DER CYBERANGRIFF IST DA

TRANSPARENZ SCHAFFEN UND REPUTATION SCHÜTZEN

von Janine Lutz

Die Bandbreite von Cyberangriffen wird immer grösser: Datendiebstahl, digitale Erpressung, Phishing oder Malware. Die Wahrscheinlichkeit für Unternehmen, Opfer eines solchen Angriffs zu werden, ist so hoch wie nie. Während die Digitalisierung grosses Potenzial für die Zukunftsfähigkeit unserer Wirtschaft bietet, öffnet sie gleichzeitig neue Türen für Missbrauch. Unternehmen müssen sich für den Krisenfall vorbereiten. Die Kommunikation spielt dabei eine Schlüsselrolle.

Nun ist der Fall eingetreten – es gilt, richtig zu kommunizieren.

In den letzten Monaten kam es in der Schweiz zu mehreren schwerwiegenden Ransomware-Attacken auf Unternehmen und Behörden: Comparis, Saurer, Huber+Suhner, Stadler Rail oder die Gemeinde Rolle, um nur einige zu nennen. Die Dunkelziffer ist gross. Tatsächlich ist die Wahrscheinlichkeit, mit der Unternehmen von Cyberangriffen bedroht werden, egal ob KMU oder Grossunternehmen, eher eine Frage des «Wann» und nicht des «Ob». Diese Tatsache stellt auch die Kommunikationsabteilungen vor Herausforderungen. Denn die richtige Kommunikation ist zentral, um die Reputation der Institutionen zu schützen.

VORBEREITUNG IST DIE HALBE MIETE

In der Hektik unmittelbar nach einem Cyberangriff ist es nahezu unmöglich, eine umfassende Krisenkommunikationsstrategie auf die Beine zu stellen. Durch eine vorsorgliche Planung gewinnt das betroffene Unternehmen im Ernstfall Zeit. Genau deshalb sollte ein entsprechender Krisenplan inklusive Kommunikationskonzept schon bereitliegen. Dieses Krisenkonzept sollte dabei nicht nur notwendige Massnahmen aus IT-Sicht und der Rechtsabteilung beinhalten, sondern auch die Unternehmenskommunikation einbeziehen. Für die Kommunikatoren bedeutet dies fest-

zulegen, welche Informationen das Unternehmen wann und an wen weitergibt. Auch über Kommunikationswege sollten sich die Verantwortlichen früh Gedanken machen: Je nach Art der Attacke stehen vielleicht Firmennetzwerk, Intranet oder E-Mail-Systeme nicht mehr zur Verfügung. Es ist daher elementar, dass Back-up-Lösungen eingeplant werden und die Unternehmenskommunikation als Mitglied des Krisenstabs vorgesehen ist.

VERTRAUEN GEWINNEN

Neben dem Schaden, der durch einen Cyberangriff selbst entsteht, leidet auch die Reputation des Unternehmens. Vielfach werden heikle Daten publik. Wenig verwunderlich ist, dass Unternehmen deshalb gerne eine Verschleierungstaktik / Salamitaktik oder den Mantel des Schweigens bei solchen Angriffen anwenden und damit versuchen, den Reputationsschaden so klein wie möglich zu halten – meistens ohne Erfolg und mit negativer Konsequenz.

Für die optimale Kommunikation im Cyber-Krisenfall gibt es kein Patentrezept. Reputationsschäden lassen sich mit guter Vorbereitung, angemessener Transparenz und rascher Kommunikation begrenzen.

Bei einer unbedachten, zu schnellen Reaktion auf Cyber-Krisenfälle besteht immer auch die Gefahr, dass unvollständige oder falsche Informationen herausgegeben werden und die Kommunikation unprofessionell wirkt. Eine zu rasche öffentliche Reaktion kann auch den Angreifer warnen. Häufig wissen Hacker zu einem frühen Zeitpunkt noch gar nicht, dass man ihnen auf die Schliche gekommen ist. Der Zeitpunkt der ersten Veröffentlichung ist somit taktisch klug zu wählen.

Wird die Attacke publik, ist beharrliches Schweigen gegenüber Mitarbeitenden, Kunden oder Medien im Falle ebenfalls nicht ratsam. Das Vertrauen in das Unternehmen könnte nachhaltig beschädigt oder komplett zerstört werden. Aus kommunikativer Sicht ist zu empfehlen, die Betroffenen mit ersten, gesicherten Fakten zeitnah zu informieren Auch in den sozialen Netzwerken will jeder Schritt gut überlegt sein. Gerade hier lösen erfolgreiche Cyberangriffe nämlich oft Proteststürme aus. Diskussionen auf diesen Kanälen sollten zwar ernst genommen, aufgeregte und emotional geführte Debatten aber vermieden werden.

Nach der Lösung des Schadenfalls beginnt die Phase der positiven Erzählungen.

FÜNF REGELN IM FALLE EINES CYBERANGRIFFS

> Agieren, nicht reagieren: Durchatmen, Fakten sammeln, Kommunikation planen und zeitnah ehrlich und offen kommunizieren.
> Kommunikation steuern: Auch schlechte Nachrichten sollte das Unternehmen wenn immer möglich selbst verkünden und nicht darauf warten, dass andere zuerst darüber berichten.
> Erreichbarkeit sicherstellen: Erreichbar sein und auf Anfragen rasch reagieren, ebenso für Rückfragen seitens der Mitarbeitenden, Kunden und Medien.
> Informationskaskade: Zuerst die Mitarbeitenden informieren, danach umgehend die Kunden und die Medien entsprechend mit Informationen nachversorgen.
> Nach der Krise ist vor der Krise: Manöverkritik durchführen, das IT-Sicherheitskonzept prüfen und die nötigen Lehren für die Kommunikation ziehen.

LEHREN ZIEHEN

Ist der Cyberangriff erfolgreich abgewehrt, ist die Kommunikation allerdings noch lange nicht beendet. Geeignete sogenannte «Recovery-Massnahmen» helfen, die Normalität für das Unternehmen nach innen und nach aussen wiederherzustellen. Die betreffenden Schritte gehören ebenfalls kommuniziert. Anhand der Cyberkrise lässt sich gegebenenfalls sogar eine positive Geschichte darüber erzählen, wie das Unternehmen eine solch extreme Herausforderung gemeistert und sich die Organisation in der Not bewährt hat – Stichwort Resilienz. Wie nach jeder Krise sollte zudem eine Nachbearbeitung stattfinden, um mögliche Verbesserungspotenziale zu identifizieren. Um bei einem Ernstfall gut vorbereitet zu sein, eignen sich zudem Krisensimulationen und -trainings.

Eine umsichtige Vorbereitung und eine transparente Kommunikation sind der Schlüssel, um in der Krisensituation schnell und adäquat reagieren zu können. Vertrauen aufbauen und erhalten – das schafft ein Unternehmen in einer Krisensituation nur mit einem offenen Dialog.

JANINE LUTZ

ist Consultant bei IRF.

www.irf-reputation.ch