Krisenmanagement und Kommunikation im Ausnahmezustand

WENN NICHTS MEHR GEHT

Viele IT-Verantwortliche erleben den Arbeitsalltag als eine ständige Krise – weil sich Probleme stapeln, Lösungen schwierig sind und die Ressourcen oft nicht ausreichen, um allen Erwartungen und Anforderungen gerecht zu werden. Das ist allerdings meist der Normalbetrieb. Echte Krise herrscht, wenn das gesamte Unternehmen den Ausnahmezustand ausruft – zum Beispiel während eines Ransomware-Angriffs. Was dann zu tun ist und mit wem worüber gesprochen werden muss, erfahren Sie in diesem Artikel.

Falls Sie es bisher nicht erleben mussten – Glückwunsch! – versetzen Sie sich nun gedanklich in die folgende Situation: Das Telefon klingelt und man informiert Sie darüber, dass die Unternehmenssysteme verschlüsselt sind. Es gibt eine Lösegeldforderung. Die ersten Führungskräfte wissen schon Bescheid. Jetzt klingelt das Telefon alle paar Minuten. Aufruhr.

Wie lange bleibt der Betrieb lahmgelegt? Wer tritt vor die Geschäftsführung und schildert die Lage – und in welcher Form? Dass vorerst gar nichts mehr geht, und auch bisher nicht klar ist, wie lange das so bleiben wird? Welche Entscheidungsgrundlage benötigt das Top-Management jetzt? Was wird den Mitarbeitern gesagt, die an ihrem PC arbeiten wollen? Wie informiert man die Produktion, die gerade nichts mehr fertigen kann? Und was sagt man Kunden und Partnern – wie geht es weiter?

VOM GUTEN ZU WENIG, VOM SCHLECHTEN ZU VIEL

Sie sind jetzt in der Phase, in der Sie wichtige Entscheidungen treffen müssen. Dabei fehlen Ihnen allerdings einige wertvolle Zutaten: Zeit, Informationen, Sicherheit und gewohnte Arbeitsmittel. Dennoch müssen Sie entscheiden, denn ansonsten bestimmt der Rhythmus der Krise die Entscheidungen. Zudem müssen Sie Menschen koordinieren. Das heißt: Kommunizieren in einer Ausnahmesituation, die für die meisten Betroffenen Neuland ist. Selten oder noch nie geübte Prozesse müssen jetzt funktionieren, herausfordernde Aufgaben müssen bewältigt werden. Das gilt übrigens auch dann, wenn es sich um einen voraussichtlich nur kurzen Ausfall handelt – sobald grundlegende Produkte und Dienstleistungen nicht mehr verfügbar sind, brauchen Organisationen einen Plan B.

DEFINITION, ESKALATION, KOORDINATION

Dafür müssen vorab Eskalationslevel festgelegt sein – Sie haben sicher eindeutige Definitionen verschiedener Betriebsstörungen, deren spezifische Eigenschaften und Anforderungen sich direkt auf das Krisenmanagement auswirken. Die Begrifflichkeiten und Abstufungen können sich organisationsspezifisch unterscheiden, als Faustregel gilt: Aus Sicht der Business-Continuity-Manager ist Krise dann, wenn Sie einen Krisenstab benötigen – aus kommunikationstheoretischer Sicht dann, wenn Ihre Stakeholder denken, dass Krise ist.

Fest steht: Im Ernstfall müssen die Meldewege klar sein und funktionieren – auch Sonntagnacht um 3 Uhr. Erstellen Sie daher eindeutige Pläne mit Lage-Definitionen und Bewertungsfaktoren, Alarmierungsstrukturen, Zuständigkeiten und aktuellen Kontaktdaten. Auch für den Krisenstab, in dem regelmäßig die aktuelle Lage erfasst und bewertet wird, Handlungsoptionen entwickelt und Maßnahmen beschlossen werden, müssen definierte Rollen und Prozesse vorliegen. Neben operativen werden hier zudem kommunikative Entscheidungen getroffen. Im besten Fall trainieren Sie ein solches Szenario auch einmal im Rahmen einer Krisenübung – ob als einfache Tabletop-Übung oder softwarebasierte Simulation.

PLÖTZLICH WILL JEDER MIT IHNEN REDEN

Kommt es zur Einberufung des Krisenstabs für den Cybervorfall, sind Sie darin ein zentrales Mitglied – es werden also häufig fragende Augen auf Sie gerichtet sein. In dem Moment, in dem Sie eigentlich fokussiert und in Ruhe arbeiten müssen, wollen sehr viele Menschen, die Sie vielleicht noch nie gesehen haben, plötzlich sehr dringend mit Ihnen reden. In der Krisenstabslagebesprechung, in Abteilungsmeetings, in dringenden Telefonaten. Schlussendlich haben zwar alle ein gemeinsames Ziel – schnellstmöglich wieder handlungsfähig zu werden. Doch die Sichtweisen der Verantwortlichen unterscheiden sich naturgemäß voneinander. Für Sie heißt das also, dass Sie – anders als vielleicht in Ihrem gewohnten Arbeitsalltag – sehr viel und vor allem strategisch klug kommunizieren oder zumindest dabei unterstützen müssen. Mit wem genau und worüber schlüsseln wir jetzt auf.

- **Human Resources:** Eine der ersten Fragen, die man an Sie heranträgt, ist die nach der Arbeitsfähigkeit der Mitarbeiter. Wenn die üblichen Aufgaben nicht erledigt werden können, müssen die Teams dann überhaupt zur Arbeit erscheinen? Wie stemmen sie das Tagesgeschäft – oder wie können sie sich gegebenenfalls in anderen Bereichen nützlich machen? Wie werden Arbeitszeiten, Urlaubstage, Krankheitsausfall und – ganz wichtig – die Überstunden zur Krisenbewältigung in der IT erfasst? Hierzu müssen Sie Input liefern – dieser ist ableitbar von den Prognosen,

wie schnell Sie welche Systeme wieder verfügbar machen können.

- **Datenschutzbeauftragte, Juristen:** Zur Runde der Fragesteller gesellen sich auch interne oder externe juristische Verantwortliche – und das ziemlich zügig, da die Melde-Uhr unerbittlich tickt. Ob Sie KRITIS-Betreiber sind und entsprechend gesetzliche Regelungen zu beachten haben – darüber haben Sie sicherlich ausreichend Klarheit? Ob Sie Auftragsverarbeiter oder Verantwortlicher im Sinne der Datenschutzgrundverordnung sind, und wen Sie bei einem potenziellen Abfluss personenbezogener Daten informieren müssen, wissen Sie auch? Und die Kontaktdaten vom Landeskriminalamt beziehungsweise der Zentralen Ansprechstellen Cybercrime (ZAC) sind in einem Papierordner abgeheftet? Super, dann können Sie an die Behörden-Gruppe schon mal einen Haken setzen.

- **Externe Spezialisten:** Sofern Sie im Bereich Forensik und Wiederaufbau mit externen Spezialisten zusammenarbeiten, müssen diese koordiniert werden. Bedenken Sie also organisatorische Aspekte: Wer ist der Ansprechpartner aus Ihrem Team, wie oft kommen Sie in welcher Form zusammen (bei anfänglicher oder dauerhafter Remote-Unterstützung technische Einschränkungen bedenken!), wer gibt Erkenntnisse und Entwicklungen an den Krisenstab weiter? Hierfür gilt es, schnell klare Regelungen zu finden und Prozesse zu etablieren, die – wenn auch in angepasster Form – eine ganze Zeit lang funktionieren müssen.

- **Geschäftsführung, Prokuristen:** Und dann wartet die nächste Herausforderung: Wenn Sie im Krisenstab über Ihren Arbeitsbereich berichten, wird das unter Umständen nicht jeder verstehen. Das liegt nicht an bösem Willen, sondern schlicht am fehlenden Verständnis für Ihre Prozesse, Zuständigkeiten, technische Aspekte oder die Tragweite der Situation. Die Erfahrung zeigt, dass in solchen Krisen jede Abteilung ihre Belange (ergo: ihre Daten) als die wichtigsten erachtet. Diese Erwartungen müssen Sie moderieren – und das gelingt Ihnen nur, wenn Sie belastbare Entscheidungen treffen, die sich an der aktuellen Realität orientieren, und diese gut vermitteln. Es braucht also nicht nur klare Ansagen, sondern eventuell auch eine „Übersetzung" dieser Fakten von „IT-Deutsch" in „DAU-Deutsch". Hier hat es sich als hilfreich erwiesen, wenn die benannte Runde schon vor Krisenfällen öfter beisammen gesessen hat. Auch das ist ein Impuls, den Sie an andere Abteilungen weitergeben können: Wer in Friedenszeiten gemeinsam mit den wichtigsten Verantwortlichen definiert, welche Daten die Kronjuwelen des Unternehmens sind, muss in der Krise keine zeitaufwendigen und nervenaufreibenden Entscheidungsfindungen vorantreiben. So ist es leichter, die erforderlichen Ressourcen zu beschaffen – sei es für Hardware, Lizenzen, externe Dienstleister oder zusätzliches Personal. Fragen nach funktionierenden Back-ups und dem Wiederanlauf der Systeme stellen sich übrigens auch vor dem Hintergrund, ob auf die Kontaktaufnahme der Erpresser eingegangen werden muss – auch das ist eine Entscheidung, die zu beträchtlichem Maße von Ihnen abhängen kann.

- **Kundenmanagement, Kommunikationsverantwortliche:** Die wenigsten von Ihnen operieren im Tagesgeschäft im luftleeren Raum – von den Produkten oder Dienstleistungen Ihrer Organisation hängen Kunden, Partner, Zulieferer und viele weitere Anspruchsgruppen ab. Sie alle sollten wissen, wenn es bei Ihnen längerfristige Technikprobleme oder -ausfälle gibt. Sofern eine explizite Kommunikations- oder Marketingabteilung vorhanden ist, müssen Sie also auch dieser im Krisenstab Rede und Antwort stehen, damit diese ihren Job machen kann. In anderen Fällen wird die Kommunikation direkt über die Geschäftsführung oder das Kundenmanagement laufen. Die Herausforderung bleibt die gleiche: Alle, mit denen Sie reden müssen, und die wiederum mit anderen Personengruppen reden müssen, benötigen eine Perspektive für die kommenden Stunden, Tage, Wochen oder schlimmstenfalls Monate. Und diese müssen Sie liefern.

DIE ZAUBERWAFFE „ZEITPLAN"

Es ist vollkommen nachvollziehbar, wenn Sie am ersten Tag noch keine belastbaren Prognosen treffen können, was wann wieder läuft. Und dennoch: Sobald Sie auch nur einen groben Plan haben, mit welchen Ständen zu welchen Zeitpunkten zu rechnen ist, teilen Sie dies mit. Sie müssen die Hoheit über Zeitpläne haben. Denn damit steuern Sie, wie das Unternehmen in dieser Krise wahrgenommen wird, und ob man ihm die Bewältigung dieser Notlage zutraut oder nicht. Die fundamentale Forderung aller internen und externen Anspruchsgruppen ist, dass Sie jetzt, im Krisenfall, alles vorbildlich richtig machen, um die Erwartungen, die man an Ihr Unternehmen stellt, nicht noch einmal zu enttäuschen. Und dazu gehört die Antwort auf die schlichte, aber wichtige Frage „Wann funktioniert wieder alles?"

„ICH WEIß, DASS ICH NICHTS WEIß"

Vielleicht ist es Ihnen schon aufgefallen – der eben formulierte Ratschlag kann einen kleinen Haken haben: Er grätscht Sie unter Umständen in einen Spagat aus Planung und Wirklichkeit. Die Lösung: pessimistische Prozesskommunikation. Sie werden Ihre Zeitpläne immer wieder anhand der Realität nachjustieren müssen: Weil die forensische Analyse länger dauert als geplant, weil der Wiederaufbau der Systeme komplexer ist als erhofft, weil Ihnen Teammitglieder durch Überlastung ausfallen und auch Sie irgendwann einmal essen und schlafen müssen. Denken Sie deshalb in kleinen Häppchen statt großen Brocken. Geben Sie klare Informationen dazu, welcher Teilschritt als Nächstes ansteht und mit welchem Ergebnis Sie wann rechnen. Tragen Sie Ihren Kommunikationsverantwortlichen auf, ihren Empfängern mitzuteilen, wann sie das nächste Mal von Ihrem Unternehmen hören oder lesen: so bald und regelmäßig wie möglich. Kommunizieren Sie auch Nichtwissen und Unsicherheiten: Ein ehrliches „Das untersuchen wir gerade noch intern und geben Ihnen dann Bescheid" ist besser als eine vollmundige, ungesicherte Tatsachenbehauptung. Und: Planen Sie lieber zu pessimistisch als zu optimistisch. Sie glauben, dass die ersten Systeme in einer Woche wieder an den Start gehen? Kommunizieren Sie anderthalb Wochen – irgendetwas wird ganz sicher schiefgehen.

TRANSPARENZ ÜBER TRANSAKTIONEN?

Bleibt die Gretchenfrage nach der Transparenz, besonders auch gegenüber Medien. Die engagierte Lokaljournalistin, die mit dieser „Erpressung!! durch Cyberkriminelle!!" die ganz große Story wittert und nach der Lösegeldsumme

CHECKLISTE
Krisenmanagement und -kommunikation

- *Vergewissern Sie sich, dass abteilungsübergreifende Krisenstrukturen existieren und wichtige Prozesse immer wieder geübt werden. Sorgen Sie dafür, dass relevante Ansprechpartner ihre Rollen in Krisenplänen kennen und wissen, wo sie Anweisungen für Notfälle finden (bestenfalls nicht auf einem dann verschlüsselten System).*
- *Definieren Sie die Qualität, Relevanz und Priorität Ihrer Daten (für Aufrechterhaltung des Geschäftsbetriebs, in Hinblick auf die Datenschutzgrundverordnung (DSGVO) et cetera). Tun Sie dies mit nachvollziehbaren Begründungen, um im Ernstfall schnelle, belastbare Entscheidungen treffen zu können.*
- *Bedenken Sie beim Thema Redundanzen nicht nur Ihre Back-ups, sondern auch Kommunikationsmittel und -kanäle (ausgedruckte Listen mit privaten E-Mail-Adressen und Handynummern der wichtigsten Kontakte, webbasierte Tools zum kollaborativen Arbeiten et cetera).*
- *Klären Sie ab, ob die Notfallpläne auch das Thema Krisenkommunikation berücksichtigen und unterstützen Sie durch Ihren fachlichen Input Ihre Kollegen dabei, schnell (aktiv und frühzeitig), wahrhaftig (sachlich, transparent und wahr), verständlich (lesbar und unkompliziert) sowie konsistent (einheitlich und kontinuierlich) zu kommunizieren. Die Verantwortlichen sollten dafür entsprechende Vorlagen für Mailings (intern/extern), Holding Statements, Sprechzettel, FAQ, Presseinformationen vorbereiten.*
- *Dokumentieren Sie alles. Vor der Krise die Maßnahmen, die Sie zur Vermeidung ergriffen hatten. Während der Krise die Maßnahmen, die Sie zur Bewältigung einsetzen. Nach der Krise, was Sie beim nächsten Mal besser machen sollten.*

fragt, der eigentlich nette IT-Blogger, der wissen will, warum nicht einfach die Back-ups wieder eingespielt wurden, die Fachzeitschrift, die Informationen zum forensischen Bericht möchte – auch solche Stakeholder werden sich melden und mehr oder weniger freundlich um Auskunft bitten. Hier müssen Sie gemeinsam mit den Kollegen aus der Kommunikation taktisch klug vorgehen. Zu viele öffentliche Informationen, beispielsweise über sensible Sicherheitsaspekte oder Geschäftsgeheimnisse, sind unter Umständen kontraproduktiv. Zu wenige Informationen wiederum könnte man als Verschleierung von öffentlichkeitsrelevanten Fakten interpretieren. Hier gilt es, gemeinsam mit den entsprechenden Experten eine grundlegende Kommunikationsstrategie zu definieren und diese dann konsequent umzusetzen.

UND JETZT?

Das waren jede Menge kommunikative Aufgaben – und dabei wollen Sie doch nur eins: in Ruhe arbeiten. Ihr Verbündeter ist in diesem Fall ein guter Krisenmanager, der Ihnen den Rücken freihält, damit Sie Ihren Notfallplan abarbeiten können, anstatt in endlosen Meetings dutzende Erklärschleifen zu drehen. Ein Krisenmanager kann umso besser mit Ihnen arbeiten, je besser Sie für ein solches Szenario aufgestellt sind. Und damit kommen wir zum Fazit: Eine Vorbereitung auf und die Bewältigung von Cybervorfällen ist dann am erfolgreichsten, wenn sie über einzelne Bereiche wie Informationstechnologie (IT), Business Continuity Management (BCM), Rechtsabteilung (Legal) und Unternehmenskommunikation hinaus ganzheitlich betrachtet und umgesetzt wird. Krisenprävention, -management und -kommunikation sind interdisziplinäre Managementprozesse.

Laufen Sie nach der ersten Krise (erfolgreicher Angriff durch technische Schwachstellen) direkt in die zweite Krise (schlechtes Krisenmanagement, oder gutes Krisenmanagement und nicht ausreichende Kommunikation darüber), kann das Ihre Organisation ziemlich schnell in Bedrängnis bringen. Beispiele, bei denen ein Ransomware-Angriff der letzte Akt war, der ein Unternehmen in die Insolvenz getrieben hat, gibt es leider einige. Durch gute Vorbereitung hingegen können Sie den Handlungsspielraum Ihrer Organisation in der Krise erweitern – indem Sie besonnen agieren, belastbare Entscheidungen treffen und zielgerichtet arbeiten. Gelingt es Ihnen und Ihren Teams, das Vertrauen der Stakeholder in Ihre Krisenmanagement-Fähigkeiten durch kluge Kommunikation zu erhalten, stehen die Chancen gut, unbeschadet oder zumindest nur mit geringem Reputationsverlust durch die Krise zu kommen. ■

JANKA KREISSL
ist Partnerin bei DUNKELBLAU Krisenmanagement & -kommunikation.