Krisenkommunikation bei Cyber Incidents

Wird ein Unternehmen angegriffen, kracht es an allen Ecken und Enden: Die IT fällt aus, das Tagesgeschäft kann nicht weitergeführt werden, vielleicht sind noch Kundendaten in falsche Hände gelangt. Neben der Bewältigung der ganzen Probleme kommt der Kommunikation in der Krisensituation eine besondere Rolle zu.

Von Janka Kreißl

Krise? Welche Krise? Sie lesen gerade ein Heft, in dem es um nichts anderes als „die Krise“ geht. „Ich hab doch eh die ganze Zeit Krise“, denken Sie sich vielleicht – weil auch Ihr Arbeitsalltag hektisch ist, Zeit fehlt und immer zu viele Probleme gleichzeitig auf eine Lösung warten; nicht ausreichend Ressourcen da sind, um Erwartungen und Forderungen zu erfüllen, und Sie vielleicht ein anderes Verständnis von Störfall, Notfall oder Krise haben als Ihre Geschäftsführung, die Prokuristen oder die Kommunikationsabteilung. Das ist meistens allerdings der Normalbetrieb. Krise ist, wenn der Normalbetrieb gar nicht mehr funktioniert – und das gesamte Unternehmen den Krisenmodus einlegt.

Fakt ist: Wenn ein Unternehmen von einem Ransomwareangriff betroffen ist, haben alle Krise – und zwar richtig. Warum das so ist, was Sie dann tun können und müssen und wie Sie auch Ihre Kolleginnen und Kollegen davon überzeugen, dass sich eine gute Vorbereitung bezahlt macht, erklärt dieser Artikel.

Vom Guten zu wenig, vom Schlechten zu viel

Sofern Sie es noch nicht miterleben mussten (Glückwunsch!), denken und fühlen Sie sich bitte jetzt einmal in die folgende Situation hinein: Das Telefon klingelt und Sie werden darüber informiert, dass Ihre Systeme verschlüsselt sind. Es gibt eine Ransom Note. Die ersten Führungskräfte wissen schon Bescheid. Jetzt klingelt das Telefon alle paar Minuten. Aufruhr. Wie lange bleiben die Systeme down? Wer erklärt der Geschäftsführung den Vorfall – und was? Dass vorerst gar nichts mehr geht und auch noch nicht klar ist, wie lange das so sein wird? Welche Entscheidungsvorlage braucht der Vorstand nun? Was wird den Mitarbeitenden gesagt, die an ihrem PC arbeiten wollen? Und die Kunden, Ihre Produkte, das ganz normale tägliche Geschäft – wie geht es weiter?

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. Und Sie müssen 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 bewältigt werden. Das gilt übrigens auch dann, wenn es sich um einen voraussichtlich nur kurzen Ausfall handelt.

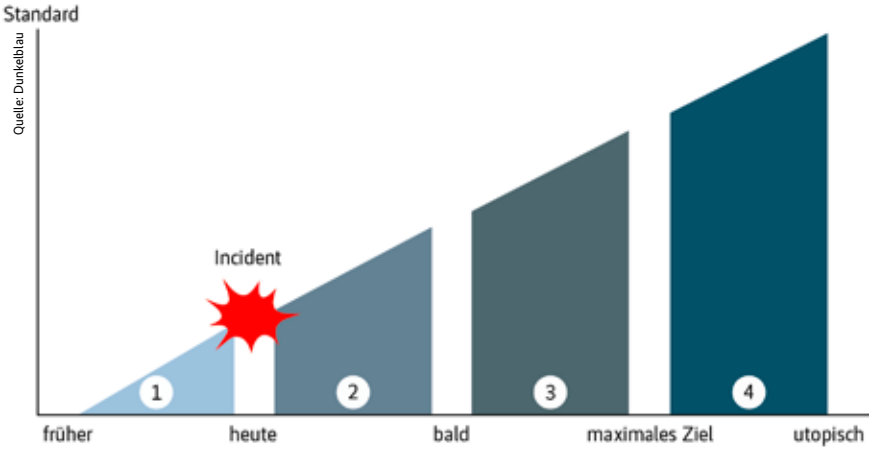
Denn – kleiner Exkurs in die Theorie der Krisenkommunikation – Krise ist dann, wenn Ihre Stakeholder das Gefühl haben, dass Krise ist. Warum? Weil interne und externe Anspruchsgruppen Erwartungen an Ihr Unternehmen oder Ihre Abteilung haben und diese Erwartung ständig mit der Realität abgleichen. Werden diese Erwartungen enttäuscht (zum Beispiel weil Mitarbeitende nicht mehr oder nur unter erschwerten Bedingungen arbeiten können, grundlegende Prozesse sich verzögern, Kunden ihr Produkt nicht mehr beziehen können), denken diese Personen darüber nach, ihr Verhalten Ihnen gegenüber zu ändern.

Und das kann dann so aussehen: Kunden wenden sich ab, Zulieferer kooperieren nicht mehr und verknüpfte IT-Partner kappen die Verbindungen. Mitarbeitende erwägen Kündigungen, potenzielle Kandidaten bewerben sich nicht. Das alles hängt damit zusammen, wie sehr diese Stakeholder Ihnen eine Verantwortung für die Auswirkungen der Krise zuschreiben. Wenn andere also glauben, dass Sie einer Bewältigung nicht gewachsen sind oder eine erneute derartige Krise nicht verhindern können, wird die Krise umso gravierender.

iX-TRACT

- Kommunizieren in einer Krise bedeutet nicht nur Kommunizieren in einer Ausnahmesituation; man muss sich zudem mit vielen, teilweise einander widersprechenden Interessen auseinandersetzen.
- Wie in anderen Bereichen gilt auch bei der Kommunikation: Je besser ein Unternehmen vorbereitet ist, etwa mit ausgedruckten Listen aller notwendigen Kontaktstellen und Ansprechpartner, desto besser kann es in der Krise kommunizieren.
- Gute und kluge Kommunikation während einer Krise kann verlorenes Vertrauen wieder zurückgewinnen und dafür sorgen, dass ein Unternehmen mit einem blauen Auge davonkommt. Dazu gehört aber auch der glaubwürdige Nachweis, dass alles unternommen wird, um kein weiteres Mal in eine solche Krise zu schlittern.

Diese Zuschreibung von Verantwortung hängt von vielem ab, beispielsweise vorhandenem Vertrauen, der öffentlichen Meinung oder den Handlungen der Organisation. Das heißt auch, Sie können diese Wahrnehmung positiv beeinflussen und diese Gespräche innerhalb Ihrer Anspruchsgruppen mitgestalten, indem Sie die Erwartungen kennen und bestmöglich erfüllen sowie per Prozesskommunikation offen, transparent und zuverlässig darüber kommunizieren. Sie betreiben Enttäuschungsmanagement.



Mit dem Vier-Räume-Modell lässt sich der zeitliche Horizont von der Zeit vor dem Angriff bis in die Zukunft hinein abbilden; den einzelnen Phasen lassen sich dann die darin ergriffenen Maßnahmen zuordnen.

Plötzlich wollen alle mit Ihnen reden

Ob bei einer Störung, einem Notfall oder einer Krise: Wenn die Dinge nicht so laufen, wie sie sollten, brauchen Organisationen einen Plan, auf den sie zurückgreifen können. Und dieser Plan muss unternehmensweit funktionieren. Abteilungen müssen also gemeinsam entscheiden, agieren und kommunizieren. Das tun sie im Rahmen des Krisenstabs, für den es bestenfalls definierte Rollen und Prozesse gibt.

Informationsbeschaffung, Erfassung und Bewertung der aktuellen Lage, Entwicklung von Handlungsoptionen und Bewertung von Erfolgsaussichten – all das findet im Krisenstab statt. Dieses Gremium stimmt Maßnahmen ab und trifft operative sowie kommunikative Entscheidungen. Und wenn Sie Mitglied dieses Krisenstabs sind, werden häufig fragende Augen auf Sie gerichtet sein. In dem Moment, in dem Sie eigentlich in Ruhe und mit klarem Fokus arbeiten müssten, wollen sehr viele Menschen, die Sie vielleicht noch nie gesehen haben, plötzlich sehr dringend mit Ihnen reden: in der Lagebesprechung des Krisenstabs, 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 mit den nachfolgend dargestellten Parteien kommunizieren oder zumindest dabei unterstützen müssen.

Human Resources: Eine der ersten Fragen, die an Sie herangetragen wird, ist die nach der Arbeitsfähigkeit der Mitarbeitenden. Wenn die üblichen Aufgaben nicht erledigt werden können, müssen die Teams dann überhaupt zur Arbeit erscheinen? Wie erledigen sie ihr 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? Auch hierfür können und sollten die Verantwortlichen relativ zügig eine Richtung vorgeben. Je mehr Infos dazu schnell und proaktiv herausgehen, umso weniger Rückfragen werden an Sie und alle anderen Verantwortlichen herangetragen.

Datenschutzbeauftragte und Juristen: Zur Runde der Fragesteller gesellen sich (interne oder externe) juristische Verantwortliche, und das ziemlich zügig, da die Meldeuhr unerbittlich tickt. Ob Sie KRITIS-Betreiber sind und entsprechend gesetzliche Regelungen zu beachten haben, darüber haben Sie ja sicherlich schon jetzt und hier ausreichend Klarheit, oder? Ob Sie Auftragsverarbeiter oder Verantwortlicher im Sinne der DSGVO sind und wen Sie bei einem potenziellen Verlust personenbezogener Daten informieren müssen, wissen Sie oder Ihre Kollegen hoffentlich auch. Und die Kontaktdaten von LKA und ZAC sind in einem Papierordner abgeheftet? Super, dann können Sie zumindest an die Behördengruppe schon mal beruhigt einen Haken setzen.

Externe Spezialisten: Sofern Sie sich entscheiden, im Bereich Forensik und Wiederaufbau mit externen Spezialisten zusammenzuarbeiten, müssen diese koordiniert werden. Mal ganz abgesehen von den inhaltlichen, operativen Herausforderungen müssen Sie also organisatorische Aspekte bedenken: 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: Danach wartet schon die nächste Herausforderung: Wenn Sie im Krisenstab über Ihren Arbeitsbereich berichten, wird das unter Umständen nicht jeder verstehen. Das hat seine Ursachen nicht in bösem Willen, sondern schlicht darin, dass ein Verständnis für Ihre Prozesse und Zuständigkeiten, für technische Aspekte oder auch die Tragweite der Situation fehlt.

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 gegebenenfalls auch eine „Übersetzung" dieser Fakten von IT-Deutsch in DAU-Deutsch. Hier hat es sich in der Praxis als hilfreich erwiesen, wenn die benannte Runde auch schon vor Krisenfällen öfters mal beisammengesessen und sich ausgetauscht hat.

Auch das ist ein Impuls, den man an andere Abteilungen weitergeben kann: Wer sich in Friedenszeiten kennen- und verstehen lernt, kann den Ausnahmezustand besser bewältigen. Wer in ruhigem Fahrwasser gemeinsam mit den wichtigsten Verantwortlichen definiert, welche Daten die „Kronjuwelen" des Unternehmens sind, muss in der Krise nicht erst zeitaufwendige und nervenaufreibende Entscheidungsfindungen vorantreiben. Und er tut sich leichter damit, benötigte Budgets und Ressourcen (für Hardware, Lizenzen, externe Dienstleister, zusätzliche Mitarbeiter et cetera) zeitnah einzuholen. Fragen nach funktionierenden Backups, dem Wiederanlauf der Systeme oder zumindest den wichtigsten Daten stellen sich übrigens auch mit dem Hintergrund, ob man auf die Kontaktaufnahme der Erpresser eingehen muss – auch das ist eine Entschei-

Checkliste für gutes Krisenmanagement und Erfolg versprechende Krisenkommunikation

- Vergewissern Sie sich, dass abteilungsübergreifende Krisenstrukturen existieren und wichtige Prozesse immer geübt werden. Reden Sie darüber mit den anderen Abteilungen.
- Sorgen Sie dafür, dass alle wichtigen Ansprechpartner die Rolle der IT sowie die Bedeutung Ihrer IT-Landschaft und der Hauptanwendungen für ihren Arbeitsbereich verstehen. So wissen die Beteiligten im Ernstfall, welche Konsequenzen ein Ausfall hat und wie sie diese an wen kommunizieren müssen. Auch hierzu sollten Sie sich mit den anderen Abteilungen abstimmen.
- Definieren Sie die Qualität, Relevanz und Priorität Ihrer Daten (für Aufrechterhaltung des Geschäftsbetriebs, in Hinblick auf DSGVO et cetera). Tun Sie dies in nachvollziehbarer Form und mit entsprechenden Begründungen. Dies hilft Ihnen im Ernstfall, schnelle und belastbare Entscheidungen zu treffen. Reden Sie auch über dieses Thema mit den anderen Abteilungen.
- Bedenken Sie beim Thema Redundanzen nicht nur Ihre Backups, sondern auch Kommunikationsmittel und -kanäle (ausgedruckte Listen mit privaten Mailadressen und Handynummern der wichtigsten Kontakte, webbasierte Tools zum kollaborativen Arbeiten und so weiter).
- 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 Hintergrundinformationen, Muster für Pressemitteilungen, Holding Statements, Sprechzettel und FAQ vorbereiten. So wissen im Ernstfall alle, auf welche einheitlichen Wordings sie zurückgreifen können, um intern und extern mit einer Stimme zu sprechen.
- 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.

Auf materieller und unternehmensstrategischer Ebene können Sie mit den genannten Maßnahmen den Handlungsspielraum Ihrer Organisation in der Krise erweitern und dazu beitragen, den Schaden zu minimieren. Und auch auf der persönlichen Ebene hilft Ihnen das Genannte: Indem Sie besonnen agieren, können Sie und Ihr Team belastbare Entscheidungen treffen und zielgerichteter arbeiten. Wenn Sie gut vorbereitet sind, können Sie vor der Krise besser schlafen – und bestenfalls während der Krise auch.

dung, die in beträchtlichem Maße von Ihnen abhängen kann.

Kundenmanagement und Kommunikationsverantwortliche: Die wenigsten von Ihnen operieren im Tagesgeschäft im luftleeren Raum – von den Produkten oder Dienstleistungen Ihrer Organisation hängen Kunden, Partner, Zulieferer und weitere Anspruchsgruppen ab. Sie alle sollten davon erfahren, wenn es bei Ihnen längerfristige Technikprobleme oder -ausfälle gibt. Sofern es eine Kommunikations- oder Marketingabteilung gibt, müssen Sie also auch dieser im Krisenstab Rede und Antwort stehen, damit sie ihren Job machen kann. In anderen Fällen wird die Kommunikation direkt über die Geschäftsführung oder das Kundenmanagement laufen. Die Herausforderung für Sie bleibt die gleiche: Sie müssen eine Perspektive liefern, wie es weitergeht. Nennen Sie diese „Zeitplan“ und bringen Sie sie zu jeder Krisensitzung mit.

Die Zauberwaffe „Zeitplan“

Es ist völlig nachvollziehbar, wenn Sie an Tag eins 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 dem Krisenstab mit. Alle, mit denen Sie reden müssen und die wiederum mit anderen Personengruppen reden müssen, benötigen nichts dringender als eine Perspektive – für die kommenden Stunden, Tage, Wochen oder schlimmstenfalls auch Monate.

Sie müssen die Hoheit über Zeitpläne haben. Denn damit steuern Sie, wie Ihr Unternehmen in dieser Krise wahrgenommen wird und ob man ihm die Bewältigung dieser Notlage dauerhaft zutraut oder nicht. Erinnern Sie sich an die Erwartungen der Stakeholder, die zum Einstieg des Textes beschrieben wurden: Eine fundamentale Forderung aller internen und externen Anspruchsgruppen ist, dass Sie jetzt, im Krisenfall, alles vorbildlich richtig machen, um nicht noch einmal zu enttäuschen. Und dazu gehört eben auch die Antwort auf die schlichte, aber wichtige Frage: „Wann funktioniert wieder alles?“

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 Infos 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, die ersten Systeme in einer Woche wieder an den Start zu bekommen? Kommunizieren Sie anderthalb Wochen – irgendetwas wird ganz sicher schiefgehen. Warten alle auf eine Lösung innerhalb einer Woche, haben Sie unter Umständen die nächste Enttäuschung generiert. Schaffen Sie das Unmögliche (oder Unerwartete) und können schon eher liefern – umso besser, Freude bei allen Beteiligten.

Transparenz über Transaktionen?

Bleibt die Gretchenfrage nach der Transparenz – besonders relevant für eine Anspruchsgruppe, die bisher noch völlig außen vor blieb, die Medien. Die engagierte Lokaljournalistin, die mit dieser Erpressung durch Cyberkriminelle die ganz große Story wittert und nach der Lösegeldsumme fragt, der eigentlich ganz nette Blogger aus Ihrem IT-Forum, der wissen will, warum nicht einfach die

Backups wieder eingespielt wurden, oder die Fachzeitschrift, die nun endlich mal Infos zum forensischen Bericht möchte. Auch solche Stakeholder werden sich melden und mehr oder weniger freundlich um Auskunft bitten.

Hier müssen Sie gemeinsam mit Ihren Kolleginnen und Kollegen aus der Kommunikation taktisch klug vorgehen. Zu viele öffentliche Informationen, beispielsweise über sensible Sicherheitsaspekte oder Geschäftsgeheimnisse, sind unter Umständen kontraproduktiv. Zu wenig Infos wiederum können als Verschleierung öffentlichkeitsrelevanter Fakten interpretiert werden. Hier gilt es, gemeinsam mit den entsprechenden Experten eine grundlegende Kommunikationsstrategie zu definieren und konsequent umzusetzen.

Die gute Nachricht: Es gibt auch Bereiche, bei denen Sie aus dem Vollen schöpfen können. Alle Karten, die überzeugend vermitteln, dass Sie dafür sorgen, dass sich ein solcher Vorfall nicht wiederholt, sollten auf den Tisch. Damit lässt sich Vertrauen generieren. Denn noch besser als eine elegant formulierte Entschuldigung funktioniert der glaubhafte Nachweis von Bemühungen, dass sich diese Situation nicht wiederholt. Hier kann es sinnvoll sein, mit dem Vier-Räume-Modell zu argumentieren (siehe Abbildung).

Das Vier-Räume-Modell hat bei einem Ransomwareangriff folgende Ebenen:

1. Welche Maßnahmen wurden in der Vergangenheit ergriffen, damit ein solcher Fall nicht eintritt: EDR, Firewalls, Patch- und Berechtigungsmanagement, Pentests, Mitarbeiterschulungen. Alles, was Sie getan haben, kann bei der Argumentation hilfreich sein und lässt sich auch schon vor Eintreten des Worst Case gut dokumentieren. Führen Sie also kontinuierlich Listen über Ihre Präventionsmaßnahmen und halten Sie sie aktuell. Das erspart im Krisenfall Zeit und Nerven.
2. Welche Maßnahmen wurden zum Zeitpunkt des Incidents ergriffen: Einrichtung eines Krisenstabs, Hinzuziehen von IT- und weiteren Experten, Meldung an die Behörden und so weiter.
3. Welche Konsequenzen werden aus dem Vorfall gezogen: Optimierung des Berechtigungsmanagements, Erhöhung der Sicherheitsvorkehrungen, präventive Pentests, weitere Schulungen et cetera.
4. Was wäre Utopie: Eine hundertprozentige Sicherheit gegen solche Angriffe – die gibt es nicht.

Verbündete im Notfall

Das waren jetzt jede Menge kommunikative Aufgaben – und dabei wollen Sie doch eigentlich nur eins: in Ruhe arbeiten. Ihr Verbündeter ist in diesem Fall ein guter Krisenmanager. Er hält Ihnen den Rücken frei, damit Sie Ihren Notfallplan abarbeiten können, anstatt in endlosen Meetings Dutzende Erklärschleifen zu drehen. Ein Krisenmanager kann umso besser mit Ihnen und für Sie arbeiten, je besser Sie auf ein solches Szenario vorbereitet sind und je mehr Infos Sie schnell und verlässlich liefern können, die dann intern und extern weitergegeben werden.

Ein weiterer Benefit: Mit gutem Krisenmanagement können Sie den gleißend hellen „Die IT ist schuld“-Scheinwerfer von sich abwenden. Eine Vorbereitung auf und die Bewältigung von Cyber Incidents ist dann am erfolgreichsten, wenn sie über Einzelbereiche wie IT, BCM, Legal und Kommunikationsabteilungen hinausgedacht und umgesetzt wird. In anderen Worten: Krisenprävention, -management und -kommunikation sind interdisziplinäre Managementprozesse. Je eher sich alle Verantwortlichen darüber bewusst werden, umso besser läuft es im Ernstfall.

Zusammengefasst: Gelingt es Ihnen und Ihren Teams, das Vertrauen der Stakeholder in Ihre Krisenmanagementfähigkeiten durch kluge Kommunikation zu erhalten, stehen die Chancen gut, unbeschadet oder zumindest mit geringerem Reputationsverlust durch die Krise zu kommen. 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 Ransomwareangriff der letzte Akt war, der ein Unternehmen in die Insolvenz getrieben hat, gibt es leider einige. (ur@ix.de)

JANKA KREISSL

ist Senior-Beraterin bei Dunkelblau und unterstützt mit ihrem Team Unternehmen und Organisationen, die Opfer von Ransomwareangriffen wurden, im Bereich Krisenmanagement und -kommunikation.