

IT-Grundschutzbausteine

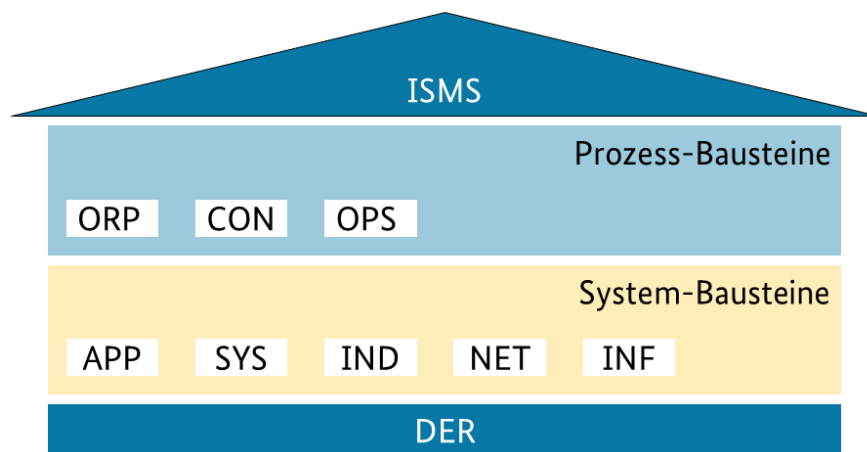
IT-Sicherheit

ITT-Net-IS

13. 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.



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.

- IT_{Grundschutzkompendium} S. 95 ff

2.1 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

3 ORP - Organisatorische und personelle Maßnahmen

Der **ORP-Baustein** legt organisatorische Maßnahmen zur Informationssicherheit fest.
IT_{Grundschutzkompendium} S. 105 ff

3.1 ORP.1 Organisation

- **Relevanz:** Strukturierung der Sicherheitsorganisation
- **Anwendung:** Klare Zuständigkeiten und Verantwortlichkeiten
- **Konkrete Maßnahmen:**
 - Benennung eines Sicherheitsbeauftragten
 - Festlegung von Meldewegen bei Sicherheitsvorfällen

3.2 ORP.2 Personal

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

3.3 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

3.4 ORP.4 Identitäts- und Berechtigungsmanagement

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

4 CON - Konzepte und Vorgehensweisen

Die **CON-Bausteine** definieren Konzepte und Vorgehensweisen zur Informationssicherheit in verschiedenen Bereichen. IT_{Grundschutzkompendium} S. 133 ff

4.1 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

4.2 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
- **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).

4.3 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

4.4 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 Lösungsverfahren (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

4.5 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

4.6 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
- **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.

4.7 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
- **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.

• 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.

4.8 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

5 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

IT Grundschutzkompendium S. 200 ff

5.1 OPS 1 Eigener Betrieb

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

5.1.1 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
- **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.

5.1.2 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

5.2 OPS 2 Betrieb von Dritten

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

5.2.1 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

5.2.2 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
- **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).

5.3 OPS 3 Betrieb für Dritte

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

5.3.1 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

6 APP - Anwendungen und Dienste

6.1 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

6.2 APP.1.2 Webbrowser

- **Relevanz:** Hauptzugriffspunkt auf Internet-Ressourcen
- **Anwendung:** Absicherung des Browsers
- **Konkrete Maßnahmen:**
 - Installation von Sicherheits-Erweiterungen
 - Deaktivierung unsicherer Browser-Funktionen

6.3 APP.5.2 E-Mail/Groupware

- **Relevanz:** Kommunikations- und Kollaborationsplattform
- **Anwendung:** Schutz der E-Mail-Kommunikation
- **Konkrete Maßnahmen:**
 - Spam- und Malware-Filter
 - Verschlüsselung vertraulicher E-Mails

7 SYS - IT-Systeme

7.1 SYS.2.1 Allgemeiner Client

- **Relevanz:** Grundlegender Baustein für Arbeitsplatzrechner
- **Anwendung:** Absicherung des Clients
- **Konkrete Maßnahmen:**
 - Starke Benutzerauthentifizierung
 - Restriktive Berechtigungsvergabe

7.2 SYS.3.1 Laptop

- **Relevanz:** Mobiles Arbeiten im HomeOffice
- **Anwendung:** Besondere Schutzmaßnahmen für mobile Geräte
- **Konkrete Maßnahmen:**
 - Festplattenverschlüsselung
 - Diebstahlsicherung

7.3 SYS.3.2.1 Smartphone/Tablet

- **Relevanz:** Mobile Kommunikation und Datenverarbeitung
- **Anwendung:** Absicherung mobiler Endgeräte
- **Konkrete Maßnahmen:**
 - Mobile Device Management (MDM)
 - Container-Lösungen zur Trennung von dienstlichen und privaten Daten

8 NET - Netzwerke und Kommunikation

8.1 NET.2.2 WLAN-Nutzung

- **Relevanz:** Drahtlose Vernetzung am Arbeitsplatz
- **Anwendung:** Absicherung des WLAN-Zugangs
- **Konkrete Maßnahmen:**
 - Einsatz von WPA3-Verschlüsselung
 - Separates Gäste-WLAN

8.2 NET.3.3 VPN

- **Relevanz:** Sichere Verbindung zum Unternehmensnetzwerk
- **Anwendung:** Verschlüsselte Kommunikation
- **Konkrete Maßnahmen:**
 - Nutzung eines sicheren VPN-Clients
 - Starke Authentifizierung beim VPN-Zugang

9 INF - Infrastruktur

9.1 INF.8 Häuslicher Arbeitsplatz

- **Relevanz:** Gestaltung des HomeOffice
- **Anwendung:** Physische Sicherheit im Heimumfeld
- **Konkrete Maßnahmen:**
 - Sicherer Aufbewahrungsort für sensible Unterlagen
 - Bildschirmsperre bei Abwesenheit

9.2 INF.9 Mobiler Arbeitsplatz

- **Relevanz:** Arbeit von unterwegs
- **Anwendung:** Schutz mobiler Arbeitsmittel
- **Konkrete Maßnahmen:**
 - Sichtschutzfilter für Bildschirme
 - Physischer Schutz der Geräte

10 DER - Detektion und Reaktion

10.1 DER.1 Detektion von sicherheitsrelevanten Ereignissen

- **Relevanz:** Erkennung von Sicherheitsvorfällen
- **Anwendung:** Monitoring-Mechanismen
- **Konkrete Maßnahmen:**

- Einsatz von Endpoint Detection and Response (EDR)
- Protokollierung sicherheitsrelevanter Ereignisse

10.2 DER.2.1 Behandlung von Sicherheitsvorfällen

- **Relevanz:** Strukturierte Reaktion auf Vorfälle
- **Anwendung:** Incident-Response-Prozesse
- **Konkrete Maßnahmen:**
 - Dokumentierte Vorgehensweise bei Vorfällen
 - Klare Meldewege und Eskalationspfade

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

11.1 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

11.2 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

11.3 Abgabeformat:

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