Datensicherheit (AP1)

Gefährdungen • Gegenmaßnahmen • BSI • TOMs • Schutzbedarf

GRUNDLAGEN

Datensicherheit: Ziel & Abgrenzung

Was ist Datensicherheit?

Datensicherheit bzw. Informationssicherheit bedeutet den Schutz von Informationen und Systemen vor Schäden. Ziel ist die Sicherstellung der Schutzziele (CIA-Triade und mehr).

Abgrenzung zum Datenschutz

Datenschutz fokussiert personenbezogene Daten und rechtliche Aspekte. Datensicherheit ist breiter gefasst und schützt alle Informationen – auch ohne Personenbezug.

> ***Merksatz:*** *Datenschutz fragt „Darf ich?" – Datensicherheit fragt „Wie schütze ich's zuverlässig?"*

SCHUTZZIELE

CIA-Triade: Die drei Säulen der Informationssicherheit

Vertraulichkeit (Confidentiality)

Nur berechtigte Personen dürfen Informationen lesen oder kennen. Schutz vor unbefugtem Zugriff durch Verschlüsselung und Zugriffskontrollen.

Integrität (Integrity)

Daten sind korrekt und unverändert. Systeme funktionieren wie vorgesehen. Schutz vor Manipulation durch Prüfsummen und Versionierung.

Verfügbarkeit (Availability)

Zugriff auf Informationen und Systeme ist rechtzeitig möglich. Services laufen stabil und können bei Bedarf genutzt werden.

Erweiterte Schutzziele

Neben der CIA-Triade gibt es weitere wichtige Schutzziele, die in modernen Sicherheitskonzepten berücksichtigt werden müssen. Diese ergänzen die Grundprinzipien und ermöglichen eine umfassende Absicherung.

***Prüfungsfalle:** Integrität bedeutet NICHT Verschlüsselung – Integrität bedeutet „nicht manipuliert und korrekt"!*

Authentizität

Echtheit von Daten und Identitäten – ist der Absender wirklich der, der er vorgibt zu sein?

Verbindlichkeit

Nachvollziehbarkeit von Aktionen – wer hat was wann getan? Wichtig für Audits und rechtliche Nachweise.

Nachweisbarkeit

Logging und Protokollierung ermöglichen die Rekonstruktion von Vorgängen und Sicherheitsvorfällen.

DEUTSCHLAND

BSI & IT-Grundschutz

Bundesamt für Sicherheit

Das BSI (Bundesamt für Sicherheit in der Informationstechnik) ist die zentrale Cyber-Sicherheitsbehörde des Bundes. Es entwickelt Standards, Methoden und Best Practices für die IT-Sicherheit.

IT-Grundschutz-Konzept

Methodisches Vorgehen mit Bausteinen und konkreten Maßnahmen gegen typische Bedrohungen. Die Idee: solide Basisabsicherung statt jedes Mal bei Null anfangen.

- *Strukturierte Vorgehensweise*
- *Praxiserprobte Maßnahmenkataloge*
- *Bausteine für verschiedene IT-Komponenten*
- *Auch für Unternehmen nutzbar*

***Wichtig:** BSI-Grundschutz ist nicht nur für Behörden – auch Unternehmen nutzen das Kompendium als Orientierung!*

SCHUTZBEDARFSANALYSE

Schutzbedarf: Kategorien & Grundlogik

Der Schutzbedarf wird für jedes Asset getrennt bestimmt – und zwar individuell für Vertraulichkeit, Integrität und Verfügbarkeit. Die Einstufung erfolgt in drei Kategorien basierend auf der Schadenshöhe bei Verletzung des jeweiligen Schutzziels.

Normal

Begrenzte Auswirkungen – der Schaden ist überschaubar und beherrschbar

Hoch

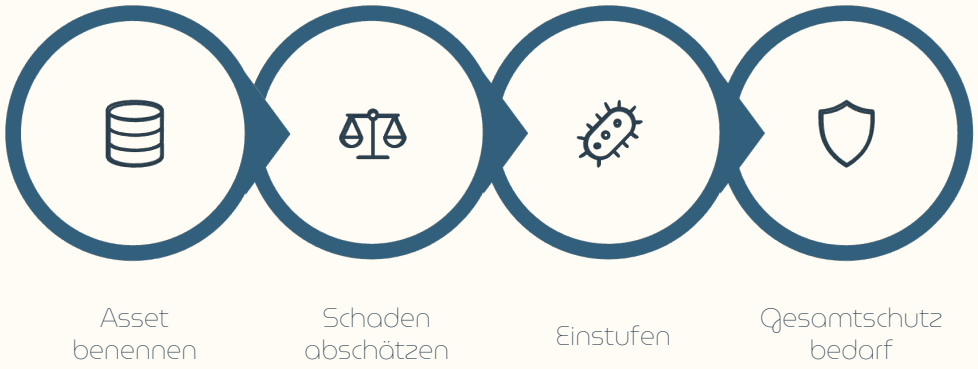
Erhebliche Auswirkungen – der Schaden kann beträchtlich sein und die Existenz gefährden

Sehr hoch

Katastrophale Auswirkungen – existenzbedrohende Schäden sind zu erwarten

Prüfungsfalle: *Es gibt NICHT einen Schutzbedarf für alles – jedes Asset wird pro Grundwert (C/I/A) getrennt betrachtet!*

Schutzbedarf praktisch bestimmen



Der Gesamtschutzbedarf ergibt sich typischerweise aus dem höchsten Einzelwert der drei Grundwerte. Diese Methodik gewährleistet ein angemessenes Schutzniveau.

Schadensabschätzung berücksichtigt:

- ***Finanzielle Schäden:*** *direkte Kosten, Umsatzverluste*
- ***Rechtliche Folgen:*** *Bußgelder, Haftung, Vertragsstrafen*
- ***Image-Schäden:*** *Vertrauensverlust, Reputationsschaden*
- ***Betriebsausfall:*** *Produktionsstillstand, Ausfallzeiten*

Praxis-Beispiel: Kundendatenbank

Vertraulichkeit: hoch *(personenbezogene Daten, DSGVO-Bußgelder möglich)*
Integrität: hoch *(falsche Kundendaten führen zu Fehlern)*
Verfügbarkeit: normal bis hoch *(je nach Geschäftsmodell)*

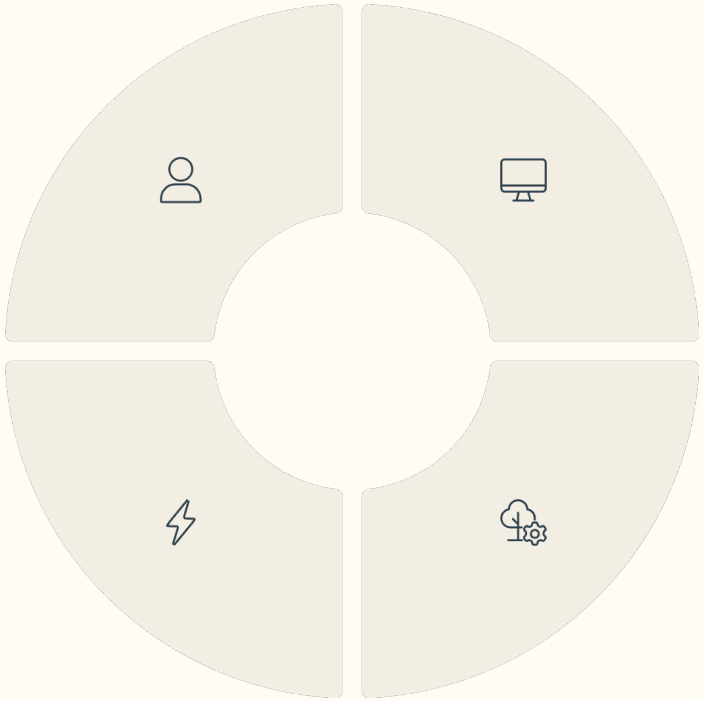
Wichtig: *„Überall hoch" ist teuer und unkonkret – Schutz muss angemessen sein!*

GEFÄHRDUNGSANALYSE

Gefährdungsquellen: Woher kommt der Ärger?

Mensch

Social Engineering, Phishing, Bedienfehler, Insider-Bedrohungen, mangelndes Sicherheitsbewusstsein



Technik

Schwachstellen, Malware, Ransomware, Fehlkonfigurationen, veraltete Software, Exploits

Umgebung & Physik

Stromausfall, Brand, Wasser, Klimaprobleme, Diebstahl, Naturkatastrophen, physischer Zugang

Organisation

Fehlende Prozesse, unklare Verantwortlichkeiten, Schatten-IT, mangelndes Rechtemanagement

Realität: *Viele Vorfälle sind „Excel + Stress + falsches Recht", nicht „Hollywood-Hacker". Interne Fehler sind extrem häufig!*

Gefährdung Mensch: Social Engineering & Bedienfehler

Typische Angriffsvektoren

- **Phishing & Spear-Phishing:** gefälschte E-Mails mit Schadsoftware oder Links
- **Fake-Calls:** Anrufe vermeintlicher IT-Support-Mitarbeiter
- **Tailgating:** unbefugtes Betreten gesicherter Bereiche
- **Bedienfehler:** falscher Empfänger, falsche Freigaben, versehentliches Löschen

Wirksame Gegenmaßnahmen

- Regelmäßige Awareness-Trainings mit Praxisübungen
- Phishing-Simulationen zur Sensibilisierung
- Multi-Faktor-Authentifizierung (MFA) überall
- Passwortmanager bereitstellen
- Klare Meldewege für verdächtige Vorgänge
- Vier-Augen-Prinzip bei kritischen Freigaben

Stop – Check – Confirm: Bei ungewöhnlichen Anfragen immer innehalten, prüfen und per zweitem Kanal bestätigen!

Technische Gefährdungen: Schwachstellen & Malware

Bedrohungslandschaft

Die Kombination aus Schwachstellen und Exploits öffnet Angreifern Tür und Tor. Verschiedene Malware-Arten verfolgen unterschiedliche Ziele – von Datendiebstahl über Verschlüsselung bis zur Spionage.

- ***Trojaner:*** *getarnte Schadsoftware*
- ***Ransomware:*** *Verschlüsselung mit Lösegeldforderung*
- ***Wurm:*** *selbstverbreitende Malware*
- ***Spyware:*** *Ausspähung von Informationen*

Präventive Schutzmaßnahmen

- ***Patch-Management:*** *zeitnahes Einspielen von Updates für OS, Anwendungen und Firmware*
- ***Endpoint-Schutz:*** *Antivirus/EDR auf allen Geräten*
- ***System-Hardening:*** *unnötige Dienste deaktivieren*
- ***Sichere Konfiguration:*** *Best Practices umsetzen*
- ***Network Segmentation:*** *Netze trennen*
- ***Backup-Strategie:*** *regelmäßig und getestet*

Organisatorische Gefährdungen: Prozesse, Rollen & Rechte

Typische Schwachstellen

Organisatorische Mängel sind oft unterschätzte Sicherheitsrisiken. Fehlende Strukturen, Verantwortlichkeiten und Regelungen schaffen Einfallstore für Angriffe und Fehler.

- *Keine klaren Verantwortlichkeiten definiert*
- *Fehlendes Berechtigungskonzept*
- *Keine Regelungen für IT-Nutzung*
- *Schatten-IT durch private Tools/Cloud-Shares*
- *Unkontrollierter Datenabfluss*

***Realität:** „Alle sind Admin, sonst geht's schneller" – genau so brennt's später!*

***Mini-Check für die Praxis:** Ist das Onboarding geregelt? Gibt es ein Offboarding-Verfahren? Werden Rechte regelmäßig überprüft? Wenn nein – dringender Handlungsbedarf!*

Rollen & Rechte

Least Privilege-Prinzip umsetzen, Vier-Augen-Prinzip bei kritischen Änderungen

Richtlinien

Passwort-Policy, Mobile Device Management, Clean Desk Policy dokumentieren

Prozesse

Strukturiertes Onboarding und Offboarding, regelmäßige Rechte-Reviews

Physische & Umwelt-Gefährdungen

Gefährdungsquellen

- Stromausfall und Spannungsschwankungen
- Brand und Rauchentwicklung
- Wasser (Leitungsbruch, Überschwemmung)
- Klimaprobleme (Hitze, Kälte, Feuchtigkeit)
- Diebstahl von Hardware/Datenträgern
- Unbefugter physischer Zugang

Schutzmaßnahmen

- **Zutrittskontrolle:** Schließsysteme, Besuchermanagement
- **USV:** unterbrechungsfreie Stromversorgung
- **Brandschutz:** Rauchmelder, Löschanlage
- **Klimatisierung:** Überwachung von Temperatur und Feuchtigkeit
- **Serverraum-Konzept:** separate, gesicherte Räume
- **Backup-Strategie:** externe/offsite-Aufbewahrung

Physische und umweltbedingte Risiken werden oft unterschätzt, können aber zu massiven Ausfällen führen. Von Stromausfall bis Diebstahl – die Palette ist breit.

Defense in Depth: Das Schichtenprinzip

SCHUTZKONZEPTE

Mehrschichtiger Schutz

Das Defense-in-Depth-Prinzip setzt auf mehrere aufeinander aufbauende Sicherheitsebenen. Wenn eine Barriere überwunden wird, greifen die nachfolgenden Schichten.

Mini-Kette zum Merken:*Policy → Rechte → Technik → Monitoring → Notfallplan*

Die vier Schutzschichten

- ***Organisatorisch:*** *Richtlinien, Prozesse, Schulungen, Awareness*
- ***Technisch:*** *Firewalls, Verschlüsselung, Zugangskontrollen, Monitoring*
- ***Physisch:*** *Gebäudesicherheit, Zutrittskontrolle, Videoüberwachung*
- ***Personell:*** *Rollen, Verantwortlichkeiten, Know-how*

Prüfungswissen: *Einzelmaßnahmen sind kein Konzept! MFA ohne Rechtemanagement ist halbgar – erst die Kombination schafft Sicherheit.*

DSGVO

TOMs: Technische & organisatorische Maßnahmen

Gemäß Art. 32 DSGVO müssen Verantwortliche und Auftragsverarbeiter geeignete TOMs implementieren, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. TOMs sind der konkrete Nachweis der „Sicherheit der Verarbeitung".

Verschlüsselung & Pseudonymisierung

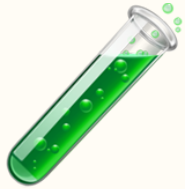
Daten verschlüsseln bei Übertragung und Speicherung. Personenbezug durch Pseudonyme reduzieren.

Zugriffskontrollen

Identitätsmanagement, Rollenkonzepte, MFA, Least-Privilege-Prinzip durchsetzen.

Backup & Restore

Regelmäßige Datensicherung, getestete Wiederherstellung, 3-2-1-Regel befolgen.



Tests & Evaluierung

Regelmäßige Überprüfung der Wirksamkeit, Penetrationstests, Audits durchführen.

Wichtig: *TOMs sind nicht nur Technik! Auch Prozesse, Schulungen und Dokumentation gehören dazu. TOMs = Konzept + Umsetzung + Nachweis.*

Zugriff & Identitäten: Der häufigste Hebel

Authentisierung vs. Autorisierung

Authentisierung: *Wer bist du? (Identität nachweisen)*
Autorisierung: *Was darfst du? (Berechtigungen prüfen)*

Grundprinzipien

- ***Least Privilege:*** *So wenig Rechte wie möglich, so viel wie nötig*
- ***Need-to-know:*** *Nur Zugriff auf tatsächlich benötigte Daten*
- ***Rollenmodell:*** *Rechte nach Funktion statt Person vergeben*
- ***Trennungsprinzip:*** *Admin-Konten getrennt von Nutzerkonten*

Multi-Faktor-Authentifizierung

MFA überall, wo's kritisch ist: Admin-Zugang, Cloud-Services, E-Mail, VPN. Mindestens zwei Faktoren kombinieren.

Identitätsmanagement

Zentrale Verwaltung von Benutzerkonten, automatisiertes Provisioning/Deprovisioning, regelmäßige Rezertifizierung.

Passwort-Strategie

Passwortmanager bereitstellen, komplexe Passwörter erzwingen, regelmäßiger Wechsel bei Verdacht.

Prüfungsfalle: *Geteilte Accounts = keine Nachvollziehbarkeit + kein sauberes Offboarding. Immer personengebundene Konten verwenden!*

Verfügbarkeit sichern: Backup, Restore & Redundanz

Die 3-2-1-Backup-Regel

Der Industriestandard für zuverlässige Datensicherung:

1. **3 Kopien der Daten**
   Original plus zwei Backups
2. **2 verschiedene Medien**
   Z.B. Festplatte + Band/Cloud
3. **1 Kopie extern/offsite**
   Schutz vor lokalem Totalausfall

Restore-Tests sind Pflicht!

Ein Backup ist wertlos, wenn die Wiederherstellung nicht funktioniert. Regelmäßige Tests garantieren die Funktionsfähigkeit im Ernstfall.

RTO & RPO verstehen

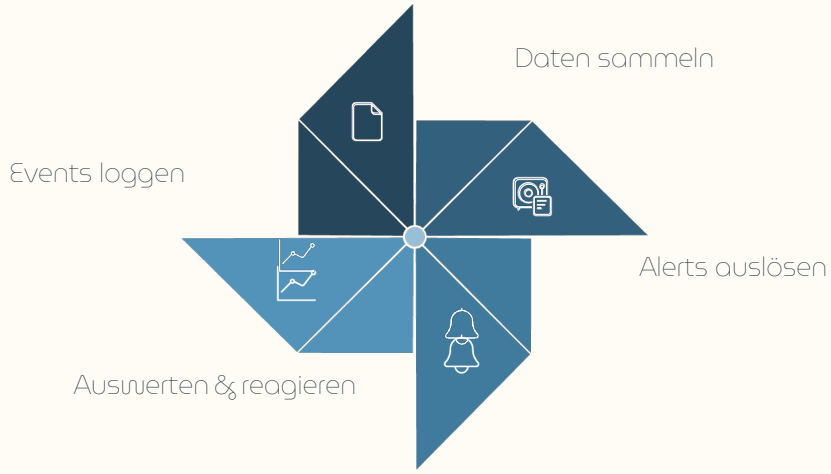
- ***RTO (Recovery Time Objective):*** *Maximale Ausfallzeit – wie schnell muss das System wieder laufen?*
- ***RPO (Recovery Point Objective):*** *Maximaler Datenverlust – wie alt dürfen wiederhergestellte Daten sein?*

Redundanz-Strategien

Mehrfache Systeme, Load Balancing, Failover-Mechanismen, geografisch verteilte Rechenzentren.

> ***Merksatz:*** *„Backup läuft durch" bedeutet NICHT „Restore klappt". Nur ein getestetes Restore ist ein Backup!*

Monitoring & Nachvollziehbarkeit



Ein umfassendes Monitoring-Konzept ist essenziell für die rechtzeitige Erkennung von Sicherheitsvorfällen und die Nachvollziehbarkeit von Aktionen.

Was muss geloggt werden?

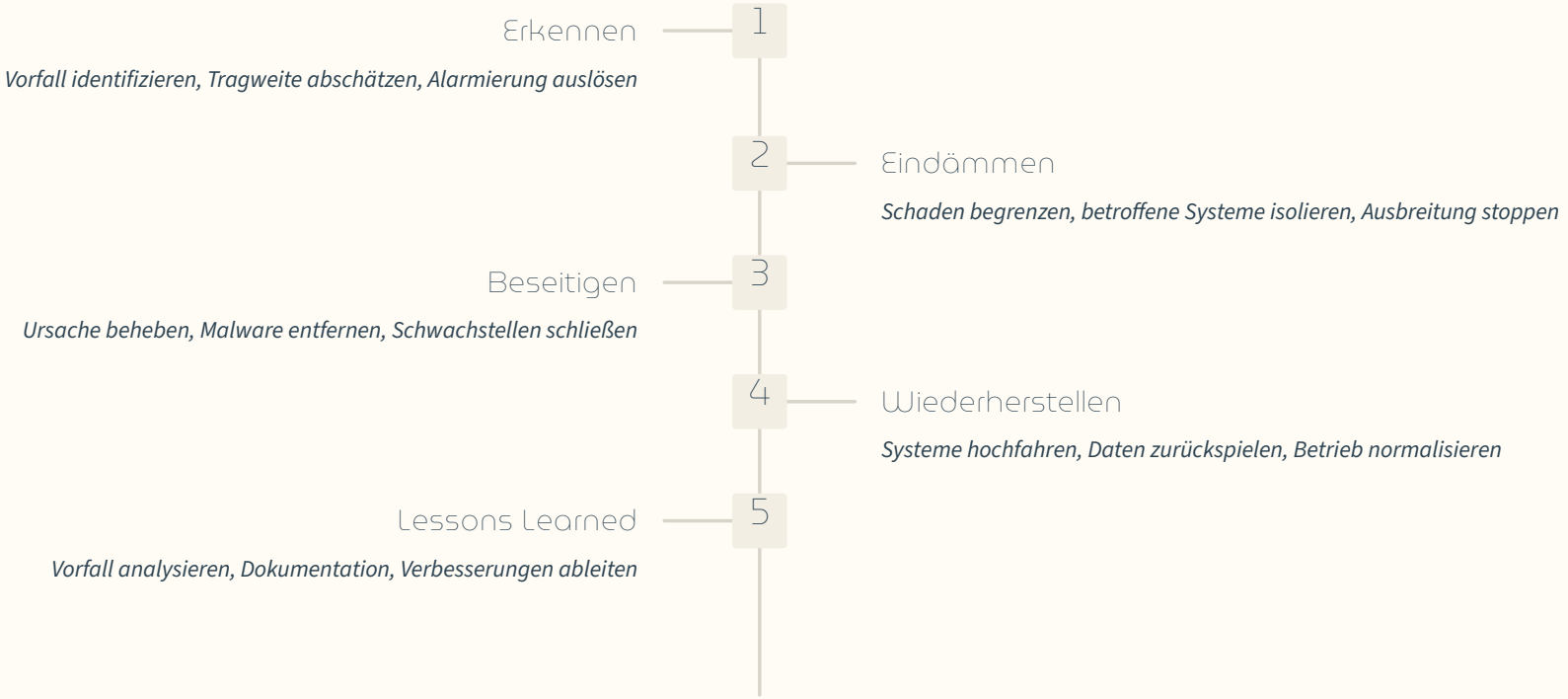
- *Login-Versuche (erfolgreich und fehlgeschlagen)*
- *Rechteänderungen und Systemkonfigurationen*
- *Administrative Aktionen und Zugriffe*
- *Fehler und Anomalien*
- *Zugriffe auf kritische Daten*
- *Systemereignisse und Performance-Metriken*

Effektive Auswertung

Logs ohne Auswertung sind nutzlos. Definieren Sie klare Alarmierungsregeln: Wer bekommt welche Alerts? Was gilt als „kritisch"? Automatisierte Korrelation und SIEM-Systeme helfen bei der Analyse.

Prüfungswissen: *Logging erfüllt das Schutzziel „Nachvollziehbarkeit" und ist Teil der TOMs gemäß Art. 32 DSGVO.*

Notfallmanagement: Wenn's trotzdem knallt



Ein durchdachter Incident-Response-Plan ist entscheidend: Wer macht was? Wann wird eskaliert? Welche Kontakte sind relevant? Ohne Runbook wird jede Störung chaotisch.

Merksatz: *Im Notfall denkst du nicht besser – du folgst dem Plan. Vorbereitung ist alles!*

PRÜFUNGSVORBEREITUNG

Prüfungsfallen & Schnell-Check

Schutzbedarf differenziert betrachten

Immer getrennt für Vertraulichkeit, Integrität und Verfügbarkeit bestimmen – dann erst Maßnahmen ableiten. Nicht „ein Wert für alles"!

Angemessenheit ist key

Maßnahmen müssen zum Risiko passen. „Überall sehr hoch" ist übertrieben und teuer. Risikobasiertes Vorgehen zeigen!

BSI-Grundschutz verstehen

Standardmaßnahmen für typische Gefährdungen. Nicht bei Null anfangen, sondern bewährte Bausteine nutzen.

Gefährdungen ganzheitlich

Nicht nur „Hacker von außen" – interne Fehler, Prozessmängel und Umwelteinflüsse sind mindestens genauso relevant!

TOMs sind mehr als Technik

Technische UND organisatorische Maßnahmen plus Dokumentation und Nachweis. Nur „Firewall" reicht niemals als Antwort!

Größe ist keine Ausrede

„Wir sind klein, wir brauchen das nicht" ist falsch – gerade kleine Ziele sind oft unvorbereitet und damit attraktiv.

10-Sekunden-Formel für die Prüfung: *Asset → C/I/A-Schaden abschätzen → Schutzbedarf einstufen → passendes Maßnahmenpaket ableiten*

SELBSTTEST

Mini-Quiz: Wissen testen

Teste dein Verständnis mit diesen vier offenen Fragen. Überlege dir die Antworten, bevor du in deine Unterlagen schaust!

Frage 1: Schutzziele

Erkläre Vertraulichkeit, Integrität und Verfügbarkeit jeweils an einem konkreten Beispiel aus einem Betrieb. Was passiert, wenn das jeweilige Schutzziel verletzt wird?

Frage 2: Schutzbedarfsanalyse

Wie würdest du den Schutzbedarf einer Lohnabrechnungstabelle für Vertraulichkeit, Integrität und Verfügbarkeit einstufen – und warum? Begründe deine Einstufung!

Frage 3: Gefährdungen & Maßnahmen

Nenne fünf typische Gefährdungen (aus verschiedenen Kategorien) und beschreibe jeweils eine konkrete, wirksame Gegenmaßnahme dazu.

Frage 4: TOMs verstehen

Was sind TOMs und warum reicht „eine Firewall" als Antwort auf die Frage nach Sicherheitsmaßnahmen fast nie aus? Welche weiteren Elemente gehören dazu?

Quellenhinweise für Vertiefung:

- *BSI: Schutzbedarfsfeststellung (Kategorien normal/hoch/sehr hoch)*
- *BSI: IT-Grundschutz-Kompendium / Elementare Gefährdungen*
- *DSGVO Art. 32 (Sicherheit der Verarbeitung)*