SWYRON GMBH · CYBERSECURITY

Cybersecurity-Checkliste für KMU

Die zwölf Massnahmen mit der grössten Wirkung – zum Abhaken für Geschäftsleitung und IT-Verantwortliche.

Warum diese Liste

Die meisten erfolgreichen Angriffe auf Schweizer KMU nutzen immer dieselben Schwachstellen: fehlende Mehrfach-Anmeldung, veraltete Systeme, ungetestete Backups und unvorbereitete Mitarbeitende. Diese Checkliste priorisiert die Massnahmen, die im Verhältnis zu Aufwand und Kosten am meisten Risiko reduzieren. Sie ersetzt keine individuelle Analyse – aber wer alle zwölf Punkte guten Gewissens abhaken kann, ist besser aufgestellt als die grosse Mehrheit der KMU.

1. **Multi-Faktor-Authentifizierung (MFA) überall**
   E-Mail, Fernzugriff (VPN), Cloud-Dienste und alle Administratoren-Konten sind mit einem zweiten Faktor geschützt. Dies ist die wirksamste Einzelmassnahme gegen Kontoübernahmen.

2. **Getrennte Backups nach der 3-2-1-Regel**
   Drei Kopien, zwei Medientypen, eine Kopie ausser Haus oder unveränderbar (offline/immutable). Ransomware verschlüsselt auch erreichbare Backups.

3. **Wiederherstellung getestet**
   Mindestens einmal jährlich wird eine echte Wiederherstellung geübt und protokolliert. Ein Backup, das nie getestet wurde, ist eine Hoffnung, kein Schutz.

4. **Updates innert nützlicher Frist**
   Betriebssysteme, Anwendungen und Firewalls erhalten Sicherheitsupdates nach definiertem Prozess – kritische Lücken innert Tagen, nicht Monaten.

5. **Administratorenrechte minimiert**
   Niemand arbeitet im Alltag mit Admin-Rechten. Separate Admin-Konten, dokumentiert und mit MFA geschützt.

6. **Zugriffe geregelt (Need-to-know)**
   Mitarbeitende sehen nur die Daten, die sie für ihre Arbeit brauchen. Austritte führen am letzten Arbeitstag zur Sperrung aller Zugänge.

7. **Mitarbeitende sensibilisiert**
   Mindestens jährliche, kurze Schulung zu Phishing und Betrugsversuchen – inklusive klarer Meldestelle für verdächtige E-Mails, ohne Schuldzuweisung.

8 **Notfallplan auf einer Seite**

Wer wird informiert, wer entscheidet, wer kommuniziert? Telefonnummern (auch ausserhalb der IT) sind offline verfügbar.

9 **Inventar der Systeme und Daten**

Eine aktuelle Übersicht aller Geräte, Server, Cloud-Dienste und der wichtigsten Datenbestände. Was man nicht kennt, kann man nicht schützen.

10 **Verträge mit Dienstleistern geprüft**

IT-Dienstleister und Cloud-Anbieter sind vertraglich zu Sicherheit, Meldung von Vorfällen und Datenschutz (DSG) verpflichtet.

11 **E-Mail-Domain technisch geschützt**

SPF, DKIM und DMARC sind konfiguriert, damit Kriminelle nicht im Namen Ihrer Firma E-Mails versenden können.

12 **Verantwortung benannt**

Eine Person oder externe Stelle trägt die Verantwortung für Informationssicherheit und berichtet der Geschäftsleitung regelmässig.

Wie weiter?

Konnten Sie nicht alle Punkte abhaken? Genau dafür gibt es den Swyron Security-Check: eine strukturierte Standortbestimmung nach ISO 27001 und IKT-Minimalstandard, pauschal ab CHF 4'900 – mit verständlichem Bericht und priorisiertem Massnahmenplan. Das kostenlose Erstgespräch (30 Minuten) vereinbaren Sie unter office@swyron.com oder auf swyron.com/kontakt.html.

© Swyron GmbH · Dieses Whitepaper darf unverändert weitergegeben werden. Stand: Juli 2026. Die Inhalte ersetzen keine individuelle Beratung.