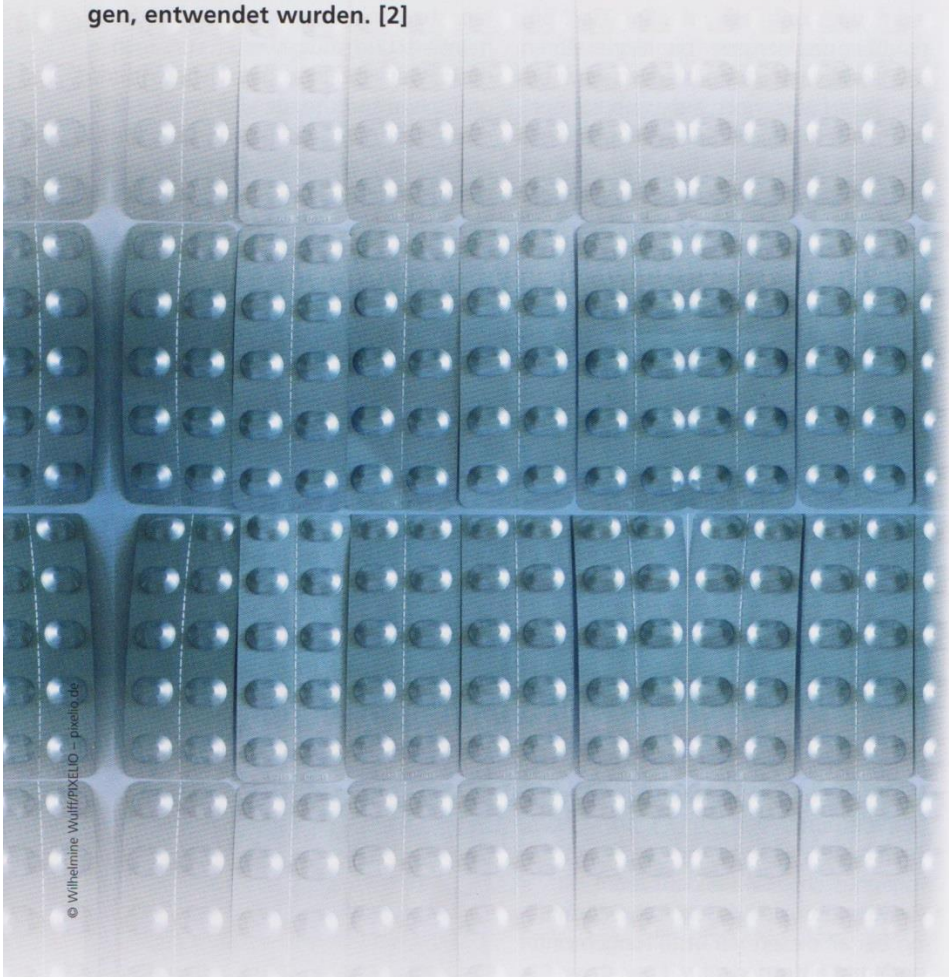
Brookes Taney

Cyber-Attacken in den Griff bekommen

In den vergangenen fünf bis zehn Jahren ist die Anzahl der Cyber-Attacken auf Unternehmen angestiegen. Dabei versuchen die Hacker sensibler Daten habhaft zu werden, um Profit daraus zu ziehen. In der Regel handelt es sich um Informationen wie Namen, Adressen, Bank- und Kreditkarteninformationen, die dann für Betrugszwecke genutzt werden. So verschafften sich Cyber-Kriminelle im April 2015 Zugang zu User Accounts auf der Website der Deutschen Lufthansa und stahlen Vielflieger-Prämienmeilen mit denen sie Gutscheine erwarben und Prämien einlösten. [1] Auch Vodafone Deutschland wurde im Jahr 2013 das Opfer eines Hackerangriffs, bei dem die Daten von knapp zwei Millionen aktuellen und ehemaligen Kunden, einschließlich Namen, Adressen, Geburtsdaten und Bankverbindungen, entwendet wurden. [2]



© Wilhelmine Wulff/fotolia – pixelio.de

Der Datenraub, dem Sony Pictures im November 2014 zum Opfer fiel, folgte jedoch einem anderen Muster. [3] Bei dieser Cyber-Attacke standen atypische Informationen im Fokus, darunter Gehälter von Mitarbeitern, persönlicher E-Mail-Verkehr zwischen Führungskräften und Prominenten, kreative Inhalte und andere Details zu Filmen, die vor der Veröffentlichung standen. Mit Hilfe dieser Daten verschafften sich die Hacker keinen wirtschaftlichen Vorteil sondern nutzten sie lediglich zur Rufschädigung des Konzerns. Die Regeln des Spiels scheinen sich zu ändern. Es sieht so aus, als bestünde unter Hackern ein Wettbewerb, bei dem der Status durch den Umfang und die Auswirkungen einer erfolgreichen Attacke bemessen wird. Kurz nachdem der Angriff auf Vodafone publik wurde, tat sich beispielsweise eine Hackergruppe mit der Behauptung hervor, für den Datenraub verantwortlich gewesen zu sein. Das Ziel der Attacke sei lediglich gewesen, dem Mobilfunkanbieter eine Lehre zu erteilen und zu zeigen, wie leicht es sei, sich Zugang zu sensiblen Daten zu verschaffen. Es stellte sich jedoch später heraus, dass es sich bei dieser Gruppe lediglich um Trittbrettfahrer handelte. [4] Dennoch können Fälle wie dieser das Image einer Marke nachhaltig beschädigen. Unternehmen sollten daher eine genaue Bewertung ihrer Präventionsmaßnahmen sowie ihrer Reaktionsfähigkeit im Falle eines Datenklaus durchführen.

→ Risiko von möglichem Datenverlust minimieren

Bis vor Kurzem begannen Firmen sich erst dann mit der Datenschutzverletzung auseinander zu setzen, nachdem der Angriff bereits stattgefunden hatte und bemerkt wurde. Das sorgte nicht selten für Panik, denn zu diesem Zeitpunkt waren das Ausmaß der Schädigung und die Art der gestohlenen Informationen meist nicht bekannt. Unternehmen suchten in der Regel 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.

Da sich das Vorgehen der Hacker jedoch verändert und von unterschiedlichen Motiven getrieben ist, arbeiten Rechtsberater und IT-Experten mittlerweile mit der Unternehmensführung umfassendere sogenannte Data-Breach-Response-Pläne aus, die in verschiedenen Szenarien Anwendung finden können. Mittlerweile arbeiten sie beispielsweise mit Experten zusammen, die einen Datenraub vom Zeitpunkt der Aufdeckung bis hin zu möglichen Gerichtsverfahren begleiten können und zusätzliche Dienstleistungen im Bereich proaktiver Information Governance anbieten. So können das Risiko einer erfolgreichen Cyber-Attacke sowie der mögliche Schaden reduziert werden. Manche Firmen kooperieren sogar mit sogenannten „Ethical Hackers", die versuchen, sich Zugang zu kritischen Informationen auf den Unternehmensservern zu ver-

schaffen und so mögliche Schwachstellen im System aufdecken. [5]

Ausreichender Schutz per Gesetz

Wenn es zum Datenklau gekommen ist, kann eine eDiscovery wertvolle Hilfestellung bei der effizienten Abwicklung rechtlicher Verfahren leisten. Das erleichtert Forensik und Beweissammlung sowie die Prüfung, Verwertung und Zusammenstellung von Dokumenten. Ob es tatsächlich zu einem Gerichtsverfahren kommt, wird häufig durch den Umfang des Schadens und die Art der gestohlenen Daten bestimmt. Oft spielt es auch eine Rolle, welche Unternehmen und Kunden betroffen sind. Durch eine eDiscovery können Firmen dann die Sammlung, Bearbeitung und Bewertung elektronischer Dokumente und Mitteilungen abwickeln. Mit Hilfe passender Technologien können beispielsweise automatisierte Stichwortsuchen durchgeführt werden, um die Relevanz bestimmter Datensätze für den Fall zu bestimmen. Dadurch können Unternehmen sowohl Zeit als auch Kosten sparen.

Mit dem neuen IT-Sicherheitsgesetz, das am 25. Juli 2015 in Kraft getreten ist, verschärfen sich die gesetzlichen Anforderungen an Betreiber sogenannter „kritischer Infrastrukturen", wie beispielsweise Energie- und Wasserversorger oder IT- und Telekommunikationsunternehmen. Derzeit sind lediglich Betreiber von Webservern und Telekommunikationsunternehmen gefordert, die Sicherheit ihrer IT-Systeme gezielt zu verbessern. Ab 13. Juni 2017 gilt dies auch für andere Betreiber solcher Infrastrukturen, wie beispielsweise Versorgungsunternehmen oder Finanzdienstleister. Cyber-Attacken müssen von diesen Firmen an das Bundesamt für Sicherheit in der Informationstechnologie (BSI) gemeldet werden – auch dann, wenn diese abgewehrt werden konnten. Auch zur Vorbeugung solcher Attacken müssen die Betreiber wirkungsvolle Maßnahmen einführen. Bei Verstoß können Bußgelder bis zu 100.000 Euro verhängt werden. [6] Außerdem müssen die Organisationen alle vier Jahre eine Prüfung ihrer Sicherheitsmaßnahmen durchführen lassen. [7] Ein Fall wie der Angriff auf Vodafone hätte demzufolge jetzt ernsthaftere Konsequenzen als noch vor zwei Jahren als das Unternehmen aufgrund des laxen Umgangs mit Datensicherheit lediglich kritisiert wurde. [8]

Schutzmechanismen entwickeln

Ist es zu einer Datenschutzverletzung durch eine Cyber-Attacke gekommen, muss das betroffene Unternehmen nachweisen können, dass es bereits zuvor Maßnahmen getroffen hatte, um das Risiko eines Datenklaus so weit als möglich einzuschränken. Die Aufsichtsbehörden verlangen in der Regel Beweise dafür, dass klare und umfassend kommunizierte Unternehmensrichtlinien zum Datenschutz und damit zusammenhängende Prüfungsverfahren vorhanden waren. Außerdem muss gezeigt werden können, dass es im Voraus keine klaren Anzeichen für eine potentielle Bedrohung gab und das Unternehmen den Schaden umgehend gemeldet hat.

Eine umfassende Dokumentenprüfung ist ein wesentlicher Bestandteil dieses Prozesses und schließt eine detaillierte Analyse relevanter Kommunikation ein. Das kann insbesondere dann eine große Herausforderung darstellen, wenn große Mengen an Dokumenten auf ihre Relevanz hin beurteilt und dann von Experten innerhalb kurzer Zeit gesichtet werden müssen. Auch in so einem Fall schafft eine eDiscovery Erleichterung für alle beteiligten Parteien.

Cyber-Attacken stellen ein immer häufiger eintretendes Bedrohungsszenario für Unternehmen aller Wirtschaftsbereiche dar. Sie können nicht nur finanziellen Schaden anrichten, sondern auch die Reputation nachhaltig beeinträchtigen. Zudem sind Hacker-Angriffe immer schwerer einzuordnen und daher weniger vorhersehbar. Deshalb sollten Firmen sicherstellen, dass sie im Fall einer Datenschutzverletzung durch Cyber-Attacken über adäquate Data-Breach-Response-Mechanismen verfügen und eine proaktive Strategie für das elektronische Informationsmanagement entwickeln.

Literatur

[1] SC Magazine, 'Lufthansa flyer miles stolen in customer database breach', 13.04.2015, http://www.scmagazineuk.com/lufthansa-flyer-miles-stolen-in-customer-database-breach/article/408659/

[2] Security Week, 'Insider Steals Data of 2 Million Vodafone Germany Customers', 12.09.2013, http://www.securityweek.com/attacker-steals-data-2-million-vodafone-germany-customers

[3] BBC News, 'Sony Pictures computer system hacked in online attack', 25.11.2014, http://www.bbc.co.uk/news/technology-30189029

[4] Zeit Online, Anonyme reklamieren Vodafone-Hack für sich, 13.09.2013, http://www.zeit.de/digital/datenschutz/2013-09/vodafone-hack-bekenner

[5] IT Finanzmagazin, Mit strikt definiertem Auftrag: Ethical Hacking soll die Datensicherheit der Finanzbranche verbessern, 18.09.2015, http://www.it-finanzmagazin.de/mit-strikt-definiertem-auftrag-ethical-hacking-soll-die-datensicherheit-der-finanzbranche-verbessern-19621/

[6] Haufe Recht, Pflichten aus IT-Sicherheitsgesetz und EU-Richtlinie zur Cybersicherheit, 02.02.2016, https://www.haufe.de/recht/weitere-rechtsgebiete/strafrecht-oeffentl-recht/it-sicherheitsgesetz-und-eu-richtlinie-zur-cybersicherheit_204_337534.html

[7] Datenschutzbeauftragter Info, IT-Sicherheitsgesetz: Zweck, Anforderungen und Sanktionen, 28.07.2015, https://www.datenschutz-beauftragter-info.de/sicherheitsgesetz-zweck-anforderungen-und-sanktionen/

[8] Heise Security, IT-Sicherheitsgesetz tritt in Kraft, 24.07.2015, http://www.heise.de/security/meldung/IT-Sicherheitsgesetz-tritt-in-Kraft-2762518.html.

Der Autor

Brookes Taney stellt als Vice President of Data Breach Solutions bei Epiq Systems zusammen mit seinem Team Dienstleistungen rund um Datenschutzverletzungen zur Verfügung. Zuvor war er als Senior Director of Corporate Services und Senior Director of Bankruptcy Creditor Solutions, ebenfalls bei Epiq Systems, tätig. Brookes Taney absolvierte einen BSc Marketing und Speech Communication an der St. Cloud State University (Minnesota, U.S.).

✉ *taney@wissensmanagement.net*