KOMM. PASSION | TEAM FARNER

KOMMUNIKATION IN DER CYBERKRISE

Einleitung

Die Zahlen sprechen eine deutliche Sprache: 95 % der deutschen Unternehmen waren in den letzten Jahren von Datenlecks betroffen, weltweit ist der Anteil sogar noch höher. Die Schäden sind oft verheerend – 83 % der Betroffenen mussten Verluste von bis zu 9,9 Millionen Dollar hinnehmen, wie die „Digital Trust Insights"-Studie von PwC zeigt.[1] Ein Cyberangriff trifft Unternehmen oft wie ein Blitz aus heiterem Himmel. Gerade in solchen Momenten zeigt sich, wie gut die vorbereitenden Maßnahmen greifen und wie robust die Krisenkommunikationsstrategie ist.

Doch die eigentliche Gefahr liegt nicht nur im Angriff selbst, sondern vor allem in der unmittelbaren und angemessenen Reaktion darauf. Unternehmen, die in der Lage sind, eine Cyberkrise souverän zu kommunizieren, können das Vertrauen der Stakeholder wahren und den langfristigen Schaden begrenzen. Dabei erfordert jede Cyberattacke eine angepasste Kommunikationsstrategie, denn kein Angriff gleicht dem anderen: Ob Ransomware, DDoS-Attacke oder Phishing-Angriff – je nach Art und Ausmaß müssen Kommunikationsmaßnahmen differenziert und zielgerichtet eingesetzt werden, um die richtigen Botschaften an Mitarbeitende, Kunden und die Öffentlichkeit zu übermitteln.

Cyberangriffe stellen daher nicht nur die IT-Sicherheit eines Unternehmens auf die Probe, sondern sind auch ein Maßstab für die Fähigkeit, Krisenkommunikation auf höchstem Niveau zu betreiben.

1. https://www.pwc.de/de/pressemitteilungen/2024/studie-deutsche-unternehmen-deutlich-haeufiger-von-datendiebstahl-und-missbrauch-betroffen-als-weltweiter-durchschnitt.html

Kommunikation in der Cyberkrise

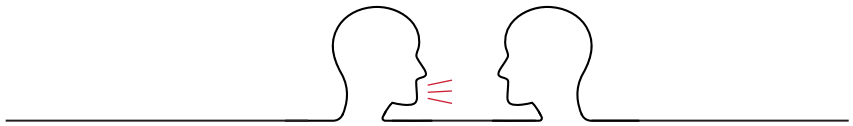
Immer wieder ist festzustellen, dass die Unternehmenskommunikation oder die Geschäftsleitung versucht ist, jede Variante von Cyberattacken kommunikativ gleich zu behandeln. Ein Fehler. Jede Attacke kann unterschiedliche Ausmaße, Ziele und Folgen haben. Eine differenzierte Herangehensweise hilft dabei, angemessene und wirksame Kommunikationsstrategien zu entwickeln, die den spezifischen Anforderungen der jeweiligen Cyberkrise gerecht werden.

Cyberattacke ist nicht gleich Cyberattacke

Enkeltrick, falscher Gasableser oder Deepfake-Anrufe. Ähnlich wie in der analogen Welt gibt es auch bei der Cyberkriminalität unzählige Angriffsstrategien mit denen Kriminelle Unternehmen schaden wollen. Deshalb sollten die Kommunikationsmaßnahmen in der Cyberkrise an den betroffenen Angriffsvektoren ausgerichtet sein.

Eine Cyberattacke, bei der personenbezogene Daten gestohlen werden, erfordert eine andere kommunikative Herangehensweise als eine, die „nur“ einen Systemausfall verursacht. Datenschutzvorfälle könnten rechtliche Konsequenzen haben und erfordern präzise und zeitnahe Kommunikation an betroffene Kunden und Aufsichtsbehörden. Ein Systemausfall hingegen könnte eine pragmatischere, technische Kommunikation mit den betroffenen Nutzer:innen erforderlich machen.

Manche Cyberattacken, wie Ransomware-Angriffe, können sofortige finanzielle Schäden verursachen, die öffentlich kommuniziert werden müssen, um Stakeholder zu beruhigen und rechtliche Verpflichtungen zu erfüllen. Andere Angriffe könnten mehr Zeit für die Analyse und Abschätzung des Schadensumfangs benötigen.



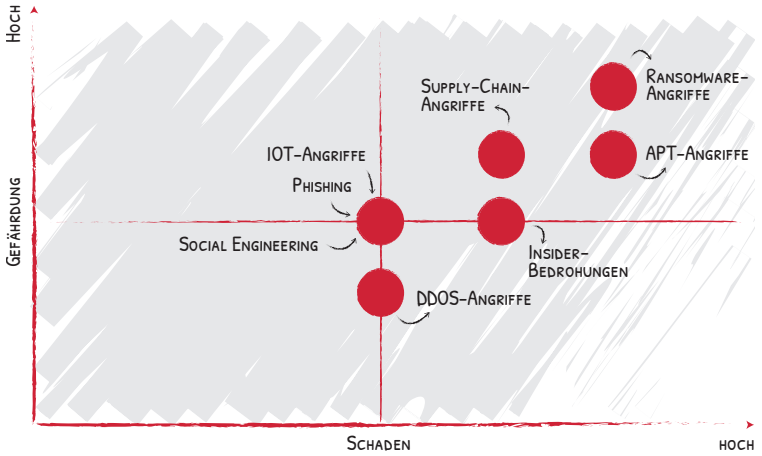
Ein Angriff von außen auf die IT-Systeme unterscheidet sich von einem internen Datenleck. Ein interner Vorfall könnte auf mangelhafte Sicherheitsvorkehrungen hinweisen und erfordert eine andere Kommunikationsstrategie, um Vertrauen wiederherzustellen, als ein externer Angriff, bei dem es darum geht, die Verteidigungsmaßnahmen gegen Cyberkriminelle hervorzuheben.

Unternehmen, die gezielt angegriffen werden (zum Beispiel von Hacktivisten oder Konkurrenten), müssen die öffentliche Kommunikation möglicherweise stärker auf die Reputation und das Unternehmensimage fokussieren. Opportunistische Angriffe, wie sie durch breit gestreute Phishing-Attacken entstehen, könnten hingegen eine allgemeinere Krisenkommunikation erfordern.

Gefahrenpotenzial unterschiedlicher Cyberkrisen

Das Gefahrenpotenzial unterschiedlicher Cyberangriffe auf Unternehmen variiert stark und hängt von der Art des Angriffs, den Zielen und den betroffenen Unternehmensbereichen ab. Unterschiedliche Gefährdungspotenziale haben in der Regel Einfluss auf die Kommunikationsstrategie im Krisenfall.

Hier ist eine Einschätzung der Risiken verschiedener Cyberattacken:



Das Gefahrenpotenzial von Cyberangriffen variiert je nach Art des Angriffs, der betroffenen Branche und den Unternehmensressourcen. Während Angriffe wie Ransomware oder Datendiebstahl unmittelbare und gravierende Auswirkungen haben, können andere wie DDoS-Attacken eher temporäre Schäden verursachen. Eine differenzierte Herangehensweise in der Prävention und Kommunikation ist daher entscheidend, um den jeweiligen Risiken angemessen zu begegnen.

„Wir stehen an einem Punkt, an dem es nicht mehr darum geht, ob ein Unternehmer Opfer eines Cyberangriffs wird, sondern wann es dazu kommt.“

Frederic Bollhorst
Co-CEO
komm.passion | Team Farner

Ad-hoc-Maßnahmen in der Cyberkrise

Nicht jeder Angriffsversuch auf die Firewall im Unternehmen erfordert eine sofortige Kommunikation. Die Abwehr und das Monitoring von Angriffsversuchen sind in viele IT-Abteilungen mittlerweile Alltag.

So berichtet beispielsweise Gerd Chrzanowski[2], Konzernchef der Schwarz-Gruppe, zu der die Discounter Lidl und Kaufland gehören, von bis zu täglich 350.000 Cyberattacken auf die Systeme des Unternehmens. Grundsätzlich ist die Unternehmenskommunikation immer dann zu informieren und zu involvieren, wenn eine Attacke erfolgreich war. Dann sollte innerhalb von 24 Stunden die ersten Kommunikationsmaßnahmen vorbereitet und bei Bedarf durchgeführt werden.

Das Krisenkommunikations-Team aktivieren

Das Team sollte aus IT, PR, Recht und dem Management bestehen. Stellen Sie sicher, dass alle Verantwortlichen regelmäßig über den aktuellen Stand informiert werden, auch wenn die Informationen noch unvollständig sind. Zwingend notwendig ist es, die Verantwortlichkeiten klar zu definieren, wer mit internen und externen Stakeholdern kommuniziert. Stellen Sie sicher, dass die Informationen koordiniert und konsistent weitergegeben werden.

Damit dies möglich ist, sollte die oberste Priorität sein, dass es mindestens einen funktionierenden Kommunikationskanal gibt, auf den alle Teammitglieder jederzeit Zugriff haben. Dies können beispielsweise eine WhatsApp-Gruppe auf privaten Smartphones oder ein separater Sharepoint sein, der nicht Teil des angegriffenen Netzwerkes ist.

Praxistipp: *Die Einrichtung eines Krisenkommunikations-Teams sollte unbedingt vor dem Eintritt einer Krise erfolgt sein. Ein Krisenkommunikations-Team oder einen Krisenstab im Unternehmen einzurichten, ist oberstes Gebot der Krisenprävention, andernfalls verlieren Sie wertvolle Zeit, bis Sie mit einer koordinierten und strukturierten Krisenintervention beginnen können.*

2. https://www.br.de/nachrichten/netzwelt/taeglich-350-000-cyberattacken-gegen-lidl-konzernmutter,UQVAvmS

Erste interne Kommunikation an Mitarbeitende

Ihre Mitarbeitenden werden oftmals die Ersten sein, die von den Auswirkungen einer erfolgreichen Cyberattacke auf Ihre Systeme Kenntnis erhalten. In der Regel werden Cyberangriffe von IT-Mitarbeitenden entdeckt, die dann auch Alarm auslösen. Deshalb ist eine schnelle, vorsichtige Information über den bisher bekannten Sachstand in der Belegschaft notwendig. Teilen Sie den Mitarbeitenden mit, dass es einen Vorfall gab und an der Klärung der Lage gearbeitet wird. Vermeiden Sie Spekulationen über den Schaden oder die Auswirkungen. Informieren Sie die Belegschaft zudem darüber, wie sie sich verhalten soll (zum Beispiel keine E-Mails öffnen, verdächtige Aktivitäten melden) und welche Maßnahmen ergriffen werden, um die Systeme zu sichern.

Praxistipp: *Wie in jeder Krise, so gilt auch hier: Wir kommunizieren intern vor extern. Je nach Ausmaß des Angriffes kann es sein, dass die Bürokommunikation über E-Mail, Telefon oder Intranet nicht mehr verfügbar ist. Stellen Sie sicher, dass wichtige Informationen für Mitarbeitende umfänglich und zeitnah von den Führungskräften in der Organisation kaskadiert werden. Hier sind beispielsweise Team-Besprechungen, die Einrichtung von WhatsApp-Gruppen auf persönlichen Smartphones oder das gute alte „Schwarze Brett" bewährte Kommunikationskanäle.*

Welche Kanäle Sie in der Cyberkrise wie, wann und wo einsetzen, sollten Sie bereits im Vorfeld in einer Krisenpräventionsstrategie als Notfallprozess definiert und funktionsfähig eingerichtet haben.

Das Monitoring intensivieren

Ein erfolgreich durchgeführter Cyberangriff hat nicht unmittelbar Berichterstattung in den Medien oder in Social Media zur Folge. Klar ist, dass je mehr ein Unternehmen im Licht der Öffentlichkeit steht, desto interessanter wird es, über eine Cyberattacke auf dieses Unternehmen zu berichten. Dennoch empfiehlt es sich im Krisenfall so früh wie möglich das Monitoring auf allen Kanälen auszuweiten, um Gerüchte oder Fehlinformationen schnell zu identifizieren und klarzustellen. Monitoren Sie dafür nicht nur Presse und Social Media, sondern vor allem auch die Kommunikation mit Lieferanten, Dienstleistern und Kunden. Die drei Letzteren stehen mit Ihren Unternehmen im direkten Geschäftskontakt und bekommen die Auswirkungen kompromittierter IT-Systeme oftmals sehr schnell zu spüren, weil beispielsweise automatisierter Datentransfer nicht mehr möglich ist, oder der Key-Account nicht mehr telefonieren kann.

Praxistipp: *Monitoring hat zum Ziel, die benötigten Informationen zum relevanten Zeitpunkt für die Kommunikation zur Verfügung zu stellen. Hier gilt: Qualität schlägt Quantität. Entwickeln Sie daher die Monitoring-Prozesse für Krisen stets zielorientiert. Wenn Sie beispielsweise wissen müssen, wie Lieferant:innen auf die Auswirkungen des Cyberangriffs reagieren, können die Mitarbeitenden im Einkauf nach kritischen Kontakten beispielsweise über ein kurzes Standardformular eine Gesprächsbewertung anlegen, die regelmäßig von der Unternehmenskommunikation gesammelt und ausgewertet wird. Auch hier empfiehlt sich, die Monitoring-Strategie bereits im Voraus zu definieren und die festgelegten Maßnahmen umzusetzen.*

„In einer Zeit, in der digitale Bedrohungen immer präsenter werden, ist eine starke Krisenkommunikation nicht nur ein zusätzlicher Schutz – sie ist ein Wettbewerbsvorteil.“

Patrick Hacker
Deputy Management Director
komm.passion | Team Farner

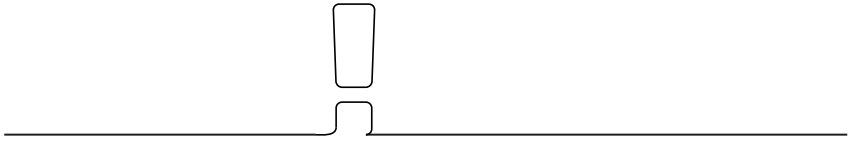
Fazit

Cyberattacken sind nicht länger eine Frage des „Ob“, sondern des „Wann“ es zu einem Angriff kommt. Die Auswirkungen können verheerend sein, von finanziellen Schäden bis hin zu Vertrauensverlust bei Stakeholdern. Wie ein Unternehmen auf eine solche Krise reagiert, entscheidet über den langfristigen Erfolg.

Ein Pfeiler zum Überstehen eines Cyberangriffs liegt in der differenzierten Kommunikationsstrategie. Keine Attacke gleicht der anderen und daher müssen die Maßnahmen auf den Angriff angepasst sein.

Die Vorbereitung ist dabei entscheidend! Die Mitglieder des Krisenkommunikationsteams sollten bereits vor dem Ernstfall festgelegt und jederzeit arbeitsfähig sein. Interne Informationswege müssen klar definiert sowie alternative Kommunikationskanäle für den Notfall funktionssatzfähig sein.

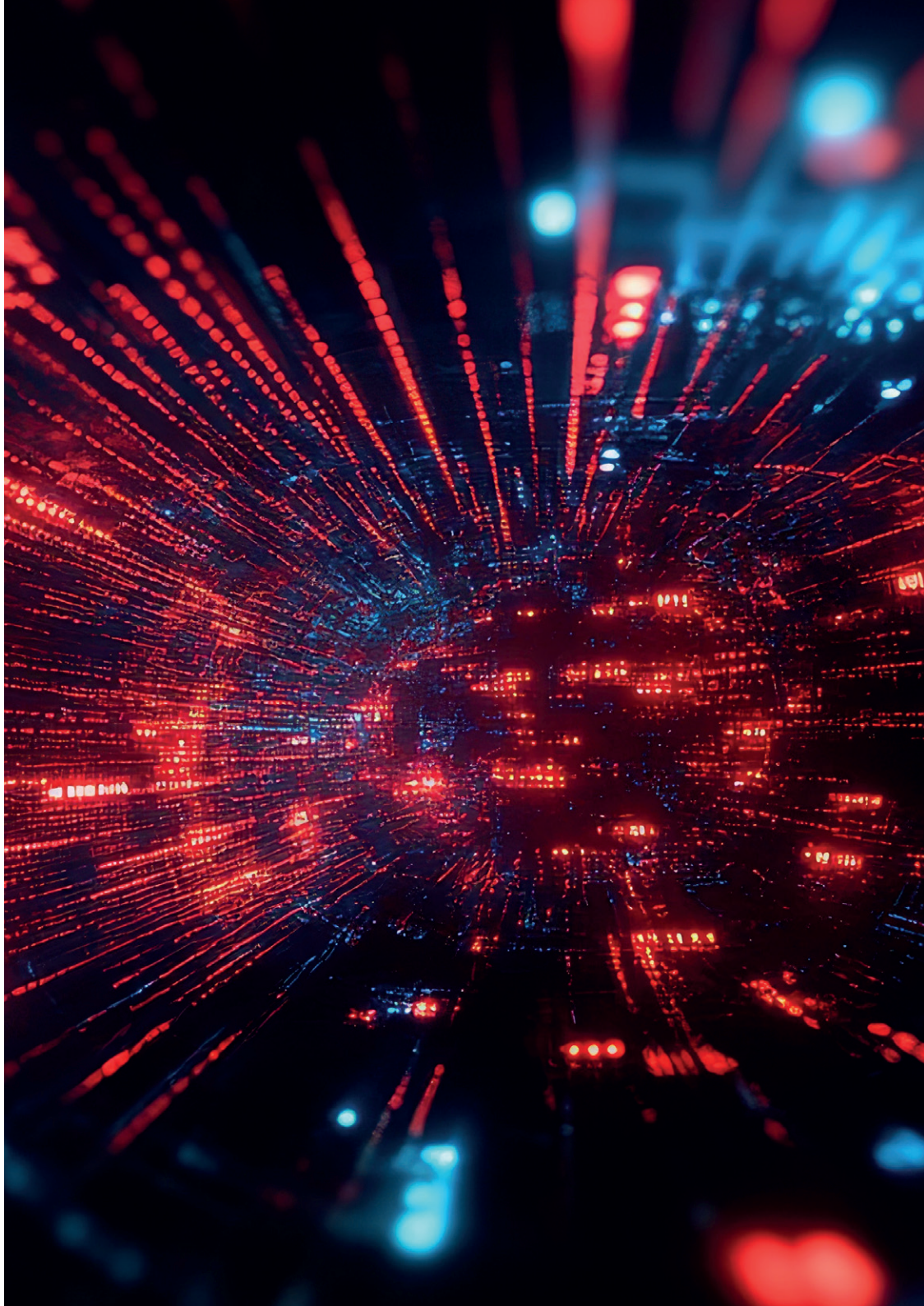
Die interne Kommunikation mit den Mitarbeitenden ist von enormer Bedeutung, um Spekulationen vorzubeugen. Auch die Kontrolle über Information die nach außen fließen, muss durch effektives Monitoring beibehalten werden.



First Aid

Was tun, wenn man angegriffen wurde? Auf die ersten Minuten kommt es an! Diese Schritte garantieren, dass sofort jeder Handgriff sitzt und die Kontrolle über die Kommunikation nicht verloren geht.

Krisenteam sofort alarmieren – Jede Sekunde zählt!	IT, PR, Recht und Management müssen unmittelbar zusammenfinden, um das Geschehene zu koordinieren. Alle Mitglieder müssen über einen unbetroffenen Kanal, wie zum Beispiel WhatsApp auf privaten Geräten, erreichbar sein.
Lage erfassen – Fakten statt Panik	Die IT-Abteilung liefert die ersten Informationen. Ab jetzt dürfen nur gesicherte Fakten die Runde machen. Klare Informationen sind entscheidend, um die nächsten Schritte effektiv zu koordinieren.
Wer spricht? Wer handelt?	Verantwortlichkeiten müssen sofort festgelegt werden. Das Krisenteam muss wissen, wer für welche Aufgabe zuständig ist. Koordination ist key. Ab jetzt minütlich Updates an das Krisenteam. Entscheidungen müssen schnell auf Basis der neusten Erkenntnisse getroffen werden. Wer informiert? Wer entscheidet?
Interne Kommunikation	Die Mitarbeiter:innen müssen so schnell wie möglich über die Bedrohung informiert werden. Wichtig: kurz, prägnant und ohne Raum für Gerüchte. Für die interne Kommunikation alternativ Kanäle nutzen, die nicht von dem Angriff betroffen sind.
Externe Kommunikation	Selbst wenn die Öffentlichkeit noch nichts ahnt, müssen Entwürfe für Pressemitteilungen oder Kundenkommunikation bereits in den ersten Minuten bereitstehen. Vorerst gilt: absolute Ruhe nach außen. Sämtliche Abteilungen müssen angewiesen werden, keine externe Kommunikation durchzuführen, bis eine abgestimmte Strategie vorliegt.
Monitoring hochfahren	Überwachung aller Kanäle startet sofort. Social Media, Nachrichtenkanäle, Kundenkontakte... Falschinformationen könnten jede Sekunde auftauchen. Kontrolle über die Informationslage muss beibehalten werden.
Krisenkommunikations-Material griffbereit halten	Templates, FAQs und Krisenpläne müssen umgehend verfügbar sein. Auch eine Krisen-Hotline oder zentrale E-Mail-Adresse für externe Anfragen einrichten.



KOMM. PASSION | TEAM FARNER

Ihr starker Partner

Kommunikation in der Krise

Prävention

Optimierung Ihrer Krisenprozesse

Individuelles Coaching
für Führungskräfte

Intervention

24/7 einsatzbereit

Als Pressesprecher, Sparrings-
partner und Strategieberater

Nachsorge

Analyse bewältigter Krisen

Lessons learned

Jetzt Kontakt aufnehmen

Patrick Hacker
+49(0) 211 600 46-161
patrick.hacker@komm-passion.de