SmartRiskSolutions
Risk & Crisis Management Consultancy

Fallstudie Krisen- und Reputationsmanagement nach einem Cyberangriff

Von Pascal Michel und Michael Pülmanns, SmartRiskSolutions GmbH

Dieser Bericht erschien in unserem halbjährlichen Newsletter im Mai 2016.

Im vergangenen Jahr war zweitgrößte amerikanische Krankenversicherer Anthem Opfer eines kriminellen Hackerangriffes geworden, der rund 80 Millionen Kunden und eigene Mitarbeiter betraf. Sozialversicherungsnummern, Wohnanschriften, Geburtsdaten, Arbeitgeber- und Emailadressen sowie Gehälter von Mitarbeitern wurden gestohlen. Es ist sehr wahrscheinlich, dass diese Daten im Dark Web - einer Art Schwarzmarkt im Internet - zu Zwecken des Identitätsdiebstahls verkauft werden.

Auch wenn es zu dem schweren Datenverlust kam, gilt das Krisenmanagement von Anthem dennoch als professionell und in weiten Teilen lehrbuchmäßig.

Schnell reagieren und transparent kommunizieren

Nicht die Medien oder Aufsichtsbehörden bemerkten den Dateneinbruch, sondern Anthem selbst, was ein entscheidender Faktor für die Krisenbewältigung und die Zurückgewinnung verlorenen Vertrauens war. Die Warnsysteme hatten angeschlagen und so eine schnelle Entdeckung ermöglicht. Es gab auch ein klares Meldewesen für entsprechende Vorfälle.

Auch wenn Anthem erst innerhalb von 60 Tagen die vom Datendiebstahl betroffenen Personen hätte informieren müssen, entschloss sich das Unternehmen, die Öffentlichkeit bereits acht Tage nach Feststellung des Vorfalles in Kenntnis zu setzen. Der schnelle Schritt in die Öffentlichkeit hat Vertrauen geschaffen und Transparenz demonstriert. Das Unternehmen legte dar, welche Daten entwendet wurden und welche Informationen aller Voraussicht nach nicht betroffen wären.
Nicht zu kommunizieren, ist im Krisenfall keine zielführende Option, denn andere Beteiligte kommunizieren in jedem Fall. Betroffene Unternehmen müssen frühzeitig Einfluss auf die Meinungsbildung nehmen. Schweigen ist hierbei wenig hilfreich und erweckt den Eindruck des Verschleierns.

Als Negativbeispiel sei die US-Supermarktkette Target genannt, die erst an die Öffentlichkeit ging, nachdem Außenstehende von dem Hackerangriff berichtet hatten. Der Einzelhandelskonzern benötigte anschließend mehrere Wochen, um die Kunden zu informieren.
Auch der Messenger-Dienst Snapchat informierte über einen Hack auf seine 4,6 Millionen Accounts erst nach Monaten, was zu einem öffentlichen Aufschrei führte.

Allerdings ist auch eine rasche Reaktion auf Krisenfälle nicht immer unproblematisch. Es besteht die Gefahr, dass in der Anfangsphase unvollständige oder falsche Informationen herausgegeben werden und die Kommunikation vage oder unvollständig wirkt. Deshalb müssen in der Krisenkommunikation Informationen stets aktualisiert werden.

Schadenbegrenzung und Lösungsangebote

Niemand erwartet sofortige Lösungen für die Betroffenen, solange das Unternehmen glaubwürdig darstellen kann, dass es mit Spezialisten den Fall mit Nachdruck untersucht und schnell und unbürokratisch Unterstützung bieten wird. Die zuständigen Behörden wurden im Fall von Anthem sofort informiert und der Krankenversicherer unterstützte vorbehaltlos deren Ermittlungen.

Anthem bot bereits mit der Offenlegung des Dateneinbruches konkrete Hilfestellungen an. Eine Hotline mit auf den Fall geschulten Telefonisten wurde geschaltet, zudem wurde eine spezielle Webseite errichtet, auf der sich Antworten zu häufigen Fragen fanden - auch um die Telefonhotline zu entlasten. Betroffene bestätigten das professionelle Handling von Anrufen durch den Krankenversicherer. Die Informationen auf der Internetseite waren gut zu finden, leicht verständlich formuliert und kompakt.

Fallstudie Krisen- und Reputationsmanagement nach einem Cyberangriff

Nach dem Datendiebstahl bei der Supermarktkette Target hingegen empfanden Anrufer die Telefonisten als unfreundlich und schlecht informiert. Die Wartezeiten in der Hotline waren zu lange. Ein Hinweis auf der Internetseite zu Hilfen für die Betroffenen war nur schwer zu finden. Die schriftlichen Informationen waren sehr unverständlich.

Betroffene erwarten klare Aussagen dazu, was sie in die Wege leiten sollen, wie das Unternehmen helfen kann und wie sie die Auswirkungen für sich selbst minimieren können. Diesen Grundsatz beachtete Anthem in seiner Reaktion.

Verantwortung übernehmen und Betroffenheit zum Ausdruck bringen

Der CEO von Anthem äußerte sich persönlich in einem offenen Brief an die Geschädigten. Er entschuldigte sich aber nicht nur bei den Kunden, sondern auch bei den eigenen Mitarbeitern, die von dem Hackerangriff betroffen waren und zeigte Verständnis für deren Verärgerung. Eine persönliche Verbindung zu den Betroffenen stellte er dadurch her, dass er darauf hinwies, dass auch seine Daten gehackt wurden.

Juristen zögern meist vor einer öffentlichen Entschuldigung - für die Krisenkommunikation ist sie aber eine wichtige Maßnahme, die nicht zu spät erfolgen darf. Sie sollte selbstverständlich nicht als Schuldeingeständnis formuliert werden.

Verantwortung zu übernehmen bedeutet auch, für den entstandenen Schaden einzutreten. Anthem beauftragte nach Bekanntwerden des Datenverlustes eine renommierte IT-Sicherheitsfirma mit der Untersuchung des Schadens und der Schwachstellen, die den Angriff ermöglicht hatten. Betroffenen standen für 24 Monate kostenfrei die Services einer auf Identitätsschutz spezialisierten Firma sowie das Monitoring der Kreditkarten zu Verfügung. Auf einer eigens eingerichteten Internetseite sind unter anderem Hinweise zu Identitätsdiebstahl und Vorgehensweise bei einem Verdachtsfall aufgelistet. Anthem legte dar, wie man zukünftig solche Vorfälle verhindern möchte.

Risikoprävention ist Reputationsmanagement

Hier liegt einer der wenigen - aber schweren - Fehler seitens Anthem. Die gestohlenen Daten lagen unverschlüsselt auf dem Server des Krankenversicherers. Da in der Vergangenheit zahlreiche Firmen Opfer von Hacking und Datendiebstahl wurden, war ein Hackerangriff ein durchaus vorhersehbares Ereignis. Eine noch so ausgeklügelte IT-Sicherheit kann keine hundertprozentige Sicherheit garantieren. Doch eine Krise, für die keine präventiven Maßnahmen etabliert wurden, obwohl die Risiken vorhersehbar waren, hat dramatische Auswirkungen auf die Reputation. Es ist nachvollziehbar, dass Öffentlichkeit, Betroffene und Kunden dafür wenig Verständnis haben und Professionalismus hier nur schwer unterstellt werden kann.

Die Autoren

Pascal Michel und Michael Pülmanns sind Geschäftsführer der auf Risiko- und Krisenmanagement spezialisierten SmartRiskSolutions GmbH (SRS). Beide waren nach langjähriger Tätigkeit bei einer bundesdeutschen Sicherheitsbehörde zunächst bei Beratungsfirmen tätig. Pascal Michel verantwortete dabei den Bereich „Sicherheit im Ausland und Krisenmanagement“. Michael Pülmanns, der viele Jahre in Lateinamerika und im Mittleren Osten gelebt hatte, war zuletzt vor allem mit Risikoanalysen, Site Surveys sowie Sicherheitstrainings befasst. SRS verfügt über ein internationales Netzwerk von erfahrenen Partnern und Beratern. Kerntätigkeitsbereiche der SRS sind Reisesicherheitsmanagement, Sicherheitstrainings, Länderinformationen einschließlich Travel Tracking sowie Krisen- und Notfallmanagement.

Kontakt unter:
www.smartrisksolutions.de