SÜDVERS
Zukunft sichern.

SÜDVERS CYBERVERSICHERUNG

Informationssicherheit und Cyberversicherung bieten existenziellen Bilanzschutz

IT-SICHERHEITSKONZEPTE SIND CHEFSACHE UND VORAUSSETZUNG FÜR EINE CYBERVERSICHERUNG

Digitalisierung ist die Basis für Innovation und Prozessoptimierung in Unternehmen. Dadurch steigt aber auch die Gefahr, Ziel von Cyberkriminalität zu werden. Um das Risiko zu minimieren, sind Investitionen erforderlich. So fließen mittlerweile rund 18 Prozent des IT-Budgets deutscher Unternehmen in die IT-Sicherheit.[1] Gut investiertes Geld: Denn Schäden, die durch Betriebsunterbrechung in Folge von Cyberangriffen entstehen – einschließlich der Kosten für die Wiederherstellung der IT – sind erheblich höher.

CYBERSICHERHEIT GANZHEITLICH DENKEN

Selbst das beste IT-Sicherheitskonzept kann leider das Angriffsrisiko keinesfalls auf null reduzieren. Unternehmen sollten daher in jedem Fall zusätzlich eine Versicherung gegen die Folgen von Cyberkriminalität abschließen. Unternehmensleiter müssen sich also auch eingehend mit Cyberversicherungen befassen. Der Vorteil: Eine passend gestaltete Police bietet wertvollen und nicht selten existenzsichernden Bilanzschutz.

CYBER UND D&O GEHEN HAND IN HAND

Denn Manager können auch für Cyberschäden haftbar gemacht werden. Somit ist es sinnvoller, Schäden aus Cyberangriffen direkt über eine Cyberversicherung zu regulieren, als auf die D&O-Versicherung zurückgreifen zu müssen, was zwingend eine persönliche Inanspruchnahme des betroffenen Unternehmensleiters zur Folge hätte.

Wichtig: Die grundlegende Verantwortlichkeit für die Schaffung eines Informationssicherheitsmanagements liegt allein beim Management. Der Aufbau eines solchen Systems gehört zu den originären Kontroll- und Lenkungsaufgaben. Dies ergibt sich insbesondere für kritische Infrastrukturen oder besonders systemrelevante Unternehmen aus den gesetzlichen Vorgaben.[2] Aber auch in Unternehmen, für die keine spezifische gesetzliche Regelung gilt, tragen die Unternehmensleiter die Verantwortung im Rahmen ihrer Sorgfaltspflicht.

GUT ZU WISSEN:
REIFEGRAD FÜR DIE VERSICHERUNG

Cyberversicherungen setzen heute das Vorhandensein eines Informationssicherheitsmanagements voraus. Hier haben sich in der Versicherungswirtschaft diverse Mindestanforderungen entwickelt. Dazu gehören Mitarbeiterschulungen, Mehrfaktorauthentifizierung oder EDR-Systeme, die Hardware vor verdächtigen Aktivitäten schützen. SÜDVERS bietet Kunden über ein Partnernetzwerk den Mehrwert, die betreffenden Mindestanforderungen mit pragmatischen Lösungsansätzen zu erfüllen.

[1]Bitkom (2025): Wirtschaftsschutz 2025, Lagebild der deutschen Wirtschaft, Seite 3
[2]IT-Sicherheitsgesetz, NIS 2-Umsetzunggesetz, DSGVO oder auch SGB V

CYBERSCHUTZ VON SÜDVERS: DAS WICHTIGSTE IN KÜRZE

Ganzheitlicher Service bei Eigen- und Drittschäden

1. Notfallmaßnahmen in den ersten 48 Stunden:
- Schadenmeldung wird 24/7/365 verarbeitet
- Steuerung über spezialisierte Dienstleister
- Krisengespräche mit Interessenvertretern und spezialisierten Datenrechtlern
- Einleiten der Untersuchungen
- Sofortmaßnahmen
- Basis für erste Deckungsprüfung
- Überleitung zum Schadenmanagement

UNTERNEHMENSLEITUNG IN DER VERANTWORTUNG

Die Unternehmensleitung trägt die Verantwortung für IT-Sicherheit. Dazu gehört auch ein reibungsloses Schadenhandling in der Folge einer Cyberattacke. Eine Cyberversicherung trägt in solchen Fällen wesentlich dazu bei, die Attacke schnellstmöglich mit versierten Experten zu beenden und den Folgeschaden zu minimieren.

2. Schadenmanagement schafft Ruhe und Gewissheit im Schadenfall:
- Unterstützung durch Spezialisten bei Schadenminderung und -beseitigung, um vor allem die Betriebsunterbrechung so kurz wie möglich zu halten
- Bewertung des Schadenumfangs sowie der Menge verlorener Daten und deren Wiederherstellung
- Juristische Beratung bei Datenschutz- oder Vertraulichkeitsverletzungen zum Umfang der Meldepflichten
- Sicherstellung einer angemessenen Krisenkommunikation
- Begleitung bei Sicherheitsverletzungen im Zahlungsverkehr

WAS IST VERSICHERT?

Eigenschäden

- Kosten der forensischen Untersuchung zur Feststellung des Schadenausmaßes & zur Wiederherstellung der Software und der gespeicherten Daten
- Betriebsunterbrechungsschaden infolge eines Cyberangriffs (auch auf Cloud Provider/externes Rechenzentrum) oder eines Bedien-/Programmierfehlers: entgangener Betriebsgewinn und fortlaufende Kosten mit zeitlichem Selbstbehalt von regelmäßig 6–12 Stunden und einer Haftzeit von 6 Monaten
- Cybererpressung: Kosten für Krisenberater und Lösegeld (teilweise begrenzt)
- Datenschutzvorfälle: Kosten zur Abwehr in behördlichen Verfahren sowie für anwaltliche Beratung & Benachrichtigung der betroffenen Kunden
- Schadenausgleich bei Cyberdiebstahl von Geldwerten mittels elektronischen Zugriffs (teilweise begrenzt)

Drittschäden

- Ausgleich begründeter & Abwehr unbegründeter Schadenersatzforderungen Dritter, u. a. wegen:
  - Verstößen gegen Datenschutzbestimmungen
  - einer vom versicherten Unternehmen zu verantwortenden IT-Sicherheitsverletzung bei Dritten (z. B. fahrlässige Weitergabe von Viren an Geschäftspartner)
- Schäden infolge von Sicherheitsverletzungen bei der Verarbeitung von Kreditkartendaten und eines Verstoßes gegen den PCI DSS (= Payment Card Industry Data Security Standard) inkl. verhängter Strafzahlungen (der Höhe nach begrenzt)

DIE VORTEILE AUF EINEN BLICK:

- Bewertung des Reifegrads der IT-Infrastruktur durch eigene zertifizierte Spezialisten
- Breites Netzwerk hilft Unternehmen, kurzfristig alle von den Versicherern geforderten IT-Sicherheitsmaßnahmen zu gewährleisten
- Identifikation der richtigen Versicherungssumme
- Analyse der Deckungsqualität von bestehendem Cyberversicherungsschutz
- Sonderkonzeptionen mit deutlich über dem Marktstandard liegender Deckungsqualität
- Zugang zu hochspezialisierten Dienstleistern
- Bilanzschutz durch Absicherung der immensen Kosten aus Cyberschäden
- Ausgestaltung der Cyberpolice mit höchster Deckungsqualität, auch als internationales Versicherungsprogramm möglich
- Verlässliche und erreichbare Regelungen zur geforderten IT-Sicherheit, um von vornherein Kontroversen mit dem Versicherer im Schadenfall auszuschließen
- Professionelle Begleitung von Schadenfällen und Regulierungsverhandlungen

DREI BEISPIELE AUS DER PRAXIS

Cybervorfälle können jedes Unternehmen treffen

Fallbeispiel 1: Ransomware-Angriff nach Phishing-Mail
Der Mitarbeiter eines Automobilzulieferers klickt in einer E-Mail unwissentlich einen manipulierten Link an, was zum Download von Malware auf den Firmenserver führt. Sämtliche Daten des Unternehmens sind daraufhin verschlüsselt. Auf dem Bildschirm des Mitarbeiters erscheint eine Nachricht mit Forderung einer Lösegeldzahlung in Bitcoins binnen 48 Stunden. Im Gegenzug würde man dem Unternehmen den Entschlüsselungscode zusenden.

Das Unternehmen kontaktiert umgehend die in der Cyberpolice ausgewiesene Hotline. Der zuständige Incident Response Manager beauftragt IT-Forensikermittler, um festzustellen, ob die Zahlung des Lösegeldes vermieden werden kann. Weitere Kostenpositionen zeigen sich später in den Honoraren des IT-Beraters für die Beurteilung der Backup-Fähigkeiten, der Rechtsberater und des Incident Response Managers; in den forensischen Ermittlungen, die zur Lokalisierung von Malware, Untersuchung von Auswirkungen, Reduzierung und der Berechnung des Schadenausmaßes durchgeführt werden – sowie nicht zuletzt in der Neuanlage verlorener oder korrupter Daten.

EXPERTENTIPP

„Unser Konzept ist sowohl für IT- als auch Versicherungslaien verständlich, da es schrittweise jeden Fachbegriff erläutert. Aufgrund unseres breiten Dienstleisternetzwerks können wir jedem Unternehmen helfen, die IT-Sicherheit pragmatisch auf ein versicherbares Niveau zu heben."

Dirk Wenning, Cyber Risk Consultant bei SÜDVERS

Fallbeispiel 2: Betriebsunterbrechung mit weitreichenden Folgen
Ein junges Pharmaunternehmen steht kurz vor dem Durchbruch und befindet sich in den letzten Zügen eines vielversprechenden und lange erwarteten Produktlaunches. Das Unternehmen hat sich mit seiner intensiven Arbeit an der Produktinnovation in den letzten beiden Jahren einen hervorragenden öffentlichen Ruf erarbeitet und wurde immer wieder in der Presse erwähnt. Doch dann bleiben die Maschinen plötzlich mitten in der finalen Produktionsphase stehen. Schnell stellt sich heraus, dass es einen gezielten Cyberangriff auf die Steuerungssoftware gegeben hat. Die Folgeschäden sind immens. Nicht nur der Umsatzausfall durch die verspätete Markteinführung machen dem Unternehmen zu schaffen, auch die Wiederherstellungskosten und der Imageschaden hinterlassen Spuren. Das Unternehmen ist nur unzureichend abgesichert und kann die immensen Kosten nicht allein tragen. Es muss Insolvenz anmelden.

Fallbeispiel 3: Massiver Datenschutzverstoß durch Mitarbeiterfehler

Die Personalabteilung eines Unternehmens aus dem Lebensmittelbereich versendet eine E-Mail an vier Bewerber. Versehentlich schickt sie dabei einen falschen Datenanhang mit. Dieser enthält die demografischen Personaldaten von 43.000 ehemaligen Mitarbeitenden (Namen, Anschriften und Personalausweisnummern). Die verantwortliche Mitarbeiterin wendet sich in ihrer Verzweiflung direkt an die Hotline der Cyberpolice. Genau die richtige Entscheidung, wie sich zeigt. Sofort wird dem Fall ein Incident Response Manager zugeteilt. Für den Umgang mit den datenschutzrechtlichen Auswirkungen wird ein Anwalt vermittelt. Die Versicherung deckt im Nachhinein die entstandenen Kosten für den Rechtsschutz im Zusammenhang mit aufsichtsbehördlichen Ermittlungen. Darüber hinaus übernimmt sie das Honorar des Incident Response Managers für die Benachrichtigung der betroffenen Personen sowie sämtliche in diesem Zusammenhang angefallenen Rechtsberatungskosten und Schadenersatzzahlungen.

BESONDERHEITEN DER CYBERVERSICHERUNG

- Mithilfe der ausgewählten Kooperationspartner kann grundsätzlich jedes Unternehmen zu einer versicherbaren IT-Infrastruktur geführt werden.
- Die Unternehmen werden im Rahmen der Vertragsanbahnung fachkundig und verlässlich bei der Angabe der Risikoinformationen begleitet, um Kontroversen zu sicherheitstechnischen Fragen in einem etwaigen Schadenfall vorzubeugen.
- Anders als herkömmliche Bedingungswerke ist das SÜDVERS-Vertragskonzept konsequent auf die Interessen der Versicherten zugeschnitten.
- Die Vertragsinhalte werden ständig weiterentwickelt und sind auch für Laien verständlich.
- Für die weit über den Markstandard gestaltete Bedingungsqualität wurden Angebote von zahlreichen renommierten Versicherern miteinander verglichen. Die Prämienhöhe ist für Kunden deshalb stets fair und transparent.
- Der Absicherungsbedarf und dessen Höhe wird immer individuell gemeinsam mit den Verantwortlichen im Unternehmen bestimmt.

„Darüber hinaus bietet eine Cyberversicherung zusätzliche Vorteile für das Unternehmen: So kann sie zum einen als Absicherungsargument für wirtschaftliche Leistungsfähigkeit gegenüber Kunden oder Banken dienen. Zum anderen beugt sie der Managerhaftung vor und kann damit die D&O-Versicherung entlasten."

Bernd Eriksen
Leiter Professional Lines bei SÜDVERS

Ihr Ansprechparter

BERND ERIKSEN

Leiter Professional Lines
bernd.eriksen@suedvers.de