DIGITAL AGENTUR BERLIN

IT-Sicherheitscheckliste

Software: Schwachstellenanalyse und Maßnahmen

Der Begriff „**Software**“ wird im Folgenden für alle Computer-Programme, also Anwendungen, Betriebssysteme, Applikationen verwendet, die lokal auf dem Gerät oder in einer Cloud, online, zur Datenverarbeitung im Unternehmen, mobil, unterwegs oder am Heim-Arbeitsplatz verwendet werden. Auch andere IT-Geräte wie Drucker, Router oder Smartgeräte werden über Software gesteuert, die mit betrachtet werden sollte.

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 eine aktuelle Übersicht über die verwendete Software?	☐	☐	▪ Erstellen Sie eine Softwareübersicht inkl. Verwendungszweck, Lizenzen und Versionen. ▪ Empfehlenswert ist zudem die Erstellung einer IT-Schnittstellenlandkarte.
2. Gibt es ein zentrales, sicheres und einheitliches Vorgehen bei der Installation von Software?	☐	☐	Definieren Sie einheitliche Prozesse zur Prüfung, Freigabe und Installation von neuer Software, bis hin zu Updates und Upgrades. Legen Sie sofern möglich Verantwortlichkeiten dafür fest.
3. Werden Berechtigungen regelmäßig auf Erforderlichkeit kontrolliert und ggf. entfernt?	☐	☐	▪ Prüfen Sie regelmäßig, ob vergebene Berechtigungen noch erforderlich sind. ▪ Es gilt das Minimalprinzip.
4. Ist systemseitig ausgeschlossen, dass Software ohne Genehmigung geändert werden kann?	☐	☐	Setzen Sie Berechtigungen so, dass Software nur durch den zuständigen Administrator angepasst werden kann. Unterscheiden Sie zwischen Administratoren- und Nutzerberechtigungen.

Software: Schwachstellen-analyse und Maßnahmen

DIGITAL AGENTUR BERLIN

IT-Sicherheitsfrage	Ja	Nein	Mögliche Maßnahme
5. Gibt es Vorgaben für die Verwendung starker Passwörter, die auch Anmeldungen zu Software umfasst?	☐	☐	Passwörter sollten nicht leicht zu erraten sein und mindestens aus 12 Zeichen, Sonderzeichen, Groß-/ Kleinbuchstaben sowie Zahlen bestehen. Vermeiden Sie eine wiederholte Nutzung derselben Kombination aus Passwort und Benutzername.
6. Wird die Sicherheits-Software regelmäßig automatisch aktualisiert?	☐	☐	▪ Stellen Sie sicher, dass alle Sicherheits-Software (Anti-Virus, Firewall, Anti-Spam, Endpoint-Security usw.) in regelmäßigen Abständen automatisch geupdated werden. ▪ Bei Bekanntwerden einer neuen Bedrohung oder Schwachstelle sollte das auch manuell möglich sein.
7. Wird die weitere Software ebenfalls regelmäßig automatisch aktualisiert?	☐	☐	Stellen Sie sicher, dass analog zur Sicherheits-Software auch jede weitere Software regelmäßige Updates erhält, insbesondere dann, wenn Sicherheitslücken bekannt werden.
8. Gibt es ein regelmäßiges Backup (Sicherungskopien) für die Daten der verwendeten Software?	☐	☐	▪ Lassen Sie regelmäßige Backups aller Daten durchführen. ▪ Testen Sie Backups auf Funktionalität.
9. Findet eine Ereignisprotokollierung in den IT-Systemen statt?	☐	☐	▪ Aktivieren Sie ggf. die systemseitige Protokollierung, um Änderungen nachverfolgen und eine Systemhistorie erstellen zu können. ▪ Schaffen Sie ggf. manuelle Ersatzprozesse, z. B. über ein Ticketsystem, in welchem beauftragte Installationen und Änderungen nachgehalten werden.
10. Gibt es vergleichbare Vorgaben für installierte Apps auf Smartphones?	☐	☐	Legen Sie fest, welche Applikationen auf dienstlichen Mobilgeräten installiert werden dürfen und stellen Sie sicher, dass die o. g. Vorgaben ebenfalls umgesetzt werden.

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.