baloise

Ideal für kleine und mittlere Unternehmen

Cyber-Risiken angucken statt wegducken

Baloise Cyber-Police

Risiken minimieren statt ignorieren.
Warum Unternehmen eine Cyber-Versicherung brauchen

Kleine und mittelständische Betriebe zunehmend betroffen

Die digitale Welt birgt nicht nur Chancen. Cyber-Angriffe sind längst keine exklusive Bedrohung für Großkonzerne mehr. Immer häufiger geraten auch kleine und mittlere Betriebe ins Fadenkreuz von Cyber-Kriminellen. Laut BSI-Bericht[1] ist die Bedrohung derzeit so hoch wie nie zuvor – und die Hacker gehen immer professioneller vor.

Cyber-Kriminalität verursacht pro Jahr Wirtschaftsschäden in Milliardenhöhe. Die Betrugsmethoden reichen dabei von Phishing bis zu Ransomware. Nicht selten steht die Existenz eines Betriebes auf dem Spiel.

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI), Bericht für 2023

Cyber-Angriffe oft nicht zielgerichtet

Fakt ist: An einer Cyber-Absicherung kommt heutzutage kein Unternehmen vorbei.

Denn inzwischen verfügen nahezu alle Unternehmen über
- E-Mail-Konten,
- E-Payment-/Kartenzahlungssysteme und
- gespeicherte Kundendaten.

Damit ist jedes Unternehmen potenziell gefährdet und für Hacker interessant. Sehr häufig schauen diese zuerst, welche Systeme gehackt werden können und um welches Unternehmen es sich handelt. Erst dann entscheiden sie, wie sie dem Betrieb schaden können.

Jedes zweite Unternehmen Opfer eines Angriffs

In den letzten Monaten wurde mehr als jedes zweite deutsche Unternehmen Opfer eines Cyber-Angriffs. Die Gefahren sind vielfältig und bedrohen Unternehmen jeder Größe. Höchste Zeit, sich proaktiv zu schützen. Durchschnittlich werden pro Tag knapp 70 neue Schwachstellen in Software-Produkten entdeckt sowie 250.000 neue Schadprogrammvarianten.

Die Gefahren für Unternehmen sind vielfältig:

- Schwache Passwörter
- Verspätet ausgeführte System-Updates/Patches (dadurch Software-Schwachstellen)
- Nutzung privater Geräte im internen WLAN-Netzwerk
- Kartenzahlungssysteme für Kundinnen und Kunden
- Nutzung öffentlicher WLAN-Netzwerke

Virenschutz, Firewall sowie starke Passwörter gehören in vielen Betrieben schon zum Standard – häufig hapert es jedoch bei der Datensicherung sowie beim Patch-Management. Wichtig ist es, alle Einfallstore für mögliche Cyber-Angriffe durch technische und organisatorische Maßnahmen zu minimieren – und das verbleibende Restrisiko mit einer Cyber-Versicherung abzusichern.

Phishing & Co.: Achillesferse Mensch

Die größte Schwachstelle in der digitalen Sicherheitskette? Der Mensch. Oftmals verursachen Mitarbeitende Cyber-Angriffe unabsichtlich mit, indem sie eine scheinbar harmlose Phishing-Mail öffnen. Das sogenannte „Social Engineering“ ist eine beliebte Methode. Dabei täuschen Cyber-Kriminelle falsche Identitäten vor – was durch den Einsatz von KI und ChatGPT begünstigt wird. Auch die Zahl der Fake-President-Fälle nimmt dadurch seit geraumer Zeit wieder zu.

Cyber-Angriffe sind weltweit das größte Risiko für Unternehmen – noch vor Betriebsunterbrechungen und Naturkatastrophen.

Wir bieten mit der Baloise Cyber-Police u. a.:

Ideal für kleine und mittlere Unternehmen

- Leistungs-Update-Garantie – für stets aktuellen Versicherungsschutz
- Volle Erstattung bei Betriebsunterbrechungs-Schäden nach Ablauf der vereinbarten Wartezeit
- Schnelle Abschlagszahlung im Schadenfall
- Einfache Antragstellung – nur wenige Risikofragen

Cyber-Kosten

- Soforthilfe und Forensikkosten (Kosten der Ursachen-ermittlung)
- Krisenkommunikation/PR-Maßnahmen
- Benachrichtigungskosten und Callcenter-Leistung
- Systemverbesserungen nach einer Informations-sicherheitsverletzung
- Kulanzgutscheine für entstandene Mehrkosten bei Kundinnen und Kunden des Versicherungsnehmers

Cyber-Drittschadendeckung (Haftpflicht)

- Befriedigung oder Abwehr von Ansprüchen Dritter
- Rechtswidrige elektronische Kommunikation
- Vertragsstrafen wegen der Verletzung von Geheim-haltungspflichten und Datenschutzvereinbarungen
- Vertragliche Haftpflicht bei Datenverarbeitung durch Dritte
- Rechtsverteidigungskosten
- Ansprüche der E-Payment-Serviceprovider

Top-Platzierung im deutschen Markt

Unsere **Baloise Cyber-Police** erhält regelmäßig hervorragende Bewertungen durch das anerkannte Ratingunternehmen Franke und Bornberg – und belegt damit eine Spitzenposition im deutschen Markt!

Cyber-Eigenschadendeckung

- Betriebsunterbrechung durch Ursachenermittlung im Schadenfall
- Betriebsunterbrechung durch Ausfall von ent- und unentgeldlichen Dienstleistern, z. B. Cloud-Anbietern, IT-Dienstleistern oder Rechenzentren
- Betriebsunterbrechung durch technische Probleme (Fehlfunktionen) der informations-verarbeitenden Systeme
- Wiederherstellung von Daten (auch Entfernen der Schadsoftware)
- Cyber-Diebstahl/Cyber-Erpressung
- Cyber-Betrug
- Übernahme von Belohnungsgeldern
- Elektronischer Zahlungsverkehr
- Ersatz von Hardware
- Fehlerhafter Versand von Waren
- Telefonmehrkosten/erhöhte Nutzungsentgelte, z. B. für Strom, Gas oder Wasser (wenn informations-verarbeitende Systeme missbraucht werden, um Krypto-Währungen zu erstellen, sogenanntes Krypto-Mining)

Verschärft:
Haftung durch EU-DSGVO erhöht das finanzielle Risiko deutlich

Mit der Einführung der Datenschutzgrundverordnung (DSGVO) im Jahr 2018 wurden die rechtlichen Anforderungen an den Schutz personenbezogener Daten verschärft. Verstoßen Unternehmen gegen die DSGVO, drohen Geldbußen von bis zu 20 Mio. EUR bzw. von bis zu 4 % des weltweiten Vorjahresumsatzes – je nachdem, welcher Betrag höher ist. Bußgelder bis zu 60.000 EUR sind selbst für kleine Betriebe keine Seltenheit. Eine **Cyber-Versicherung** kann Unternehmen helfen, diese finanziellen Risiken abzudecken.

Professionelle Unterstützung ist notwendig und hilfreich, z. B. bei
- behördlichen Meldefristen bei verlorenen Daten,
- Betriebsstillstand oder
- Krisenmanagement.

Durch frühzeitiges Handeln und eine qualifizierte Meldung nach DSGVO verringern Unternehmen das Bußgeld und sichern so ihre Existenz.

Eine **Cyber-Versicherung** deckt Informationssicherheitsverletzungen ab. Dazu zählen:

- Klassische Hackerangriffe (Netzwerksicherheitsverletzungen)
- Datenschutzverletzungen

Schadenfälle können damit auch ohne Infektion durch Schadsoftware entstehen, z. B. durch versehentliches Veröffentlichen von Daten der Kundinnen und Kunden. Auch für diese Fälle wurde die **Cyber-Versicherung** entwickelt.

Wer benötigt eine Cyber-Versicherung?

Jedes Unternehmen ist durch Cyber-Angriffe gefährdet. Ohne Ausnahme. Selbst kleine und mittelständische Betriebe
- besitzen E-Mail-Konten,
- speichern wichtige (Kunden-)Daten in elektronischer Form,
- nutzen Geräte für Kartenzahlung.

Ein erster Einstieg in die Cyber-Absicherung ist z. B. auch mit dem Baustein **Cyber-Basisrisiko** möglich.

Einsteigeroption Cyber-Basisrisiko

Einen preisgünstigen, ersten Basisschutz gegen Cyber-Gefahren erhalten Unternehmen mit dem Baustein **Cyber-Basisrisiko**, der zusammen mit unserer Betriebshaftpflichtversicherung abgeschlossen werden kann.

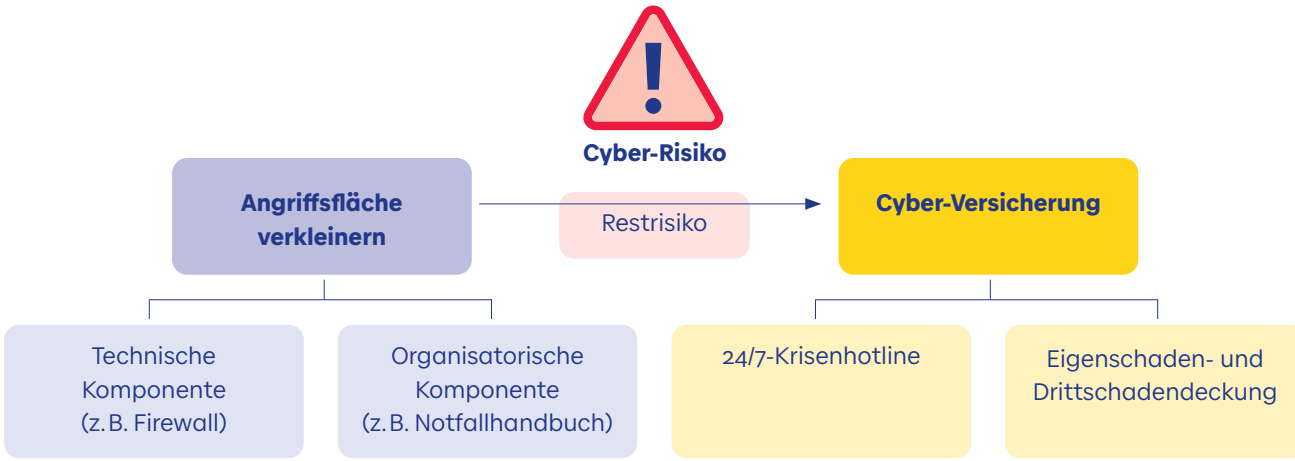
Welche Tätigkeiten erhöhen das Risiko?

Viele Tätigkeiten erhöhen Ihr betriebliches Cyber-Risiko. Die wichtigsten im Überblick:

- Betrieb einer eigenen Infrastruktur für Online-Handel
- Speichern und Bearbeiten von sensiblen Daten (z. B. Daten von Kundinnen und Kunden, Kontoverbindungen/Kreditkartendaten)
- Nutzung von Dienstleistern zur Auftragsdatenverarbeitung
- Erlaubnis zur Nutzung privater Geräte innerhalb des Unternehmens

Betriebliches Restrisiko eingrenzen: effektiver Schutz gegen Cyber-Risiken

Technologien wie Firewall und Antivirensoftware bieten hohen Schutz vor Cyber-Attacken. Auch organisatorische Maßnahmen wie geregelte Zugangsrechte oder das Vieraugenprinzip unterstützen diese. Wichtig, denn man geht allein von circa 250.000 neuen Schadsoftware-programmen täglich aus. Ein Unternehmen wird nie eine hundertprozentige Absicherung erreichen. Und kein IT-Dienstleister kann eine hundertprozentige Sicherheit vor Cyber-Attacken garantieren – oder die Haftung übernehmen, wenn doch etwas passiert. **Ein Restrisiko bleibt immer. Dieses Restrisiko sichert eine Cyber-Versicherung ab.**



Expertinnen und Experten der Schadenhotline sind täglich rund um die Uhr für Sie erreichbar

Auch wenn die eigene IT-Abteilung oder die beauftragten IT-Dienstleister die Firmennetzwerke hervorragend administrieren und sich perfekt um die Technik kümmern, gibt es keinen absoluten Schutz. Im Schadenfall stehen Ihnen unsere Spezialistinnen und Spezialisten zur Seite.

1. Am Telefon
Spezialisierte IT-Expertinnen und -Experten helfen im Versicherungsfall direkt weiter.

2. Per Fernwartung
Die Expertinnen und Experten der Assistance-Hotline verbinden sich mit dem System und lösen so die meisten Probleme.

3. Vor Ort
Spezialistinnen und Spezialisten veranlassen vor Ort alle erforderlichen Schritte.

Volle Kostenübernahme für die Prüfung

Ist das eine Cyber-Attacke? Eine schwierige Entscheidung – da hilft nur anrufen. Je schneller Unternehmen unsere Hotline kontaktieren, umso effektiver können die Ursachen behoben und das Schadenausmaß begrenzt werden. Wir übernehmen alle Forensikkosten, bis feststeht, ob ein Versicherungsfall vorliegt oder nicht.

Liegt kein Versicherungsfall vor, fordern viele Versicherungsunternehmen eine Beteiligung von 50 % an den angefallenen Kosten. Nicht bei uns! Wir garantieren die volle Kostenübernahme für die Prüfung bis zum vereinbarten Betrag.

Informieren Sie sich jetzt!

Baloise Sachversicherung AG
Deutschland

Basler Str. 4
61352 Bad Homburg
info@baloise.de
www.baloise.de

BAS 3556 05.24 WMD