Digitale Sicherheit für Ihr Unternehmen

Checkliste KuBuS® Cyber

Dringender Sicherheitshinweis

Kaum ein Tag vergeht ohne Cyber-Attacken. Das Risiko nimmt täglich zu.
Das Problem: 80 % aller Unternehmer/-innen sind der Meinung, dass Ihr Unternehmen ausreichend gegen Cyber-Angriffe geschützt ist oder das eigene Unternehmen für Angreifer nicht interessant genug sei.

Oftmals werden die notwendigen Sicherheitsvorkehrungen in den Unternehmen jedoch gar nicht getroffen oder die risikogerechten Sicherheitsstandards nicht eingehalten. Zum Beispiel verzichtet noch jedes fünfte Unternehmen auf einen Schutz durch ein Virenschutzprogramm.

Andere wichtige Elemente im betrieblichen Alltag sind ebenfalls nicht zu unterschätzen, wie zum Beispiel die Datenschutzgrundverordnung. Insbesondere die technischen und organisatorischen Maßnahmen (TOMs) sollten bei allen Unternehmen ein Begriff sein.

Haben Sie alle notwendigen Sicherheitsvorkehrungen getroffen?

Wir haben für Sie eine Checkliste erarbeitet, um Ihnen unsere Mindestvoraussetzungen für den Abschluss einer Cyber-Versicherung näher zu bringen. Denn wir möchten Ihnen auch im Ernstfall sagen: **Wenn Ihr IT-System gehackt wird, stehen wir an Ihrer Seite!**

Wir empfehlen Ihnen diese Checkliste zusammen mit Ihrem IT-Fachmann im eigenen Haus oder Ihrem externen Dienstleister gemeinsam durchzugehen und gegebenenfalls entsprechende Maßnahmen zu ergreifen. Bedenken Sie immer: **IT-Sicherheit ist Chefsache!**

KuBuS® Cyber im Überblick

Voraussetzungen an die IT-Systeme

Zugangskontrollen für die IT-Systeme

1.	Es sind für alle IT-Systeme unterschiedliche Benutzerebenen vorhanden (Administrator/Benutzer)?	☐
2.	Jeder Mitarbeiter verfügt über ein eigenes Benutzerkonto	☐
3.	Administratorenrechte werden nur von Administratoren zur Erledigung entsprechender Tätigkeiten verwendet?	☐
4.	Die Nutzer wurden angewiesen komplexe Passwörter zu verwenden (z. B. gemäß Empfehlung des BSI)?	☐

Schutz gegen unberechtigten Zugriff

5.	Die IT-Systeme sind durch einen zusätzlichen Schutz gegen unberechtigten Zugriff ausgerüstet, wie z. B. Firewall, 2-Faktor-Authentifizierung, Verschlüsselung von Datenträgern oder VPN-Verbindungen?	☐
6.	Die IT-Systeme verfügen über einen Schutz gegen Schadsoftware mit automatischen Sicherheitsupdates/Virendefinitionen, wie z. B. Virenscanner, Code Signing, Application Firewall oder ähnlich wirksamen Maßnahmen?	☐

Patch-Management

7.	Die unverzügliche Installation von relevanten Sicherheitspatches auf den IT-Systemen ist gewährleistet?	☐
8.	Systeme und Anwendungen mit bekannten Sicherheitslücken befinden sich nicht ohne zusätzliche Sicherheitsmaßnahmen im Firmennetzwerk?	☐

Schadenminderungskosten

9.	Datensicherungen werden mindestens wöchentlich durchgeführt und physisch getrennt aufbewahrt?	☐
10.	Datensicherungen werden nach Abschluss auf Fehler überprüft (verifiziert)?	☐
11.	Es werden regelmäßige Sicherungs- und Wiederherstellungstest durchgeführt?	☐

Zurücksetzen

S.6e.5075/06.22

Continentale Sachversicherung AG
Ruhrallee 92 • 44139 Dortmund
www.continentale.de
Ein Unternehmen des Continentale Versicherungsverbundes auf Gegenseitigkeit

Die Continentale