Überwältigt von der Krise: Auswirkungen von Cyberkrisen auf den Menschen

Cyberkrisen wie eine Ransomwareattacke sind nicht nur eine technische und organisatorische Herausforderung, sondern auch eine besondere Belastung für die Mitarbeitenden. Sich dieser Belastung bewusst zu werden und gegenzusteuern hilft, die Krise schnell und gut zu bewältigen.

Von Sebastian Pöhlchen und Malko Steinorth

„Jede Krise ist einzigartig" ist eine geläufige Weisheit im Krisenmanagement. Dennoch ergeben sich aus den Cyberkrisen, die ich miterlebt habe, vier Gemeinsamkeiten: Ein Ransomwareangriff konnte nicht verhindert werden; die Wiederherstellung des Business war nicht zu den definierten Zeiten möglich; die Notfallpläne waren nur teilweise oder gar nicht anwendbar; der Faktor Mensch wurde zu wenig berücksichtigt.

Wenn ein Ransomwareangriff nahezu alle IT-Systeme verschlüsselt hat, muss sich das betroffene Unternehmen auf einen Marathon einstellen. Eine Rückkehr zur Normalität kann Wochen oder Monate dauern. Damit sind Cyberkrisen nicht nur eine Bedrohung für die technische Infrastruktur, sondern auch eine Belastung für das menschliche Wohlbefinden.

Mit Auswirkungen im Kontext Krise assoziieren die meisten Menschen in erster Linie finanzielle und Reputationsschäden. Im Vordergrund steht meist eine schnellstmögliche Bewältigung der Krise, die negativen Auswirkungen auf Menschen werden den technischen und wirtschaftlichen Auswirkungen nachgeordnet. Dieser Artikel konzentriert sich auf die negativen Auswirkungen von Cyberkrisen auf Menschen und beleuchtet die psychologischen, sozialen und emotionalen Folgen, die oft übersehen werden.

iX-TRACT

- Cyberkrisen erzwingen eine schnelle technische und organisatorische Reaktion. Dabei wird leicht übersehen, wir groß die Belastung für die Mitarbeitenden ist.
- Cyberkrisen sind von vielfältigen Unsicherheiten geprägt: Was genau ist passiert? Wie groß ist der Schaden? Wie lange dauert es, bis man zum Normalzustand zurückkehren kann?
- Direkt betroffene Personen, die in die Bewältigung der Krise involviert sind, müssen Entscheidungen unter hohem Zeitdruck bei einem Mangel an sicheren Informationen treffen. Zudem fällt häufig Nacht- und Wochenendarbeit an, die nötige Erholung kommt zu kurz. All das erhöht das Stresslevel.
- Mitarbeitende, die ihrer Arbeit nicht mehr wie gewohnt nachgehen können, sind indirekt betroffen und ebenfalls belastet.
- Eine gute Vorbereitung und eine Reihe von Maßnahmen während der Krise können die Situation für alle Beteiligten erheblich erleichtern.

Reagieren auf die Krise

Während in der Cyber Incident Response meist nur wenige Ressourcen an der Lösung mitwirken, sieht es bei der Bewältigung einer Cyberkrise ganz anders aus. Bei einem großen Cyberangriff, beispielsweise einem erfolgreichen Ransomwareangriff, gibt es zahlreiche Handlungsstränge, die idealerweise parallel ablaufen.

Da wäre das **Crisis Handling,** zu dem das Einberufen oder Aufsetzen des Krisenstabs, die Erarbeitung eines verständlichen Lagebilds auf Basis von meist unzureichenden Informationen und das Bewerten von wiederherstellenden Maßnahmen gehören. Hinzu kommen die tatsächliche Ausführung von Aktionen und die Dokumentation von Ereignissen, Entscheidungen, potenziellen Risiken und Aktionen unter hohem Zeitdruck.

Nötig ist zudem eine zielgruppenspezifische, kontinuierliche **Cyber Crisis Communication.** Die Informationswege in einer Krise weichen dabei von den Informationswegen im Normalbetrieb ab. Die interne Krisenkommunikation an Mitarbeitende, Management, Betriebsrat et cetera muss zur aktuellen Lage informieren und helfen, den Betrieb aufrechtzuerhalten, Vertrauen aufzubauen und

Gerüchten vorzubeugen. Bei der externen Kommunikation an Medien, Aufsichtsbehörden, Kunden, Lieferanten, Geschäftspartner, Aufsichtsrat et cetera geht es um die Information der Öffentlichkeit, um Reputationsschutz und möglicherweise die Erfüllung rechtlicher oder regulatorischer Anforderungen. Auf Basis einer Stakeholder-Analyse sind an alle Stakeholder klare Botschaften zu kommunizieren und Informationsflüsse zu kanalisieren, sodass ein einheitliches Bild nach außen entsteht. Erfahrungsgemäß steht der Erfolg des Cyber Crisis Management im engen Zusammenhang mit der Qualität und Umsetzung der Crisis Communication.

Business Continuity Management (BCM) bezeichnet die organisatorische Umsetzung von Maßnahmen zur Aufrechterhaltung eines Notbetriebs für die kritischen Geschäftsprozesse mithilfe von Ausweichlösungen.

Bei der **Cyber Incident Response** geht es um technische Fragen:

- Wo hat der Angreifer Zugang zu Systemen bzw. dem Netzwerk erlangt (Initial Access/Patient Zero)?
- Wie ist der Angreifer vorgegangen (Tactics, Techniques, Procedures – TTP)?
- Wohin ist der Angreifer vorgedrungen (betroffener Scope)?
- Wozu hat der Angreifer den Angriff durchgeführt (Intention des Angreifers)?

Cyberangriffe, die eine ganze Organisation lahmlegen, können sehr komplex sein. Ihre Vielfalt erfordert ein breites Spektrum an Fachwissen und Fähigkeiten im Cyber Incident Response Team. Cyberangriffe können sich sehr schnell ausbreiten und dazu führen, dass CIR-Teams Schwierigkeiten haben, die Ausbreitung zu stoppen oder die Angriffe zu isolieren.

Ebenfalls eine technische Aufgabe ist die **Disaster Recovery,** also die Wiederherstellung des Normalbetriebs. Das kann mehr oder weniger umfangreich sein: Im schlimmsten Fall muss die gesamte IT-Infrastruktur neu aufgebaut und betroffene Systeme und Daten müssen durch Verwendung von Backups wiederhergestellt werden. Dabei müssen neu aufgesetzte Systeme auf dem neuesten Stand und alle Sicherheitspatches und Updates installiert sein. Nach der Wiederherstellung muss man die Systeme sorgfältig überwachen und auf Anzeichen für verdächtige Aktivitäten prüfen.

Warum eine Krise überfordert

Während einer Krise ist also viel zu tun und vieles davon läuft parallel. Insbesondere innerhalb der ersten Stunden und Tage ist das Ziel, Ordnung ins Chaos zu bringen und die neue Situation bestmöglich zu kontrollieren. Es wird in ungewohnten Teams gearbeitet und aufgrund der besonderen Aufbauorganisation gibt es plötzlich veränderte Hierarchien. Die Flut an Informationen ist groß und Ereignisse müssen analysiert und priorisiert werden, während man gleichzeitig mit anderen Teams und Stakeholdern kommuniziert. Zeit ist ein entscheidender Faktor, es entsteht enormer Druck, schnelle Entscheidungen zu treffen.

Dies kann, zusammen mit der Verantwortung für die Sicherheit und Zukunft des Unternehmens, zu Überforderung führen. Die Folgen sind Stress, Erschöpfung und Unsicherheit, da es in der Krise oft viele unbekannte Faktoren gibt: Wie weit hat sich der Angriff ausgebreitet? Sind Daten abgeflossen? Wie lange wird die Krise andauern? Wie wird diese Krise ausgehen? Häufig erfordert eine Krise zusätzliche Arbeit außerhalb der normalen Arbeitszeit und damit einhergehend die Umplanung privater Verpflichtungen wie Kinderbetreuung. Zudem fehlen Gelegenheiten zum Erholen.

Auswirkungen von Cyberkrisen auf direkt Beteiligte

Die vielen wichtigen und dringenden Maßnahmen in einer Cyberkrise führen zu einer stark erhöhten Arbeitslast der beteiligten Mitarbeitenden. Wenn mehr Aufgaben zu erledigen sind, als Ressourcen zu Verfügung stehen, führt das zu Stress – insbesondere, wenn die aktive Bewältigung einer Cyberkrise mehrere Wochen dauert und ab einem gewissen Zeitpunkt zusätzlich das Tagesgeschäft zumindest teilweise aufrechterhalten werden muss.

Bei Cyberkrisen, die sich über Wochen oder Monate hinziehen, steigt das Frustrationslevel der Beteiligten, da die Durchhaltefähigkeit häufig erschöpft ist und die Belastungsgrenzen dauerhaft überschritten werden. Je länger Mitarbeitende dieser chaotischen Situation ausgesetzt sind, desto größer sind die negativen Auswirkungen auf ihre mentale Gesundheit. Dazu kommt die Ungewissheit darüber, wie lang die Krise andauern wird und wann der normale Arbeitsalltag wieder einsetzt. Zudem beeinflusst Druck von innen und außen die mentale Stabilität der Beteiligten.

Wenn dann gerade zu Beginn der Krise Kommunikationstechnologien oder Kollaborationsplattformen nicht verfügbar sind, leiden Zusammenarbeit und Kommunikation. In einer Krise kann es auch sehr rau zugehen – vor allem, wenn die Entstörung der Cyberkrise nicht so läuft wie geplant, können zwischenmenschliche Konflikte entstehen. Als Konsequenz eines schlechten Krisenmanagements verlassen womöglich Personen das Unternehmen, die das Vertrauen in die Unternehmensführung und die IT-Security verloren haben.

All das kann sich negativ auf die Handlungssicherheit, Reaktionsfähigkeit und Entscheidungskompetenz der beteiligten Personen auswirken, zu Effizienzverlusten in der Krisenbewältigung führen und deren Erfolg beeinträchtigen. Folgende negative Effekte können während Cyberkrisen auftreten:

- **Schlafstörungen:** Schicht- und Bereitschaftsdienste sowie Überstunden können zu Schlafmangel führen, der wiederum die kognitiven Funktionen und das Urteilsvermögen beeinträchtigt.
- **Burn-out:** Lange und intensive Arbeitszeiten während der Krise lassen wenig Zeit für Erholung und der andauernde hohe Druck in der Krise kann zu Burnout führen.
- **Frustration:** Läuft die Bewältigung der Krise nicht wie geplant und gibt es Rückschläge, steigert das das Frustrationslevel, beeinträchtigt das Selbstwertgefühl und löst Zweifel an der eigenen Kompetenz aus.
- **Schuldgefühle:** Das Gefühl, man hätte etwas tun können, um den Vorfall zu verhindern, kann Schuldgefühle auslösen. Wenn die Krise auf menschliches Versagen zurückzuführen ist, wie der Klick auf einen schädlichen Link, kann Schamgefühl entstehen. Die Angst, für die Krise verantwortlich gemacht zu werden, führt zu zusätzlichem Stress.
- **Enttäuschung:** Mitarbeitende können enttäuscht das Vertrauen in die Sicherheitsmaßnahmen oder das Management verlieren, wenn trotz aller Bemühungen ein Sicherheitsvorfall eintritt und persönliche Daten nicht ausreichend geschützt wurden.
- **Wut:** Das Gefühl, dass die Organisation nicht ausreichend in präventive Maßnahmen investiert hat, kann Wut auslösen. Die Wut kann sich auch gegen die Angreifer richten.
- **Hilflosigkeit:** Wird das eigene Unternehmen Opfer eines Cyberangriffs, kann das besonders bei den für die Sicherheit Verantwortlichen ein Gefühl der Hilflosigkeit auslösen.
- **Physische gesundheitliche Auswirkungen:** Wenig Pausen, unregelmäßige Mahlzeiten und ein Mangel an Bewegung können zu Rückenschmerzen,

erhöhtem Blutdruck und Magenbeschwerden führen.
- **Verlust der Work-Life-Balance:** Da die Grenze zwischen Arbeit und Privatleben verschwimmt und es sehr schwer ist, sich nach Ende des Arbeitstages zu erholen und abzuschalten, kann die Work-Life-Balance leiden.
- **Soziale Isolation:** Aufgrund der intensiven Arbeit kann eine Krise zu sozialer Isolation führen.

Auswirkungen auf indirekt betroffene Personen

Die negativen Auswirkungen einer Cyberkrise treffen nicht nur die Menschen, die direkt zur Bewältigung der Krise beitragen. Mitarbeitende, die ihrer Arbeit nicht mehr wie gewohnt nachgehen können, sind indirekt betroffen. Wenn bereits die mentale und physische Gesundheit der direkt betroffenen Menschen zu wenig Aufmerksamkeit erhält, so wird noch viel seltener an indirekt betroffene Menschen gedacht.

Dazu ein kurzes Beispiel aus einem Gespräch mit dem Leiter der IT-Infrastruktur eines Unternehmens. Er ist alleinerziehender Vater und der Cyberangriff fiel in seinen Urlaub. Er konnte seinen Urlaub nicht verschieben und fühlte sich schuldig, weil er das Gefühl hatte, sein Team und das Unternehmen hängen zu lassen. Hier war seine Familie indirekt betroffen, weil der Vater mit seinen Gedanken bei seinem Team war, das mit der Bewältigung der Krise kämpfte. Es gilt, die negativen Auswirkungen auf die Mitarbeitenden vor, während und nach einer Krise möglichst gering zu halten. Dabei können die folgenden Punkte helfen.

Was man vor der Krise tun kann

Wenn **die wichtigsten Prozessdokumente** im Krisenfall bereitliegen, hilft das enorm weiter:
- **Business-Impact-Analyse** zur Identifikation von kritischen Systemen und Ressourcen, die für den Geschäftsbetrieb unerlässlich sind, zur Priorisierung der Wiederherstellung und zur Definition der Wiederherstellungszeiten;
- **Cyber Crisis Management Plan** mit Strategien, Verantwortlichkeiten und Abläufen zur Bewältigung von Cyberkrisen;
- **Incident Response Plan,** ein detaillierter Leitfaden zur Reaktion auf Sicherheitsvorfälle, einschließlich Schritten zur Identifizierung, Eindämmung und Wiederherstellung;

Cyberkrisen sind belastend – nicht nur für die Personen, die direkt damit kämpfen.

- **Business Continuity Plan** zur Sicherstellung der Geschäftskontinuität und zur Wiederherstellung nach einer Krise;
- **Communication Plan** zur effektiven Kommunikation mit internen und externen Stakeholdern;
- **Risk Assessment Report,** eine Bewertung der potenziellen Risiken und Schwachstellen im Unternehmen;
- **Data Breach Response Plan** zur Reaktion auf Datenverletzungen und zum Schutz von Kundendaten;
- **Post-Incident Review Template,** ein Dokument zur Analyse und Verbesserung der Reaktion auf vergangene Sicherheitsvorfälle.

Bei lang anhaltenden Krisen kann ein Schichtdienst sinnvoll sein. Eine **nachhaltige Einsatzplanung und Vertretungsregelung** mit definierten Übergabeprozessen lässt sich bereits vor der Krise erstellen. Hier proaktiv tätig zu werden und somit während kommender Krisen bereits für ausreichend Erholungszeiten zu sorgen, ermöglicht es, auch in länger andauernden Krisen noch handlungsfähig zu bleiben und seine Mitarbeitenden vor Überlastung zu schützen.

Crisis Simulation: Im Rahmen von Krisenübungen kann die Bewältigung der Krise geprobt und trainiert werden, damit alle Beteiligten im Ernstfall ruhiger, zielgerichteter und effektiver handeln können. Auch Stresssituationen lassen sich bis zu einem gewissen Punkt simulieren, damit Mitarbeitende widerstandsfähiger dagegen werden. Im Idealfall verkürzt sich dadurch auch die Chaosphase (Norming Phase) zu Beginn einer Krise.

Eine gute und erfahrene **Krisenstabsleitung** kann für eine effektive und effiziente Bewältigung der Krise sorgen und auch ein Auge auf das Wohlergehen aller Beteiligten halten.

Der **Krisenstabsraum** muss so ausgestattet sein, dass man darin über längere Zeit effektiv eine Krise managen kann. Zur Ausstattung gehören Kommunikationsmittel wie Telefon- und Videokonferenzsysteme, Internetzugang, Drucker und Faxgeräte. Zur Visualisierung von Informationen sind Whiteboards, Pinnwände und Flipcharts nützlich.

Erwartungen managen: Während Krisen sind manche Informationen nicht direkt verfügbar und es kann manchmal ein paar Tage dauern, bis eine vom Vorstand gestellte Frage beantwortet werden kann. Wurde bereits vor Kriseneintritt Verständnis dafür im Unternehmen entwickelt, begünstigt dies eine gesunde Arbeitsatmosphäre. Selbstverständlich kann man das Management während der Krise an diesen Punkt erinnern.

Während der Krise

Ruhezonen sorgen dafür, dass Mitarbeitende in einem geschützten Raum in Ruhe und konzentriert arbeiten können, ohne kontinuierlich nach Updates gefragt zu werden.

Fokussierung: Multitasking erhöht das Stresslevel, frisst Energie und führt zu Fehlern. Mitarbeitende sollten sich möglichst auf einen eng abgesteckten Aufgabenbereich konzentrieren können. Aufgaben, die nicht zur Bewältigung der Krise beitragen, sollten ihnen abgenommen werden.

Um zu gewährleisten, dass keine Informationen verloren gehen, ist eine **konsistente und übergreifende Dokumentation** anzufertigen. Bedeutende Ereignisse, Entscheidungen und potenzielle Risiken sollten dort ebenso dokumentiert sein wie die nächsten Schritte inklusive der Verantwortlichen.

Eine **faktenbasierte Maßnahmenplanung** kann blindem Aktionismus vorbeugen. Annahmen sollten dabei als solche kenntlich gemacht und schnellstmöglich überprüft werden. Entscheidungen werden auf Basis von Fakten getroffen, die nicht mit Annahmen vermischt sein dürfen. Man muss außerdem darauf achten, dass keine Gerüchte entstehen, die mit Fakten vermischt werden.

Vor allem zu Beginn ist eine **Situationsklärung und -beschreibung** wichtig, auf deren Basis eine fachkundige dritte Person die Situation verstehen und zielgerichtet handeln kann. Eine gute Situationsklärung kann ebenfalls blindem Aktionismus vorbeugen.

Lagevisualisierung: Mithilfe von Whiteboards, Pinnwänden, Flipcharts und anderen Tools kann man die Lage visuell darstellen und so für noch mehr Transparenz sorgen. So visualisiert eine Lagekarte die geografischen Auswirkun-

gen einer Krise und ein Zeitstrahl stellt komplexe Ereignisse und Entwicklungen chronologisch dar.

Es ist hilfreich, **wechselnde Arbeitsmodi** zu vereinbaren aus Phasen mit Besprechungen und Updates und Phasen, in denen konzentriert (in einem geschützten Raum) gearbeitet wird.

Für die Mitarbeitenden sorgen

Verpflegung: Für ausreichend Wasser sollte gesorgt und die Verpflegung gesichert sein, insbesondere für Zeiten, in denen die Kantine nicht zur Verfügung steht.

Die Mitarbeitenden müssen ausreichende und **regelmäßige Pausen** erhalten. Eine Cyberkrise ist kein Sprint, sondern ein Marathon.

Trotz einer nachhaltigen Einsatzplanung kann eine lang andauernde Krise einen vollständigen **Personalwechsel** nötig machen, um für Entlastung bei überlasteten Mitarbeitenden zu sorgen. Dies ist nicht immer notwendig und auch nicht immer möglich. Dann muss man im Nachgang die kritischen Engpässe daraufhin bewerten, wie in kommenden Krisen für Entlastung gesorgt werden kann.

Während der Krisenbekämpfung gilt: **Schuldzuweisungen vermeiden** und nachhaltig unterbinden, da sich dadurch das Arbeitsklima verschlechtert. Besser ist eine Kultur, die Krisen als Chance für Wachstum begreift und in der aus Fehlern gelernt wird.

Damit die Mitarbeitenden in einer außerordentlichen Stresssituation motiviert und leistungsbereit bleiben, müssen sie **wertschätzend** behandelt werden. Krisensituationen sind eine enorme Belastung für alle. Wenn eine Krise Wochen andauert und es zu Schwierigkeiten kommt, kann der Ton rauer werden und man sollte bei emotionalen Diskussionen den Emotionen ausreichend Raum geben, aber dennoch niemals die Sachebene bei den Diskussionen verlassen.

Positive Grundstimmung: Schaffen es Unternehmensführung und Krisenstabsleitung, statt einer Opferstimmung ein positives Wirgefühl zu verbreiten, profitieren davon alle an der Krisenbewältigung Beteiligten.

Der Krisenstab muss **Transparenz** darüber herstellen, wie die Krisenbewältigung ablaufen wird. Wichtig dabei ist eine langfristige Ausrichtung und das Bieten einer Perspektive.

Routinen: Bekannte Abläufe und Prozesse geben in Chaosphasen und Zeiten der Ungewissheit Sicherheit.

Personen, die besonders stark belastet sind, sollten ein Angebot für **Unterstützung im privaten Umfeld** wie die Übernahme von Besorgungen oder Kinderbetreuung erhalten.

Es erspart Zeit nach der Krise, wenn bereits währenddessen eine **Lessons-Learned-Liste** die Erfahrungen dokumentiert.

Nach der Krise

Nach Abschluss sollte ein Lessons-Learned-Prozess folgen. Idealerweise betrachtet und erweitert man hier die während der Krise erstellte Liste und führt nach der Rückkehr zur Normalität mit einigen Stakeholdern einen Workshop durch. Hier wird besprochen, was gut lief, was weniger gut lief und was geändert werden sollte mit dem Ziel, aus vergangenen Cyberkrisen zu lernen, um für kommende Krisen besser aufgestellt zu sein. Hier lassen sich kurz-, mittel- und langfristige Maßnahmen zur Steigerung der Resilienz festlegen.

Fazit

Organisationen müssen auch in einer Krise auf die Gesundheit und das Wohlbefinden ihrer Mitarbeitenden achten. Zahlreiche Maßnahmen vor, während und nach einer Cyberkrise können helfen, mögliche negative Effekte auf direkt und indirekt beteiligte Menschen gering zu halten. Im besten Fall handeln Unternehmen proaktiv, indem sie sich auf potenzielle Cyberkrisen vorbereiten und zugleich die Cyberresilienz erhöhen, um deren Eintrittswahrscheinlichkeit zu verringern. Zudem ist es ratsam, auch die Krisenbewältigung regelmäßig zu üben und gut durchdacht zu haben, damit die Bewältigung der Krise möglichst effektiv und effizient ist und negative Auswirkungen so gering wie möglich bleiben – einen hundertprozentigen Schutz vor Cyberkrisen gibt es nicht. (odi@ix.de)

SEBASTIAN PÖHLCHEN

ist Senior Manager im Bereich Cyber Defense & Response bei Deloitte. Er hat Wirtschaftsinformatik und Wirtschaftspsychologie studiert.

MALKO STEINORTH

verantwortet bei Deloitte den Bereich Cyber Defense & Response und hilft Kunden, bedrohungsgerechte Cyberstrategien zu entwickeln und umzusetzen.