DIGITAL AGENTUR BERLIN

IT-Sicherheitscheckliste

Home-Office: Schwachstellenanalyse und Maßnahmen

Der Begriff „**Home-Office**“ wird im Folgenden für alle Arbeiten, die außerhalb der Geschäftsräume stattfinden, verwendet. „Heim-Arbeit“, „Mobile Office“, „Remote Work“ oder „Tele-Arbeit“ sind u. a. auch dafür gebräuchlich.

Prüfen Sie anhand 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 Beispiel-Maßnahmen benannt, mit denen Sie Ihre IT-Sicherheit verbessern können.

IT-Sicherheitsfrage	Ja	Nein	Mögliche Maßnahme
1. Gibt es eindeutige Regelungen für Arbeit im Home-Office?	☐	☐	Erstellen, dokumentieren und kommunizieren eindeutiger Regelungen
2. Wird im Home-Office ausschließlich dienstliche Hard- und Software genutzt?	☐	☐	▪ Regeln zur getrennten Verwendung privat und beruflich genutzter IT-Ausrüstung ▪ Ggf. Genehmigungsverfahren zur Nutzung von Privatgeräten („Bring your own Device“-Regelung)
3. Sind auch im Home-Office firmeninterne Dokumente und sensible Informationen vor dem Zugriff Dritter geschützt?	☐	☐	▪ Anweisungen um Passwörter, Informationen, Daten und Datenträger im Home-Office vor dem Zugriff Dritter zu schützen ▪ Wegschließen von Arbeitsmitteln ▪ Sperren des Bildschirms beim Verlassen des Arbeitsplatzes
4. Ist die Verbindung von Ihrem Arbeitsort zu Ihrem Firmennetz gesichert?	☐	☐	Verschlüsselter Zugriff (mind. https bei Webseiten, WPA3-Verschlüsselung bei WLAN, VPN)

Home-Office: Schwachstellen-analyse und Maßnahmen

DIGITAL AGENTUR BERLIN

	IT-Sicherheitsfrage	Ja	Nein	Mögliche Maßnahme
5.	**Wird auch die im Home-Office verwendete IT-Ausrüstung durch eine Sicherheits-Software geschützt?**	☐	☐	▪ IT-Ausrüstung auch im Home-Office durch Sicherheitssoftware (Firewall, Anti-Virus-Software) schützen ▪ Sicherheitssoftware aktuell halten (Updates)
6.	**Gibt es verbindliche Vorgaben für die Erstellung sicherer Passwörter?**	☐	☐	▪ Passwortlänge mindestens 8 besser 12 Zeichen ▪ Zeichenmix aus Sonderzeichen, Groß- und Kleinbuchstaben, Zahlen ▪ Keine leicht erratbaren Wortzusammensetzungen ▪ Passwörter und Anmeldenamen in Kombination nicht anderweitig verwenden
7.	**Werden Zugriffe zu Systemen oder Software mehrstufig abgesichert?**	☐	☐	Sofern möglich, Mehrfach-Authentisierung (z. B. Zwei-Faktor-Authentifizierung) nutzen
8.	**Werden im Home-Office regelmäßig Backups von wesentlichen Daten durchgeführt?**	☐	☐	▪ Regelmäßiges Backup (Datensicherung) durchführen ▪ Täglich, wöchentlich, monatlicher Turnus nach Relevanz der verarbeiteten Daten (Verlusttoleranz) ▪ Ggf. auch Daten auf privaten Endgeräten mit einplanen
9.	**Werden im Home-Office auch regelmäßig Updates der Software durchgeführt?**	☐	☐	Regelmäßige, insbesondere sicherheitskritische Updates aller Programme durchführen (Sicherheitslücken schließen)
10.	**Kennen Ihre Mitarbeitenden die geltenden Verhaltensweisen für IT-Notfälle?**	☐	☐	▪ Erstellen und Kommunizieren des Notfallplans und von Meldewegen an Mitarbeitende[1] ▪ Wichtige Kontaktdaten für Notfälle in Papierform (z. B. BSI-Notfallkarte[2])

1 www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/Massnahmenkatalog/massnahmenkatalog.html
2 www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/IT-Notfallkarte/it-notfallkarte_node.html

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.