Cash.ONLINE
FINANZNACHRICHTEN, 24. MÄRZ 2016

11. Februar 2016, 09:38

Berater

Cyber-Attacken: Datenschutzverletzungen in den Griff bekommen

Cyber-Attacken auf Unternehmen machen immer wieder große Schlagzeilen. Für Hacker kann es äußerst profitabel sein, sensibler Daten habhaft zu werden. Am häufigsten werden dabei Finanzdienstleister ins Visier genommen, denn hier sind die Chancen auf finanziellen Gewinn am höchsten.

Gastbeitrag von Brookes Taney, Data Breach Solutions, Epiq Systems

Finanzdienstleister können als Folge erfolgreicher Cyber-Attacken mit Klagen, behördlichen Bußgeldern und infolgedessen möglicher Rufschädigung oder dem Verlust von Kunden konfrontiert werden.

Insbesondere bargeldlose Zahlungssysteme stehen im Fokus der Angreifer: im Jahr 2014 zielten 30 Prozent der Fälle von Cyberkriminalität in Deutschland auf solche Anwendungen ab.

In der Regel wollen die Hacker Informationen wie Namen, Adressen, Bank- und Kreditkarteninformationen erbeuten, die sie dann für Betrugszwecke nutzen.

Strenge Auflagen für Datenschutz

Bis vor Kurzem setzten sich Finanzdienstleister mit dieser Art von Datenschutzverletzungen erst dann auseinander, nachdem die Cyber-Attacke bereits stattgefunden hatte und bemerkt wurde.

Zu diesem Zeitpunkt waren das Ausmaß der Schädigung und die Art der gestohlenen Informationen meist nicht bekannt. Unternehmen suchten dann umgehend die Unterstützung von Versicherungsunternehmen, Anwaltskanzleien, Beratern und externen Ermittlern, um alle offenen Fragen in Bezug auf den Datenklau zu klären und zu sehen, wie dem Datenverlust ein Riegel vorgeschoben werden könne.

Mehr zum Thema Cyberpolicen

Studie: Steigende Schäden durch Cyber-Kriminalität im Mittelstand

Cyber-Versicherungen: Zwischen Chance und Risiko

Axa erweitert Cyber-Schutz auf kleine und mittlere Betriebe

Die Anforderungen für Datenschutz von Seiten der Aufsichtsbehörden werden jedoch insbesondere für den Finanzdienstleistungssektor immer strenger und Unternehmen ergreifen deshalb verstärkt Maßnahmen, um das Risikobewusstsein ihrer Mitarbeiter zu stärken und Risikomanagement-Strategien zu verbessern.

Rufschädigung droht

In vielen Fällen arbeitet die Unternehmensführung gemeinsam mit Rechtsberatern und IT-Experten umfassende Data-Breach-Response-Pläne aus, die in verschiedenen Szenarien Anwendung finden können.

Das Ziel dabei ist, eine Strategie für den Umgang mit Datenschutzverletzungen durch Cyber-Attacken vom Zeitpunkt der Aufdeckung bis hin zu möglichen Rechtsverfahren im Griff zu haben – denn Finanzdienstleister können als Folge erfolgreicher Cyber-Attacken mit Klagen, behördlichen Bußgeldern und infolgedessen möglicher Rufschädigung oder dem Verlust von Kunden konfrontiert werden.

Seite zwei: Zeit und Kosten sparen