

IT-Security Checkliste für Geschäftsführer (KMU)

Ziel: Überblick über den Sicherheitsstatus Ihres Unternehmens – einfach, verständlich, versicherungsrelevant.

Zugangssicherheit

- ☐ Alle Mitarbeitenden haben individuelle Benutzerkonten (kein Teilen von Zugängen).
- ☐ Ein Passwortmanager (z. B. Keeper, Bitwarden, 1Password) ist im Einsatz, um die Einhaltung sicherer, einzigartiger Passwörter zu gewährleisten.
- ☐ Multi-Faktor-Authentifizierung (MFA) ist für alle sicherheitsrelevanten Anwendungen aktiviert (z. B. E-Mail, Cloud, Remote-Zugriffe).
- ☐ Zugriffsrechte werden regelmäßig überprüft und veraltete Konten deaktiviert.

Arbeitsplatzsicherheit

- ☐ Alle PCs/Laptops verfügen über ein aktuelles Antivirenprogramm, das automatische Updates erhält.
- ☐ Automatische Bildschirmsperre nach Inaktivität ist aktiv (max. 5 Minuten).
- ☐ Alle Systeme und Programme werden regelmäßig aktualisiert (idealerweise zentral gesteuert).
- ☐ USB-Geräte sind beschränkt oder kontrolliert freigegeben, um Schadsoftware zu vermeiden.

Netzwerk & Internet

- ☐ Eine moderne Firewall schützt das Unternehmensnetzwerk (Hardware oder professionelle Lösung).
- ☐ VPN-Zugänge sind nur dort eingerichtet, wo kein direkter Cloud-Zugriff möglich ist (z. B. für lokale Server oder Systeme).
- ☐ Gast-WLAN ist vom Firmen-WLAN getrennt, um interne Systeme zu schützen.
- ☐ Verdächtiger Datenverkehr wird erkannt (z. B. durch UTM-Firewalls oder EDR-Lösungen).

Backups & Wiederherstellung

- ☐ Backups aller wichtigen Daten erfolgen automatisiert und mindestens täglich.
- ☐ Backups sind physisch oder logisch getrennt gespeichert (z. B. in der Cloud mit Ransomware-Schutz oder offline).
- ☐ Rücksicherung der Backups wurde in den letzten 3 Monaten erfolgreich getestet.

Richtlinien & Sensibilisierung

- ☐ Es existieren klare Regeln zur IT-Nutzung (z. B. für E-Mail, Internet, Passwortverwendung).
- ☐ Mitarbeitende erhalten mindestens 1x jährlich IT-Sicherheitsschulungen, z. B. zu Phishing, Passwortnutzung und Verhalten im Ernstfall.
- ☐ Es gibt ein definiertes Verfahren zur Meldung von Sicherheitsvorfällen.

Notfallvorsorge & Verantwortlichkeiten

- ☐ Ein IT-Notfallplan ist vorhanden, der Zuständigkeiten und Abläufe im Ernstfall beschreibt.
- ☐ Eine verantwortliche Person für IT-Sicherheit ist benannt (intern oder extern).
- ☐ Wichtige IT-Kontakte sind dokumentiert (IT-Dienstleister, Versicherer, Datenschutzbeauftragter).
- ☐ Eine Cyber-Versicherung ist vorhanden, und deren Mindestanforderungen werden erfüllt.

Selbstbewertung

Bereich **Bewertung** **Kommentar**

Zugangssicherheit   

Arbeitsplatzsicherheit   

Netzwerk & Internet   

Backups &
Wiederherstellung   

Richtlinien & Schulung   

Notfallvorsorge   

 = OK |  = Verbesserung nötig |  = kritisch