Ein Kaufleitfaden für Cyberversicherungen

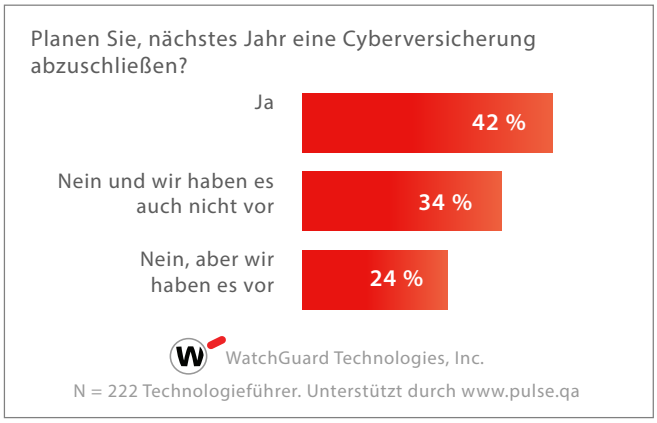
Multifaktor-Authentifizierung (MFA) ist unverzichtbar, wenn Sie eine Cyberversicherung für Ihr Unternehmen abschließen wollen.

Angesichts der jüngsten Zunahme von Cybersicherheitsvorfällen und Ransomware-Attacken beantragen immer mehr Unternehmen Cyberversicherungen. Dabei müssen sie inzwischen eine neue Voraussetzung erfüllen: den Schutz ihrer Anwender und Vermögenswerte durch Multifaktor-Authentifizierung.

Die richtige Herangehensweise bei der Wahl Ihrer Cyberversicherung

Woher wissen Sie, ob Sie eine Cyberversicherung brauchen?

Die Anforderungen an eine Cyberversicherung unterscheiden sich bei großen und kleineren Unternehmen in wesentlichen Punkten. Das Risiko, Opfer eines erfolgreichen Cyberangriffs zu werden, ist für kleinere Firmen höher als für größere, da sie häufig nicht über das Budget und Know-how verfügen, um wirksame Cybersicherheitsstrategien umzusetzen. Große Konzerne werden mit höherer Wahrscheinlichkeit von Hackern angegriffen und schließen daher Policen direkt bei den Versicherern ab. Zudem haben sie eigene Rechts-, PR- und Technologie-Experten. Kleine und mittlere Unternehmen betrachten Cyberversicherungen zunehmend als weiteres Mittel zur Risikoeindämmung. Sie beziehen sie meist über Agenturen und brauchen fürs Krisenmanagement in der Regel Hilfe von außen.



Finden Sie die richtige Police

Wussten Sie, dass Cyberangriffe nicht durch eine allgemeine Unternehmensversicherung gedeckt sind? Je nach Ihren Anforderungen gibt es verschiedene Abdeckungen und Bedingungen. Mit diesem Leitfaden können Sie sichergehen, dass Sie keine zu hohen Prämien zahlen und die Haftpflichtversicherung wählen, die Ihren Risiken und Schwachstellen tatsächlich entspricht.

Stellen Sie sicher, dass Ihr Unternehmen die Voraussetzungen erfüllt

Versicherer können Unternehmen ablehnen, die keine Multifaktor-Authentifizierung oder bestimmte Produktarten zum Schutz von Endpunkten nutzen. Manche Anbieter bevorzugen bei der Wahl ihrer Versicherungsnehmer Firmen, die Netzwerkfunktionen nutzen, um zu verhindern, dass Attacken das ganze System befallen.

Was ist durch eine Cyberversicherung abgedeckt?

Anders als bei allgemeinen Haftpflichtversicherungen gibt es bei Cyber-Haftpflichtversicherungen keine Pauschalabdeckung. Die meisten KMU mit einer Cyberversicherung haben nur eine Haftpflichtdeckung (50.000 USD), was bei schwerwiegenden Datenschutzverletzungen nicht ausreicht. Die Cyber-Haftpflicht kommt nur für Kosten auf, die durch Datenschutzverletzungen entstehen. Diese Kosten können jedoch rasant in die Höhe schnellen, wenn eine Verletzung aufgedeckt und publik gemacht wird. Folgendes ist in der Regel abgedeckt:

- **Kundenverlust**
- **Betriebsunterbrechung**
- **Bußgelder**
- **Rechtskosten**
- **Öffentlichkeitsarbeit**
- **Direkte finanzielle Verluste**

Arten von Cyberversicherungen

Hackerschutz: Versicherung gegen Cyberattacken und Hackerangriffe.

Diebstahl und Betrug: Deckt die Zerstörung oder den Verlust von Daten des Versicherungsnehmers infolge eines kriminellen oder betrügerischen Cybervorfalls ab, einschließlich Gelddiebstahl oder -transfer.

Forensik: Deckt die notwendigen rechtlichen, technischen oder forensischen Dienstleistungen zur Feststellung eines Cyberangriffs ab.

Betriebsunterbrechung: Deckt Ertragsausfälle und verbundene Kosten ab, wenn der Geschäftsbetrieb des Versicherungsnehmers aufgrund eines Cybervorfalls oder Datenverlusts zum Erliegen kommt.

Erpressung: Deckt die Kosten für die Untersuchung angedrohter Cyberangriffe gegen die Systeme des Versicherungsnehmers sowie für Zahlungen an Erpresser, die drohen, sensible Informationen zu erlangen und offenzulegen, ab.

Reputationsversicherung: Greift im Falle von Reputationsschäden und Verleumdung im Internet.

Verlust und Wiederherstellung von Computerdaten: Deckt physische Schäden an Computern und zugehörigen Komponenten ab, einschließlich der Kosten für die Wiederherstellung von Daten, Hardware, Software und anderen Informationen, die bei einer Cyberattacke zerstört oder beschädigt wurden.

Checkliste für Cyberversicherungen

Vor dem Risiko eines Cyberangriffs ist kein Unternehmen gefeit. Wenn Sie erwägen, Ihre Sicherheitsinfrastruktur um eine Versicherung zu ergänzen, werden Sie für deren Abschluss höchstwahrscheinlich Multifaktor-Authentifizierung einführen müssen. Mit dieser Checkliste können Sie Ihre derzeitigen Cybersicherheitsmaßnahmen prüfen und ermitteln, welche Versicherungsart für Sie die richtige ist.

Verwaltung

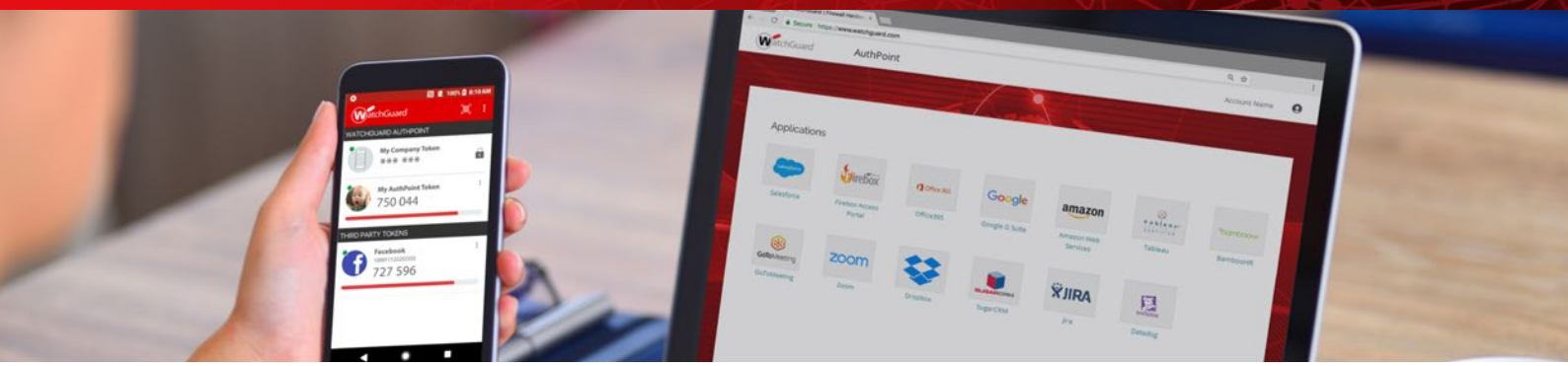
- Haben Sie genügend Budget für die Implementierungskosten und Versicherungsprämie?
- Haben Sie eine Bescheinigung?
- Wissen Sie, welche Versicherungsart zu Ihrem Unternehmen passt?
- Schulen Sie Ihr Personal in Best Practices bezüglich der Cybersicherheit?
- Kennen Sie die wesentlichen Schwachstellen Ihres Unternehmens?
- Halten Sie Vorgaben wie die DSGVO, HIPAA und PCI DSS ein, sofern Sie für Ihr Unternehmen gelten?

IT-Betrieb

- Haben Sie interne IT-Mitarbeiter oder Dienstleister, die sich um die Sicherheit kümmern?
- Führen Sie Sicherheitsprüfungen durch?
- Verfügen alle Computer über Antivirensoftware?
- Haben Sie einen Zeitplan für regelmäßige Systemsicherungen?
- Dokumentieren Sie bekannte Probleme oder Risiken?

Sicherheitskontrollen

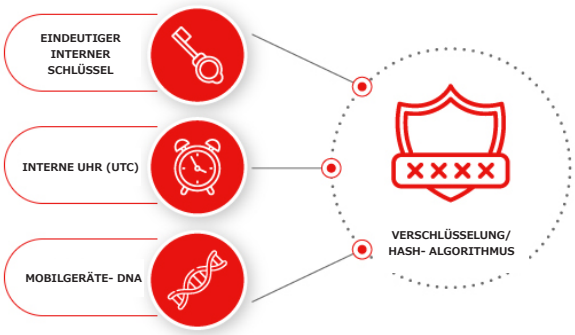
- Ist MFA vorgeschrieben, um den E-Mail-Zugang zu sichern?
- Ist MFA für jeglichen Fernzugriff auf Ihr Firmennetzwerk vorgeschrieben? Schützen Sie den lokalen und Remote-Zugriff auf Komponenten der Netzwerkinfrastruktur (Router, Firewalls)?
- Schützen Sie den lokalen und Remote-Zugriff auf die Endpunkte und Server Ihres Unternehmens?



Erfüllen Sie mit AuthPoint MFA die Voraussetzungen für Cyberversicherungen

Effektiver MFA-Schutz mit eindeutiger Mobilgeräte-DNA

AuthPoint verwendet eine Mobilgeräte-DNA zum Abgleich der Smartphones autorisierter Benutzer, bevor der Zugriff auf Systeme und Anwendungen gewährt wird. So kann ein Angreifer, der das Gerät eines Benutzers klont, um Zugang zu geschützten Systemen zu erhalten, blockiert werden, da sich die Geräte-DNA unterscheidet.



AuthPoint schützt Ihr Unternehmen und wehrt Cyberangriffe ab

SICHERHEIT FÜR SCHWERPUNKTBEREICHE	VERMEIDUNG DER GÄNGIGSTEN GEFAHREN
Benutzerzugang	Hacking von Zugangsdaten
Cloud-Anwendungen	Phishing
Unternehmensnetzwerke	Keylogger
Remote-Zugriff/VPN	Brute-Force-Angriffe

Anwenderfreundlich, Cloud-basiert und kosteneffizient.

Starten Sie noch heute Ihre 30-Tage-Testversion: watchguard.com/mfa-trial

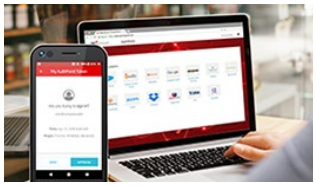
Informationen zu WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Netzwerksicherheit, Endpoint-Sicherheit, sicheres WLAN, Multifaktor-Authentifizierung und Network Intelligence. Über 18.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens und sorgen somit für den Schutz von mehr als 250.000 Kunden. Die Philosophie von WatchGuard ist es, Sicherheit auf Enterprise-Niveau für Unternehmen jeder Größenordnung und Art zu realisieren. Das macht WatchGuard insbesondere für mittelständische und dezentral aufgestellte Unternehmen zum idealen Anbieter. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im Pazifikraum.

Weitere Informationen finden Sie unter WatchGuard.de.

DIE UNIFIED SECURITY PLATFORM™ VON WATCHGUARD

Netzwerksicherheit



Multifaktor-Authentifizierung

Sicheres cloud-basiertes WLAN

Endpoint-Security

Mit diesem Dokument werden keine ausdrücklichen oder implizierten Gewährleistungen gegeben. Alle hier aufgeführten technischen Daten können sich ändern. Informationen zu zukünftigen Produkten, Ausstattungsmerkmalen und Funktionen werden zu gegebener Zeit zur Verfügung gestellt. ©2021 WatchGuard Technologies, Inc. Alle Rechte vorbehalten. WatchGuard, das WatchGuard Logo und AuthPoint sind eingetragene Marken von WatchGuard Technologies, Inc. in den USA und/oder anderen Ländern. Alle weiteren Markennamen sind das Eigentum ihrer jeweiligen Inhaber. Teilenr. WGCE67528_100821