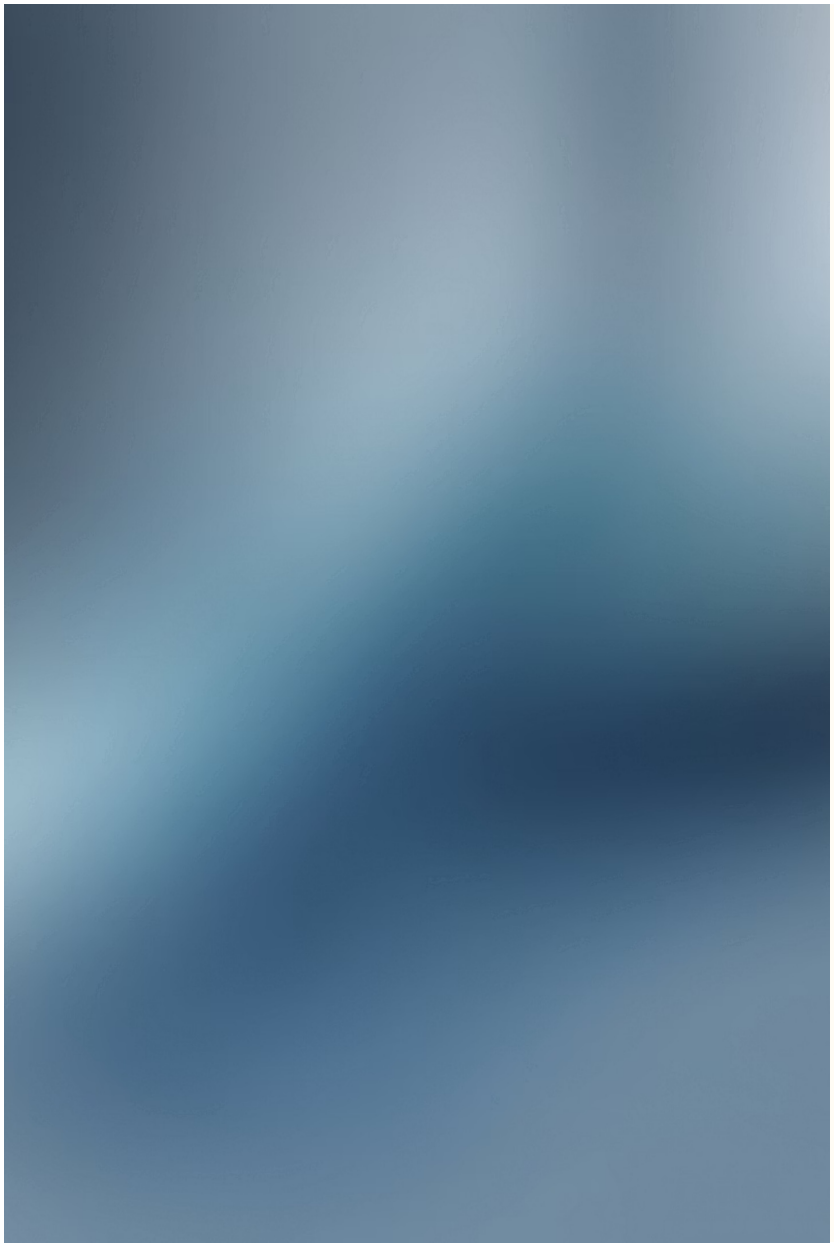


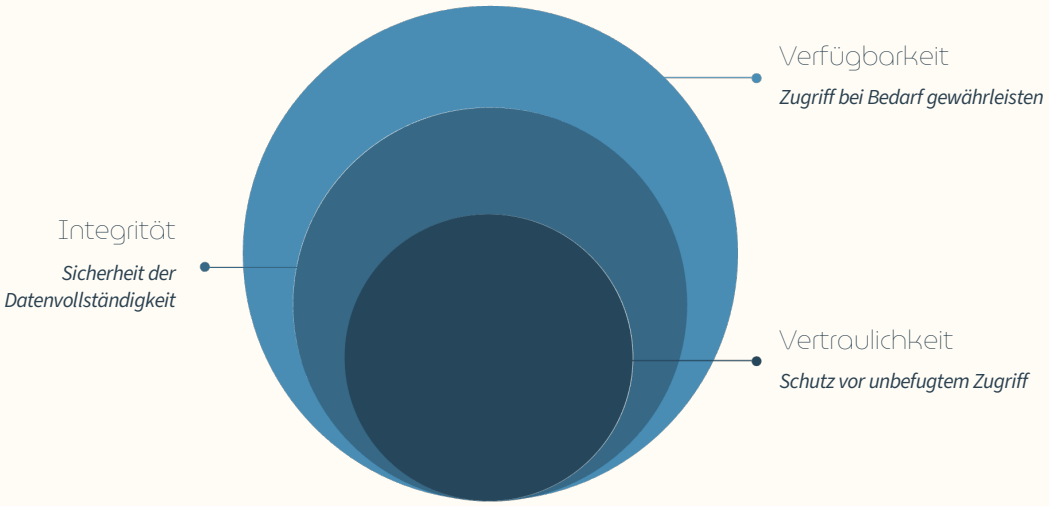
IT-Sicherheit & Datenschutz

KAPITEL 6

Grundlagen, Maßnahmen und rechtliche Anforderungen für sichere IT-Systeme im Unternehmensumfeld

EINFÜHRUNG

Schutzziele der IT-Sicherheit



Das CIA-Dreieck bildet die Grundlage jeder IT-Sicherheitsstrategie. Alle drei Schutzziele müssen gleichzeitig berücksichtigt werden, um einen wirksamen Schutz zu gewährleisten.

Technische Maßnahmen allein reichen nicht aus – nur durch die Kombination von Organisation, Technik und geschulten Mitarbeitenden entsteht echte Sicherheit.

Ziele der IT-Sicherheit

Vertraulichkeit

Schutz vor unbefugtem Zugriff auf sensible Informationen

Integrität

Sicherstellung der Korrektheit und Vollständigkeit von Daten

Verfügbarkeit

Gewährleistung des Zugriffs auf Systeme und Daten bei Bedarf

Darüber hinaus: Risikominimierung, Schadensbegrenzung und Einhaltung rechtlicher Vorgaben wie DSGVO und branchenspezifischer Compliance-Anforderungen.

Typische Fehleinschätzungen

„Security = Firewall"

Sicherheit umfasst weit mehr als technische Schutzmaßnahmen: Prozesse, Berechtigungskonzepte, Backup-Strategien und regelmäßige Schulungen sind ebenso entscheidend.

Fehlende Verantwortlichkeiten

Ohne klar definierte Zuständigkeiten bleiben Sicherheitsmaßnahmen oft unumgesetzt. Ein IT-Sicherheitsbeauftragter muss aktiv koordinieren und treiben.

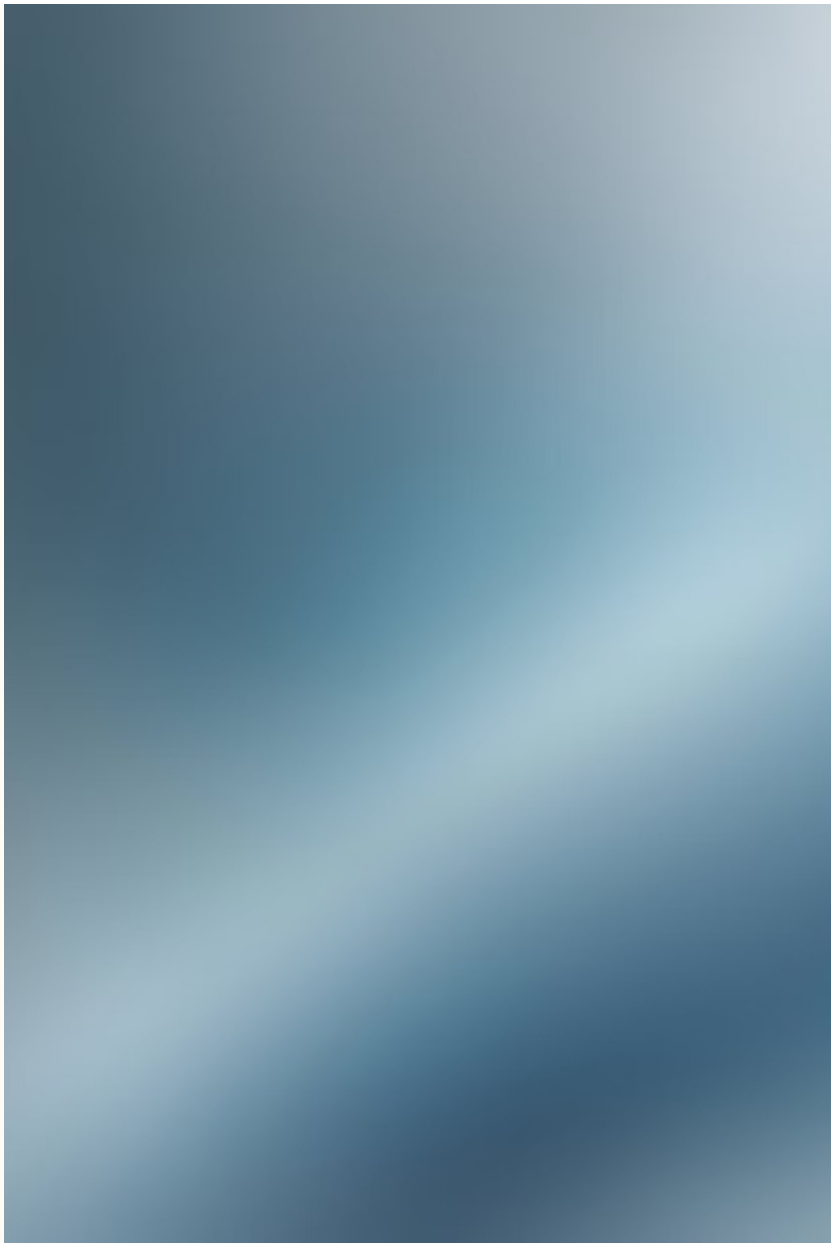
Keine Nachweisbarkeit

Fehlende Dokumentation und Logs machen Sicherheitskonzepte im Ernstfall wertlos. Audit-Trails und Nachweise sind unverzichtbar.

Praxis im Betrieb

Erfolgreiche IT-Sicherheit basiert auf einem ausgewogenen Mix aus organisatorischen Vorgaben, technischen Schutzmaßnahmen und sensibilisierten Mitarbeitenden.

Der Mensch bleibt oft das schwächste Glied – selbst die beste Technik hilft nicht, wenn Passwörter weitergegeben oder Phishing-Mails nicht erkannt werden.



QUIZ

Verständnisfragen: Grundlagen

1 CIA-Dreieck

Erklären Sie Vertraulichkeit, Integrität und Verfügbarkeit jeweils mit einem konkreten IT-Beispiel aus dem Betriebsalltag.

2 Grundschutzniveau

Welche fünf Maßnahmen würden Sie sofort einführen, wenn bisher kaum Security-Maßnahmen existieren?

3 Papier-Konzept

Woran erkennen Sie, dass ein Sicherheitskonzept nur auf dem Papier existiert, aber nicht gelebt wird?

4 Prüfbarkeit

Welche drei Dinge müssen dokumentiert sein, damit Security im Betrieb nachweisbar und prüfbar ist?

ORGANISATORISCHE MASSNAHMEN

Organisation schafft Sicherheit

Rollen und Verantwortung

Klare Zuständigkeiten sind die Grundlage: IT-Sicherheitsbeauftragter, definierte Eskalationswege und dokumentierte Verantwortlichkeiten verhindern, dass Sicherheitsaufgaben zwischen den Stühlen fallen.

Regeln ohne Durchsetzung bleiben wirkungslos – Policies müssen gelebt, geschult und kontrolliert werden.

Wesentliche Regeln und Policies

IT-Sicherheitsrichtlinie

Definiert erlaubte und verbotene Verhaltensweisen im Umgang mit IT-Ressourcen

Passwort-Policy

Regelt Komplexität, Länge, Wiederverwendung und MFA-Anforderungen

Clean-Desk-Policy

Verhindert unbefugten Zugriff auf sensible Dokumente und Bildschirminhalte

Remote-Work-Richtlinie

Definiert sichere Arbeitsweisen außerhalb des Büros, VPN-Pflicht und Geräteschutz

Kritische Prozesse etablieren

01

Patch- und Update-Management

Regelmäßige, koordinierte Aktualisierung aller Systeme

02

Incident-Meldeprozess

Klare Wege zur Meldung von Sicherheitsvorfällen

03

Berechtigungsprozess

Strukturierte Vergabe und Entzug von Zugriffsrechten

04

Schulungsprogramm

Kontinuierliche Awareness-Trainings für alle Mitarbeitenden

Typische Fehler vermeiden

Eine Policy ohne Schulung und technische Durchsetzung bleibt wirkungslos. Beispiel: Eine Passwort-Policy ohne MFA und ohne technische Kontrollen wird in der Praxis ignoriert.

QUIZ

Verständnisfragen: Organisation

1

Richtlinien-Inhalte

Welche sechs Inhalte muss eine IT-Sicherheitsrichtlinie mindestens abdecken, damit sie im Betrieb brauchbar ist?

2

Passwort-Details

Was gehört konkret in eine Passwort-Policy – über „länger ist besser" hinaus?

3

Durchsetzung

Wie stellen Sie sicher, dass Policies wirklich gelebt werden (Kontrollen, Schulungen, Tools)?

4

Organisation vs. Technik

Welche organisatorischen Maßnahmen senken das Risiko stärker als neue Technik – und warum?

TECHNISCHE MASSNAHMEN

Technische Schutzschichten

Technische Sicherheitsmaßnahmen bilden mehrere Verteidigungsebenen: Virenschutz und EDR erkennen Malware, Firewalls trennen Netzsegmente, E-Mail-Schutz filtert Phishing-Angriffe.

Entscheidend ist nicht nur die Installation, sondern der zentrale Betrieb mit Logging, regelmäßigen Updates und systematischer Reaktion auf Alerts.

Endpoint Protection

Virenschutz / EDR

Malware erkennen und stoppen, zentral verwalten, Alarme systematisch auswerten und auf Bedrohungen reagieren

Firewall

Netzsegmente trennen, Ports und Dienste minimieren, umfassendes Logging, VPN für sichere Fernzugriffe

E-Mail-Schutz

Phishing-Angriffe reduzieren, Anhänge und Links prüfen, DMARC/SPF/DKIM zur Absenderauthentifizierung

Wirksamkeit sicherstellen

Praxis-Check

Technische Maßnahmen entfalten ihre Wirkung erst durch systematischen Betrieb

- *Zentrale Verwaltung aller Schutzkomponenten*
- *Strukturiertes Logging und Monitoring*
- *Regelmäßige Updates und Patch-Management*
- *Definierte Prozesse zur Reaktion auf Sicherheits-Alerts*
- *Dokumentation von Konfigurationen und Änderungen*

Der Unterschied zwischen „installiert" und „wirksam" liegt im operativen Betrieb.

QUIZ

Verständnisfragen: Technik

1 Wirksamer Schutz

Was unterscheidet „Antivirus installiert" von „wirksamem Schutz im Betrieb"?

2 Firewall-Prinzipien

Welche drei Firewall-Regeln oder Prinzipien senken das Risiko am stärksten (minimale Freigaben, Segmentierung, ...)?

3 E-Mail-Bedrohungen

Welche typischen E-Mail-Angriffe fängt Anti-Spam ab – und welche Bedrohungen bleiben trotzdem übrig?

4 Erkennung

Welche Logs und Alarme benötigen Sie, um Sicherheitsvorfälle überhaupt zu bemerken?

NORMEN & STANDARDS

Strukturierter Ansatz statt Bauchgefühl

Normen und Standards bieten einen systematischen Rahmen für IT-Sicherheit. Sie helfen, Security nicht dem Zufall zu überlassen, sondern methodisch aufzubauen.

Die typische Falle: Unternehmen streben Zertifizierungen an, ohne die Prozesse wirklich zu leben – das Label allein schützt nicht.

ISO 2700x vs. BSI IT-Grundschutz

ISO 27001/27002

Management-getriebener Rahmen für ISMS (Information Security Management System)

- *Fokus auf Managementprozesse*
- *International anerkannt*
- *Flexibel, aber abstrakt*

BSI IT-Grundschutz

Praxisnahe Bausteine mit konkretem Maßnahmenkatalog

- *Fokus auf praktische Umsetzung*
- *Deutsche Behörden-Anforderung*
- *Detaillierte Anleitungen*

Strukturierter Ansatz

Standards verhindern „Security nach Bauchgefühl" und bieten nachvollziehbare Methoden zur Risikobeurteilung und Maßnahmenauswahl.

Schutzbedarf-Kategorien helfen, Prioritäten zu setzen und Ressourcen gezielt einzusetzen.

QUIZ

Verständnisfragen: Standards

1

Unterschiede

Worin unterscheiden sich ISO 2700x und BSI-Grundschutz vom Fokus her (Management vs. Maßnahmen)?

2

Nutzen im Alltag

Warum helfen Standards im Alltag, obwohl sie zunächst bürokratisch wirken?

3

Konkrete Umsetzung

Wie leiten Sie aus einem Standard eine konkrete To-do-Liste für Ihr Team ab?

4

Leere Labels

Woran erkennen Sie, dass ein Standard nur als Label genutzt wird, nicht als tatsächliche Arbeitsweise?

DATENSCHUTZ

DSGVO und BDSG

Rechtlicher Rahmen

Die DSGVO regelt EU-weit die Verarbeitung personenbezogener Daten und definiert Rechte, Pflichten sowie Nachweispflichten.

Das BDSG ergänzt als deutsches Gesetz die DSGVO mit nationalen Spezifika und Anpassungen.

Datenschutz ist ein kontinuierlicher Prozess mit umfassender Dokumentation – nicht nur das Abhaken von Checklisten.

Datenschutz in der IT-Praxis

Typische IT-Situationen

Log-Auswertungen, User-Support mit Ticketsystemen, Backup-Prozesse, Monitoring, Zugriffsprotokolle – all dies kann personenbezogene Daten enthalten.

Risiken

Wird Datenschutz nur als Rechtsthema ohne technische Umsetzung behandelt, entstehen Lücken: fehlende Verschlüsselung, ungeklärte Löschfristen, unsichere Backups.

Grundpflichten

Rechtmäßigkeit der Verarbeitung, Zweckbindung, Datenminimierung, Transparenz gegenüber Betroffenen, technische und organisatorische Maßnahmen (TOM).

Mindest-Dokumentation

Verzeichnis der Verarbeitungstätigkeiten, TOM-Dokumentation, Auftragsverarbeitungsverträge, Löschkonzepte.

QUIZ

Verständnisfragen: DSGVO-Grundlagen

1 IT-Datenverarbeitung

Welche typischen Situationen im IT-Betrieb sind „Datenverarbeitung" im DSGVO-Sinn?

2 Unternehmenspflichten

Welche drei Pflichten entstehen für Unternehmen bei personenbezogenen Daten grundsätzlich?

3 Technische Umsetzung

Welche Risiken entstehen, wenn Datenschutz nur als Rechtsthema gesehen und nicht technisch umgesetzt wird?

4 Compliance-Nachweis

Welche Dokumentation führen Sie als Minimum, um DSGVO-Compliance nachweisen zu können?

Personenbezogene Daten erkennen

Definition

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen.

Typische Beispiele

- *Offensichtlich: Name, Adresse, Telefonnummer, E-Mail*
- *Technisch: IP-Adressen, Geräte-IDs, Session-Tokens*
- *Organisatorisch: Personalnummer, Mitarbeiter-ID, Kundennummer*

Missverständnis 1

„Nur Name zählt" – falsch. Auch Kombinationen von Daten können personenbezogen sein.

Missverständnis 2

„Technische Daten sind nie personenbezogen" – falsch. IP-Adressen, Logs und Metadaten können Personen zuordenbar sein.

QUIZ

Verständnisfragen: Personenbezogene Daten

1

IT-Beispiele

Geben Sie sechs Beispiele für personenbezogene Daten aus IT-Systemen (nicht nur „Name/Adresse").

2

Log-Problematik

Warum können Logs problematisch sein (IP-Adressen, Usernames, Zeitstempel) und wie gehen Sie damit um?

3

Datensparsamkeit

Welche Daten würden Sie in Tickets und Chats vermeiden, obwohl es praktisch wäre, sie zu erfassen?

4

Datenminimierung

Wie minimieren Sie Daten, ohne den Betrieb oder den Support lahmzulegen?

Rechte der Betroffenen

Auskunftsrecht

Betroffene können Auskunft über gespeicherte Daten verlangen

Berichtigung

Falsche Daten müssen auf Anfrage korrigiert werden

Löschung

Recht auf Löschung bei fehlendem Verarbeitungsgrund

Datenübertragbarkeit

Daten müssen in strukturiertem Format bereitgestellt werden können

Einschränkung & Widerspruch

Betroffene können Verarbeitung einschränken oder widersprechen

Praktische Herausforderungen

Organisatorische Vorbereitung

Prozesse benötigen Nachweisbarkeit: Wo liegen welche Daten? Wie können sie exportiert oder gelöscht werden?

Ohne systematisches Dateninventar sind Auskunft und Löschung kaum umsetzbar, besonders wenn Daten in Schatten-IT-Systemen liegen.

Klare Workflows mit definierten Fristen verhindern, dass Anfragen untergehen oder zu spät bearbeitet werden.

QUIZ

Verständnisfragen: Betroffenenrechte

1 Schwierige Rechte

Welche drei Betroffenenrechte sind im Betrieb organisatorisch am schwierigsten umzusetzen – und warum?

2 Technische Vorbereitung

Wie bereiten Sie technisch vor, dass Auskunft und Löschung überhaupt möglich sind (Dateninventar)?

3 Workflow-Definition

Welche Fristen und Workflows definieren Sie im Team, damit Anfragen nicht untergehen?

4 Schatten-IT-Risiko

Welche Risiken entstehen, wenn Daten in nicht genehmigten Schatten-IT-Systemen landen?

SCHUTZBEDARFSANALYSE

Schutzbedarf ermitteln

Die Schutzbedarfsanalyse legt fest, wie kritisch Assets sind, um daraus passende Schutzmaßnahmen abzuleiten.

Schutzbedarf wird in drei Stufen klassifiziert: ***normal***, ***hoch***, ***sehr hoch*** *– jeweils anhand der Auswirkungen bei Sicherheitsvorfällen.*

Die Betrachtung erfolgt entlang der CIA-Dimensionen: Vertraulichkeit, Integrität und Verfügbarkeit können unterschiedlichen Schutzbedarf haben.

Schutzbedarf-Kategorien

Normal

Schaden ist begrenzt und überschaubar

- *Standardmaßnahmen ausreichend*
- *Typische Büroanwendungen*
- *Öffentliche Informationen*

Hoch

Erheblicher Schaden möglich

- *Finanzielle Verluste*
- *Rechtliche Konsequenzen*
- *Betriebsunterbrechungen*

Sehr hoch

Existenzbedrohende Folgen

- *Kritische Infrastruktur*
- *Hochsensible Daten*
- *Strenge Compliance-Vorgaben*

Wenn alles als „hoch" oder „sehr hoch" eingestuft wird, reichen die Ressourcen nicht aus – am Ende ist nichts richtig geschützt.

QUIZ

Verständnisfragen: Schutzbedarf-Grundlagen

1

Beispiele

Geben Sie je ein konkretes Beispiel, wann „normal", „hoch" und „sehr hoch" als Einstufung sinnvoll wären.

2

Abgrenzung

Welche Fragen stellen Sie, um „hoch" von „sehr hoch" sauber zu unterscheiden?

3

Stakeholder-Management

Wie gehen Sie mit Stakeholdern um, die alles maximal geschützt haben wollen?

4

Realistische Kompromisse

Welche Kompromisse sind realistisch, ohne die Security zu verraten?

Schutzbedarfsanalyse: Anwendungen

Bewertungskriterien

- *Verarbeitet die Anwendung personenbezogene Daten oder Geschäftsgeheimnisse?*
- *Welche Fehlerfolgen können entstehen (falsche Berechnungen, rechtliche Schäden)?*
- *Wie kritisch ist die Verfügbarkeit für Geschäftsprozesse?*
- *Welche Abhängigkeiten bestehen zu anderen Systemen (Auth, Datenbanken)?*
- *Welcher Rufschaden könnte bei Sicherheitsvorfällen entstehen?*

Abhängigkeiten zu Authentifizierungs-Systemen, Datenbanken oder Schnittstellen können den Schutzbedarf erhöhen, selbst wenn die Anwendung selbst klein wirkt.

QUIZ

Verständnisfragen: Anwendungen

1 Einstufungskriterien

Welche fünf Kriterien nutzen Sie, um den Schutzbedarf einer Anwendung einzustufen?

2 Integrität absichern

Wie würden Sie die Integrität einer Anwendung praktisch absichern, ohne direkt in den Code einzugreifen?

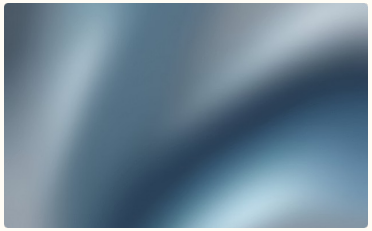
3 Abhängigkeiten

Welche Abhängigkeiten können den Schutzbedarf erhöhen, obwohl die App selbst klein wirkt?

4 Dokumentation

Welche Dokumentation muss zur Anwendung existieren, damit Security-Maßnahmen wartbar sind?

Schutzbedarfsanalyse: IT-Systeme

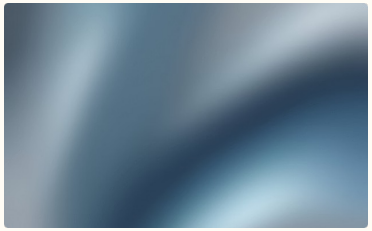


Server-Kritikalität

Welche Daten liegen auf dem System? Wie exponiert ist es im Netz? Ist es patchbar und redundant ausgelegt?

Client-Systeme

Welche Zugriffe haben Clients auf kritische Ressourcen? Sind sie mobil oder stationär?



Netzposition

Liegt das System in der DMZ, im internen Netz oder extern erreichbar?

Praxis-Maßnahmen: System-Härtung, aktueller Patch-Status, regelm. Backups, strukturierte Zugriffskontrolle, kontinuierliches Monitoring.

QUIZ

Verständnisfragen: IT-Systeme

1

Risiko-Treiber

Welche fünf System-Merkmale treiben den Schutzbedarf nach oben (Daten, Exponierung, ...)?

2

Grundschutz-Unterschiede

Welche Maßnahmen sind „Grundschutz" für Server im Vergleich zu Clients – wo liegen die Unterschiede?

3

Nachweis-Dokumentation

Wie dokumentieren Sie Patch- und Backup-Status als Nachweis für Audits?

4

Typische Schwachstellen

Welche typischen Systemschwachstellen finden Sie in der Praxis am häufigsten?

Schutzbedarfsanalyse: Räume

Physische Sicherheit

Räume mit kritischer IT-Infrastruktur benötigen besonderen Schutz – nicht nur gegen externe Bedrohungen, sondern auch gegen interne Risiken.

Typische Kriterien

- *Zutritt kontrolliert und protokolliert*
- *Schutz vor Diebstahl und unbefugtem Zugriff*
- *Brand- und Wasserschutz*
- *Klimatisierung und USV für Verfügbarkeit*
- *Sichere Lagerung von Datenträgern*

QUIZ

Verständnisfragen: Räume

1 Hoher Schutzbedarf

Warum kann ein Raum „hohen Schutzbedarf" haben, obwohl dort „nur Hardware" steht?

2 Sicherungsmaßnahmen

Welche vier technischen oder organisatorischen Maßnahmen sichern einen Serverraum sinnvoll ab?

3 Unkontrollierte Zutritte

Welche Risiken entstehen durch unkontrollierte Zutritte – auch von internen Mitarbeitenden?

4 Dokumentations-Nachweise

Welche Nachweise würden Sie für Raum-Schutzmaßnahmen dokumentieren?

Schutzbedarfsanalyse: Verbindungen

Bewertungskriterien

Internet/WAN-Verbindungen, Admin-Zugänge und VPN-Tunnel erfordern besondere Beachtung. Verschlüsselung, Segmentierung und Monitoring sind essentiell.

Praxis-Maßnahmen

- *VPN für alle Fernzugriffe*
- *TLS für Web-Anwendungen*
- *Netzsegmentierung durch Firewalls*
- *Strukturiertes Zertifikatsmanagement*
- *Kontinuierliches Monitoring kritischer Verbindungen*

QUIZ

Verständnisfragen: Verbindungen

1

Kritische Verbindungen

Welche Verbindungen sind im Betrieb besonders kritisch (Admin, Standort, Cloud) und warum?

2

Verschlüsselung prüfen

Wie prüfen Sie praktisch, ob Verbindungen wirklich verschlüsselt sind?

3

Typische Fehler

Welche drei typischen Fehler machen Verbindungen unsicher (offene Ports, schwache Protokolle, ...)?

4

Betriebsdokumentation

Was dokumentieren Sie bei Verbindungen, damit Betrieb und Audit damit arbeiten können?

BSI-GRUNDSCHUTZ-KONZEPT

Strukturiertes Sicherheitskonzept

Das BSI-Grundschutz-Konzept bietet einen praxisorientierten Ansatz zur systematischen Absicherung der IT-Infrastruktur.

Bausteine aus dem Grundschutzkatalog liefern Module mit konkreten Maßnahmen für typische IT-Komponenten.

Ein ISMS (Information Security Management System) sorgt dafür, dass Security nicht einmalig umgesetzt, sondern dauerhaft gesteuert wird.

Kernelemente des Grundschutzes

Bausteine

Grundschutzkatalog liefert standardisierte Module für Komponenten wie Server, Clients, Netze, Anwendungen und Räume

Schutzbedarf

Kategorien normal/hoch/sehr hoch steuern die Tiefe und den Umfang der erforderlichen Maßnahmen

ISMS

Managementsystem zur dauerhaften Steuerung, Überwachung und kontinuierlichen Verbesserung der Security

IT-Sicherheitsbeauftragter

Koordiniert die Umsetzung, berichtet an die Leitung und treibt Maßnahmen aktiv voran

QUIZ

Verständnisfragen: Grundschutz-Konzept

1 Baustein vs. Maßnahme

Wie erklären Sie den Unterschied zwischen „Baustein" und „Maßnahme" im Grundschutz?

2 Schutzbedarf-Wirkung

Wie hängt der Schutzbedarf mit dem Umfang der umzusetzenden Maßnahmen zusammen?

3 ISMS-Elemente

Welche vier Elemente braucht ein funktionierendes ISMS – praktisch gedacht, nicht nur theoretisch?

4 Tägliche Aufgaben

Welche Aufgaben hat ein IT-Sicherheitsbeauftragter im Alltag wirklich, über den Titel hinaus?

Umsetzung des Sicherheitskonzepts

01

Bausteine auswählen

Passende Module für die eigene Umgebung identifizieren (Organisation, Server, Clients, Netze)

02

Maßnahmen ableiten

Aus Bausteinen konkrete To-dos mit Verantwortlichen und Terminen erstellen

03

Umsetzen

Technische, infrastrukturelle, organisatorische und personelle Maßnahmen realisieren

04

Nachweisen

Dokumentation und Belege führen, um Umsetzung zu validieren

Die typische Falle: Eine Maßnahmenliste ohne Verantwortliche, Termine und Nachweise bleibt wirkungslos.

Security by Design & Default

Security by Design

Sicherheit wird von Anfang an in Systeme und Prozesse eingebaut, nicht nachträglich aufgesetzt

Security by Default

Systeme sind in der Standardkonfiguration sicher – Nutzer müssen aktiv unsichere Optionen wählen

Wesentliche Maßnahmen

- *Rechtekonzept nach Least Privilege*
- *Backup- und Wiederherstellungsstrategien*
- *Hochverfügbarkeit für kritische Systeme*
- *End-to-End-Verschlüsselung*
- *Starke Authentifizierung (MFA)*
- *Sichere Protokolle als Standard*

QUIZ

Verständnisfragen: Umsetzung

1

Effektive Maßnahmen

Welche sechs Umsetzungsmaßnahmen liefern den größten Security-Effekt im Alltag?

2

Security by Default

Was bedeutet „Security by Default" an einem konkreten Beispiel aus dem IT-Betrieb?

3

Nachweise erbringen

Welche Nachweise liefern Sie, um die Umsetzung wirklich zu belegen – nicht nur zu behaupten?

4

Priorisierung

Wie priorisieren Sie Maßnahmen, wenn Budget und Zeit knapp sind?

Sicherheitsbewusstsein fördern

Menschen als Sicherheitsfaktor

Der Mensch bleibt eine zentrale Angriffsfläche: Phishing, Social Engineering, unsichere Passwörter und USB-Sticks sind klassische Einfallstore.

Wirksame Awareness-Maßnahmen

- *Kurze, regelmäßige Schulungen statt Einmal-Events*
- *Praktische Phishing-Übungen zur Sensibilisierung*
- *Klare, niedrigschwellige Meldewege*
- *„Kein Blame"-Kultur beim Melden von Vorfällen*
- *Messung der Wirksamkeit durch Kennzahlen*

Zugangs- und Zugriffskontrolle

Zugangskontrolle

Wer darf physisch oder logisch in Gebäude, Räume oder Systeme? Authentifizierung und Identifikation stehen im Vordergrund.

Zugriffskontrolle

Was darf ein authentifizierter Nutzer im System tun? Rechte- und Rollenmodelle, Autorisierung und Berechtigungen werden geregelt.

Praxis: Least Privilege, rollenbasierte Zugriffskontrolle (RBAC), Multi-Faktor-Authentifizierung (MFA), umfassendes Logging und regelmäßige Rechte-Reviews.

Datensicherung und Wiederherstellung

Backup ist nicht gleich Wiederherstellung

Viele Unternehmen haben Backups, können aber im Ernstfall nicht wiederherstellen. Das 3-2-1-Prinzip ist Standard: 3 Kopien, 2 verschiedene Medien, 1 Kopie offline.

RPO und RTO

Recovery Point Objective (RPO) und Recovery Time Objective (RTO) definieren, wie viel Datenverlust akzeptabel ist und wie schnell Systeme wieder verfügbar sein müssen.

Restore-Tests

Backups ohne regelmäßige Restore-Tests sind nur Hoffnung. Testen Sie Wiederherstellung, Datenintegrität und benötigte Zeit.

Ransomware-Schutz

Backups müssen offline oder immutable sein, sonst können sie von Ransomware verschlüsselt werden.