IT-Sicherheitscheckliste

Software: 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.	**Besteht eine Softwareübersicht oder -landschaft?**	☐	☐	› Erstellung einer Softwareübersicht (Kategorisierung der IT-Software etc.) › Visualisierung der IT- Softwarelandschaft
2.	**Gibt es ein sicheres, einheitliches Installationsvorgehen für Software?**	☐	☐	Die Installation von Software sollte nur von Befugten standardisiert und IT-sicher durchgeführt werden.
3.	**Wird regelmäßig kontrolliert, dass Nutzer*innen nur Zugriff auf die IT-Software haben, die berechtigt sind?**	☐	☐	Regelmäßiges Software-Monitoring wird empfohlen (z.B. monatliche Berechtigungs-kontrolle).
4.	**Kennwörterverwaltung: werden starke Kennwörter systemseitig sichergestellt?**	☐	☐	Vorhandene Passwortregeln sollten in der IT-Software eingestellt werden für die IT-Nutzer*innen: › Passwörter sollten mindestens 8-stellig sein. › Verwenden Sie keine leicht zu erratenen „Wörter“, sondern Sonderzeichen, Groß-/Kleinbuchstaben und Zahlen als Passwort. › Verwenden Sie NIE das gleiche Passwort mehrmals.
5.	**Wurden IT-Änderungen in Systemen oder in der Software vor der Produktivsetzung getestet?**	☐	☐	Z.B. Tests: Systemabnahmetests, User Acceptance Tests, Systemsicherheitstests, Performancetests etc.
6.	**Ist ausgeschlossen, dass Software ohne Genehmigung geändert werden kann?**	☐	☐	Funktionstrennung zwischen Entwickler*in, Administrator*in und IT-Anwender*in
7.	**Wird die Antivirus-Software und Firewall regelmäßig aktualisiert?**	☐	☐	Jede*r Nutzer*in sollte seine*ihre Anti-virus-Software regelmäßig updaten.
8.	**Schauen Sie regelmäßig nach Updates und Patches für Ihre Software und spielen Sie diese ein?**	☐	☐	Die IT sollte über aktuelle Patches infor-miert sein und diese bei Bedarf einspielen.
9.	**Gibt es ein regelmäßiges Backup für die Daten der Software?**	☐	☐	Bestenfalls wird ein tägliches Backup aller Daten durchgeführt.
10.	**Findet eine DSGVO-konforme Ereignis-protokollierung in den IT-Systemen statt?**	☐	☐	Protokolle sind in Systemen anzuschalten oder es ist eine protokollierende, DSGVO-konforme Software einzusetzen. Alternativ kann eine IT-Nutzer*innen-Historie im Sys-tem hinterlegt werden, z.B. für Revisions-zwecke.

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**.