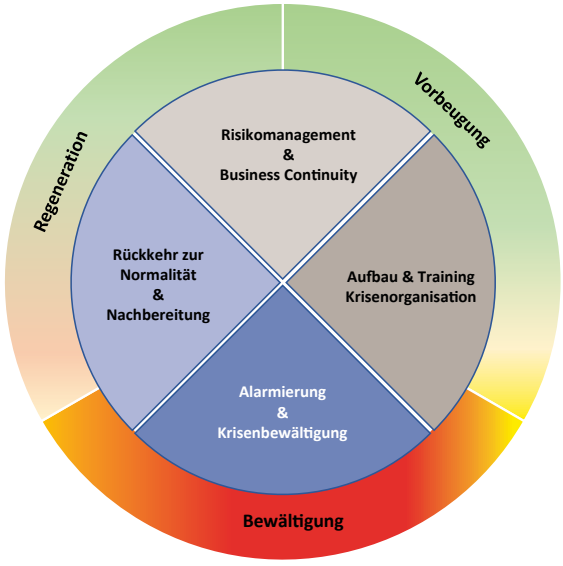
Vorbereitet in die Krise – gestärkt daraus hervor

Und plötzlich erscheint eine Lösegeldforderung auf dem Bildschirm: Wie Krisen wie ein Cyberangriff dank guter Vorbereitung gemeistert werden und wie man widerstandsfähiger daraus hervorgeht, erläutern hier vier Expert/-innen für Krisenmanagement und organisationale Resilienz.

ALDO C. SCHELLENBERG, GUY LACHAPPELLE, ANJA ZIMMERMANN UND KAI KRUTHOFF

Der Cyberangriff auf einen mittelgrossen Bürobedarfshändler kommt aus dem Nichts. Eines Abends stellt der Geschäftsführer fest, dass der Zugang zum Intranet blockiert ist. Ein Hacker hat sämtliche Serverzugänge gesperrt und die Daten verschlüsselt. Für die Freischaltung verlangt er Geld. Am nächsten Tag geht im Unternehmen nichts mehr: Die Filialen können weder geöffnet noch telefonisch oder via E-Mail erreicht werden. Die Logistikkette ist durchtrennt, die Bestellungen können nicht bearbeitet werden. Kurz: Die Existenz des Unternehmens steht auf dem Spiel.



Krisenmanagement und Resilienz.
EIGENE DARSTELLUNG




Autor/-innen

Aldo C. Schellenberg, Guy Lachappelle, Anja Zimmermann und Kai Kruthoff (von oben nach unten) engagieren sich gemeinsam im CAS Krisenmanagement und Organisationale Resilienz an der Hochschule Luzern – Wirtschaft. In dieser Weiterbildung trainieren die Teilnehmenden im Austausch mit erfahrenen Krisenmanager/-innen und in Echtzeit-Krisensimulationen die Führung eines Krisenstabs in Grossunternehmen, KMUs und öffentlichen Verwaltungen.

> *www.hslu.ch/krisenmanagement*

Die Widerstandskraft steigern

Was wie ein Albtraum daherkommt, ist heutzutage bittere Realität. In der Schweiz wurden dem Nationalen Zentrum für Cybersicherheit (NCSC) allein in der Woche zwischen dem 28. August und dem 3. September 2023 insgesamt 1163 Cybercrime-Vorfälle gemeldet.

Cyberangriffe lassen sich trotz grosser Anstrengungen oft nicht verhindern. Umso wichtiger ist es, eine unternehmerische Resilienz gegenüber Cyberattacken aufzubauen, also die Fähigkeit, Angriffe ohne nachhaltige Beeinträchtigungen zu überstehen. Eine gute Strategie gegen Cyberangriffe beginnt deshalb lange vor dem eigentlichen Ereignis. «Der grösste Fehler im Notfall- und Krisenmanagement ist, nicht vorbereitet zu sein», sagt Daniel Schlup, Leiter Notfall- und Krisenmanagement bei den SBB und damit in der Fachführungsverantwortung für die Einsatzbereitschaft der Notfallstäbe und Center of Competence sowie des Krisenstabs der SBB. Was für ein Unternehmen wie die SBB gilt, gilt auch für KMU und andere Organisationen.

Vorbereitung ist die halbe Miete

Im Rahmen des Risiko- und Business-Continuity-Managements geht es darum, die Auswirkungen möglicher Krisenauslöser wie z.B. Cyberattacken auf das Unternehmen abzuwägen und vorsorgliche Massnahmen zu ergreifen, die entweder die Eintretenswahrscheinlichkeit oder das Ausmass eines Angriffs auf ein akzeptables Mass reduzieren.

«Erledigt ein Unternehmen die Nachbearbeitung seriös, geht es gestärkt aus der Krise hervor.»

Als Erstes sollte man sich überlegen, welches die gefährlichsten Cyberszenarien für das Unternehmen sind. Welche Systeme wären dabei wie betroffen und was wären die Folgen? Darauf aufbauend gilt es, sich Gedanken zur Prävention zu machen: Welche IT-Kompetenzen zum Aufbau und Erhalt eines wirksamen Cyberschutzes sollen unternehmensintern entwickelt, welche Kompetenzen durch externe Fachpersonen abgedeckt werden? Inwiefern möchte man den Cyberschutz durch Dritte testen lassen (z.B. mit Penetrationstests)? Wie ist die Back-up-Strategie definiert? Welche Redundanzen bestehen? Das Management sollte zudem seine Erwartungen

Wenn Hacker sämtliche Serverzugänge sperren und die Daten verschlüsseln, kann dies die Existenz von Unternehmen bedrohen.

zur Aufrechterhaltung des Geschäftsbetriebs in der Krise formulieren. Stichworte sind: Degradationsfähigkeit, minimal service/minimal performance, Notbetrieb. Es benennt zudem die Desaster-Recovery-Prioritäten im Ereignisfall.

Training für den «Krisenmuskel»

Essenziell ist die frühzeitige Einsetzung eines Krisenteams. Ist die Krise da, ist es zu spät, sich Gedanken über dessen Zusammensetzung, Aufgaben und Kompetenzen zu machen. Es sollte so aufgestellt sein, dass die Mitglieder auch unter hoher Belastung effizient zusammenarbeiten. Anhand von realistischen Szenarien trainiert es regelmässig den Ernstfall. So lernen die Mitglieder sich und ihre Rollen gegenseitig kennen. Zudem sollte ein permanent zugänglicher Krisenführungsraum mit Kommunikationsmöglichkeiten, die auch im Fall eines Cyberangriffs funktionieren, eingerichtet werden.

Krisen muss man erleben, um an ihnen zu wachsen. Wer in Simulationen die Krisendynamik spürt, Grenzerfahrungen macht und die eigene sowie die organisationale Resilienz überprüft, bereitet sich nachhaltig auf den Ernstfall vor. Die Erkenntnisse aus den Trainings werden in einem Handbuch dokumentiert.

Gelerntes anwenden, flexibel bleiben

Keine Krise läuft exakt so ab, wie sie geübt wurde. Die Zusammensetzung der Task-Force muss ereignisbezogen überprüft und allenfalls angepasst werden. Gerade Cyberattacken stellen höchste Anforderungen an das Krisenteam, denn es sind multiple Krisen: Praktisch alle Geschäftsprozesse sind betroffen und die finanziellen, personellen, rechtlichen und reputationsmässigen Folgen haben unter Umständen schicksalshafte Dimensionen. Das Krisenteam muss all diese Risiken gleichzeitig bearbeiten. Für die Schadensbegrenzung ist es entscheidend, dass es seine Arbeit schnellstmöglich aufnimmt. Hat es optimale Vorgaben bezüglich Recovery-Prioritäten, kann es seine Arbeit fokussieren.

Von enormer Bedeutung ist die Krisenkommunikation. Im Ereignisfall treten Mitarbeitende, Kundinnen und Kunden, Behörden, Medien und die Öffentlichkeit gleichzeitig mit Anliegen an das Unternehmen heran. Die interne Kommunikation hat Vorrang vor der Kommunikation gegen aussen. Lange vor dem Ereignis muss festgelegt werden, wer die interne Kommunikation verantwortet und über welche Kanäle sie laufen soll, vor allem für den Fall, dass die üblichen Unternehmenskanäle nicht mehr genutzt werden können.

Nach der Krise ist vor der Krise

Um organisationales Lernen zu ermöglichen und die Resilienz des Unternehmens zu erhöhen, muss die Krise sorgfältig nachbearbeitet werden. Die daraus gezogenen Lehren werden systematisch in die Verbesserung des IT-Schutzes, in die internen Prozesse, Dokumentationen, Übungen und in die Unternehmensführung eingebunden. Erledigt ein Unternehmen die Nachbearbeitung seriös, geht es gestärkt aus der Krise hervor. Denn: Vor der Krise ist nach der Krise. Krisen lassen sich nicht vorhersagen – ihnen vorbereitet zu begegnen und sie selbstwirksam zu managen, ist für Organisationen und ihre Führungskräfte aber lernbar.