IT-Sicherheitscheckliste

IT-Verbindungen: Schwachstellenanalyse und Maßnahmen

DIGITAL AGENTUR BERLIN

Prüfen Sie an Hand der folgenden 10 Fragen, wie Ihr Unternehmen in Bezug auf IT-Sicherheit aufgestellt ist. Wenn Sie eine Frage mit **Nein** beantworten, haben wir für Sie Maßnahmen benannt, mit denen Sie Ihre IT-Sicherheit verbessern können.

	IT-Sicherheitsfrage	Ja	Nein	Mögliche Maßnahme
1.	**Gibt es eine Dokumentation über Ihre Kommunikationsverbindungen?**	☐	☐	Erstellung eines Netzwerkplanes für Kommunikationsverbindungen
2.	**Werden Richtlinien zur sicheren Informationsübertragung und für interne und externe Netzwerke vorgegeben und geprüft?**	☐	☐	› Erstellung von Richtlinien für Kommunikationsverbindungen › Regelmäßige Kontrolle oder Monitoring der Verbindungen (z.B. via Software)
3.	**Werden Netzwerke verwaltet, um IT-Kommunikationsverbindungen zu schützen?**	☐	☐	Netzwerksoftware wird zum Schutz von Netzwerken und auch Verbindungen eingesetzt.
4.	**Werden Netzwerke, Benutzer*in und Informationssysteme getrennt voneinander gehalten?**	☐	☐	Technische Trennung von Netzwerken, Benutzer*innen und Systemen
5.	**Sind die Informationen in der elektronischen Nachrichtenübertragung angemessen geschützt?**	☐	☐	Es sollte mindestens eine Anti-Virus-Software und eine Firewall vorhanden sein. Bestenfalls ist die Verbindung via „End-to-End“-Verschlüsselung geschützt.
6.	**Sind Web-Browser und die Mail-Umgebung IT-sicher eingestellt?**	☐	☐	Prüfung und Realisierung von Einstellungsmöglichkeiten im Web-Browser und in der Mail-Umgebung
7.	**Ist der WLAN-Router passwortgeschützt?**	☐	☐	› Einstellung eines Passwortes im WLAN-Router › Das Passwort sollte mindestens 16 Stellen haben und schwer zu erraten sein
8.	**Interne Verbindungen: Sind interne Verbindungen verschlüsselt?**	☐	☐	› Auch interne Verbindungen sollten verschlüsselt sein › Z.B. bei SQL-Servern kann die Transport Layer Security (TLS)-Verschlüsselung genutzt werden
9.	**Sind Verbindungen zwischen Rechnern verschlüsselt?**	☐	☐	Nutzung der „Secure Socket Layer“ (SSL)-Verschlüsselung zwischen Rechnern
10.	**Wird beim Zugriff von außen auf ein bestehendes, vertrauliches Netzwerk eine VPN-Verbindung genutzt?**	☐	☐	Virtual Private Network (VPN) – Verbindungen sind sicherer als übliche Verbindungen, z.B. verschlüsselt VPN die IP-Adresse und anonymisiert. Daher wird VPN für vertrauliche Daten und externen Zugriff genutzt.

Gerne unterstützen wir Sie bei der Umsetzung der Maßnahmen zur Erhöhung der IT-Sicherheit in Ihrem Unternehmen. Wir freuen uns auf Ihre Anfrage an **info@digitalagentur.berlin**.

Weitere Informationen finden Sie auch auf **digitalagentur.berlin**.