# 1. Rapport Timo Ruben

Erstellt von Ju[redacted]& Fl[redacted], 31.01.2025

Dieses Dokument ist eine Sicherheitsüberprüfung der IT-Infrastruktur mit Fokus auf Schwachstellenanalyse & Massnahmenvorschläge.

**Wichtige Punkte:**

| Fehlender Punkt | Empfolende Massnahme |
|---|---|
| **Unzureichende Dokumentation von USV-Wattzahlen** → Risiko eines Ausfalls im Notfall. | Führen Sie eine Lastberechnung durch, um sicherzustellen, dass die USV alle kritischenKomponenten im Notfall versorgen kann. Dokumentieren Sie die Ergebnisse in der Netzwerkinfrastruktur- Dokumentation & im Netzwerkplan. |
| **Brandschutzmassnahmen in den EDV-Räumen** fehlen oder sind unklar. | Überprüfen Sie die bestehenden Brandschutzvorrichtungen (z.B. Rauchmelder, Feuerlöscher) & führen Sie gegebenenfalls eine Brandschutzinspektion durch. Stellen Sie sicher, dass alle Mitarbeiter über die Brandschutzmassnahmen informiert sind. |
| **Unklare ISMS-Planung** → Keine klare Abgrenzung, welche Netzwerkteile abgesichert werden. | Definieren Sie den Umfang des ISMS & identifizieren Sie die spezifischen Teile des Netzwerks, die abgedeckt werden sollen. Dokumentieren Sie dies in einem ISMS-Plan. |
| **Kein Backup für Firewalls** → Risiko eines Netzwerkausfalls bei Störung. | Implementieren Sie eine Hochverfügbarkeitslösung (HA) für Firewalls, einschliesslich automatischer Failover-Mechanismen. Erstellen Sie regelmässige Backups der Firewall-Konfiguration & dokumentieren Sie diese Verfahren. |
| **Nicht dokumentierte VPN-Verschlüsselung** → Gefahr veralteter oder unsicherer Verschlüsselung. | Überprüfen Sie die implementierte Verschlüsselung (z.B. AES-256) für die VPN-Verbindungen & stellen Sie sicher, dass sie den aktuellen Sicherheitsstandards entspricht. Dokumentieren Sie die verwendeten Protokolle & Verschlüsselungsmethoden. |
| **Fehlende Antivirus-Strategie für Clients** → Risiko von Malware-Infektionen. | Erstellen & dokumentieren Sie eine umfassende Antivirus-Strategie, die regelmässige Updates, Scans & Schulungen für Benutzer umfasst. Halten Sie diese Informationen in einer zentralen Sicherheitsdokumentation fest. |

| | |
|---|---|
| **Fehlende Dokumentation der Softwareverwaltung** → Gefahr unsicherer oder nicht autorisierter Software. | Implementieren Sie ein Softwaremanagement-System, das alle Installationen dokumentiert & genehmigt. Führen Sie regelmässige Audits durch, um sicherzustellen, dass nur autorisierte Software installiert ist. |
| **Unklarheiten bei der Videoüberwachung** → Kein dokumentiertes VLAN/Subnetz für Überwachungssysteme. | Überprüfen Sie das bestehende Videoüberwachungssystem auf Funktionalität & Abdeckung der kritischen Bereiche. Stellen Sie sicher, dass alle Aufzeichnungen gemäss den Datenschutzrichtlinien behandelt werden. |
| **Fehlende standortspezifische Firewall-Regeln** → Erhöhtes Risiko durch uneinheitliche Sicherheitsrichtlinien. | Dokumentieren Sie das VLAN & Subnetz, in dem sich das Videoüberwachungssystem befindet, um sicherzustellen, dass es von anderen Netzwerksegmenten getrennt ist & Sicherheitsrichtlinien eingehalten werden. |

**Tests:**

**Interner Netzwerkscan**

- Ziel: Überprüfen der Sicherheit und Erreichbarkeit aller Geräte innerhalb des internen Netzwerks.

Tools:

- Nmap: Ein leistungsstarkes Tool zum Scannen von Netzwerken, das Informationen über aktive Hosts, offene Ports und Dienste liefert.
- Angry IP Scanner:
  - Ein einfaches Tool zur schnellen Erkennung aktiver IP-Adressen im Netzwerk.

**Externer Netzwerkscan**

- Ziel: Überprüfen der Sicherheitskonfigurationen von externen Zugriffspunkten (z.B. Firewalls, Router).

Tools:

- Nessus: Ein umfassendes Vulnerability-Scanning-Tool, das Schwachstellen im externen Netzwerk identifizieren kann.
- OpenVAS: Eine Open-Source-Alternative zu Nessus, die ebenfalls Schwachstellen im Netzwerk aufdecken kann.

**Backup-Wiederherstellungstest**

- Ziel: Überprüfen der Funktionsfähigkeit des Backup-Systems und der Wiederherstellungsprozesse.

Tools:

- Veeam Backup & Replication: Ein Tool zur Verwaltung und Durchführung von Backup Wiederherstellungen.
- TERRA Cloud Management Console: Zum Testen der Wiederherstellung von Backups aus der Cloud.

**Firewall-Konfigurationstest**

- Ziel: Überprüfen der Firewall-Regeln und deren Wirksamkeit.

Tools:

- GFI Languard: Ein Tool zur Überprüfung von Firewall-Regeln und zur Durchführung von Sicherheitsüberprüfungen.
- Netcat: Ein einfaches Tool zur Durchführung von Portscans und zum Testen der Erreichbarkeit bestimmter Ports.

---

## 2. "Sicherheitsbericht IT-Infrastruktur"

Dieser Bericht bewertet die IT-Sicherheitsmassnahmen des Unternehmens mit einem Punktesystem (1-8) & schlägt Verbesserungen vor.

**Hauptergebnisse:**

1. **Netzwerk- & Zugriffssicherheit (6/8)**
    - Positiv: **OPNSense-Firewalls**, **WireGuard VPN**, VLAN-Segmentierung in Planung.
    - Schwächen: **Unvollständige VLAN-Segmentierung**, **keine Netzwerkscan-Protokolle**.
    - Verbesserung: **Erweiterung der VLAN-Segmentierung, regelmässige Netzwerkscans mit Nmap/OpenVAS**.
2. **Authentifizierung & Zugriffskontrolle (7/8)**
    - Positiv: **Zentrale Benutzerverwaltung mit Active Directory (AD), Self-hosted Bitwarden**.
    - Schwächen: **Kein Multi-Faktor-Authentifizierung (MFA), Standardpasswörter zu schwach**.
    - Verbesserung: **MFA für Admin-Konten, längere Passwortvorgaben (mind. 14 Zeichen)**.
3. **Datensicherung & Disaster Recovery (8/8)**
    - Positiv: **3-2-1 Backup-Strategie mit Hetzner/NAS, DR-Plan mit RTO/RPO-Werten**.
    - Schwächen: **Kein automatisierter DR-Test, keine Immutable Backups**.
    - Verbesserung: **Automatisierte Tests mit Veeam SureBackup, Aktivierung von Immutable Backups**.
4. **Endpoint-Sicherheit & Monitoring (5/8)**
    - Positiv: **Security Awareness-Schulungen, Firewall-Logging mit Zabbix**.
    - Schwächen: **Keine EDR/XDR-Lösung, kein zentrales Patch-Management**.
    - Verbesserung: **Einführung einer Endpoint-Security-Lösung wie Microsoft Defender for Endpoint**.
5. **Externe Angriffe & Penetrationstests (4/8)**
    - Positiv: **Geplante Audits & Penetrationstests**.
    - Schwächen: **Noch keine Tests durchgeführt, keine Behebung früherer Schwachstellen dokumentiert**.
    - Verbesserung: **Regelmässige externe & interne Penetrationstests alle 6 Monate, internes Red Team etablieren**.

**Empfohlene Massnahmen gemäss Sicherheitsbericht (Prioritäten):**

| Bereich | Massnahme | Priorität |
|---|---|---|
| **Netzwerk-Sicherheit** | VLAN-Segmentierung abschliessen | Hoch |
| **Zugriffskontrolle** | MFA für Admin-Konten | Hoch |
| **Backup-Strategie** | Immutable Backups aktivieren | Hoch |
| **Endpoint-Sicherheit** | EDR/XDR für Endgeräte einführen | Mittel |
| **Sicherheitsüberprüfung** | Regelmässige Netzwerkscans | Hoch |
| **Notfallplanung** | Automatisierte DR-Tests implementieren | Mittel |
| **Penetrationstests** | Jährliche externe & halbjährliche interne Tests | Hoch |

**Gesamtnote: 7/8**

- **Gute IT-Sicherheit**, aber Verbesserungen notwendig in **Netzwerksegmentierung, Endpoint-Sicherheit & Penetrationstests**.
- **Empfohlene nächste Schritte**:
    1. **Verantwortlichkeiten zuweisen**
    2. **Zeitplan für Umsetzung erstellen**
    3. **Regelmässige Sicherheitsüberprüfungen durchführen**

---