

IT-Security-Checkliste für KMU

Einfach. Verständlich. Sicher.

Stand: 22.02.2026

Herausgeber: neustifter.net

So nutzen Sie diese Checkliste

Diese Checkliste hilft Ihnen, die wichtigsten IT-Sicherheitsmaßnahmen in Ihrem Unternehmen strukturiert umzusetzen. Die Maßnahmen sind praxiserprobt und für kleine und mittlere Unternehmen geeignet. Haken Sie die Punkte ab, sobald sie eingeführt sind – so verbessern Sie den Schutz Ihrer E-Mails, Geräte und Unternehmensdaten und senken das Risiko von Ausfällen und Betrugsfällen.

1) Konten & Passwörter

- Mehrfaktor-Anmeldung (2FA/MFA) aktivieren**
Bei allen Diensten die MFA ermöglichen, wie Microsoft 365, Online-Banking oder Google
- Passwortmanager im Unternehmen einführen**
Hierfür gibt es zahlreiche Tools, beispielsweise das kostenlose KeePassXC
- Passwort-Regel schriftlich festlegen**
Zum Beispiel: keine Mehrfachverwendung, mindestens 12 Zeichen, keine ganzen Wörter

2) Rechte & Zugänge

- Erstellen eines Berechtigungskonzepts für Dateien und Programme**
Beschränken Sie den Zugriff auf Ordner, Dateien und Anwendungen auf die Nutzer, die diesen wirklich benötigen
- Admin-Zugänge trennen**
Normale Benutzeraccounts sollten keine Admin-Berechtigungen haben, um schädliche oder unerwünschte Installationen zu vermeiden
- Prozess für den Eintritt und Austritt von Benutzern definieren**
Wer macht was, bis wann (Konten, Rechte, Sperrung)

3) Geräte-Basisschutz (PC, Laptop, Smartphone)

- Automatische Updates verbindlich aktivieren**
Für Betriebssystem und Anwendungen, soweit möglich
- Einheitlichen Virenschutz/Endpoint-Schutz festlegen und zentral verwalten**
Sorgen Sie dafür, dass nur ein Virenschutz konsequent verwendet wird, nach Möglichkeit mit zentraler Überwachung und Verwaltung
- Festplattenverschlüsselung aktivieren**
Für Laptops und mobile Datenträger wie USB-Sticks und externe Festplatten, um den Zugriff durch Dritte bei Verlust zu verhindern
- Bildschirmsperre als Standard festlegen**
Automatische Sperre nach Inaktivität des Benutzers

4) E-Mail-Sicherheit & Betrugsprävention

- Mitarbeitende sensibilisieren (Phishing & Betrug)**
Typische Warnzeichen erkennen (fehlerhafte Absenderadresse, Abfrage von sensiblen Daten, dubiose Links oder Anhänge, Empfänger unter Druck setzen) und Einführen eines Vier-Augen-Prinzips bei Zweifeln
- Meldeweg für verdächtige E-Mails festlegen**
An wen melde ich verdächtige E-Mails intern und extern (Geschäftsführer, IT-Verantwortlicher oder externer IT-Dienstleister)
- Zahlungsregel einführen**
Telefonische oder persönliche Rückfrage bei veränderten Bankdaten oder neuen Zahlungsempfängern

5) Datenablage & Backup

- ❑ **Festlegen wo Daten gespeichert werden müssen**
mit einem einheitlichen Speicherort verhindern Sie Wildwuchs und Datenverlust bei Defekt oder Verlust eines Geräts, auf lokalen Geräten dürfen ausschließlich unwichtige Daten gesichert werden
- ❑ **Backup-Konzept festlegen und überprüfen**
Backups sollten nach 3-2-1-Regel gesichert werden (3 Kopien, 2 Medien, 1 externes Backup) um Datenverlust und langfristige Ausfälle zu verhindern
- ❑ **Wiederherstellungstest als festen Termin definieren**
Zum Beispiel quartalsweise oder jährlich, zudem sollte ein Verantwortlicher benannt werden, der sich darum kümmert

6) Homeoffice & Remote

- ❑ **Homeoffice-/Remote-Richtlinie festlegen**
Beispielsweise: sind Privatgeräte erlaubt, dürfen Daten lokal gespeichert werden, welche WLAN-Netzwerke dürfen verwendet werden, notwendiger Endpoint-Schutz, aktive Festplattenverschlüsselung, sichere Passwörter für Endgeräte
- ❑ **Sichere Zugriffstechnologien**
Nutzen Sie für den Zugriff aktuelle VPN-Standards oder Fernwartungsanwendungen mit entsprechendem Sicherheitsniveau und sicheren Passwörtern

7) Notfall & Zuständigkeiten

- ❑ **Notfall-Kontaktliste erstellen**
Interner Verantwortlicher, Geschäftsführer und externer IT-Dienstleister
- ❑ **Notfallplan (1 Seite) definieren**
Erste Schritte: trennen, sperren, informieren, dokumentieren.

Umsetzungsstatus

umgesetzt in Arbeit offen

Verantwortlich: _____

Unterschrift: _____ Datum: _____

Notizen
