Grundschutzniveau: was heißt das im Betrieb?

Prüfungswissen

Solide Basisabsicherung gegen typische Bedrohungen

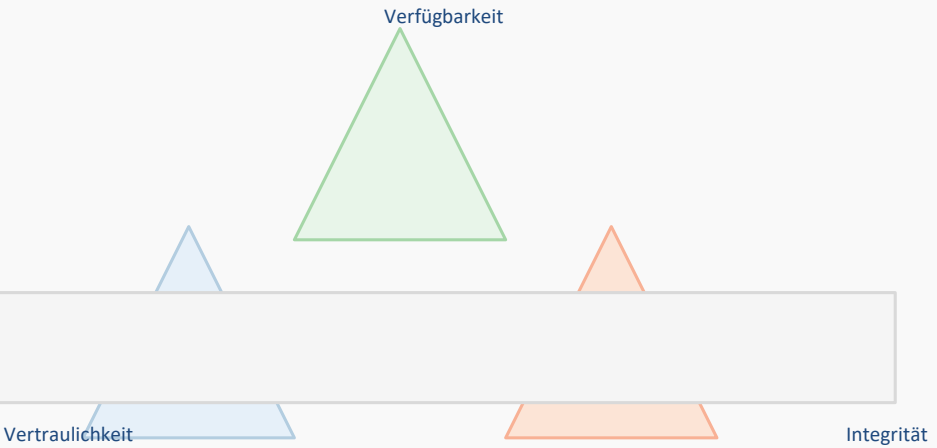
Schutz der Vertraulichkeit, Integrität & Verfügbarkeit (CIA)

Standardmaßnahmen plus organisatorische Regeln und technische Kontrollen

Prüfungsfallen & Tipps

Grundschutz ist ein laufender Prozess – nicht einmalig

Technik ohne Organisation greift zu kurz (keine Policy, keine Verantwortlichen)



Merker: „Basis-Schutz = Prozesse + Technik + Menschen“

[1]

Organisatorische Maßnahmen: Rollen & Verantwortung

Prüfungswissen

IT-Sicherheitsbeauftragter koordiniert Sicherheit, Policies und Awareness

Verantwortlichkeiten für Systeme, Daten und Prozesse klar festlegen

Sicherheitsrichtlinien regeln Nutzung, Zugriff, Updates und Datenumgang

Prüfungsfallen & Tipps

„Alle sind zuständig“ ⇒ niemand fühlt sich verantwortlich

Richtlinien ohne Schulung und Kontrolle versanden schnell

Beispiel: Owner für Fileserver, Patch-Verantwortlicher, Incident-Kontakt

[2]

IT-Sicherheitsrichtlinie: typische Inhalte

Prüfungswissen

Passwort- und MFA-Regeln, Geräte- und Softwarefreigabe, Patch-Management

Datenklassifizierung, sichere Speicherung und Übertragung

Remote Access: VPN, RDP/SSH, Logging und Überwachung

Prüfungsfallen & Tipps

Zu komplexe Policies werden ignoriert – kurz, klar und durchsetzbar

Fehlende Ausnahmeregeln fördern Schatten-IT

Merker: Policy muss im Alltag funktionieren.

[3]

Passwort-Policy & MFA (AP1-Klassiker)

Prüfungswissen

Lange, merkbare Passphrasen statt kurzer, komplexer Kennwörter

Keine Passwortweitergabe; Passwortmanager nutzen; Lockout/Sperrregeln umsetzen

MFA als zweiter Faktor – besonders für Admins und kritische Dienste

Prüfungsfallen & Tipps

„Komplex aber kurz“ ist schlechter als „lang & merkbar“

MFA nur für Admins? Besser auch für kritische Benutzerkonten

Merker: Passphrase + MFA schlägt Sonderzeichen-Zwang.

[4] [5]

Technische Maßnahmen: Virenschutz & EDR

Prüfungswissen

EDR überwacht kontinuierlich Endpunkte, analysiert Telemetrie und erkennt Malware, Credential-Theft und Laterale Bewegung

Verhaltenserkennung, maschinelles Lernen und Threat Intelligence identifizieren auch unbekannte Angriffe

Automatische Maßnahmen: Isolation, Prozessbeendigung, Forensik und zentrale Verwaltung

Prüfungsfallen & Tipps

Antivirus ohne aktuelle Signaturen ist wirkungslos

EDR ersetzt keine restriktive Rechtevergabe; Härtung bleibt Pflicht

Beispiel: EDR-Alarm → Client isolieren → Ticket & Incident bearbeiten

[6] [7]

Technische Maßnahmen: Firewall & Netzsegmentierung

Prüfungswissen

Firewall kontrolliert Datenverkehr auf Basis von Regeln (Ports, IPs, Anwendungen)

Netzsegmentierung trennt VLANs/Netze für Clients, Server, Gäste und Admins

„Default Deny“: nur notwendige Ports und Protokolle freigeben

Prüfungsfallen & Tipps

„Alles freigeben, damit es läuft“ öffnet Einfallstore für Angreifer

Flache Netze erleichtern laterale Bewegungen innerhalb des Unternehmens

Merker: Trennen reduziert Schaden.

[8] [9] [10]

Technische Maßnahmen: Anti-Spam & Mail-Sicherheit

Prüfungswissen

Einsatz von Spam-/Phishing-Filtern, Attachment-Sandboxing und URL-Checks

SPF, DKIM & DMARC authentifizieren Absender und begrenzen Spoofing

Awareness: Nutzer melden verdächtige E-Mails – schnelle Reaktion schützt alle

Prüfungsfallen & Tipps

Filter sind nie 100 % – Anwenderprozesse bleiben nötig

Ein Klick kann reichen – Meldewege müssen klar sein

Merker: Verdächtig? Nicht klicken, melden.

[11] [12]

Normen & Standards: ISO 2700x & BSI Grundschutz

Prüfungswissen

ISO 27001 definiert Anforderungen an ein ISMS, basierend auf CIA, Risikoanalyse und kontinuierlicher Verbesserung

ISO 2700x-Familie liefert Begriffe, Controls und Guidelines

BSI IT-Grundschutz: Baustein-Kataloge und Vorgehen für Schutzmaßnahmen

Prüfungsfallen & Tipps

Norm ≠ automatische Sicherheit – es ist ein Rahmen mit Nachweisen

Zertifizierung bedeutet nicht Unverwundbarkeit

Merker: ISO = Managementsystem; Grundschutz = Maßnahmenkatalog & Methodik

[13] [14] [15] [16]

Datenschutz: DSGVO & BDSG

Prüfungswissen

DSGVO: EU-weite Regeln zur Verarbeitung personenbezogener Daten

BDSG ergänzt die DSGVO national in Deutschland

Kernthemen: Rechtsgrundlage, Zweckbindung, Datenminimierung, TOMs

Prüfungsfallen & Tipps

„Wir brauchen das vielleicht“ ist kein legitimer Zweck

Verarbeitung ohne Rechtsgrundlage führt zu hohem Risiko

Merker: Zweck + Rechtsgrundlage + TOMs + Löschung

[17] [18]

Personenbezogene Daten: Definition & Beispiele

Prüfungswissen

Personenbezogen = identifizierte oder identifizierbare natürliche Person

Beispiele: Name, Adresse, E-Mail, IP-Adresse, Personalnummer, Standortdaten

Besonders schützenswert: z. B. Gesundheitsdaten, Religion

Prüfungsfallen & Tipps

Pseudonymisiert ≠ anonym – oft weiter personenbezogen

Logfiles können personenbezogene Daten enthalten

Beispiel: Kundenticket mit Name + IP = personenbezogen

[19]

Betroffenenrechte (DSGVO)

Prüfungswissen

Recht auf Auskunft, Berichtigung, Löschung (Recht auf Vergessenwerden)

Recht auf Einschränkung der Verarbeitung und Datenübertragbarkeit

Recht auf Widerspruch und Beschwerde bei der Aufsichtsbehörde

Prüfungsfallen & Tipps

Fehlende Fristen/Prozesse verursachen Stress und Bußgelder

Daten ohne Übersicht verstreut ⇒ Auskunft & Löschung kaum möglich

Merker: Rechte brauchen Prozesse + Datenübersicht.

[20] [21]

Technische & organisatorische Maßnahmen (TOMs)

Prüfungswissen

Technisch: Zugriffskontrolle, Verschlüsselung, Backup/Restore, Logging, Network & System Protection, Session Isolation

Organisatorisch: Richtlinien, klare Rollen, Prozesse (Incident, On-/Offboarding), Bewertung von Dienstleistern

Training & Awareness, ISMS & Dokumentation, regelmäßige Audits

Prüfungsfallen & Tipps

Backup ohne Restore-Test ist nutzlos

Rechte wachsen unkontrolliert ohne Rezertifizierung – Least Privilege beachten

Merker: TOMs = Technik + Organisation.

[22]

Schutzbedarfsanalyse: warum macht man das?

Prüfungswissen

Ziel: angemessene Schutzmaßnahmen durch Klassifizierung nach normal, hoch oder sehr hoch

Basis: Schadensauswirkung bei Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit

Verhindert Over-/Under-Engineering durch differenzierte Einstufung

Prüfungsfallen & Tipps

Schutzbedarf bewertet Auswirkungen – Eintrittswahrscheinlichkeit gehört zur Risikoanalyse

Alles als „sehr hoch“ zu deklarieren ist unbrauchbar

Merker: Schutzbedarf = wie schlimm, wenn’s schiefgeht.

[23] [24]

Schutzbedarfsanalyse nach BSI: Vorgehen

Prüfungswissen

Assets identifizieren: Anwendungen, Systeme, Räume, Verbindungen

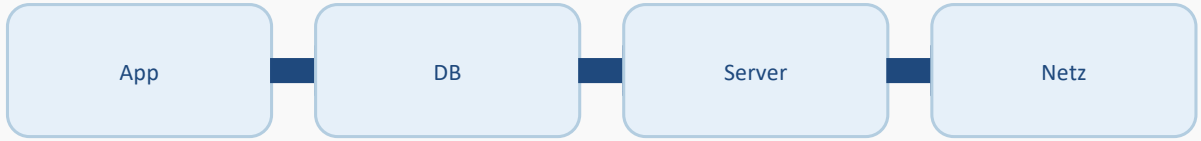
Für jedes Asset CIA bewerten und Schutzbedarf ableiten

Abhängigkeiten & Vererbung berücksichtigen: höchster Bedarf dominiert

Prüfungsfallen & Tipps

Abhängigkeiten vergessen (Netz, AD, Backup)

Ohne Dokumentation kein Nachweis – Prüfung scheitert



Bildidee: Asset-Kette „App → DB → Server → Netz“

[25]

Schutzbedarf: Anwendungen

Prüfungswissen

Kriterien: Datenart (personenbezogen?), Kritikalität der Geschäftsprozesse, benötigte Verfügbarkeit

Beispiel: HR-App hat oft hohe Vertraulichkeit; Monitoring-System eher hohe Verfügbarkeit

Testsysteme enthalten häufig Echtdaten – entsprechend schützen

Prüfungsfallen & Tipps

„Nur intern“ bedeutet nicht ungefährlich – interne Apps können sehr sensibel sein

Testsysteme mit Echtdaten werden oft vergessen und ungeschützt gelassen

Beispiel: Lohnabrechnung = hohe/sehr hohe Vertraulichkeit.

[26] [27]

Schutzbedarf: IT-Systeme (Server & Clients)

Prüfungswissen

Server: Rollen (AD, Fileserver, DB) → oft hohe Kritikalität – Verlust wirkt sich stark aus

Clients: Massenhaft, aber Zugriff auf Daten – durch Härtung, EDR und MDM schützen

Backup & Wiederherstellung für kritische Systeme; Identitätssysteme sind Kronjuwelen

Prüfungsfallen & Tipps

Admin-Rechte auf Clients ermöglichen laterale Bewegung

Uneinheitliche Patchstände öffnen Angreifern Tür und Tor

Merker: AD/Identität ist die Kronjuwel – besonders schützen.

[28]

Schutzbedarf: Räume

Prüfungswissen

Physische Sicherheit: Zutrittskontrolle, Schlüsselmanagement, Brandschutz

Klima/Strom: USV, ggf. Notstrom, Kühlung entsprechend dem Schutzbedarf

Serverräume nur für Berechtigte und protokollierter Zutritt

Prüfungsfallen & Tipps

Serverraum als Abstellkammer erhöht Ausfall- und Brandrisiko

Unbegleitete Besucher in sensiblen Bereichen stellen ein Risiko dar

Beispiel: Serverraum nur für Berechtigte, Zutritt wird protokolliert.

[29]

Schutzbedarf: Kommunikationsverbindungen

Prüfungswissen

Übertragungen sichern: VPN, TLS/HTTPS, IPsec – Verschlüsselung schützt Daten unterwegs

Verfügbarkeit sicherstellen: Redundanz, Monitoring und Failover je nach Schutzbedarf

Segmentierung und Zugriffskontrolle auch für interne Verbindungen

Prüfungsfallen & Tipps

„Internes Netz ist sicher“ – gefährliche Annahme; Verschlüsselung intern nicht vergessen

Unverschlüsselte Admin-Protokolle (z. B. Telnet) sind zu vermeiden

Merker: Verbindung = Angriffsfläche.

[30] [31]

Sicherheitskonzept nach BSI: Bausteine

Prüfungswissen

Grundschutz-Kompendium enthält Bausteine (ORP, ORG, CON, OPS, SYS, NET, APP etc.)

Jeder Baustein definiert Anforderungen und Maßnahmen zur Umsetzung

Konzept dokumentiert Ziele, Scope, Maßnahmen und Verantwortlichkeiten

Prüfungsfallen & Tipps

Bausteine ohne Umsetzung und Prüfung bleiben reines Papier

Scope muss klar definiert sein – welche Systeme und Prozesse werden erfasst?

Merker: Baustein = Maßnahmenpaket.

[32]

Schutzbedarfskategorien: normal • hoch • sehr hoch

Prüfungswissen

Normal: begrenzter Schaden; Standardmaßnahmen genügen

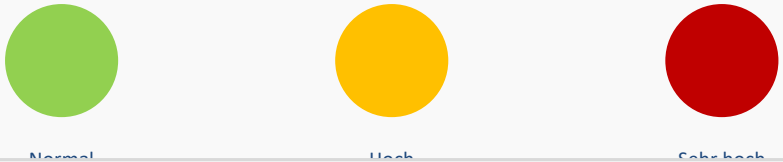
Hoch: erheblicher Schaden; erhöhte Schutzmaßnahmen notwendig

Sehr hoch: existenzbedrohend; stärkste Maßnahmen & strenge Kontrollen

Prüfungsfallen & Tipps

Kategorien müssen nachvollziehbar begründet sein

„Alles sehr hoch“ macht die Analyse unbrauchbar



Beispiel: Kundendatenbank: Vertraulichkeit hoch; Produktionssystem: Verfügbarkeit hoch

[33] [34] [35]

ISMS implementieren (PDCA-Zyklus)

Prüfungswissen

ISMS ist ein Managementsystem: Policies, Risikoanalyse, Maß
Audits und Verbesserung

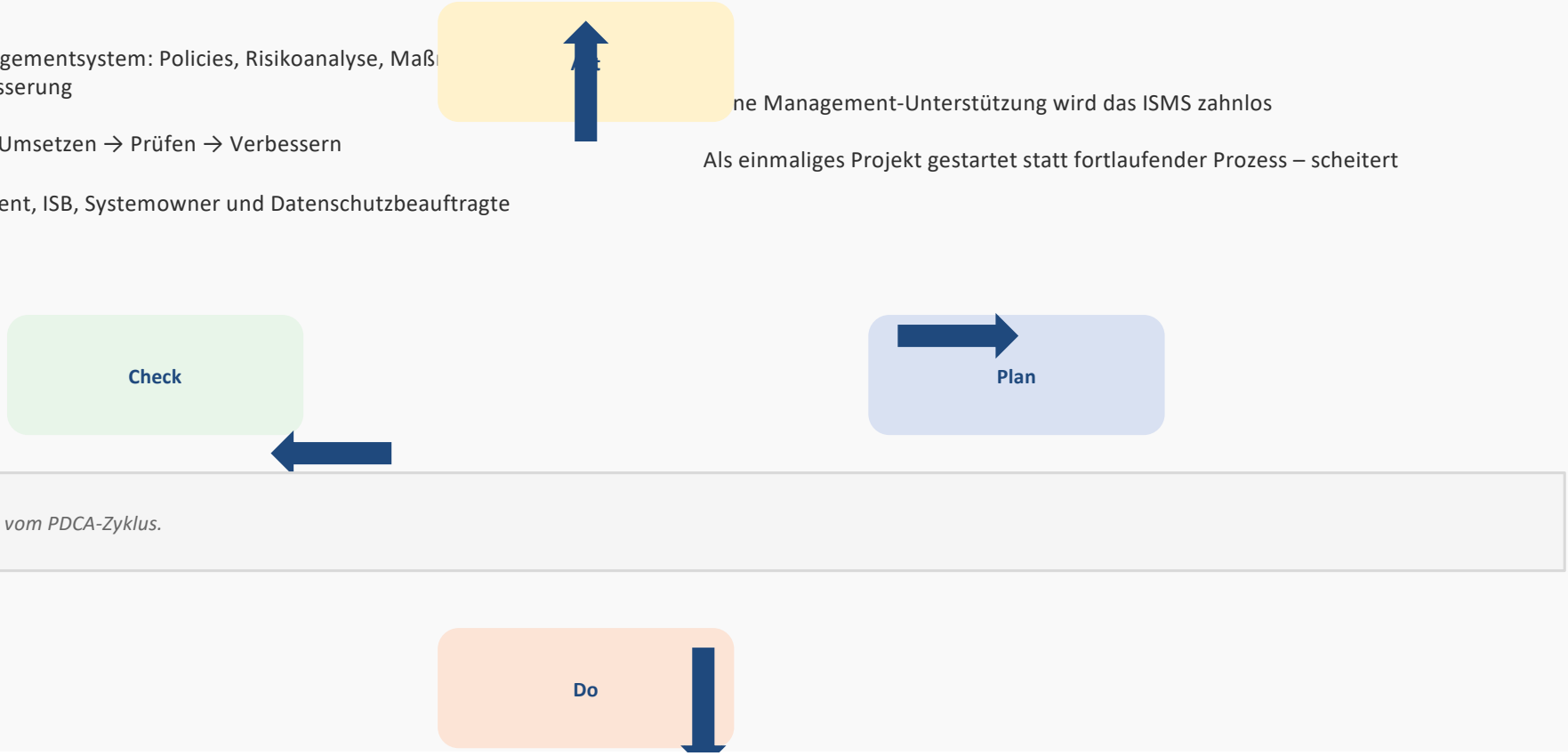
Zyklus: Planen → Umsetzen → Prüfen → Verbessern

Rollen: Management, ISB, Systemowner und Datenschutzbeauftragte

Prüfungsfallen & Tipps

ne Management-Unterstützung wird das ISMS zahnlos

Als einmaliges Projekt gestartet statt fortlaufender Prozess – scheitert



Merker: ISMS lebt vom PDCA-Zyklus.

[36]

Awareness: Sicherheitsbewusstsein schaffen

Prüfungswissen

Schulungen zu Phishing, Passwörtern, Datenhandling und Meldewegen durchführen

Sicherheitskultur fördern: melden statt verstecken; klare Ansprechpartner

Phishing-Simulationen, kurze Micro-Learnings und Poster zur Erinnerung

Prüfungsfallen & Tipps

Einmal jährlich 60 Minuten reichen nicht – kontinuierliche Trainings nötig

Schuldzuweisungen verhindern Meldungen und schwächen die Kultur

Merker: Lieber einmal zu viel melden als einmal zu wenig.

[37]

Security by Design & Security by Default

Prüfungswissen

Security by Design: Sicherheit als integraler Bestandteil des Entwicklungsprozesses (Anforderungen, Threat Modeling, sichere Komponenten, Tests)

Security by Default: Produkte werden mit sicheren Standardkonfigurationen ausgeliefert (z. B. MFA, keine Default-Passwörter, Logging aktiviert)

Ziel: „Build it in“ statt „Bolt it on“; sichere Basis von Anfang an

Prüfungsfallen & Tipps

Nachträgliches „Anschrauben“ von Sicherheit ist teuer und ineffektiv

Unsichere Default-Einstellungen werden in der Produktion oft vergessen

Merker: Sicher ist Standard, nicht Option.

[38] [39] [40] [41]

Zugang & Zugriff: Authentifizierung & Autorisierung

Prüfungswissen

Authentifizierung: verifiziert Identität (z. B. Benutzername/Passwort, MFA, Zertifikate)

Autorisierung: bestimmt, was der authentifizierte Nutzer tun darf (Rollen, Rechte, ACL)

Prinzipien: Least Privilege, Need-to-Know, regelmäßige Rezertifizierung der Berechtigungen

Prüfungsfallen & Tipps

Shared Accounts zerstören Nachvollziehbarkeit

Rechte wachsen schleichend ohne Entzug (Role Creep) – regelmäßige Reviews notwendig

Merker: AuthN = wer bist du? AuthZ = was darfst du?

[42] [43] [44]

Backup, Verfügbarkeit, Verschlüsselung, SSH vs Telnet

Prüfungswissen

Backup: 3-2-1-Regel (3 Kopien, 2 Medien, 1 Off-site); Restore testen; RPO/RTO definieren

Verfügbarkeit: RAID/SAN, Redundanz, Monitoring & Failover – ersetzt kein Backup

Verschlüsselung: symmetrisch (ein Schlüssel) vs. asymmetrisch (Public/Private, Zertifikate, PKI) – TLS/HTTPS schützt Transport

SSH verschlüsselt und authentifiziert; Telnet überträgt alles im Klartext – daher vermeiden

Prüfungsfallen & Tipps

RAID ersetzt kein Backup – Datenverlust durch Fehlkonfiguration oder Malware bleibt möglich

Abgelaufene Zertifikate legen Dienste lahm; Telnet/unsichere Admin-Zugänge sind No-Go

Merker: Backup = Wiederherstellung; SSH/TLS = sichere Übertragung.

[45] [46] [47] [48] [49]