Firmen-Cyberversicherung

Wie gut ist Ihre IT-Sicherheit? Machen Sie den Check.

Für einen guten Schutz vor Cyber-Angriffen sollte die Cyber-Sicherheit fest im Arbeitsalltag verankert sein. Eine klare Sicherheits-Organisation, transparente Informationen für die Mitarbeiter und regelmäßige Sensibilisierung sorgen für höchstmöglichen Schutz.

Je häufiger Sie – oder Ihr IT-Beauftragter – die hier aufgeführten Punkte mit einem „JA" abhaken können, umso besser ist Ihr Unternehmen geschützt. Punkte, die Sie mit „NEIN" ankreuzen, sollten Sie auf den Prüfstand stellen und Maßnahmen zu Ihrer Verbesserung einleiten. Cyber-Sicherheit ist Chefsache.

Zugänge zu den IT-Systemen	JA	NEIN
Für alle IT-Systeme sind unterschiedliche Nutzer- und Befugnisebenen vorhanden (Administrator/Benutzer).	☐	☐
Jeder Mitarbeiter verfügt über ein eigenes Benutzerkonto.	☐	☐
Administratorenrechte werden nur von Administratoren zur Erledigung entsprechender Tätigkeiten verwendet.	☐	☐
Es ist technisch sichergestellt, dass Passwörter bestimmte Mindestanforderungen erfüllen – insbesondere mit Blick auf die Mindestanzahl der Zeichen. Empfehlung: Passwortrichtlinie des Bundesamtes für Sicherheit und Informationstechnik (bsi.bund.de)	☐	☐

Schutz gegen unberechtigten Zugriff	JA	NEIN
IT-Systeme mit erhöhtem Risiko* sind beispielsweise durch ■ eine Firewall, ■ ein Intrusion Detection System (IDS) und durch ein Intrusion Prevention System (IPS), ■ 2-Faktor-Authentisierung oder durch ähnlich wirksame Maßnahmen geschützt.	☐	☐
Mobile Geräte, wie Smartphones oder Laptops, sind z. B. durch ■ Verschlüsselung von Datenträgern, ■ Remote-Wipe-Funktionen, ■ Endpoint Detection and Response (EDR) oder durch ähnlich wirksame Maßnahmen geschützt.	☐	☐
Die IT-Systeme verfügen über einen stets aktuellen Schutz gegen Schadsoftware – z. B. Virenscanner, Code Signing, Application Firewall oder ähnlich wirksame Maßnahmen.	☐	☐

Formular Zurücksetzen

Firmen-Cyberversicherung

Wie gut ist Ihre IT-Sicherheit? Machen Sie den Check.

Patch Management	JA	NEIN
Sicherheitsupdates werden zeitnah** installiert.	☐	☐
Systeme und Anwendungen mit bekannten Sicherheitslücken befinden sich nur mit zusätzlichen Sicherheitsmaßnahmen im Firmennetzwerk. Zum Beispiel durch Segmentierung ohne Internetzugriff.	☐	☐

Datensicherung	JA	NEIN
Datensicherungen/Backups werden mindestens wöchentlich erstellt.	☐	☐
Sie werden ■ physisch getrennt aufbewahrt oder ■ auf Datenträgern/Systemen gespeichert, bei denen sichergestellt ist, dass eine Änderung oder Vernichtung durch das System selbst oder durch Nutzer und Befugnisebenen nicht möglich ist. Die Backup-Server sind nicht im gleichen Managementsystem (z. B. Active Directory) eingebunden.	☐	☐
Die Funktion des Sicherungs- und Wiederherstellungsprozesses wird mindestens jährlich getestet und dokumentiert.	☐	☐

Hinweise & Erläuterungen:

***IT-Systeme mit erhöhtem Risiko** sind z. B. Geräte, die dauerhaft oder zeitweise direkt über das Internet erreichbar sind, wie Server, Industriesteuerungssysteme, Medizintechnik, Gebäudeautomatisierung oder mobil eingesetzte Geräte wie Laptops.

Die **zeitnahe Installation von Sicherheitsupdates bedeutet bei Geräten mit einem erhöhten Risiko innerhalb von 14 Tagen nach Veröffentlichung. Bei allen übrigen Geräten innerhalb von 30 Tagen.

Firmen-Cyberversicherung – Verlässlichkeit und Transparenz von Beginn an

Falls Sie sich für die Firmen-Cyberversicherung der Mannheimer entscheiden oder bereits entschieden haben, sollten Sie sich bei einem Schaden auf die von Ihnen erwarteten Leistungen verlassen können. Dazu sind die hier beschriebenen Sicherheitsaspekte Mindestvoraussetzungen, die Ihre IT-Systeme vor Eintritt eines Schadens erfüllen müssen. Im Detail können Sie die sogenannten Obliegenheiten in den **Allgemeinen Versicherungsbedingungen für die Firmen-Cyberversicherung** unter dem Abschnitt A1-16.1 nachlesen.

Formular Zurücksetzen

Mannheimer Versicherung AG

Augustaanlage 66, 68165 Mannheim
Telefon 06 21. 4 57 80 00
Telefax 06 21. 4 57 80 08
mannheimer.de

Ein Unternehmen des Continentale Versicherungsverbundes auf Gegenseitigkeit.

HF_065 0124