ITSECCON

IT-Sicherheits-Checkliste

für kleine Unternehmen (KMU)

Die 10 wichtigsten Maßnahmen für mehr IT-Sicherheit im Alltag

1 Starke Passwörter & 2FA verwenden

Verwenden Sie für alle Zugänge sichere, individuelle Passwörter mit mindestens 12 Zeichen, Sonderzeichen, Zahlen und Groß-/Kleinbuchstaben. Ergänzen Sie wichtige Konten um eine Zwei-Faktor-Authentifizierung (2FA), um den Schutz bei gestohlenen Passwörtern zu erhöhen.

Tipp: Nutzen Sie Passwort-Manager, um komplexe Passwörter sicher zu speichern.

2 Regelmäßige Backups wichtiger Daten

Sichern Sie alle geschäftskritischen Daten regelmäßig – idealerweise automatisch und redundant (z. B. lokal & in der Cloud). So sind Sie im Falle eines Cyberangriffs oder Hardwareausfalls abgesichert.

Tipp: Testen Sie regelmäßig, ob Ihre Backups auch wirklich wiederherstellbar sind.

3 Aktuelle Firewall- und Virenschutzsoftware einsetzen

Eine gute Firewall schützt Ihr Netzwerk vor ungewolltem Zugriff, Antivirensoftware erkennt Schadprogramme frühzeitig. Halten Sie beide Komponenten aktuell, um auch neue Bedrohungen abwehren zu können.

Tipp: Verwenden Sie Sicherheitslösungen von vertrauenswürdigen Anbietern mit regelmäßigen Updates.

4 Betriebssysteme und Programme aktuell halten

Veraltete Software enthält häufig bekannte Sicherheitslücken. Installieren Sie Sicherheitsupdates und Patches zeitnah, um Schwachstellen zu schließen.

Tipp: Aktivieren Sie automatische Updates, wo möglich.

5 Mitarbeitende zu IT-Sicherheit schulen

Sensibilisieren Sie Ihr Team regelmäßig für IT-Sicherheit. Viele Angriffe beginnen mit menschlichem Fehlverhalten.

Tipp: Kleine Schulungen oder Infomails zu aktuellen Bedrohungen können große Wirkung zeigen.

6 E-Mail-Anhänge und Links sorgfältig prüfen

Phishing-Mails sehen oft täuschend echt aus. Öffnen Sie keine Anhänge oder Links aus unbekannten Quellen.

Tipp: Achten Sie auf Absenderadresse, Grammatikfehler und ungewöhnliche Inhalte.

7 Zugriffsrechte auf Daten und Systeme einschränken

Nicht jeder braucht Zugriff auf alles. Begrenzen Sie Berechtigungen auf das notwendige Minimum.

Tipp: Nutzen Sie rollenbasierte Zugriffsmodelle und dokumentieren Sie diese.

8 Netzwerkzugänge (z. B. WLAN) mit sicheren Passwörtern schützen

Offene oder schwach geschützte Netzwerke sind leicht angreifbar. Verwenden Sie sichere WPA3-Verschlüsselung und ändern Sie Standardpasswörter.

Tipp: Trennen Sie Gäste-Netzwerke vom Unternehmensnetzwerk.

9 Automatische Sperre bei Inaktivität aktivieren

Verhindern Sie unbefugten Zugriff, wenn Geräte unbeaufsichtigt bleiben. Aktivieren Sie automatische Sperrmechanismen nach kurzer Inaktivität.

Tipp: Bildschirm nach 5 Minuten automatisch sperren lassen.

10 Notfallplan für Cyberangriffe erstellen

Ein klarer Notfallplan hilft, im Ernstfall schnell und strukturiert zu reagieren. Legen Sie Zuständigkeiten und Maßnahmen fest.

Tipp: Notfallkontakte, Backup-Zugänge und Kommunikationswege schriftlich festhalten.

Noch Fragen zur IT-Sicherheit? Jetzt unverbindlich beraten lassen: ITSECCON – Karsten Heimers · IT- & Security Consulting
Spargelweg 11 · 38179 Schwülper ✉ info@itseccon.com 🌐 www.itseccon.com