Fragen

Was ist Greylisting?

Greylisting ist ein einfacher Spam-Schutz, bei dem ein Mailserver von unbekannten Absendern zunächst per SMTP-Temporary-Error (4xx) zurückweist.

- Legitime Mailserver versuchen kurz darauf erneut zuzustellen und werden dann auf eine „Whitelist“ gesetzt.
- Viele Spam-Bots retryen nicht und bleiben ausgesperrt.
- Nachteil: Erstzustellung verzögert sich um einige Minuten.

Was ist ISO 27001?

- **Definition:** Internationaler Standard für ein Informationssicherheits-Managementsystem (ISMS)
- **Ziel:** Systematische Einrichtung, Umsetzung, Betrieb, Überprüfung und kontinuierliche Verbesserung der Informationssicherheit
- **Normnummer & Herausgeber:** ISO/IEC 27001, veröffentlicht von der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC)
- **Aufbau:** Basierend auf dem PDCA-Zyklus (Plan–Do–Check–Act)
- **Anhang A:** Enthält 114 Controls in 14 Domänen (z. B. Zugriffssteuerung, Kryptografie, Vorfallmanagement)
- **Zertifizierung:** Externes Audit, Gültigkeit in der Regel 3 Jahre mit jährlichen Überwachungsaudits
- **Nutzen:** Verbesserte Risikobewertung, Compliance-Nachweis, Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen.

Was sind Standards und wofür braucht man diese?

- **Definition:**
  - Dokumentierte Vorgaben und Empfehlungen, auf Basis von Konsens – oft international oder national erarbeitet
  - Legen Anforderungen, Prozesse und Kontrollen fest, um bestimmte Ziele verlässlich zu erreichen
- **Zweck in der Informationssicherheit:**
  - **Konsistenz:** Einheitliche Vorgehensweisen in Organisationen und über Branchen hinweg
  - **Interoperabilität:** Kompatibilität von Technologien, Systemen und Prozessen

- **Risikomanagement:** Klare Orientierung bei Identifikation, Bewertung und Behandlung von Risiken
- **Compliance & Nachweis:** Erfüllung gesetzlicher/regulatorischer Vorgaben; Audit-fähige Dokumentation
- **Best Practices:** Übertragung erprobter Maßnahmen zur Absicherung von Vertraulichkeit, Integrität und Verfügbarkeit
- **Vertrauen:** Glaubwürdigkeit gegenüber Kunden, Partnern und Aufsichtsbehörden
- **Kontinuierliche Verbesserung:** Grundlage für regelmäßige Überprüfung und Weiterentwicklung des Sicherheitsniveaus

Was ist die Common Criteria?

- **Definition:** Internationaler Standard zur Bewertung und Zertifizierung der Sicherheit von IT-Produkten und -Systemen (ISO/IEC 15408)
- **Ziel:** Objektive, vergleichbare Beurteilung, ob ein Produkt definierte Sicherheitsanforderungen erfüllt
- **Kernbestandteile:**
  - **Protection Profile (PP):** Vorgabe von Sicherheitsanforderungen für eine Produktkategorie
  - **Security Target (ST):** Spezifikation der Anforderungen und des Einsatzkontexts eines konkreten Produkts
- **EAL-Stufen (Evaluation Assurance Levels):** EAL 1 bis EAL 7 – steigend in formaler Strenge und Aufwand
- **Nutzen:**
  - International anerkanntes Prüfsiegel
  - Erhöhtes Vertrauen bei Anwendern und Behörden
  - Grundlage für Beschaffungsentscheidungen und Compliance in sicherheitskritischen Umgebungen

Was ist die Bürgerkarte?

- **Definition:** Österreichisches System für elektronische Identifikation und qualifizierte Signaturen („Bürgerkarte“)
- **Zweck:** Sichere Authentifizierung und rechtsverbindliches Unterzeichnen von Dokumenten im E-Government
- **Technische Umsetzung:**
  - Chipkarte (häufig in der e-Card integriert) oder USB-Token
  - Alternativ mobile Varianten wie Handy-Signatur bzw. ID Austria
- **Einsatzgebiete:**
  - Online-Behördenservices (z. B. FinanzOnline, Melderegisterauskünfte)
  - Elektronische Einreichung von Formularen und Verträgen
- **Rechtsgrundlage:** Signaturgesetz 2001, E-Government-Gesetz, eIDAS-Verordnung

- **Äquivalent:** Bürgerkarte-Funktionalität ist heute weitgehend durch die Handy-Signatur und ID Austria abgedeckt

Was sind gängige Bedrohungen in kleinen Unternehmen?

- **Phishing/Spear-Phishing**
  Gefälschte E-Mails oder Nachrichten, die Mitarbeitende zur Herausgabe von Zugangsdaten oder Klick auf Schadlinks verleiten.
- **Malware & Ransomware**
  Schadsoftware, die Daten verschlüsselt oder ausspäht; erpresst Lösegeld (z. B. WannaCry, Ryuk).
- **Ungepatchte Systeme & Software-Schwachstellen**
  Ausnutzung von veralteten Betriebssystemen oder Anwendungen, da keine Sicherheitsupdates installiert wurden.
- **Schwache Passwörter & fehlendes Authentifizierungs-Hardening**
  Einfache oder mehrfach genutzte Passwörter sowie fehlende Multi-Factor-Authentication (MFA) erleichtern Angreifern den Zugang.
- **Insider-Threats & menschliche Fehler**
  Unachtsamkeit beim Umgang mit Daten, versehentliches Löschen, Freigabe vertraulicher Informationen oder böswillige Mitarbeitende.
- **Fehlende Backups & schlechte Wiederherstellungs-Strategie**
  Kein regelmäßiges, getestetes Backup: Datenverlust bei Ausfall oder Ransomware führt zu langwierigen Ausfallzeiten.
- **Physischer Diebstahl & Verlust von Endgeräten**
  Abhandenkommen von Laptops, Smartphones oder USB-Sticks ohne Verschlüsselung eröffnet unbefugten Datenzugriff.

Was sind Firewalls?

- **Definition:** Netzwerksicherheitssystem, das ein- und ausgehenden Datenverkehr gemäß festgelegter Regeln kontrolliert.
- **Zweck:** Schutz vor unautorisiertem Zugriff, Angriffen und unerwünschtem Datenverkehr.
- **Arbeitsweise:**
  - Paketfilterung: Prüfen von IP-Adressen, Ports und Protokollen
  - Zustandsorientierte Filter (Stateful Inspection): Verfolgen des Verbindungsstatus
  - Anwendungsschicht-Filter (Proxy/Next-Gen): Analyse von Daten bis zur Anwendungsebene
- **Arten:**
  - **Hardware-Firewall:** Eigenständiges Gerät meist im Perimeter
  - **Software-Firewall:** Auf Endgeräten oder Servern installiert
  - **Cloud/Virtual Firewall:** In virtuellen Netzwerken oder Cloud-Umgebungen
- **Regeltypen:**

    - Erlaubnisregeln (Allow) und Verweigerungsregeln (Deny)
    - Whitelist vs. Blacklist
- **Einsatzszenarien:** Perimeter-Schutz, Segmentierung interner Netze, Schutz von Servern und Endpunkten

Was sind funktionale und Zuverlässigkeitsandforderungen?

- **Funktionale Anforderungen**
    - Beschreiben **Was?** – welche Aufgaben, Dienste und Funktionen das System leisten muss
    - Beispiel: „Das System muss Benutzern erlauben, sich per E-Mail/Passwort zu authentifizieren.“
    - Konkretisiert durch Use-Cases, User Stories oder Lasten-/Pflichtenheft
- **Zuverlässigkeitsanforderungen (Reliability)**
    - Beschreiben **Wie gut?** – Verfügbarkeit, Fehlertoleranz und Wiederherstellbarkeit
    - Kennzahlen z. B.
        - **Verfügbarkeit:** 99,9 % Uptime pro Jahr
        - **MTBF (Mean Time Between Failures):** z. B. ≥ 500 Stunden
        - **MTTR (Mean Time To Repair):** z. B. ≤ 2 Stunden
    - Maßnahmen: Fehlertoleranz (Redundanz), automatische Wiederherstellung (Failover), Monitoring und Alarmierung

Erkläre Zusammenhang zwischen ISO 27001 und ISO 27002.

- **ISO/IEC 27001** definiert die **Normanforderungen** an ein Informationssicherheits-Managementsystem (ISMS): Prozess- und Managementvorgaben, Aufbau des PDCA-Zyklus, Audit- und Zertifizierungsanforderungen.
- **ISO/IEC 27002** ist ein **Code of Practice** zur **Unterstützung** von 27001: Liefert detaillierte **Implementierungs- und Gestaltungsempfehlungen** für die in 27001 (Anhang A) gelisteten Controls.
- **Normativ vs. Informativ:**
    - 27001 (inkl. Anhang A) ist **normativ** (Zertifizierungsbasis).
    - 27002 ist **informativ**, hilft bei Auswahl und Ausgestaltung der Controls.
- **Verknüpfung:** Organisationen wählen in der Risikobehandlung gemäß 27001 passende Controls aus Anhang A und orientieren sich an 27002 für deren konkrete Umsetzung.
- **Ziel:** 27001 stellt das **„Was?“** (Anforderungen), 27002 das **„Wie?“** (Best Practices).

Erkläre Zusammenhang zwischen BSI und ISO 27001.

- **BSI (Bundesamt für Sicherheit in der Informationstechnik):** Nationale Cybersecurity-Behörde in Deutschland, Herausgeber der IT-Grundschutz-Standards.

- **ISO/IEC 27001:** Internationaler Standard für ein Informationssicherheits-Management-system (ISMS), definiert Anforderungen und Zertifizierungsverfahren.
- **IT-Grundschutz und ISO 27001:**
  - IT-Grundschutz-Kataloge des BSI liefern eine praxisnahe Methodik und detaillierte Controls, die direkt auf die Anforderungen von ISO 27001 (Anhang A) abgebildet sind.
  - BSI stellt mit dem IT-Grundschutz-Kompendium konkrete Umsetzungshinweise zu den in ISO 27001 geforderten Sicherheitsmaßnahmen bereit.
- **Zertifizierung:**
  - In Deutschland akkreditieren BSI und Deutsche Akkreditierungsstelle (DAkkS) Zertifizierungsstellen für ISO 27001-Audits.
  - Organisationen können sich sowohl nach ISO 27001 als auch nach BSI-IT-Grundschutz zertifizieren lassen; letztere Zertifizierung schließt i. d. R. auch die ISO-27001-Anforderungen ein.
- **Fazit:** Das BSI ergänzt und detailliert mit seinen IT-Grundschutz-Standards das internationale ISO-27001-Rahmenwerk und übernimmt in Deutschland die Rolle des Anleiters, Umsetzers und Akkreditierers.

Was ist starke Authentifizierung?

- **Definition:** Verfahren, das zur Identitätsprüfung mindestens zwei voneinander unabhängige Faktoren nutzt.
- **Faktorklassen:**
  1. **Wissen** (z. B. Passwort, PIN)
  2. **Besitz** (z. B. Token, Smartphone mit OTP-App)
  3. **Inhärenz** (z. B. Fingerabdruck, Gesichtserkennung)
- **Umsetzung:** Kombination aus „etwas, das ich weiß“ + „etwas, das ich habe“ (oder „bin“)
- **Beispiele:**
  - Passwort + SMS-/App-TAN (One-Time-Password)
  - Smartcard + biometrische Verifikation
- **Vorteile:**
  - Stärkerer Schutz gegen Phishing, Passwortdiebstahl und Replay-Angriffe
  - Erhöhte Sicherheit für sensible Anwendungen (Banking, E-Government)

Welche personenbezogenen Daten sind für die IT wichtig?

- **Identitäts- und Kontaktdaten**
  – Name, Anschrift, Geburtsdatum, Personal-/Mitarbeiternummer
  – E-Mail-Adresse, Telefonnummer
- **Authentifizierungs- und Autorisierungsdaten**
  – Benutzername, Passwort (hashes), PIN, OTP-Seeds
  – Rollen, Gruppenmitgliedschaften, Rechtezuweisungen

- **Geräte- und Netzwerkinformationen**
  – IP-Adresse, MAC-Adresse, Gerätetyp und Seriennummer
  – Standortdaten (z. B. WLAN-Zugangspunkte, GPS)
- **Log- und Protokolldaten**
  – Login-/Logout-Zeitstempel, Sitzungs-IDs
  – System- und Applikationslogs mit Nutzer-IDs
- **Zertifikats- und Schlüssel-Daten**
  – Public-/Private-Key-Paare, Zertifikat-Fingerabdrücke
  – Smartcard- oder Token-Kennungen
- **Sensible Zusatzdaten (falls verarbeitet)**
  – Biometrische Templates (Fingerabdruck, Gesichtserkennung)
  – Gesundheits- oder Personaldaten, sofern IT-Systeme sie verwalten

Was sind besondere personbezogene Daten welche nur in Ausnahmefällen mit Zustimmung gesammelt werden dürfen?

- **Sonderkategorien gemäß Art. 9 DSGVO (nur mit expliziter Einwilligung oder legaler Ausnahme):**
  - Rassische und ethnische Herkunft
  - Politische Meinungen
  - Religiöse oder weltanschauliche Überzeugungen
  - Gewerkschaftszugehörigkeit
  - Genetische Daten
  - Biometrische Daten (zur Identifikation)
  - Gesundheitsdaten
  - Daten zum Sexualleben oder zur sexuellen Orientierung
- **Strafrechtliche Daten gemäß Art. 10 DSGVO:**
  - Daten über strafrechtliche Verurteilungen und Straftaten
- **Verarbeitungs-Ausnahmen (ohne Einwilligung) in Ausnahmefällen:**
  - Schutz lebenswichtiger Interessen (z. B. medizinischer Notfall)
  - Erfüllung arbeits- oder sozialrechtlicher Pflichten (z. B. Gesundheitschecks im Beschäftigungsverhältnis)
  - Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
  - Verarbeitung im öffentlichen Interesse (z. B. Epidemiologie)

Was ist Compliance?

- **Definition:** Einhaltung aller relevanten gesetzlichen Vorgaben, regulatorischen Anforderungen und internen Richtlinien.
- **Ziel:** Vermeidung von Rechtsverstößen, Bußgeldern, Imageschäden und Geschäftsrisiken.
- **Komponenten:** Policies, Kontrollen, Audits, kontinuierliches Monitoring und Schulungen.

- **IT-Relevanz:** Datenschutz (z. B. DSGVO), Sicherheitsstandards (ISO 27001), branchenspezifische Regulatorien (SOX, MiFID II).
- **Maßnahmen:** Risikoanalysen, Implementierung technischer/logischer Kontrollen, regelmäßige Compliance-Reviews.

Was ist Governance?

- **Definition:** Strukturiertes Rahmenwerk zur Steuerung und Überwachung von Unternehmens- oder IT-Aktivitäten, um strategische Ziele zu erreichen.
- **Ziel:** Sicherstellen, dass Entscheidungen und Prozesse wertschöpfend, transparent und regelkonform ablaufen.
- **Kernbestandteile:**
  - **Strategische Ausrichtung:** Festlegung von Vision, Zielen und Prioritäten
  - **Rollen & Verantwortlichkeiten:** Klare Zuordnung von Entscheidungskompetenzen (z. B. Vorstand, IT-Leitung, Gremien)
  - **Richtlinien & Verfahren:** Policies, Standards und Steuerungsprozesse
  - **Kontrolle & Reporting:** Monitoring, Kennzahlen (KPIs), Audits
- **Frameworks & Normen:**
  - COBIT (Control Objectives for Information and Related Technologies)
  - ISO/IEC 38500 (Grundsätze der IT-Governance)
- **Beziehung zu Compliance & Risiko:** Governance definiert den übergeordneten Rahmen, innerhalb dessen Compliance- und Risikomanagement-Maßnahmen wirksam implementiert werden.

Wie kann eine Betriebsvereinbarung in Bezug auf Informationssicherheit in einem Unternehmen hilfreich sein?

- **Rechtssicherheit & Klarheit**
  - Legt verbindliche Regeln für Umgang, Zugriff und Schutz von Informationen fest
  - Vermeidet Auslegungs- und Haftungsfragen
- **Mitbestimmung & Akzeptanz**
  - Einbindung des Betriebsrats stärkt Legitimation und Vertrauen
  - Fördert Akzeptanz bei Mitarbeitenden durch Beteiligung
- **Verantwortlichkeiten & Zuständigkeiten**
  - Definiert Rollen (z. B. IT-Leitung, Datenschutzbeauftragter, Anwender)
  - Verhindert Kompetenzgerangel und Zuständigkeitslücken
- **Schulungen & Sensibilisierung**
  - Vereinbart regelmäßige Awareness-Maßnahmen
  - Sichert notwendige Ressourcen für Training
- **Überwachung & Sanktionen**
  - Regelt Art und Umfang technischer Kontrollen (z. B. Log-Monitoring)

    - Legt Verfahren bei Verstößen und disziplinarische Maßnahmen fest
- **Kontinuierliche Verbesserung**
    - Verankert Überprüfungs- und Anpassungszyklen (Audits, Reviews)
    - Ermöglicht Reaktion auf neue Bedrohungen und Technikänderungen

Was ist Discretionary, Role-Based und Mandatory Access-Controll?

- **Discretionary Access Control (DAC)**
    - **Grundprinzip:** Ressourceneigentümer (z. B. Dateibesitzer) legen Zugriffsrechte selbst fest
    - **Verteilung:** Über Access Control Lists (ACLs) oder Capability-Listen
    - **Flexibilität:** Feingranulare Erlaubnisvergabe, aber anfällig für fehlerhafte Rechtevergabe
- **Role-Based Access Control (RBAC)**
    - **Grundprinzip:** Rechte werden nicht einzelnen Nutzern, sondern vordefinierten Rollen zugewiesen
    - **Aufbau:** Nutzer → Rollen → Berechtigungen
    - **Vorteil:** Einfache Administration bei Personalwechsel und Organisationsstruktur; verhindert Überprivilegierung
- **Mandatory Access Control (MAC)**
    - **Grundprinzip:** Zentrale Sicherheitsrichtlinie erzwingt Zugriff basierend auf Klassifizierungsstufen und Sicherheitslabels
    - **Labels:** Subjekt-Label (z. B. „Geheim“), Objekt-Label (z. B. „Vertraulich“)
    - **Strenge:** Nutzer können eigene Rechte NICHT verändern; hoher Schutzbedarf in hochsicheren Umgebungen (z. B. Militär)

Was ist das Chinese Wall Modell?

- **Definition:** Zugriffsmodell zur Vermeidung von Interessenkonflikten, auch „Brewer-and-Nash-Modell“ genannt.
- **Grundprinzip:** Dynamische Zugriffsbeschränkung basierend auf bisherigen Lese- und Schreiboperationen.
- **Datengruppen:** Objekte werden zu Interessenskonflikt-Klassen (Conflict of Interest Classes, CoI-Klassen) zusammengefasst.
- **Simple-Security-Regel:** Nutzer darf nur auf Objekte in einer CoI-Klasse zugreifen, wenn er noch kein Objekt einer konkurrierenden Klasse gelesen hat.
- **Property („Star-Property“):** Schreiben nur, wenn Lesen und Schreiben keine Konflikte mit anderen Objekten in dieser Klasse erzeugt.
- **Ziel:** Sicherstellung, dass z. B. Analysten nach Zugriff auf Daten eines Kunden nicht gleichzeitig Zugriff auf die Daten direkter Wettbewerber erhalten.

Was muss beachtet werden, wenn in einem Unternehmen ein biometrischer Authentifizierungsprozess eingeführt wird?

- **Rechtliche Grundlage & Datenschutz**
  - Verarbeitung nur bei eindeutiger Rechtsgrundlage (Einwilligung oder berechtigtes Interesse nach Art. 6 DSGVO)
  - Datenschutz-Folgenabschätzung (DSFA) gemäß Art. 35 DSGVO durchführen
  - Zweckbindung und Information der Betroffenen
- **Verhältnismäßigkeit & Alternativen**
  - Abwägung: Ist Biometrie wirklich erforderlich, oder reichen PIN/MFA?
  - Notfallverfahren und Ausweichmethoden (z. B. Token) vorsehen
- **Technische Sicherheit der Templates**
  - Verschlüsselung und sichere Speicherung (idealerweise auf Hardware-Sicherheitsmodul oder Secure Element)
  - Template-Protection (z. B. Cancelable Biometrics, Biometric Cryptosystems)
  - Liveness-Detection gegen Replay- und Fotoangriffe
- **Systemintegration & Lifecycle-Management**
  - Klare Architektur: Erfassung, Verarbeitung, Matching und Löschung der biometrischen Daten
  - Periodische Updates und Patches für Sensor- und Matching-Software
  - Regelmäßige Überprüfung der Erkennungsraten (False Accept/Reject Rates)
- **Verträge & Drittanbieter**
  - Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO mit Biometrie-Anbieter
  - Nachweis von Zertifizierungen (z. B. ISO/IEC 30107, Common Criteria)
- **Awareness & Schulung**
  - Mitarbeitende über Funktionsweise, Risiken und korrekten Umgang aufklären
  - Notfall- und Supportprozesse kommunizieren
- **Dokumentation & Audit**
  - Technische und organisatorische Maßnahmen (TOMs) dokumentieren
  - Regelmäßige Audits und Penetrationstests durchführen

Was sind TOMs?

- **Definition:** Technische und Organisatorische Maßnahmen (TOMs) sind alle Vorkehrungen, die Vertraulichkeit, Integrität und Verfügbarkeit von Daten sicherstellen.
- **Technische Maßnahmen:**
  - Zugriffskontrollen (Passwörter, MFA)
  - Verschlüsselung (TLS, Festplatten-/Datenbank-Verschlüsselung)
  - Firewalls, Antivirus, Intrusion Detection Systeme
  - Backup- und Wiederherstellungsverfahren
- **Organisatorische Maßnahmen:**

    - Richtlinien und Verfahren (z. B. Datenklassifizierung, Passwortpolicy)
    - Schulungen und Sensibilisierung der Mitarbeitenden
    - Rollen- und Berechtigungsmanagement
    - Notfallpläne und Incident-Response-Prozesse
- **Rechtsgrundlage:** Erforderlich nach Art. 32 DSGVO, um angemessenes Sicherheitsniveau zu