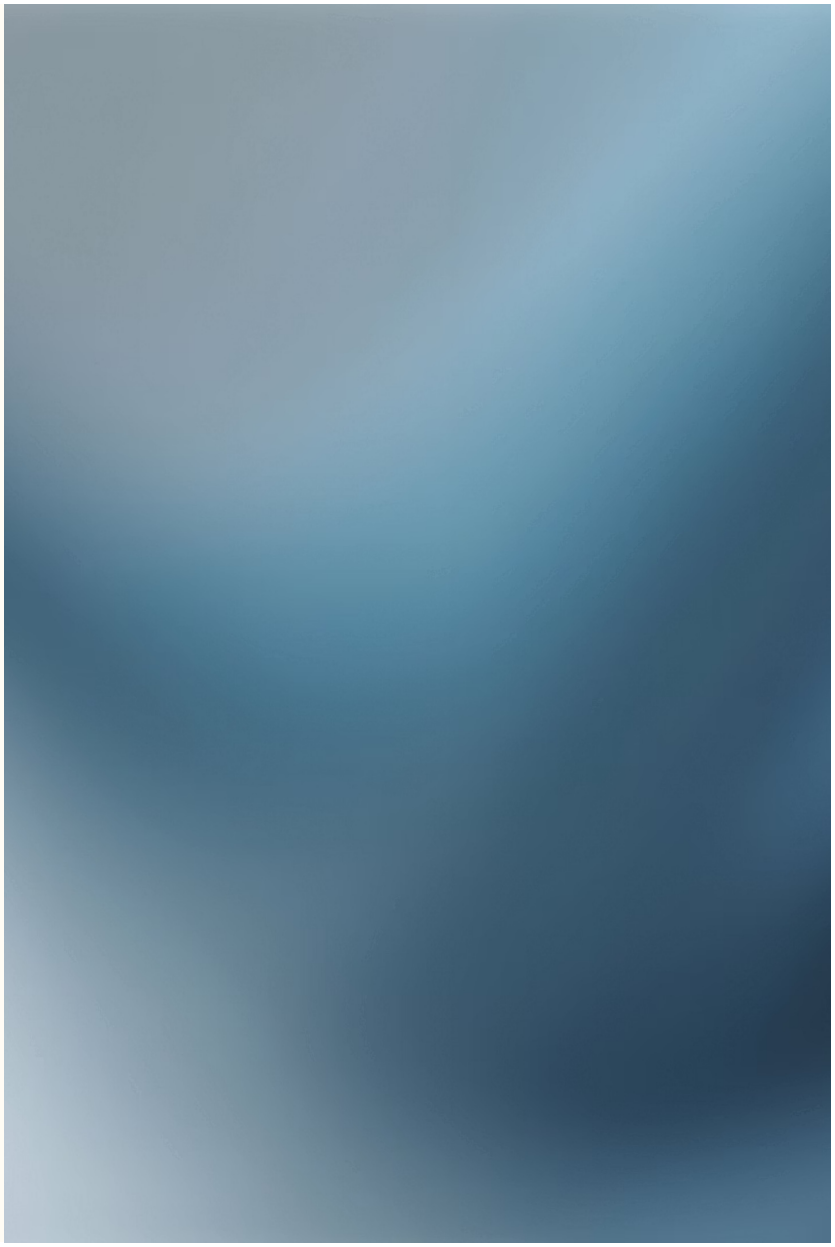
# Modellierung eines Sicherheitskonzepts nach BSI IT-Grundschutz

*Ein strukturierter Ansatz zur Entwicklung und Umsetzung von IT-Sicherheitsmaßnahmen für IT-Fachpersonal und Studierende*



ZIEL & MERKSATZ

# Vom Schutzbedarf zum umsetzbaren Sicherheitskonzept

## Ziel der Modellierung

*Aus dem ermittelten Schutzbedarf und den Grundschutz-Bausteinen ein praktisch umsetzbares und nachweisbares Sicherheitskonzept entwickeln*

## Der zentrale Merksatz

***Konzept = „Welche Maßnahmen wo, warum, wer, bis wann"***

*Ein Sicherheitskonzept muss konkrete Antworten liefern auf:*

- *Welche spezifischen Schutzmaßnahmen werden implementiert?*
- *Wo werden diese Maßnahmen angewendet (Systeme, Räume, Verbindungen)?*
- *Warum sind sie erforderlich (Schutzbedarf, Risiken)?*
- *Wer ist verantwortlich für Umsetzung und Kontrolle?*
- *Bis wann müssen die Maßnahmen realisiert sein?*

# Grundschutz-Bausteine verstehen

*Der BSI IT-Grundschutz arbeitet mit standardisierten Bausteinen – thematischen Modulen, die spezifische Anforderungen und Maßnahmen für verschiedene IT-Sicherheitsbereiche definieren. Ein Baustein ist dabei* ***kein einzelnes Produkt oder Tool****, sondern ein strukturiertes Maßnahmenpaket.*

## Organisation & Management

*Beispielmaßnahme: Etablierung einer Informationssicherheitsrichtlinie mit definierten Rollen und Verantwortlichkeiten*

## Personal & Awareness

*Beispielmaßnahme: Regelmäßige Sicherheitsschulungen und Verpflichtung der Mitarbeitenden auf Vertraulichkeit*

## IT-Betrieb

*Beispielmaßnahme: Implementierung eines strukturierten Patch-Management-Prozesses mit Logging und Monitoring*

## Netzwerk & Kommunikation

*Beispielmaßnahme: Netzsegmentierung mit Firewall-Regeln und verschlüsselten VPN-Verbindungen*

## Server, Clients & Anwendungen

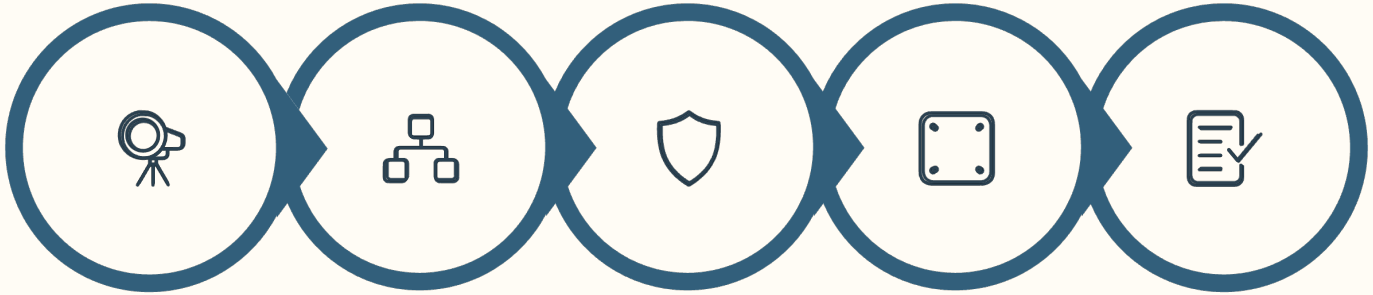
*Beispielmaßnahme: System-Hardening durch Deaktivierung unnötiger Dienste und restriktive Rechtevergabe*

## Physische Infrastruktur

*Beispielmaßnahme: Zutrittskontrollsystem für Serverräume mit Klimaüberwachung und Brandmeldeanlage*

# Der 7-Stufen-Ablauf zur Konzepterstellung

*Die systematische Entwicklung eines Sicherheitskonzepts folgt einem strukturierten Prozess, der vom Scope bis zur Wirksamkeitsprüfung reicht.*




*Dieser Ablauf stellt sicher, dass alle relevanten Aspekte systematisch erfasst und bearbeitet werden. Jede Phase baut auf der vorherigen auf und schafft die Grundlage für die nächste.*

01

### Festlegen

*Scope und Grenzen des Sicherheitskonzepts definieren*

02

### Erfassen

*Strukturanalyse aller Anwendungen, Systeme und Räume*

03

### Bewerten

*Schutzbedarf für jedes Objekt ermitteln*

04

### Zuordnen

*Passende Bausteine den Objekten zuweisen*

05

### Ableiten

*Konkrete Maßnahmen definieren und priorisieren*

06

### Planen

*Umsetzung mit Verantwortlichen und Terminen*

07

### Prüfen

*Wirksamkeit durch Kontrollen und Audits sicherstellen*

# Schutzbedarfskategorien: Normal, Hoch, Sehr hoch

*Die Einstufung des Schutzbedarfs ist entscheidend für die Auswahl angemessener Sicherheitsmaßnahmen. Der Schutzbedarf orientiert sich am **potenziellen Schaden**, der bei Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit entstehen kann.*

> ***Prüfungswichtig:** „Hoch" bedeutet nicht automatisch „teure Tools kaufen", sondern systematisch **Schadenpotenzial begründen und Schutz erhöhen**.*

PRAXISBEISPIEL

# Konzept-Modell: Struktur eines Sicherheitskonzepts

*Ein Sicherheitskonzept besteht aus einer strukturierten Liste von Maßnahmenpaketen pro Objekt. Jedes Objekt wird einzeln betrachtet und bewertet.*

## Objekt: Firewall (IT-System)

***Schutzbedarf:*** *Verfügbarkeit hoch, Integrität hoch, Vertraulichkeit mittel/hoch*

***Bausteine:*** *Netzwerk, IT-Betrieb, Admin-Zugänge*

***Maßnahmen:***

- *Multi-Faktor-Authentifizierung für alle administrativen Zugriffe*
- *Dokumentiertes und geprüftes Firewall-Regelwerk*
- *Zentrales Logging aller Firewall-Events*
- *Automatisiertes Backup der Konfiguration (täglich)*
- *Strukturierter Patch-Management-Plan*
- *High-Availability-Tests (quartalsweise)*

## Objekt: Ticketsystem (Anwendung)

***Schutzbedarf:*** *Vertraulichkeit hoch, Integrität mittel/hoch, Verfügbarkeit mittel*

***Bausteine:*** *Anwendungssicherheit, Datenschutz, Zugriffskontrolle*

***Maßnahmen:***

- *Rollenbasiertes Berechtigungskonzept nach Need-to-know-Prinzip*
- *Definierte Löschfristen für personenbezogene Daten*
- *Umfassende Protokollierung aller Zugriffe und Änderungen*
- *Auftragsverarbeitungsvertrag bei externer Hosting-Lösung*
- *Verschlüsselte Datenübertragung (TLS 1.3)*

# Das ISMS: Managementrahmen für IT-Sicherheit

*Ein Information Security Management System (ISMS) ist **kein statisches Dokument**, sondern ein kontinuierlicher Betriebsprozess. Es schafft den organisatorischen Rahmen für systematische IT-Sicherheit.*

## Der PDCA-Zyklus als Kernprinzip

***Plan:** Sicherheitsziele definieren, Risiken bewerten, Schutzbedarf ermitteln, Maßnahmenplan erstellen*

***Do:** Maßnahmen technisch und organisatorisch umsetzen, Ressourcen bereitstellen, Verantwortlichkeiten zuweisen*

***Check:** Wirksamkeit prüfen durch interne Audits, Security-Reports, Penetrationstests, Compliance-Checks*

***Act:** Lessons Learned dokumentieren, Verbesserungen ableiten, Prozesse anpassen, Maßnahmen optimieren*

# Minimal-ISMS für den Praxiseinsatz

*Auch kleinere Betriebe benötigen ein funktionierendes ISMS. Hier die wesentlichen Komponenten für einen praktikablen Einstieg:*

### Grundlegende Richtlinien

*Informationssicherheitsrichtlinie und Passwort-Policy als dokumentierte Basis*

### Definierte Rollen

*Informationssicherheitsbeauftragter (ISB), Datenschutzbeauftragter (DSB), IT-Betrieb, Management*

### Kernprozesse

*Patch-Management, Backup & Restore-Tests, Berechtigungsmanagement, Incident-Management*

### Nachweise & KPIs

*Update-Reports, Auftragsverarbeitungs-Listen, Audit-Logs, Restore-Protokolle, messbare Kontrollpunkte*

### Regeltermine

*Quartalsweise Reviews mit aktualisierter Maßnahmenliste und Statusbericht an Management*

***Beispiel-KPIs:*** *Patch-Management → „95% aller kritischen Patches innerhalb 14 Tage installiert"; Backup → „Monatlicher erfolgreicher Restore-Test dokumentiert"; Berechtigungen → „Quartalsweise Rezertifizierung aller administrativen Rechte"*

# Rollen und Verantwortlichkeiten: ISB vs. DSB

## Informationssicherheitsbeauftragter (ISB)

***Fokus:*** *Informationssicherheit (CIA-Triade), Maßnahmen, Betrieb, Risiken*

***Kernaufgaben:***

- *Erstellen und Aktualisieren von Sicherheitsrichtlinien*
- *Koordinieren von Schutzmaßnahmen und Priorisierung mit Management*
- *Moderieren der Risiko- und Schutzbedarfsanalyse*
- *Organisieren von Awareness-Schulungen*
- *Begleiten von Sicherheitsvorfällen (Koordination, interne Kommunikation)*
- *Vorbereiten von Nachweisen und Audits*

> *Der ISB muss nicht alle Maßnahmen selbst technisch umsetzen – er sorgt dafür, dass sie erfolgen und kontrolliert werden.*

## Datenschutzbeauftragter (DSB)

***Fokus:*** *Datenschutz (DSGVO), Betroffenenrechte, Rechtskonformität*

***Kernaufgaben:***

- *Überwachung der DSGVO-Compliance*
- *Bearbeitung von Betroffenenanfragen (Auskunft, Löschung)*
- *Prüfung von Rechtsgrundlagen für Datenverarbeitung*
- *Verhandlung und Kontrolle von Auftragsverarbeitungsverträgen*
- *Entwicklung und Überwachung von Löschkonzepten*
- *Beratung zu Datenschutz-Folgenabschätzungen*

## Zuordnungsbeispiele

***ISB:*** *Multi-Faktor-Authentifizierung, Log-Aufbewahrungsdauer aus Security-Sicht, Patch-Management*

***DSB:*** *Auskunftsanfragen von Betroffenen, Löschfristen personenbezogener Daten, Datenschutzerklärungen*

KONZEPT-CHECKLISTE

# Vollständigkeit prüfen: Ihre Sicherheitskonzept-Checkliste

1 **Scope eindeutig definiert**

*Alle relevanten Systeme, Anwendungen, Räume und Verbindungen sind identifiziert und dokumentiert*

2 **Schutzbedarf je Objekt begründet**

*Für jedes Objekt liegt eine nachvollziehbare Schutzbedarfsbewertung (normal/hoch/sehr hoch) vor*

3 **Bausteine und Anforderungen zugeordnet**

*Passende Grundschutz-Bausteine sind den Objekten zugewiesen, relevante Anforderungen identifiziert*

4 **Maßnahmenliste mit Priorisierung**

*Konkrete Maßnahmen sind definiert und nach Priorität kategorisiert (Muss/Soll/Kann)*

5 **Verantwortliche, Termine, Nachweise**

*Für jede Maßnahme sind Verantwortliche benannt, Umsetzungstermine festgelegt und Nachweisverfahren definiert*

6 **Kontrollpunkte etabliert**

*Audit-Termine, Review-Prozesse und Kontrollmechanismen zur Wirksamkeitsprüfung sind implementiert*

7 **Incident-Prozess definiert**

*Vorgehen bei Sicherheitsvorfällen ist dokumentiert, Kommunikationswege und Eskalationsstufen sind festgelegt*

---

## Mini-Prüfung: Praxisaufgabe VPN-Verbindung

***Aufgabe:*** *Erstellen Sie ein Mini-Sicherheitskonzept für eine VPN-Verbindung zum Homeoffice mit Schutzbedarf „hoch" und mindestens 5 konkreten Maßnahmen. Berücksichtigen Sie Vertraulichkeit, Integrität und Verfügbarkeit.*