Gefahr einer Cyberkrise wächst – die Bedeutung der Krisenkommunikation auch

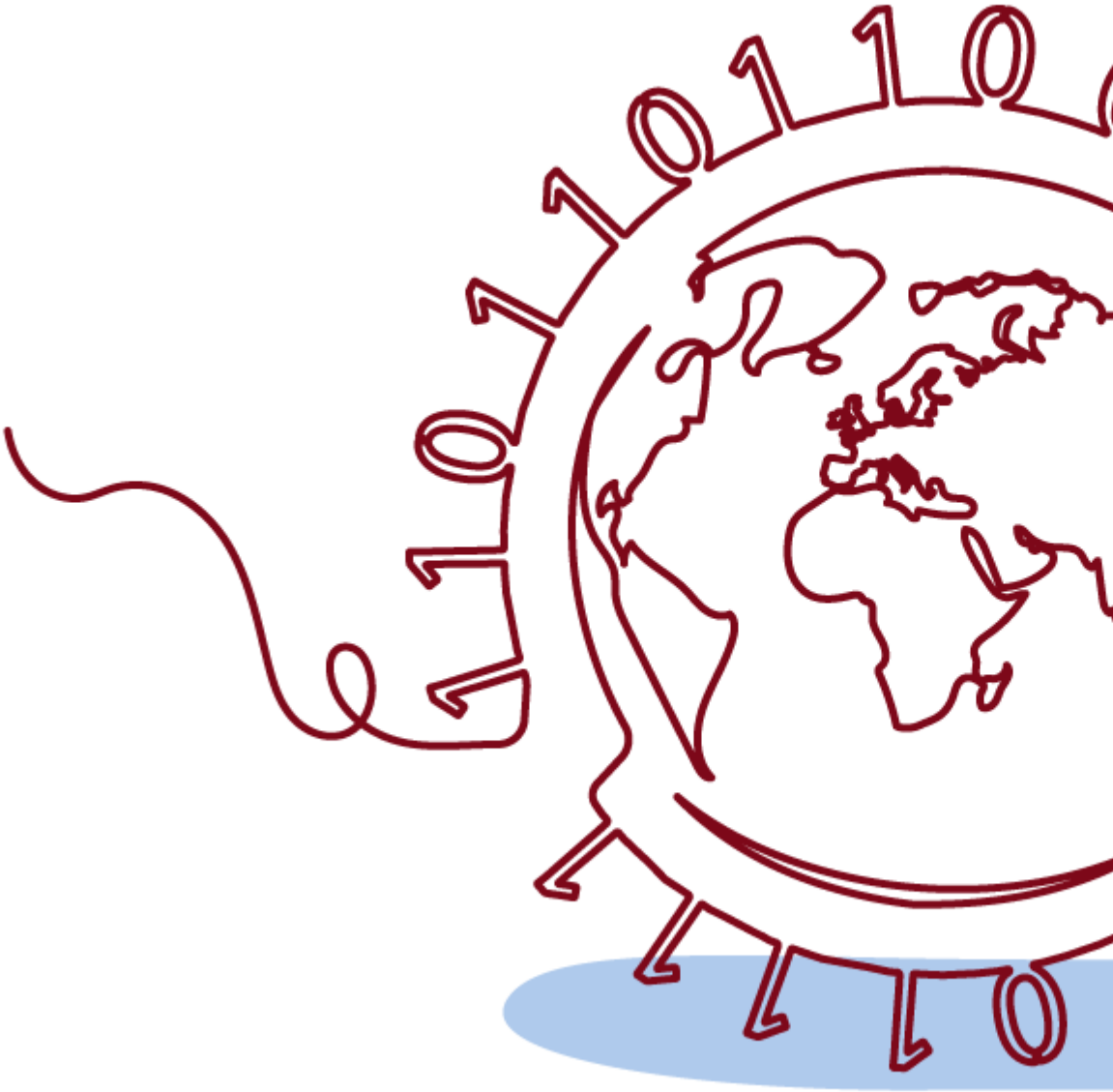
22.01.2021

von

Beller, Tanja

Schlagworte

Corona
Phishing
Cybersicherheit
Cyberattacken
Unternehmen
Künstliche Intelligenz
Sicherheit
Cyberkriminalität



Cyberrisiken zählen mittlerweile zu den größten operationellen Risiken für Unternehmen. In seinem Cybercrime-Lagebericht kommt das Bundeskriminalamt (BKA) 2020 zu dem Ergebnis, dass die Bedeutung von Cybercrime in den nächsten Jahren weiter zunehmen wird und sich die Angriffe vor allem auf Unternehmen und öffentliche Einrichtungen konzentrieren werden. Auch für Banken und deren Infrastrukturen wird mit zunehmenden Cyberangriffen gerechnet. Was bedeutet das für das Krisenmanagement und vor allem für die Krisenkommunikation der Banken?

Corona: Banken im Krisenmodus

Um eine Krise zu bewältigen, ist eine schnelle und transparente Kommunikation mittlerweile genauso wichtig wie die operativ-technischen Maßnahmen. Denn in unserer digitalen Welt verbreiten sich Nachrichten binnen Sekunden in Echtzeit und können selbst wiederum Krisen auslösen oder wie ein Brandbeschleuniger verstärken. Die Banken haben in der der Corona-Zeit gezeigt, dass sie ihrer besonderen Aufgabe und Verantwortung in einer Krisensituation gerecht werden. Es gab keine Beeinträchtigungen des Zahlungsverkehrs, alle Bankgeschäfte konnten weiter reibungslos abgewickelt werden. Die sichere Erreichbarkeit der Bankberater für die Kunden spielte hier eine wesentliche Rolle. Die Kommunikationswege waren stabil – auch bei geschlossenen Filialen und ohne persönliche Kontakte – und für die Kunden bestand kein Grund zur Unruhe oder Sorge.

Dabei war auch hilfreich, dass mit der Kommunikation sehr schnell begonnen wurde und Banken die nächsten geplanten Schritte – beispielsweise Filialschließungen – schnell ankündigt haben. Allzu häufig wird in der Krisenkommunikation – aus der Not geboren – sehr aus einer Abwehrhaltung heraus agiert. Gibt man aber schnell und transparent Informationen bekannt, die in aller Regel sowieso schnell an die Öffentlichkeit gelangen, kann dies nicht nur zu einem Zeit-, sondern auch zu einem Glaubwürdigkeits- und Vertrauensgewinn führen.

Bei Krisenkommunikation zählt jede Minute – wenn nicht gar Sekunde

Bei einer Cyberkrise kann als Worst-Case-Szenario hinzukommen, dass gerade die Kommunikationswege unterbrochen sind, die im „Normalbetrieb“ genutzt werden. Umso wichtiger ist es, gut vorbereitet zu sein und Alternativen in der Hinterhand zu haben, die schnell genutzt werden können. Auch für kleinere Unternehmen und Organisationen ist es also ratsam, sich vor einer Cyberkrise nicht nur mit den technischen Maßnahmen, sondern zugleich mit kommunikativen Fragen zu befassen. Denn im digitalen Zeitalter gibt es quasi keine Zeit zur Vorbereitung: Kommunikation in Echtzeit wird gefordert, auch weil sie machbar ist – ist die Website blockiert und offline, müssen andere Kanäle genutzt werden. Über Soziale Medien verbreiten sich Cybervorfälle wie ein Lauffeuer in den entsprechenden Communities. Zugleich kann über diese Kanäle (Twitter, Facebook, Instagram, Messenger-Dienste) jederzeit reagiert werden.

Bei den Vorbereitungen jeder Krisenkommunikation geht es zunächst um viele organisatorische Fragen: Jede Krise beginnt mit einem Vorfall, der schon eingetreten ist oder sich unabwendbar ankündigt. Ein Krisenstab bestimmt, koordiniert und überwacht die Ausführung aller Maßnahmen zur Bewältigung der Krise und ihrer Auswirkungen bzw. zur Wiederherstellung des Normalzustandes. Doch schon für diese erste

Maßnahme – das Einberufen eines Krisenstabs oder -teams – sind Vorüberlegungen notwendig. Denn wer meldet den Vorfall an wen? Wer muss Teil des Krisenstabs sein, wer ruft ihn zusammen? Sofern es bereits vorbereitete und im besten Fall vorgetestete Strukturen gibt, spart dies wertvolle Zeit.

Es muss beim ersten Zusammenkommen des Krisenstabs oder -teams nach Meldung einer Krise entschieden werden, wer die Leitung übernimmt. Wichtig für eine erfolgreiche Krisenarbeit ist, dass das Krisenteam beschlussfähig ist und keine weiteren Abstimmungen notwendig sind. Zudem ist eine Person zu bestimmen, die die Koordination für die Medienarbeit übernimmt bzw. die nach außen spricht. Je nach Ausmaß der Krise kann dies auch ein Team sein. Bei einem weitreichenden Systemausfall müsste gegebenenfalls externe Unterstützung in Anspruch genommen werden.

Das Bundesministerium des Innern bietet in seinem „Leitfaden der Krisenkommunikation“ eine mehrseitige Checkliste zur konzeptionellen, organisatorischen, personellen und technischen Vorbereitung an, die einen guten Überblick über die relevanten Fragen gibt:

- Wer gehört zum Krisenstab?
- Wer alarmiert den Krisenstab, wie wird alarmiert? Wen benachrichtigt man zuerst, in welcher Reihenfolge die weiteren Ansprechpartner?
- Sind Meldeprozesse und Kontakte den Mitarbeitern bekannt?
- Wer ist zuständig für die Aktualisierung der Kontaktliste „Krisenstab“?
- Gibt es eine Kontaktliste für Meldungen zu relevanten Behörden?
- Wurde das Notfallmanagement bereits getestet?
- Ist der Zugriff auf wichtige Materialien auch bei Ausfall der Technik sichergestellt?
- Gibt es eine vorbereitete Darksite, wer pflegt diese?
- Wer führt das Krisenteam, wer spricht nach außen?
- Gibt es allgemeine Sprachregelungen, Argumentarien, Kernbotschaften, FAQs für unterschiedliche Szenarien?
- Wer ist verantwortlich für Aktualisierungen?

Netzwerke für Cybersicherheit sind entscheidend

Die Zeiten, in denen allein die IT-Kompetenz einzelner Experten oder eines IT-Bereichs ausreicht, um für die Sicherheit der Systeme zu sorgen, sind längst vorbei. Cyberkriminelle nutzen die enorm gewachsenen technischen Möglichkeiten (beispielsweise der künstlichen Intelligenz) und arbeiten teilweise wie gut organisierte globale Wirtschaftsunternehmen zusammen. Netzwerke, die zeitnah, über Unternehmen und

Wirtschaftssektoren hinweg Informationen über aktuelle Cyberangriffe austauschen, sind wiederum selbst ein wesentliches Instrument zur Abwehr und zum Eindämmen von Cyberangriffen geworden. So ist der Austausch über ausgewertete Vorfälle für Banken längst Teil der Sicherheitsstrategie. Beispielsweise hilft der Informationsaustausch über kursierende Schadsoftware dabei, diese durch Systemanalysen zu identifizieren und schon abzuwehren, bevor sie aktiv werden können.

Es gibt bereits eine Reihe von Plattformen, die Informationen zu aktuellen Angriffen, neuer Schadsoftware und laufenden Phishing-Kampagnen zusammenführen. In Deutschland hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) einige Initiativen und Aktivitäten für die Informationssicherheit im Cyberraum gestartet. Hierzu zählen:

Allianz für Cybersicherheit

Laut BSI das größte Cybersicherheitsnetzwerk Deutschlands. Es wurde 2012 gegründet mit dem Ziel, die Widerstandsfähigkeit Deutschlands gegenüber Cyberangriffen zu stärken. Es bietet Wirtschaft, Behörden, Forschung, Wissenschaft sowie anderen Institutionen eine Plattform. Auch der Bankenverband ist seit 2018 Multiplikator des Netzwerks.

IT-Lagezentrum

Das Nationale IT-Lagezentrum soll laut BSI jederzeit über ein verlässliches Bild der aktuellen IT-Sicherheitslage in Deutschland verfügen und bei Sicherheitsvorfällen schnell und kompetent den Handlungsbedarf einschätzen können. Das IT-Lagezentrum arbeitet mit dem Cyber-Abwehrzentrum zusammen.

IT-Krisenreaktionszentrum

Das IT-Krisenreaktionszentrum soll eine schnelle Reaktion auf schwere IT-Sicherheitsvorfälle sicherstellen und rechtzeitige Gegenmaßnahmen ermöglichen sowie Schäden größeren Ausmaßes vermeiden.

Nationales Cyber-Abwehrzentrum (Cyber-AZ)

Das Cyber-Abwehrzentrum dient als zentrale Kooperationsplattform dem Informationsaustausch zwischen allen sicherheitsverantwortlichen Behörden dienen und soll dadurch für eine effektive Gefahrenabwehr und wirksame Prävention sorgen.

Single Point of Contact (SPOC)

Über SPOCs (Single Points of Contact) als Meldestellen und Bindeglied sind Unternehmen, insbesondere Betreiber kriti-

scher Infrastrukturen, mit dem BSI-Lagezentrum verbunden. Hierdurch soll eine schnelle, unverfälschte und zuverlässige Weiterleitung von Informationen und die Alarmierung der Unternehmen der eigenen Branche bzw. des BSI-Lagezentrums gewährleistet werden. Dies ist für die Früherkennung und Bewältigung von IT-Krisen unerlässlich.

Auch in der Privatwirtschaft gibt es Gruppen, die sich zum Schutz gegen Cybercrime zusammengeschlossen haben, wie beispielsweise das G4C German Competence Centre against Cyber Crime. Der Verein G4C hat das Ziel, für seine Mitglieder Frühwarnsystem und Informationsplattform zu sein. Kooperationen mit dem Bundesamt für Sicherheit in der Informationstechnik und dem Bundeskriminalamt sollen die Prävention und auch Strafverfolgung von Cyberkriminalität durch einen engen Informationsaustausch unterstützen.

Cyberangriffe können von überall auf der Welt aus gestartet werden. Deshalb gibt es internationale Initiativen wie das Financial Services Information Sharing and Analysis Center (FS-ISAC), das sich als globale Plattform und Netzwerk zur Früherkennung und zur Abwehr von Cyberangriffen speziell auf Finanzdienstleistungen gegründet hat.

Zur Bündelung der Kräfte ist eine internationale Zusammenarbeit gegen organisierte Cyberkriminalität erforderlich. Das von Europol eingerichtete European Cybercrime Center - EC3 soll die Strafverfolgungsbehörden im Kampf gegen Cybercrime in der EU stärken und so dazu beizutragen, europäische Bürger, Unternehmen und Regierungen vor Online-Kriminalität zu schützen.

Dreh- und Angelpunkt von Cybersicherheit bleibt der Mensch

In gleicher Weise, wie uns die Digitalisierung bei der Corona-Pandemie in allen Lebens- und Wirtschaftsbereichen stützt, hat sie neue Abhängigkeiten und Angriffsflächen geschaffen. Das verstärkte Remote-Arbeiten – im Homeoffice oder von unterwegs – wird auch nach der Pandemie bleiben. Dass dies technisch machbar ist, zeigen die Erfahrungen aus der Krise. Die Herausforderung für die IT-Sicherheitsexperten bleibt vor allem der einzelne Mitarbeiter, der einzelne Mensch. Mit beständig weiter ausgefeilten Methoden und Techniken gelingt es immer wieder, den Menschen zu manipulieren, so dass er in Fallen tappt und damit Cyberkriminellen die notwendige Lücke für Angriffe eröffnet. Deshalb bleibt es eine Daueraufgabe auch für die Banken, über die Gefahren von Cybercrime zu informieren und zu sensibilisieren.