Aufgabe 1.1

Server Hardware: NAS-Laufwerke, Server

Netzwerk und dessen Komponenten: Zentraler Switch(Router), DSL-Anschluss, IoT-Geräte(Playstation und Kaffe-Maschine), WLAN

Arbeitsgeräte: PCs, VoIP-Telefone, ein PC für Besucher

Anwendungen und Dienste: Home-Office Zugang auf Firmendaten

Daten: Kundendaten, Zugangsdaten, Sicherungsdaten

Aufgabe 1.2

Interne: Home-Office, Stammhaus

Externe: Kaffee-Maschine und Playstation

Aufgabe 1.3

Es gibt keine vollständige Dokumentation über die Struktur.

Es gibt 3 Personen, die mit Passwörtern und Systemen sich sehr gut auskennen.

Manuelle Backups von NAS-Laufwerken wöchentlich

Aufgabe 2

1. Leichte Störung:

Kleinere Verzögerungen oder Ausfallzeiten

2. Erheblicher Schaden:

Finanzielle Verluste

Verluste von Kundendaten

3. Existenzbedrohender Schade:

Verlusten von privaten Kundendaten oder Geschäftsgeheimnisse

Längere Ausfällen der Systeme

Kunden Vertrauen uns nicht mehr

Aufgabe 2.1

Leichte Störung->Projektinformationen

Erheblicher Schaden->Geschäftsgeheimnisse

Existenzbedrohender Schaden->Kundendaten und Zugangsdaten

Aufgabe 2.2

Leichte Störung->Entwicklungsdaten

Erheblicher Schaden->Konfigurationsdateien

Existenzbedrohender Schaden->Backups

Aufgabe 2.3

IT-Infrastruktur: DSL-Anschluss, WLAN und Server

Kommunikationssysteme: E-Mail, VoIP-Telefone

Kundensysteme: Systeme für Betrieb und Angebote

Daten/Systeme	Leichte Störung	Erheblicher Schaden	Existenzbedrohender Schaden
IT-Infrastruktur		x	X
Kommunikationssysteme	X	x	
Kundensysteme	x	X	x

Aufgabe 3.1

Menschliches Fehlverhalten:

1. Fehlerhafte Konfigurationen-> Switch als Router
2. Regelmäßige Backups nicht ausgeführt
3. Alte Hardware und Systeme

Technisches Versagen:

1. Überhitzung des Servers

Höhere Gewalt:

1. Brand oder Überschwemmung

Cyberangriffe:

1. Phishing Angriffe
2. Vieren

Aufgabe 3.2

Software:

1. Netzwerke sind nicht getrennt

Zugriffsrechte:

1. 3 Admins mit allen Rechten (erhöht das Risiko)
2. Kennwörter nicht sicher bewahren (an der Pinnwand)

Backups:

1. Werden manuell gemacht-> man kann es mal vergessen zu machen
2. Server Raum nicht zugeschlossen

Physische Sicherheit:

1. Serverraum nicht gesichert
2. PC für Kunden ein Punkt für Angriffe

Aufgabe 4

Schutzobjekt	Vertraulichkeit	Integrität	Verfügbarkeit	Schutzbedarf insgesamt
Kundendatenbank	Hoch	Hoch	Mittel	Hoch
E-Mail-System	Mittel	Mittel	hoch	hoch
Entwickler-PCs	Hoch	Hoch	Hoch	Hoch
Backups	mittel	hoch	hoch	Hoch
Kunden PC	Niedrig	Mittel	mittel	Mittel
Kaffee Maschine und Playstation	Gering	Mittel	gering	gering

Aufgabe 5

Technische Maßnahmen:

a. Zugriffsrechte->jeder Mitarbeiter soll nur die Rechte haben, die er braucht, z.B. die wichtigen Passwörter benötigen nicht alle 3 Admins
b. Netzwerksicherheit->Kunden-PC, Playstation und Kaffeemaschinen auf einem separaten Netzwerk
c. Backups automatisch machen

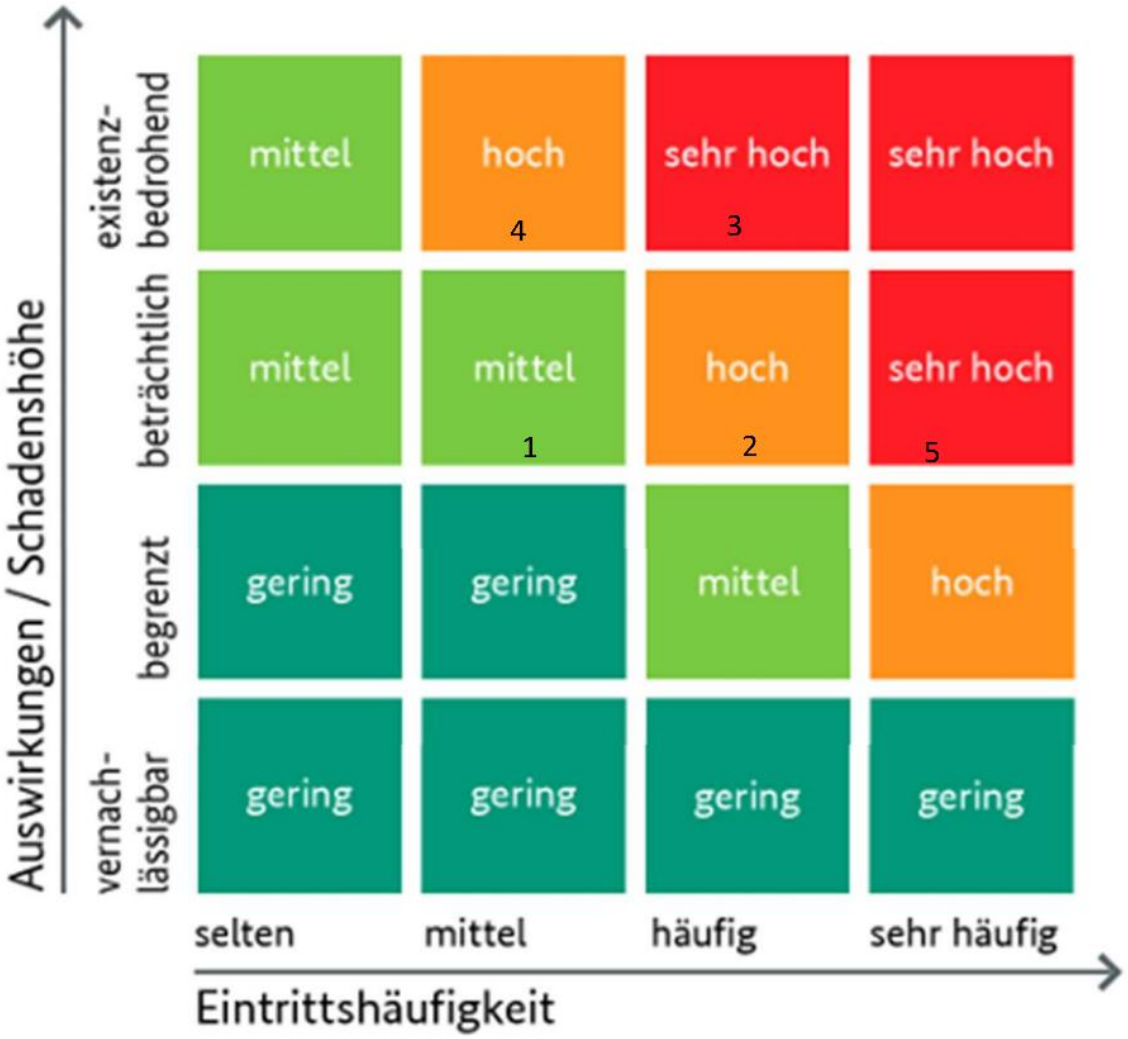
Organisatorische Maßnahmen:

a. Sicherheitsrichtlinien einführen->Schulungen für Mitarbeiter und regelmäßiges Update der Software

Physische Maßnahmen:

a. Serverraum schließen
b. Kühlung für den Server
c. Kunden-PC nicht im selben Netzwerk haben

1. Keine Datensicherung durch das Vergessen von Back-Ups
2. Überhitzung des Servers
3. Malware durch den Kunden-PC
4. Phishing E-Mails
5. Viele haben Zugriff auf die wichtigen Daten->Häufigkeit der Fehler wird erhöht


Auswirkungen / Schadenshöhe
existenz-bedrohend
beträchtlich
begrenzt
vernach-lässigbar
mittel
hoch
4
sehr hoch
3
sehr hoch
mittel
mittel
1
hoch
2
sehr hoch
5
gering
gering
mittel
hoch
gering
gering
gering
gering
selten
mittel
häufig
sehr häufig
Eintrittshäufigkeit