werden drei Bereiche unterschieden:

OPT 1 Eigener Betrieb

OPT 2 Betrieb von Dritten (Outsourcing)

OPS 3 Betrieb für Dritte

Notes

IT_Grundschutzkompendium S. 200 ff

6.1 OPS 1 Eigener Betrieb

Dieser Abschnitt behandelt die Identifikation potenzieller Gefährdungen sowie die erforderlichen Maßnahmen zur Absicherung des eigenen IT-Betriebs innerhalb des Unternehmens.

6.1.1 OPS.1.1 Allgemeiner IT-Betrieb

- **Relevanz**: Sicherstellung eines reibungslosen und sicheren IT-Betriebs
- **Anwendung**: Standardisierte Prozesse für IT-Administration, Betrieb und Monitoring
- **Konkrete Maßnahmen**:
  - Dokumentation und Inventarisierung der IT-Ressourcen
  - IT-Monitoring zur frühzeitigen Erkennung von Problemen
  - Festlegung von Zuständigkeiten und Rollen
  - Patch- und Änderungsmanagement zur Absicherung der IT-Infrastruktur
  - Sicherstellung von Personalkapazitäten und Schulungen für Betriebspersonal

Notes

- **Patch** Ein **Patch** ist eine Aktualisierung oder Korrektur für eine Software, ein Betriebssystem oder eine Anwendung. Patches werden veröffentlicht, um:
  - Sicherheitslücken zu schließen,
  - Fehler (Bugs) zu beheben,
  - die Leistung oder Kompatibilität zu verbessern,
  - neue Funktionen hinzuzufügen.

6.1.2 OPS 1.2 Weiterführende Aufgaben

- **Relevanz**: Ergänzung des allgemeinen IT-Betriebs um spezifische organisatorische und technische Aufgaben zur Sicherstellung der IT-Sicherheit und Effizienz.
- **Anwendung**: Festlegung und Umsetzung erweiterter Maßnahmen für Archivierung, Telearbeit, Fernwartung und Zeitsynchronisation.
- **Konkrete Maßnahmen**:
  - IT-Dokumentation: Systematische Erfassung und Pflege von IT-Dokumentationen
  - Archivierung: Sichere und langfristige Speicherung elektronischer Dokumente
  - IT-Notfallmanagement: Minimierung von Betriebsunterbrechungen und schnellen Wiederherstellung nach Ausfällen.
  - Telearbeit: Gewährleistung des Schutzes sensibler Daten.
  - Fernwartung: verschlüsselte Verbindungen und kontrollierte Authentifizierung
  - NTP-Zeitsynchronisation: Präzise Zeitsteuerung innerhalb des Netzwerks

6.2 OPS 2 Betrieb von Dritten

Hier geht es um die Sicherstellung und Überwachung von IT-Dienstleistungen, die von externen Dienstleistern erbracht werden (Outsourcing).

6.2.1 OPS.2.2 Cloud-Nutzung

- **Relevanz**: Sicherstellung der Informationssicherheit bei der Nutzung von Cloud-Diensten
- **Anwendung**: Identifikation und Umsetzung von Sicherheitsmaßnahmen bei Cloud-Diensten
- **Konkrete Maßnahmen**:
  - Erstellung einer Cloud-Strategie mit Sicherheitsanforderungen
  - Definition klarer Verantwortlichkeiten und Schnittstellen
  - Einführung von Richtlinien zur sicheren Cloud-Nutzung
  - Integration von Sicherheitsmaßnahmen in Cloud-Verträge
  - Regelmäßige Überprüfung der Cloud-Sicherheitsmaßnahmen

6.2.2 OPS.2.3 Nutzung von Outsourcing

- **Relevanz**: Sicherstellung der Informationssicherheit bei der Auslagerung von IT-Prozessen
- **Anwendung**: Identifikation und Umsetzung von Sicherheitsmaßnahmen im Outsourcing
- **Konkrete Maßnahmen**:
  - Erstellung einer Outsourcing-Strategie mit Sicherheitsanforderungen
  - Vermeidung von Abhängigkeiten durch Multi-Sourcing-Ansätze
  - Einführung von Sicherheitsrichtlinien für Outsourcing-Dienstleister
  - Regelmäßige Überprüfung und Auditierung der Outsourcing-Partner
  - Definition von Notfall- und Exit-Strategien für ausgelagerte IT-Dienste

Notes

- **Was ist ein Audit / eine Auditierung** Ein **Audit** oder eine **Auditierung** ist eine systematische Überprüfung und Bewertung von IT-Systemen, Prozessen oder Sicherheitsmaßnahmen. Ziel eines Audits ist es, die Einhaltung von Richtlinien, Standards oder gesetzlichen Vorgaben zu überprüfen. Arten von Audits:
  - **Interne Audits**: Durch das eigene Unternehmen zur Selbstkontrolle durchgeführt.
  - **Externe Audits**: Von unabhängigen Prüfstellen oder Behörden durchgeführt.
  - **Sicherheitsaudits**: Fokus auf IT-Sicherheit und Datenschutz.
  - **Compliance-Audits**: Überprüfung der Einhaltung von Normen (z. B. ISO 27001, DSGVO).

6.3 OPS 3 Betrieb für Dritte

Dieser Abschnitt beschreibt, welche Aspekte zu beachten sind, wenn das eigene Unternehmen IT-Dienstleistungen für externe Kunden erbringt.

6.3.1 OPS.3.2 Anbieten von Outsourcing

- **Relevanz**: Sicherstellung der Informationssicherheit durch Anbieter von Outsourcing-Dienstleistungen
- **Anwendung**: Implementierung und Einhaltung von Sicherheitsmaßnahmen im Outsourcing-Prozess
- **Konkrete Maßnahmen**:
  - Implementierung eines Informationssicherheitsmanagements zur Einhaltung der Schutzziele
  - Definition einheitlicher Vertragsanforderungen mit Sicherheitsklauseln
  - Weitergabe vertraglicher Sicherheitsanforderungen an Sub-Dienstleister
- Umsetzung eines Mandantentrennungskonzepts zur Datensicherheit
- Erstellung eines Sicherheitskonzepts für jede Outsourcing-Dienstleistung
- Regelung zur Beendigung eines Outsourcing-Verhältnisses mit sicherer Datenrückgabe und -löschung
- Durchführung regelmäßiger Audits und Überprüfungen der Outsourcing-Partner
- Einführung einer Notfall- und Exit-Strategie für ausgelagerte IT-Dienste

7 APP - Anwendungen und Dienste

IT-Anwendungen sind ein zentraler Bestandteil moderner IT-Infrastrukturen. Sie umfassen Office-Produkte, Webbrowser, mobile Anwendungen und viele weitere Softwarelösungen, die zur Verarbeitung und Verwaltung von Informationen verwendet werden. Aufgrund ihrer Verbreitung und Funktionalität stellen sie ein potenzielles Sicherheitsrisiko dar. Der IT-Grundschutz stellt Anforderungen an die sichere Nutzung und Konfiguration dieser Anwendungen, um Bedrohungen zu minimieren und Datenschutz sowie Informationssicherheit zu gewährleisten.

7.1 APP 1 Anwendungen

7.1.1 APP.1.1 Office-Produkte

- **Relevanz**: Standard-Software am Arbeitsplatz
- **Anwendung**: Sichere Konfiguration der Office-Programme
- **Konkrete Maßnahmen**:
  - Deaktivierung unsicherer Makro-Funktionen
  - Regelmäßige Updates der Office-Programme
  - Nutzung sicherer Dokumentenformate
  - Schulung der Benutzer:innen zu sicheren Office-Einstellungen

Notes

- Makros Makros sind kleine Programme oder Skripte, die innerhalb von Office-Anwendungen wie Microsoft Word oder Excel ausgeführt werden können. Sie werden oft in der Programmiersprache VBA (Visual Basic for Applications) geschrieben und ermöglichen die Automatisierung wiederkehrender Aufgaben, wie das Formatieren von Dokumenten, das Erstellen von Tabellen oder das Ausführen komplexer Berechnungen. Während Makros die Produktivität steigern können, stellen sie jedoch auch ein erhebliches Sicherheitsrisiko dar. Angreifer können schädliche Makros in Office-Dokumenten verstecken, die beim Öffnen automatisch ausgeführt werden und beispielsweise Schadsoftware nachladen oder Daten stehlen. Daher ist es eine bewährte Sicherheitsmaßnahme, Makros standardmäßig zu deaktivieren und nur signierte oder vertrauenswürdige Makros zuzulassen.

7.1.2 APP.1.2 Webbrowser

- **Relevanz**: Hauptzugriffspunkt auf Internet-Ressourcen
- **Anwendung**: Absicherung des Browsers
- **Konkrete Maßnahmen**:
  - Installation von Sicherheits-Erweiterungen
  - Deaktivierung unsicherer Browser-Funktionen
  - Nutzung eines sicheren Passwortmanagers
  - Aktivierung von HTTPS-Only-Modus und DNS-over-HTTPS

Notes

- **Sicherheits-Erweiterungen**: Browser-Add-ons oder Plugins, die zusätzliche Sicherheitsfunktionen bereitstellen, etwa zur Blockierung von Werbung, zum Schutz vor Phishing oder zur Verhinderung der Ausführung schädlicher Skripte.
- **Unsichere Browser-Funktionen**: Funktionen oder Einstellungen im Browser, die potenziell Sicherheitslücken öffnen können, beispielsweise automatische Ausführung von Skripten, veraltete Protokolle oder nicht benötigte Features, die als Einfallstor für Angriffe dienen könnten.
- **Sicherer Passwortmanager**: Eine Softwarelösung, die Passwörter sicher speichert, verwaltet und bei Bedarf generiert. Dabei werden die gespeicherten Daten verschlüsselt, sodass sie nur von autorisierten Benutzern eingesehen werden können.
- **HTTPS-Only-Modus**: Eine Einstellung im Browser, die sicherstellt, dass ausschließlich HTTPS-Verbindungen (also verschlüsselte Verbindungen) aufgebaut werden, um die Vertraulichkeit und Integrität der übertragenen Daten zu gewährleisten.
- **DNS-over-HTTPS (DoH)**: Eine Technik, bei der DNS-Anfragen über das HTTPS-Protokoll verschlüsselt übertragen werden, um zu verhindern, dass diese Anfragen von Dritten abgefangen oder manipuliert werden können.

7.1.3 APP.1.3 E-Mail-Clients

- **Relevanz**: Zentrales Kommunikationsmittel in Unternehmen
- **Anwendung**: Schutz vor Phishing und Malware in E-Mails
- **Konkrete Maßnahmen**:

- Aktivierung von Spam- und Phishing-Filtern
- Deaktivierung aktiver Inhalte (Makros, JavaScript) in Anhängen
- Nutzung sicherer Authentifizierungsverfahren (z. B. 2FA)
- Regelmäßige Schulungen zur Erkennung von Phishing-Mails

Notes

Erklärungen unklarer Begriffe:

- **Spam- und Phishing-Filter**: Softwaremechanismen, die unerwünschte oder betrügerische E-Mails erkennen und automatisch in den Spam-Ordner verschieben. Phishing-Filter identifizieren speziell E-Mails, die versuchen, Benutzer:innen zur Herausgabe vertraulicher Informationen zu verleiten.
- **Aktive Inhalte (Makros, JavaScript) in Anhängen**: Programme oder Skripte, die in E-Mail-Anhängen eingebettet sein können und beim Öffnen automatisch ausgeführt werden. Diese werden häufig für Angriffe genutzt, um Schadsoftware zu verbreiten oder Daten zu stehlen.
- **Sichere Authentifizierungsverfahren (z. B. 2FA)**: Methoden zur sicheren Anmeldung, die über ein einfaches Passwort hinausgehen. Bei der Zwei-Faktor-Authentifizierung (2FA) wird zusätzlich ein zweiter Faktor wie ein Einmalpasswort (OTP) oder eine Bestätigung über eine App benötigt.
- **Phishing-Mails**: Betrügerische E-Mails, die darauf abzielen, Nutzer:innen zur Preisgabe sensibler Daten (z. B. Passwörter, Kreditkarteninformationen) zu bewegen. Sie erscheinen oft als legitime Nachrichten von bekannten Unternehmen oder Personen.
- **Schulungen zur Erkennung von Phishing-Mails**: Maßnahmen zur Sensibilisierung von Mitarbeitenden, um verdächtige E-Mails anhand typischer Merkmale wie gefälschten Absenderadressen, ungewöhnlichen Anhängen oder dringlichen Handlungsaufforderungen zu erkennen.

7.1.4 APP.1.4 Mobile Anwendungen (Apps)

- **Relevanz**: Nutzung von Smartphones und Tablets im Arbeitsumfeld
- **Anwendung**: Sichere Verwaltung und Nutzung von Apps
- **Konkrete Maßnahmen**:
  - Einschränkung der App-Berechtigungen
  - Nutzung von Mobile Device Management (MDM) zur zentralen Steuerung
  - Vermeidung unsicherer Cloud-Speicherlösungen
  - Absicherung der Datenkommunikation über VPN

Notes

- **App-Berechtigungen**: Zugriffsrechte, die eine App auf Funktionen oder Daten eines Mobilgeräts erhält, z. B. Kamera, Mikrofon, Kontakte oder Standort. Zu viele oder unnötige Berechtigungen können ein Sicherheitsrisiko darstellen.
- **Mobile Device Management (MDM)**: Eine zentrale Verwaltungsplattform, mit der IT-Abteilungen mobile Geräte im Unternehmensumfeld konfigurieren, steuern und absichern können. Dazu gehören u. a. das Erzwingen von Sicherheitsrichtlinien, die Fernlöschung von Daten und die Verwaltung installierter Apps.
- **Unsichere Cloud-Speicherlösungen**: Cloud-Dienste, die keine ausreichenden Sicherheitsmechanismen wie Verschlüsselung, Zugriffskontrollen oder Datenschutzrichtlinien bieten. Unsichere Cloud-Nutzung kann zu Datenlecks oder unbefugtem Zugriff führen.
- **VPN (Virtual Private Network)**: Eine Technologie zur sicheren, verschlüsselten Verbindung zwischen einem Gerät und einem privaten Netzwerk über das Internet. VPNs schützen vor Datenabgriff in unsicheren Netzwerken, indem sie den Datenverkehr verschlüsseln und die Identität des Nutzers verschleiern.

7.2 APP.2 Verzeichnisdienste

7.2.1 APP.2.1 Allgemeiner Verzeichnisdienst

- **Relevanz**: Zentrale Verwaltung von Benutzer- und Ressourcendaten
- **Anwendung**: Schutz der Verzeichnisdienstdaten und Absicherung der Authentifizierung
- **Konkrete Maßnahmen**:
  - Erstellung einer Sicherheitsrichtlinie für Verzeichnisdienste
  - Planung des Einsatzes von Verzeichnisdiensten
  - Sichere Konfiguration und Betrieb des Verzeichnisdienstes
  - Einschränkung und Kontrolle der Zugriffsrechte

Notes

- **Verzeichnisdienst**: Eine zentrale Datenbank oder Infrastruktur, die Benutzer, Gruppen, Computer, Geräte und andere Ressourcen verwaltet. Sie ermöglicht eine einheitliche Authentifizierung und Autorisierung innerhalb eines Netzwerks.
- **Sicherheitsrichtlinie**: Dokumentierte Vorgaben und Regeln zur sicheren Nutzung und Verwaltung des Verzeichnisdienstes. Dazu gehören Zugriffskontrollen, Passwortanforderungen und Sicherheitsmaßnahmen zur Verhinderung unbefugter Zugriffe.
- **Einschränkung und Kontrolle der Zugriffsrechte**: Umsetzung des Prinzips der geringsten Berechtigungen (Least Privilege), sodass Benutzer:innen nur die für ihre Aufgaben notwendigen Rechte erhalten. Dies verhindert unautorisierte Zugriffe und reduziert potenzielle Sicherheitslücken.

7.2.2 APP.2.2 Active Directory Domain Services (AD DS)

- **Relevanz**: Verwaltung von Windows-basierten IT-Infrastrukturen
- **Anwendung**: Absicherung der Authentifizierungs- und Berechtigungsverwaltung

- **Konkrete Maßnahmen**:
  - Härtung von Domänencontrollern und AD-DS-Konten
  - Sichere Konfiguration von Vertrauensbeziehungen
  - Begrenzung der Berechtigungen und Anmeldeprivilegien
  - Nutzung sicherer Authentisierungsmechanismen (Kerberos)

Notes

- **Active Directory Domain Services (AD DS)**: Ein Verzeichnisdienst von Microsoft zur Verwaltung von Benutzern, Computern und Ressourcen in einem Windows-Netzwerk. AD DS ermöglicht zentrale Authentifizierung, Autorisierung und Verwaltung von Sicherheitsrichtlinien.
- **Domänencontroller (DC)**: Server, die AD DS bereitstellen und alle Authentifizierungsanfragen im Netzwerk verwalten. Eine Härtung der Domänencontroller beinhaltet Maßnahmen wie das Deaktivieren unnötiger Dienste, die Einschränkung administrativer Zugriffe und regelmäßige Sicherheitsupdates.
- **Kerberos**: Ein sicheres Authentifizierungsprotokoll, das verschlüsselte Tickets verwendet, um Benutzer:innen innerhalb eines Netzwerks zu identifizieren. Die Nutzung von Kerberos erhöht die Sicherheit, da Passwörter nicht im Klartext übertragen werden.

7.2.3 APP.2.3 OpenLDAP

- **Relevanz**: Open-Source-Alternative für Verzeichnisdienste
- **Anwendung**: Sicherer Betrieb und Nutzung von OpenLDAP
- **Konkrete Maßnahmen**:
  - Planung und Auswahl von Backends und Overlays für OpenLDAP
  - Sichere Konfiguration von OpenLDAP und seiner Laufzeitumgebung
  - Kontrolle der Zugriffsrechte und sichere Authentisierung
  - Einschränkung von Attributen und Partitionierung des Verzeichnisses

Notes

- **OpenLDAP**: Eine Open-Source-Implementierung des Lightweight Directory Access Protocol (LDAP), die für die zentrale Verwaltung von Benutzern, Gruppen und Ressourcen in einem Netzwerk verwendet wird. OpenLDAP ermöglicht eine flexible Authentifizierung und Autorisierung von Nutzern.
- **Backends** sind die Speichermodule in OpenLDAP, die definieren, wie und wo Daten gespeichert werden (z. B. ‘mdb‘, ‘hdb‘).
- **Overlays** sind Erweiterungen, die zusätzliche Funktionen für LDAP-Datenbanken bieten, wie Passwort-Richtlinien, Replikation oder Zugriffskontrolle.
- **Partitionierung des Verzeichnisses** ermöglicht eine Aufteilung der LDAP-Datenbank in mehrere logische Einheiten, um Lastverteilung und Sicherheit zu verbessern.

7.3 APP.3 Netzbasierte Dienste

7.3.1 APP.3.1 Webanwendungen und Webservices

- **Relevanz**: Nutzung von Webanwendungen und Webservices im internen und externen Netzwerk
- **Anwendung**: Schutz der Daten und Sicherstellung der Verfügbarkeit
- **Konkrete Maßnahmen**:
  - Sichere Authentisierung und Protokollierung von Zugriffen
  - Kontrolle der Einbindung externer Inhalte
  - Schutz vor unberechtigter automatisierter Nutzung
  - Sicherstellung der sicheren Speicherung von Zugangsdaten
  - Regelmäßige Sicherheitsüberprüfungen und Penetrationstests

7.3.2 APP.3.2 Webserver

- **Relevanz**: Basis für den Betrieb von Webanwendungen
- **Anwendung**: Absicherung des Webservers gegen Angriffe und Missbrauch
- **Konkrete Maßnahmen**:
  - Sichere Konfiguration und Minimierung der Angriffsfläche
  - Verschlüsselung über TLS und sichere Authentisierung
  - Schutz vor Denial-of-Service-Angriffen
  - Regelmäßige Integritätsprüfungen und Penetrationstests

Notes

- **Denial-of-Service-Angriffe**: versuchen, Webserver durch übermäßige Anfragen lahmzulegen.

7.3.3 APP.3.3 Fileserver

- **Relevanz**: Zentrale Bereitstellung von Dateien im Netzwerk
- **Anwendung**: Schutz von gespeicherten Daten vor Verlust und Manipulation
- **Konkrete Maßnahmen**:
  - Planung und Strukturierung der Datenhaltung
  - Einsatz von Speicherbeschränkungen und Schutzmechanismen gegen Schadsoftware
  - Regelmäßige Überprüfung der Speicherintegrität
  - Sicherstellung einer zuverlässigen Datensicherung

7.3.4 APP.3.4 Samba

- **Relevanz**: Bereitstellung von Datei- und Druckdiensten zwischen Windows- und Linux-Systemen
- **Anwendung**: Absicherung von Samba-Diensten gegen unberechtigten Zugriff
- **Konkrete Maßnahmen**:
  - Sichere Grundkonfiguration und Einschränkung von Standardfreigaben

- Schutz der Samba-Kommunikation durch Verschlüsselung
- Einschränkung der Berechtigungen für Benutzer und Dienste
- Regelmäßige Sicherung und Kontrolle der Samba-Registry

7.3.5 APP.3.6 DNS-Server

- **Relevanz**: Zentrale Komponente zur Namensauflösung in Netzwerken
- **Anwendung**: Absicherung der DNS-Infrastruktur gegen Manipulation und Ausfälle
- **Konkrete Maßnahmen**:
  - Einsatz redundanter DNS-Server
  - Schutz vor DNS-Cache-Poisoning und anderen Manipulationsversuchen
  - Sichere Konfiguration von Zonentransfers und Anfragen
  - Regelmäßige Überprüfung der DNS-Server-Protokolle auf Anomalien

Notes

- **Redundanter DNS-Server**:
  - Redundante DNS-Server sorgen für Ausfallsicherheit und Lastverteilung.
  - Primäre und sekundäre DNS-Server sollten geografisch verteilt sein, um gegen Netzwerkausfälle resilient zu sein.
- **DNS-Cache-Poisoning und Manipulationsschutz**:
  - Beim **DNS-Cache-Poisoning** wird ein DNS-Cache durch gefälschte Einträge manipuliert, sodass Benutzer:innen auf betrügerische Seiten umgeleitet werden.
  - Schutzmaßnahmen beinhalten den Einsatz von DNSSEC (Domain Name System Security Extensions), Query Name Minimization und regelmäßige Cache-Invalidierung.
- **Zonentransfers**:
  - Zonentransfers (AXFR/IXFR) erlauben die Replikation von DNS-Daten zwischen Servern. Unautorisierte Transfers können sensible DNS-Daten preisgeben.
  - Zonentransfers sollten nur zwischen autorisierten Servern über verschlüsselte Verbindungen (z. B. TSIG) erlaubt sein.
- **Verschlüsselung:**
  - DNS-Anfragen sollten über DNS-over-TLS (DoT) oder DNS-over-HTTPS (DoH) verschlüsselt werden, um Abhörversuche zu verhindern.

7.4 APP.4 Business-Anwendungen

7.4.1 APP.4.2 SAP-ERP-System

- **Relevanz**: Automatisierung und Unterstützung interner sowie externer Geschäftsprozesse
- **Anwendung**: Sicherer Betrieb und Konfiguration von SAP-ERP-Systemen
- **Konkrete Maßnahmen**:
  - Berücksichtigung der SAP-Sicherheitsleitfäden
  - Regelmäßiges Einspielen von Patches und SAP-Sicherheitshinweisen

- Planung und Umsetzung eines SAP-Berechtigungskonzeptes
- Dokumentation und Notfallkonzepte für SAP-Systeme

Notes

- **SAP-ERP-System (Enterprise Resource Planning)**:
  - Eine integrierte Unternehmenssoftware von SAP, die Geschäftsprozesse wie Finanzen, Logistik, Personalwesen und Produktion verwaltet.
  - ERP-Systeme ermöglichen eine zentrale und effiziente Steuerung von Unternehmensressourcen.

7.4.2 APP.4.3 Relationale Datenbanken

- **Relevanz**: Verwaltung großer Datensammlungen mit hohen Sicherheitsanforderungen
- **Anwendung**: Schutz der Datenbanken vor Manipulation und unbefugtem Zugriff
- **Konkrete Maßnahmen**:
  - Erstellung einer Sicherheitsrichtlinie für Datenbanken
  - Restriktive Handhabung von Datenbank-Berechtigungen
  - Verschlüsselung der Datenbankanbindung
  - Schutz vor SQL-Injection und unsicheren Datenbank-Skripten

Notes

- **SQL-Injection** ist eine Angriffsart, bei der manipulierte SQL-Befehle über Eingabefelder eingeschleust werden, um unautorisierten Zugriff auf Daten zu erhalten.
  - Schutzmaßnahmen umfassen:
    * Nutzung von vorbereiteten Anweisungen (**Prepared Statements**)
    * Validierung und Bereinigung von Benutzereingaben
    * Einschränkung der Datenbankrechte für Web-Anwendungen
- Unsichere Skripte, die SQL-Abfragen dynamisch generieren, sollten vermieden oder stark abgesichert werden.

7.4.3 APP.4.4 Kubernetes

- **Relevanz**: Orchestrierung von Containern in modernen IT-Infrastrukturen
- **Anwendung**: Schutz und Absicherung von Kubernetes-Clustern
- **Konkrete Maßnahmen**:
  - Mangelhafte Authentisierung und Autorisierung in der Control Plane verhindern
  - Planung der Separierung von Anwendungen in Kubernetes-Namespaces
  - Umsetzung von Netzwerk-Segmentierung für Kubernetes-Pods
  - Nutzung sicherer Service-Accounts und Automatisierungsprozesse

Notes

- **Kubernetes**:
  - Ein Open-Source-System zur Automatisierung der Bereitstellung, Skalierung und Verwaltung von containerisierten Anwendungen.
  - Ermöglicht effiziente Ressourcenverwaltung und hohe Verfügbarkeit von Anwendungen.
- **Control Plane**:
  - Die zentrale Steuerungsebene von Kubernetes, die für die Verwaltung des gesamten Clusters zuständig ist.
  - Besteht aus Komponenten wie API-Server, Scheduler und Controller-Manager.
  - Eine fehlerhafte oder ungesicherte Control Plane kann Angreifern ermöglichen, den Cluster zu kompromittieren.
- **Kubernetes-Namespaces**:
  - Kubernetes-Namespaces ermöglichen eine logische Trennung innerhalb eines Clusters.
  - Anwendungen oder Teams können in getrennten Namespaces arbeiten, um Zugriffsrechte zu isolieren und Sicherheitsrisiken zu minimieren.
- **Netzwerk-Segmentierung für Kubernetes-Pods**:
  - Kubernetes-Pods (die kleinste ausführbare Einheit in Kubernetes) sollten durch Netzwerk-Richtlinien voneinander isoliert werden.
  - Dies verhindert, dass kompromittierte Pods unkontrolliert auf andere Dienste zugreifen können.
  - Tools wie **Calico** oder **Cilium** helfen, granulare Netzwerkregeln umzusetzen.

7.4.4 APP.4.6 SAP ABAP-Programmierung

- **Relevanz**: Eigenentwicklungen in SAP-Systemen erfordern besondere Sicherheitsmaßnahmen
- **Anwendung**: Sichere Entwicklung und Verwaltung von ABAP-Programmen
- **Konkrete Maßnahmen**:
  - Implementierung sicherer Programmierpraktiken in ABAP
  - Schutz vor unbefugtem Code-Zugriff und Manipulation
  - Integration von Berechtigungsprüfungen in ABAP-Anwendungen
  - Regelmäßige Code-Audits und Sicherheitsüberprüfungen

7.5 APP.5 E-Mail/Groupware/Kommunikation

7.5.1 APP.5.2 Microsoft Exchange und Outlook

- **Relevanz**: Groupware-Lösung für mittlere bis große Institutionen
- **Anwendung**: Sicherer Betrieb und Nutzung von Microsoft Exchange und Outlook
- **Konkrete Maßnahmen**:
  - Planung des Einsatzes von Exchange und Outlook
  - Auswahl einer geeigneten Exchange-Infrastruktur
  - Berechtigungsmanagement und Zugriffsrechte

- Sichere Konfiguration von Exchange-Servern und Outlook-Clients
- Absicherung der Kommunikation zwischen Exchange-Systemen
- Schutz vor unzulässigem Browserzugriff und unsachgemäßer Anbindung anderer Systeme

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

- **Relevanz**: Grundlegende E-Mail-Kommunikation in Institutionen
- **Anwendung**: Schutz der E-Mail-Infrastruktur und sichere Nutzung von E-Mail-Clients
- **Konkrete Maßnahmen**:
  - Sichere Konfiguration der E-Mail-Clients
  - Sicherer Betrieb von E-Mail-Servern
  - Datensicherung und Archivierung von E-Mails
  - Spam- und Virenschutz auf dem E-Mail-Server
  - Nutzung von SPF, DKIM und DMARC zur E-Mail-Authentifizierung
  - Förderung einer Ende-zu-Ende-Verschlüsselung und Signatur

7.5.3 APP.5.4 Unified Communications und Collaboration (UCC)

- **Relevanz**: Integration moderner Kommunikationsdienste in IT-Umgebungen
- **Anwendung**: Sicherer Betrieb und Nutzung von UCC-Diensten
- **Konkrete Maßnahmen**:
  - Planung und Netzwerkintegration von UCC-Diensten
  - Regelmäßiges Testen der UCC-Komponenten
  - Sichere Konfiguration und Berechtigungsmanagement für UCC
  - Verschlüsselung der UCC-Kommunikation und Daten
  - Absicherung von KI-Funktionen und Vermeidung von Identitätsmanipulation
  - Einschränkung von Metadaten-Speicherung und Sichtbarkeit für Administratoren

7.6 APP.6 Allgemeine Software

7.6.1 APP.6.1 Einführung in Allgemeine Software

- **Relevanz**: Betrifft jegliche Software im Informationsverbund
- **Anwendung**: Sicherheit über den gesamten Software-Lebenszyklus gewährleisten
- **Konkrete Maßnahmen**:
  - Planung, Beschaffung, Installation, Betrieb und Außerbetriebnahme sicher gestalten
  - Sicherheitsanforderungen in den gesamten Software-Lebenszyklus integrieren
  - Vermeidung fehlerhafter Konfigurationen und unsicherer Software-Quellen
  - Regelmäßige Sicherheitsüberprüfungen und Updates einplanen

7.6.2 APP.6.2 Sicherheitsanforderungen an Allgemeine Software

- **Relevanz**: Erfüllt die grundlegenden Anforderungen an sichere Software-Nutzung
- **Anwendung**: Sicherstellung der Software-Integrität und Schutz vor Manipulation
- **Konkrete Maßnahmen**:
  - Erstellung eines Anforderungskatalogs für Software
  - Sichere Beschaffung von Software aus vertrauenswürdigen Quellen
  - Regelung zur sicheren Installation und Konfiguration
  - Sicherstellung regelmäßiger Software-Updates und Sicherheits-Patches
  - Inventarisierung eingesetzter Software zur Sicherheitsüberwachung

7.7 APP.7 Entwicklung von Individualsoftware

7.7.1 APP.7.1 Planung und Anforderungen für Individualsoftware

- **Relevanz**: Betrifft Institutionen, die maßgeschneiderte Software entwickeln oder beauftragen
- **Anwendung**: Berücksichtigung von Sicherheitsaspekten bereits in der Planungsphase
- **Konkrete Maßnahmen**:
  - Definition von Sicherheitsanforderungen für Individualsoftware
  - Geeignete Steuerung des Entwicklungsprozesses sicherstellen
  - Dokumentation der Sicherheitsfunktionen und Systemintegration
  - Einbindung von Fachverantwortlichen in alle Entwicklungsphasen
  - Berücksichtigung von gesetzlichen und regulatorischen Anforderungen

7.7.2 APP.7.2 Sicherer Entwicklungsprozess und Betrieb

- **Relevanz**: Betrifft sowohl intern als auch extern entwickelte Softwarelösungen
- **Anwendung**: Schutz von Software-Entwicklungsprozessen vor Sicherheitsrisiken
- **Konkrete Maßnahmen**:
  - Vorgaben für sichere Software-Architektur und Codequalität definieren
  - Durchführung sicherheitsorientierter Tests und Code-Reviews
  - Berücksichtigung sicherer Entwicklungspraktiken (z. B. Secure Coding)
  - Nutzung von sicheren Entwicklungsumgebungen mit Zugriffskontrolle
  - Sicherstellung der Nachvollziehbarkeit und Dokumentation des Codes

7.7.3 APP.7.3 Anforderungen an Individualsoftware mit erhöhtem Schutzbedarf

- **Relevanz**: Notwendig für sicherheitskritische Anwendungen und Systeme
- **Anwendung**: Gewährleistung hoher Sicherheitsstandards in besonders sensiblen Bereichen
- **Konkrete Maßnahmen**:
  - Beauftragung zertifizierter Software-Entwicklungsunternehmen
  - Nutzung geprüfter Entwicklungsframeworks mit Sicherheitsgarantien

- Einrichtung eines Escrow-Mechanismus zur Quellcode-Hinterlegung
- Durchsetzung strengerer Sicherheitskontrollen für Zugriffsrechte und Berechtigungen
- Sicherstellung einer kontinuierlichen Sicherheitsüberwachung der Individualsoftware

8 SYS - IT-Systeme

Der Baustein **SYS - IT-Systeme** behandelt die Sicherheit verschiedener IT-Komponenten, darunter Server, Desktop- und mobile Endgeräte sowie spezielle Systeme wie Drucker, IoT-Geräte und Wechseldatenträger. Er beschreibt typische Bedrohungen, wie unbefugten Zugriff, Datenverlust und Manipulation, sowie Maßnahmen zur Absicherung, darunter Zugriffskontrollen, Verschlüsselung und regelmäßige Updates. Besondere Schwerpunkte liegen auf der Härtung von Betriebssystemen, Netzwerksicherheit und sicheren Nutzungskonzepten für IT-Geräte. Ziel ist es, die Verfügbarkeit, Vertraulichkeit und Integrität der IT-Infrastruktur zu gewährleisten und Risiken durch organisatorische und technische Schutzmaßnahmen zu minimieren.

8.1 SYS.1 Server

Folgende Serverlösungen werden behandelt:

1. Allgemeine Server
2. Windows-Server
3. Linux- und Unix-Server
4. Hochverfügbarkeitslösungen
5. Virtualisierung
6. Containerisierung
7. IBM-Z-Server
8. Speicherlösungen
9. Backup und Wiederherstellung

8.1.1 SYS.1.1 Allgemeiner Server

- **Relevanz**: Zentrale IT-Komponente zur Bereitstellung von Diensten
- **Anwendung**: Schutz der auf Servern verarbeiteten Informationen und Dienste
- **Konkrete Maßnahmen**:
  - Physische Zugriffsbeschränkung auf Serverräume
  - Strikte Rollen- und Rechtevergabe (Least Privilege-Prinzip)
  - Regelmäßige Sicherheitsupdates und Patch-Management
  - Einsatz von Virenschutz-Programmen und Intrusion Detection Systemen
  - Protokollierung und Überwachung sicherheitsrelevanter Ereignisse
  - Deaktivierung nicht benötigter Dienste und Schnittstellen
  - Einbindung in Notfallmanagement und Sicherheitsrichtlinien

8.1.2 SYS.1.2 Windows-Server

- **Relevanz**: Häufig genutztes Betriebssystem für Serverumgebungen
- **Anwendung**: Sicherstellung einer robusten Konfiguration und Administration von Windows-Servern
- **Konkrete Maßnahmen**:
  - Nutzung von Active Directory für zentrale Authentifizierung
  - Härtung des Betriebssystems durch Gruppenrichtlinien (GPOs)
  - Schutz vor Schadsoftware durch signierte Software und AppLocker
  - Einschränkung von Fernzugriffen (z. B. RDP-Gateway)
  - Minimierung von Telemetrie- und Diagnosedatenübertragungen
  - Regelmäßige Sicherheitsprüfungen und forensische Analysen

8.1.3 SYS.1.3 Linux- und Unix-Server

- **Relevanz**: Weit verbreitete Serverplattform für kritische IT-Dienste
- **Anwendung**: Absicherung und Härtung von Unix- und Linux-Servern
- **Konkrete Maßnahmen**:
  - Einsatz sicherer SSH-Konfigurationen und Schlüsselmanagement
  - Keine unnötigen Root-Rechte für Anwendungen (Least Privilege)
  - Nutzung von Mandatory Access Control (z. B. SELinux, AppArmor)
  - Härtung des Kernels durch ASLR, DEP/NX und Stackschutz
  - Deaktivierung unnötiger Dienste und Ports
  - Einsatz von Paketmanagement aus vertrauenswürdigen Quellen
  - Regelmäßige Überprüfung der Systemintegrität (z. B. AIDE, Tripwire)

8.1.4 SYS.1.4 Hochverfügbarkeitslösungen

- **Relevanz**: Sicherstellung der kontinuierlichen Verfügbarkeit kritischer IT-Dienste
- **Anwendung**: Absicherung und Redundanzkonzepte für hochverfügbare Systeme
- **Konkrete Maßnahmen**:
  - Einsatz von Cluster-Technologien und Failover-Mechanismen
  - Nutzung redundanter Netzwerkanbindungen und Stromversorgungen
  - Regelmäßige Tests von Ausfallszenarien und Notfallwiederherstellung
  - Implementierung von Datenreplikationstechniken für Konsistenz und Verfügbarkeit

8.1.5 SYS.1.5 Virtualisierung

- **Relevanz**: Effiziente Ressourcennutzung und flexible Bereitstellung von IT-Diensten
- **Anwendung**: Sicherstellung der Isolation und Sicherheit virtueller Umgebungen
- **Konkrete Maßnahmen**:
  - Einschränkung von Administratorrechten in Virtualisierungsumgebungen
  - Strikte Trennung von Netzwerken für Management- und Betriebsfunktionen

- Nutzung von sicheren Images aus vertrauenswürdigen Quellen
- Verschlüsselung und sichere Speicherung von Zugangsdaten für virtuelle Maschinen
- Einführung von Monitoring- und Audit-Mechanismen für Virtualisierungsplattformen

8.1.6 SYS.1.6 Containerisierung

- **Relevanz**: Standardisierte Bereitstellung und Portabilität von Anwendungen
- **Anwendung**: Absicherung und Härtung von Container-Umgebungen
- **Konkrete Maßnahmen**:
  - Nutzung minimaler, gehärteter Basis-Images
  - Einschränkung von Root-Rechten innerhalb von Containern
  - Überwachung von Container-Logs und Speicherung außerhalb des Containers
  - Trennung von Container-Netzwerken zur Minimierung von Angriffsflächen
  - Implementierung von Signaturen und Verifikationen für Container-Images

8.1.7 SYS.1.7 IBM Z (z/OS)

- **Relevanz**: Hochskalierbare Unternehmens-IT-Infrastruktur mit speziellen Sicherheitsanforderungen
- **Anwendung**: Schutz und Härtung von z/OS-Systemen
- **Konkrete Maßnahmen**:
  - Restriktive Vergabe von Hochprivilegierten Benutzerrechten (RACF)
  - Trennung von Test- und Produktionsumgebungen zur Vermeidung von Sicherheitsrisiken
  - Implementierung von Workload-Management und Batch-Job-Scheduling
  - Nutzung interner Kanäle für Betriebssystemkommunikation (HiperSockets)
  - Sicherstellung der Systemintegrität durch regelmäßige Audits und Notfallvorsorge

8.1.8 SYS.1.8 Speicherlösungen

- **Relevanz**: Sichere und effiziente Verwaltung von Unternehmensdaten
- **Anwendung**: Schutz sensibler Daten in Speicherumgebungen
- **Konkrete Maßnahmen**:
  - Verwendung von Verschlüsselung für gespeicherte Daten und Übertragungen
  - Regelmäßige Überprüfung und Aktualisierung der Speicherinfrastruktur
  - Umsetzung eines Sicherheitsrichtlinienkonzepts für Speicherlösungen
  - Implementierung von Zugriffskontrollen und Mandantentrennung (LUN Masking, VSANs)
  - Zentrale Überwachung und Verwaltung von Speicherlösungen zur Erkennung von Anomalien

8.1.9 SYS.1.9 Backup und Wiederherstellung

- **Relevanz**: Gewährleistung der Datenverfügbarkeit bei Systemausfällen
- **Anwendung**: Entwicklung von Backup-Strategien und Notfallwiederherstellungsplänen
- **Konkrete Maßnahmen**:
  - Nutzung redundanter Speichermedien zur Absicherung kritischer Daten
  - Implementierung von Offsite- und Air-Gapped-Backups zum Schutz vor Ransomware
  - Regelmäßige Überprüfung der Backup-Integrität und Testen der Wiederherstel

8.2 SYS.2 Desktop-Systeme

Hier werden Best-Practices für folgende Desktoplösungen beschrieben:

1. Allgemeine Clients
2. Windows-Clients
3. Linux- und Unix-Clients
4. macOS-Clients
5. Client-Virtualisierung
6. Virtual Desktop Infrastruktur

8.2.1 SYS.2.1 Allgemeiner Client

- **Relevanz**: Grundlegendes IT-System für den Endnutzer
- **Anwendung**: Absicherung von Arbeitsplatzrechnern unabhängig vom Betriebssystem
- **Konkrete Maßnahmen**:
  - Trennung von Administrations- und Benutzerumgebungen
  - Starke Benutzerauthentifizierung und Nutzung von Bildschirmsperren
  - Aktivierung von Autoupdate-Mechanismen für Sicherheitsaktualisierungen
  - Verwendung von Schutzprogrammen gegen Schadsoftware
  - Absicherung des Bootvorgangs gegen Manipulation
  - Minimierung von Cloud- und Online-Funktionen

8.2.2 SYS.2.2 Windows-Clients

- **Relevanz**: Weit verbreitetes Client-Betriebssystem in Unternehmen
- **Anwendung**: Schutzmaßnahmen für Windows-Systeme, insbesondere Windows 10 und 11
- **Konkrete Maßnahmen**:
  - Planung der Nutzung von Cloud-Diensten unter Windows
  - Auswahl geeigneter Windows-Versionen mit langfristigem Support
  - Einschränkung von Telemetrie- und Datenschutzeinstellungen
  - Nutzung sicherer Authentifizierungsmethoden (z. B. Kerberos, NTLMv2)
  - Absicherung von Datei- und Freigabeberechtigungen
  - Einschränkung von Microsoft-Store- und Online-Konto-Funktionen
  - Sichere Konfiguration von Remote-Zugriffen (z. B. RDP, Remote-Unterstützung)

8.2.3 SYS.2.3 Linux- und Unix-Clients

- **Relevanz**: Alternative zu Windows mit hoher Sicherheit und Anpassbarkeit
- **Anwendung**: Härtung von Linux- und Unix-Clients
- **Konkrete Maßnahmen**:
  - Auswahl geeigneter Distributionen mit langfristigem Support
  - Regelmäßige Kernel-Aktualisierungen und Live-Patching
  - Strikte Rechtevergabe und Nutzung von SELinux oder AppArmor
  - Einschränkung der automatischen Einbindung von Wechseldatenträgern
  - Schutz von Systemdateien durch restriktive Mount-Optionen
  - Sicherer Umgang mit Skriptsprachen und gemeinsam genutzten Bibliotheken

8.2.4 SYS.2.4 macOS-Clients

- **Relevanz**: Betriebssystem für Apple-Geräte mit speziellen Sicherheitsanforderungen
- **Anwendung**: Absicherung von macOS-Systemen in Unternehmen
- **Konkrete Maßnahmen**:
  - Nutzung von FileVault für die Verschlüsselung von Festplatten
  - Absicherung der Systemintegrität mit Gatekeeper und SIP (System Integrity Protection)
  - Einschränkung von Apple-ID-gebundenen Funktionen
  - Verwaltung und Härtung von macOS-Geräten durch MDM-Lösungen
  - Deaktivierung unnötiger Cloud- und Synchronisationsdienste
  - Strenge Kontrolle von Drittanbieter-Anwendungen und Berechtigungen

8.2.5 SYS.2.5 Client-Virtualisierung

- **Relevanz**: Effiziente Nutzung von Hardware-Ressourcen durch zentrale Verwaltung virtueller Clients
- **Anwendung**: Absicherung und Performance-Optimierung virtualisierter Clients
- **Konkrete Maßnahmen**:
  - Planung des Einsatzes virtueller Clients, basierend auf Leistungs- und Sicherheitsanforderungen
  - Nutzung von sicheren Templates zur Provisionierung neuer virtueller Clients
  - Absicherung der Kommunikation zwischen Virtualisierungsserver und Client
  - Minimierung von lokalen Datenablagen, um Datenverlust zu verhindern
  - Automatische Sperrung von Sitzungen und Härtung der Clients gegen unautorisierte Änderungen
  - Einbindung in zentrale Patch- und Änderungsmanagement-Systeme
  - Erweiterte Protokollierung und Monitoring virtueller Clients zur Bedrohungserkennung
  - Hochverfügbare Bereitstellung und Redundanzstrategien für Virtualisierungsinfrastrukturen

8.2.6 SYS.2.6 Virtual Desktop Infrastructure (VDI)

- **Relevanz**: Zentralisierte Bereitstellung und Verwaltung standardisierter virtueller Desktops
- **Anwendung**: Sichere und leistungsfähige Implementierung einer VDI-Lösung
- **Konkrete Maßnahmen**:
  - Planung der benötigten VDI-Kapazitäten anhand der Nutzeranforderungen
  - Sichere Installation und Konfiguration der VDI-Komponenten gemäß Herstellerempfehlungen
  - Regelmäßige Aktualisierung der VDI-Templates, um Software-Schwachstellen zu vermeiden
  - Netzsegmentierung der VDI-Komponenten zur Isolation sicherheitskritischer Systeme
  - Redundanzkonzepte und Hochverfügbarkeit für kritische VDI-Dienste
  - Integration der VDI in ein Security Information and Event Management (SIEM)
  - Nutzung nicht-persistenter Clients zur Reduzierung von Sicherheitsrisiken
  - Strikte Zugriffskontrollen und Absicherung der VDI-Managementsysteme gegen Missbrauch

8.3 SYS.3 Mobile Devices

Im mobile Bereich werden folgende Lösungen beschrieben:

1. Laptops
2. Tablets und Smartphones
3. Mobiltelefone

8.3.1 SYS.3.1 Laptops

- **Relevanz**: Weit verbreitete mobile Arbeitsgeräte mit erhöhtem Schutzbedarf
- **Anwendung**: Schutzmaßnahmen für die Nutzung von Laptops in Institutionen
- **Konkrete Maßnahmen**:
  - Absicherung des Bootvorgangs und der Firmware (Secure Boot, BIOS/UEFI-Passwort)
  - Einsatz von Festplattenverschlüsselung (z. B. BitLocker, LUKS)
  - Regelmäßige Aktualisierung des Betriebssystems und der installierten Software
  - Schutz vor physischem Zugriff (Kensington-Schlösser, sichere Aufbewahrung)
  - Nutzung von VPN für sichere Verbindungen zu Unternehmensnetzen
  - Deaktivierung nicht benötigter Schnittstellen (USB, Bluetooth, WLAN)
  - Integration in zentrale IT-Sicherheitsrichtlinien und Verwaltungssysteme
  - Regelmäßige Sicherung der gespeicherten Daten

8.3.2 SYS.3.2 Tablets und Smartphones

- **Relevanz**: Zunehmend genutzte Alternative zu Laptops für mobile Arbeitsumgebungen
- **Anwendung**: Sicherstellung eines sicheren Einsatzes von Tablets im Unternehmenskontext
- **Konkrete Maßnahmen**:
  - Nutzung von Geräteverschlüsselung zum Schutz sensibler Daten

- Einschränkung von App-Installationen auf vertrauenswürdige Quellen
- Einsatz von Mobile Device Management (MDM) zur zentralen Verwaltung
- Kontrolle der Cloud-Synchronisation und Datenfreigaben
- Deaktivierung von nicht benötigten drahtlosen Schnittstellen (Bluetooth, NFC)
- Verwendung von Multi-Faktor-Authentifizierung für kritische Anwendungen
- Regelmäßige Sicherheitsupdates und Überprüfung auf Schwachstellen

8.3.3 SYS.3.3 Mobiltelefone

- **Relevanz**: Weit verbreitete mobile Kommunikationsgeräte mit sicherheitskritischen Aspekten
- **Anwendung**: Absicherung von dienstlich genutzten Mobiltelefonen
- **Konkrete Maßnahmen**:
  - Definition und Durchsetzung einer Sicherheitsrichtlinie für Mobiltelefone
  - Aktivierung und Nutzung verfügbarer Sicherheitsmechanismen (z. B. PIN-Schutz, SIM-Lock)
  - Regelmäßige Sicherheitsupdates und Firmware-Aktualisierungen
  - Sensibilisierung der Benutzer für sicheres Telefonieverhalten und Phishing-Angriffe
  - Nutzung von Mechanismen zur Fernlöschung und Sperrung bei Verlust oder Diebstahl
  - Kontrolle und Einschränkung von installierbaren Apps auf dienstlichen Geräten
  - Begrenzung der Nutzung drahtloser Schnittstellen (Bluetooth, NFC, WLAN) auf das Notwendige
  - Absicherung der Datenübertragung durch VPN und verschlüsselte Kommunikation
  - Einrichtung eines Mobiltelefon-Pools für häufig wechselnde Benutzer
  - Maßnahmen zur Minimierung der Erstellung von Bewegungsprofilen durch Dritte
  - Sicherstellung der ordnungsgemäßen Entsorgung und Löschung von Geräten und Speicherkarten

8.4 SYS.4 Sonstige Systeme

Hier werden Lösung für weitere wichtige IT-Komponente beschrieben:

1. Drucker, Kopierer und Multifunktionsgeräte
2. Eingebettete Systeme (Embedded Systems)
3. IoT-Geräte
4. Wechseldatenträger

8.4.1 SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte

- **Relevanz**: Verarbeitung vertraulicher Informationen und Anbindung an IT-Netzwerke erfordern besondere Sicherheitsmaßnahmen
- **Anwendung**: Schutz von gedruckten, gescannten und gespeicherten Dokumenten sowie Netzwerksicherheit
- **Konkrete Maßnahmen**:
  - Zugriffskontrolle und Authentifizierung am Gerät (Secure Print, PIN-Freigabe)
  - Regelmäßige Firmware-Updates zur Schließung von Schwachstellen

- Verschlüsselung gespeicherter und übertragener Daten
- Einschränkung von Schnittstellen (USB, SD-Karten, WLAN) auf notwendige Funktionen
- Sichere Entsorgung von Geräten und Speichermedien
- Netzsegmentierung zur Trennung von Druck- und Unternehmensnetzwerken
- Logging und Monitoring von Druck- und Scanjobs zur Nachvollziehbarkeit

8.4.2 SYS.4.3 Eingebettete Systeme

- **Relevanz**: Weit verbreitete spezialisierte IT-Systeme mit sicherheitskritischen Anwendungen
- **Anwendung**: Schutz und Härtung von eingebetteten Systemen in Unternehmens- und Industrieumgebungen
- **Konkrete Maßnahmen**:
  - Einschränkung von Debugging- und Entwicklerschnittstellen
  - Verwendung eines sicheren Boot-Prozesses und verifizierter Firmware
  - Regelmäßige Sicherheitsprüfungen und Patching-Mechanismen implementieren
  - Schutz vor physischem Zugriff durch robuste Gehäuse und Manipulationsschutz
  - Minimierung von Netzwerkschnittstellen und Absicherung gegen unbefugten Fernzugriff
  - Nutzung von Hardware-Trust-Mechanismen wie TPM oder Secure Boot

8.4.3 SYS.4.4 Allgemeines IoT-Gerät

- **Relevanz**: Zunehmende Verbreitung vernetzter Geräte erfordert spezielle Sicherheitsmaßnahmen
- **Anwendung**: Absicherung von IoT-Geräten gegen Manipulation und unbefugten Datenzugriff
- **Konkrete Maßnahmen**:
  - Regelmäßige Firmware-Updates und Schwachstellenanalysen
  - Deaktivierung von nicht benötigten Netzwerkprotokollen (z. B. UPnP)
  - Nutzung von separaten Netzwerksegmenten für IoT-Geräte
  - Einschränkung von Cloud-Zugriffen und externen Steuerungsmöglichkeiten
  - Logging und Überwachung von Netzwerkaktivitäten
  - Nutzung von sicheren Authentifizierungsmechanismen für die Geräteverwaltung

8.4.4 SYS.4.5 Wechseldatenträger

- **Relevanz**: Häufig verwendete Datenträger für Transport, Speicherung und mobilen Zugriff
- **Anwendung**: Absicherung und sichere Nutzung von Wechseldatenträgern
- **Konkrete Maßnahmen**:
  - Sensibilisierung der Benutzer für den sicheren Umgang mit Wechseldatenträgern
  - Festlegung klarer Richtlinien zur Nutzung und Mitnahme von Wechseldatenträgern
  - Pflicht zur Meldung von Verlust oder Verdacht auf Manipulation
  - Einsatz sicherer Verschlüsselungsmethoden für schutzbedürftige Daten
  - Schutz vor Schadsoftware durch regelmäßige Überprüfung der Daten
  - Nutzung zertifizierter Wechseldatenträger zur Sicherstellung der Datenerhaltung

- Einschränkung der Nutzung auf definierte IT-Systeme mit autorisierten Schnittstellen
- Sichere Lagerung und Zugriffskontrolle für Wechseldatenträger
- Sicheres Löschen von Daten auf Wechseldatenträgern vor Weitergabe oder Entsorgung
- Nutzung dedizierter IT-Systeme zur Schadsoftwareprüfung vor Datenübertragung
- Vorgaben für die sichere Versandverpackung und Kennzeichnung von Wechseldatenträgern

9 IND - Industrielle Systeme

Der Baustein **IND - Industrielle IT** beschreibt Schutzmaßnahmen für industrielle Steuerungs- und Automatisierungssysteme, Produktionsnetzwerke und kritische Infrastruktur. Er behandelt die Absicherung von **Prozessleittechnik (ICS)**, **Speicherprogrammierbaren Steuerungen (SPS)**, **Safety Instrumented Systems (SIS)** und **industriellen Netzwerken**. Wichtige Maßnahmen sind Netzsegmentierung, Zugriffskontrollen, sichere Protokolle sowie regelmäßige Sicherheitsüberprüfungen. Ziel ist es, Manipulationen, unbefugte Zugriffe und Betriebsstörungen zu verhindern, um die Sicherheit und Verfügbarkeit industrieller Prozesse zu gewährleisten.

9.1 IND.1 Prozessleit- und Automatisierungstechnik

- **Relevanz**: Steuerung und Überwachung technischer Prozesse in der Industrie
- **Anwendung**: Schutzmaßnahmen für industrielle Steuerungssysteme (ICS)
- **Konkrete Maßnahmen**:
  - Härtung der OT-Systeme gegen Cyberangriffe und physische Bedrohungen
  - Segmentierung von OT- und IT-Netzwerken zur Vermeidung von Angriffsvektoren
  - Regelmäßige Sicherheitsüberprüfungen und Schwachstellenanalysen
  - Zugriffskontrollen und Protokollierung sicherheitskritischer Ereignisse
  - Sensibilisierung des Personals für IT-Sicherheitsrisiken in der OT

Notes

ICS (Industrial Control Systems): Industrielle Steuerungssysteme, die zur Automatisierung und Überwachung technischer Prozesse genutzt werden. **OT (Operational Technology)**: Hardware- und Softwarekomponenten zur Steuerung physischer Prozesse, insbesondere in der Industrie. **Segmentierung**: Aufteilung eines Netzwerks in verschiedene Sicherheitszonen, um Angriffe einzudämmen.

9.2 IND.2 ICS-Komponenten

9.2.1 IND.2.1 Allgemeine ICS-Komponente

- **Relevanz**: Grundbaustein industrieller Steuerungssysteme
- **Anwendung**: Schutzmaßnahmen für einzelne ICS-Komponenten
- **Konkrete Maßnahmen**:
  - Einsatz sicherer Authentifizierungsmechanismen für den Zugriff auf ICS-Geräte
  - Deaktivierung nicht benötigter Dienste und Schnittstellen
  - Absicherung der Firmware und regelmäßige Sicherheitsupdates
  - Schutz der ICS-Kommunikation durch sichere Protokolle
  - Implementierung von Monitoring- und Detektionssystemen

Notes

Firmware: Eingebettete Software, die die Grundfunktionen eines Geräts steuert. Sie kann Sicherheitslücken enthalten, wenn sie nicht regelmäßig aktualisiert wird. **Monitoring**: Überwachung von IT-Systemen, um Anomalien oder Angriffe frühzeitig zu erkennen. **Detektionssysteme**: Systeme zur Erkennung von Angriffen, z. B. Intrusion Detection Systems (IDS).

9.2.2 IND.2.2 Speicherprogrammierbare Steuerung (SPS)

- **Relevanz**: Zentrale Steuerungseinheit für industrielle Prozesse
- **Anwendung**: Sicherheit in SPS-basierten Steuerungssystemen
- **Konkrete Maßnahmen**:
  - Absicherung von Fernwartung und Konfigurationsschnittstellen
  - Einsatz sicherer Kommunikationsprotokolle für Steuerungsbefehle
  - Regelmäßige Sicherheitsupdates und Patches für SPS-Systeme
  - Zugriffskontrolle und Protokollierung von Änderungen
  - Dokumentation der Konfiguration und Netzwerkschnittstellen

Notes

SPS (Speicherprogrammierbare Steuerung): Industriecomputer, der Maschinen und Prozesse steuert. Wird in Produktions- und Fertigungsprozessen verwendet. **Fernwartung**: Remote-Zugriff auf ein System zur Wartung oder Fehlerbehebung, oft über das Internet oder geschützte VPN-Verbindungen.

9.2.3 IND.2.3 Sensoren und Aktoren

- **Relevanz**: Datenerfassung und Steuerung industrieller Prozesse
- **Anwendung**: Schutz vor Manipulation und unbefugtem Zugriff auf Sensoren und Aktoren
- **Konkrete Maßnahmen**:
  - Sicherung von Kommunikationsschnittstellen gegen unbefugten Zugriff
  - Nutzung sicherer Protokolle für die Übertragung von Messdaten
  - Kalibrierung und regelmäßige Überprüfung der Sensoren
  - Schutz vor Umwelteinflüssen und physischen Angriffen
  - Dokumentation von Konfigurationsänderungen und Wartungsmaßnahmen

Notes

Sensoren: Geräte, die physikalische Größen (z. B. Temperatur, Druck) messen und in digitale Signale umwandeln. **Aktoren**: Geräte, die Steuerbefehle in physische Aktionen umsetzen (z. B. Ventile öffnen oder Roboterarme bewegen). **Kalibrierung**: Anpassung und Justierung eines Sensors, um präzise Messwerte sicherzustellen.

9.2.4 IND.2.4 Maschinen

- **Relevanz**: Automatisierung industrieller Prozesse durch computergesteuerte Maschinen
- **Anwendung**: Absicherung elektronisch gesteuerter Maschinen
- **Konkrete Maßnahmen**:
  - Kontrolle und Absicherung von externen Wartungsschnittstellen
  - Schutz gegen Manipulationen durch lokale oder Netzwerkschnittstellen
  - Implementierung von Sicherheitsrichtlinien für Maschinensteuerungen
  - Dokumentation von Software- und Hardware-Änderungen
  - Nutzung sicherer Verfahren für Software-Updates und Konfigurationsanpassungen

Notes

Maschinensteuerung: Software- oder hardwarebasierte Systeme zur automatisierten Steuerung von Maschinen, häufig über SPS oder industrielle PCs (IPC). **Manipulation**: Unbefugte Änderungen an Maschinensteuerungen, die zu fehlerhaften Prozessen oder Produktionsausfällen führen können.

9.2.5 IND.2.7 Safety Instrumented Systems (SIS)

- **Relevanz**: Schutzmechanismen zur Gewährleistung der funktionalen Sicherheit in industriellen Steuerungssystemen
- **Anwendung**: Implementierung und Absicherung von SIS zur Verhinderung gefährlicher Betriebszustände
- **Konkrete Maßnahmen**:
  - Dokumentation und Erfassung aller SIS-Hard- und Softwarekomponenten
  - Sicherstellen der Integrität und Authentizität von SIS-Programmen und Konfigurationsdaten
  - Zweckgebundene Nutzung von SIS-Komponenten ohne Zweckentfremdung
  - Sicherer Umgang mit Fernwartung und Konfigurationsschnittstellen
  - Trennung von SIS von IT- und OT-Netzwerken zur Vermeidung von Sicherheitsrisiken
  - Umsetzung des **Functional Safety Management (FSM)** zur Sicherstellung der Sicherheitsanforderungen
  - Implementierung von Maßnahmen zur Alarmierung und Überwachung von Manipulationen

Notes

Safety Instrumented Systems (SIS): Spezielle industrielle Steuerungssysteme, die eingesetzt werden, um Risiken für Menschen, Umwelt und Anlagen zu minimieren, indem sie bei Gefahrensituationen Schutzmaßnahmen auslösen.
Sicherheits-Integritätslevel (SIL): Standardisierte Klassifizierung der Sicherheit von SIS gemäß **IEC 61508**, mit vier Stufen (SIL1 bis SIL4), wobei SIL4 die höchste Sicherheitsanforderung darstellt.
Functional Safety Management (FSM): Managementsystem für funktionale Sicherheit, das sicherstellt, dass Sicherheitsmaßnahmen in industriellen Steuerungssystemen über den gesamten Lebenszyklus hinweg eingehalten werden.
Manipulation des Logiksystems: Unautorisierte Änderungen an Steuerungsprogrammen, die dazu führen können, dass Schutzmaßnahmen nicht oder fehlerhaft ausgelöst werden.

9.3 IND.3 Produktionsnetze

9.3.1 IND.3.1 Produktions- und Steuerungsnetzwerke

- **Relevanz**: Grundlage für den sicheren Betrieb industrieller Prozesse durch stabile und geschützte Netzwerke
- **Anwendung**: Absicherung und Überwachung von Netzwerken zur Verhinderung unbefugter Zugriffe und Manipulationen
- **Konkrete Maßnahmen**:
  - Netzsegmentierung zur Trennung von OT- und IT-Netzwerken
  - Implementierung von Firewalls und Intrusion Detection Systemen für OT-Netze
  - Protokollierung und Überwachung sicherheitskritischer Netzwerkaktivitäten
  - Beschränkung des Remote-Zugriffs auf Steuerungssysteme
  - Nutzung sicherer Protokolle für die Kommunikation zwischen Produktionssystemen
  - Absicherung gegen physische Angriffe auf Netzwerkkomponenten
  - Regelmäßige Schwachstellenanalysen und Penetrationstests

Notes

Produktionsnetzwerke: Spezialisierte Netzwerke in industriellen Umgebungen, die für die Kommunikation zwischen Maschinen, Steuerungssystemen und Produktionsanlagen genutzt werden.
Netzsegmentierung: Aufteilung eines Netzwerks in isolierte Zonen zur Minimierung der Angriffsfläche und Verhinderung unautorisierter Zugriffe.
Intrusion Detection System (IDS): Sicherheitslösung zur Erkennung von Angriffen oder Anomalien in Netzwerken, die auf unbefugte Aktivitäten hinweisen.
Penetrationstests: Simulierte Angriffe auf ein Netzwerk oder System, um Schwachstellen zu identifizieren und Sicherheitsmaßnahmen zu verbessern.

9.3.2 IND.3.2 Fernwartung im industriellen Umfeld

- **Relevanz**: Notwendige Wartungszugänge für Industrieanlagen bergen Sicherheitsrisiken, wenn sie nicht geschützt sind
- **Anwendung**: Sicherstellung von Zugriffsschutz und Protokollierung für Fernwartungsverbindungen
- **Konkrete Maßnahmen**:
  - Zentrale Verwaltung aller Fernwartungszugänge mit Zugriffsbeschränkungen
  - Nutzung von Multi-Faktor-Authentifizierung für Fernzugriffe
  - Strikte Protokollierung und Monitoring von Fernwartungssitzungen
  - Implementierung dedizierter Sprungserver zur Kontrolle von Fernwartungsverbindungen
  - Festlegung von Wartungsfenstern und Einschränkungen für externe Dienstleister
  - Einsatz von VPN und verschlüsselten Kommunikationskanälen für Fernzugriffe

Notes

- **Fernwartung**: Zugriff auf Maschinen und Steuerungssysteme aus der Ferne zur Wartung oder Fehlerbehebung, oft über gesicherte Netzverbindungen.
- **Multi-Faktor-Authentifizierung (MFA)**: Sicherheitsmechanismus, bei dem mehrere Authentifizierungsfaktoren (z. B. Passwort und Token) erforderlich sind, um Zugriff zu gewähren.
- **Sprungserver (Jump Server)**: Speziell gesicherter Server, über den externe Wartungstechniker auf industrielle Steuerungssysteme zugreifen, um direkten Zugriff auf kritische Systeme zu vermeiden.

10 NET - Netzwerke und Kommunikation

Die **NET-Bausteine** behandeln die sichere Planung, Verwaltung und Nutzung von **Netzwerken**, **Funknetzen**, **Netzkomponenten** und **Telekommunikation**. Wichtige Maßnahmen umfassen Netzsegmentierung, Firewalls, Verschlüsselung und Authentifizierung für eine geschützte Kommunikation. Spezielle Sicherheitsanforderungen bestehen für **drahtlose Netze** (WLAN) und **VoIP-Telefonie**. Durch Überwachung, Protokollierung und regelmäßige Sicherheitsprüfungen wird die Integrität und Verfügbarkeit der Netzwerke gewährleistet.

10.1 NET.1 Netzarchitektur und -design

10.1.1 NET.1.1 Netzarchitektur und -design

- **Relevanz**: Grundlegende Struktur für sichere und effiziente Netzwerke
- **Anwendung**: Planung und Umsetzung sicherer Netzstrukturen für Unternehmen und Institutionen
- **Konkrete Maßnahmen**:
  - Trennung von Netzsegmenten für verschiedene Sicherheitsanforderungen
  - Absicherung von Übergängen zwischen internen und externen Netzwerken durch Firewalls
  - Einführung eines Sicherheitskonzepts für WAN, LAN und Funknetze
  - Implementierung sicherer Authentifizierungs- und Verschlüsselungsmechanismen
  - Dokumentation und regelmäßige Überprüfung der Netzstruktur
  - Einsatz von Monitoring und Intrusion Detection Systemen zur Überwachung des Netzwerkverkehrs
  - Regelmäßige Sicherheitsupdates und Schwachstellenanalysen zur Netzabsicherung
  - Notfallplanung zur Wiederherstellung der Netzwerkverfügbarkeit

10.1.2 NET.1.2 Netzmanagement

- **Relevanz**: Notwendige Prozesse zur Überwachung und Steuerung der Netzwerkinfrastruktur
- **Anwendung**: Sicherstellung der Stabilität und Sicherheit von Netzwerken
- **Konkrete Maßnahmen**:
  - Einführung eines zentralisierten Netzwerkmanagements mit definierten Rollen und Verantwortlichkeiten
  - Protokollierung von Netzereignissen zur Fehleranalyse und Sicherheitsüberprüfung
  - Absicherung von Netzmanagement-Schnittstellen gegen unbefugten Zugriff
  - Regelmäßige Backups von Netzwerkkonfigurationen zur schnellen Wiederherstellung im Notfall

  - Nutzung sicherer Netzwerkprotokolle für Managementzugriffe (z. B. SSH, SNMPv3)
  - Implementierung eines Notfallkonzepts für den Betrieb des Netzwerks
  - Schulungen für IT-Personal zur korrekten Handhabung und Verwaltung der Netzwerkinfrastruktur
  - Integration des Netzmanagements in ein Security-Information-and-Event-Management (SIEM)

10.2 NET.2 Funknetze

10.2.1 NET.2.1 WLAN-Betrieb

- **Relevanz**: Drahtlose Netze bieten Flexibilität, erfordern aber besondere Sicherheitsmaßnahmen
- **Anwendung**: Sicherer Betrieb von WLAN-Infrastrukturen in Unternehmen und Institutionen
- **Konkrete Maßnahmen**:
  - Nutzung moderner Verschlüsselungsstandards wie WPA2/WPA3 zur Sicherung des WLANs
  - Regelmäßige Überprüfung und Aktualisierung der WLAN-Sicherheitsrichtlinien
  - Segmentierung von WLAN-Netzen zur Trennung von Gäste- und Unternehmensnetzwerken
  - Implementierung von Authentifizierungsmechanismen wie 802.1X (RADIUS-Server)
  - Schutz vor Rogue Access Points und unautorisierten Verbindungen durch Monitoring
  - Physische Absicherung von Access Points gegen Diebstahl und Manipulation
  - Vermeidung unsicherer WLAN-Konfigurationen (z. B. deaktivierte Verschlüsselung)
  - Nutzung sicherer Managementschnittstellen für WLAN-Controller und Access Points

10.2.2 NET.2.2 WLAN-Nutzung

- **Relevanz**: WLAN-Clients sind potenzielle Sicherheitsrisiken, wenn sie unsicher konfiguriert oder genutzt werden
- **Anwendung**: Sichere Nutzung von WLAN durch Mitarbeitende und externe Nutzer
- **Konkrete Maßnahmen**:
  - Sensibilisierung der Benutzer für sicheres WLAN-Verhalten (z. B. Vermeidung offener Netze)
  - Nutzung von VPNs bei Zugriff auf Unternehmensressourcen über öffentliche WLANs
  - Deaktivierung der automatischen Verbindung zu ungesicherten Netzwerken
  - Regelmäßige Überprüfung und Aktualisierung von WLAN-Zugangsberechtigungen
  - Einschränkung der Nutzung mobiler Geräte in sensiblen Bereichen
  - Logging und Überwachung der WLAN-Nutzung zur Identifikation verdächtiger Aktivitäten
  - Implementierung von Netzsegmentierung zur Begrenzung der Reichweite sensibler Daten
  - Nutzung sicherer Authentifizierungsverfahren zur Identitätsprüfung von Nutzern

10.3 NET.3 Netzkomponenten

10.3.1 NET.3.1 Router und Switches

- **Relevanz**: Router und Switches bilden das Rückgrat moderner Datennetze und müssen besonders abgesichert werden.
- **Anwendung**: Sicherer Betrieb und Verwaltung von Routern und Switches in IT-Infrastrukturen

- **Konkrete Maßnahmen**:
  - Trennung von Netzsegmenten durch VLANs und Routing-Regeln
  - Sichere Grundkonfiguration durch Deaktivierung nicht benötigter Dienste und Ports
  - Regelmäßige Sicherheitsupdates und Firmware-Patches
  - Einsatz von Zugriffskontrolllisten (ACLs) zur Filterung des Datenverkehrs
  - Schutz der Administrationsschnittstellen durch IP-Whitelisting und Verschlüsselung (SSH, SNMPv3)
  - Verwendung sicherer Authentifizierungsverfahren für Administratoren (z. B. RADIUS, TACACS+)
  - Implementierung von Schutzmechanismen gegen DDoS-Angriffe und Spoofing
  - Protokollierung und Überwachung von Netzwerkaktivitäten zur Erkennung von Anomalien

10.3.2 NET.3.2 Firewall

- **Relevanz**: Firewalls sind essenzielle Sicherheitskomponenten zur Kontrolle und Filterung des Netzverkehrs.
- **Anwendung**: Schutz von Netzsegmenten durch gezielte Zugriffsbeschränkungen und Sicherheitsregeln
- **Konkrete Maßnahmen**:
  - Definition und Durchsetzung einer Firewall-Sicherheitsrichtlinie
  - Einsatz von mehrstufigen Firewall-Architekturen (z. B. „Paketfilter – Application-Level-Gateway – Paketfilter“)
  - Implementierung von Stateful-Inspection-Mechanismen zur Analyse des Datenverkehrs
  - Deaktivierung nicht benötigter Netzwerkprotokolle und Dienste
  - Protokollierung und Monitoring von Firewall-Logs zur Identifikation von Angriffen
  - Sicherstellung der regelbasierten Filterung und Minimierung der Angriffsfläche durch restriktive Regeln
  - Integration der Firewall in das zentrale Sicherheits- und Netzwerkmanagement (SIEM)
  - Regelmäßige Sicherheitsüberprüfungen und Penetrationstests zur Identifikation von Schwachstellen

10.3.3 NET.3.3 Virtual Private Networks (VPN)

- Relevanz: VPNs ermöglichen eine sichere und verschlüsselte Kommunikation über unsichere Netzwerke.
- Anwendung: Absicherung von Remote-Zugriffen und Vernetzung unterschiedlicher Standorte.
- Konkrete Maßnahmen:
  - Erstellung einer Sicherheitsrichtlinie zur VPN-Nutzung.
  - Geeignete Auswahl von VPN-Produkten gemäß den Anforderungen der Institution.
  - Sicherer Betrieb eines VPN unter Berücksichtigung von Qualitätsmanagement, Überwachung und Wartung.
  - Sichere Anbindung externer Netze, um zu gewährleisten, dass VPN-Verbindungen nur zwischen vorgesehenen IT-Systemen aufgebaut werden.
  - Zentralisierte Konten- und Zugriffsverwaltung für Fernzugriff-VPNs.
  - Integration von VPN-Komponenten in die bestehende Firewall-Architektur

10.4 NET.4 Telekommunikation

10.4.1 NET.4.1 TK-Anlagen

- **Relevanz**: Telekommunikationsanlagen verbinden interne und externe Telefonsysteme und sind durch die Vernetzung mit IT-Systemen sicherheitskritisch.
- **Anwendung**: Absicherung von TK-Anlagen und Schutz der übertragenen Informationen
- **Konkrete Maßnahmen**:
  - Sicherstellen der Verschlüsselung der übertragenen Daten und Gespräche
  - Einschränkung von Leistungsmerkmalen, die unautorisiertes Abhören ermöglichen könnten
  - Schutz vor Manipulation durch regelmäßige Überprüfung der Systemkonfiguration
  - Einsatz sicherer Authentifizierungsmechanismen für administrative Zugriffe
  - Sicherstellung der Protokollierung von Konfigurationsänderungen und sicherheitskritischen Ereignissen
  - Implementierung von Sicherheitsrichtlinien für TK-Nutzer und Administratoren
  - Regelmäßige Sicherheitsupdates und Patching der TK-Software
  - Einrichtung redundanter Kommunikationswege für Notfälle

10.4.2 NET.4.2 VoIP

- **Relevanz**: Voice over IP (VoIP) ersetzt zunehmend traditionelle Telefonanlagen und benötigt spezielle Sicherheitsmaßnahmen.
- **Anwendung**: Absicherung von VoIP-Kommunikation und Infrastruktur
- **Konkrete Maßnahmen**:
  - Nutzung verschlüsselter Kommunikationsprotokolle (z. B. SRTP für Sprachdaten)
  - Implementierung sicherer Authentifizierungsverfahren für VoIP-Endgeräte
  - Einschränkung und Filterung von VoIP-Traffic durch Firewalls und Session Border Controller (SBC)
  - Regelmäßige Sicherheitsüberprüfungen und Testen der VoIP-Konfigurationen
  - Schutz gegen Spoofing- und Phishing-Angriffe durch sichere Identitätsprüfung
  - Trennung von VoIP- und Datennetzwerken zur Reduzierung von Sicherheitsrisiken
  - Regelmäßige Überprüfung der Firmware und Software der VoIP-Systeme

10.4.3 NET.4.3 Faxgeräte und Faxserver

- **Relevanz**: Faxgeräte und Faxserver werden weiterhin für die Dokumentenübertragung genutzt, erfordern aber zusätzliche Sicherheitsvorkehrungen.
- **Anwendung**: Sicherer Betrieb und Nutzung von Faxsystemen
- **Konkrete Maßnahmen**:
  - Sicherstellen der Vertraulichkeit von Faxübertragungen durch sichere Leitungen und Verschlüsselung
  - Absicherung von Faxservern durch Zugriffskontrollen und Logging
  - Einschränkung von Faxnummern auf autorisierte Empfänger
  - Sensibilisierung der Mitarbeiter für Risiken von Faxkommunikation

- Regelmäßige Wartung und Überprüfung der Faxserver-Software
- Implementierung sicherer Löschmechanismen für alte Faxdokumente
- Schutz vor Manipulation von Faxinhalten durch digitale Signaturen oder Bestätigungsverfahren

11 INF - Infrastruktur

Die **INF-Bausteine** konzentrieren sich auf den Schutz von IT-relevanten physischen Strukturen wie **Rechenzentren**, **Verkabelung**, **Arbeitsplätzen** und **Gebäudeautomation**. Sicherheitsmaßnahmen umfassen Zutrittskontrollen, Brandschutz, Energieversorgung und sichere Entsorgung sensibler Daten. Spezielle Regelungen gelten für mobile und häusliche Arbeitsplätze sowie für IT-Systeme in Fahrzeugen. Eine sichere und effiziente Verwaltung der **technischen Gebäudesysteme (TGM und GA)** trägt zur Gesamtresilienz der IT-Infrastruktur bei.

11.1 INF.1 Allgemeines Gebäude

- **Relevanz**: Basis für sichere IT-Infrastruktur
- **Anwendung**: Schutz von Gebäuden und Einrichtungen
- **Konkrete Maßnahmen**:
  - Sichere Türen und Fenster
  - Zutrittskontrollen
  - Einhaltung von Brandschutzvorschriften
  - Gefahrenmeldeanlagen

11.2 INF.2 Rechenzentrum sowie Serverraum

- **Relevanz**: Schutz geschäftskritischer IT-Systeme
- **Anwendung**: Sicherheit und Verfügbarkeit von Servern
- **Konkrete Maßnahmen**:
  - Zutrittskontrolle und Überwachung
  - Einsatz einer Brandmeldeanlage
  - Schutz vor Stromausfällen durch USV und Netzersatzanlagen
  - Einhaltung von Sicherheitszonen für IT-Infrastruktur

11.3 INF.5 Raum für technische Infrastruktur

- **Relevanz**: Schutz der kritischen Infrastruktur
- **Anwendung**: Sicherheitsmaßnahmen für Technikräume
- **Konkrete Maßnahmen**:
  - Schutz vor Brand, Rauch und Wasserschäden
  - Redundante Stromversorgung
  - Erweiterter Schutz vor Einbruch und Sabotage

11.4 INF.6 Archivierung von Datenträgern

- **Relevanz**: Schutz und Verfügbarkeit archivierter Daten
- **Anwendung**: Sicherstellung der Integrität von Archivsystemen
- **Konkrete Maßnahmen**:
  - Zugangskontrollen für Archive
  - Temperatur- und Feuchtigkeitskontrolle
  - Schutz vor Einbruch und Sabotage

11.5 INF.7 Büroarbeitsplatz

- **Relevanz**: Schutz sensibler Informationen am Arbeitsplatz
- **Anwendung**: Sichere Handhabung von Informationen
- **Konkrete Maßnahmen**:
  - Zutrittskontrolle zu Büros
  - Sichere Aufbewahrung von Dokumenten
  - Einsatz von Diebstahlsicherungen

11.6 INF.8 Häuslicher Arbeitsplatz

- **Relevanz**: Telearbeitende benötigen eine sichere und ergonomische Arbeitsumgebung.
- **Anwendung**: Schutz von sensiblen Informationen und IT-Systemen im Homeoffice.
- **Konkrete Maßnahmen**:
  - Trennung von privatem und beruflichem Arbeitsbereich
  - Schutz vor unbefugtem Zutritt (z. B. abschließbare Räume)
  - Sichere Entsorgung vertraulicher Informationen
  - Regelungen für den Transport von Arbeitsmaterial
  - Ergonomische Arbeitsplatzgestaltung zur Vermeidung von Beeinträchtigungen

11.7 INF.9 Mobiler Arbeitsplatz

- **Relevanz**: Mobile Arbeitsplätze unterliegen zusätzlichen Risiken durch wechselnde Umgebungen.
- **Anwendung**: Absicherung mobiler Arbeitsgeräte und Daten unterwegs.
- **Konkrete Maßnahmen**:
  - Nutzung verschlüsselter Datenträger und gesicherter VPN-Verbindungen
  - Vermeidung ungesicherter öffentlicher WLANs
  - Schutz vor Diebstahl und unbefugtem Zugriff
  - Regelung für Transport und Entsorgung sensibler Dokumente
  - Einführung einer Sicherheitsrichtlinie für mobiles Arbeiten

11.8 INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume

- **Relevanz**: Räume mit wechselnder Nutzung erfordern spezifische Sicherheitsvorkehrungen.
- **Anwendung**: Sicherstellung von Datenschutz und Gerätesicherheit in geteilten Räumen.
- **Konkrete Maßnahmen**:
  - Zugangskontrollen für Besprechungsräume mit sensiblen Daten
  - Schutz vor Diebstahl und Manipulation von Präsentationssystemen
  - Regelungen für die Nutzung externer IT-Systeme in Schulungsräumen
  - Dokumentation der Raumbelegung zur Nachverfolgbarkeit
  - Sicherstellung der Kompatibilität von Präsentationstechnologien

11.9 INF.11 Allgemeines Fahrzeug

- **Relevanz**: Fahrzeuge mit IT-Systemen und Daten speichern oft vertrauliche Informationen.
- **Anwendung**: Absicherung der IT-Infrastruktur in dienstlich genutzten Fahrzeugen.
- **Konkrete Maßnahmen**:
  - Verschlüsselung von Daten in Fahrzeug-IT-Systemen
  - Regelungen für die Nutzung von Kommunikationsschnittstellen (WLAN, Bluetooth)
  - Schutz vor unbefugtem Zugriff und Diebstahl
  - Erstellung von Sicherheitsrichtlinien für mobile IT-Arbeitsplätze in Fahrzeugen
  - Vorgaben für sichere Wartung und Entsorgung von IT-Systemen in Fahrzeugen

11.10 INF.12 Verkabelung

- **Relevanz**: Physische Netzwerkinfrastruktur bildet die Grundlage sicherer Kommunikation.
- **Anwendung**: Schutz und ordnungsgemäße Verlegung von Kabeln in IT-Umgebungen.
- **Konkrete Maßnahmen**:
  - Strukturierte Verkabelung zur Reduktion von Störquellen
  - Brandschutzmaßnahmen für Netzwerkkabelschächte
  - Absicherung physischer Netzwerkzugänge gegen Manipulation
  - Dokumentation und regelmäßige Überprüfung der Verkabelung

11.11 INF.13 Gebäudetechnik

- **Relevanz**: Technische Infrastruktur muss auf IT-Sicherheitsanforderungen abgestimmt sein.
- **Anwendung**: Schutz technischer Systeme in Gebäuden.
- **Konkrete Maßnahmen**:
  - Schutz vor Sabotage und Manipulation von Klimaanlagen und Stromversorgung
  - Redundante Energieversorgung für kritische IT-Systeme
  - Überwachung der Gebäudetechnik durch zentrale IT-Managementsysteme
  - Integration von Sicherheitssystemen in IT-Notfallpläne

11.12 INF.14 Rechenzentrum-Infrastruktur

- **Relevanz**: Schutz von Servern und Datenzentren ist essenziell für den sicheren IT-Betrieb.
- **Anwendung**: Sicherstellung der physischen Sicherheit von Rechenzentren.
- **Konkrete Maßnahmen**:
  - Zutrittskontrollen und Sicherheitsüberwachung für Serverräume
  - Klimakontrolle und Brandschutzmaßnahmen für Rechenzentren
  - Regelmäßige Prüfung und Aktualisierung der Infrastruktur
  - Einsatz redundanter Komponenten zur Sicherstellung der Ausfallsicherheit

12 DER - Detektion und Reaktion

12.1 DER.1 Detektion von sicherheitsrelevanten Ereignissen

- **Relevanz**: Die frühzeitige Erkennung von sicherheitsrelevanten Ereignissen ist essenziell für den Schutz von IT-Systemen und Daten.
- **Anwendung**: Planung und Umsetzung technischer, personeller und organisatorischer Maßnahmen zur Identifikation von Sicherheitsvorfällen.
- **Konkrete Maßnahmen**:
  - Einführung eines Detektionskonzepts mit definierten Zuständigkeiten
  - Einsatz von Intrusion Detection/Prevention Systemen (IDS/IPS)
  - Schulung der Mitarbeitenden zur Erkennung und Meldung von Vorfällen
  - Nutzung von zentralen Protokollierungs- und Monitoring-Lösungen
  - Regelmäßige Audits und Tests zur Sicherstellung der Funktionsfähigkeit der Detektionssysteme

12.2 DER.2 Security Incident Management

12.2.1 DER.2.1 Behandlung von Sicherheitsvorfällen

- **Relevanz**: Sicherheitsvorfälle müssen systematisch behandelt werden, um Schäden zu begrenzen.
- **Anwendung**: Entwicklung von Prozessen zur strukturierten Bearbeitung von Sicherheitsvorfällen.
- **Konkrete Maßnahmen**:
  - Definition und Dokumentation von Sicherheitsvorfällen
  - Erstellung einer Richtlinie zur Vorfallsbehandlung
  - Etablierung klarer Meldewege und Verantwortlichkeiten
  - Sicherstellung der Beweissicherung zur späteren Analyse

12.2.2 DER.2.2 Vorsorge für die IT-Forensik

- **Relevanz**: IT-Forensik ermöglicht die Untersuchung und Aufklärung von Sicherheitsvorfällen.
- **Anwendung**: Etablierung von Prozessen zur rechtskonformen Spurensicherung.
- **Konkrete Maßnahmen**:
  - Prüfung der rechtlichen Rahmenbedingungen für forensische Analysen

- Auswahl und Implementierung geeigneter Forensik-Tools
- Schulung von Personal für Beweissicherung und Datenanalyse
- Dokumentation und sichere Lagerung von Beweismitteln

12.2.3 DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle

- **Relevanz**: Advanced Persistent Threats (APT) und gezielte Angriffe erfordern eine umfangreiche Bereinigung.
- **Anwendung**: Maßnahmen zur vollständigen Bereinigung kompromittierter IT-Systeme.
- **Konkrete Maßnahmen**:
  - Einrichtung eines Leitungsgremiums zur Koordination der Bereinigung
  - Entscheidung über eine vollständige Neuinstallation oder gezielte Säuberung betroffener Systeme
  - Isolation der betroffenen Netzsegmente zur Verhinderung weiterer Angriffe
  - Sicherstellung der langfristigen Überwachung zur Identifikation möglicher Hintertüren

12.3 DER.3 Sicherheitsprüfungen

12.3.1 DER.3.1 Audits und Revisionen

- **Relevanz**: Audits und Revisionen sind essenziell, um die Informationssicherheit zu bewerten, Lücken aufzudecken und Maßnahmen zur Verbesserung abzuleiten.
- **Anwendung**: Regelmäßige Audits und Revisionen zur Überprüfung der Sicherheitsmaßnahmen in einer Institution.
- **Konkrete Maßnahmen**:
  - **Definition von Verantwortlichkeiten**: Die Institutionsleitung muss eine verantwortliche Person für Audits und Revisionen benennen
  - **Durchführung von Audits**: Das Auditteam muss überprüfen, ob Sicherheitsanforderungen gemäß Normen, Richtlinien und Standards eingehalten werden
  - **Prüfung der Dokumentation**: Alle relevanten Sicherheitsdokumente sollten aktuell, vollständig und nachvollziehbar sein
  - **Stichprobenprüfung**: Auswahl von Prüfobjekten anhand eines risikoorientierten Ansatzes
  - **Erstellung eines Auditberichts**: Ergebnisse der Audits müssen nachvollziehbar dokumentiert und zeitnah kommuniziert werden
  - **Nachbereitung von Audits**: Identifizierte Sicherheitsmängel müssen behoben und in das Sicherheitsmanagement zurückgeführt werden

12.3.2 DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision

- **Relevanz**: Standardisierte IS-Revisionen dienen der kontinuierlichen Verbesserung der Informationssicherheit.
- **Anwendung**: Umsetzung von IS-Revisionen unter Einhaltung definierter Leitfäden und Standards.
- **Konkrete Maßnahmen**:
  - **Benennung von Verantwortlichen**: Die Institutionsleitung muss eine Person für IS-Revisionen festlegen

- **Erstellung eines IS-Revisionshandbuchs**: Enthält Ziele, gesetzliche Vorgaben, Rahmenbedingungen und Archivierungsvorgaben
- **Definition der Prüfungsgrundlage**: Die BSI-Standards 200-1 bis 200-3 und das IT-Grundschutz-Kompendium müssen als Prüfungsgrundlagen verwendet werden
- **Sichtung und Prüfung der Dokumentation**: Relevante Dokumente müssen auf Aktualität und Vollständigkeit überprüft werden
- **Durchführung von Interviews**: Ergänzende Gespräche mit Verantwortlichen zur Klärung von Prüfungsfragen
- **Erstellung eines IS-Revisionsberichts**: Enthält Ergebnisse, Maßnahmenempfehlungen und Klassifizierung von Risiken
- **Nachbereitung der IS-Revision**: Dokumentierte Maßnahmenumsetzung mit Nachverfolgung der Korrekturmaßnahmen

12.4 DER.4 Notfallmanagement

- **Relevanz**: Ein effektives Notfallmanagement sichert den Fortbestand von Geschäftsprozessen und die Informationssicherheit im Krisenfall.
- **Anwendung**: Planung, Umsetzung und Überprüfung von Maßnahmen zur Vorbereitung, Reaktion und Wiederherstellung im Notfall.
- **Konkrete Maßnahmen**:
  - Erstellung eines Notfallhandbuchs mit definierten Rollen, Eskalationsstufen und Kommunikationsplänen
  - Integration des Notfallmanagements in bestehende Organisationsstrukturen und IT-Sicherheitsprozesse
  - Regelmäßige Notfallübungen zur Sicherstellung der Praxistauglichkeit der geplanten Maßnahmen
  - Dokumentation und regelmäßige Überprüfung des Notfallmanagements durch die Institutionsleitung

13 Praktische Übung: Anwendung der IT-Grundschutzbausteine auf den eigenen Arbeitsplatz

13.1 Arbeitsauftrag:

1. **Analyse des Ist-Zustands**:
   - Erstellen Sie eine Inventarliste aller IT-Komponenten an Ihrem Arbeitsplatz (Hardware, Software, Netzwerkkomponenten)
   - Dokumentieren Sie die aktuell implementierten Sicherheitsmaßnahmen
2. **Identifikation relevanter Bausteine**:
   - Identifizieren Sie auf Basis der Inventarliste die für Ihren Arbeitsplatz relevanten IT-Grundschutzbausteine
   - Begründen Sie Ihre Auswahl für jeden ausgewählten Baustein
3. **Gap-Analyse**:
   - Vergleichen Sie die Anforderungen der identifizierten Bausteine mit den aktuell implementierten Maßnahmen

- Dokumentieren Sie Abweichungen und Lücken

4. **Maßnahmenplan**:
    - Entwickeln Sie einen priorisierten Maßnahmenplan zur Schließung der identifizierten Lücken
    - Berücksichtigen Sie dabei praktische Einschränkungen (Budget, Machbarkeit, Aufwand)
5. **Dokumentation und Präsentation**:
    - Erstellen Sie eine strukturierte Dokumentation Ihrer Analyse und des Maßnahmenplans
    - Bereiten Sie eine kurze Präsentation (5-10 Minuten) Ihrer Ergebnisse vor

13.2 Hinweise zur Bearbeitung:

- Konzentrieren Sie sich auf die für Ihren Arbeitsplatz relevantesten Bausteine
- Berücksichtigen Sie bei HomeOffice-Arbeitsplätzen besonders die Bausteine OPS.1.2.4 (Telearbeit) und INF.8 (Häuslicher Arbeitsplatz)
- Nutzen Sie die BSI-Website (www.bsi.bund.de) für detaillierte Informationen zu den einzelnen Bausteinen
- Die Übung kann sowohl individuell als auch in Kleingruppen bearbeitet werden

13.3 Abgabeformat:

- Dokumentation als PDF (max. 10 Seiten)
- Präsentationsfolien als PDF oder PowerPoint
- Abgabefrist: 2 Wochen