

Cyber-Security-Checkliste für KMU

IT-Sicherheit Schritt für Schritt, auch ohne eigenes Security-Team

Diese Checkliste richtet sich an Geschäftsführung und IT-Verantwortliche in kleinen und mittleren Unternehmen. Sie deckt die wichtigsten Grundmaßnahmen ab, von Passwörtern über Backups bis zum Notfallplan. Gehen Sie die Punkte in Ruhe durch und haken Sie ab, was bei Ihnen schon passt.

Passwörter und Zugänge

- ☐ Führen Sie einen Passwort-Manager ein und nutzen Sie für jeden Dienst ein eigenes, langes Passwort.
Ohne Passwort-Manager sind eigene Passwörter pro Dienst im Alltag nicht durchzuhalten.
- ☐ Aktivieren Sie Multi-Faktor-Authentifizierung (MFA) zumindest für E-Mail, Cloud-Dienste und Fernzugriffe.
- ☐ Ändern Sie Standardpasswörter auf Routern, Druckern, NAS und anderen Geräten.
- ☐ Vergeben Sie Administrator-Rechte nur an Personen, die sie wirklich brauchen.
Für die tägliche Arbeit reicht ein normales Benutzerkonto.
- ☐ Vermeiden Sie Sammelkonten. Jede Person arbeitet mit einem eigenen Zugang.
- ☐ Sperren Sie beim Austritt von Mitarbeitern alle Zugänge noch am letzten Arbeitstag.
Eine fixe Offboarding-Liste stellt sicher, dass kein Konto vergessen wird.

Geräte und Updates

- ☐ Führen Sie eine einfache Liste aller Geräte, Programme und wichtigen Konten.
Was man nicht kennt, kann man nicht schützen.
- ☐ Aktivieren Sie automatische Updates für Betriebssysteme, Browser und Anwendungen.
- ☐ Ersetzen Sie Software und Geräte, für die es keine Sicherheitsupdates mehr gibt.
- ☐ Stellen Sie sicher, dass auf allen Rechnern ein aktiver Virenschutz läuft.
Unter Windows reicht dafür der eingebaute Microsoft Defender.
- ☐ Aktivieren Sie die Festplattenverschlüsselung auf allen Laptops.
Unter Windows BitLocker oder Geräteverschlüsselung, bei Apple FileVault. Aktuelle Smartphones sind meist ab Werk verschlüsselt.
- ☐ Stellen Sie auf allen Geräten eine automatische Bildschirmsperre ein.

Datensicherung

- ☐ Sichern Sie Ihre Daten nach der 3-2-1-Regel.
Drei Kopien, zwei verschiedene Speichermedien, eine Kopie außer Haus.
- ☐ Automatisieren Sie die Backups.
Manuelle Sicherungen werden im Alltag erfahrungsgemäß vergessen.
- ☐ Halten Sie mindestens eine Backup-Kopie vom Netzwerk getrennt.
So übersteht sie auch einen Verschlüsselungstrojaner.
- ☐ Testen Sie die Wiederherstellung mindestens zweimal pro Jahr.
Ein Backup zählt erst, wenn die Rücksicherung nachweislich funktioniert.

Netzwerk und WLAN

- ☐ Richten Sie ein eigenes Gäste-WLAN für Besucher und private Geräte ein.
- ☐ Sichern Sie das Firmen-WLAN mit WPA2 oder WPA3 und einem langen Passwort.
- ☐ Erlauben Sie Zugriffe von außen auf das Firmennetz nur über VPN.
- ☐ Halten Sie die Firmware von Router und Firewall aktuell.

Phishing und E-Mail

- ☐ Schulen Sie Ihr Team mindestens zweimal pro Jahr im Erkennen von Phishing-Mails.
Kurze Einheiten mit echten Beispielen wirken besser als eine lange Schulung pro Jahr.
- ☐ Bestätigen Sie Zahlungsanweisungen und geänderte Kontodaten immer telefonisch über eine bekannte Nummer.
- ☐ Legen Sie fest, an wen verdächtige Mails gemeldet werden.
Wer meldet, darf keine Nachteile fürchten. Auch dann nicht, wenn schon geklickt wurde.

Notfall und Lieferanten

- ☐ Erstellen Sie eine Notfallliste: Wer wird intern verständigt und wer ist der externe IT-Ansprechpartner.
Auch ausgedruckt aufbewahren. Im Ernstfall sind die Systeme vielleicht nicht erreichbar.
- ☐ Dokumentieren Sie bei einem Vorfall von Beginn an Zeitpunkt, betroffene Systeme und gesetzte Maßnahmen.
- ☐ Klären Sie vorab, wann eine Datenpanne an die Datenschutzbehörde zu melden ist.
Nach DSGVO gilt dafür in der Regel eine Frist von 72 Stunden.
- ☐ Prüfen Sie, ob Ihr Unternehmen ab Oktober 2026 unter das NISG 2026 (NIS2) fällt.
Das Gesetz gilt ab 1. Oktober 2026 für mittlere und größere Unternehmen in 18 Sektoren, betroffene Betriebe müssen sich bis 31. Dezember 2026 registrieren.

-
- ☐ Prüfen Sie bei neuen Cloud-Diensten, wo die Daten gespeichert werden und ob ein Auftragsverarbeitungsvertrag vorliegt.
-
- ☐ Fragen Sie Ihre IT-Dienstleister, wie sie selbst mit MFA, Updates und Backups umgehen.

Wenn Sie bei einzelnen Punkten Unterstützung brauchen, helfen wir von Frankford's IT-Solutions in Innsbruck gerne weiter. Melden Sie sich einfach unverbindlich.