techbold

IT-SECURITY CHECKLISTE

Mit dieser Checkliste erhälst du in neun schnellen Schritten einen Überblick über den IT-Sicherheits Status deines Unternehmens.

1 GEFAHREN IDENTIFIZIEREN ☐

Verschaffe dir einen Überblick über alle Daten die dein Unternehmen sammelt. Welche Personen (in- & extern), Anwendungen und Geräte haben Zugriff auf diese Daten? Achte Besonders auf:

- Kundendaten (persönliche Daten, Kontonummern, usw.)
- Mitarbeiterdaten (p. Daten, Gehaltsabrechnung, HR usw.)
- Finanzdaten (Kontoinformationen, online Zugange usw.)
- sensibile Daten wie Geschäftsberichte, Marketingpläne und Produktspezifikationen usw.

2 SCHUTZ- & BACKUPROUTINE ☐

Vergewissere dich, dass eine regelmäßige Datensicherung erfolgt. Ein redudantes Back-up aller stationären und mobilen Arbeitsgeräte, als auch Server sollte gegeben sein. Die Daten in Clouds (SaaS-Daten) sollten extern zusätzlich gesichert sein. Überprüfe, ob es mindestens 1x täglich ein automatisches Backup gibt, das im Notfall eine schnelle und vollständige Wiederherstellung garantiert.

3 UPDATE ROUTINE ☐

Prüfe, ob eine automatische Software Update Routine aktiv ist: Antivirussoftware, Webbrowser und Betriebssysteme müssen immer am letzten Softwarestand sein, um Schutz vor aktuellen Viren, Malware und anderen Online-Bedrohungen zu gewährleisten. Die Antivirus Software sollte so konfiguriert sein, dass nach jedem Update ein automatischer Scan ausgeführt wird. Auch andere große Software-Updates sollten installiert werden, sobald sie verfügbar sind.

4 NETZWERKSICHERUNG ☐

Stelle sicher, dass die WLAN-Netzwerke für interne und externe Personen(z.B. Gäste, Kunden) getrennt sind. Weiters sollte die Firewall des Betriebssystems oder die eingebette Firewall der Antivirus-Lösung (z.B. Bitdefender) immer aktiviert sein. Auch Arbeiten im Homeoffice sollten immer über eine verschlüsselte Verbindung zur Firmen-Firewall oder über eine VPN-Verbindung erfolgen.

5 DATENVERSCHLÜSSELUNG ☐

Stelle sicher, dass alle Daten verschlüsselt und sicher übertragen werden, egal über Datenträger, Netzwerke oder Business Devices wie Notebooks, Tablets und Smartphones.

6 MOBILE GERÄTE ☐

Mobile Geräte sind eine erhebliche Herausforderung für die Datensicherheit und das Sicherheitsmanagement. Besonders wenn sie auf vertrauliche Informationen oder das Unternehmensnetzwerk zugreifen. Stelle sicher, dass alle Mobilgeräte passwortgeschützt sind und eine Datenverschlüsselung erfolgt. Wenn ein VPN im Einsatz ist, sollte dieses auch mobil, per APP, genützt werden. So kann Datendiebstahl bei der Benützung von öffentlichen Netzwerken unterbunden werden. Weiters muss ein verbindliches Meldeverfahren für verlorene oder gestohlene Ausrüstung festgelegt sein.

7 ZUGANGSRICHTLINIEN

Der Zugriff auf und die Verwendung von Unternehmenscomputern darf nur durch autorisierte Benutzer möglich sein. Notebooks können leicht verloren oder gestohlen werden. Sie müssen in jedem unbeaufsichtigten Moment gesperrt sein. Stelle sicher, dass jeder Mitarbeiter über ein eigenes Benutzerkonto verfügt und eine starke Passwortrichtlinie aktiv ist. Administrator-Rechte sollten dem IT-Personal vorbehalten sein.

8 MITARBEITER SCHULUNG

Eine Grundlage an Sicherheitspraktiken und Richtlinien müssen für jeden Mitarbeiter gelten und klar kommuniziert werden. Das betrifft beispielsweise starke Passwörter, Richtlinien für die Internetnutzung, aber auch den Umgang mit und die Sicherung von Kundendaten. Schulungen helfen dabei Mitarbeiter zu sesibilisieren und IT-Sicherheitsmaßnahmen erfolgreich zu implementieren.

9 DISASTER RECOVERY PLAN

Viel schmerzhafter als die direkten Kosten eines Cyber Angriffs selbst (IT-Technikerstunden, Hardwareaustausch) sind für Unternehmen die damit verbunden betrieblichen Ausfallzeiten. Daher muss im Ernstfall ein klarer Maßnahmenplan (Disaster Revocery Plan) vordefiniert sein. Überprüfe, ob bereits ein solcher Notfallplan besteht und wie schnell dein Unternehmen alle Daten erfolgreich wiederherstellen kann, um wieder voll betriebsfähig zu sein.

LERNE UNS KENNEN

Wir von techbold sind ein langjährig erfahrenes Team von IT & Computer Experten und Pionieren. Uns verbindet die gemeinsame Leidenschaft für Technologie und für die Vernetzung der Menschen untereinander. Wir sind überzeugt, dass uns Mut und Leidenschaft sowohl als Mensch, als auch als Unternehmen besser und erfolgreicher macht.

MARIO NOVAK
Head of New Business

+4359555501
mno@techbold.at

TECHBOLD IT-AUDITS
EXPERTEN ANALYSIEREN DEINE IT

Solltest du Interesse an einer tieferen Prüfung deiner IT-Systeme haben, ist ein IT-Audit das Richtige. Unsere IT Audits beinhalten unteranderem:

- ☑ Genaue Dokumentation aller für die IT relevanten Aspekte
- ☑ Klarer Überblick über die gesamte IT, die Auslastung und das Potential
- ☑ Unterstützung bei Bewertung und zukünftige Ausrichtung der IT-Systeme
- ☑ Mit Priorität versehene Formulierung des Handlungsbedarfs
- ☑ Vorschläge für Aktualisierungs-, Optimierungs- und Einsparungsmöglichkeiten

Weitere Infos unter:
www.techbold.at/it-audit-und-it-check