Ideal für kleine und mittlere Unternehmen

Basler Cyber-Police

Machen Sie Ihr Unternehmen cybersicher!

Cyber-Angriffe: weltweit größtes Risiko und Auslöser für zahlreiche Betriebsunterbrechungen

Corona, Homeoffice, Digitalisierung – seit Jahren steigt die Cyber-Kriminalität

In den letzten Jahren stieg die Anzahl der Hackerangriffe auf kleine wie große Unternehmen kontinuierlich an. Weltweit wird die Bedrohung durch Cyber-Attacken als größtes Risiko angesehen. In Deutschland liegt das Cyber-Risiko auf Platz 2 – nach der Betriebsunterbrechung, die jedoch auch durch zahlreiche Hackerangriffe verursacht wird. Unternehmen befürchten den Ausfall ihrer IT sowie Umsatzeinbußen. Häufig kommt bei einem Cyber-Angriff beides zusammen.

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

Denn selbst kleine und mittelständische Betriebe

- speichern wichtige Daten in elektronischer Form und
- akzeptieren Kartenzahlungen.

Durch die Möglichkeit, private elektronische Geräte wie Laptops, Smartphones oder Tablets im Netzwerk eines Unternehmens zu nutzen (Bring Your Own Device), entstanden und entstehen zudem weitere neue Einfallstore für Cyber-Kriminelle.

Cyber-Angriffe sind oft nicht zielgerichtet

Hacker schauen häufig zuerst, welche Systeme sie hacken können – meist durch Massenangriffe. Abhängig von Größe und Betriebsart entscheiden sie erst dann, wie sie dem Unternehmen schaden können.

Die größte Gefahr droht per E-Mail

Immer wieder öffnen Mitarbeiter harmlos aussehende E-Mails oder infizierte Anhänge und Links. Täglich werden mehrere Milliarden dieser Phishing-Mails verschickt. Daher sind E-Mails auch weiterhin das größte Risiko für eine erfolgreiche Cyber-Attacke.

Weitere Gefahren für Unternehmen

- Schwache Passwörter
- Verspätet ausgeführte System-Updates/Patches (dadurch Softwareschwachstellen)
- Nutzung privater Geräte im internen WLAN-Netzwerk
- Kartenzahlungssysteme für Kunden
- Nutzung der Firmenkreditkarte
- Nutzung öffentlicher WLAN-Netzwerke

Virenschutz, Firewall sowie starke Passwörter gehören bei vielen Betrieben schon zum Standard – häufig hapert es bei der Datensicherung sowie beim Patchmanagement. Wichtig ist es, alle Einfallstore für mögliche Cyber-Angriffe durch technische und organisatorische Maßnahmen zu minimieren.

Risiken erkennen, vermeiden, vermindern – so schützen sich Betriebe optimal

- Mitarbeiterschulung und Sensibilisierung
- Regelmäßige Software-Updates
- Regelmäßige Datensicherung
- **Restrisiko-Absicherung durch eine Cyber-Versicherung**
- Notfall-Strategie

Verschärfte Haftung durch EU-DSGVO

Die EU-DSGVO gilt für alle Unternehmen. Bei einer Datenschutzverletzung droht Betrieben eine Geldbuße 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.

Professionelle Unterstützung ist notwendig und hilfreich, z. B. bei:

- Behördlichen Meldefristen bei verlorenen Daten
- Betriebsstillstand
- 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**) sowie
- **Datenschutzverletzungen**.

Schadenfälle können damit auch ohne Infektion durch Schadsoftware entstehen, z. B. durch versehentliches Veröffentlichen von Kundendaten. 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 speichern wichtige Daten in elektronischer Form oder akzeptieren Kreditkartenzahlungen. Hier ist ein Einstieg über den **Basler Cyber-Schutzbrief** ideal.

Einstieg mit Cyber-Schutzbrief

Ein preisgünstiger, umfassender Schutz mit einer festen Versicherungssumme von 50.000 EUR – ohne weitere Sublimits. Volles Krisenmanagement – zudem Versicherungsschutz für Eigenschäden, wie z. B. eine Betriebsunterbrechung, oder Ansprüche Dritter.

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. Kundendaten, 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 Vier-augenprinzip unterstützen diese. Wichtig, denn man geht allein von circa 380.000 neuen Schadsoftwareprogrammen täglich aus.

Ein Unternehmen wird jedoch nie **hundertprozentige Absicherung** erreichen. Und kein IT-Dienstleister kann 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.

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

Auch wenn die eigene IT-Abteilung oder der beauftragte IT-Dienstleister die Firmennetzwerke hervorragend administriert und sich perfekt um die Technik kümmert, gibt es keinen absoluten Schutz. Im Schadenfall stehen Ihnen unsere Spezialisten zur Seite.

Hilfe in drei Stufen

3 Vor Ort
Ein Spezialist veranlasst vor Ort alle erforderlichen Schritte.

2 Per Fernwartung
Der Experte der Assistance-Hotline verbindet sich mit dem System und löst so die meisten Probleme.

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

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 Versicherer 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!

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

- **NEU**: Leistungs-Update-Garantie
- **NEU**: automatische Mitversicherung von Tochterfirmen bis zur nächsten Hauptfälligkeit
- **NEU**: höhere und einheitliche Sublimits in Höhe von 100.000 EUR
- Schnelle Abschlagszahlung im Schadenfall
- Einfache Antragstellung – nur wenige Risikofragen

Cyber-Kosten

- Soforthilfe und Forensikkosten (Kosten der Ursachenermittlung)
- Krisenkommunikation/PR-Maßnahmen
- Benachrichtigungskosten und Callcenter-Leistung
- Systemverbesserungen nach einer Informationssicherheitsverletzung

Cyber-Drittschadendeckung (Haftpflicht)

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

Cyber-Eigenschadendeckung

- Betriebsunterbrechung durch Ursachenermittlung im Schadenfall
- Betriebsunterbrechung durch Ausfall von Dienstleistern
- **NEU**: Betriebsunterbrechung durch technische Probleme (Fehlfunktionen) der informationsverarbeitenden Systeme
- Wiederherstellung von Daten (auch Entfernen der Schadsoftware)
- Cyber-Diebstahl/Cyber-Erpressung
- Cyber-Betrug
- **NEU**: Übernahme von Belohnungsgeldern (kein Lösegeld)
- Elektronischer Zahlungsverkehr
- Ersatz-Hardware
- Fehlerhafter Versand von Waren
- Telefonmehrkosten/erhöhte Nutzungsentgelte, z. B. für Strom, Gas oder Wasser (wenn informationsverarbeitende Systeme missbraucht werden, um Krypto-Währungen zu erstellen, sogenanntes Krypto-Mining)

Top-Platzierung im deutschen Markt

Für die **Basler Cyber-Police** gibt es eine hervorragende Bewertung durch das anerkannte Ratingunternehmen Franke und Bornberg – damit halten wir eine Spitzenposition im deutschen Markt!

BAS 3556 07.22 WMD

Basler Versicherungen
Ein Unternehmen der Baloise Group
Basler Str. 4, 61345 Bad Homburg