Danny Penno, Kundenbetreuer bei Gossler, Gobert & Wolters

ZEIT, NEU ZU DENKEN

Der Begriff Cyberkriminalität ist nicht mehr neu, aber zugleich brandaktuell. Vor allem aber ist es ein branchenunabhängiges Risiko, das niemand unterschätzen sollte, auch kein Bühnenvermieter. Kran & Bühne informiert.

Im Jahr 2018 wurden rund zehn Personen oder Unternehmen Opfer eines Cyber-Angriffs, und zwar stündlich – allein in Deutschland. Und das sind lediglich die offiziell erfassten Vorfälle. Die Art der Attacken ist dabei vielfältig. Die Digitalisierung ist notwendiger denn je und absolut sinnvoll, doch sie macht uns in vielen Fällen auch angreifbarer. Verhindern lassen sich derartige Angriffe kaum. Ähnlich wie bei Einbrüchen kann man es den Tätern durch Schutzsysteme erschweren, doch hundertprozentigen Schutz gibt es nicht.

Gerade für Unternehmen ist es daher umso wichtiger, sich zu informieren und gegen mögliche Folgeschäden abzusichern. Noch immer ist vielen Verantwortlichen nicht klar, wie angreifbar nahezu jeder (scheinbar noch so kleine) Betrieb ist. Hacker sind erstaunlich einfallsreich; ihre „Ideen" reichen vom Phishing über Schadprogramme und Erpressung bis hin zu Datendiebstahl und Identitätsklau, um nur ein paar der häufigsten Methoden zu nennen.

WAS PASSIERT BEI SOLCH EINER ATTACKE?

- *Angreifer hacken die Datenbank und greifen auf sensible Daten zu, zum Beispiel aus der Buchhaltung*
- *Täter sperren digitalisierte Abläufe und legen so die Arbeitskette lahm bis hin zum völligen Stillstand*
- *technische Systeme, die Maschinen und Geräte steuern, werden gehackt*

Schon diese wenigen Beispiele machen deutlich, welch immenser Schaden durch Cyber-Angriffe entstehen kann. Die Gefahr selbst ist aber nicht sichtbar. Darum sind Ursachen und Auswirkungen noch immer für viele Entscheider in den Unternehmen schwer erkennbar. Die Gefahr wird oft nicht ernst genug genommen, und wenn es dann zum Angriff kommt, fehlt jeglicher Schutz.

Bild: © Cyber_Hacker_freise Bild - pixabay

Auch wenn ein Angriff an sich nur schwer zu vermeiden ist, können sich Unternehmen mit einer Cyberversicherung zumindest gegen den entstehenden Schaden absichern. Das ist gerade dann wichtig, wenn in der Folge auch Auftraggeber betroffen sind und einen finanziellen Schaden erleiden. Ohne Absicherung können Zahlungsverpflichtungen in einem solchen Fall ein Unternehmen in den Ruin treiben. Die Cyberversicherung dagegen deckt die Wiederherstellungskosten des Systems und die Auswirkungen der Betriebsunterbrechung ab – der Ausfall laufender Gewinne und die entstehenden Zusatzkosten werden somit nicht zur finanziellen Belastung.

Schlimmer kann es auch den Verantwortlichen in den Unternehmen ergehen. Unter Umständen können Sie für den Schaden persönlich haftbar gemacht werden, weil sie die Gefahr nicht gesehen und entsprechend wenig oder nichts zur Absicherung getan haben. Solche Fälle gab es bereits.

„Wer glaubt, dass das Risiko von der Unternehmensgröße abhängt, täuscht sich", sagt Danny Penno, Kundenbetreuer beim Versicherungsmakler Gossler, Gobert und Wolters. „Nicht immer geht es den Tätern um einen Gewinn, sondern oft eher darum, einen möglichst großen Schaden zu verursachen."

Nehmen wir als Beispiel den Diebstahl von Kundendaten. Ob der Täter durch einen Verkauf dieser Daten einen großen Gewinn macht, ist fraglich, ebenso, ob es ihm überhaupt gelingt. Aber: Das betroffene Unternehmen ist gemäß der Datenschutzgrundverordnung (Art. 33 und 34) verpflichtet, diesen Diebstahl innerhalb von 72 Stunden der Datenschutzbehörde zu melden und außerdem die betroffenen Personen zu informieren. Pro Datensatz kommen da schnell rund 30 bis 50 Euro zusammen. Bei einem Mittelwert von 40 Euro und einem – nicht sonderlich hohen – Datenbestand von tausend Kunden-Datensätzen summieren sich die Kosten allein hierfür auf 40.000 Euro. Deutlich höher fällt der Schaden bei größeren Datenmengen oder sensibleren Daten aus. Viele Firmen können derartige Kosten aus den laufenden Betriebseinnahmen nicht stemmen. Hinzu kommt der Imageschaden und Vertrauensverlust; beides nicht messbar, kann aber doch enorm sein. Zudem folgt auf den Diebstahl nicht selten der Versuch, dem geschädigten Unternehmen ein „Lösegeld" abzupressen.

„Gerade hier wird die fundamentale Bedeutung einer guten Cyberversicherung deutlich", so Fachmann Danny Penno. „Ohne Absicherung ist das betroffene Unternehmen in einer solchen Situation auf sich allein gestellt. Mit einer optimalen Cyberversicherung können Sie hingegen auf ausgewiesene Fachleute zurückgreifen. Zu den Cyber-Assistance-Leistungen zählen außerdem ein 24/7-Telefonservice sowie ein schneller Vor-Ort-Service."

Gerade bei kleinen Unternehmen mit Nischen-Expertise und gefragtem Knowhow gelingt solch ein Angriff erschreckend gut, indem vertrauliche Unterlagen wie Konstruktions- und Baupläne aus nicht ausreichend geschützten Netzwerken gestohlen werden. So erging es beispielsweise einem deutschen Unternehmer, der eines seiner Produkte, das er entwickelt hatte, auf einer Messe in China entdeckte. Erst, als der Mann bereits zurück war, ließ er das heimische Netzwerk überprüfen, und der Hackerangriff bzw. die Sicherheitslücken wurden entdeckt. In diesem speziellen Fall ist ein passender Versicherungsschutz schwierig, bei vielen anderen Ein- und Angriffen bietet eine passend abgestimmte Cyberversicherung aber eine gute Vorsorge.

Ein weiterer Vorteil: Wer sich mit dieser Gefahr intensiv auseinandersetzt – durch eigene interne Prüfungen oder besser noch durch externe Audits –, bekommt Sicherheitslücken in seinem Unternehmen aufgezeigt. Das heißt, die Vorsorge wird optimiert und im Schadenfall der finanzielle Verlust abgedeckt. Das gibt nicht nur dem Unternehmen selbst viel größere Sicherheit, sondern auch den Auftraggebern und -nehmern, deren Daten und Aufträge sonst mit betroffen wären.

K&B

Bild: Cyber_Sicherheit_Netzwerk-©deepagopi2011-fotolia.com