Security Management – Case Study 2

Student: Philip Magnus

Student ID: c2410537022

Datum: *05.12.2025*

Aufgabenstellung

1. **Design an IT security plan for at least three identified risks in your organization.**
2. **Design a backup plan for your organization.**
    - Amount and classification of data to be backed up (e.g. business data, system files, data bases, devices)
    - Backup technologies and media (e.g. retaining bands, removable discs, cloud storage, USB sticks, CS/DVD)
    - Time interval and point in time of backups (daily, weekly, on weekdays,…)
    - Responsibilities for enforcement, supervision and documentation of back ups
    - Safekeeping of backup media

Die Case Study 2 wird als Beispiel das erfundene Unternehmen aus Case Study 1 verwenden, die PointPoint GmbH, ein SaaS-Anbieter mit Hauptsitz in Wien mit etwa 250 Mitarbeitern.

1. IT Security Plan for Three Identified Risks

Basierend auf dem Risk Register aus Case Study 1 für die PointPoint GmbH werden drei Risiken ausgewählt:

- SQL-Injection auf die Kundendatenbank
- Phishing auf Mitarbeiter-Accounts
- Diebstahl von Laptops ohne Verschlüsselung

1.1 Risiko 1: SQL-Injection auf die Kundendatenbank

Ausgangslage (Case Study 1)

- **Asset:** Kundendatenbank
- **Threat/Vulnerability:** Schwache Eingabevalidierung (SQL-Injection)
- **Likelihood:** Medium
- **Impact:** High
- **Risk Level:** High
- **Bisherige Controls:** WAF, Secure Coding (geplant)

Security Plan

Kategorie	Details

Kategorie	Details
Risk	SQL-Injection → unautorisierter Zugriff, Datenmanipulation, vollständiger DB-Export
Level of Risk	High
Recommended Controls	**Management/Organisational:** • Secure Development Policy (SDLC mit Security Gates) • Code-Review-Verpflichtung (4-Augen-Prinzip) **Operational/People:** • Entwickler-Schulung zu OWASP Top 10 • Playbooks für Secure Coding Standards **Technical:** • Einsatz einer Web Application Firewall (WAF) • Parametrisierte Queries & ORMs • Automatisierte SAST/DAST-Scans • Logging & Monitoring aller DB-Queries
Priority	Sehr hoch (personenbezogene Kundendaten, DSGVO-Risiken)
Selected Controls	• Fixierung sämtlicher SQL-Endpunkte auf parametrisierte Queries • Rollout einer standardisierten Secure-Coding-Guideline • Einführung eines vollständigen CI/CD-Security-Checks (SAST/DAST) • Aktivierung von WAF-Regeln speziell gegen Injection-Attacken
Required Resources	DevOps Team, AppSec Engineer, externer Pentest-Dienstleister
Responsible Persons	Head of Development, IT Security Lead
Start/End Date	01.03.2026 – 31.05.2026
Maintenance	• Halbjährliche Penetration Tests • Quartalsreview der WAF-Logs • SDLC-Compliance-Check

1.2 Risiko 2: Phishing gegen Mitarbeiter-Accounts

Ausgangslage (Case Study 1)

- **Asset:** Mitarbeiter-Accounts
- **Threat/Vulnerability:** Phishing, mangelnde Schulung
- **Likelihood:** High
- **Impact:** High
- **Risk Level:** High

Security Plan

Kategorie	Details

Kategorie	Details
Risk	Erfolgreiches Phishing → Account-Kompromittierung, Datenverlust, lateral movement
Level of Risk	High
Recommended Controls	**Management/Organisational:** • E-Mail- und Acceptable-Use-Policy • Incident-Reporting-Prozess **Operational/People:** • Pflicht-Awareness-Schulung für alle Mitarbeiter • Quartalsweise Phishing-Simulationen **Technical:** • MFA für alle kritischen Systeme • Mail-Filter, URL-Rewrite, Sandboxing • Zentralisiertes Endpoint-Security-Tool
Priority	Hoch (häufigster Angriffsvektor)
Selected Controls	• Umsetzung eines unternehmensweiten MFA-Zwangs • Ausbau des Advanced Threat Protection Mailgateways • Einführung eines “Report Phishing”-Buttons • Wiederkehrende Trainings & Simulationen
Required Resources	Security Awareness Team, HR, IT-Admin
Responsible Persons	IT Security Manager, HR Manager
Start/End Date	01.04.2026 – 30.06.2026
Maintenance	• Jährliche Schulungspflicht • Auswertung der Simulationsergebnisse zur Wirksamkeitsmessung

1.3 Risiko 3: Diebstahl von Laptops (fehlende Verschlüsselung)

Ausgangslage (Case Study 1)

- **Asset:** Laptops
- **Threat/Vulnerability:** Keine Festplattenverschlüsselung
- **Likelihood:** Medium
- **Impact:** High
- **Risk Level:** High

Security Plan

Kategorie	Details
Risk	Gestohlener Laptop → Verlust sensibler Kundendaten, GDPR-Breach

Kategorie	Details
Level of Risk	High
Recommended Controls	**Management/Organisational:** • Mobile Device Security Policy **Operational/People:** • Schulung: Umgang mit mobilen Geräten • Sofort-Meldepflicht bei Verlust **Technical:** • Full-Disk Encryption (BitLocker/FileVault) • Mandatory MDM Enrollment • Remote-Lock & Remote-Wipe
Priority	Hoch
Selected Controls	• Rollout einer standardisierten MDM-Lösung • Automatisierte Gerätedeployment-Pipeline inkl. Encryption Enforcement • Aktivierung von Geotracking & Remote-Wipe
Required Resources	Endpoint Team, IT Security Lead
Responsible Persons	Endpoint Manager, CISO
Start/End Date	01.05.2026 – 31.07.2026
Maintenance	• Quartalsweise Prüfung der MDM-Compliance • Jährliche Software-/Hardware-Inventur

2. Backup Plan for the Organization

Basierend auf den Assets aus Case Study 1.

2.1 Amount and Classification of Data

Kategorie	Systeme / Beispiele	Klassifikation	Geschätzter Umfang
Kundendatenbank	SQL-DB, CRM	Hoch (personenbezogen)	~2,5 TB
Cloud-Server-Daten	VM-Images, Logs, Konfigs	Hoch	~1,5 TB
Source Code / Repository	Git-Server, Pipelines	Hoch (IP)	~500 GB
HR-Systemdaten	Personalakten, Payroll	Hoch	~200 GB
Mitarbeiter-E-Mails	Mailserver/Cloud-Mail	Mittel	~2 TB

Kategorie	Systeme / Beispiele	Klassifikation	Geschätzter Umfang
Laptops/Endgeräte	Benutzerprofile, lokale Dateien	Mittel	variabel
SIEM & Log-Daten	Security Logs, Audit Trails	Mittel	~2 TB pro Monat
Backupsysteme selbst	Konfigurationsdaten	Mittel	<100 GB

2.2 Backup Technologies & Media

- **Primäre Technologie**
  - Zentrales Backup-System (Backup Appliance / Veeam o.Ä.)
  - Zielsystem: disk-basierte Backups (NAS/SAN)
- **Sekundäre / Offsite Backups**
  - Replikation in Cloud Object Storage (verschlüsselt)
  - Optional: Monatliches Band-Archiv (LTO) für Langzeitaufbewahrung (Compliance)
- **Spezielle Medien**
  - Git-Repo-Snapshots in verschlüsselten Buckets
  - VM-Konfigurationsbackups in dedizierten Repositories

2.3 Backup Intervals & Strategy

a) **Kundendatenbank**

- Tägliche inkrementelle Backups (22:00–04:00)
- Wöchentliches Vollbackup
- **RPO:** 24h
- **RTO:** 4–8h

b) **Cloud-Server / VMs**

- Tägliche Snapshots
- Wöchentlich Vollbackup der VMs

c) **Source Code**

- Real-time Replikation (Git Mirroring)
- Tägliches Repo-Full-Backup

d) **HR-System & Finance**

- Tägliche inkrementelle Backups
- Monatliches Vollbackup + Bandarchiv für 7 Jahre

e) **E-Mail- und Office-Daten**

- Täglich inkrementell
- Wöchentlich voll

f) **Endgeräte-Laptops**

- Tägliche Synchronisation ins MDM/OneDrive/Fileshare
- Fileshare ist Teil des normalen Backupplans

2.4 Responsibilities

Rolle	Aufgaben
IT-Leiter	Strategische Verantwortung, Budget, Toolauswahl
IT Security Manager	Sicherstellen von Verschlüsselung, Zugriffskontrolle, DR-Konzept
System Administrator	Backup-Jobs konfigurieren, überwachen, Restore-Tests
Compliance Officer	Kontrolle gesetzlicher Aufbewahrungsfristen (HR/Finance)
Helpdesk	Erstkontakt für Restore-Anfragen

2.5 Safekeeping of Backup Media

Onsite Storage

- Im Serverraum mit Zutrittskontrolle
- Nur System Admins und Security haben Zugang

Offsite / Cloud Storage

- End-to-End-Verschlüsselung
- Zugriff nur via MFA & RBAC

Band-Archiv

- Physisch gesichert im externen Tresor
- Klimatisierte, zugriffsbeschränkte Umgebung

2.6 Tests, Change & Incident Management

Restore-Tests

- Vierteljährlicher Restore der Kundendatenbank
- Halbjährlicher Restore eines ganzen Systems
- Dokumentation & Lessons Learned

Change Management

- Jede neue Anwendung muss geprüft werden: *„Ist sie im Backup-Scope?“*
- Update der CMDB bei Backup-Änderungen

Incident Handling

- Definierter Prozess für Ransomware: Wiederherstellung nur aus „clean backups“
- Integration des Backupkonzepts in das Business Continuity Management