# IT-Sicherheits-Checkliste für KMU

10 Punkte, die jeder Betrieb prüfen sollte — schnell, praxisnah, ohne Fachchinesisch.

RÖSCHI
IT- Systems & Security

Die meisten Sicherheitsvorfälle in kleinen und mittleren Unternehmen entstehen nicht durch gezielte Angriffe, sondern durch breit gestreute, automatisierte Attacken, die einfach die nächste offene Tür finden. **Gehen Sie diese zehn Punkte durch, kreuzen Sie an, was bei Ihnen schon sicher ist — und sehen Sie sofort, wo noch Handlungsbedarf besteht.**

- [ ] 1 **Starke Passwörter & Zwei-Faktor-Authentifizierung**
  Passwort-Manager im Einsatz, individuelle Passwörter pro Account, 2FA überall dort aktiv, wo es möglich ist.

- [ ] 2 **Software-Updates & Patch-Management**
  Betriebssysteme, Browser, Fachsoftware und Router-Firmware laufen automatisch oder regelmäßig auf dem neuesten Stand.

- [ ] 3 **Datensicherung nach der 3-2-1-Regel**
  Mind. 3 Kopien, auf 2 verschiedenen Medien, 1 davon offline/unveränderlich extern gelagert (z. B. S3) — und regelmäßig auf Wiederherstellbarkeit geprüft.

- [ ] 4 **Moderne Endpoint-Security & Managed Detection & Response**
  EDR/XDR erkennt auffälliges Verhalten und Ransomware in Echtzeit — im Managed-Betrieb (MDR) rund um die Uhr von Sicherheitsspezialisten überwacht.

- [ ] 5 **Firewall & abgesichertes Netzwerk**
  Firewall korrekt konfiguriert, WLAN mit starkem Passwort, separates Gäste-WLAN ohne Zugriff auf interne Systeme.

- [ ] 6 **Mitarbeitersensibilisierung gegen Phishing**
  Team kennt aktuelle Betrugsmaschen und weiß: Bei Zahlungsanfragen lieber einmal zu viel telefonisch nachfragen.

# Fortsetzung: Punkte 7 – 10

☐ **7** **Zugriffsrechte nach dem Prinzip der geringsten Berechtigung**
Jede:r hat nur Zugriff auf das, was für die eigene Aufgabe nötig ist — Rechte werden bei Austritt/Wechsel sofort angepasst.

☐ **8** **Sichere mobile Geräte & Homeoffice**
Festplattenverschlüsselung, Bildschirmsperre, VPN-Zugriff und klare Regeln für private Geräte (BYOD) sind Standard.

☐ **9** **Notfallplan & klare Verantwortlichkeiten**
Es ist schriftlich festgelegt, wer im IT-Notfall was tut — inklusive Kontaktliste, auch offline verfügbar.

☐ **10** **Regelmäßige Überprüfung des Sicherheitsstands**
Mindestens einmal jährlich wird der eigene Stand strukturiert geprüft, z. B. mit dem CyberRisikoCheck nach DIN SPEC 27076.

### So werten Sie Ihr Ergebnis

8–10 Häkchen: Solide Basis — regelmäßig weiter prüfen. 5–7 Häkchen: Erste Lücken schließen, bevor sie teuer werden. Unter 5 Häkchen: Zeitnah handeln — hier lohnt sich ein professioneller Blick von außen.

## Fragen offen? Wir schauen gemeinsam drauf.

**Röschi Systems & Security** unterstützt kleine und mittlere Unternehmen dabei, aus dieser Checkliste ein alltagstaugliches Sicherheitskonzept zu machen — von der ersten Einschätzung bis zur laufenden Betreuung Ihrer IT. Sprechen Sie uns einfach an.