Checkliste: So schützen Sie Ihre Firma vor Cyber-Attacken

 **Sichere Passwörter:** Verwenden Sie starke, einzigartige und komplexe Passwörter für alle Konten und ändern Sie diese regelmässig. Vermeiden Sie unbedingt die Mehrfachverwendung von Passwörtern! Denn kommt eines in falsche Hände, haben Sie sonst gleich mehrere Sicherheitsrisiken auf einmal.

**Multi-Faktor-Authentifizierung (MFA):** Wo immer möglich: Aktivieren Sie MFA, um eine zusätzliche Sicherheitsebene hinzuzufügen. Dies erschwert es potenziellen Angreifern, auf Konten zuzugreifen, selbst wenn sie ihr Passwort kennen.

**Regelmässige Backups:** Führen Sie regelmässige Backups Ihrer Daten durch und speichern Sie diese an einem sicheren Ort – respektive: möglichst an mehreren Orten. Dies stellt sicher, dass Sie im Falle eines Angriffs Ihre Daten wiederherstellen können.

**Schutz vor Viren und Malware:** Installieren und aktualisieren Sie regelmässig Antivirus- und Anti-Malware-Software, und halten Sie diese stets aktuell. Denn Betrüger lassen sich immer wieder Neues, Ausgeklügeltes einfallen, um an Ihre Daten und in Ihr System zu gelangen.

**Firewall - Ihr persönliches Schutzschild**: Installieren Sie eine Firewall, um Ihren Datenverkehr  
zu sichern und Ihr Netzwerk zu schützen.

**Sicherheitsupdates:** Halten Sie Ihre Software und Betriebssysteme stets auf dem neuesten Stand, um Sicherheitslücken zu schliessen. Updates erst einige Wochen oder gar Monate nach deren Verfügbarkeit zu machen und "erst mal abzuwarten" ist eine schlechte Idee.

**Schulung und Info der Mitarbeiter:**Halten Sie Ihre Mitarbeiter auf dem Laufenden in Bezug auf Cybersicherheit und schaffen Sie transparente, einheitliche Informationen – etwa durch einen Leitfaden, den Sie zusammen mit IT-Experten aufstellen, und der im ganzen Betrieb gilt.

**VPN (virtuelles privates Netzwerk)**: Verwenden Sie ein VPN, um sichere Verbindungen zu gewährleisten, insbesondere bei der Arbeit aus der Ferne. In einem öffentlichen/ungesicherten  
WLAN auf Ihre Geschäftsdaten zugreifen? – Keine gute Idee.

**Verwaltung der Zugriffsrechte:**Beschränken Sie den Zugriff auf sensible Daten und Systeme auf diejenigen Mitarbeitenden, die ihn wirklich benötigen. Grundregel für den Zugriff: So wenige Leute wie möglich, so viele wie nötig.

**Incident Response (Notfallplan):**Definieren Sie ein einheitliches Vorgehen zur Reaktion auf Sicherheitsvorfälle, um im Falle eines Angriffs schnell und effektiv agieren zu können**.**