IT SICHERHEITS-CHECKLISTE FÜR DEIN UNTERNEHMEN

Auswertung siehe Seite 3

1. ALLGEMEINE SICHERHEITSRICHTLINIEN

- ☐ Gibt es eine IT-Sicherheitsrichtlinie im Unternehmen?
- ☐ Kennen alle Mitarbeitenden die IT-Richtlinien und wurden sie unterwiesen?
- ☐ Werden regelmäßige Schulungen zu IT-Sicherheit durchgeführt (z. B. Phishing, Passwortsicherheit)?
- ☐ Gibt es eine zuständige Person oder Abteilung für IT-Sicherheit?

2. ENDGERÄTE & ARBEITSPLATZSICHERHEIT

- ☐ Sind alle Geräte (PCs, Laptops, Smartphones) mit aktueller Antivirus-Software geschützt?
- ☐ Werden alle Betriebssysteme und Programme regelmäßig aktualisiert (Patch-Management)?
- ☐ Werden USB-Sticks oder externe Geräte kontrolliert oder eingeschränkt?
- ☐ Gibt es Richtlinien zur Nutzung privater Geräte (BYOD – Bring Your Own Device)?

3. ZUGANGSKONTROLLE & PASSWÖRTER

- ☐ Haben alle Nutzer individuelle Benutzerkonten?
- ☐ Werden starke Passwörter erzwungen (z. B. Mindestlänge, Sonderzeichen)?
- ☐ Wird eine Zwei-Faktor-Authentifizierung (2FA) eingesetzt?
- ☐ Gibt es ein Verfahren zur Deaktivierung von Konten ehemaliger Mitarbeitender?

4. DATENSICHERUNG & WIEDERHERSTELLUNG

- ☐ Werden regelmäßig Backups erstellt?
- ☐ Werden die Backups auch getrennt vom Netzwerk aufbewahrt?
- ☐ Wird regelmäßig getestet, ob die Wiederherstellung der Backups funktioniert?
- ☐ Gibt es ein Notfallkonzept bei Datenverlust?

5. NETZWERK & SERVER

- ☐ Ist das Unternehmensnetzwerk durch eine Firewall geschützt?
- ☐ Gibt es ein Gäste-WLAN, das vom internen Netzwerk getrennt ist?
- ☐ Werden Zugriffe auf Server, Router und Switches protokolliert?
- ☐ Sind ungenutzte Ports deaktiviert?

6. E-MAIL- & KOMMUNIKATIONSSICHERHEIT

- ☐ Gibt es einen Spam- und Virenfilter für E-Mails?
- ☐ Werden verdächtige Anhänge und Links automatisch blockiert oder markiert?
- ☐ Gibt es eine Verschlüsselung für interne und externe E-Mail-Kommunikation?
- ☐ Gibt es ein Meldesystem für Phishing-Versuche?

7. CLOUD & EXTERNE DIENSTE

- ☐ Werden Cloud-Dienste DSGVO-konform verwendet?
- ☐ Werden Daten in der Cloud verschlüsselt gespeichert?
- ☐ Gibt es Verträge mit Auftragsverarbeitern (AV-Verträge)?
- ☐ Wird geprüft, welche Drittanbieter Zugriff auf Daten haben?

8. PROTOKOLLIERUNG & MONITORING

- ☐ Werden sicherheitsrelevante Ereignisse protokolliert?
- ☐ Gibt es ein zentrales Log-Management oder SIEM-System?
- ☐ Wird das System regelmäßig auf ungewöhnliches Verhalten überwacht?

9. NOTFALLMANAGEMENT & REAKTION

- ☐ Gibt es einen Notfallplan für IT-Sicherheitsvorfälle?
- ☐ Sind Zuständigkeiten und Kommunikationswege im Krisenfall klar geregelt?
- ☐ Wird das Notfallmanagement regelmäßig getestet (z. B. durch Planspiele)?
- ☐ Ist eine schnelle externe Unterstützung im Ernstfall verfügbar (z. B. IT-Dienstleister)?

10. REGELMÄSSIGE ÜBERPRÜFUNG

- ☐ Gibt es regelmäßige interne oder externe Audits zur IT-Sicherheit?
- ☐ Werden Ergebnisse dokumentiert und Maßnahmen abgeleitet?
- ☐ Wurden die letzten Sicherheitsupdates und Maßnahmen bereits überprüft?

AUSWERTUNG & PUNKTESYSTEM

So funktioniert die Bewertung deiner IT Sicherheits-Checkliste:

> Für jede angehakte Checkbox erhält man 1 Punkt
> Maximal erreichbar: 38 Punkte

Bewertung der IT Sicherheitslage:

Sicher aufgestellt:	80–100 % (31–38 Punkte)
Verbesserungsbedarf:	50–79 % (19–30 Punkte)
Kritisch:	Unter 50 % (0–18 Punkte)

Diese Checkliste dient als erste Orientierung und ersetzt keine professionelle IT-Sicherheitsanalyse.

IT-Sicherheit ist kein Luxus, sondern eine Notwendigkeit!
Vereinbare jetzt ein unverbindliches Beratungsgespräch mit der MXP GmbH, um individuelle Handlungsempfehlungen für deine IT-Sicherheit zu erhalten.