Hausaufgabe zum Thema DLP (Data Loss Prevention):

Gegebenes Szenario:

Ein mittelständisches Unternehmen mit ca. 500 Mitarbeitenden plant die Einführung eines Data Loss Prevention (DLP)-Systems.
Ziel ist es, den Verlust oder die unbefugte Weitergabe sensibler Daten zu verhindern.

Das Unternehmen speichert und verarbeitet verschiedene Arten von sensiblen Daten, darunter:

- Kundendaten (personenbezogene Daten, Zahlungsinformationen)
- Vertrauliche Unternehmensdokumente (Strategiepläne, Finanzberichte)
- Forschung & Entwicklung (Patente, technische Entwürfe)

Die Geschäftsführung hat festgestellt, dass es in der Vergangenheit mehrere sicherheitskritische Vorfälle gab, darunter:

- Ein Mitarbeiter hat sensible Finanzdaten per privater E-Mail verschickt.
- Eine ungesicherte Cloud-Speicherlösung wurde genutzt, um vertrauliche Dokumente zu teilen.
- Ein Ex-Mitarbeiter hatte noch Zugriff auf interne Daten, nachdem er das Unternehmen verlassen hatte.

Aufgaben:

1. Theoretische Grundlagen (20 Punkte)

a) Erkläre den Begriff „Data Loss Prevention“ und beschreibe die wichtigsten Funktionen eines DLP-Systems. (5 Punkte)

b) Welche Arten von DLP-Technologien gibt es?
Vergleiche Endpoint-DLP, Netzwerk-DLP und Cloud-DLP hinsichtlich ihrer Funktionsweise, Vorteile und Herausforderungen. (5 Punkte)

c) Welche Bedrohungen und Risiken führen typischerweise zu Datenverlust?
Nenne drei konkrete Szenarien und beschreibe, wie DLP in diesen Fällen helfen kann. (5 Punkte)

d) Welche rechtlichen und Compliance-Vorgaben sind in Europa für DLP relevant?
Gehe dabei (im Rahmen deines Kenntnisstandes) auf die DSGVO und ISO 27001 ein. (5 Punkte)

2. Planung einer DLP-Strategie (30 Punkte)

a) Versuche eine Datenklassifizierungsstrategie für das Unternehmen zu entwickeln.
Wie würdest du die Daten in Schutzkategorien einteilen? (5 Punkte)

b) Entwirf eine DLP-Richtlinie, die festlegt, wie Mitarbeitende mit vertraulichen Daten umgehen dürfen. (5 Punkte)

c) Welche technischen Maßnahmen würdest du vorschlagen, um die drei genannten Sicherheitsvorfälle zu verhindern?
Beschreibe für jeden Vorfall eine DLP-Lösung. (10 Punkte)

d) Welche Herausforderungen könnten bei der Einführung einer DLP-Lösung auftreten?
Nenne mindestens drei Probleme und schlage Lösungen vor. (5 Punkte)

e) Welche Schulungsmaßnahmen würdest du vorschlagen, um Mitarbeitende für das Thema DLP zu sensibilisieren? (5 Punkte)

3. Technische Umsetzung und Integration (30 Punkte)

a) Das Unternehmen nutzt bereits ein SIEM-System (Security Information and Event Management). Wie könnte eine Integration mit DLP erfolgen, um die Sicherheitsüberwachung zu verbessern? (5 Punkte)

b) Beschreibe, wie DLP in einer Cloud-Umgebung eingesetzt werden kann, um Datenverluste durch Cloud-Speicher oder SaaS-Anwendungen zu verhindern. (5 Punkte)

c) Welche Methoden der Erkennung sensibler Daten sollte das Unternehmen in seinem DLP-System aktivieren (z. B. Pattern Matching, Machine Learning)?
Begründe deine Auswahl. (10 Punkte)

d) Welche automatisierten Maßnahmen könnte das DLP-System ergreifen, wenn eine Richtlinie verletzt wird?
Differenziere zwischen sofortiger Blockierung, Warnung und Eskalation an die IT-Sicherheit. (5 Punkte)

e) Wie kann DLP mit einem Zero-Trust-Sicherheitsmodell kombiniert werden, um den Schutz vertraulicher Daten zu verbessern? (5 Punkte)

4. Szenario-Analyse (20 Punkte)

Du erhältst zwei Szenarien und musst analysieren, wie DLP helfen kann:

Szenario 1 (10 Punkte):

Ein Mitarbeitender aus der Entwicklungsabteilung kündigt und verlässt das Unternehmen. Ein Tag vor seinem letzten Arbeitstag schickt er eine E-Mail an seine private Adresse mit einer ZIP-Datei, die mehrere technische Entwürfe enthält.

Wie könnte ein DLP-System diesen Vorfall erkennen und verhindern?

Welche Maßnahmen sollten ergriffen werden, um zukünftige Vorfälle dieser Art zu vermeiden?

Szenario 2 (10 Punkte):

Ein Außendienstmitarbeiter verliert sein unverschlüsseltes Firmen-Laptop in einem Café. Auf dem Gerät befinden sich mehrere vertrauliche Kundendaten.

Welche technischen und organisatorischen Maßnahmen hätte das Unternehmen treffen müssen, um den Schaden zu minimieren?

Wie könnte eine DLP-Strategie den Schutz mobiler Geräte verbessern?