SmartRiskSolutions
Risk & Crisis Management Consultancy

Krisenmanagement nach einem Datendiebstahl oder Cyber-Fällen

Der Fall des Datendiebstahls beim Fahrdienst-Vermittler Uber ist ein Beispiel dafür, wie Krisenmanagement und Krisenkommunikation nicht aussehen sollten. Es lassen sich einige wichtige Lehren daraus ziehen.

Was nach und nach bekannt wird

Cyberkriminellen gelang es im Oktober 2016, rund 57 Millionen Daten von Kunden und Fahrern von einem Server zu entwenden. Die Erpresser kontaktierten Uber und verlangten 100.000 USD für die Löschung der Kopien. Uber lies die Hacker eine Verschwiegenheitsvereinbarung unterschreiben. Die Lösegeldzahlung wurde durch den Leiter Unternehmenssicherheit, auf Anweisung des damaligen Vorstandes, durchgeführt. Zur weiteren Verschleierung des Datendiebstahls wurde die Zahlung firmenintern als Honorar für einen Penetrationstest durch Hacker verbucht.
Erst am 21. November 2017 – gut ein Jahr später - räumte das Unternehmen diesen schwerwiegenden Vorfall ein. Der Sicherheitsmanager, ein Jurist, verlor inzwischen seinen Arbeitsplatz; ebenso sein Stellvertreter.

Es wird oft gegen wesentliche Grundsätze des Krisenmanagements verstoßen

1. Einen Vorfall zu vertuschen ist oft schlimmer als der Vorfall an sich

Es ist immer wieder überraschend, wie häufig gegen diese Grundregel verstoßen wird. Durch das Vertuschen wird Vertrauen zerstört. Das darauf aufbauende Problem ist, dass man dem Unternehmen – auch wenn es anschließend ehrlich kommuniziert – nur noch schwer Glauben schenkt. Die Datenschutzgesetze in den meisten Ländern schreiben beim Diebstahl personenbezogener Daten eine zeitnahe Unterrichtung der Aufsichtsbehörden und Betroffenen vor. Im Fall Uber bleibt der Eindruck, dass das verspätete Eingeständnis aus rechtlichen Gründen erfolgte, nicht aber weil man dachte, dass es auch sittlich und moralisch geboten sei.

2. Eine Krisenkommunikation sollte Antworten auf die Fragen liefern, die von Interesse sind

Die ersten Presseerklärung von Uber nach Bekanntwerden des Vorfalles warfen mehr Fragen auf, als Antworten geliefert wurden. Der neue CEO gab an, seit Anfang September von dem Hackerangriff gewusst zu haben. Man sei aber erst im November an die Öffentlichkeit gegangen, da man die (nichtbehördlichen) Ermittlungsergebnisse abwarten wollte. Hier stellt sich die Frage, warum dann in der Krisenkommunikation, nachdem anscheinend die Ermittlungsergebnisse vorlagen, so wenig Informationen weitergegeben wurden. Eine Salamitaktik ist mit das Schlechteste, was man in der Krisenkommunikation tun kann.

3. Bei Cyberangriffen ist die Krisenreaktion oft zu sehr auf die Technologie gerichtet

Häufig ist die Krisenreaktion zu sehr auf technologische Aspekte fokussiert, statt auf strategische Entscheidungen auf Grundlage einer soliden Stakeholderanalyse. Teilweise haben Unternehmen separate Krisenstäbe für Cyberfälle. Das ist nicht optimal, denn hier wird oftmals der Unterschied zwischen "Krise" und "Notfall" nicht verstanden. Eine Vielzahl von Krisenstäben parallel für unterschiedliche Krisenszenarien zu unterhalten führt zudem nur zu Verwirrung. Es ist auch nicht Aufgabe des Krisenstabes, die forensischen Untersuchungen durchzuführen oder sich in der operativen Arbeit zu verlieren, sondern aufgrund der Ermittlungsergebnisse strategische Entscheidungen zu treffen und operativen Maßnahmen die Richtung zu geben.

4. Es kommt auf die Entscheidungen an

Dies mag sehr banal klingen, ist aber in der Realität nicht so leicht. In jeder Krise sind es die Entscheidungen auf der strategischen Ebene, die der Krisenstab trifft, die über Sieg oder Niederlage entscheiden. Das Training des Krisenstabes im Vorfeld muss auch auf den Entscheidungsfindungsprozess abzielen und die Mitglieder müssen sich der psychologischen Aspekte bewusst sein, die zu Fehlentscheidungen führen.
Wie falsch man als Unternehmen mit seinen Entscheidungen liegen kann, zeigt auch der diesjährige Fall des Datendiebstahls beim börsennotierten Unternehmens Equifax. Anfangs verlangte das Unternehmen von Kunden, die wissen wollten, ob deren Daten gehackt wurden, dass sie zuerst einen Verzicht auf Schadensersatzklagen unterzeichnen. Erst durch den Druck des Generalstaatsanwaltes sah das Unternehmen davon ab.

Fazit

Es ist immer wieder erstaunlich, wie Unternehmen, die mit einem Börsenwert von mitunter mehreren Milliarden notiert sind, beim Krisenmanagement schwere Fehler begehen. Da Cyberfälle für jedes Unternehmen eine ernste Bedrohung darstellen, sollten das Krisenmanagement und die Krisenkommunikation darauf im Vorfeld ausgerichtet und beübt werden. Dem Krisenstab sollte klar sein, was seine Aufgaben sind und wie schnell weitreichende und belastbare Entscheidungen getroffen werden können und müssen.

Der Autor, Marc Brandner, ist Partner der auf Sicherheits- und Krisenmanagement spezialisierten SmartRiskSolutions GmbH und leitet dort den Bereich Krisenmanagement. SmartRiskSolutions unterstützt Firmen beim Aufbau und der Optimierung eines unternehmensweiten Krisen- und Notfallmanagements, bei Krisenstabsübungen (auch zu Cyber-Themen) und in der Krisenreaktion. Kontakt unter www.smartrisksolutions.de