expertenReport

Cyberkriminalität: 445 Milliarden US-Dollar Schaden jährlich

Unternehmen müssen sich gegen eine neue Dimension von sich schnell entwickelnden Cyberrisiken wappnen. Fürchten Unternehmen heute vor allem Datendiebstähle, Datenschutzverletzungen und Reputationsschäden, so werden künftig Betriebsunterbrechungen in den Vordergrund rücken. Auch katastrophale Schadenszenarien sind denkbar.

„Vor nur 15 Jahren waren Cyberangriffe sporadisch und die wenigen Vorfälle meist das Werk von ‚Hacktivisten'. Mit der zunehmenden digitalen Vernetzung, der Globalisierung und der Kommerzialisierung von Internetkriminalität kam es zu einer Explosion der Cyberangriffe sowohl hinsichtlich ihrer Häufigkeit als auch hinsichtlich ihrer Schwere", sagt Chris Fischer Hirs, CEO von AGCS. „Eine Cyberversicherung kann eine robuste IT-Security keinesfalls ersetzen, aber sie schafft eine zweite Verteidigungslinie, um die negativen Folgen von Cyberangriffen abzufedern. Wir beobachten eine zunehmende Nachfrage solcher Deckungen. Und wir möchten unsere Kunden dabei unterstützen, Gefahren aus dem Netz zu verstehen und sich besser dagegen zu wappnen."

Strengere Regulierung steigert Nachfrage

Auch wenn derzeit erst weniger als zehn Prozent der Unternehmen Cyberpolicen kaufen, geht AGCS davon aus, dass das weltweite Prämienaufkommen von Cyberversicherungen von derzeit zwei Milliarden US-Dollar in den kommenden zehn Jahren auf über 20 Milliarden US-Dollar steigen wird. Das entspräche einer durchschnittlichen jährlichen Wachstumsrate von über 20 Prozent. Zwei Faktoren werden die Nachfrage nach Cyberversicherungen beschleunigen: Zum einen wächst das Risikobewusstsein in vielen Unternehmen. Zum anderen verschärft sich das regulatorische Umfeld.

„In den USA ist der Cyberversicherungsmarkt bereits gut entwickelt, was strengere Datenschutzgesetze entscheidend beeinflusst haben. Auch in vielen anderen Ländern weltweit werden gesetzliche Regelungen verschärft und Haftungsgrenzen angehoben – und das befördert die Nachfrage nach Cyberversicherungen", erklärt Nigel Pearson, der bei der AGCS weltweit für Cyberversicherung zuständig ist. „Es gibt einen allgemeinen Trend zu strengeren Datenschutzsystemen, deren Verletzung mit empfindlichen Geldstrafen geahndet wird." Hongkong, Singapur und Australien gehören zu den Ländern, die entsprechende neue Gesetze planen oder bereits umgesetzt haben. Selbst wenn sich die Europäische Union nicht auf die geplanten paneuropäischen Datenschutzvorschriften einigen könnte,

ist mit strengeren Richtlinien in den einzelnen Ländern zu rechnen.

Bisher fürchteten Unternehmen vor allem Datendiebstähle und Datenschutzverletzungen, wenn es um Internetkriminalität geht. Doch die jüngste Generation der Cyberrisiken hat eine neue Qualität erreicht: Unternehmen drohen künftig der Diebstahl geistigen Eigentums, virtuelle Erpressungen und die kostspieligen Folgen von Betriebsunterbrechungen (BU) in Folge von Cyberangriffen oder auch rein technischen IT-Ausfällen oder Prozessfehlern.

„Wenn Unternehmen an Cyberrisiken denken, dann denken sie nicht zuallererst daran, dass ihr Betrieb oder ihre Produktion still stehen könnten. Das ändert sich gerade“, beobachtet Georgi Pachov, Cyber-Experte im Global Property Underwriting-Team der AGCS. „Innerhalb der nächsten fünf bis zehn Jahre wird sich Betriebsunterbrechung zu einem zentralen Risiko für internet- und technologiebasierte Unternehmen entwickeln – und die entsprechende Deckung zu einem wichtigen Element von Cyberversicherungen.”.

BU-Deckungen für Cyber- und IT-Risiken sind breit angelegt und schließen sowohl die sogenannte „Business IT“ als auch industrielle IT-Systeme ein, wie sie Energieunternehmen oder Produktionsbetriebe zur Steuerung von Industrieanlagen oder Robotern nutzen.

Vernetzung schafft Risiko

Die virtuelle Vernetzung von Geräten und Maschinen sowie das wachsende Vertrauen in die Übertragung von Echtzeit-Daten auf persönlicher und geschäftlicher Ebene („Internet der Dinge“) schafft weitere Angriffspunkte für Internetkriminalität. Schätzungen zufolge könnten bis 2020 eine Billion Geräte untereinander vernetzt sein; 50 Milliarden Maschinen könnten täglich Daten austauschen. Industrielle Steuerungssysteme, wie sie in Kraftwerken oder Fabriken zum Einsatz kommen, stellen ein weiteres Einfallstor für Hacker dar. Denn viele sich heute noch in Betrieb befindende Systeme stammen aus einer Zeit, als IT-Sicherheit noch keinen hohen Stellenwert hatte. Würden industrielle IT-Systeme durch einen Hackerangriff lahmgelegt, könnte dies Sachschäden durch Feuer oder Explosion auslösen und auch zu Betriebsunterbrechungen führen.

Katastrophenereignis denkbar

Während es bereits einige schwere Fälle von Datendiebstahl gab, nimmt die Wahrscheinlichkeit eines durch Internetkriminalität verursachten Katastrophenschadens zu. Zu denkbaren Szenarien zählen ein erfolgreicher Angriff auf die Internetinfrastruktur, ein weitreichender Datenvorfall oder ein Netzwerkausfall bei einem Cloud-Service-Provider; ein schwerer Cyberangriff auf einen Energieanbieter oder ein Versorgungsunternehmen könnte nicht nur zu einem großflächigen Ausfall von Dienstleistungen führen, sondern auch hohe Sachschäden verursachen oder schlimmstenfalls sogar Menschenleben kosten.

Eigenständige Deckung

Aus Sicht der Allianz sollten Cyberversicherungen ihren Deckungsumfang erweitern und auch Betriebsunterbrechungsrisiken einschließen. Cyberausschlüsse in klassischen Schaden- und Haftpflichtpolicen werden sich weiter durchsetzen. Im Gegenzug werden sich Cyberversicherungen als eine eigenständige Produktkategorie etablieren. Außerdem werden sich die Versicherer – wie bei anderen neu aufkommenden Risiken und Versicherungslösungen auch – mit Herausforderungen hinsichtlich Tarifierung, nicht getesteten Policen-Wordings, Modellierung und Risikoakkumulation konfrontiert sehen.

Ganzheitliche Antwort auf Cyberrisiken

Die AGCS-Studie stellt Maßnahmen heraus, die Unternehmen ergreifen können, um Cyber-Risiken zu begegnen. Die Versicherung kann lediglich Teil der Lösung sein, notwendig ist vielmehr ein umfassender Risikomanagement-Ansatz, um Gefahren aus dem Netz abzuwehren. „Eine Cyberversicherung abgeschlossen zu haben, bedeutet nicht, bei der IT-Sicherheit sparen zu können. Vielmehr gehen die technologischen, betrieblichen und versicherungstechnischen Aspekte des Risikomanagements bei Cyberrisiken Hand in Hand”, erklärt Jens Krickhahn, AGCS-Experte für Cyberversicherungen in Deutschland.

Cyber-Risikomanagement im Unternehmen ist zu komplex, um einer einzigen Abteilung vorbehalten zu sein; deshalb empfiehlt die AGCS das Wissen von Stakeholdern aus verschiedenen Unternehmensbereichen in einen ‚Think-Tank’ zusammenzuführen, um das Risiko in den Griff zu bekommen. So können unterschiedliche Perspektiven und Szenarien untersucht und berücksichtigt werden, beispielsweise neue Risiken, die durch Fusionen und Übernahmen oder durch die Nutzung Cloudbasierter oder ausgelagerter Dienstleistungen entstehen. Eine unternehmensübergreifende Beteiligung hilft auch, die durch Cybergefahren besonders bedrohten

Vermögenswerte eines Unternehmens zu identifizieren und robuste Krisenreaktionspläne zu entwickeln und zu testen.

Bild: © Creativa / fotolia.com

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4941784/cyberkriminalitaet-445-milliarden-us-dollar-schaden-jaehrlich/