Cyberattacken erfolgreich begegnen

Worauf es im modernen Krisenmanagement ankommt

Die Digitalisierung hat die Angriffsfläche für Cyberattacken erheblich vergrößert. Eine vorausschauende Planung und proaktives Krisenmanagement sind nötig, um im Notfall die Kontrolle wieder zu erlangen. Vorrausetzung ist eine Kommunikations- und Krisenmanagementplattform, die unabhängig von der eigenen IT zuverlässig und ausfallsicher funktioniert.

Ob Ransomware- oder DDoS-Angriffe – Cyberkriminalität ist in aller Munde und bedroht geschäftliche Existenzen: Laut einer Studie des Digitalverbands Bitkom hat sich der Anteil an Unternehmen, die innerhalb eines Jahres mindestens einmal Opfer einer Cyberattacke geworden sind, zwischen 2017 und 2021 von 53 % auf 88 % erhöht – nahezu 9 von 10 Unternehmen aller Branchen und Größen sind somit direkt betroffen [1]. Damit stehen Cybervorfälle weltweit schon heute auf Platz eins der Top-Risiken für Unternehmen (Allianz Risk Barometer 2022 [2]) und verursachten laut aktuellen Zahlen des BCI Emergency and Crisis Communications Report 2022 32 % der Aktivierungen von Notfallplänen im vergangenen Jahr [3].

Die Zahlen verdeutlichen: Bei allen Potenzialen, die die Digitalisierung für Unternehmen bereithält, bietet sie auch eine neue Angriffsfläche für Cyberattacken. Damit Unternehmen im Ernstfall schnell die Kontrolle über die Situation zurückzuerlangen und Schaden minimieren können, sind eine vorausschauende Planung und proaktives Krisenmanagement essenziell.

*/ Die Maßnahmen der ersten Minuten und vor allem der ersten Stunde – in der Branche auch »golden hour« genannt – bestimmen Ausgang und Kosten einer Krise maßgeblich.

Die 4 Kernbereiche des Krisenmanagements:

1. Früherkennung und Prävention

Menschliche Fehler stellen zumeist die größte Schwachstelle in der IT-Sicherheit dar, beispielsweise durch das arglose Öffnen infizierter E-Mail-Anhänge. Spezielle Sicherheitssoftware und Antivirenprogramme können zwar einen Teil davon erkennen und eliminieren, stoßen allerdings spätestens bei einem gezielten Angriff auf Unternehmen oder einzelne Mitarbeitende an ihre Grenzen. Um Gefahren frühzeitig zu begegnen und unterbinden zu können, müssen Risikofaktoren daher fortlaufend analysiert und Mitarbeitende entsprechend geschult werden. Entscheidend sind zudem die sorgfältige Erstellung und Aufrechterhaltung von Business-Continuity-Plänen sowie der Aufbau qualifizierter Personalressourcen, etwa durch spezialisierte Response-Teams.

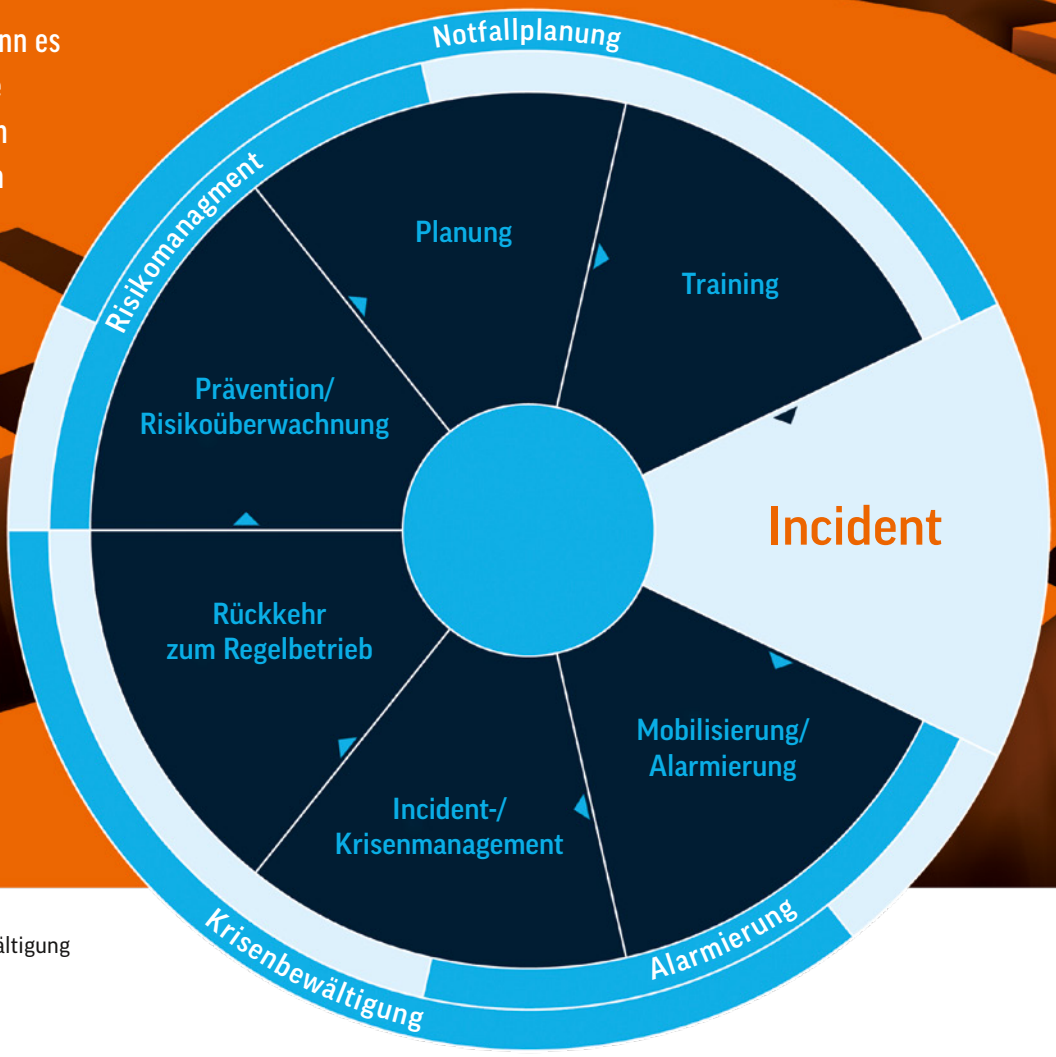
2. Schnelles Handeln

Die Maßnahmen der ersten Minuten und vor allem der ersten Stunde – in der Branche auch »golden hour« genannt – bestimmen Ausgang und Kosten einer Krise maßgeblich. Grundvoraussetzung für schnelles Handeln ist dabei eine schnelle, gezielte Kommunikation und Zusammenarbeit über Standort- und Bereichsgrenzen hinweg. Mit dem manuellen Abtelefonieren einer Liste aller zu alarmierenden Personen ist das nicht zu schaffen. Auch E-Mail-Kommunikation stellt im Krisenfall zumeist keine zuverlässige Option dar, schließlich beeinträchtigen Cyberattacken häufig auch die internen E-Mail-Server beziehungsweise sollten diese zum Schutz vor weiteren Schäden vorerst außer Betrieb genommen werden. Nahezu ausfallsichere Krisenkommunikation lässt sich daher nur durch eine extern gehostete Software-as-a-Service-Lösung (SaaS) sicherstellen, die vollkommen unabhängig vom eigenen IT-System funktioniert. Immer mehr Unternehmen und Organisationen setzten laut BCI auf professionelle SaaS-Lösungen [4]. Sie ermöglichen Unternehmen in nahezu 80 % der Fälle innerhalb der »golden hour« auf die Krise zu reagieren und ihren Notfallkommunikationsplan ausfallsicher umzusetzen.

3. Etablierung fester Prozesse und verlässlicher Kommunikationswege

Im Krisenfall kommt es darauf an, dass jeder weiß, was zu tun, wer wofür zuständig und wer wie erreichbar ist. Die klare Definition von Verantwortlichkeiten spart Zeit und hilft zudem die Reputation des Unternehmens zu schützen. Denn mindestens ebenso wichtig wie die Wiederherstellung der Hoheit über das eigene IT-System ist es, durch gutes Handling der Situation Vertrauen von Kunden, Geschäftspartnern und Behörden sowie die Geschäftsfähigkeit des Unternehmens zu bewahren. Schließlich sind fast 40 % der Gesamtkosten eines Cybervorfalls auf den Ausfall der Geschäftsfähigkeit zurückzuführen (Cost of a Data Breach Report 2021 [5]). Unternehmen, die für die Notfallkommunikation ausschließlich allgemeine (Enterprise) Messenger wie etwa Teams nutzen, müssen sich mit einem deutlich limitierten Funktionsumfang für die Notfallkommunikation arrangieren und riskieren im Krisenfall einen Totalausfall der internen Kommunikationswege. Im BCI Report äußern sich auch daher fast viermal so viele Nutzer von Enterprise Messengern unzufrieden mit der Anwendung im Notfallszenario, als dies bei Nutzern dedizierter Messaging Apps der Fall ist [6]. Auch vor diesem Hintergrund sind extern gehostete SaaS-Lösungen für das Krisenmanagement eine gute Wahl, da sie auch im Ernstfall zuverlässig und unabhängig von den eingesetzten Endgeräten kommunizieren und alarmieren können.

*/ Vor Cyberangriffen kann es nie eine hundertprozentige Absicherung geben. Wer im Ernstfall nicht vollkommen die Kontrolle über die eigenen Prozesse verlieren möchte, muss sich daher vorbereiten.



Kreislauf zur Prävention und Bewältigung von Krisensituationen.

4. Revisionssicher dokumentieren und nachbereiten

Cybervorfälle sind immer sensible Situationen, die besondere Anforderungen an Datenschutz und Sicherheit der internen Kommunikation stellen. Trotzdem nutzen mehr als ein Drittel der im BCI Report befragten Unternehmen noch keine dezidierten Tools und Software für die Notfallkommunikation beziehungsweise das Krisenmanagement. Professionelle SaaS-Lösungen helfen bei der revisionssicheren Dokumentation aller Geschehnisse – und das komplett automatisiert. Das ist entscheidend, um aus den Geschehnissen zu lernen oder bei Untersuchungen von Behörden und Versicherungen belastbare Nachweise liefern zu können.

Fazit. Nicht zuletzt die Sicherheitslücke Log4Shell machte im Dezember 2021 erneut deutlich: Vor Cyberangriffen kann es nie eine hundertprozentige Absicherung geben. Wer im Ernstfall nicht vollkommen die Kontrolle über die eigenen Prozesse verlieren möchte, muss sich daher vorbereiten. Dazu gehört eine Kommunikations- und Krisenmanagementplattform, die unabhängig von der eigenen IT zuverlässig und ausfallsicher funktioniert. Professionelle SaaS-Lösungen setzen hier an. Sie unterliegen deutlich höheren Sicherheitsvorkehrungen als andere Tools und garantieren dank mehrfacher Redundanz, dass Unternehmen auch im Ernstfall handlungsfähig bleiben. Durch automatisiertes Notfallmanagement können weltweit die Abläufe in Krisensituationen passgenau optimiert und fortlaufend überwacht und gesteuert werden. Dies ermöglicht, Zeit und Kosten zu sparen sowie existenzbedrohende Schäden in der Regel abzuwehren.

Eske Ofner,
Head of Sales
bei F24 AG

[1] https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr

[2] https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2022-press-de.html

[3] [4] [6] https://fact24.com/de/bci-emergency-crisis-communications-reports/

[5] https://www.ibm.com/de-de/security/data-breach