Foto: © istock.com / anyaberkut

Cyber-Attacken: Versicherungsschutz wichtiger denn je

Ein Handy oder iPad, das verloren gegangen ist. Ein Laptop, das gestohlen wurde. Eine E-Mail mit manipuliertem Anhang, die das Ausspähen von Daten ermöglicht hat. Ein bekannt gewordenes Datenschutz-Versäumnis. Wir kennen sie alle und wissen um die stetig steigende Gefahr, Opfer einer Cyber-Attacke zu werden – und doch sitzen immer noch viele da wie das Kaninchen vor der Schlange. Es ist ein teures Unterfangen.

Am unangenehmsten nach einem Cyber-Angriff ist der Stillstand des Betriebs. Neben Einnahmeausfällen kann der daraus erwachsende Reputationsverlust enorm sein. Wenngleich von Kunden zunächst Verständnis bekundet und Bedauern zugesichert wird, ist faktisch das Vertrauen in das Unternehmen stark gefährdet, sodass die geschäftlichen Beziehungen in der Folge hinterfragt werden. Wen wundert es? Tröstlich: Die staatlichen Datenschutzbehörden sind hilfsbereit, sofern die Pflichterfüllung belegt werden kann. Und doch wechseln Kunden zu Mitbewerbern.

Es gibt keinen 100-Prozent-Schutz

Fakt ist: Es gibt keinen 100-Prozent-Schutz vor Cyber-Attacken! Denn sicher ist kein einziges Datenverarbeitungs- oder Datenspeicherprogramm. Zahlreiche, über die Medien bekannt gewordene Schadenfälle belegen dies. Und es ist kein Wunder, dass technische Sicherheit nicht allumfassend sein kann. Letztlich steigt die Zahl der Schadprogramm-Varianten kontinuierlich. 2021 zählte das Bundesamt für Sicherheit in der Informationstechnik rund 394.000 neue Varianten pro Tag. Im Jahr waren es rund 144 Millionen und damit eine Steigerung von 22 Prozent gegenüber 2020.

Cyber-Versicherer reagieren

Die Cyber-Versicherer reagieren. Überlegungen einiger Anbieter gehen sogar in die Richtung, sich aus dem Markt zurückzuziehen. Diejenigen Versicherer, die im Markt bleiben,

erhöhen die Preise – und zwar deutlich. Im Durchschnitt sind es mehr als 20 Prozent. Zudem steigen die Auflagen der Versicherer bezüglich der Versicherbarkeit. Bedeutet: Einkaufbarer Versicherungsschutz wird knapper und teurer, gleichzeitig werden Deckungsinhalte deutlich reduziert. Klug war, der sich früh geeigneten Versicherungsschutz eingekauft hat.

Deutlich verschärfte Angebotsknappheit

Nach Jahren der geringen Risikowahrnehmung, vor allem bei kleineren und mittelständischen Unternehmen, verzeichnet der Markt in den letzten zwei Jahren eine deutliche Zunahme der Bereitschaft bei Unternehmern, sich mit dem Thema Cyber-Versicherung zu beschäftigen. Immer mehr Unternehmen erkennen die Notwendigkeit. Gehandelt wird leider immer noch viel zu selten. So bleiben Tür und Tor geöffnet bei einer deutlichen Zunahme von Risikoereignissen – auch als Folge der Corona-Pandemie oder des Angriffskriegs auf die Ukraine. Die Zunahme von Risikoereignissen trifft auf eine sich deutlich verschärfende Angebotsknappheit.

Doch nicht überall, wo Cyber-Versicherung draufsteht, ist auch ein ausreichender Risikoschutz drin. Vor allem bei Standardprodukten gilt es, genau hinzuschauen. Der individuelle Bedarf und das tatsächliche Risikoprofil sind viel zu unterschiedlich, als dass Lösungen von der Stange wirklich bei allen passen könnten.

Ermittlung des Risikoprofils mit Experten

Bedarf und Risikoprofil sind relevante Grundlage für die richtige Wahl der Versicherungspolice und sollten im ersten Schritt mit einem Experten ermittelt werden. Dazu gehört unter anderem, dass die Widerstandsfähigkeit des Unternehmens überprüft wird. Das reicht vom Schutz der IT-Systeme gegen Zugriff von außen und innen, geht weiter über die bereits getroffenen organisatorischen Methoden wie Mitarbeiterschulungen. Es endet bei einem Systemcheck, der offene Stellen der IT-Infrastruktur feststellen kann. Strukturierte Fragenkataloge – zum Beispiel zu IT-Sicherheit und Datenschutz-Richtlinien – oder Telefoninterviews ergänzen die Analysephase.

Wirtschaftliches Restrisiko übertragen

Allein durch diese Herangehensweise werden für den Unternehmer Verbesserungsmöglichkeiten erkennbar. Manches ist unmittelbar und ohne großen Aufwand lösbar – zum Beispiel durch systemische Einstellungen und organisatorische Handlungen. Allein das kann das Risiko für alle Beteiligten spürbar verringern. Das wirtschaftliche Restrisiko kann dann durch den Einkauf einer Cyber-Police auf den Versicherer übertragen werden. Dabei helfen die vorgenannten Schritte auch dabei, ordentliche Deckungs- und Preisverhandlungen führen zu können. Der Versicherer weiß um das Risiko, das er in seine Bücher nehmen soll.

INFORMATION

Die Sorge der Unternehmer vor Cyber-Angriffen hat es im Allianz-Risk-Barometer 2022 auf den zweiten Platz geschafft. Jedes zweite deutsche Unternehmen wurde bereits Opfer eines Hackerangriffs. Die derzeitigen globalpolitischen Spannungen erhöhen das Risiko zusätzlich.

Ob Diebstahl, Erpressung, Systemausfall oder Betriebsstörung – seit Jahren entstehen der deutschen Wirtschaft enorme Schäden durch Cyber-Angriffe. Der jährliche Schaden wird laut bitkom.org auf über 220 Milliarden Euro geschätzt.

Kommt es zu einem erfolgreichen Angriff, betragen die Ausfallzeiten laut Experten im Schnitt bis zu 23 Tage. Manch ein Unternehmer zahlt die von Erpressern geforderte Summe – in dem Glauben, schnell wieder arbeiten zu können. Laut der im letzten Jahr veröffentlichten Sophos-Studie betrug die durchschnittliche Lösegeldzahlung weltweit 140.000 Euro und in Deutschland 115.000 Euro. Die Studie zeigt auch: Nur wenige Firmen bekommen alle Daten nach Zahlung zurück.

International haben sich die Durchschnittskosten für die Wiederherstellung nach einem Ransomware-Angriff in einem Jahr mehr als verdoppelt.

Kaum zu glauben ist, dass Unternehmen nach einem erfolgreichen Hacker-Angriff die „virtuelle Tür“ weiter offen stehen lassen. Der nächste Angriff ist damit vorprogrammiert.

Eine der Konsequenzen dieser und weiterer Entwicklungen: Der Kauf geeigneter Versicherungspolicen wird schwieriger, die Auflagen restriktiver und die Deckungen geringer.

Gleichzeitig kann der Unternehmer benötigte Deckungssummen besser einschätzen – weil er weiß, welches Risiko er selbst zu tragen im Stande ist.

Mögliche Inhalte einer Cyber-Versicherung

Mit der richtigen Cyber-Police sollte ein Unternehmer im Fall einer erfolgreichen Cyber-Attacke an 24 Stunden und 365 Tagen im Jahr mit einem Telefonanruf Zugriff auf alle erforderlichen Spezialisten haben. Nur so geht keine wertvolle Zeit nach dem virtuellen Angriff verloren. Von IT-Forensikern über Juristen bis hin zu Public-Relations-Agenturen sind alle Spezialisten verfügbar. Die sofortige Entwicklung einer Notfallstrategie, die Schadenbehebung und vor allem auch die persönliche Betreuung sind in diesen Stunden die größte Stütze. Schließlich gilt es, den eigenen Betrieb schnellstmöglich wieder arbeitsfähig zu schalten und gleichzeitig weiteren Schaden einzugrenzen – zum Beispiel durch nicht eingehaltene Behördenauflagen oder unzureichendes Beschwerdemanagement.

CHRISTIAN VON GÖLER
Mitglied der Geschäftsführung bei der BEST GRUPPE

christian.von-goeler@bestgruppe.de

CHRISTIAN VON GÖLER ist seit 2013 Partner und Geschäftsführer der BEST GRUPPE. Er berät und optimiert seit über 30 Jahren erfolgreich die Versicherungsportfolios für Unternehmer und Unternehmen. Seit 2014 beschäftigt er sich mit dem Markt der Cyberpolicen und zählt zu den „Experten der ersten Stunde".

Drei Fragen an Christian von Göler

Woran erkenne ich einen seriösen Versicherer?

Es kommt auf die Finanzstärke des Risikoträgers und die Dauer des Produktangebots an. Ferner sollte geprüft werden, ob der Versicherer Erfahrung in der Branche hat und seine Angebote darauf ausrichten kann. Eine Kernfrage ist, ob es sich um ein sogenanntes durchgeschriebenes Wording handelt. Hier sind keine Klauseln vorhanden, die den eigentlich benannten Versicherungsschutz wieder einschränken, sondern es ist klar benannt, was als versichert gilt und was nicht. Hinzu kommt die Frage nach Obliegenheiten, zum Beispiel dem erwarteten Schutz durch die IT-Sicherheitsarchitektur des Kunden. Je mehr hier verlangt wird, desto eher gibt es im Schadenfall das Risiko des Einwands und reduzierter Entschädigungen. Ebenfalls sind Einschränkungen im Versicherungsschutz bei „Dritt-Daten" und Daten des Unternehmens, die Dritte „betreuen", zu beachten. Häufig sind Daten sowohl im Unternehmen als auch an anderen Orten bis hin zu Kunden zu finden, die vom Unternehmen erstellt, verarbeitet oder zur Verfügung gestellt wurden. Hinzu kommt der „24/7" zur Verfügung stehende Spezialisten-Pool von IT-Forensik, PR-lern und Juristen. Sind dies tatsächlich Spezialisten?

Welche unterschiedlichen Versicherungsmodelle gibt es?

Es gibt den Eigenschutz der Eigen-Daten, überlassener Daten, verarbeiteter Daten und an Dritte übergebener Daten sowohl in elektronischer wie auch in analoger Form, Daten bei und von Cloud-Dienstleistern sowie den Einschluss der Hardware. Darüber hinaus gibt es die Begleichung bzw. Abwehr von Ansprüchen Dritter wegen Datenschutzvergehen, den Schutz und selbstverständlich die Begleichung von Betriebsunterbrechungsschäden. Dann wäre da noch die Begleitung und Abwehr bei behördlichen Datenschutzermittlungen.

Was kostet mich ein Versicherungsschutz?

Die Prämien berechnen sich in der Regel nach Umsatz und Deckungssumme sowie benötigter Module, zum Beispiel der Standardabdeckung, zusätzlicher Cloud-Nutzung oder Schutz bei Ausfall wegen technischer Probleme. Für einen Verwalter mit 650 Wohneinheiten heißt das: Zwischen 450 und 600 Euro kann ein gutes Deckungskonzept mit ausreichenden Versicherungssummen eingekauft werden. Ein Verwalter mit 1.300 Wohneinheiten sollte zwischen 600 und 800 Euro rechnen, wenn ein adäquater Schutz gewünscht wird.