/ Mehr als 100 Mio. Bankkundendaten in den USA gehackt – welche Konsequenzen sollten Unternehmen aus solchen Cyberangriffen ziehen?

13.08.2019

Datenschutz | Digital Business | Prozessführung, Schiedsverfahren & ADR

Am 30.07.2019 ist bekannt geworden, dass eine Hackerin bei der US-Bank Capital One Millionen von sensiblen Kundendaten gestohlen hat. Bei diesem Cyberangriff sind gemäß Pressemitteilung der Bank überwiegend personenbezogene Daten entwendet worden, die in Kreditkartenanträgen enthalten waren. Die Bank teilte auch mit, dass sie Mehrkosten von etwa USD 100 Mio. bis USD 150 Mio. wegen des Cyberangriffs allein in 2019 erwarte. Diese Kosten entstünden maßgeblich für Kundenbenachrichtigungen, technische Aufrüstung und Rechtsberatung. Trotz offenbar weitreichender Transparenz und zugesagter Aufklärung sank der Aktienkurs binnen 24 Stunden um etwa 8%. Bereits jetzt – innerhalb weniger Tage nach Veröffentlichung des Angriffs – sind zahlreiche US-Kanzleien damit befasst, Verbraucher für Sammelklagen gegen die Bank zusammenzubringen. Zwar ist dieser Fall in seinen Auswirkungen besonders drastisch, zeigt aber doch exemplarisch, dass Unternehmen die Risiken von Cyberangriffen sehr ernst nehmen müssen.

Was sollten Unternehmen aus diesem Cyberangriff ableiten?

Nicht öffentlich bekannt ist bisher, ob die Angreiferin eine Sicherheitslücke im System der Bank oder in der Firewall eines Cloud-Servers für ihre Cyberattacke genutzt hat. Die Konsequenzen des Angriffs zeigen jedenfalls, dass selbst Unternehmen aus dem Finanzsektor, für die in Bezug auf die IT-Sicherheit besondere regulatorische Anforderungen gelten, oftmals nicht ausreichend vor Cyberangriffen geschützt sind. Umso mehr dürften Unternehmen Cyberrisiken ausgesetzt sein, für die keine speziellen Anforderungen an die IT-Sicherheit gestellt werden. Zudem wäre es verfehlt zu glauben, dass Unternehmen, die nur wenig personenbezogene Daten verarbeiten, nicht gefährdet wären. Vielmehr sind nach jüngsten Erkenntnissen zur Hackergruppe „Winnti“ Unternehmen, die über besonderes Knowhow verfügen, dem Risiko ausgesetzt, Opfer von Industriespionage zu werden.

Notfallplan vorbereiten

Wie der jüngste Angriff auf Capital One zeigt, kann ein Cyberangriff zu einer ernsthaften Unternehmenskrise führen, auf die ebenso rasch wie durchdacht reagiert werden muss. Unternehmen, die sogenannte Betreiber Kritischer Infrastrukturen sind, wozu auch Finanzinstitute oder Versicherungen gehören, sind gemäß § 8 a Abs. 1 Satz 1 BSIG ohnehin dazu verpflichtet, *„angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind“*. Zudem sind Betreiber Kritischer Infrastrukturen gemäß § 8 b Abs. 3 BSIG zur Benennung einer Kontaktstelle für das Bundesamt für Sicherheit in der Informationstechnik sowie gemäß § 8 b Abs. 4 BSIG zur unverzüglichen Meldung bestimmter Störungen verpflichtet. Auch wenn diese Vorgaben nicht unmittelbar für Unternehmen außerhalb des Anwendungsbereichs des BSIG gelten, sondern nur als Leitlinie herangezogen werden können, wird damit deutlich, dass IT-Sicherheit Kernaufgabe der Unternehmensleitung ist. Insofern sollte in jedem Unternehmen ein Notfallplan für Unternehmenskrisen bereit liegen, der eine eindeutige Zuordnung von Aufgaben und Verantwortlichkeiten einschließlich der festgelegten Kommunikationswege kaskadenmäßig von der Geschäftsleitung bis zum Mitarbeiterstab vorsieht, sobald der Cyberangriff entdeckt wurde. Tatsächlich besteht aber bisher bei weniger als der Hälfte der Unternehmen ein Notfallmanagement (43% laut BSI-Cyber-Sicherheits-Umfrage 2018).

Hier besteht Handlungsbedarf:

- Im Notfallplan sind wichtige externe Ansprechpartner zu bestimmen, allem voran ein technischer Dienstleister, der die Infrastruktur des Unternehmens analysiert und Beweise sichert, die später für Gerichtsverfahren verwendbar sind. Die Einbindung von solchen Spezialisten ist erforderlich, damit die Beweissicherungsmaßnahmen keine Veränderung am Systembetrieb oder den gespeicherten Daten herbeiführen, durch die ein Angreifer feststellen kann, dass er entdeckt wurde.

- Je nach Schwere bzw. Umfang der Cyperattacke ist eine gezielte und ganzheitliche Krisen-PR erforderlich, damit Investoren, Kunden und Vertragspartner sachlich richtig und transparent unterrichtet werden. In den ersten Stunden nach Entdeckung des Angriffs entscheidet sich, welche „Story“ mit der Krise verbunden wird.

- Besonderen Pflichten zur Information unterliegen börsennotierte Unternehmen oder solche, denen personenbezogene Daten abhandengekommen sind.

- Auch sollten Ansprechpartner für die Ermittlungsbehörden feststehen. Idealerweise haben diese Kontakt zu den jeweiligen Schwerpunktstaatsanwaltschaften zur Verfolgung von Cyberkriminalität, die in den meisten Bundesländern inzwischen eingerichtet sind (z.B. die Zentral- und Ansprechstellen für Cybercrime des Landes Nordrhein-Westfalen (ZAC) der die Zentralstelle Cybercrime Bayern (ZCB)).

Ob dieses Krisenmanagement intern oder durch externe Berater gesteuert wird, sollte unter Einbeziehung von Rechtsabteilung, Compliance und IT vorab geklärt werden. Wichtig ist dabei aber, dass die Geschäftsleitung in die Vorbereitung und die laufende Überwachung der Notfallplanung verantwortlich einbezogen ist. Andernfalls besteht das Risiko der persönlichen Haftung wegen unzureichender Schutzmaßnahmen für das Unternehmens vor Cyberangriffen oder Verstößen gegen Datenschutz.

Weitere Einzelheiten zum Thema Cyber Risks finden Sie demnächst auch auf unserer Webseite.

Haben Sie Fragen? Kontaktieren Sie gerne: Dr. Sarah Schmidt-Versteyl oder Dr. Martin Schorn
Practice Groups: Datenschutz , Digital Business , Prozessführung, Schiedsverfahren & ADR

Contact Person

Dr. Sarah Schmidt-Versteyl, LL.M.
Mitglied der Practice Group Prozessführung, Schiedsverfahren & ADR
Mitglied der Practice Group Gesellschaftsrecht/Mergers & Acquisitions
Rechtsanwältin

T +49 211 49986279

Dr. Martin Schorn
Mitglied der Practice Group Prozessführung, Schiedsverfahren & ADR
Mitglied der Practice Group Compliance & Interne Ermittlungen
Rechtsanwalt

T +49 211 49986 243