FAGELAXY GmbH

Köln, 10.0ktober 2026 CF

Cyberversicherung: Anforderungen an die IT-Sicherheit

Cyberversicherer stellen zunehmend konkrete Anforderungen an die IT-Sicherheit von Unternehmen. Diese Maßnahmen sind häufig Voraussetzung für den Abschluss einer Police, beeinflussen die Prämienhöhe und können im Schadenfall entscheidend dafür sein, ob und in welchem Umfang Leistungen erbracht werden.

Wichtig ist dabei nicht allein das Vorhandensein einzelner Schutzmaßnahmen. Versicherer erwarten in der Regel, dass diese Maßnahmen dokumentiert, verbindlich umgesetzt und regelmäßig überprüft werden.

Typische Anforderungen

Mehr-Faktor-Authentifizierung (MFA)
Versicherer erwarten häufig eine Mehr-Faktor-Authentifizierung für E-Mail-Konten, Fernzugriffe, Cloud-Dienste und Administratorkonten. Zunehmend werden phishing-resistente Verfahren gefordert, etwa Hardware-Sicherheitsschlüssel, Passkeys oder FIDO2-basierte Lösungen.

Schutz von Endgeräten und Servern
Auf Arbeitsplatzrechnern und Servern wird in der Regel ein moderner Endpoint-Schutz erwartet, etwa EDR- oder XDR-Lösungen. Oft wird zusätzlich eine zentrale Überwachung beziehungsweise eine kontinuierliche Alarmierung verlangt. Ein herkömmlicher Virenschutz allein genügt vielen Versicherern nicht mehr.

Datensicherung und Wiederherstellung
Backups sollten regelmäßig erstellt, verschlüsselt und vom Produktivsystem getrennt aufbewahrt werden. Besonders wertvoll sind offline gespeicherte oder unveränderbare Sicherungen. Zusätzlich erwarten Versicherer häufig dokumentierte Wiederherstellungstests, die belegen, dass Daten im Ernstfall tatsächlich nutzbar sind.

Patch-Management
Ein strukturierter Update-Prozess gehört zu den zentralen Voraussetzungen. Dazu zählen ein vollständiges Systeminventar, festgelegte Reaktionszeiten und Nachweise darüber, wann Sicherheitsupdates eingespielt wurden. Kritische Schwachstellen müssen häufig innerhalb eines definierten Zeitraums, beispielsweise sieben bis 30 Tagen, behoben werden.

Zugriffs- und Rechteverwaltung
Administrative Zugänge sollten von normalen Benutzerkonten getrennt sein. Versicherer erwarten häufig das Prinzip der minimalen Berechtigungen, eine kontrollierte Vergabe privilegierter Zugriffe und gegebenenfalls eine Segmentierung des Netzwerks, um die Ausbreitung eines Angriffs einzuschränken.

Notfall- und Incident-Management
Ein schriftlicher Notfallplan beschreibt, welche Personen im Ernstfall welche Aufgaben übernehmen, wie Vorfälle gemeldet werden und in welcher Reihenfolge Systeme wiederhergestellt werden. Versicherer legen zunehmend Wert darauf, dass dieser Plan nicht nur existiert, sondern auch regelmäßig geübt wird.

Sensibilisierung der Mitarbeitenden
Da viele Angriffe über E-Mails oder manipulierte Links beginnen, werden Sicherheits- und

© Copyright by Christian Fagel * Fagelaxy GmbH, Köln * www.fagelaxy .de * info@fagelaxy.de

Phishing-Schulungen häufig erwartet. Teilnahmenachweise, Testergebnisse und regelmäßige Wiederholungen können dabei als Beleg dienen.

Bedeutung von Nachweisen

Im Antrags- oder Verlängerungsprozess fragen Versicherer häufig nicht nur, ob bestimmte Maßnahmen vorhanden sind, sondern verlangen auch Belege. Dazu können Richtlinien, Auswertungen zur Abdeckung von Endgeräten, Backup-Konzepte, Protokolle von Wiederherstellungstests, Patch-Berichte sowie Schulungsnachweise gehören.

Ein täglich laufender Backup-Job ist allein meist nicht ausreichend. Entscheidend ist unter anderem, ob eine vom Produktivnetz getrennte oder unveränderbare Sicherungskopie existiert und wann zuletzt erfolgreich Daten wiederhergestellt wurden.

2do:

Unternehmen sollten ihre IT-Sicherheitsmaßnahmen vor Abschluss oder Verlängerung einer Cyberversicherung sorgfältig prüfen und dokumentieren. Die Anforderungen unterscheiden sich je nach Versicherer und Policenbedingungen. Eine lückenlose, nachvollziehbare Dokumentation reduziert nicht nur das Risiko im Schadenfall, sondern erleichtert auch die Zusammenarbeit mit dem Versicherer.

© Copyright by Christian Fagel * Fagelaxy GmbH, Köln * www.fagelaxy .de * info@fagelaxy.de