DLP (Data Loss Prevention) -> Schutz vor Datenverlust

- persönliche Daten
- Betriebsgeheimnisse (Arbeitsergebnisse, Prozesse, Unternehmensstruktur, Kundendaten, Geschäftspartner, ...)

Gesetze und Normen:
- BSI-Standards (200-1 bis 200-4 und 100-4)
- ISO 27001 (ISMS)
- DSGVO
- BDSG
- NIS2
- branchenspezifische Standards (PCIDSS)
- StGB

Umsetzung:
1. Daten erkennen bzw. identifizieren
   - Klassifizierung der Daten:
     - öffentlich
     - intern
     - vertraulich
     - streng vertraulich
   - Netzwerk-DLP
   - Endpoint-DLP
   - Cloud-DLP
2. Schutzmaßnahmen implementieren
   - Erhöhung der Awareness durch Schulungen
   - Signaturerkennung, Mustererkennung, TPM (HSM), ML , Verschlüsselung, SIEM, ISMS, RBAC,
   - Simulation von Incidents
3. Überwachung
   - IDS/ IPS, SIEM,
4. Meldekette
5. Maßnahmen (sogenannter Incident Response Plan)
6. "Lessons Learned"
7. PDCA / regelmäßige Überprüfung

Arten bzw. Formen von Datenverlusten:
- externe Angriffe:
  - mögliche Einfallstore:

  - Hacking
  - Phishing
  - unsichere Software (nicht gepatched)
  - social Engineering
- physischer Natur: Hardwareausfälle, Elementarschäden,
- Insider Angriffe, z.B. durch:
  - Mitarbeiter (Geschäftsführung, aktuelle aber auch ehemalige)
  - Geschäftspartner
    - Frage: "Wer garantiert mir, dass Geschäftspartner sicher mit meinen Daten umgehen?" / Ist der Gesch.-Partner zertifiziert?
  - "die Motivation" kann ebenfalls einen Insiderangriff auslösen:
    frustrierte MA, Rache, Erpressung, Sabotage, ideologische Gründe (z.B. wg. Tierschutz)
- versehentliches Löschen
-

Was kann man tun, um Datenverlust vorzubeugen?
- Backups (3-2-1)
- klare Regeln definieren (Nutzung der Assets, etc. ...)
- Für die entsprechende Infrastruktur sorgen (ausreichend dimensionierte PSUs,
  Pflege (Staub ...), Sicherheitsüberprüfung der Geräte (BGUV),
- Implementierung von Schutzmechanismen (Zutrittskontrolle, Fw, IDS/ IPS,
  Verschlüsselung anwenden, sichere PWs,

Konsequenzen:
- juristische Folgen
- Reputationsverlust (Vertrauensverlust durch die Kunden)
- finanzielle Verluste
-
