5 Sicherheitslücken, die wir bei nahezu jedem KMU finden

Cyberangriffe treffen längst nicht mehr nur Konzerne. Mittelständische Unternehmen sind besonders attraktiv – weil sie wertvolle Daten besitzen, aber oft keine vollständige Sicherheitsvalidierung durchführen.

---

1. Ungeschützte oder falsch konfigurierte Active Directory Strukturen

- Überprivilegierte Benutzerkonten
- Fehlende Netzwerksegmentierung
- Keine regelmäßige Rechte-Überprüfung
- Legacy-Protokolle weiterhin aktiv

Warum das kritisch ist: Ein kompromittierter Benutzer kann sich oft innerhalb weniger Minuten bis zum Domain-Admin hocharbeiten.

---

2. Öffentlich erreichbare Systeme mit bekannten Schwachstellen

- Veraltete VPN-Gateways
- Nicht gepatchte Webserver
- Offene Verwaltungsports
- Unsichere SSL-Konfigurationen

Warum das kritisch ist: Exponierte Dienste sind der häufigste Einstiegspunkt für Ransomware-Angriffe.

---

3. Schwache E-Mail-Sicherheit & fehlende DMARC-Konfiguration

- Kein korrekt gesetztes SPF / DKIM

- DMARC nicht aktiv oder auf "none"
- Keine Anti-Spoofing-Absicherung
- Fehlende Awareness im Unternehmen

Warum das kritisch ist: Angreifer können unter Ihrer Domain Rechnungen oder Zahlungsanweisungen versenden.

---

4. Webapplikationen ohne tiefgehende Sicherheitsprüfung

- Fehlende Zugriffskontrollen
- IDOR-Schwachstellen
- Schwache Authentifizierungsmechanismen
- Business-Logic-Fehler

Warum das kritisch ist: Kundendaten, Vertragsinformationen oder interne Dashboards sind oft unerwartet zugänglich.

---

5. Keine getestete Backup- und Wiederherstellungsstrategie

- Backups werden nie zurückgespielt
- Keine Offline- oder Immutable-Backups
- Unklare Wiederanlaufzeiten
- Backup-Systeme nicht segmentiert

Warum das kritisch ist: Viele Unternehmen haben Backups – aber keine funktionierende Wiederherstellungsstrategie.

Fazit: Sicherheit beginnt nicht mit einem Tool – sondern mit einer realistischen Bewertung der eigenen Angriffsfläche. Wer seine Schwachstellen kennt, kann Risiken gezielt reduzieren – bevor es teuer wird.