CYBER-ANGRIFF – DIE GEFAHR AUS DEM NICHTS

Es geht oft schneller als gedacht und dauert dann länger als befürchtet – mit der Digitalisierung einher geht die zunehmende digitale Kriminalisierung, vom Datendiebstahl über Erpressung bis zu konkreten, digital gesteuerten Sabotageakten. Damit wird dann oft nicht nur der betroffene Verband oder das betroffene Unternehmen geschädigt, sondern in Folge auch Kunden oder Partner. Zur Sorge über entwendete oder unzugänglich gemachte Daten kommt dann oft noch der nicht unerhebliche Aufwand für den richtigen Umgang mit der Krise, für die Fortführung des Betriebes und für die Wiederherstellung, Reparatur und Sicherung der Systeme. Gegen den man sich am besten mit einer Cyber-Versicherung absichert.

Gunhild Peiniger

DAS RISIKO DES DIGITALEN ZEITALTERS

Nahezu kein Verband ist heutzutage nicht digitalisiert. Hierdurch können unkalkulierbare Risiken entstehen, die nicht nur die eigene Infrastruktur betreffen, sondern sich auch gegenüber Vertragspartnern negativ auswirken können, was wiederum Haftpflichtansprüche nach sich ziehen kann. Hierbei kann theoretisch jedes Netzwerk Opfer eines Hackerangriffs werden.

Sicherlich werden die meisten PCs mit sogenannten Firewalls oder Antiviren-Programmen ausgestattet sein, sodass den Angreifern das Eindringen erschwert wird. Leider sind diese Angreifer jedoch in der Entwicklung von Schadsoftware immer einen Schritt voraus, sodass eine absolute Sicherheit der eigenen Netzwerke nicht gegeben ist.

Dies führt dazu, dass die Versicherungswirtschaft neben den herkömmlichen Versicherungssparten Konzepte entwickelt hat, die sozusagen als Schirm über den bestehenden Versicherungsverträgen einen weitergehenden Schutz gegen Cyber-Attacken darstellen und somit das bestehende Versicherungsprogramm sinnvoll ergänzen sollen.

Das Problem allerdings ist, dass Cyber-Angriffe oft keine Identität des Schadenstifters hinterlassen, meist Voraussetzung für das Wirksamwerden beispielsweise einer Vertrauensschaden-Versicherung. Vielmehr nutzen Eindringlinge diese Angriffe, um Verbände zu erpressen, Schäden anzurichten und Informationen zu erhalten.

Eine der bisher gefährlichsten Cyber-Angriffe aus dem Jahre 2010 war der Computerwurm „Stuxnet“. Der Wurm hatte zum Ziel, Steuerungssysteme von Industrieanlagen zu sabotieren. Durch Sicherheitslücken im System Windows waren Betriebssysteme auf der ganzen Welt betroffen.

Einer Cyber-Versicherung geht weit über die Absicherung des sogenannten Datenschutzrisikos hinaus.

Hierbei findet die Versicherung viele Schnittstellen zu anderen Versicherungen, wie beispielsweise der Betriebshaftpflichtversicherung, die allerdings immer ein Verschulden des Versicherungsnehmers an der Entstehung des Schadens voraussetzt, oder aber einer Vermögensschaden-Haftpflichtversicherung, die jeweils einen bekannten Schadenstifter voraussetzt.

Die Cyber-Versicherung soll sowohl Dritt- als auch Eigenschäden absichern.

Drittschaden:

Ein Drittschaden entsteht, wenn der Versicherungsnehmer einen Kunden oder sonstigen Dritten, zum Beispiel aufgrund einer Datenrechtsverletzung, geschädigt hat.

Eigenschäden:

Bei einem Hackerangriff oder der Spionage von persönlichen Daten kann auch dem Versicherungsnehmer selbst ein Schaden entstehen. Versicherungsrechtlich spricht man dann von einem Eigenschaden.

Daneben übernimmt der Cyber-Versicherer zumeist weitere Kosten, die durch einen Angriff entstehen können. Hierzu zählen unter anderem:

- professionelles Krisenmanagement und Öffentlichkeitsarbeit;
- die Beauftragung hierfür spezialisierter Rechtsanwälte;
- die notwendigen Mehrkosten zur Fortführung des Betriebes;
- die Wiederherstellung und Reparatur der IT-Systeme.

Cyber-Angriffe richten sich gezielt gegen einzelne Personen und Verbände, um wertvolle Daten zu stehlen. Hier hat sich bereits ein regelrechter Geschäftszweig entwickelt, der auch dazu führen kann, dass Verbände erpresst werden und nur gegen Zahlung eines Lösegelds der Schaden an dem eigenen Computersystem wieder abgewendet werden kann. Hierbei spielen auch die eigenen Mitarbeiter, sei es durch Vorsatz oder unachtsamen Umgang mit dem Öffnen von E-Mails oder infizierten Dateien, eine Rolle.

Ein weiteres Problem eines Cyber-Angriffs liegt darin begründet, dass dieser zunächst möglicherweise nicht bemerkt wird und Daten so manipuliert werden, dass die Inhalte erst zu einem späteren Zeitpunkt gestohlen werden. Hierbei wird das Netzwerk des Verbands weiter ausspioniert, damit Sicherheitslücken ausfindig gemacht werden.

Nach Analysen von Bitcom ist in den letzten Jahren fast jedes dritte Unternehmen in Deutschland Opfer eines Cyber-Angriffs gewesen. Oftmals gerät dieses zunächst gar nicht an die Öffentlichkeit – anders im Fall des IT-Systems eines Krankenhauses in Nordrhein-Westfalen. Dort musste aufgrund eines Hacker-Angriffs das gesamte IT-System heruntergefahren werden, was dazu führte, dass Operationen nicht durchgeführt werden konnten. Die Staatsanwaltschaft geht davon aus, dass es sich hier um eine versuchte Erpressung gehandelt hat, da eine bestimmte Schadsoftware in das Krankenhaussystem eingespielt wurde. Diese führt zur Verschlüsselung der Daten. Danach wird Lösegeld verlangt, woraufhin die Daten wieder entschlüsselt werden.

Immer häufiger gibt es auch sogenannte Verschlüsselungstrojaner auf Smartphones und PCs. Hier schleusen Angreifer eine sogenannte Ransomware auf das Gerät, die entweder den kompletten Zugriff sperrt oder wichtige Daten verschlüsselt. Zugang erhalten die Betroffenen erst nach Zahlung eines Lösegelds.

Als einer der bekanntesten Schädlinge gilt der seit Februar 2016 sein Unwesen treibende Krypto-Trojaner „Locky“, der Zehntausende PCs infizierte. Aus diesem Grunde werden vereinzelt in der Versicherungswirtschaft auch für private Internetnutzer Cyberpolicen angeboten. Diese sogenannte Schadsoftware kann darüber hinaus über verdächtige E-Mail-Anhänge an Dritte – Geschäftspartner oder eigene Mitarbeiter – verbreitet werden. In der Regel kann Ransomware oder Schadsoftware jeden treffen, da sowohl Endnutzer als auch Mitarbeiter des Verbandes angegriffen werden. Sollte ein Mitarbeiter attackiert worden sein, so ist eine sofortige Trennung vom Verbandsnetzwerk, zur Verhinderung weiterer Verbreitung, erforderlich.

SCHADENBEISPIELE

Androhung von Veröffentlichung sensibler Kundendaten

Hacker haben sich Zugriff zum Netzwerk eines Verbandes und somit zu sensiblen Mitgliederinformationen verschafft. Der Verband erhielt einen Anruf von dem Eindringling, der 10.000 Euro forderte und drohte, andernfalls die Daten online zu stellen. Der Verband wendete für die forensischen Ermittlungen, für erpressungsbezogene Verhandlungen, eine Lösegeldzahlung, Kommunikationsmaßnahmen, Kontenmonitoring, Wiederherstellungsmaßnahmen und das Honorar für unabhängige Anwälte 100.000 Euro auf. Darüber hinaus verursachte der Netzwerk-Zusammenbruch einen finanziellen Schaden von 150.000 Euro.

Schaden: 250.000 Euro

Viele Verbände gehen davon aus, dass sie bereits umfassenden Versicherungsschutz auch in Bezug auf mögliche Angriffe auf das eigene Netzwerk abgeschlossen haben. Leider berücksichtigen jedoch traditionelle Versicherungssparten zumeist nicht die große Abhängigkeit von Computer- und Netzwerktechnologie auf der einen und die potenziell existenzbedrohenden Auswirkungen eines Angriffs auf der anderen Seite. Dieses liegt u. a. darin begründet, dass die herkömmlichen Versicherungssparten erst seit einigen Jahren die rasante Entwicklung in Bezug auf die kriminelle Energie im Netz und damit verbunden die Sorgfaltspflichten der Geschäftsleitung teilweise in die Policen integriert haben.

Diebstahl eines Desktop-PC

Beim Einbruch in das Büro eines Verbandes wird der PC mit Datensätzen von 50 bis 100 Spendern entwendet. Dem Verband erwachsen daraus erhebliche Aufwendungen für Rechtsberatung und Informationsverpflichtungen ebenso wie für Forensik und Kreditüberwachungsleistungen.

Schaden: 105.000 €

WELCHES SIND DIE GÄNGIGEN VORBEHALTE GEGEN DEN ABSCHLUSS EINER CYBER-VERSICHERUNG?

Unsere IT-Abteilung ist gegen Störfälle bestens gewappnet!

Dies ist eine perfekte Voraussetzung, um überhaupt in den Genuss einer Cyber-Police zu kommen. Allerdings ist es für sehr gut aufgestellte IT-Abteilungen in einer Krise oftmals schwierig, einen optimalen Krisenplan zu verfolgen, der es ermöglicht, gerichtsverwertbare Feststellungen der Krisenursache bis hin zur Kommunikationsarbeit zu leisten.

Unser Verband ist viel zu klein. Hacker interessieren sich nur für Großkonzerne!

Auch kleine, mittelständische Verbände werden Opfer von zielgerichteten Hacker-Angriffen, die erhebliche Schäden verursachen können, z. B. an der Hard- und Software, für die der Verband unter Umständen keine Rückstellungen gebildet hat.

IN DER REGEL KANN RANSOMWARE ODER SCHADSOFTWARE JEDEN TREFFEN, DA SOWOHL ENDNUTZER ALS AUCH MITARBEITER DES VERBANDES ANGEGRIFFEN WERDEN. SOLLTE EIN MITARBEITER ATTACKIERT WORDEN SEIN, SO IST EINE SOFORTIGE TRENNUNG VOM VERBANDSNETZWERK, ZUR VERHINDERUNG WEITERER VERBREITUNG, ERFORDERLICH.

Eine Bedrohung durch eigene Mitarbeiter können wir ausschließen!

Leider können Statistiken dieses nicht bestätigen. Diese attestieren, dass bis zu 80 Prozent der Datenschutzfälle durch eigene Mitarbeiter verursacht werden. Dies kann durch die vorsätzliche Weitergabe von Daten an Dritte passieren oder aber schlicht durch Unachtsamkeit.

Cyber ist kein Thema für die Geschäftsleitung, sondern für die IT-Abteilung!

Eine Cyber-Krise z. B. durch Betriebsunterbrechung, Schadenersatz, Lösegeldforderungen und Reputationsschäden kann einen Verband wirtschaftlich massiv schaden. Deshalb sollte das Cyber-Thema auch immer Chefsache sein.

Unsere Daten wurden an externe Dienstleister ausgelagert!

Aber die Verantwortung für die Sicherheit der Daten kann nicht ausgelagert werden. Ein Verband, der personenbezogene Daten erhoben hat, haftet auch dann als verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes (BDSG), wenn ein Datenverlust auf dem Handeln von Mitarbeitern oder einem externen Anbieter, wie z. B. einem Rechenzentrum oder Cloud-Provider, beruht.

WELCHE VORTEILE BIETET DIE CYBER-VERSICHERUNG?

Zunächst schützt die Cyber-Versicherung den Verband nicht nur vor den finanziellen Auswirkungen eines Cyber-Angriffs, sondern sie trägt auch dazu bei, die Fortsetzung des Alltagsgeschäfts zu gewährleisten. Vor Abschluss der Versicherung sollte ein Gespräch mit einem professionellen Berater stattfinden, um zunächst zu überprüfen, welche Versicherungen bereits durch den Verband abgeschlossen wurden. Im Anschluss daran wird ein entsprechender Fragebogen ausgefüllt, der zusammen mit dem Versicherer und gegebenenfalls ei-

ner IT-Sicherheitsfirma durchgesprochen wird. Später kann ein maßgeschneidertes Konzept für den Verband erarbeitet werden. Das Risikomanagement sollte hierbei immer im Zusammenwirken mit den IT-Experten der Verbandsleitung sowie dem Versicherer erfolgen.

WELCHE VERSICHERUNGSSUMMEN SOLLTEN ABGESCHLOSSEN WERDEN?

Die Versicherungssummen reichen von 100.000 € bis 10 Mio. € im Bereich von kleinen und mittelständischen Verbänden Leider gibt es bisher bei dieser doch recht jungen Sparte wenig Schadenerfahrung. Der Gesetzgeber wird zukünftig durch nähere Konkretisierung von Meldepflichten und Schadensersatzsummen, die hier zu zahlen wären, sicherlich zu einer weiteren Konkretisierung gelangen. Die Prämien bewegen sich aktuell zwischen 500 € und 50.000 €, je nach Größe des Verbandes.

TROTZ DER HOHEN ANZAHL DER ANGRIFFE FÜHLEN SICH VERBÄNDE IMMER NOCH RECHT SICHER

Als Fazit lässt sich jedoch feststellen, dass Cyber-Gefahren und Datenschutzverletzungen nach jüngsten Erhebungen das größte Risikopotenzial für die Bevölkerung in Deutschland darstellen. Hierbei zeigen repräsentative Studien, dass es durchschnittlich mehr als 220 Tage dauert, bis ein Angriff überhaupt erkannt wird. Versicherungslösungen nehmen in diesem Zusammenhang immer mehr Raum ein. Aus diesem Grunde sollte sich die Geschäftsführung eines Verbandes intensiv mit dem Thema beschäftigen. ■

AUTOR

GUNHILD PEINIGER

Ist Geschäftsführerin der PP Business Protection GmbH, Spezialmakler für beratende Berufe und Management.

PP Business Protection GmbH,
Frau Gunhild Peiniger – Geschäftsführerin
Telefon: (040) 413 45 32-0
→ www.pp-business.de

www.verbaende.com/fachartikel
(geschützter Bereich für Abonnenten und DGVM-Mitglieder)