DIGITAL AGENTUR BERLIN

IT-Sicherheitscheckliste

IT-Verbindungen: Schwachstellenanalyse und Maßnahmen

Der Begriff „**IT-Verbindungen**“ wird im Folgenden für alle Schnittstellen und Transportwege verwendet, um Informationen bzw. Daten von einem System zu einem anderen, von einer Software zu einer anderen oder zwischen Anwendenden zu übermitteln.

Prüfen Sie anhand der folgenden 9 Fragen, wie Ihr Unternehmen in Bezug auf IT-Sicherheit aufgestellt ist. Wenn Sie eine Frage mit **Nein** beantworten, haben wir für Sie Beispiel-Maßnahmen benannt, mit denen Sie Ihre IT-Sicherheit verbessern können.

	IT-Sicherheitsfrage	Ja	Nein	Mögliche Maßnahme
1.	**Gibt es eine Übersicht über Ihre IT-Verbindungen?**	☐	☐	Erstellen Sie eine Übersicht der Kommunikationswege, mit denen Sie und Ihre Mitarbeiter*innen intern und extern kommunizieren (Fax, E-Mail, Messengerdienste, Telefon, Handy, Social Media) sowie Netzwerkverbindungen, worüber Daten übermittelt werden (Netzwerk, WLAN, VPN).
2.	**Gibt es eine Liste aller Geräte, die eine Netzwerkverbindung benötigen?**	☐	☐	Prüfen Sie, welche Geräte alle mit dem Firmennetzwerk verbunden sind, um sicherzustellen, dass wirklich alle bestehenden Netzwerkverbindungen gesichert sind (z. B. Netzwerkdrucker, Info-Bildschirme, Überwachungskameras o. ä.).

IT-Verbindungen: Schwachstellen-analyse und Maßnahmen

DIGITAL AGENTUR BERLIN

	IT-Sicherheitsfrage	Ja	Nein	Mögliche Maßnahme
3.	**Ist die sichere Informationsübertragung sowohl intern als auch extern sichergestellt, z. B. durch verbindliche Vorgaben oder technische Einrichtungen?**	☐	☐	Folgendes sollte technisch sichergestellt oder von Mitarbeiter*innen umgesetzt werden: ▪ Verschlüsselter Versand von sensiblen Informationen (z. B. Passwortschutz oder Tauschlaufwerk) ▪ Angemessene Absicherung von Netzwerkkomponenten (z. B. geändertes Standard-Router-Passwort, kein freier Zugang zu Netzwerk-Ports) ▪ Erstellung von Richtlinien für Kommunikationsverbindungen ▪ Regelmäßige Kontrolle oder Monitoring der Verbindungen (z. B. via Software)
4.	**Sind Ihre Beschäftigten geschult, um bspw. passwortgeschützte Anhänge erstellen zu können oder eingesetzte Verschlüsselungssoftware richtig anwenden zu können?**	☐	☐	Beschäftigte sollten in der Lage sein, Dokumente oder Zip-Archive mit Passwort erzeugen, oder Verschlüsselungssoftware bedienen zu können, sofern welche eingesetzt wird. (Schlüssel einbinden oder exportieren)
5.	**Ist Ihre elektronische Kommunikation mit standardisierten Schutzmaßnahmen versehen?**	☐	☐	Die eingesetzten Anwendungen sollten https unterstützen und ggf. bei Unterschreitung warnen. Optimalerweise ist der Datenverkehr Ende-zu-Ende-verschlüsselt, bis hin zu lokal archivierten E-Mails.
6.	**Werden Netzwerke nach ihrem Anwendungszweck unterschieden bzw. getrennt, z. B. mit einem separaten Gäste-WLAN?**	☐	☐	Optimalerweise wird ein separates Gäste-Netzwerk für Externe eingerichtet, getrennt von dem für eigene Mitarbeitende.
7.	**Ist der WLAN-Router passwortgeschützt und auf einen aktuellen Sicherheitsstandard eingestellt?**	☐	☐	▪ Einstellung eines sicheren Passwortes im WLAN-Router ▪ Ändern des voreingestellten Standardpasswortes ▪ Passwort mit mindestens 20 Stellen und schwer zu erraten ▪ Es sollte, sofern technisch möglich, WPA3 als Verschlüsselung gewählt werden

IT-Verbindungen: Schwachstellen-analyse und Maßnahmen

	IT-Sicherheitsfrage	Ja	Nein	Mögliche Maßnahme
8.	**Interne Verbindungen: Greifen Beschäftigte über ein erschlüsseltes Firmennetzwerk auf Unternehmens-daten zu?**	☐	☐	▪ Auch interne Verbindungen sollten verschlüsselt sein ▪ Z. B. bei SQL-Servern kann die Transport Layer Security (TLS)-Verschlüsselung genutzt werden
9.	**Wird beim Zugriff von Außerhalb (insbesondere aus öffentlichen Netz-werken, z. B. Hotels, Café, Bahnhof usw.) auf ein bestehendes, vertrau-liches Netzwerk eine VPN-Verbindung genutzt?**	☐	☐	Virtual Private Network (VPN) – Verbindungen sind sicherer als übliche Verbindungen, z. B. verschlüsselt VPN die IP-Adresse und anonymi-siert alle Online-Aktivitäten. 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** oder rufen Sie uns unter der **Cyberhotline 030 166 360 580** an.