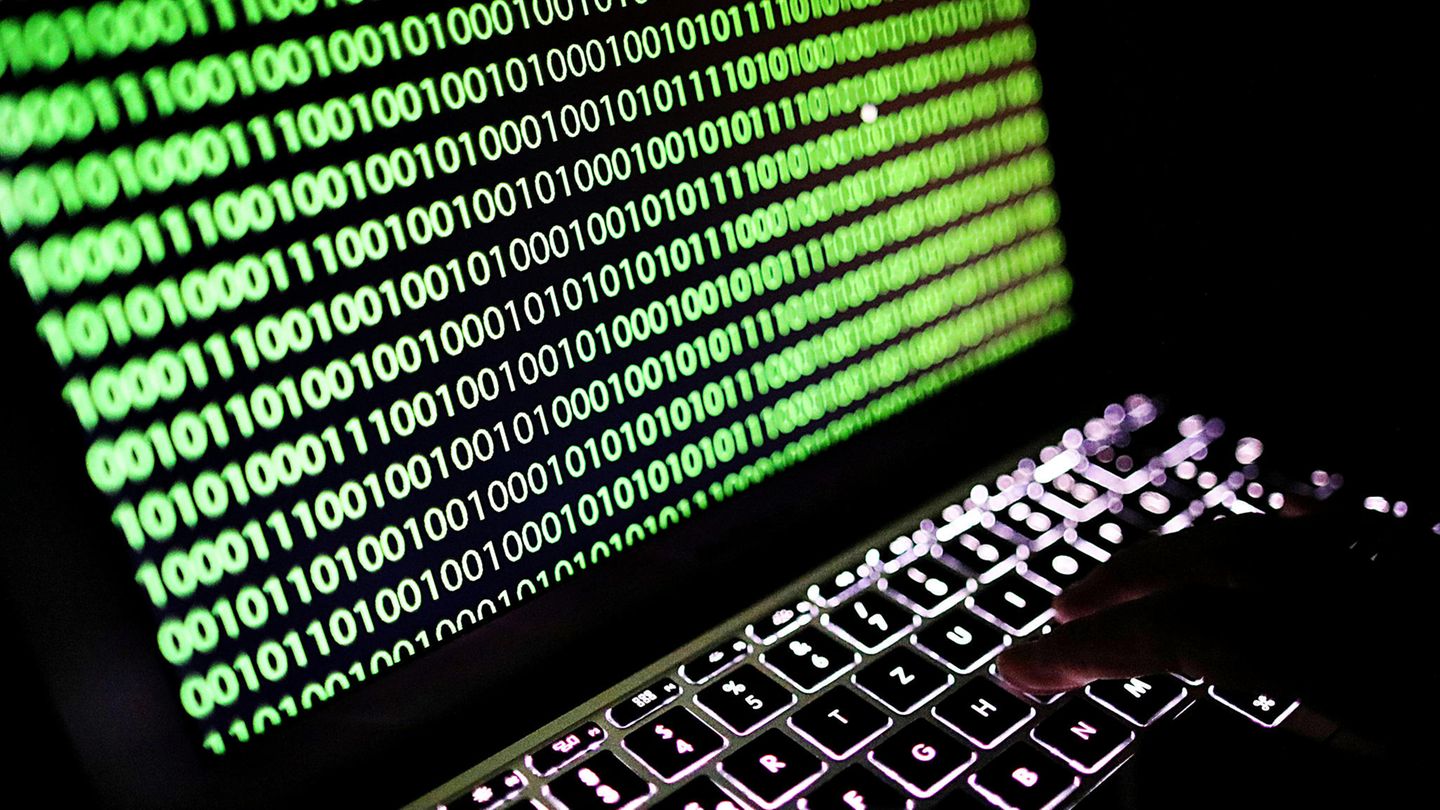
**LS Häcker AG**



**Christian Alexander Knapp,**

**Niklas Engst,**

**Janik Lohyn,**

**Joel Gaudio**

## Aufgabe 1.1:

* Server-Hardware
  + NAS-Array
  + Server
* Netzwerk und dessen Komponenten (Switch, Router, ...)
  + Switch
  + Router
  + DSL
  + WLAN AP
* Arbeitsgeräte (PC, Laptops, ...)
  + Laptops
* Anwendungen und Dienste (z. B. ERP-Systeme, spezielle Software)
* Daten (z. B. Kundendaten, Entwicklungsdaten, Zugangsdaten)

## Aufgabe 1.2:

Es gibt, wie es aussieht keine Datenschnittstellen an externe Partner. Es gibt als Schnittstellen zum externen System durch das VPN, womit sich die Mitarbeiter in das Firmennetz einwählen

## Aufgabe 1.3:

Es besteht keine Dokumentation für zum Beispiel die Server. Die einzige Dokumentation zum Netzwerk ist das Diagramm.

# Aufgabe 2:

Definition der Schadenskategorien:

* **Leichte Störung**: Temporäre Verzögerungen, geringer Reputationsschaden.
* **Erheblicher Schaden**: Finanzielle Verluste, Reputationsverlust.
* **Existenzbedrohender Schaden**: Insolvenz, dauerhafter Vertrauensverlust.

## 2.1 Vertraulichkeit

* **Kundendaten:** Persönliche Informationen, Zahlungsdaten und Verträge.
* **Entwicklungsdaten:** Software-Quellcode, Prototypen und technische Dokumentationen.
* **Zugangsdaten:** Administrator-Passwörter und Zugangsschlüssel zu internen Systemen.
* **Interne Geschäftsunterlagen:** Strategien, Finanzberichte und vertrauliche Korrespondenz.

**Folgen eines unbefugten Zugriffs:**

| **Information** | **Folgen** | **Kategorie** |
| --- | --- | --- |
| Kundendaten | Reputationsverlust | Erheblicher Schaden |
| Entwicklungsdaten | Verlust von Wettbewerbsvorteilen | Existenzbedrohender Schaden |
| Zugangsdaten | Kompromittierung der gesamten IT-Infrastruktur | Existenzbedrohender Schaden |
| Interne Geschäftsunterlagen | Verlust von Vertrauen bei Partnern | Erheblicher Schaden |

## 2.2 Integrität

* **ERP-System:** Für korrekte Geschäftsprozesse und Buchhaltung.
* **Konfigurationsdateien:** Von Servern, Netzwerkgeräten und Anwendungen.
* **Software-Quellcode:** Um sicherzustellen, dass keine Schwachstellen eingefügt werden.
* **Backups:** Um sicherzustellen, dass wiederhergestellte Daten unverändert sind.

**Folgen einer Manipulation:**

| **Daten/Systeme** | **Folgen** | **Kategorie** |
| --- | --- | --- |
| ERP-System | Fehlerhafte Abrechnungen und Prozesse | Erheblicher Schaden |
| Konfigurationsdateien | Ausfall des Netzwerks oder der Systeme | Erheblicher Schaden |
| Software-Quellcode | Sicherheitslücken oder Funktionsausfälle | Existenzbedrohender Schaden |
| Backups | Datenverlust bei Wiederherstellung | Existenzbedrohender Schaden |

## 2.3 Verfügbarkeit

* **IT-Infrastruktur:** Netzwerk, Server und Arbeitsgeräte (PCs).
* **Produktionssysteme:** ERP-Systeme und Entwicklungsumgebungen.
* **Kundensysteme:** Webshop und Kommunikationssysteme (E-Mail, VoIP).

**Matrix der Folgenkategorien für Verfügbarkeit:**

| **Systeme/Daten** | **Leichte Störung** | **Erheblicher Schaden** | **Existenzbedrohender Schaden** |
| --- | --- | --- | --- |
| IT-Infrastruktur | Verzögerte Arbeitsprozesse | Stillstand der Abteilung | Komplettausfall des Unternehmens |
| Produktionssysteme | Verzögerte Lieferung | Vertragsstrafen | Insolvenzgefahr |
| Kundensysteme | Kurzzeitige Nichterreichbarkeit des Webshops | Kundenverlust | Reputationsverlust mit langfristigen Folgen |

Durch die Analyse wird deutlich, dass die Häcker AG insbesondere bei der Vertraulichkeit von Zugangsdaten, der Integrität von Quellcode sowie der Verfügbarkeit von IT-Infrastruktur und Produktionssystemen einen hohen Schutzbedarf hat.

# 3.1 Bedrohungen

## Menschliches Fehlverhalten

* **Unzureichende IT-Dokumentation** – Nur drei Personen haben Wissen über Passwörter und Systeme.
* **Passwörter öffentlich zugänglich** – WLAN-Passwort ist im Konferenzraum an der Pinnwand sichtbar.
* **Mangelhafte Backup-Disziplin** – Backups werden manuell durchgeführt, Risiko von Nachlässigkeit.
* **Falsche Nutzung von Hardware** – Nutzung privater oder nicht verwalteter Geräte für die Arbeit.
* **Unachtsamer Umgang mit sensiblen Daten** – Fehlende Sicherheitsmaßnahmen für Homeoffice-Mitarbeiter.

## Technisches Versagen

* **Single Point of Failure (Netzwerk)** – Ein Router wird als zentraler Switch genutzt, aber niemand traut sich an die Konfiguration.
* **Hitzeprobleme im Serverraum** – Fenster nach Süden, hohe Temperaturen könnten Hardware beschädigen.
* **Kein physischer Schutz der Server** – Server stehen ungesichert im offenen Lagerraum.
* **Veraltete oder ungepatchte Software** – Risiko durch nicht aktualisierte Systeme.

## Höhere Gewalt (Brand, Feuer, etc.)

* **Brandgefahr im Serverraum** – Papierlagerung neben NAS-Laufwerken und Servern erhöht das Risiko.
* **Wasserschäden** – Keine Schutzmaßnahmen gegen Leckagen oder Überschwemmungen.
* **Stromausfälle** – Keine Erwähnung einer unterbrechungsfreien Stromversorgung (USV).

## Cyberangriffe (Phishing, Malware, Ransomware, Rootkit, etc.)

* **Hackerangriff auf Kundendatenbank** – Bereits passiert, zeigt bestehende Schwachstellen.
* **Phishing-Risiko** – Fehlende Schulung der Mitarbeiter könnte zu erfolgreichem Phishing führen.
* **Ransomware-Gefahr** – Unzureichende Backup-Strategie erhöht das Risiko von Datenverlust.
* **IoT-Sicherheitsrisiko** – Smarte Geräte (IoT-Kaffeemaschine, Playstation) im Firmennetzwerk könnten Einfallstore sein.

# 3.2 Schwachstellen im Arbeitsbereich

#### **Software**

* **Ungepatchte oder veraltete Systeme** – Keine Hinweise auf regelmäßige Updates oder Patch-Management.
* **Fehlende Sicherheitssoftware** – Kein expliziter Hinweis auf Firewalls, Antivirus oder Intrusion Detection Systeme.

#### **Zugriffsrechte**

* **Administrationsrechte für alle IT-Admins auf allen Systemen** – Erhöht das Risiko von Insider-Bedrohungen und Fehlkonfigurationen.
* **Unklarheit über Benutzerrollen und Rechtevergabe** – Fehlende Richtlinien für den Zugriff auf sensible Daten.

#### **Backups**

* **Manuelle Backup-Strategie** – Risiko, dass Backups nicht regelmäßig oder korrekt durchgeführt werden.
* **Keine räumliche Trennung der Backups** – NAS steht direkt neben den Servern, Risiko bei Brand oder Diebstahl.

#### **Physische Sicherheit**

* **Offener Serverraum** – Jeder kann auf Server und Backup-Systeme zugreifen.
* **Gäste-PC mit Internetzugang** – Potenzielles Einfallstor für Angriffe.
* **LAN-Anschlüsse im Konferenzraum** – Risiko, dass unautorisierte Personen Zugang zum Firmennetzwerk erhalten.

Diese Punkte sollten in einer Schutzbedarfsanalyse weiter bewertet und priorisiert werden.

### **4. Bewertung des Schutzbedarfs**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Schutzobjekt** | **Vertraulichkeit** | **Integrität** | **Verfügbarkeit** | **Schutzbedarf insgesamt** | | | |
| **Kundendatenbank** | Hoch | Hoch | Mittel | Hoch | | | |
| **E-Mail-System** | Mittel | Hoch | Hoch | Hoch | | | |
| **Entwickler-PCs** | Mittel | Hoch | Mittel | Mittel | | | |
| **Unternehmensserver** | Hoch | Hoch | Hoch | Hoch | | | |
| **Backups** | Hoch | Hoch | Hoch | Hoch | | | |
| **Netzwerkkomponenten** (Router, Switches) | Mittel | Hoch | Hoch | Hoch | | | |
| **Zugangsdaten (Passwörter, API-Keys)** | Hoch | Hoch | Mittel | Hoch | | | |
| **ERP-System** (zentrales Verwaltungssystem) | | | | Hoch | Hoch | Hoch | Hoch |
| **Dokumentationsserver** | | | | Mittel | Hoch | Mittel | Mittel |
| **Homeoffice-Zugänge (VPN, Remote-Desktop)** | | | | Hoch | Hoch | Mittel | Hoch |
| **IoT-Geräte im Netzwerk (Smart-Kaffeemaschine, Playstation)** | | | | Niedrig | Niedrig | Mittel | Niedrig |
| **Gäste-PC mit Internetzugang** | | | | Niedrig | Niedrig | Niedrig | Niedrig |

### **5. Gefährdungen und Risikoeinstufung**

| **Gefährdung** | **Eintrittshäufigkeit** | **Schadenhöhe** | **Risikostufe** |
| --- | --- | --- | --- |
| **Phishing-Angriffe** | häufig | hoch | sehr hoch |
| **Ausfall des Unternehmensservers** | mittel | hoch | hoch |
| **Diebstahl von Entwickler-PCs** | selten | mittel | mittel |
| **Brand im Serverraum** | selten | existenzbedrohend | hoch |
| **Ungepatchte Software-Schwachstellen** | häufig | mittel | hoch |

### **5.1 Maßnahmen zur Risikominderung**

#### **1. Technische Maßnahmen:**

* **Phishing-Angriffe:** Einsatz von Spam-Filtern, Multi-Faktor-Authentifizierung (MFA) und regelmäßige Software-Updates.
* **Ungepatchte Software-Schwachstellen:** Automatische Updates und Patch-Management einführen.
* **Ausfall des Unternehmensservers:** Redundante Systeme und Cloud-Backups nutzen.

#### **2. Organisatorische Maßnahmen:**

* **Phishing-Angriffe:** Mitarbeiterschulungen zur Erkennung von Phishing-Mails.
* **Brand im Serverraum:** Notfallpläne und regelmäßige Brandschutzübungen einführen.
* **Diebstahl von Entwickler-PCs:** Einführung einer Verschlüsselung und Zugriffsbeschränkungen.

#### **3. Physische Maßnahmen:**

* **Brand im Serverraum:** Feuerlöscher bereitstellen, Server in brandgeschützten Raum verlegen.
* **Diebstahl von Entwickler-PCs:** Sicherheitsmaßnahmen wie abschließbare Büros und Alarmanlagen einführen.