Die Gefahr aus dem Netz – Abstrakt und doch so real: Cyberschäden können jeden treffen

Bild: © Tomasz Zajda – Fotolia.com

Früher brauchte es Brecheisen, Taschenlampe und den Schutz der Dunkelheit, heute genügt ein ordentliches Quäntchen Computerverstand: Im digitalen Zeitalter hat es der Kriminelle nicht mehr nötig, bei Nacht und Nebel durch fremde Flure zu schleichen. Er erschleicht sich anderer Leute Eigentum über virtuelle Kanäle.

Von Ralf Michaelys, IAK Inter-Assekuranz Versicherungsmakler GmbH

Daten, vor allem sensible wie Bank- und Kundendaten, sind ein wertvolles und begehrtes Gut. Hacker und Konsorten haben im Cyberraum längst eine äußerst lukrative Einnahmequelle entdeckt.

Wir leben und arbeiten heute in einer weitgehend digitalisierten Welt. Kaum ein Tag vergeht, ohne dass irgendwo ein neues Datenleck gemeldet wird. Noch in Erinnerung dürften die Schlagzeilen um das Virus WannaCry sein, das Daten von mehr als 220.000 Computern verschlüsselte. Massenhaft Betriebsausfälle bei den betroffenen Unternehmen waren die – teilweise existenzbedrohende – Folge.

Cyberschäden gehören zu den Top-Risiken unserer Zeit. Keine Branche ist gefeit. Studien sagen voraus, dass sich die Angriffe auf IT-Systeme binnen zwei Jahren verdoppeln werden. Viele Betrüger setzen vornehmlich auf den Faktor Mensch. Der berüchtigte „Layer 8“, wie der „dümmste anzunehmende User“ vor dem Bildschirm in der Nerdsprache genannt wird, ist und bleibt die größte Schwachstelle im System.

Schadenszenario: „Revenge Wipe“

In einer nächtlichen Aktion hat sich ein Täter Zugang zum Netz verschafft und die IT-Systeme an zwei Standorten vollständig gelöscht sowie die Netzkomponenten funktionsunfähig gemacht.

Kosten für folgende Maßnahmen entstehen:

- Vor-Ort-Einsatz eines Notfallteams
- Parallele Streams für den Wiederanlauf der Umgebung und die Aufklärung des Vorfalls
- Zuarbeit zur Ermittlung der Kriminalpolizei (IT-Forensik)

Schadenszenario: Datenverschlüsselung mit Erpressung

Plötzlich geht nichts mehr. Eine Schadsoftware – wie z. B. das Virus WannaCry – hat sämtliche Daten auf den Firmenrechnern verschlüsselt. Die Mitarbeitenden haben keinen Zugriff mehr, die Arbeit liegt brach, der Betrieb steht still.

Die Täter verlangen ein Lösegeld für die (vermeintliche) Entsperrung der Daten, die laut Bundesamt für Sicherheit in der Informationstechnik (BSI) meist ausbleibt – auch wenn man zahlt.

Auch Datenhacks mit anschließender Erpressung erfreuen sich in der kriminellen Hackerszene großer Beliebtheit. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) rät betroffenen Unternehmen dringend davon ab, auf Lösegeldforderungen von Cyber-Erpressern einzugehen. Viele Unternehmen halten sich allerdings nicht an die Empfehlung in der Hoffnung, weiteren Schaden abwenden zu können. So hat sich mittlerweile ein regelrechter Industriezweig für Schadsoftware entwickelt, mit der sich Hacker Schätzungen zufolge rund eine Milliarde US-Dollar pro Jahr beschaffen. Ein Ende der Fahnenstange ist nicht ins Sicht.

Alle Unternehmen, die mit Daten von EU-Bürgern arbeiten, sind betroffen ...

Allerdings sind es nicht nur kriminelle Handlungen wie Datenklau oder Infiltration von

Schadenszenario: „Virusepedemie“

Das Antivirusprogramm des Unternehmens erkennt eine aktive Schadsoftware auf mehreren Rechnern. Bereinigungsversuche des IT-Dienstleisters scheitern; die Schadsoftware kommt immer wieder.

Der Einsatz eines Vor-Ort-Spezialisten ist notwendig.
Kosten für folgende Maßnahmen entstehen:

- Analyse des Verbreitungswegs
- Immunisierung der Systeme durch lokale Firewall-Regeln und manuelle Bereinigungsmaßnahmen
- Prüfung des Erfolgs, Automatisierung der Bereinigung für die übrigen Systeme


Bild: © Gajus – Fotolia.com

Systemen durch Schadsoftware, denen sich Unternehmen stellen müssen. Auch vergleichsweise banale Ereignisse wie System- oder Bedienfehler, aber auch Hardwareprobleme können zum Supergau im Netz und damit schlimmstenfalls zum Betriebsstillstand führen.

Mit Inkrafttreten des IT-Sicherheitsgesetzes für Deutschland (2015) sowie der Europäischen Datenschutz-Grundverordnung (EU-DSGVO, ab Mai 2018) müssen sich Unternehmen im Zusammenhang mit Cybersicherheit und Datenschutz mit verschärften Auflagen auseinandersetzen.

Versicherungen federn die finanziellen Folgen von Cybervorfällen ab.

Gemäß IT-Sicherheitsgesetz müssen deutsche Unternehmen bereits zum 3. Mai 2018 erste Prüfungsnachweise vorlegen, um zu dokumentieren, dass sie bestimmte Sicherheitsvorschriften nach dem Stand der Technik vorgenommen haben. Betroffen von der Prüfpflicht durch das BSI sind die so genannten KRITIS (Betreiber Kritischer Infrastrukturen). Dazu zählen Unternehmen aus den Sektoren Energie, Telekommunikation, Informationstechnik, Transport oder Verkehr wie auch Unternehmen aus den Bereichen Wasser, Ernährung sowie Finanz- und Versicherungswesen.

Während sich das IT-Sicherheitsgesetz mit Kritischen Infrastrukturen befasst, ist die Europäische Datenschutz-Grundverordnung darauf ausgerichtet, europaweit eine einheitliche und verbindliche Regelung für Datensicherheit zu schaffen. Alle Unternehmen, die mit Daten von EU-Bürgern arbeiten, sind betroffen, auch wenn sie ihren Sitz außerhalb der EU haben. Bis zum Inkrafttreten am 25. Mai 2018 müssen Firmen dafür Sorge tragen, dass europäische Privatpersonen mehr Kontrolle darüber enthalten, wie und zu welchem Zweck ihre Daten verarbeitet werden.

Der bereits existierende Bußgeldkatalog für „Datensünder“ wird sich mit Inkrafttreten der EU-DSGVO nochmals verschärfen. Bei Verstößen gegen IT-Sicherheitspflichten oder gegen die Informationspflicht den zuständigen Behörden bzw. den Betroffenen gegenüber belaufen sich die neuen Bußgelder für Unternehmen auf bis zu 20 Mio. Euro bzw. 4 % des Vorjahresumsatzes weltweit – je nachdem, welcher der beiden Beträge höher ist. Zudem können weitere Anordnungen der Aufsichtsbehörden erfolgen.

Versicherungen federn die finanziellen Folgen von Cybervorfällen ab. Wie genau der Versicherungsschutz für das einzelne Unternehmen ausgestaltet sein sollte, hängt von den betrieblichen Abläufen und den verwendeten Technologien ab. In jedem Fall ist es ratsam, eine Cyberversicherung abzuschließen.

Die Cyberversicherung ist ein Kombi-Produkt, das sich aus verschiedenen Bausteinen zusammensetzt. Die Bedingungen unterscheiden sich von Anbieter zu Anbieter. Alle Produkte stellen aber im Wesentlichen auf zwei Arten von Versicherungsfällen ab: den Cybervorfall und die Datenschutzrechtsverletzung.

Unter der Datenschutzrechtsverletzung versteht man dabei einen nicht ordnungsgemäßen Umgang mit Daten, die unter die Datenschutzbestimmungen fallen – dies sind meist personenbezogene Daten.

Bei einem Cybervorfall handelt es sich hingegen um einen unberechtigten Zugriff auf das IT-System, sei es durch einen zielgerichteten Hack oder durch das unwissentliche Öffnen eines mit Schadsoftware kontaminierten Mailanhangs.

Zu den wichtigsten Leistungsbestandteilen der Cyberversicherung gehören Schadenersatzleistungen für Drittschäden bei Datenschutzverletzungen, entgangener Gewinn bei Betriebsunterbrechung, Kosten für die Wiederherstellung von Daten, Erstattung von Forensik-Kosten, Assistenzleistungen im Krisenfall – meist via Hotline des Versicherers – und optional die Erarbeitung neuer beziehungsweise Überprüfung bestehender Krisenpläne – über externe Dienstleister zukaufbarer Zusatzbaustein bei einigen Versicherern.

Weil die Bedingungen und Leistungsangebote am Markt sehr unterschiedlich sind, empfiehlt sich vor Abschluss einer Cyberversicherung eine bedarfsgerechte Beratung einschließlich individueller Risikoanalyse. Nur so lässt sich sicherstellen, dass das Versicherungsprodukt am Ende auch wirklich perfekt zum eigenen Unternehmensrisiko passt.

Weil die Bedingungen und Leistungsangebote am Markt sehr unterschiedlich sind, empfiehlt sich vor Abschluss einer Cyberversicherung eine bedarfsgerechte Beratung ...

In der Cyberdeckung versicherbar sind sowohl die Folgen eines konkreten Hackerangriffs als auch die Folgen einer Fehlbedienung. Im Einzelnen vom Versicherungsschutz erfasst sind der Ertragsausfall, Ausfall der Telekommunikation/Website,Bedienfehler, DoS-Attacke, Hackerangriff, Manipulation durch eigene Mitarbeiter/innen, Ausfall von IT-Dienstleitungen, Sachverständigenkosten, Datenwiederherstellung, Rufschädigung/Krisenmanagement, Datenschutzverletzung, In-ternetbetrug, Erpressung und die Cyberhaftpflicht.

Der richtige Versicherungsschutz ist natürlich nur die halbe Miete: Ein funktionierendes IT-Sicherheitskonzept muss auch auf schadenverhindernde und -mindernde Maßnahmen setzen. In diesem Zusammenhang sind Regelwerke zu erstellen, Brandschutzfragen zu klären, Krisenpläne zu erarbeiten und mehr.

KM