STORMSHIELD

MEINUNGEN

CYBERATTACKEN: WENN KOMMUNIKATION ZUM TAKTISCHEN INSTRUMENT IM DIENSTE DESKRISEN-MANAGEMENTS WIRD

Julien Paffumi
Senior Product Manager, Stormshield

Wenn sie Opfer eines Cyberangriffs werden, entscheiden sich einige Unternehmen dafür, nicht oder nur wenig über das Thema zu kommunizieren. Dennoch ermutigen nationale Sicherheitsagenturen und CERT (Computer Emergency Response Teams) dazu, so transparent wie möglich zu kommunizieren. Das Ziel? Verbesserung der allgemeinen Zusammenarbeit angesichts der Internetkriminalität und Beruhigung des Wirtschaftsgefüges. Aber warum ist Kommunikation dann manchmal tabu? Soll man kommunizieren oder nicht? Und gegenüber wem?

Im Hinblick auf die Kommunikation von Opfern von Cyberangriffen ist das Beispiel von Norsk Hydro beeindruckend. 2019 wird dieser norwegische Industriebetrieb Opfer einer Ransomware, die mehrere Produktionsstätten und Teile seiner Kommunikationsdienste lahmlegt. Das Unternehmen beschloss dennoch, transparent zu sein und eröffnete bereits am Tag nach dem Angriff eine öffentliche Seite auf seiner Website, die seiner Krisenkommunikation gewidmet war. Diese wurde regelmäßig aktualisiert. In den Monaten nach der Krise berichten die Medien dann über Norsk Hydro als leuchtendes Beispiel in der Kommunikation von Cyberangriffen

WARUM ENTSCHEIDEN SICH MANCHE UNTERNEHMEN FÜR DISKRETION?

Dieser Schulfall wird bis heute aus Sicht des Krisenmanagements als Beispiel angeführt. Wie ist es also zu erklären, dass manche Opfer es stattdessen vorziehen, sich diskreter zu verhalten?

„Für ein Unternehmen ist es natürlich schwierig, zuzugeben, dass es Opfer eines Cyberangriffs geworden ist", erklärt **Yannick Duvergé** , CEO und Gründer von Exemplary, einem Unternehmen, das auf Krisenkommunikation spezialisiert ist. *„Das ist so, als würde man zugeben, dass man Schwächen hat, was schwerwiegende Folgen für das Geschäft haben kann."* Aus Image-Gründen und somit auch aus geschäftlichen Gründen ist es üblich, Strategien zu verfolgen, die darauf abzielen, die Folgen eines Angriffs zu verschleiern oder zu minimieren. Ein weiteres Argument gegen die Kommunikation: **die Befürchtung, dass es zu einem Mitnahmeeffekt kommen könnte**. Andere Personen mit bösen Absichten könnten die Zeit zwischen der Entdeckung des Cyberangriffs und dem Patch, der die ausgenutzte Softwareschwachstelle behebt, nutzen, um ihrerseits eine Reihe von Übeltaten zu begehen. Es ist daher von entscheidender Bedeutung, den Grad der öffentlich kommunizierten technischen Details genau zu dosieren, sowohl um eine verständliche Botschaft zu vermitteln als auch um das Opferunternehmen zu schützen", erklärt **Stéphanie Ledoux**, Gründerin und CEO von Alcyconie, einer Firma, die sich mit dem Management und der Kommunikation von Cyberkrisen befasst. *„Wenn eine Software-Schwachstelle ausgenutzt wurde, kann die Kommunikation mit Kollegen in der Branche auch verhindern, dass der Angriff andere Organisationen trifft, die die gleiche Software verwenden."*

„Für ein Unternehmen ist es natürlich schwierig, zuzugeben, dass es Opfer eines Cyberangriffs geworden ist. Dies ist gleichbedeutend mit dem Eingeständnis, Schwächen zu haben, was schwerwiegende Folgen für das Geschäft haben kann."

Yannick Duvergé, CEO und Gründer von Exemplary

Parallel dazu **regeln Gesetzestexte einen Teil der Äußerungen von Unternehmen** – von denen einige gezwungen werden können, nicht zu kommunizieren. Bei gerichtlich verhandelten Fällen *„ist es häufig so, dass die Unternehmen ihren Krisenkommunikationsplan erst dann in dem von ihnen gewünschten Tempo umsetzen können, wenn die Ermittler ihre Arbeit getan haben*", erinnert **Pierre-Yves Hentzen,** CEO von Stormshield. Auf der Seite der gefährdeten Unternehmen, seien es Betreiber von vitaler Bedeutung (OIV) auf französischer Ebene oder Betreiber wesentlicher Dienste (OSE) auf europäischer Ebene, sind sie **an ein strenges Kommunikationsprotokoll gebunden**. Andererseits schreiben andere Gesetzestexte den Unternehmen eine gewisse Kommunikation vor, diesmal nicht öffentlich, sondern um die zuständigen Behörden über den erlittenen Cyberangriff zu informieren. Artikel 33 der Datenschutz-Grundverordnung (DSGVO)) verpflichtet Unternehmen, die mit den personenbezogenen Daten von EU-Bürgern umgehen, Warnprotokolle zu befolgen, die in den Ländern gelten, in denen sie tätig sind; beginnend mit der *„Benachrichtigung der Aufsichtsbehörde über eine Verletzung der personenbezogenen Daten*". Das Unternehmen, das Opfer eines

Cyberangriffs wurde, muss die Behörden spätestens 72 Stunden nach Entdeckung des Datenlecks alarmieren. Darüber hinaus verpflichtet Artikel 34 derselben DSGVO diese Unternehmen, die betroffenen Personen über ein Datenleck zu informieren. Die Frist für die Mitteilung ist jedoch ungenau und liegt im Ermessen des Unternehmens, das Opfer des Cyberangriffs geworden ist, und/oder der Justizbehörden, im Falle einer Untersuchung. Personenbezogene, sensible, kritische oder auch lebenswichtige Daten; auch das Vokabular kann zu Verwirrung führen. Wie dem auch sei, Stéphanie Ledoux erinnert daran, dass *„diese Unternehmen oft vertraglich verpflichtet sind, ihre Stakeholder oder Kunden zu informieren. Deshalb ist es wichtig, von einer kompetenten Rechtsabteilung begleitet zu werden, um genau zu wissen, was in der jeweiligen Situation zu tun oder zu sagen ist.*"

„Diese Unternehmen sind oft vertraglich verpflichtet, ihre Stakeholder oder Kunden zu informieren. Deshalb ist es wichtig, von einer kompetenten Rechtsabteilung begleitet zu werden, um genau zu wissen, was in der jeweiligen Situation zu tun oder zu sagen ist."

Stéphanie Ledoux, Gründerin und CEO von Alcyconie

Aber auch wenn diese Faktoren das Schweigen einiger Unternehmen erklären können, sind sich die Experten dennoch einig, dass die Kommunikation im Falle eines Cyberangriffs eine Notwendigkeit ist.

WARUM EMPFEHLEN EXPERTEN EINE TRANSPARENTE KRISENKOMMUNIKATION?

So stellt Stéphanie Ledoux die Kommunikation als *„ein taktisches Instrument im Dienste des Krisenmanagements dar"*. Wenn sie effektiv durchgeführt wird, trägt sie wesentlich zu einer positiven Auflösung bei, wie der Fall von Anthem unterstreicht. Am 27. Januar 2015 wurde diese US-amerikanische Krankenversicherung (eine der größten auf dem Markt in den USA), Opfer eines Cyberangriffs. Am 4. Februar veröffentlichte das Unternehmen seine erste Mitteilung, in der es zugab, Opfer einer *„hochentwickelten Aktion"* geworden zu sein. Und schlimmer noch: Die Daten von mehreren zehn Millionen Kunden fielen in die Hände von Cyberkriminellen. In den folgenden Tagen sendet Anthem persönliche Nachrichten an alle betroffenen Kunden und rät ihnen, welche Maßnahmen sie ergreifen sollten. Obwohl die Situation für das Image des Unternehmens katastrophal sein könnte, wird die Strategie von Anthem, ähnlich wie die von Norsk Hydro, immer wieder als seriöses und transparentes Beispiel herangezogen.

Die positiven und nachhaltigen Auswirkungen eines transparenten Ansatzes in der Krisenkommunikation würden sich größtenteils durch eine bessere Sensibilisierung der breiten Öffentlichkeit erklären lassen. In der Vergangenheit konnte diese die Unternehmen, die Opfer von Cyberangriffen wurden, belasten, doch dies wäre nicht mehr der Fall, da *„sie weiß, dass Cyberangriffe immer häufiger vorkommen und jedes Unternehmen treffen können, selbst die am besten vorbereiteten"*, sagt **Sébastien Viou**, Direktor für Produktsicherheit und Cyber-Spezialist bei Stormshield. Wenn ein Fall eines

Cyberangriffs in den Medien bekannt wird, wäre der erste Reflex der Öffentlichkeit eher, *„mehr darüber in Erfahrung zu bringen, wie das Unternehmen die Krise bewältigt und mit seinen Schwierigkeiten umgeht*", analysiert Stéphanie Ledoux. *Die Öffentlichkeit lässt sich nicht mehr täuschen. Wenn ein Unternehmen versucht, die Auswirkungen eines Cyberangriffs zu verschleiern, alarmiert sie das umso mehr*". Aus Angst vor dem Zorn der öffentlichen Meinung nicht zu kommunizieren, wäre daher unsinnig geworden.

„Die breite Öffentlichkeit weiß, dass Cyberangriffe immer häufiger vorkommen und jedes Unternehmen treffen können, selbst die am besten vorbereiteten."

Sébastien Viou, Direktor für Produktsicherheit und Cyber-Spezialist bei Stormshield

Pierre-Yves Hentzen betont seinerseits, dass die **meisten Argumente gegen transparente Kommunikation auf einen gemeinsamen Nenner gebracht werden: Angst**, insbesondere die Angst, den eigenen Geschäftsbeziehungen zu schaden. Nun *„ist es genau das, wozu Krisenkommunikation dient: zu beruhigen. Je nach Situation ist das Unternehmen nicht verpflichtet, sofort die Öffentlichkeit zu alarmieren, aber es muss seine Mitarbeiter, Stakeholder und Kunden beruhigen! Die Folgen der Krise können für sie genauso wichtig sein, und diese Tatsache zu leugnen, wird dem Ruf des angegriffenen Unternehmens wahrscheinlich mehr schaden."*

Die ANSSI hält die Schädigung des Markenimages eines Unternehmens für eine der vier Hauptmotivationen für Cyberangriffe.. Die französische Agentur bestätigt damit, dass die häufigsten Cyberangriffe *„hauptsächlich darauf abzielen, das Image ihres Ziels zu schädigen*". Außerdem erinnert Sébastien Viou daran, dass *„Cyberkriminelle nach ihren Vergehen nicht selten Kommunikationsmaßnahmen in sozialen Netzwerken durchführen, um den Datenbestand, den sie im Darknet weiterverkaufen wollen, zu bewerben und/oder das Markenimage des Opfers zu schädigen*". Das Unternehmen kann sich noch so sehr bemühen, die Auswirkungen des Cyberangriffs zu verschleiern oder herunterzuspielen, es **ist sehr wahrscheinlich, dass jemand die Informationen für das Unternehmen durchsickern lässt**. *„Es ist besser, sofort eine transparente Haltung einzunehmen, um zu zeigen, dass man das Feld besetzt; dass man nicht wegläuft*", schließt Stéphanie Ledoux.

WIE KOMMUNIZIERT MAN WÄHREND EINES CYBERANGRIFFS?

Für Unternehmen, die kommunizieren möchten, bleibt die Frage, wie sie dabei vorgehen sollen. Der erste Ratschlag ist, *„schnell zu handeln*", unterstreicht Yannick Duvergé. Wie bereits erwähnt, muss das Unternehmen davon ausgehen, dass früher oder später Informationen durchsickern werden. **Wenn der Unternehmenskommunikation jedoch mehr oder weniger konkrete Gerüchte vorausgehen, können die Auswirkungen auf das Vertrauen, das die Öffentlichkeit der Marke entgegenbringt, verheerend sein**. Zwischen November und Dezember 2013 wurde das amerikanische Unternehmen Target Opfer eines Cyberangriffs, der dazu führt, dass die Bankdaten von etwa zehn Millionen Kunden im Internet verbreitet werden. Das Unternehmen zieht es vor, nicht zu kommunizieren. Keine Chance: Eine externe Quelle informiert die Öffentlichkeit als Erste. Diese Strategie bringt Target den Vorwurf ein, den Angriff und seine möglichen Folgen

für die Öffentlichkeit verschleiert zu haben. Die Auswirkungen auf das Markenimage sind verheerend, und die Wahrnehmung der Verbraucher erreicht einen historischen Tiefstand. Laut Sébastien Viou werden Informationen, die von „externen" Quellen an das Unternehmen weitergegeben werden, immer häufiger von Cyberkriminellen genutzt. *„Sie sehen darin eine Möglichkeit, die betroffenen Unternehmen zu Lösegeldzahlungen (z. B. bei Ransomware-Angriffen) zu zwingen oder die gestohlenen Daten bei möglichen Käufern anzupreisen. „Um nicht das gleiche Schicksal wie Target zu erleiden, wird den Unternehmen daher empfohlen, als Erste zu kommunizieren. Ein Prinzip, das oft mit „stealing thunder"* bezeichnet wird: **Die Kommunikation von Unternehmen soll Cyberkriminellen den Wind aus den Segeln nehmen**.

Aber an wen sollen die ersten Nachrichten gerichtet werden? Aus Erfahrung weiß Pierre-Yves Hentzen, dass es unbedingt notwendig ist, die Phase der Krisenkommunikation mit den Mitarbeitern des Unternehmens zu beginnen. Sie sollten so weit wie möglich informiert werden, aber vor allem eine beruhigende Haltung in Bezug auf *„den Zustand des Unternehmens und ihre Zukunft"* einnehmen. Dies ist auch der ideale Zeitpunkt, um ihnen das Verhalten zu vermitteln, das von ihnen während der gesamten Krise erwartet wird, insbesondere in Bezug auf die Vertraulichkeit. *„Sie werden von der Presse oder externen Akteuren angesprochen und müssen sich an den festgelegten Kommunikationsplan halten. Sie einzubeziehen hilft daher sehr bei der positiven Lösung der Krise."* Stéphanie Ledoux betont ihrerseits, wie wichtig es ist, *„keine kalte, technische oder gar schuldbewusste Haltung einzunehmen"*, da dies die Scham verstärken könnte, die Mitarbeiter empfinden, die unfreiwillig zur Verbreitung des Cyberangriffs beigetragen haben. *„Sie sind die ersten Opfer von Cyberkriminellen und solange keine Beweise für eine **Verletzung der Sicherheitsregeln vorliegen**, sollten sie auch als solche behandelt werden"*, ergänzt Sébastien Viou. Die Meinung der Experten stimmt mit den Empfehlungen der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) und den verschiedenen europäischen CERT überein. Beide Institutionen raten dazu, die verschiedenen Zielgruppen in dieser Reihenfolge anzusprechen: Mitarbeiter, Stakeholder (oder Aktionäre), Wirtschaftspartner (und Auftragnehmer), Kunden und schließlich die Presse.

„Die Mitarbeiter werden von der Presse oder externen Akteuren angesprochen und müssen sich an den festgelegten Kommunikationsplan halten. Sie einzubeziehen hilft daher sehr bei der positiven Lösung der Krise."

Pierre-Yves Hentzen, Vorstandsvorsitzender von Stormshield

Es muss jedoch noch sichergestellt werden, dass **die Qualität der übermittelten Informationen gewährleistet ist**. In den Stunden nach der Entdeckung eines Cyberangriffs ist es jedoch sehr schwierig, genau zu wissen, was passiert ist, und sich daher eine Kommunikationsmaßnahme zu diesem Thema vorzustellen. Je nach Fall und Schwere des Angriffs kann das Unternehmen potenziell auf die Hilfe der zuständigen Behörden zurückgreifen. In Frankreich kann die ANSSI technische Untersuchungen veranlassen, um den geschädigten Unternehmen zu helfen, die Aspekte des Angriffs einzuordnen. Bedeutet dies, dass keine Nachricht übermittelt werden darf, solange der Modus Operandi des Cyberkriminellen nicht bekannt ist? *„Das Unternehmen kann damit*

beginnen, den Angriff einzugestehen, ohne sich in Mutmaßungen zu ergehen. Es kann auch erklären, inwiefern dies das reibungslose Funktionieren beeinträchtigt. Das hat den Vorteil, dass es transparent ist und zeigt, dass die Unternehmensleitung sich dem Thema stellt und Verantwortung übernimmt", erklärt Stéphanie Ledoux. Dieses Gefühl kann übrigens noch verstärkt werden, wenn die Unternehmenskommunikation „*von einem leitenden Angestellten oder sogar dem Geschäftsführer des Unternehmens verkörpert wird*", fügt Yannick Duvergé hinzu. „*Dieses Verfahren vermenschlicht die Kommunikation. Dadurch wird das Vertrauensverhältnis zur Öffentlichkeit viel leichter aufgebaut.*" Wenn ein Unternehmen der Meinung ist, dass es noch nicht die Möglichkeit hat, außerhalb seiner Organisation zu kommunizieren, kann es dennoch von bestimmten privaten Einrichtungen und Clubs wie den Clubs für vernetzte Informationssicherheit (Clusir) profitieren. Die Mitglieder erhalten so **einen relativ vertraulichen Raum für den Austausch von bewährten Verfahren und Erfahrungen im Bereich der Cybersicherheit.**

Was kommt nach der Cyberattacke? Mehrere Monate nach einem Cyberangriff ziehen einige Unternehmen eine detaillierte Bilanz ihrer Missgeschicke. Diese Art der Kommunikation hat den Vorteil, dass auch andere von diesem Feedback profitieren können. Sébastien Viou erklärt, dass Cybersicherheitsunternehmen wie Stormshield besonders an Berichten interessiert sind, die den Ablauf von Cyberangriffen und die Kompromittierungsindizes der inkriminierten Lösungen detailliert beschreiben: „*das ermöglicht uns, ständig das Ohr am realen Geschehen zu haben*". Außerdem: „*Wenn das Unternehmen seine Kommunikation fortsetzt und sich diesmal auf die von ihm durchgeführten Maßnahmen und die daraus gewonnenen Erfahrungen konzentriert, könnte es sehr wohl aufgewertet daraus hervorgehen*", erklärt Yannick Duvergé. Dieser transparentere Ansatz half Target, sich aus seiner anfänglichen Flaute zu befreien. Im Jahr nach dem Angriff setzte die neue Führung zahlreiche Baustellen für die Cyber-Resilienz in Gang, die insgesamt fast 17 Millionen US-Dollar kosteten. Indem sie die Öffentlichkeit ständig über diese Entwicklungen informierte, gelang es ihr, ihr Image wieder aufzupolieren und das Quartal auf dem gleichen Niveau wie vor dem Cyberangriff zu beenden.

Ein Beweis dafür, dass die Öffentlichkeit versteht und sogar einen Sicherheitsmangel verzeihen kann. Vorausgesetzt, dass die Kommunikation gute Argumente wertschätzt.

STORMSHIELD

Stormshield, eine hundertprozentige Tochtergesellschaft von Airbus CyberSecurity, bietet innovative End-to-End-Sicherheitslösungen zum Schutz von Netzwerken (Stormshield Network Security), Desktops (Stormshield Endpoint Security) und Daten (Stormshield Data Security). **www.stormshield.com**