Die Häcker AG – Alexandra Han

1. Analysieren Sie die Systeme und Daten in Ihrem Arbeitsbereich auf mögliche Schwachstellen, die Angreifer ausnutzen könnten.

1.1 Welche Systeme, Anwendungen und Daten sind Bestandteil Ihres Arbeitsbereichs? Erstellen Sie eine Auflistung mit den folgenden Gruppen:

- Server-Hardware

1. File-Server (SAMBA)
2. SQL-Kunden-DB
3. Active-Directory
4. Print-Server
5. Backup-Server

- Netzwerk und dessen Komponenten

1. Router
2. Switch
3. VPN-Server

- Arbeitsgeräte

1. PCs
2. Laptops (Home-Office und vor Ort)

- Anwendungen und Dienste

1. ERP-System
2. Entwicklungsumgebungen
3. Kollaborationstools (z. B. Git, JIRA)
4. E-Mail-Server

- Daten (z. B. Kundendaten, Entwicklungsdaten, Zugangsdaten)

1. Kundendaten
2. Entwicklungsdaten (Quellcode)
3. Zugangsdaten
4. Backup-Daten

1.2 Gibt es Schnittstellen zu anderen Systemen oder externen Partnern?

Ja, Mitarbeiter können über eine VPN-Verbindung sicher auf das Stammunternehmen zugreifen. Dies ermöglicht sowohl Home-Office als auch mobilen Mitarbeitern den Zugriff auf Firmendaten. Für Besucher steht ein separater PC mit Internetzugang zur Verfügung.

1.3 Besteht eine Dokumentation?

Es gibt keine Dokumentation, und nur drei Personen kennen die IT-Infrastruktur und Passwörter.

2. Bewerten Sie den Schutzbedarf anhand der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit (CIA). Für die Bewertung müssen Sie zunächst festlegen, was man in Ihrem Fall als „Leichte Störung", Erheblicher Schaden" und „Existenzbedrohender Schaden" versteht. Man unterscheiden nur diese drei Kategorien. Legen Sie diese für Ihren Arbeitsbereich fest.

2.1 Vertraulichkeit

Welche Informationen dürfen nur bestimmten Personen zugänglich sein? Erstellen Sie ebenfalls eine Liste. Welche Folgen hätte ein unbefugter Zugriff? Ordnen Sie die gefundenen Informationen den Folgen zu:

- Leichte Störung
    - Allgemeine interne Anweisungen
    - Interne Kommunikationsprotokolle (ohne vertraulichen Inhalt)
- Erheblicher Schaden, wie z. B. Reputationsverlust
    - Kunden- und Geschäftspartnerdaten
    - Finanzberichte
    - Strategische Planungsdokumente
- Existenzbedrohender Schaden
    - Zugangsdaten zu IT-Systemen und Passwörtern
    - Datenbank mit sensiblen personenbezogenen Informationen
    - Betriebsgeheimnisse und Forschungsdaten
    - Notfallpläne und sicherheitskritische Dokumente

2.2 Integrität

Welche Daten oder Systeme müssen frei von Manipulationen sein?

(z. B. Konfigurationsdateien von Systemen, Software-Quellcode, usw.)

Welche Folgen hätte ein unbefugter Zugriff? Ordnen Sie die gefundenen Informationen den Folgen zu:

- Leichte Störung
    - Allgemeine interne Dokumentationen
    - Vorlagen für standardisierte Berichte
    - Nicht-kritische Konfigurationsdateien

- Erheblicher Schaden, wie z. B. Reputationsverlust
    - Kundendatenbanken
    - Software-Quellcode für veröffentlichte Produkte
    - Finanz- und Steuerdaten
    - Kommunikationssysteme und -protokolle

- Existenzbedrohender Schaden
    - Kernsysteme der IT-Infrastruktur (z. B. Server-Konfigurationen, Netzwerkeinstellungen)
    - Software-Quellcode für sicherheitskritische Anwendungen
    - Sicherheits- und Zugriffsprotokolle
    - Datenbanken mit sensiblen oder geschäftskritischen Informationen
    - Backup-Daten

2.3 Verfügbarkeit

Welche Systeme und Daten müssen immer verfügbar sein. Nennen Sie die Systeme, wie z.B. IT-Infrastruktur, Produktions- und Kundensysteme, Email- und Kommunikations-Systeme. Erstellen Sie ebenfalls eine Matrix mit den drei Folgen-Kategorien.

Systeme/Daten	Leichte Störung	Erheblicher Schaden	Existenzbedrohender Schaden
Interne Dokumentationssysteme	X		
Kommunikationssysteme (E-Mail, Chat)		X	
Kundendatenbanken		X	
Produktionssysteme			X
IT-Infrastruktur (z. B. Server, Netzwerke)		X	X
Backup- und Wiederherstellungssysteme			X
CRM-Systeme (Customer Relationship Mgmt.)		X	
Finanzbuchhaltungssysteme		X	

3. Bedrohungen und Schwachstellen auflisten

3.1 Bedrohungen. Nennen Sie Bedrohungen, die durch

- menschliches Fehlverhalten

    - Fehlerhafte Konfiguration von Systemen

    -Unachtsamer Umgang mit Zugangsdaten (z. B. Passwörter notieren oder weitergeben)

    - Unabsichtliches Löschen von Daten

    - Missachtung von Sicherheitsrichtlinien (z. B. Nutzung privater USB-Sticks)

    - Social-Engineering-Angriffe (z. B. durch Phishing)

- technisches Versagen

    - Hardwareausfälle (z. B. Festplatten- oder Serverdefekte)

    - Softwarefehler oder Bugs

- Ausfall von Stromversorgung oder Netzwerkverbindungen
- Datenverluste durch fehlerhafte Backups

- höhere Gewalt (Brand, Feuer, ...)
  - Brand oder Feuer in Betriebsräumen
  - Überschwemmungen oder Wasserschäden
  - Erdbeben oder andere Naturkatastrophen
  - Stromausfälle durch externe Einflüsse

- Cyberangriffe (z. B. Phishing, Malware, Ransomware, Rootkit, ...)
  - Phishing: Täuschung von Nutzern, um Zugangsdaten zu stehlen
  - Malware: Schadsoftware, die Systeme infiziert und Daten manipuliert
  - Ransomware: Verschlüsselung von Daten, um Lösegeld zu fordern
  - Rootkit: Unsichtbare Manipulation von Betriebssystemen zur Übernahme von Kontrolle
  - DDoS-Angriffe: Lahmlegen von Diensten durch Überlastung von Netzwerken
  - Datendiebstahl: Unbefugter Zugriff auf sensible Informationen

entstehen können.

3.2 Wo liegen Schwachstellen in Ihrem Arbeitsbereich? Nennen Sie welche aus den Bereichen:

- Software
- Zugriffsrechten
- Backups
- Physische Sicherheit. (z. B. Zugang zu Räumen)

4. Bewertung des Schutzbedarfs

Ergänzen Sie die unten stehende Tabelle, in der alle Systeme und Daten (sog. Schutzobjekte) aufgelistet werden, die Sie gefunden haben. Ordnen Sie diesen in den Kategorien

„Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“ jeweils einen Schutzbedarfs-Level zu.

5. Maßnahmen ergreifen zur Risikominderung

Überlegen Sie sich zunächst welche

- Technischen
- Organisatorischen und
- Physischen

Maßnahmen Sie treffen können, um die Schutzobjekte schützen zu können.

Listen Sie mindestens fünf Gefährdungen auf und lokalisieren Sie diese in der oben dargestellten Risikomatrix. Die Gefährdungen, die im Bereich „sehr hoch“ liegen müssen mit hoher Priorität angegangen werden, was die Maßnahmen betrifft.

Siehe hierzu auch die Liste „Elementare Gefährdungen“ vom BSI. (Infopool)