Basler Versicherungen

Basler Cyber-Police

Gewappnet für die Herausforderungen der modernen Welt

Cyber-Risiken nehmen zu

Unsere moderne Welt ist vernetzt wie nie zuvor. Wir sind mehr on- als offline, teilen, liken und speichern virtuell. Natürlich nicht nur privat – auch Wirtschaftsprozesse sind ohne Informationstechnologie heute nicht mehr denkbar. Produktionsprozesse sind vernetzt und das Internet ist damit längst zum Dreh- und Angelpunkt geworden. Das klingt wunderbar nach technologischem Fortschritt ohne Grenzen. Doch haben Sie schon einmal an die damit verbundenen Risiken gedacht?

Datendiebstahl oder Betriebsstillstand durch einen Hacker- oder DDoS-Angriff sind heute keine Seltenheit mehr. Unternehmen jeglicher Größe und Branche sind von Angriffen bedroht. Die finanziellen Folgen von Cyber-Kriminalität können vor allem für kleine und mittelständische Unternehmen sehr schnell existenzbedrohende Ausmaße annehmen. Denn diese Betriebe verfügen in der Regel weder über die finanziellen Mittel, noch sind sie für die Bewältigung einer solchen Attacke gewappnet.

Die Gründe, warum das Cyber-Risiko innerhalb der letzten Jahre verstärkt ansteigt, sind vielfältig. Sicherlich sind Cyber-Kriminelle professioneller geworden. Doch daneben entstehen weitere Risiken durch den wachsenden technischen Fortschritt:

Rasante Entwicklungen erhöhen die Cyber-Risiken

- **Industrie 4.0**
- **Internet of Things / Smart Home**
- **Verstärkte Nutzung von Online-Bezahlvorgängen**
- **Rasantes Wachstum gespeicherter Datenmengen**
- **Abhängigkeit der Produktions- und Kommunikationsprozesse von Online-Anbindungen**
- **Trends (Clouds, Bring Your Own Device „BYOD“, autonomes Fahren)**
- **Internet – keine Landesgrenzen für Kriminelle**

Das moderne Risiko kommt also virtuell daher. Man kann es nicht sehen – vielleicht wird es deshalb auch häufig unterschätzt. Obwohl drei Viertel aller Unternehmen schon einem Angriff ausgesetzt waren[1] und Cyber-Risiken unter den Top-Risiken für Unternehmen rangieren[2]. Das bedeutet: Es trifft nicht nur die anderen!

Über den bisher üblichen Versicherungsschutz sind die vielen neuen Risiken nicht gedeckt. Gerne helfen wir Ihnen und Ihren Kunden auf diesem neuen Weg. Lassen Sie uns gemeinsam die Schwachstellen erkennen, geeignete präventive Maßnahmen ergreifen und Ihre Kunden mit dem passenden Versicherungsschutz für die Herausforderungen der modernen Welt wappnen.

1 Bitkom e.V., 2015, Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter

2 KPMG 2017

Wer benötigt eine Cyber-Versicherung?

Wirklich jedes Unternehmen und damit jeder Ihrer Firmenkunden ist durch Cyber-Angriffe gefährdet. Ohne Ausnahme. Selbst kleine und mittelständische Betriebe speichern wichtige Daten in elektronischer Form oder akzeptieren Kreditkartenzahlungen.

Welche Tätigkeiten erhöhen das Risiko?

Viele Tätigkeiten erhöhen das Risiko Ihrer Kunden. Welche die wichtigsten sind, sehen Sie hier im Überblick:

- Betrieb einer eigenen Infrastruktur für Online-Handel
- Speichern und Bearbeiten von sensiblen Daten
- Nutzung von Dienstleistern zur Auftragsdatenverarbeitung
- Erlaubnis zur Nutzung privater Geräte innerhalb des Unternehmens
- Nutzung automatisierter Produktionssysteme (ICS)

Was ist eine Distributed-Denial-of-Service-Attacke (DDoS)?

DDoS ist ein Angriff mehrerer Computer im Verbund (Botnetze) auf eine Website oder Netzinfrastruktur, was zu Überlastung und Ausfällen führt.

Angreifer und ihre Motivation

Doch wer sind die Angreifer aus der virtuellen Welt? Was sind ihre Motive?

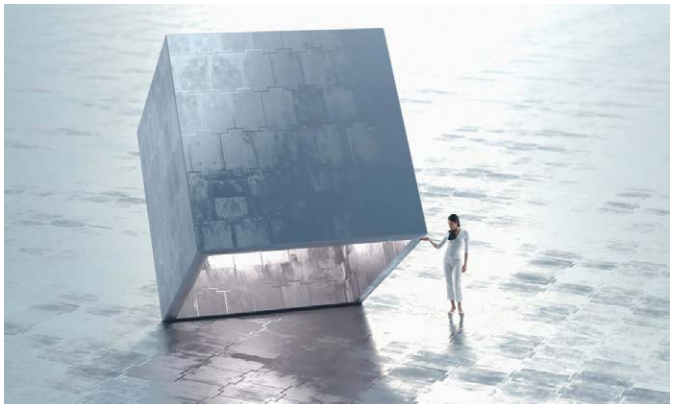
Sehen Sie selbst: Den einen speziellen Angreifer gibt es leider nicht. Und genauso vielfältig wie die Angreifer selbst sind deren Beweggründe.

Angreifer	Ziele
(Organisierte) Kriminalität	Finanzielles Interesse (bspw. durch Erpressung)
(Ehemalige) Mitarbeiter	Rache, destruktive Motive
Geheimdienste	(Wirtschafts-)Spionage
Wettbewerber	(Wirtschafts-)Spionage
Hacktivisten	Destruktive, religiöse oder idealistische Motive
Scriptkiddies	Reputation, destruktive Motive

Die Angriffsarten reichen vom physischen Datendiebstahl über Hackerangriffe mittels Trojaner oder Phishing bis hin zur Erpressung über Ransomware. Und täglich kommen neue Angriffsarten hinzu.

Wie gravierend sind die Auswirkungen von Cyber-Risiken?

Ihren Kunden ist sicherlich bewusst, dass eine Gefahr durch Cyber-Risiken besteht. Trotzdem werden die Auswirkungen häufig unterschätzt bzw. wird die Gefahr für das eigene Unternehmen nicht richtig erkannt.



Stellen Sie sich vor, die Systeme eines Online-Shops werden durch einen DDoS-Angriff eine Woche lahmgelegt. Nichts geht mehr – tagelang! Ein immenser finanzieller Verlust für das Unternehmen!

Daneben sind natürlich auch Datenmanipulation oder Datenverlust durch Erpressung denkbar. Auch kleine und mittelständische Betriebe können so bedroht werden. Im schlimmsten Fall kommt es zur Unterbrechung der gesamten Produktion und damit zu einer Betriebsunterbrechung.

Oder denken Sie an Hotels, Galerien und Fitnesscenter! Diese speichern z. B. Kundendaten und nutzen die Abrechnungssysteme von Kreditkartenfirmen. Bei Kreditkartenmissbrauch sind dann auch die Forderungen der Kreditkartenindustrie zu ersetzen. So können schnell bedrohlich hohe Summen zusammenkommen.

Alles zu abstrakt? Schadenbeispiele helfen!

Ein paar weitere reale Schadenbeispiele sollen Ihnen die Gefahr verdeutlichen. Sie werden sehen, dass insbesondere kleine und mittelständische Betriebe von vielfältigen Cyber-Risiken bedroht werden und nicht nur große Industriebetriebe davon betroffen sind.

Arztpraxen

Ein Mitarbeiter der Praxis veröffentlicht anstelle einer Unternehmensbroschüre eine Patientenakte auf der Homepage. Der betroffene Patient wird auf den Fehler aufmerksam und erhebt einen Anspruch auf Geldentschädigung wegen der Verletzung des Persönlichkeitsrechts.

Produktionsbetriebe

Durch einen Hackerangriff werden Produktionsparameter verändert, wodurch die Produktion gestört wird. Der Abnehmer des Produzenten kann nicht mehr just in time produzieren und macht Schadenersatzansprüche geltend. Dadurch, dass der Fehler zunächst nicht lokalisiert wurde, steht der Betrieb für eine kurze Zeit still und es fallen hohe Kosten für die Forensik an.

Online-Händler

Ein Online-Händler erhält ein Erpresserschreiben. Darin wird mit einer DDoS-Attacke gedroht, wenn nicht innerhalb von 3 Tagen ein Lösegeld in Bitcoins gezahlt wird. Zum Beweis der Fähigkeit des Erpressers wird der Online-Shop bereits für 10 Minuten attackiert und ist dadurch für Kunden nicht erreichbar. Da das Lösegeld nicht gezahlt wird und auch keine Cyber-Police inklusive einer IT-Dienstleistung besteht, wird der Online-Shop 3 Tage später für 2 Wochen angegriffen. Darunter leidet die Reputation des Online-Shops und es kommt durch Kundenabgänge zu Umsatzeinbußen.

Handelsbetriebe

Ein mittelständischer Einzelhandelsbetrieb hat im letzten Jahr als Kundenbindungsmaßnahme eine Kundenkarte eingeführt. Durch einen Hackerangriff werden die Daten gestohlen. Neben Namen, Adresse und Geburtsdatum der Kunden sind auch Daten über das Kaufverhalten betroffen. Diese Daten werden im Darknet zum Kauf angeboten. Der Vorfall wird bekannt und es entstehen hohe Forensikkosten sowie Benachrichtigungs- und Informationspflichten nach dem Bundesdatenschutzgesetz.

Gaststätten

Hacker verschaffen sich Zugang zu den Kassensystemen eines Restaurants. Über eine längere Zeit werden Kreditkartendaten von Kunden abgegriffen und später zum Verkauf angeboten. Die Kreditkartendaten werden missbräuchlich verwendet und die Kreditkartenbetreiber nehmen das Restaurant für den entstandenen Schaden in Anspruch.

Hotels

Ein Hotel wird zu Beginn der Saison Opfer eines Hackerangriffs, der auf das komplette System abzielt. Der Zugriff auf die Daten der letzten 3 Wochen (so lange wurde kein Back-up erstellt) wird durch eine sogenannte Ransomware komplett verhindert. Das bedeutet aber auch keinen Zugriff auf die Reservierungen! Da gleichzeitig das elektronische Schlüsselsystem attackiert wurde, können die Hotelgäste zusätzlich ihre Zimmer nicht betreten. Ein wahres Horrorszenario – und leider trotzdem Realität.

Richtig vorbereitet

Technische und organisatorische Maßnahmen, die den Betrieb Ihres Kunden sicherer machen, sind:

- Regelmäßiges Einspielen von Updates
- Erstellen von minutengenauen Back-ups
- Sensibilisierung der Mitarbeiter durch Schulungen/ Informationen zum Thema Informationssicherheit
- Nichtöffnen von unsicheren Dateianhängen
- Ausarbeitung von konkreten Krisenplänen sowie turnusmäßige Krisensimulation
- zudem natürlich Firewalls und Spamfilter
- und nicht zuletzt: die richtige Versicherung!

Richtig abgesichert mit der Basler Cyber-Police

Mit der Basler Cyber-Police erhalten kleine und mittelständische Betriebe umfangreichen Versicherungsschutz für Vermögensschäden, die durch Verletzungen der Informationssicherheit entstanden sind. Bedarfsgerechter Versicherungsschutz – alles in einer Police! Außerdem erhalten Ihre Kunden den passenden Support durch unsere Assistance-Hotline.

Hilfe in drei Stufen

1 Am Telefon

Spezialisierte IT-Experten helfen Ihren Kunden im Versicherungsfall direkt weiter.

2 Per Fernwartung

Der Experte der Assistance-Hotline verbindet sich mit dem System Ihrer Kunden und löst so die meisten Probleme.

3 Vor Ort

Ein Spezialist veranlasst bei Ihren Kunden vor Ort alle erforderlichen Schritte.

Unsere Hotline steht Ihren Kunden an sieben Tagen in der Woche rund um die Uhr zur Verfügung. Hier werden Informationen gesammelt und der Handlungsrahmen abgeklärt. Die weitere Analyse umfasst, sofern erforderlich, eine Befragung der Mitarbeiter sowie die Beweissicherung und die Analyse von Logfiles. Anschließend wird das Problem eingedämmt, beseitigt und die Systeme Ihres Kunden werden wiederhergestellt.

Ihre Kunden und deren Betriebe sind mit der Basler Cyber-Police bestens vor den finanziellen Risiken geschützt, die durch Cyber-Attacken und Datenrechtsverletzungen auf sie zukommen können. Insbesondere kleine und mittelständische Betriebe wählen mit der Basler Cyber-Police den idealen Versicherungsschutz.

Was ist eine Verletzung der Informationssicherheit?

Eine Informationssicherheitsverletzung ist eine Beeinträchtigung der

- → Verfügbarkeit,
- → Integrität oder
- → Vertraulichkeit

von elektronischen Daten oder von informationsverarbeitenden Systemen, die zur Ausübung der betrieblichen oder beruflichen Tätigkeit genutzt werden.

Wir bieten Absicherung bei

Cyber-Kosten

- Forensikkosten (Kosten der Ursachenermittlung)
  - Ermittlung der Ursache und Feststellung des versicherten Schadens durch externe Sachverständige
- Benachrichtigungskosten und Callcenter-Leistungen
- Krisenkommunikation und PR-Maßnahmen

Cyber-Drittschadendeckung (Haftpflicht)

- Befriedigung oder Abwehr von Schadenersatzansprüchen Dritter bei Verletzungen der Informationssicherheit inklusive folgender Erweiterungen
  - Rechtswidrige elektronische Kommunikation
  - E-Payment (Ansprüche der E-Payment-Serviceprovider)
  - Vertragliche Schadenersatzansprüche
  - Vertragliche Haftpflicht bei Datenverarbeitung durch Dritte
  - Rechtsverteidigungskosten auch bei Straf-, Ordnungswidrigkeits- oder sonstigen behördlichen Verfahren

Cyber-Eigenschadendeckung

- Betriebsunterbrechung/Unterbrechungsschäden
- Mehrkosten
- Wiederherstellung von Daten und Programmen (beinhaltet auch das Entfernen der Schadsoftware)
- Elektronischer Zahlungsverkehr
- Versand von Waren
- Cyber-Erpressung

Produkthighlights

- Schadenhotline 24/7
- Erste Krisenbewältigungs-Maßnahmen durch Spezialisten und schnelle Hilfe durch Fernzugriff
- Eine Versicherungssumme (250.000 EUR pauschal bis 5 Mio. EUR pauschal) für alle Deckungsbausteine – transparenter Versicherungsschutz; auf Wunsch können individuelle Sublimits gewählt werden
- Auf Wunsch kostengünstige Präventionsangebote

Ablauf bei Verdacht auf einen Cyber-Angriff

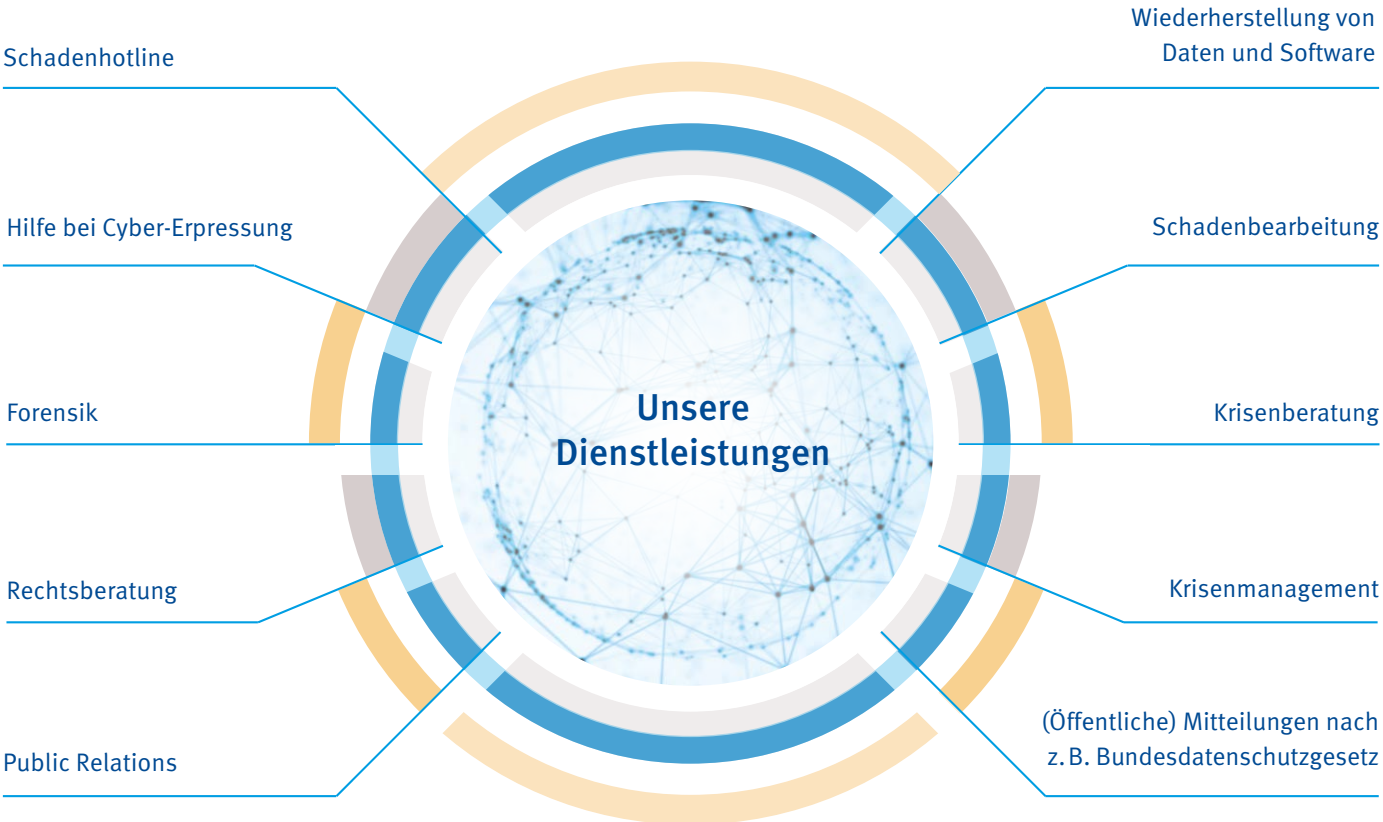
Ihr Kunde vermutet einen Cyber-Angriff? Über die extra für die Basler Cyber-Police eingerichtete Hotline erreicht er rund um die Uhr einen Spezialisten:

Unsere Hotline hilft umgehend weiter! Wir übernehmen die vollen Forensikkosten bis feststeht, ob ein Versicherungsfall vorliegt oder nicht.

Ein Spezialist der Hotline klärt, ob es sich um einen Cyber-Angriff handelt. Häufig erhält Ihr Kunde per Fernzugriff eine erste Hilfestellung und/oder Unterstützung bei der Organisation von weiteren Maßnahmen zur Krisenbewältigung.

Kann der Schaden per Fernzugriff nicht behoben bzw. untersucht werden? Auch kein Problem. In diesem Fall wird die forensische Dienstleistung direkt beim Kunden vor Ort erbracht. Auch dabei übernimmt die Basler die Kosten für die Schadensuche.

Nach Abschluss aller forensischen Arbeiten werden je nach Bedarf weitere Dienstleistungen angeboten. Unser gesamtes Angebot im Überblick:



Volle Kostenübernahme für die Prüfung

Ist das jetzt eine Cyber-Attacke? Eine schwierige Entscheidung für Ihren Kunden. Da hilft nur anrufen. Je schneller Ihr Kunde unsere Hotline kontaktiert, 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 Versicherer häufig eine Beteiligung von 50 % für die angefallenen Kosten. Nicht so bei den Basler Versicherungen! Wir garantieren die volle Kostenübernahme für die Prüfung bis zum vereinbarten Sublimit.

Wie kommt Ihr Kunde zum Versicherungsschutz?

Ganz leicht! Wir sehen diese Absicherung als so sinnvoll an, dass wir sie einfach und unkompliziert für alle kleinen und mittelständischen Unternehmen anbieten. Kleinere Betriebe füllen einzig einen kurzen Fragebogen aus.

Werden Tätigkeiten im Betrieb durchgeführt, die das Risiko erhöhen (siehe Infokasten, Seite 3), benötigen wir noch weitere Informationen. Gegebenenfalls erfolgt eine Risikoabschätzung vor Ort. Unser Ziel ist es, uns vorab schon ein möglichst komplettes Bild zu machen, um so den Abschluss für Sie und Ihre Kunden einfach und schlank zu halten.

Leistungsübersicht

Leistungspunkte	Unsere Leistungen	Gegen Zuschlag versicherbar
Versicherungssummen für Vermögensschäden[1] → 250.000 EUR pauschal → bis zu 5 Mio. EUR pauschal	✓	✓
Vermögensschäden durch Informationssicherheitsverletzung	✓	
Forensikkosten	✓	
Versicherte Kosten im Versicherungsfall → Benachrichtigungskosten und Callcenter-Leistungen → Krisenkommunikation und PR-Maßnahmen → Aufwendungen vor Eintritt des Versicherungsfalls	✓	
Cyber-Drittschadendeckung mit folgenden Deckungserweiterungen → Rechtswidrige elektronische Kommunikation → E-Payment → Vertragliche Schadenersatzansprüche → Vertragliche Haftpflicht bei Datenverarbeitung durch Dritte → Rechtsverteidigungskosten	✓	
Cyber-Eigenschadendeckung → Betriebsunterbrechung/Unterbrechungsschaden → Mehrkosten → Wiederherstellung von Daten und Programmen → Entfernung der Schadsoftware → Deckungserweiterungen – Elektronischer Zahlungsverkehr – Versand von Waren – Cyber-Erpressung	✓	
Nachhaftung	✓	
Rückwärtsdeckung	✓	
Repräsentantenklausel	✓	
Auslandsschäden weltweit mit Ausnahme Ansprüche Dritter → die vor einem Gericht in den USA oder Kanada geltend gemacht werden → infolge der Verletzung US-amerikanischen oder kanadischen Rechts → in Zusammenhang mit einer in den USA oder Kanada vorgenommenen Tätigkeit → aus der Beauftragung von externen Dienstleistern, welche außerhalb der EWR-Staaten oder nicht nach dem Recht der EWR-Staaten geltend gemacht werden	✓	
Vorrangige Versicherung	✓	

[1] 1-fach maximiert im Versicherungsjahr

Ihr kompetenter Ansprechpartner

Basler Versicherungen
Basler Str. 4, 61345 Bad Homburg

Telefon 0 61 72/125 4600
Montag bis Freitag von 8.00 bis 18.00 Uhr

BAS 3464 07.17 WMD