Cybererpressung – die neue Art der Kriminalität

Kelkheim, 8. Februar 2016

In den vergangenen Jahren ist ein ganz neuer, aber rasant wachsender Kriminalitätszweig entstanden: die Cybererpressung. Allein in den vergangenen 6 Monaten gab es einige zum Teil sehr aufsehenerregender Fälle. Wie zum Beispiel der Hacker-Angriff auf das Seitensprung-Portal Asley Madison im Juli 2015. Die Hacker hatten sich Zugang zu den Nuterinformationen des Portals verschafft und versuchten durch ihren Angriff die Betreiber zu zwingen, das Portal zu schließen. Als diese nicht darauf eingingen, veröffentlichten die Erpresser Kundenprofile. Oder ein anderer Fall: Im Oktober wurde der britische Telekommunikationsanbieter TalkTalk Opfer einer Cybererpressung. Anscheinend wurden Kundennamen, Adressen und Kreditkarteninfos angezapft. Durch ein Lösegeld, das die Erpresser forderten, sollte TalkTalk die Weitergabe der Daten verhindern.

Flickr : Chris Potter

Doch es sind nicht immer nur Daten, die geklaut werden, wie ein anderes Beispiel aus Großbritannien, zeigt. Zurzeit stehen dort große Finanzinstitute im Visier einer Erpresser-Gruppe, die sich DD4BC nennt. Diese fordern die betroffenen Institute auf, Lösegeld in Bitcoins zu zahlen. Falls die Unternehmen sich weigern, droht die Gruppe mit einem anhaltendenen „Denial of Service Atack"-Angriff (DDoS), so dass die Kunden nicht mehr auf die Website ihrer Bank zugreifen könnten. Damit wäre jeglicher Online-Kundenverkehr lahmgelegt. Mehr als 140 Attacken werden dieser Gruppe bereits zugerechnet.

Ähnliches hatte auch der US-Konzern Apple in Australien erlebt. Im Jahr 2014 sperrte ein Verschlüsselungstrojaner den Apple-Usern den Zugang zu ihren Geräten.

Cybererpressung legt die Schwachstellen in der Cybersicherheit offen

Für Unternehmen kann der Schaden bei einer Cyber-Attage schnell in die Millionenhöhe gehen. Nicht nur, wenn sie auf die Lösegeldfoderung eingehen. Abgesehen von dem Imageschaden, der entsteht, wenn Lücken in der

Cybersicherheit offenkundig werden, können zudem eventuelle Schadenersatzforderungen von Kunden und Nutzern ein Unternehmen die Existenz kosten. Hinzu kommen im Fall von Zugangs-Blockaden noch die entgangenen Umsätze. Und wenn dem Unternehmen dann noch nachgewiesen wird, dass es seine Daten nur unzureichend geschützt hat, kann zudem noch eine saftige Geldstrafe hinzu kommen, weil Datenschutzbestimmungen verletzt wurden. Alles in allem nicht billig.

Versicherung gegen Cyber-Erpressung: Cyber-Extortion

Die Gefahr Opfer einer Cyber-Erpressung zu werden ist real und wächst mit der zunehmenden Abhängigkeit von Unternehmen von Internet und Online-Plattformen. Inzwischen gibt es jedoch spezielle Versicherungslösungen, die Deckungsschutz bieten. Erst unlängst wurde der Schutz von Sachwerten auch auf elektronische Daten ausgeweitet, der Begriff „Eigentum“ umschließt daher bei vielen Versicherungen inwischen auch elektronische Daten.

Es gibt auch Versicherungen, die schon auf das wachsende Risiko einer Cybererpressung reagiert haben und im Rahmen ihrer Cyberhaftpflichtversicherung eine so genannte „Cyber-Extortion“ anbieten. Hier gibt es eine Überlappung mit der üblichen Cyberpolice, bei der unter anderem Eigenschäden sowie Schäden durch Betriebsunterbrechungen, Ermittlungskosten und Drittschäden infolge von Datenschutzverletzungen abdeckt sind.

So können die Kosten, die ein Unternehmen hat, wenn es einen Cyber-Angriff abwehren muss, erstattet werden. Allerdings sind noch nicht immer die oben genannten „Denial of Acess“-Attacken eingeschlossen. Diese können jedoch häufig durch eine Deckungserweiterung hinzugefügt werden. Es werden immer mehr Versicherungen, die diese Form des Cyberangriffes in ihre Cybererweiterung des Deckungsschutzes mit aufnehmen. Hier sind dann teilweise auch Betriebsunterbrechungen aufgrund der Attacke sowie Ermittlungskosten mit eingeschlossen.

Wichtig bei jeder Art von Cybererpressung ist, so schnell wie möglich zu klären, wo die Schwachstelle lag. Dazu gibt es spezielle Datenschutz- und IT-Forensik-Spezialisten. Auch deren Kosten können in der Deckung miteingeschlossen werden. Die Cyber-Extortion-Deckung ergänzt somit die normale Cyber-Haftpflichtversicherung und kann im Falle eines Falles die Existenz des Unternehmens sichern.

Über die gb.online gmbh

Die gb.online gmbh hat sich auf die berufliche Absicherung von Freelancern spezialisiert und bietet mit www.easy-insure.eu das umfangreichste Online-Versicherungsportal für freie und beratende Berufe in Deutschland. Seit 2011 können Selbstständige und Unternehmen bis 1 Million Euro Umsatz pro Jahr hier ihre beruflichen Risiken versichern.

Steigt der Umsatz, und wird eine individuelle Lösung benötigt, so steht mit dem Schwesterunternehmen groot bramel versicherungsmakler gmbh ein verlässlicher Partner zur Seite, der seit über 25 Jahren Gewerbetreibende und industriellen Unternehmen in Versicherungsfragen vertritt. Die groot bramel versicherungsmakler gmbh ist in 18 Ländern vertreten und begleitet sie, wohin au

ch immer sich ihr Geschäftsfeld entwickelt.

Kontaktdaten

gb.online gmbh

Frankfurter Straße 93

65779 Kelkheim

Ansprechpartner: Lutz-Hendrik Groot Bramel, Geschäftsführer

Folgen Sie uns auch auf