Einführung in den IT-Grundschutz des BSI

IT-Sicherheit

ITT-Net-IS

9. März 2025

1 Das Bundesamt für Sicherheit in der Informationstechnik (BSI)

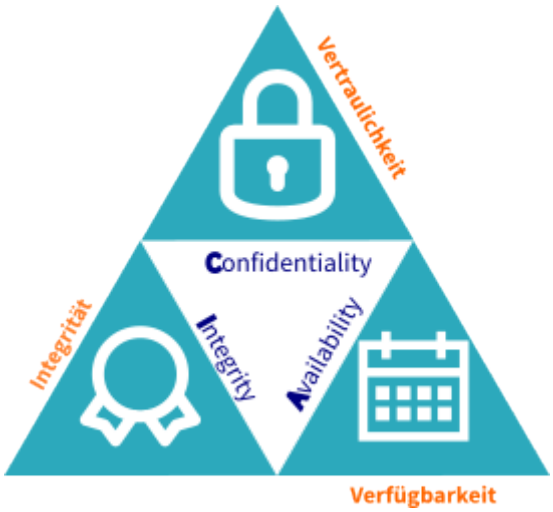
Das BSI ist die zentrale deutsche Cyber-Sicherheitsbehörde und fungiert als Gestalter der Informationssicherheit in Deutschland. Das BSI wurde 1991 gegründet und hat seinen Hauptsitz in Bonn. Zu den Hauptaufgaben gehören:

- Entwicklung von Sicherheitsstandards und -richtlinien
- Beratung von Behörden und Unternehmen in Sicherheitsfragen
- Zertifizierung von IT-Produkten und Systemen
- Aufklärung der Öffentlichkeit über IT-Sicherheitsrisiken
- Abwehr von Cyberangriffen auf kritische Infrastrukturen

2 Der IT-Grundschutz des BSI

Der IT-Grundschutz bietet eine systematische Methodik zur Identifizierung und Umsetzung angemessener Sicherheitsmaßnahmen für IT-Systeme. Das IT-Grundschutz-Kompendium beschreibt praxisnahe Anforderungen und Maßnahmen für verschiedene IT-Komponenten und -Systeme.

2.1 Die wesentlichen Schutzziele (CIA-Triade)



Die drei grundlegenden Schutzziele der Informationssicherheit sind:

1. ***Vertraulichkeit (Confidentiality): Informationen dürfen nur von autorisierten Personen eingesehen und bearbeitet werden.***
2. ***Integrität (Integrity): Die Korrektheit, Vollständigkeit und Unverfälschtheit von Informationen muss gewährleistet sein.***
3. ***Verfügbarkeit (Availability): Informationen und IT-Systeme müssen bei Bedarf funktionsfähig und zugänglich sein.***

Ergänzende Schutzziele sind:

- ***Authentizität: Die Echtheit und Glaubwürdigkeit von Informationen und Identitäten.***
- ***Nichtabstreitbarkeit: Die Nachweisbarkeit von Handlungen und Transaktionen.***
- ***Zurechenbarkeit: Die eindeutige Zuordnung von Aktionen zu Personen oder Systemen.***

3 Der IT-Grundschutz-Prozess

Der IT-Grundschutz-Prozess besteht aus folgenden Hauptphasen:

1. **Initiierung**: Einrichtung eines Informationssicherheitsmanagements
2. **Organisation**: Festlegung von Rollen, Verantwortlichkeiten und Ressourcen
3. **Strukturanalyse**: Erfassung aller relevanten Informationen, IT-Systeme und Geschäftsprozesse
4. **Schutzbedarfsfeststellung**: Bestimmung des Schutzbedarfs für jedes Objekt
5. **Modellierung**: Abbildung der IT-Infrastruktur nach IT-Grundschutz
6. **IT-Grundschutz-Check**: Überprüfung der Umsetzung der Sicherheitsanforderungen
7. **Risikoanalyse**: Identifikation und Bewertung von Risiken
8. **Realisierung**: Umsetzung der Sicherheitsmaßnahmen
9. **Aufrechterhaltung**: Kontinuierliche Verbesserung

4 Beispielszenario: Mittelständisches Ingenieurbüro ”TechPlan GmbH”

Die TechPlan GmbH ist ein Ingenieurbüro mit 50 Mitarbeitern, das Planungsleistungen für Industrieanlagen anbietet. Die IT-Infrastruktur umfasst:

- Einen Serverraum mit 5 physischen Servern
- 50 Arbeitsplatzrechner
- Ein internes WLAN und kabelgebundenes Netzwerk
- Eine Internetverbindung mit Firewall
- Spezielle CAD-Software für Konstruktionszeichnungen
- Ein Dokumentenmanagementsystem für Projektdaten

Das Unternehmen arbeitet mit vertraulichen Kundendaten und wertvollen Konstruktionsplänen, die vor unbefugtem Zugriff geschützt werden müssen.

4.1 Schritt 1: Initiierung des IT-Grundschutz-Prozesses

Der Geschäftsführer hat die Bedeutung der Informationssicherheit erkannt und einen **IT-Sicherheitsbeauftragten** ernannt. Es wurde ein **Budget** für Sicherheitsmaßnahmen bereitgestellt.

4.2 Schritt 2: Definition des Informationsverbunds

Der Informationsverbund wurde definiert als alle IT-Systeme, Anwendungen und Räumlichkeiten, die für die Geschäftsprozesse der TechPlan GmbH relevant sind.

4.3 Schritt 3: Strukturanalyse

In der Strukturanalyse wurden folgende **Komponenten** identifiziert:

- Geschäftsprozesse (Kundenakquise, Projektplanung, Konstruktion)
- Anwendungen (CAD-Software, Dokumentenmanagementsystem, E-Mail)
- IT-Systeme (Server, Arbeitsplatzrechner, Netzwerkkomponenten)
- Räumlichkeiten (Serverraum, Büros)

CAD-Software (Computer-Aided Design) ist eine Software zur computergestützten Konstruktion, Modellierung und Detaillierung technischer Zeichnungen und 3D-Modelle in Bereichen wie Ingenieurwesen, Architektur und Produktdesign.

4.4 Schritt 4: Schutzbedarfsfeststellung

Für jede Komponente wurde der Schutzbedarf nach den drei Grundwerten festgelegt:
Beispiel: CAD-Daten und Konstruktionspläne

- Vertraulichkeit: **HOCH** (Enthält wertvolles geistiges Eigentum)
- Integrität: **HOCH** (Fehler können zu Planungs- und Produktionsfehlern führen)
- Verfügbarkeit: **MITTEL** (Kurzzeitige Ausfälle sind verkraftbar)

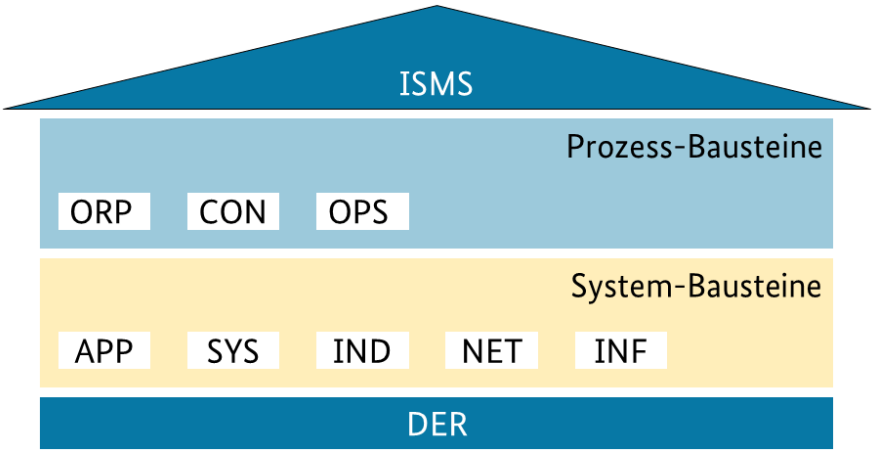


Abbildung 1: Bausteine IT-Grundschutz | Quelle: BSI-Kompendium

4.5 Schritt 5: Modellierung

Die IT-Komponenten wurden den Bausteinen des IT-Grundschutz-Kompendiums zugeordnet:

- **ISMS**: Sicherheitsmanagement
- Prozessbausteine
  - **ORP**: Organisation und Personal
  - **CON**: Konzepte und Vorgehensweisen
  - **OPS**: Betrieb
- Systembausteine:
  - **APP**: Anwendungen
  - **SYS**: IT-Systeme
  - **IND**: Industrielle IT
  - **NET**: Netze und Kommunikation
  - **INF**: Infrastruktur
- **DER**: Detektion und Reaktion

5 Sicherheitskonzepte im Detail

IT-Sicherheit erfordert ein mehrschichtiges Konzept aus **technischen**, **organisatorischen** (TOM) sowie personellen **Maßnahmen**, das auf den IT-Grundschutz des BSI basiert und an die spezifischen Anforderungen einer Organisation angepasst werden muss. Ein zentraler Aspekt ist die Verhältnismäßigkeit der Sicherheitsmaßnahmen im Verhältnis zum Schutzbedarf. Durch das Zusammenspiel dieser Maßnahmen entsteht eine mehrstufige Verteidigung nach dem Prinzip der **Defense-in-Depth**.

5.1 Zugangskontrolle (physischer Zugang)

- **Definition**: Maßnahmen, die den physischen Zugang zu IT-Systemen regeln.
- **Beispiel bei TechPlan**:
- Zutrittskontrollsystem mit Chipkarten für den Serverraum

- Protokollierung aller Zutritte
- Videoüberwachung an kritischen Zugangspunkten

5.2 Zugriffskontrolle (logischer Zugriff)

- **Definition**: Maßnahmen, die den logischen Zugriff auf IT-Systeme und Daten regeln.
- **Beispiel bei TechPlan**:
- Rollenbasierte Zugriffsrechte im Dokumentenmanagementsystem
- Zwei-Faktor-Authentifizierung für administrative Zugriffe
- Berechtigungskonzept nach dem Need-to-Know-Prinzip

5.3 Netzwerksicherheit

Bei TechPlan wurden folgende Maßnahmen implementiert:

- Segmentierung des Netzwerks durch VLANs
- Firewall mit restriktiven Regelsets
- VPN für externen Zugriff
- Intrusion Detection System zur Erkennung von Angriffsversuchen

5.4 Datensicherung

Die Datensicherungsstrategie umfasst:

- Tägliche inkrementelle Backups
- Wöchentliche Vollsicherungen
- Monatliche Auslagerung von Backup-Medien an einen externen Standort
- Regelmäßige Tests der Wiederherstellbarkeit

5.5 Notfallmanagement

TechPlan hat ein Notfallkonzept erstellt, das folgende Aspekte umfasst:

- Notfallrollen und -verantwortlichkeiten
- Eskalationswege
- Wiederanlaufpläne für kritische Systeme
- Jährliche Notfallübungen

6 Praktische Umsetzung ausgewählter Maßnahmen

Die theoretischen Sicherheitskonzepte müssen in der Praxis durch konkrete Maßnahmen umgesetzt werden. Diese Maßnahmen sind in drei Kategorien unterteilt:

1. Personelle Maßnahmen.
2. Technische Maßnahmen.
3. Organisatorische Maßnahmen.

Diese Dreiteilung verdeutlicht den ganzheitlichen Ansatz des IT-Grundschutzes, der nicht nur auf technische Lösungen setzt, sondern auch die menschlichen und prozessualen Aspekte der Informationssicherheit berücksichtigt.

6.1 Maßnahmen für Mitarbeiter

- Regelmäßige Sensibilisierungsschulungen
- Klare Regelungen für den Umgang mit Passwörtern
- Verpflichtung zur Einhaltung der Sicherheitsrichtlinien
- Clean-Desk-Policy

6.2 Technische Maßnahmen

- Einsatz von Verschlüsselung für sensible Daten
- Automatisierte Sicherheitsupdates
- Zentrale Protokollierung und Auswertung von Sicherheitsereignissen
- Malware-Schutz auf allen Systemen

6.3 Organisatorische Maßnahmen

- Dokumentation der IT-Landschaft
- Regelmäßige Sicherheitsaudits
- Einbindung der Informationssicherheit in Veränderungsprozesse
- Incident-Response-Prozesse

7 Übung: Schutzbedarfsanalyse für den eigenen Computerarbeitsplatz

7.1 Aufgabenstellung

Führen Sie eine Schutzbedarfsanalyse für Ihren Computerarbeitsplatz durch. Gehen Sie dabei wie folgt vor:

1. **Inventarisierung**:
    - Listen Sie alle wichtigen Komponenten auf (Hardware, Software, Daten)
    - Beschreiben Sie kurz ihre Funktion und Bedeutung
2. **Schutzbedarfsfeststellung**:

- Bewerten Sie für jede Komponente den Schutzbedarf bezüglich Vertraulichkeit, Integrität und Verfügbarkeit
- Verwenden Sie die Kategorien NIEDRIG, MITTEL, HOCH
- Begründen Sie Ihre Einschätzung

3. **Bedrohungsanalyse**:
   - Identifizieren Sie mindestens 5 relevante Bedrohungen
   - Beschreiben Sie potenzielle Auswirkungen
4. **Maßnahmenplanung**:
   - Leiten Sie konkrete Schutzmaßnahmen ab
   - Priorisieren Sie diese nach Wichtigkeit und Aufwand
5. **Dokumentation**:
   - Erstellen Sie ein kurzes Dokument (2-3 Seiten), das Ihre Ergebnisse zusammenfasst
   - Fügen Sie einen Maßnahmenplan mit Zeitschiene bei

7.2 Hilfsmittel

Nutzen Sie zur Orientierung folgende Bausteine aus dem IT-Grundschutz-Kompendium:

- SYS.2.1: Allgemeiner Client
- APP.1.1: Office-Produkte
- NET.2.2: WLAN-Nutzung
- ORP.1: Organisation
- CON.2: Datenschutz

7.3 Bewertungsgrundlage

Die Schutzbedarfsanalyse wird anhand folgender Kriterien bewertet:

- Vollständigkeit der Inventarisierung
- Nachvollziehbarkeit der Schutzbedarfsbewertungen
- Relevanz der identifizierten Bedrohungen
- Angemessenheit der vorgeschlagenen Maßnahmen
- Qualität der Dokumentation