IT-Sicherheits-Checkliste für kleine Unternehmen

24 Punkte, mit denen Sie den Stand Ihrer IT-Sicherheit selbst einschätzen können.

> So nutzen Sie die Liste: Haken Sie jeden Punkt ab, den Sie sicher mit „Ja“ beantworten können. Offene Punkte sind Ihre Prioritäten. Die Liste ist eine erste Orientierung und ersetzt weder einen Penetrationstest noch eine Rechtsberatung.

1. Zugänge & Passwörter

- [ ] Für jeden Dienst gibt es ein eigenes, langes Passwort (Passwortmanager im Einsatz).
- [ ] Mehrfaktor-Authentifizierung ist für E-Mail, Cloud-Dienste und Administratorkonten aktiv.
- [ ] Wo möglich, werden Passkeys oder Hardware-Schlüssel statt Passwörtern genutzt.
- [ ] Standardpasswörter bei Routern, Druckern und Kameras wurden geändert.

2. Updates & Software

- [ ] Betriebssysteme, Browser und Programme werden automatisch aktualisiert.
- [ ] Geräte und Software ohne Herstellersupport sind ausgetauscht oder isoliert.
- [ ] Es gibt eine Liste aller genutzten Geräte, Programme und Cloud-Dienste.
- [ ] Nicht mehr benötigte Programme und Benutzerkonten werden entfernt.

3. Datensicherung

- [ ] Wichtige Daten werden regelmäßig gesichert, mindestens eine Kopie liegt getrennt vom Netzwerk (offline oder unveränderbar).
- [ ] Die Wiederherstellung wurde mindestens einmal praktisch getestet.
- [ ] Es ist festgelegt, welche Daten wie lange wiederhergestellt werden müssen.

4. E-Mail & Mitarbeiter

- [ ] Mitarbeiter wissen, wie man Phishing erkennt und an wen verdächtige Mails gemeldet werden.
- [ ] Für Zahlungsanweisungen und Kontoänderungen gilt eine Rückfrage über einen zweiten Kanal (z. B. Rückruf).
- [ ] Es gibt eine klare Regel, welche KI-Dienste mit welchen Daten genutzt werden dürfen.
- [ ] Niemand führt Befehle aus, die eine Webseite zum Kopieren und Einfügen anzeigt.

5. Geräte & Netzwerk

- [ ] Laptops und Smartphones sind verschlüsselt und per PIN oder Biometrie gesperrt.
- [ ] Auf allen Geräten läuft ein aktueller Virenschutz bzw. eine Endpoint-Lösung.
- [ ] Das WLAN ist mit WPA2/WPA3 gesichert; Gäste nutzen ein getrenntes Netz.
- [ ] Der Fernzugriff (VPN, Remote-Desktop) ist abgesichert und nicht offen aus dem Internet erreichbar.

6. Rechte & Notfall

- [ ] Mitarbeiter haben nur die Zugriffsrechte, die sie für ihre Arbeit brauchen.
- [ ] Beim Ausscheiden von Mitarbeitern werden Zugänge am selben Tag gesperrt.
- [ ] Ein Notfallplan nennt, wen Sie bei einem Vorfall anrufen und was zuerst zu tun ist.
- [ ] Eine Meldepflicht (z. B. DSGVO, NIS2) wurde geprüft und ist der verantwortlichen Person bekannt.
- [ ] Die eigene Website und die Systeme wurden schon einmal von unabhängiger Seite geprüft.

Wie viele Punkte sind offen? Gern bespreche ich mit Ihnen in einem kostenlosen 20-Minuten-Erstgespräch, wo der größte Hebel liegt.
christian-noack.com/contact.html · admin@christian-noack.com