IT-Sicherheit für KMU in 10 Schritten:

1. Datensicherung und -wiederherstellung

Das Backup ist die Versicherung für alle Notfälle!
Verwenden Sie z.B. das 3-2-1 Konzept für Ihre täglichen Backups:

- 3-fache Ausführung der Daten (Original + 2 Kopien)
- 2 verschiedene Medientypen verwenden (z.B. Festplatte und Band)
- 1 Kopie ausser Haus (Georedundanz)

Führen Sie regelmässige Kontrollen durch:

- sind die Daten vorhanden und lesbar?
- Regelmässig ein Recovery (Wiederherstellung) durchführen um den gesamten Prozess zu testen

2. Virenschutz

Täglich werden rund 400 000 neue Schadsoftware-Varianten im Umlauf gebracht! Ein guter und verlässlicher Schutz vor Viren ist deshalb unerlässlich.

- verwenden Sie ein Antivirus-Programm eines vertrauenswürdigen Herstellers
- installieren Sie das Antivirus-Programm auf jedem einzelnen Computer
- verwenden Sie ein Programm mit «Echtzeit-Prüfung» und automatischen Updates

3. Firewall

Eine Firewall überprüft laufend den internen und externen Datenverkehr und kann Angriffe von aussen rechtzeitig identifizieren und ausfiltern.

- Setzen Sie eine Firewall aus einer Kombination von Soft- und Hardware ein
- lassen Sie die Firewall von Ihrem IT-Dienstleister richtig (restriktiv) konfigurieren (Filterregeln)
- installieren Sie neue Firmwareupdates umgehend
- verwenden Sie ein sicheres Administrator-Passwort für die Firewall
- verwenden Sie auf jedem Arbeitsplatz zusätzlich eine Firewall-Software

4. Patches & Updates

Mit Patches & Updates schliessen Softwarehersteller nachträglich Sicherheitslücken und korrigieren Fehler in den Programmen.

- Installieren Sie Patches & Updates unmittelbar nach deren Erscheinen
- prüfen Sie regelmässig, ob neue Firmware oder Treiber (z.B. Drucker usw.) verfügbar sind

5. WLAN Konfiguration

Das WLAN ist eine günstige Möglichkeit um den Internetzugang für die Arbeitsplätze zu ermöglichen. Um das WLAN nicht zu einem Risikofaktor zu machen, sichern Sie es wie folgt ab:

- Erstellen Sie für Gäste einen eigenen WLAN-Zugang
- Konfigurieren Sie das interne WLAN so, dass keine SSID gesendet wird
- Verwenden Sie für das WLAN ein sicheres Administrator-Passwort
- Setzen Sie eine starke Verschlüsselung für den Datenverkehr ein

6. Passwörter

Ein Passwort ist nur dann wirkungsvoll, wenn es den Zugang für Unbefugte tatsächlich und dauerhaft verhindert. Neueste Erkenntnisse raten davon ab, das Passwort regelmässig zu ändern, da Mitarbeiter dann dazu tendieren, einfachere Passwörter zu verwenden.
Regeln Sie in Ihrer Passwort-Policy deshalb folgende Punkte:

- Jeder Nutzer hat ein eigenes Konto/Passwort für den Zugang ins Firmennetz
- Jeder Nutzer hat pro Applikation ein eigenes Konto/Passwort
- Jeder Nutzer hat nur die für seine Aufgabe notwendigen Rechte (keine Adminrechte für alle!)
- möglichst lange Passwörter verwenden (mind. 12, besser 20 Zeichen)
- Verwenden Sie Fantasiesätze mit typisch «schwyzerdütsche» Wörter
- Prüfen Sie den Einsatz eines Passwortmanager
- Für externe Logins wo immer möglich die Zwei-Faktor-Authentifizierung verwenden

7. Schulung Personal

Sensibilisieren Sie Ihr Personal regelmässig über Themen der IT-Sicherheit und informieren Sie über aktuelle Gefahren aus der Cyberkriminalität. Die Sicherheitsziele der Personalschulung sind:

- Phishing-Attacken erkennen und sich entsprechend verhalten
- Sicher im Internet surfen
- sichere Downloads aus dem Internet
- potentieller Datendiebstahl und/oder Betrugsversuche frühzeitig erkennen
- Passwortregeln beherrschen
- Social Media Plattformen mit Vorsicht nutzen
- Verdachtsmomente erkennen und melden
- neue Bedrohungs- und Betrugsarten kennen und sich sicher verhalten
- Clean Desk Policy anwenden (aufgeräumter Arbeitsplatz)
- Anlaufstelle für IT-Sicherheitsvorfall oder Fragen ist jedem bekannt

8. Zugriffs-Management

Um IT-Gefahren abzuwenden, ist die Einschränkung der User bezüglich der IT-Rechte zentral. Die User sollen die zur Ausführung Ihrer Aufgaben notwendigen Rechte erhalten. Administratorrechte dürfen nur Mitarbeiter in der IT-Abteilung und/oder Ihr externer IT-Dienstleister haben.

9. Clean Desk Policy

Beim Thema Datensicherheit spielt der physische Arbeitsplatz der Mitarbeitenden eine immer wichtigere Rolle. Nicht selten verlassen Mitarbeitende ihren Arbeitsplatz und lassen dort den Laptop, USB-Stick, Smartphone usw. ungesichert liegen. Wichtige Sicherheitsvorkehrungen können sein:

- Unbefugter Zugang zu Dokumenten verhindern
- Computer & Smartphone bei Nichtbenutzung sperren oder die automatische Bildschirmsperre aktivieren
- Dokumente-Schränke und Schubladen verschliessen
- Festplatte verschlüsseln
- keine Logindaten auf Notizzettel

10. Notfallplan erstellen

Kleinere Betriebe haben selten einen Notfallplan für IT-Ausfälle. Bei einem Brand- oder Wasserschaden, oder bei einem Cybervorfall ist es elementar einen Notfallplan zu haben um so rasch wie möglich einen Notbetrieb sicherzustellen. Ein KMU muss sich überlegen, welche Infrastruktur und welche Applikationen für einen Notbetrieb erforderlich sind. Wichtig ist ebenfalls, den Übergang vom Notbetrieb in den Normalbetrieb zu planen und die richtigen Prioritäten zu setzen.