

Datensicherheit - Grundlagen, Maßnahmen und Übungsaufgaben

Datensicherheit - Grundlagen, Maßnahmen und Übungsaufgaben

Datensicherheit umfasst technische, organisatorische und personelle Maßnahmen, die Daten vor Verlust, unberechtigter Veränderung und unbefugtem Zugriff schützen.

Dabei werden nicht nur personenbezogene Daten geschützt, sondern beispielsweise auch Konstruktionszeichnungen, Software, Konfigurationen und Geschäftsunterlagen.

Abgrenzung wichtiger Begriffe

Begriff	Bedeutung	Beispiel
Datensicherheit	Schutz von Daten unabhängig von ihrem Personenbezug	Eine Konstruktionsdatei wird verschlüsselt und gesichert.
Datenschutz	Schutz von Menschen beim Umgang mit ihren personenbezogenen Daten	Beschäftigtendaten dürfen nur für zulässige Zwecke verarbeitet werden.
Informationssicherheit	Schutz von Informationen in jeder Form	Auch Papierakten und vertrauliche Gespräche werden geschützt.
Datensicherung	Erstellung wiederherstellbarer Sicherungskopien	Ein Backup ermöglicht die Wiederherstellung gelöschter Dateien.

Merksatz: Datensicherung ist eine Maßnahme der Datensicherheit.

Schutzziele der Datensicherheit

Die drei zentralen Schutzziele sind Vertraulichkeit, Integrität und Verfügbarkeit. Die englischen Bezeichnungen ergeben die Abkürzung CIA: Confidentiality, Integrity und Availability.

Schutzziel	Bedeutung	Verletzung des Schutzziels	Geeignete Maßnahmen
Vertraulichkeit	Informationen sind nur für Berechtigte zugänglich.	Ein Unbefugter liest Gehaltsabrechnungen.	Verschlüsselung, Berechtigungen, MFA
Integrität	Daten bleiben korrekt und vollständig; unberechtigte Veränderungen werden verhindert oder erkannt.	Eine Kontonummer auf einer Rechnung wird manipuliert.	Änderungsrechte begrenzen, digitale Signaturen, geschützte Protokolle
Verfügbarkeit	Daten und Systeme sind bei Bedarf im vereinbarten Umfang nutzbar.	Ein Serverausfall verhindert die Auftragsbearbeitung.	Redundanz, Backups, USV, Wiederanlaufplanung

Konkrete Umsetzung

- **Vertraulichkeit:** Ein Personalordner wird ausschließlich für die Personalabteilung freigegeben.
- **Integrität:** Eine heruntergeladene Datei wird mit einem über einen vertrauenswürdigen Weg bereitgestellten Hashwert verglichen.
- **Verfügbarkeit:** Ein zweiter Server übernimmt bei Ausfall des ersten Servers.

Wichtige Unterschiede

Verschlüsselung allein stellt keine Verfügbarkeit sicher. Ein verschlüsseltes, aber defektes Speichermedium kann weiterhin unlesbar sein.

Ein einfacher Hashwert beweist nicht automatisch die Herkunft einer Datei. Kann ein Angreifer Datei und Vergleichswert ändern, reicht der Vergleich nicht aus. Für einen Herkunftsnachweis kommen beispielsweise digitale Signaturen infrage.

Eckdaten zur Verfügbarkeit

Verfügbarkeit wird häufig als Prozentwert angegeben:

Verfügbarkeit = verfügbare Zeit ÷ betrachtete Gesamtzeit × 100

Verfügbarkeit	Rechnerische Ausfallzeit pro Jahr
99 %	ca. 87,6 Stunden
99,9 %	ca. 8,76 Stunden
99,99 %	ca. 52,6 Minuten

Annahme: 365 Tage und durchgehender Betrieb. Welche Ausfälle und Wartungszeiten tatsächlich mitzählen, hängt von der vereinbarten Messweise ab.

Übungsaufgabe

Ordne die folgenden Fälle den Schutzzielen zu:

1. Kundendaten werden öffentlich zugänglich.
2. Ein Angreifer verändert Bestellmengen.
3. Das Warenwirtschaftssystem ist zwei Stunden nicht erreichbar.

Lösung anzeigen

1. Vertraulichkeit.
2. Integrität.
3. Verfügbarkeit.

Ein Vorfall kann mehrere Schutzziele gleichzeitig betreffen.

Technische und organisatorische Maßnahmen (TOMs)

TOMs setzen Sicherheitsziele praktisch um.

- **Technische Maßnahmen:** beispielsweise Verschlüsselung, Firewall und automatische Datensicherung.
- **Organisatorische Maßnahmen:** beispielsweise Zuständigkeiten, Freigabeprozesse und Schulungen.

Maßnahme	Zweck	Beispiel und Umsetzung
Zutrittskontrolle	Unberechtigte Personen aus Gebäuden oder Räumen fernhalten	Serverraum abschließen, persönliche Schlüsselkarten vergeben, Besucher begleiten
Zugangskontrolle	Unberechtigte Nutzung eines Systems verhindern	Persönliche Benutzerkonten, MFA und automatische Bildschirmsperre einsetzen
Zugriffskontrolle	Erlaubte Aktionen auf bestimmte Daten beschränken	Einer Gruppe Leserechte geben, Schreib- und Löschrechte nur zuständigen Personen erlauben
Weitergabekontrolle	Übertragung und Weitergabe von Daten absichern	TLS verwenden, Empfänger prüfen und Freigabelinks zeitlich begrenzen
Eingabekontrolle	Eingaben, Änderungen und Löschungen nachvollziehbar machen	Benutzer, Zeitpunkt und Aktion in geschützten Protokollen erfassen
Auftragskontrolle	Verarbeitung entsprechend festgelegten Vorgaben sicherstellen	Aufgaben und zulässige Verarbeitung eines Dienstleisters festlegen und kontrollieren
Verfügbarkeitskontrolle	Daten und Dienste gegen Ausfall und Verlust absichern	Backups, Ersatzsysteme und Wiederherstellungstests einrichten
Trennung von Daten	Unterschiedliche Zwecke oder Mandanten voneinander abgrenzen	Getrennte Datenbanken, Mandantenbereiche und Berechtigungen verwenden

Zutritt, Zugang und Zugriff unterscheiden

Frage	Zugehörige Kontrolle
Darf die Person den Serverraum betreten?	Zutrittskontrolle
Darf sie sich am Server anmelden?	Zugangskontrolle
Darf sie die Personaldatei öffnen oder verändern?	Zugriffskontrolle

Merksatz: Zutritt zum Raum – Zugang zum System – Zugriff auf Daten.

Beispiel für das Zusammenspiel

Ein Administrator darf den Serverraum betreten und sich an einem Wartungssystem anmelden. Daraus folgt nicht automatisch, dass er sämtliche fachlichen Daten lesen dürfen soll. Berechtigungen müssen passend zur Aufgabe gestaltet werden.

Übungsaufgabe

Ordne die Maßnahmen zu:

1. Anmeldung mit Passwort und Sicherheitsschlüssel.
2. Zugang zum Rechenzentrum über eine Schlüsselkarte.
3. Eine Mitarbeiterin darf Rechnungen lesen, aber nicht löschen.
4. Änderungen an Kundenadressen werden protokolliert.
5. Produktivdaten und Testdaten werden getrennt gespeichert.

Lösung anzeigen

1. Zugangskontrolle.
2. Zutrittskontrolle.
3. Zugriffskontrolle.
4. Eingabekontrolle.
5. Trennung von Daten.

Bedrohungsszenarien und Gegenmaßnahmen

SQL-Injection

Bei SQL-Injection beeinflussen manipulierte Eingaben eine Datenbankabfrage. Das kann passieren, wenn eine Anwendung Eingaben unmittelbar mit SQL-Befehlstext zusammensetzt.

Beispiel: Ein Suchfeld verarbeitet eine Eingabe als Bestandteil der SQL-Syntax statt ausschließlich als Suchwert.

Gegenmaßnahmen und Umsetzung

- Prepared Statements beziehungsweise parametrisierte Abfragen verwenden.
- Benutzereingaben getrennt von der SQL-Befehlsstruktur übergeben.
- Datentypen, Wertebereiche und zulässige Auswahlwerte prüfen.
- Dem Datenbankkonto der Anwendung nur erforderliche Rechte geben.

Unterschied: Eingabevalidierung prüft, ob ein Wert zulässig ist. Parametrisierung verhindert, dass ein übergebener Wert die vorgesehene SQL-Struktur verändert. Validierung ersetzt keine Parametrisierung.

Cross-Site Scripting (XSS)

Bei XSS werden fremde Inhalte so in eine Webseite eingebunden, dass der Browser sie als ausführbaren Code verarbeitet.

Beispiel: Ein Kommentar wird ungeprüft als HTML ausgegeben und führt unerwünschte Aktionen im Browser anderer Besucher aus.

Gegenmaßnahmen und Umsetzung

- Ausgaben passend zum jeweiligen Kontext kodieren.
- Sichere Ausgabefunktionen des verwendeten Frameworks nutzen.
- Falls HTML ausdrücklich erlaubt sein soll, eine geeignete HTML-Bereinigung verwenden.
- Unsichere direkte HTML-Einfügungen vermeiden.
- Eine Content Security Policy als zusätzliche Schutzschicht einsetzen.

Unterschied zu SQL-Injection: SQL-Injection betrifft Datenbankabfragen. XSS betrifft die Verarbeitung von Inhalten im Browser.

Phishing

Phishing täuscht eine vertrauenswürdige Nachricht, Person oder Website vor, um beispielsweise Zugangsdaten zu erlangen.

Beispiel: Eine E-Mail behauptet, das Firmenkonto werde gesperrt. Der enthaltene Link führt zu einer gefälschten Anmeldung.

Gegenmaßnahmen und Umsetzung

- Anmeldeseiten über bekannte Adressen oder gespeicherte Lesezeichen aufrufen.
- Absender, Zieladresse und ungewöhnliche Aufforderungen prüfen.
- Verdächtige Nachrichten über einen festgelegten Meldeweg melden.
- Spamfilter und Schulungen einsetzen.
- MFA aktivieren; möglichst phishingresistente Verfahren wie FIDO2-Sicherheitsschlüssel nutzen.

Wichtig: Ein HTTPS-Schloss beweist nicht, dass eine Website seriös ist. Auch eine Phishing-Seite kann eine verschlüsselte Verbindung anbieten.

Malware

Malware ist der Oberbegriff für Schadsoftware.

Art	Kennzeichen	Beispiel
Virus	Verbreitet sich durch Infektion anderer Dateien oder Programme	Eine infizierte Programmdatei verändert weitere Dateien.
Trojaner	Tarnt sich als legitime oder nützliche Software	Ein angebliches Hilfsprogramm installiert eine Hintertür.
Ransomware	Sperrt oder verschlüsselt Daten zur Erpressung; häufig zusätzlich Datendiebstahl	Projektdateien werden unbrauchbar und ein Lösegeld wird verlangt.

Diese Kategorien können sich überschneiden.

Gegenmaßnahmen und Umsetzung

- Betriebssystem und Anwendungen aktuell halten.
- Virenschutz beziehungsweise geeigneten Endgeräteschutz einsetzen.
- Im Alltag ohne Administratorrechte arbeiten.
- Software aus vertrauenswürdigen Quellen beziehen.
- Makros und ausführbare Anhänge kontrollieren.
- Getrennte oder unveränderbare Backups vorhalten und Wiederherstellungen testen.

Brute-Force

Bei Brute-Force werden viele mögliche Passwörter automatisiert ausprobiert.

Beispiel: Ein Angreifer versucht wiederholt verschiedene Kennwörter an einer Anmeldung.

Gegenmaßnahmen und Umsetzung

- Lange, einzigartige Passwörter und einen Passwortmanager verwenden.
- Anmeldeversuche begrenzen oder verzögern.
- MFA einsetzen.
- Auffällige Fehlversuche überwachen.
- Kontosperrern sorgfältig gestalten, damit Angreifer nicht gezielt alle Benutzer aussperren können.

Abgrenzung: Beim Credential Stuffing werden bereits gestohlene Zugangsdaten anderer Dienste ausprobiert. Einzigartige Passwörter begrenzen dieses Risiko.

Man-in-the-Middle

Ein Angreifer befindet sich zwischen Kommunikationspartnern und versucht, Daten mitzulesen oder zu verändern.

Beispiel: In einem manipulierten Netzwerk wird eine ungeschützte Verbindung abgefangen.

Gegenmaßnahmen und Umsetzung

- HTTPS beziehungsweise TLS mit korrekter Zertifikatsprüfung verwenden.
- Zertifikatswarnungen nicht ignorieren.
- Für administrative Verbindungen sichere Protokolle wie SSH einsetzen.
- Bei Bedarf einen vertrauenswürdigen VPN-Zugang nutzen.

Unterschied: Verschlüsselung schützt den Inhalt. Die Authentisierung des Kommunikationspartners hilft sicherzustellen, dass mit dem richtigen Gegenüber kommuniziert wird.

Social Engineering

Social Engineering manipuliert Menschen, damit sie Sicherheitsregeln umgehen.

Beispiel: Ein angeblicher Vorgesetzter verlangt unter Zeitdruck die Herausgabe eines Einmalcodes.

Gegenmaßnahmen und Umsetzung

- Anfragen über bekannte, unabhängige Kontaktwege überprüfen.
- Keine Passwörter oder Anmeldecodes weitergeben.
- Klare Freigabeverfahren festlegen.
- Beschäftigte anhand realistischer Situationen schulen.

Abgrenzung: Phishing ist eine Form von Social Engineering. Social Engineering kann auch telefonisch oder persönlich stattfinden.

Datenverlust

Datenverlust entsteht beispielsweise durch Defekte, Bedienfehler, Angriffe oder Schäden am Standort.

Beispiel: Ein Mitarbeiter löscht versehentlich einen Projektordner.

Gegenmaßnahmen und Umsetzung

- Regelmäßige, versionierte Backups erstellen.
- Sicherungskopien räumlich und technisch trennen.
- Wiederherstellungen testen.
- Redundanz gegen bestimmte Hardwareausfälle einsetzen.

Wichtig: RAID und Cloud-Synchronisation ersetzen nicht automatisch ein Backup.

DDoS

Distributed Denial of Service bedeutet, dass viele verteilte Quellen einen Dienst oder seine Anbindung überlasten.

Beispiel: Ein Onlineshop ist durch massenhafte Anfragen nicht mehr erreichbar.

Gegenmaßnahmen und Umsetzung

- DDoS-Schutz beim Provider oder einem vorgeschalteten Dienst nutzen.
- Angriffsverkehr möglichst vor der eigenen Anbindung filtern.
- Anfragen angemessen begrenzen.
- Lastverteilung und ausreichende Kapazität einplanen.
- Einen abgestimmten Notfallablauf vorbereiten.

Unterschied: Load Balancing verteilt Last. Es kann eine bereits überlastete Internetanbindung allein nicht entlasten.

Übungsaufgaben zu den Bedrohungen

Ordne jedem Fall eine Bedrohung und eine passende Gegenmaßnahme zu:

1. Ein Suchfeld verändert unbeabsichtigt die Struktur einer Datenbankabfrage.
2. Ein Kommentar führt Code im Browser anderer Benutzer aus.
3. Eine gefälschte Kontowarnung fordert zur Anmeldung auf.
4. Ein angebliches Gratisprogramm verschlüsselt Dateien.
5. Eine Anmeldung erhält Tausende Passwortversuche.
6. Eine unverschlüsselte Verbindung wird mitgelesen.
7. Ein angeblicher Supportmitarbeiter verlangt telefonisch einen Anmeldecode.
8. Ein Projektordner wird versehentlich gelöscht.
9. Viele verteilte Systeme überlasten einen Webdienst.

Lösungen anzeigen

1. SQL-Injection → parametrisierte Abfragen.
2. XSS → kontextgerechte Ausgabekodierung.
3. Phishing → bekannte Anmeldewege nutzen, MFA und Schulungen.
4. Malware; hier Trojaner-Verteilung und Ransomware-Wirkung → vertrauenswürdige Softwarequellen, Endgeräteschutz und geschützte Backups.
5. Brute-Force → Rate-Limiting, starke Passwörter und MFA.
6. Man-in-the-Middle beziehungsweise Abhören → TLS mit Zertifikatsprüfung.
7. Social Engineering → unabhängige Identitätsprüfung, keine Codes weitergeben.
8. Datenverlust → Wiederherstellung aus einem geeigneten Backup.

Authentifizierung und Autorisierung

Begriff	Leitfrage	Beispiel
Authentifizierung	Wer bist du?	Ein Benutzer weist seine Identität durch ein Anmeldeverfahren nach.
Autorisierung	Was darfst du?	Das System prüft, ob dieser Benutzer einen bestimmten Datensatz ändern darf.

Ein Benutzername benennt zunächst eine Identität. Erst die Prüfung eines geeigneten Nachweises authentifiziert sie.

Praktische Umsetzung

1. Benutzer meldet sich mit seinem persönlichen Konto an.
2. Das System prüft die erforderlichen Authentifizierungsnachweise.
3. Bei einer angeforderten Aktion werden die passenden Berechtigungen geprüft.
4. Nicht erlaubte Aktionen werden abgewiesen.

Übungsaufgabe

Eine Mitarbeiterin kann sich anmelden, erhält beim Öffnen eines Personalordners aber „Zugriff verweigert“. Welche Prüfung war erfolgreich, welche Berechtigung fehlt?

Lösung anzeigen

Die Authentifizierung war erfolgreich. Die Autorisierung für den Personalordner fehlt. Ein erfolgreicher Login erlaubt nicht automatisch den Zugriff auf alle Ressourcen.

Authentifizierungsfaktoren

Faktor	Bedeutung	Beispiele	Mögliche Schwäche
Wissen	Etwas, das man kennt	Passwort, PIN	Kann erraten, ausgespäht oder weitergegeben werden.
Besitz	Etwas, das man besitzt	Sicherheitsschlüssel, Chipkarte, registriertes Smartphone	Kann verloren gehen oder gestohlen werden.

Faktor	Bedeutung	Beispiele	Mögliche Schwäche
Sein	Ein körperliches Merkmal	Fingerabdruck, Gesichtserkennung	Erkennung ist nicht fehlerfrei; Merkmale lassen sich nicht einfach austauschen.

Mehrfaktor-Authentifizierung

MFA kombiniert mindestens zwei unabhängige Faktoren unterschiedlicher Kategorien.

- Passwort und Sicherheitsschlüssel: Wissen und Besitz.
- Chipkarte und PIN: Besitz und Wissen.
- Zwei Passwörter: zweimal Wissen, deshalb keine echte Zwei-Faktor-Authentifizierung.

Ein Smartphone zählt nicht allein deshalb als Faktor, weil es vorhanden ist. Das Verfahren muss den Besitz beispielsweise über einen registrierten Schlüssel oder eine Authenticator-App nachweisen.

Praktische Umsetzung

- MFA für wichtige Konten und administrative Zugänge aktivieren.
- Wiederherstellungsverfahren und Ersatzfaktoren planen.
- Wiederherstellungscodes geschützt aufbewahren.
- Anmeldebestätigungen nur für selbst gestartete Vorgänge freigeben.

Übungsaufgabe

Welche Kombinationen nutzen unterschiedliche Faktoren?

1. Passwort und Sicherheitsfrage.
2. Chipkarte und PIN.
3. Passwort und Code einer registrierten Authenticator-App.

Lösung anzeigen

1. Nein: beide Nachweise gehören zu Wissen.
2. Ja: Besitz und Wissen.
3. Ja: Wissen und Besitz, sofern das Verfahren entsprechend unabhängig und sicher umgesetzt ist.

Autorisierung

Autorisierung legt fest, welche Aktionen ein Benutzer auf welchen Ressourcen ausführen darf.

Modell	Funktionsweise	Beispiel	Besonderheit
RBAC	Rechte werden über Rollen vergeben.	Die Rolle „Buchhaltung“ darf Rechnungen bearbeiten.	Gut für stabile Zuständigkeiten.
ABAC	Regeln werten Eigenschaften von Benutzer, Ressource und Umgebung aus.	Zugriff nur für die zuständige Abteilung von einem verwalteten Gerät.	Flexibel, aber aufwendiger zu gestalten und zu prüfen.
ACL	Eine Liste an einer Ressource enthält Berechtigungen für Benutzer oder Gruppen.	Gruppe „Projekt A“ darf einen Ordner lesen und ändern.	Konkrete Rechte direkt am Objekt.

RBAC, ABAC und ACL sind nicht immer Alternativen. Ein System kann Rollen über Gruppen abbilden und diese Gruppen in ACLs eintragen.

Praktische Umsetzung

- Rollen anhand tatsächlicher Aufgaben definieren.
- Standardmäßig keinen Zugriff gewähren.
- Berechtigungen serverseitig für jede relevante Aktion prüfen.
- Gruppen statt zahlreicher individueller Ausnahmen verwenden.
- Rechtevergabe und Änderungen dokumentieren.

Übungsaufgabe

Ordne zu:

1. Zugriff abhängig von Abteilung, Gerät und Schutzklasse.
2. Zugriff entsprechend der Rolle „Einkauf“.
3. Eine Ordnerliste erlaubt einer Gruppe Lesen und Schreiben.

Lösung anzeigen

1. ABAC.
2. RBAC.
3. ACL.

Wichtige Prinzipien der Rechtevergabe

Prinzip	Bedeutung	Umsetzung
---------	-----------	-----------

Least Privilege	Nur notwendige Rechte vergeben	Für das Lesen eines Berichts keine Änderungs- oder Administratorrechte vergeben.
Need-to-know	Informationen nur bei fachlichem Bedarf zugänglich machen	Beschäftigte sehen nur die für ihre Arbeit benötigten Kundendaten.
Trennung von Aufgaben	Kritische Schritte auf mehrere Personen verteilen	Eine Person legt eine Zahlung an, eine andere genehmigt sie.
Regelmäßige Rechteprüfung	Überflüssige Berechtigungen erkennen und entziehen	Rechte bei Abteilungswechsel, Projektende und Austritt überprüfen.

Unterschied zwischen Least Privilege und Need-to-know

Least Privilege betrifft den Umfang erlaubter Aktionen. Need-to-know betrifft den erforderlichen Zugang zu Informationen.

Übungsaufgabe

Ein Mitarbeiter wechselt vom Vertrieb in den Einkauf. Seine bisherigen Kundenexportrechte bleiben bestehen. Was ist zu tun?

Lösung anzeigen

Die Rechte anhand der neuen Aufgaben prüfen, nicht mehr benötigte Vertriebsrechte entfernen und nur erforderliche Einkaufsrechte vergeben. Der Wechsel muss einen geregelten Berechtigungsprozess auslösen.

IT-Grundschutz des BSI

Der IT-Grundschutz bietet eine systematische Vorgehensweise, um Informationssicherheit aufzubauen und zu verbessern.

Typisches Vorgehen

1. Geschäftsprozesse, Informationen und Systeme erfassen.
2. Schutzbedarf bestimmen.
3. Passende Anforderungen und Maßnahmen auswählen.
4. Den vorhandenen Sicherheitsstand überprüfen.
5. Lücken schließen und bei Bedarf Risiken vertieft analysieren.
6. Umsetzung und Wirksamkeit regelmäßig überprüfen.

Beispiel

Für einen Dateiserver werden Datenbestände, Zugriffsrechte, Sicherungen, Stromversorgung und Verantwortlichkeiten untersucht. Fehlende Restore-Tests werden als Lücke erkannt und verbindlich

eingepplant.

Wichtige Eckdaten

BSI-Standard	Schwerpunkt
200-1	Managementsysteme für Informationssicherheit
200-2	IT-Grundschutz-Methodik
200-3	Risikoanalyse auf Basis von IT-Grundschutz

Vorgehensweisen unterscheiden

- **Basis-Absicherung:** Einstieg mit grundlegender Absicherung in der Breite.
- **Kern-Absicherung:** Schwerpunkt auf besonders wichtigen Geschäftsprozessen und Werten.
- **Standard-Absicherung:** umfassende Anwendung der IT-Grundschutz-Methodik.

Übungsaufgabe

Ein Unternehmen kauft eine Firewall und erklärt anschließend seine Informationssicherheit für abgeschlossen. Was fehlt?

Lösung anzeigen

Es fehlen unter anderem eine systematische Bestandsaufnahme, die Schutzbedarfsbetrachtung, organisatorische Zuständigkeiten, weitere passende Maßnahmen und eine regelmäßige Wirksamkeitsprüfung. Ein einzelnes Produkt ersetzt kein Sicherheitsmanagement.

Zertifizierungen und ISMS

Ein ISMS ist ein Informationssicherheitsmanagementsystem. Es organisiert, wie Informationssicherheit geplant, umgesetzt, kontrolliert und verbessert wird.

ISO/IEC 27001 legt Anforderungen an ein solches Managementsystem fest.

Begriff	Bedeutung
ISMS	Das tatsächlich betriebene Managementsystem der Organisation
ISO/IEC 27001	Norm mit Anforderungen an ein ISMS
Zertifizierung	Unabhängige Prüfung der Normerfüllung innerhalb eines festgelegten Geltungsbereichs

Typische Bestandteile eines ISMS

- Sicherheitsziele und Leitlinien.
- Verantwortlichkeiten.
- Risikobeurteilung und Behandlung von Risiken.
- Geregelte Sicherheitsmaßnahmen.
- Schulungen und dokumentierte Abläufe.
- Interne Überprüfungen und Managementbewertung.
- Kontinuierliche Verbesserung.

Beispiel für kontinuierliche Verbesserung

Planen: Unberechtigte Kontonutzung reduzieren.

Umsetzen: MFA einführen und Benutzer schulen.

Prüfen: Abdeckung und Vorfälle auswerten.

Verbessern: Ausnahmen beseitigen und den Wiederherstellungsprozess nachbessern.

Wichtige Unterschiede

Ein ISMS kann auch ohne Zertifizierung betrieben werden. Eine Zertifizierung garantiert keine absolute Sicherheit und gilt nicht automatisch für alle Standorte, Produkte oder Dienstleistungen eines Unternehmens.

Übungsaufgabe

Ein Dienstleister wirbt mit einer ISO-27001-Zertifizierung. Warum muss der Geltungsbereich geprüft werden?

Lösung anzeigen

Weil die tatsächlich genutzte Dienstleistung oder der betreffende Standort außerhalb des zertifizierten Bereichs liegen könnte. Entscheidend ist, welche Organisationseinheiten, Prozesse und Leistungen das Zertifikat umfasst.

Härtung eines Betriebssystems

Härtung reduziert die Angriffsfläche eines Systems durch eine gezielte sichere Konfiguration.

Wichtige Maßnahmen

Maßnahme	Konkrete Umsetzung	Zweck
----------	--------------------	-------

Nicht benötigte Dienste deaktivieren	Einen ungenutzten Web- oder Dateifreigabedienst abschalten	Weniger erreichbare Angriffspunkte
Updates und Patch-Management	Sicherheitsupdates bewerten, testen, verteilen und Installation kontrollieren	Bekannte Schwachstellen schließen
Benutzerrechte einschränken	Standardkonto für den Alltag, separates Administratorkonto	Auswirkungen von Fehlern und Angriffen begrenzen
MFA einsetzen	Administrative und externe Zugänge zusätzlich absichern	Gestohlene Passwörter allein reichen nicht aus
Firewall konfigurieren	Nur erforderliche Verbindungen von zulässigen Quellen erlauben	Unerwünschte Netzwerkzugriffe begrenzen
Daten verschlüsseln	Laufwerksverschlüsselung aktivieren und Wiederherstellungsschlüssel geschützt verwahren	Daten bei Verlust eines Geräts schützen
Unnötige Schnittstellen deaktivieren	Nicht benötigtes Bluetooth oder nicht erforderliche externe Speicherschnittstellen beschränken	Zusätzliche Angriffswege reduzieren
Protokollierung und Monitoring	Sicherheitsereignisse zentral erfassen und relevante Alarme bearbeiten	Auffälligkeiten erkennen und untersuchen
Sicherheitsrichtlinien durchsetzen	Konfigurationen zentral verteilen und Abweichungen prüfen	Einheitlichen Sicherheitsstand erhalten

Wichtige Unterschiede

- Eine Firewall behebt keine Schwachstelle in einer erlaubten Anwendung.
- Verschlüsselung schützt nicht automatisch vor einem Angreifer, der bereits im entsperreten Benutzerkonto arbeitet.
- Protokollierung sammelt Ereignisse. Monitoring wertet sie aus und macht Auffälligkeiten erkennbar.
- Härtung ist eine laufende Aufgabe, weil Software und Anforderungen sich ändern.

Übungsaufgabe

Ein Bürorechner besitzt veraltete Software, einen unnötigen Fernzugriffsdienst und ein dauerhaft verwendetes Administratorkonto. Nenne drei Verbesserungen.

Lösung anzeigen

Software aktualisieren, den nicht benötigten Fernzugriffsdienst deaktivieren und ein Standardkonto für die tägliche Arbeit verwenden. Administrative Tätigkeiten erfolgen über einen getrennten, passend abgesicherten Zugang.

Datensicherung

Datensicherung, auch Backup genannt, erstellt zusätzliche Datenbestände, aus denen benötigte Informationen wiederhergestellt werden können.

Beispiel: Nach versehentlichem Löschen einer Projektdatei wird deren vorheriger Stand aus einer Sicherung zurückgespielt.

Ein Backup ist erst praktisch nützlich, wenn die Wiederherstellung funktioniert.

Übungsaufgabe

Ein Sicherungsprogramm meldet erfolgreiche Läufe. Wiederherstellungen wurden nie getestet. Ist die Wiederherstellbarkeit ausreichend nachgewiesen?

Lösung anzeigen

Nein. Ein erfolgreicher Sicherungslauf beweist nicht, dass sämtliche benötigten Daten vollständig, konsistent und rechtzeitig wiederhergestellt werden können. Dafür sind Restore-Tests erforderlich.

Ziele der Datensicherung

- Daten nach Verlust oder Beschädigung wiederherstellen.
- Frühere Datenstände verfügbar halten.
- Betriebsunterbrechungen begrenzen.
- Wiederanlauf nach einem Vorfall ermöglichen.

Wichtige Eckdaten

Kennzahl	Bedeutung	Beispiel
RPO – Recovery Point Objective	Maximal tolerierbarer Datenverlust, als Zeitspanne ausgedrückt	Höchstens eine Stunde an Änderungen darf verloren gehen.
RTO – Recovery Time Objective	Angestrebte maximal tolerierbare Zeit bis zur Wiederherstellung	Ein Dienst soll innerhalb von vier Stunden wieder nutzbar sein.

Unterschied: RPO fragt, wie viele neue Daten verloren gehen dürfen. RTO fragt, wie lange die Wiederherstellung dauern darf.

Übungsaufgabe

Ein System wird nur jede Nacht gesichert. Die Fachabteilung verlangt maximal eine Stunde Datenverlust. Passt das zusammen?

Lösung anzeigen

Nein. Eine ausschließlich tägliche Sicherung kann kurz vor dem nächsten Lauf fast einen Tag an Änderungen verlieren. Es ist ein häufigeres oder ergänzendes Sicherungsverfahren nötig, dessen tatsächlich erreichbare Wiederherstellungspunkte das RPO erfüllen.

Ursachen für Datenverlust

Ursache	Beispiel	Vorbeugung und Begrenzung
Stromausfall	Ein Schreibvorgang wird unterbrochen.	USV, kontrolliertes Herunterfahren und Backups
Hardwarefehler	Eine Festplatte fällt aus.	Geeignete Redundanz, Überwachung und Ersatzhardware
Menschliches Versagen	Ein Ordner wird gelöscht oder überschrieben.	Begrenzte Rechte, Versionierung und Backups
Böswilliger Angriff	Ransomware verschlüsselt Daten.	Härtung, MFA, Endgeräteschutz und getrennte Sicherungen
Standortschaden	Brand zerstört Server und lokale Sicherungen.	Räumlich getrennte Sicherungskopien

Übungsaufgabe

Warum ist eine Sicherung auf einer zweiten Festplatte im gleichen Rechner allein unzureichend?

Lösung anzeigen

Beide Datenträger können durch denselben Angriff, Diebstahl, Brand oder elektrischen Schaden betroffen sein. Die zusätzliche Kopie deckt deshalb nicht alle relevanten Ausfallursachen ab.

Anforderungen an Datensicherung

Ein Sicherungskonzept legt fest:

- Welche Daten und Systeme gesichert werden.
- Wer verantwortlich ist.
- Wie häufig gesichert wird.
- Welche Verfahren und Medien verwendet werden.
- Wie lange Sicherungen aufbewahrt werden.
- Wie Sicherungen gegen unberechtigten Zugriff geschützt werden.
- Wo zusätzliche Kopien lagern.
- Wie Fehler erkannt und bearbeitet werden.

- Wie Wiederherstellungen durchgeführt und getestet werden.

Planungsdaten

Kriterium	Leitfrage
Datenmenge	Wie groß ist der Bestand, und wie schnell wächst er?
Änderungsmenge	Wie viele Daten ändern sich zwischen Sicherungsläufen?
Sicherungsfenster	Wie viel Zeit steht für einen Lauf zur Verfügung?
Übertragungsrate	Wie schnell können Quelle, Netzwerk und Ziel tatsächlich arbeiten?
Kosten	Welche Ausgaben entstehen für Speicher, Lizenzen, Betrieb und Wiederherstellung?
RPO und RTO	Welche Datenverluste und Unterbrechungen sind tolerierbar?
Aufbewahrung	Welche Wiederherstellungspunkte werden wie lange benötigt?

Übungsaufgabe

500 GB sollen mit effektiv 100 MB/s gesichert werden. Wie lange dauert die reine Datenübertragung ungefähr?

Lösung anzeigen

Bei dezimalen Einheiten: 500 GB = 500.000 MB.

$500.000 \text{ MB} \div 100 \text{ MB/s} = 5.000 \text{ Sekunden} = 83 \text{ Minuten und } 20 \text{ Sekunden.}$

Zusätzliche Zeit für Vorbereitung, Metadaten, Prüfung oder langsamere Einzeldateizugriffe ist dabei nicht enthalten.

Backup-Medien

Medium	Vorteile	Grenzen	Geeigneter Einsatz
Magnetband	Gut offline lagerbar; bei großen Beständen wirtschaftlich möglich	Bandlaufwerk erforderlich; sequenzieller Zugriff	Große Sicherungsbestände und längerfristige Aufbewahrung
Externe HDD	Viel Kapazität zu vergleichsweise niedrigen Kosten	Mechanisch empfindlich; angeschlossen für Angriffe erreichbar	Rotierende lokale Sicherungsmedien

Medium	Vorteile	Grenzen	Geeigneter Einsatz
Externe SSD	Schneller Zugriff, keine beweglichen Teile	Meist teurer pro Speichereinheit	Mobile oder schnelle Sicherungs- und Wiederherstellungsaufgaben
Cloud-Speicher	Räumliche Trennung und skalierbarer Speicher möglich	Abhängigkeit von Netzwerk, Anbieter, Kosten und Kontosicherheit	Externe Sicherungskopie mit passendem Backup-Verfahren

Praktische Umsetzung

- Externe Medien nach dem Sicherungslauf sicher trennen, sofern das Konzept Offline-Kopien vorsieht.
- Medien beschriften und Aufbewahrung dokumentieren.
- Sicherungen verschlüsseln und benötigte Schlüssel getrennt absichern.
- Cloud-Zugriffe mit geeigneten Berechtigungen und MFA schützen.
- Wiederherstellung auch aus extern gelagerten Kopien testen.

Wichtig: Cloud-Speicher ist zunächst nur ein Speicherort. Ob daraus ein geeignetes Backup wird, hängt unter anderem von Versionierung, Aufbewahrung, Unveränderbarkeit und Wiederherstellbarkeit ab.

Übungsaufgabe

Ein Unternehmen besitzt eine schnelle lokale Sicherung, möchte aber auch gegen einen Brand am Standort geschützt sein. Welche Ergänzung ist sinnvoll?

Lösung anzeigen

Eine räumlich getrennte Kopie, beispielsweise in einem geeigneten Cloud-Backup oder auf extern gelagerten Sicherungsmedien. Zusätzlich müssen Zugriffsschutz, Aufbewahrung und Wiederherstellung geprüft werden.

Backup-Arten

Verfahren	Gesicherte Daten	Typischer Sicherungsaufwand	Klassische Wiederherstellung
Vollsicherung	Alle ausgewählten Daten	Vergleichsweise hoch	Gewünschte Vollsicherung
Inkrementelle Sicherung	Änderungen seit der letzten Sicherung der Kette	Meist gering je Lauf	Vollsicherung und sämtliche benötigten Inkremente
Differenzielle Sicherung	Änderungen seit der letzten Vollsicherung	Wächst bis zur nächsten Vollsicherung meist an	Vollsicherung und gewünschte Differenzsicherung

Die Angaben beschreiben klassische Verfahren. Moderne Sicherungsprodukte können intern zusätzliche Techniken verwenden.

Beispiel

Am Sonntag erfolgt eine Vollsicherung. Montag, Dienstag und Mittwoch werden Änderungssicherungen erstellt.

- **Inkrementell:** Mittwoch enthält nur Änderungen seit Dienstag.
- **Differenziell:** Mittwoch enthält alle Änderungen seit Sonntag.

Übungsaufgabe

Welche Sicherungen werden für den Stand Mittwochabend benötigt?

Lösung anzeigen

Inkrementell: Vollsicherung vom Sonntag sowie die Inkremente von Montag, Dienstag und Mittwoch.

Differenziell: Vollsicherung vom Sonntag und Differenzsicherung vom Mittwoch.

Rechenaufgabe

Ein Vollbackup umfasst 100 GB. Danach kommen täglich 10 GB neue, unterschiedliche Daten hinzu. Wie viel wird Montag bis Mittwoch zusätzlich gesichert?

Annahme: keine Kompression, Deduplizierung oder Löschung.

Lösung anzeigen

Inkrementell: $10 + 10 + 10 = 30$ GB.

Differenziell: $10 + 20 + 30 = 60$ GB.

Mit dem Vollbackup ergeben sich 130 GB beziehungsweise 160 GB.

Backup-Prinzipien

Großvater-Vater-Sohn-Prinzip

Dieses Rotationsschema kombiniert mehrere zeitliche Aufbewahrungsstufen.

Stufe	Typisches Beispiel
Sohn	Tägliche Sicherungen
Vater	Wöchentliche Sicherungen
Großvater	Monatliche Sicherungen

Die genaue Anzahl und Aufbewahrungsdauer legt das Unternehmen fest.

Beispiel: Tägliche Sicherungen werden für kurzfristige Fehler benötigt, Monatsstände für ältere Wiederherstellungspunkte.

3-2-1-Regel

- **3** Kopien der Daten insgesamt, einschließlich der produktiven Daten.
- **2** unterschiedliche Medientypen.
- **1** Kopie außerhalb des Hauptstandorts.

Beispiel: Produktivdaten auf SSD, lokale Sicherung auf HDD und eine weitere Kopie auf extern gelagertem Band.

Offline oder unveränderbar aufbewahrte Kopien ergänzen den Schutz gegen Ransomware.

Hot Backup und Cold Backup

Verfahren	Bedeutung	Vorteil	Herausforderung
Hot Backup	Sicherung während des laufenden Betriebs	Dienst kann weiter genutzt werden.	Ein konsistenter Datenstand muss durch das Verfahren sichergestellt werden.
Cold Backup	Anwendung oder Datenbank ist angehalten.	Konsistenz ist leichter sicherzustellen.	Geplante Unterbrechung erforderlich.

Unterschied der Prinzipien

Großvater-Vater-Sohn regelt die zeitlichen Aufbewahrungsstufen. Die 3-2-1-Regel betrifft Anzahl, Medien und Standort der Kopien. Hot und Cold beschreiben den Betriebszustand während der Sicherung.

Übungsaufgaben

1. Wofür ist ein älterer Monatsstand nützlich?
2. Erfüllen drei Kopien auf derselben Festplatte die 3-2-1-Regel?
3. Eine Datenbank muss während der Sicherung weiterarbeiten. Welches Verfahren passt?

Lösungen anzeigen

1. Beispielsweise für einen Fehler, der erst nach mehreren Wochen entdeckt wird.
2. Nein. Es fehlen unabhängige Medien und die räumliche Trennung.
3. Ein geeignetes Hot-Backup-Verfahren, das einen konsistent wiederherstellbaren Datenstand erzeugt.

Identifikation schützenswerter Daten

Kategorie	Beispiele	Bewertung
Maschinell wiederherstellbar oder wiederbeschaffbar	Temporäre Dateien, reproduzierbare Build-Dateien, erneut herunterladbare Installationspakete	Wiederbeschaffung ist möglich, kann aber Zeit und Aufwand verursachen.
Unersetzlich oder nur mit hohem Aufwand rekonstruierbar	Eigene Projektdokumente, Geschäftsvorgänge, individuelle Konfigurationen	Hohe Priorität bei der Sicherungsplanung.

Zusätzlich berücksichtigen

- Wie kritisch sind die Daten für den Betrieb?
- Wie schnell ändern sie sich?
- Wie lange dauert ihre Rekonstruktion?
- Welche Abhängigkeiten bestehen?
- Werden Schlüssel, Zertifikate oder Konfigurationen zur Wiederherstellung benötigt?

Beispiel: Eine Anwendung lässt sich neu installieren. Ohne gesicherte Datenbank und Konfiguration ist sie trotzdem nicht wieder einsatzfähig.

Übungsaufgabe

Ordne die Sicherungspriorität ein:

1. Ein erneut herunterladbares Installationspaket.
2. Selbst erstellte Kundenangebote.
3. Eine individuell aufgebaute Firewall-Konfiguration.

Lösung anzeigen

1. Meist geringere Priorität, sofern Quelle und passende Version zuverlässig verfügbar bleiben.
2. Hohe Priorität, weil die Inhalte nicht einfach wiederbeschafft werden können.

3. Hohe Priorität, weil die Wiederherstellung ohne Konfiguration zeitaufwendig und fehleranfällig sein kann.

Gegenmaßnahmen gegen Ausfall und Datenverlust

Maßnahme	Wirkung	Grenze
Redundante Systeme	Übernehmen bei Ausfall einzelner Komponenten	Können denselben Softwarefehler oder Angriff gemeinsam erleiden.
Regelmäßige Backups	Ermöglichen die Rückkehr zu gesicherten Datenständen	Wiederherstellung kostet Zeit; Änderungen seit dem letzten geeigneten Stand können fehlen.
USV	Überbrückt begrenzte Stromausfälle und ermöglicht geordnetes Herunterfahren	Laufzeit ist begrenzt; ersetzt kein Backup.
Überspannungsschutz	Begrenzt schädliche Spannungsspitzen	Liefert bei einem Stromausfall keine Ersatzenergie.
Firewall	Kontrolliert Netzwerkverkehr anhand von Regeln	Verhindert nicht jeden Angriff über erlaubte Verbindungen.
Virens Scanner beziehungsweise Endgeräteschutz	Erkennt und blockiert bestimmte Schadsoftware oder verdächtiges Verhalten	Erkennt nicht zwangsläufig jede neue oder angepasste Bedrohung.

RAID und Backup unterscheiden

RAID verbindet mehrere Laufwerke zu einem Speicherverbund.

- RAID 1 spiegelt Daten.
- Andere redundante RAID-Level können ebenfalls bestimmte Laufwerksausfälle abfangen.
- RAID 0 bietet keine Redundanz.
- Löschungen, unerwünschte Änderungen und Verschlüsselung durch Schadsoftware können auch den RAID-Datenbestand betreffen.

Merksatz: RAID unterstützt die Verfügbarkeit bei bestimmten Hardwareausfällen. Backups ermöglichen die Wiederherstellung gesicherter Datenstände.

Beispiel für kombinierte Maßnahmen

Ein Dateiserver verwendet redundante Laufwerke, eine USV, eingeschränkte Zugriffsrechte und aktuelle Schutzsoftware. Zusätzlich werden versionierte Backups erstellt; eine Kopie ist getrennt aufbewahrt. Wiederherstellungen werden regelmäßig getestet.

Übungsaufgabe

Ein Dateiserver besitzt RAID 1 und eine USV, aber kein Backup. Ein Mitarbeiter überschreibt eine wichtige Datei. Helfen RAID und USV bei der Rückkehr zur vorherigen Version?

Lösung anzeigen

Nein. RAID 1 übernimmt auch die unerwünschte Änderung auf die Spiegelung. Die USV schützt gegen bestimmte Stromprobleme. Für den vorherigen Dateistand ist eine geeignete Versionierung oder Sicherung erforderlich.

Zusammenhängende Prüfungsaufgabe

Ein Unternehmen betreibt einen Dateiserver. Alle Mitarbeiter arbeiten mit Administratorrechten. Die einzige Sicherung liegt auf einer dauerhaft angeschlossenen USB-Festplatte im Serverraum. Wiederherstellungen wurden noch nie getestet. Ein Fernzugang ist nur mit Passwort abgesichert.

Nenne mindestens sechs Verbesserungen und begründe sie.

Musterlösung anzeigen

1. **Standardkonten verwenden:** Das begrenzt die Auswirkungen von Fehlbedienung und Schadsoftware.
2. **Berechtigungen nach Aufgaben vergeben:** Nicht jeder Beschäftigte benötigt Zugriff auf sämtliche Daten.
3. **MFA für den Fernzugang aktivieren:** Ein gestohlenes Passwort allein soll nicht ausreichen.
4. **Eine räumlich getrennte Sicherung ergänzen:** Ein Standortschaden darf nicht Original und sämtliche Kopien zerstören.
5. **Offline oder unveränderbare Sicherungen vorsehen:** Angreifer sollen nicht alle Sicherungskopien verändern können.
6. **Restore-Tests durchführen:** Wiederherstellbarkeit und benötigte Zeit müssen überprüft werden.
7. **RPO und RTO festlegen:** Sicherungshäufigkeit und Wiederanlaufplanung sollen zu den betrieblichen Anforderungen passen.
8. **Updates, Härtung und Überwachung etablieren:** Schwachstellen reduzieren und Auffälligkeiten erkennen.

Kurzmerksatz

Datensicherheit schützt Daten durch technische, organisatorische und personelle Maßnahmen vor Verlust, Manipulation und unbefugtem Zugriff.

Die wichtigsten Unterschiede auf einen Blick

Begriffe	Unterschied
Vertraulichkeit, Integrität, Verfügbarkeit	Wer darf lesen? Sind die Daten korrekt? Sind sie bei Bedarf nutzbar?
Zutritt, Zugang, Zugriff	Raum, System, Daten beziehungsweise Aktionen
Authentifizierung, Autorisierung	Identität prüfen, Berechtigung prüfen
RBAC, ABAC, ACL	Rollen, Attribute, konkrete Zugriffslisten
Least Privilege, Need-to-know	Notwendige Rechte, notwendige Informationen
SQL-Injection, XSS	Datenbankabfrage, Browserausführung
Phishing, Social Engineering	Phishing ist eine spezielle Form menschlicher Manipulation.
ISMS, ISO 27001, Zertifizierung	Managementsystem, Anforderungsnorm, unabhängige Prüfung
Voll, inkrementell, differenziell	Alles, seit letzter Sicherung, seit letzter Vollsicherung
Hot Backup, Cold Backup	Laufender Betrieb, angehaltene Anwendung
RPO, RTO	Tolerierbarer Datenverlust, tolerierbare Wiederherstellungszeit
RAID, Backup	Ausfalltoleranz, Wiederherstellung von Datenständen
USV, Überspannungsschutz	Ersatzenergie auf Zeit, Begrenzung von Spannungsspitzen
Synchronisation, Backup	Abgleich von Beständen, gezielt wiederherstellbare Sicherung

Quellen und Vertiefung

Grundlage: der bereitgestellte Text aus [FI-Wiki – Datensicherheit](#). Beispiele und Übungsaufgaben wurden ergänzend formuliert.

- [OWASP – SQL Injection Prevention](#)
 - [OWASP – Cross Site Scripting Prevention](#)
 - [OWASP – Multifactor Authentication](#)
 - [OWASP – Authorization](#)
 - [ISO – ISO/IEC 27001](#)
 - [BSI – IT-Grundschutz-Methodik, Standard 200-2](#)
-