Krisenmanagement und organisationale Resilienz

Das Schutzschild vor, während und nach der Krise

Mit der Coronapandemie hat sich die Krisenthematik einen Platz in unserem Alltag erobert. Zwischenzeitlich ist die latente Bedrohung durch Cyberattacken für viele Organisationen allgegenwärtig, und die wirtschaftlichen Folgen von Krisen sind meist kaum vorhersehbar. Den eigenen Krisenmuskel zu trainieren und die individuelle und organisationale Resilienz zu stärken, ist daher ein Gebot der Stunde.

Von Anja Zimmermann, Aldo C. Schellenberg und Guy Lachappelle

Nichts geht mehr, alle Bildschirme schwarz, Kommunikationskanäle offline, Kund*innen können nicht mehr bedient, Transaktionen nicht abgewickelt, Rechnungen und Lohnzahlungen nicht mehr ausgelöst werden – das System steht still. Das «PhantomLock» verschlüsselt sämtliche Datenbanken, E-Mail-Server und Back-up-Systeme, die Kundendaten enthalten. Die Hacker drohen mit Datenexfiltration ins Dark Web, sollte das Lösegeld nicht gezahlt werden.

Cyberattacken – wenn die Existenz bedroht ist

So, oder so ähnlich, könnte eine Cyberattacke Gestalt annehmen. Trifft diese auf eine unvorbereitete Organisation, ist deren Existenz bedroht. Die Auswirkungen einer solchen Krise auf persönlicher, unternehmerischer und gesamtwirtschaftlicher Ebene sind kaum vorhersehbar, das skizzierte Szenario zum Glück (noch) nicht alltäglich. Jedoch steigt die Zahl der Cyberangriffe in der DACH-Region stetig. In der Schweiz wurden dem Nationalen Zentrum für Cybersicherheit (NCSC) allein zwischen 19. und 24. August 801 Cybercrime-Vorfälle gemeldet (Quelle: statista): Schadenmeldungen von der Bevölkerung oder von KMU, aber auch Cybervorfälle, die frühzeitig erkannt wurden und keinen Schaden anrichteten. Die latente Bedrohung ist eine Tatsache; die Notwendigkeit, sich auf Krisen – ausgelöst durch Cyberattacken – vorzubereiten, gegeben.

Krisen kommen meist überraschend, erfordern rasches Handeln unter hohem Zeit- und Problemdruck. Dabei hat jede Krise eigene Herausforderungen. Gerade Cyberangriffe stellen enorme Anforderungen an die Organisation und die installierten Krisenstäbe. Sie lösen oft multiple Problemherde aus, die ein Krisenteam nicht nur hinsichtlich der IT und der Wiederherstellung der Systeme und der Sicherung sensibler Daten fordern. Cyberattacken betreffen im schlimmsten Fall sämtliche Geschäftsprozesse. Insbesondere bei digitalen Geschäftsmodellen oder im Fall sehr sensibler Kundendaten können finanzielle und rechtliche Konsequenzen existenzgefährdend sein. Der drohende Reputations- und Vertrauensverlust stellt die Krisenkommunikation vor grosse Herausforderungen. Im Unternehmen wird die Krise sofort spürbar für nahezu jeden Mitarbeitenden, Ängste und Ohnmachtsgefühle machen sich breit. Hier sind schnelle und stabilisierende Botschaften in der internen Kommunikation gefragt.

In der Schweiz wurden dem Nationalen Zentrum für Cybersicherheit (NCSC) allein zwischen 19. und 24. August 801 Cybercrime-Vorfälle gemeldet. (Quelle: statista)

Fragen, die vor der Krise geklärt sein müssen

Krise kann und muss man üben. Vor allem grössere, systemrelevante und regulierte Organisationen, Behörden oder Betreiber kritischer Infrastrukturen verfügen über Krisenstäbe, Handbücher, Checklisten und Prozessbeschriebe für den Ernstfall. KMU verfügen meist nicht über Ressourcen für solch ausgeklügelte Konzepte. Trotzdem müssen auch sie sich mit der Prävention, Bewältigung und dem Lernen aus Krisen beschäftigen. Grundlage der Krisenprävention ist ein realistisches Risiko- und Business Continuity Management sowie ein präventives betriebliches Gesundheitsmanagement. In vielen der vorgenannten Organisationen liegen solche Konzepte dokumentiert, teils sogar zertifiziert oder geprüft vor und schaffen die Voraussetzungen für organisationale Resilienz. Aber auch KMU müssen sich kritische Fragen stellen und Antworten darauf finden: Welche Ereignisse können Kernprozesse des

Unternehmens gefährden, wie reduzieren wir Eintrittswahrscheinlichkeiten sowie das Ausmass des eintretenden Schadens?

Den Krisenmuskel kann man trainieren

Krisenprävention allein genügt nicht: Eine Organisation muss in der Lage sein, adäquat und zeitgerecht zu reagieren. Die Erfahrungswerte sind hier eindeutig: Wer sich systematisch und anhand von Szenarien regelmässig in Trainings und Simulationen auf den Krisenmodus vorbereitet, ist in der Krisenbewältigung erfolgreicher: Führungsstrukturen sind dann bekannt, Führungsprozesse in der Krise trainiert, die Zusammenarbeit im Krisenführungsteam unter Zeit- und Handlungsdruck eingespielt. Damit kann sich das Führungsteam rasch auf die Problemlösung konzentrieren und verliert weder Zeit noch Energie in einer überlangen Chaosphase. Im Fall einer Cyberattacke sollte dazu vorgängig geklärt sein, wer zum Krisenteam gehört, welche Kompetenzen das Team hat, wer über eine Lösegeldforderung entscheidet und welche Rollen weitere Stakeholder, beispielsweise ein Regulator oder die Schadenversicherung, beanspruchen. Trainings und Simulationen sind deshalb das A & O.

Auf die organisationale und die individuelle Resilienz in der Krise kommt es an

Dabei gilt es auch, die individuellen Stresssituationen, die Krisen auslösen, zu beachten. Die im Krisenstab involvierten Personen sind sich zwar aus dem Berufsalltag bekannt. Weniger bekannt ist, wie diese in besonders belastenden Situationen reagieren und wie «stressfest» sie sind. Werden, wie im Fall einer Cyberkrise, allfällige Experten temporär als Taskforce in die Arbeit der Krisenstäbe eingebunden, ist das Zusammenspiel der Personen unter hohem Druck essenziell, vorher häufig aber nicht überprüft worden.

Trainings und Simulationen generieren Selbstwirksamkeitserfahrung und bauen Sicherheit auf. Sie steigern die individuelle Resilienz und sensibilisieren für eigene Grenzen. Verhaltens- und Reaktionsmuster der Teammitglieder zu kennen, schafft zusätzliche Sicherheit. Persönliche Belastungsgrenzen oder «Kipppunkte» zu erfahren, darf dabei kein Grund für Scham sein. Im Gegenteil: Grenzen zu kennen und damit im Krisenstab umzugehen, ist für die individuelle und organisationale Resilienz gleichermassen nachhaltig. Dennoch: Auch die erfahrensten Krisenmanager können in einer Krise ans Limit kommen. Nach Trainings und Assessments von der eigenen Stressfestigkeit überzeugt zu sein und die Grenzen zu kennen, ist eine gute Voraussetzung, die nächste Krise erfolgreich zu bewältigen. Die Persönlichkeit bestimmt mit, wie Individuen in Phasen von Disstress Copingstrategien entwickeln, um widerstandsfähig und handlungsfähig zu bleiben. Krisensimulationen sollten daher unbedingt auch emotionale, körperliche sowie mentale Stressreaktionen im Blick haben und durch externe Assessoren begleitet werden. Gerade Führungskräfte sind in der Krise gefordert, denn sie müssen Verhalten unter hoher Anspannung bei ihren Mitarbeitenden wahrnehmen, bei Bedarf intervenieren und gleichzeitig eine individuelle Stressregulation realisieren.

Krisenszenarien bedrohen unseren Alltag bereits heute, und sie werden es weiterhin tun. Sie lassen sich kaum vorhersagen, die Bedrohung und damit verbundene Ängste werden bleiben. Was sich aber klar vorhersagen lässt: Wer der Krise vorbereitet begegnet, auf ein eingespieltes Team sowie vertraute Prozesse und Abläufe bauen kann, der kann die Krise meistern, gestärkt aus ihr hervorgehen und damit einen wesentlichen Beitrag zur unternehmerischen Nachhaltigkeit leisten.

Anja Zimmermann, Aldo C. Schellenberg und **Guy Lachappelle** engagieren sich gemeinsam mit Kai Kruthoff im Themenfeld Krisenmanagement und Organisationale Resilienz an der Hochschule Luzern – Wirtschaft. Sie trainieren im Rahmen des CAS Krisenmanagement und Organisationale Resilienz und im Austausch mit erfahrenen Krisenmanager*innen in Echtzeit-Krisensimulationen die Führung eines Krisenstabs in Grossunternehmen, KMU und öffentlichen Verwaltungen.