Cyberrisiken minimieren – geschützt im Schadenfall

Cyberangriffe sind längst nicht mehr nur ein Problem grosser Konzerne – auch KMU geraten ins Visier. Die Folgen reichen von hohen Kosten über Reputationsverlust bis hin zur Existenzbedrohung. Mit der Cyberversicherung der AXA sind Unternehmen dreifach geschützt: durch Prävention, Soforthilfe im Ernstfall und Kostenübernahme für die Schadenbehebung.

1. Welche Leistungen sind versichert?

Unsere Versicherung übernimmt die Kosten für wirtschaftliche Schäden, schadenersatzrechtliche Folgen sowie Massnahmen, die helfen, einen drohenden Reputationsschaden abzuwenden. Und das nicht nur bei kriminellen Delikten, sondern auch, wenn fehlbares Handeln von Mitarbeitenden zugrunde liegt.

Soforthilfe und Expertenbegleitung	• 24/7-Hotline mit Cyberexpertinnen und -experten • Unterstützung bei der Schadenbehebung, auch wenn kein versichertes Ereignis vorliegt • Analyse von Sicherheitslücken und Präventionsempfehlungen • Kostenübernahme für Krisenkommunikation
Daten- und Systemwiederherstellung	• Kostenübernahme für die Wiederherstellung von Daten und Systemen, Beseitigung von Schadprogrammen und Wiederinstallation sowie Konfiguration von Systemen
Betriebsunterbrechung	• Ersatz von Ertragsausfall • Übernahme zusätzlicher Kosten zur Betriebsaufrechterhaltung
Datenschutzverletzungen	• Kosten für gesetzlich vorgeschriebene Benachrichtigungen, für juristische Beratung, für die Identifizierung von Betroffenen im Zusammenhang mit einem Straf-, Aufsichts- oder Verwaltungsverfahren
Haftpflichtschäden	• Übernahme berechtigter Schadenersatzansprüche • Abwehr unberechtigter Forderungen

2. Welche Erweiterungen zur Cyberversicherung gibt es?

Für lückenlosen Cyberschutz kann es je nach Branche und Grösse eines Betriebs sinnvoll sein, die Deckung der Cyberversicherung durch weitere Versicherungsleistungen zu individualisieren. Versicherbar sind:

Manipulation von E-Banking, Webshop oder Warenversand: Kostenübernahme bei Geldentwendung durch Manipulation an Zahlungsverkehrs-Apps, Online-Shops und Websites.

Telefon-Hacking und Zweckentfremdung des IT-Systems: Übernahme von Mehrkosten durch unbefugte Nutzung von Telefonanlagen oder IT-Systemen

Social Engineering: Absicherung bei Vermögensschäden infolge gezielter Täuschung von Mitarbeitenden durch Hacker

Cybererpressung: Erstattung von Lösegeldforderungen sowie Übernahme der Kosten für Verhandlungen mit Erpresserinnen und Erpressern

3. Welche Präventionsservices sind in der Cyberversicherung kostenlos enthalten?

Die Cyberversicherung der AXA schützt Sie nicht nur im Schadenfall, sondern bietet Ihnen auch ein kostenloses Basispaket an Präventionsservices. Diese Services helfen Ihnen dabei, Ihre eigenen Sicherheitslücken aufzudecken und Ihre Mitarbeitenden zu sensibilisieren.

Security Assessment	• 10-Fragen-Check für einen schnellen Überblick über potenzielle Cyberrisiken • Online-Support bei Fragen und Problemen
Schwachstellen-Scan	• Einmaliger automatisierter Scan zur Ersteinschätzung von IT-Schwachstellen • Benachrichtigung über identifizierte Schwachstellen
Security-Awareness-Training	• Eine Lizenz für interaktive Trainingseinheiten zu KMU-Cyberrisiken
Sensibilisierung durch Phishing-Simulationen	• Simulierte Phishing-Mails zur Sensibilisierung der Mitarbeitenden
Monitoring	• Überwachung einer E-Mail-Domain und einer Telefonnummer im Internet und im Darknet • Warnmeldung bei Datenlecks
Notfallplan	• Vorbereitung für den Ernstfall
Warnmeldungen	• Regelmässige Warnmeldungen zu aktuellen Cyberbedrohungen

Aktivieren Sie Ihre integrierten Präventionsservices ganz einfach unter **AXA.ch/basic-prevention**. Folgen Sie dort der Anleitung auf der Plattform – und halten Sie die Policennummer Ihrer Cyberversicherung bereit.

4. Welche Upgrades können bei den Präventionsservices vorgenommen werden?

Erweitern Sie die kostenlosen Präventionsservices Ihrer Cyberversicherung mit einem Upgrade und profitieren Sie von 20 % Rabatt auf die kostenpflichtigen Präventionsservices.



Security Assessment
- **Unbegrenzter** Onlinezugang zum umfassenden Assessment mit **80** Fragen
- **Detaillierter Risikobericht** mit Handlungsempfehlungen



Schwachstellen-Scan
- **Kontinuierliche** Überprüfung Ihrer IT-Sicherheit
- **Handlungsempfehlungen** zur Behebung der Schwachstellen
- **Monitoring** von Kreditkarten und Telefonnummern



Security-Awareness-Training
- **Unbegrenzte** Lizenzen für interaktive Trainingseinheiten zu KMU-Cyberrisiken

5. Was sind typische Schadenfälle?

Datenverlust
Der Server einer Werbeagentur wird trotz neuester Schutzsysteme von einem Computervirus befallen. Die Schadsoftware löscht oder beschädigt sämtliche Daten. Die AXA übernimmt alle Kosten für die Neuinstallation des Betriebssystems und der Programme sowie für das Zurückspielen der gesicherten Daten.

Ertragsausfall
Ein Spezialist für Outdoor-Bekleidung bietet seine Waren im eigenen Webshop an. Eine Attacke des Typs «Denial of Service» (DoS) blockiert das System, und der Webshop fällt für drei Tage aus. Die AXA übernimmt den Ertragsausfall von mehreren tausend Franken.

Schadenersatzforderung
Ein Möbelhändler betreibt einen Webshop. Ein Hotel bestellt neue Möbel und erhält eine vom System generierte Bestätigung. Aufgrund einer Hackerattacke beim Möbelhändler geht die Bestellung verloren. Der Hotelier reklamiert die unterbliebene Lieferung, verzichtet auf Nachlieferung und macht Schadenersatz geltend. Die AXA prüft die Schadenersatzforderung. Sie stuft einen Teil als ungerechtfertigt ein und wehrt ihn ab, übernimmt aber den gerechtfertigten Anteil.

Für die Soforthilfe bei einem Cybereereignis stehen Ihnen ausgewiesene Cyberexpertinnen und -experten von Oneconsult unter **+41 58 218 11 33** zur Verfügung (24/7).