LEITFADEN

Krisenkommunikation

Organisation der Kommunikation im Krisenfall

Dr. Helmut Merschmann, Vitako
Stand: Juni 2012

VITAKO
Bundes-Arbeitsgemeinschaft der
Kommunalen IT-Dienstleister e.V.

Inhalt

1. Vorwort

Stromausfall, Datenverlust, Hackerangriff – vor einem Krisenfall ist kein Unternehmen, auch kein öffentlicher IT-Dienstleister, gefeit. Nach einer aktuellen Bitkom-Untersuchung zur Cyber-Sicherheit in der deutschen IT-Wirtschaft erkennen 57 Prozent aller Unternehmen Angriffe auf ihre IT-Systeme als reale Gefahr. 40 Prozent haben bereits konkrete Angriffe auf die IT oder vergleichbare Sicherheitsvorfälle erlebt, 10 Prozent sogar häufiger als zehn Mal. Die Angriffe betreffen Attacken auf vertrauliche Daten, elektronische Prozesse und digitale Identitäten sowie Online-Spionage und Sabotage. Sie können die Handlungsfähigkeit von Verwaltungen und Unternehmen erheblich einschränken. Da muss es verwundern, dass nicht einmal jedes zweite Unternehmen einen Notfallplan für derartige Fälle hat.

Umso wichtiger erscheint es, geeignete Vorüberlegungen und Vorkehrungen zu treffen, um einer Krise im Fall der Fälle souverän begegnen zu können. Da es in einem Krisenfall wichtig ist, alle Verantwortlichen auf den gleichen Informations- und Wissensstand zu bringen, erhält die Krisenkommunikation eine besondere Relevanz. Die Abläufe und Verantwortlichkeiten müssen intern, manchmal auch mit externen Partnern abgestimmt werden. Auch Medien, Kunden und betroffene Bürger sollten umfassend, aktuell, widerspruchsfrei und wahrheitsgemäß über den Krisenfall, die Gründe und Auswirkungen unterrichtet werden. Krisenkommunikation ist daher Teil des Krisenmanagements.

Dieser „Leitfaden Krisenkommunikation“ will den Vitako-Mitgliedern Kommunikationsstrategien und Handlungsempfehlungen für den Krisenfall an die Hand geben. Er umfasst einige typische Krisenszenarien, von denen öffentliche IT-Dienstleister betroffen sein können, eine Aufstellung der möglicherweise beschädigten Infrastruktur, Handlungsempfehlungen zur Teambildung und zur Kommunikationsstrategie sowie Hinweise zu einzelnen Verfahrensabläufen.

Krisenkommunikation ist eine wesentliche Aufgabe der Führungskräfte, sozusagen „Chefsache“. In der Regel entscheidet ein Krisenstab, welche Informationen nach außen gelangen. Generell ist zu bedenken, dass es kontraproduktiv ist, Tatbestände zu

vertuschen oder zu verschweigen. Die Liste misslungener Krisenkommunikation ist lang. Fast immer ‘fliegt die Sache auf‘ und die Wahrheit kommt ans Licht. Dann stehen die Verantwortlichen meist nicht sehr gut da.

Das Ziel gelungener Krisenkommunikation ist es, Vertrauens- und Imageverluste zu vermeiden oder Vertrauen wieder herzustellen. Hierzu ist eine kontinuierliche und glaubwürdige Kommunikation notwendig. Dass eine kleinere oder größere Störung passieren kann, dafür haben die meisten Menschen Verständnis. Unternehmen werden allerdings daran gemessen, wie sie im Krisenfall handeln. Eine kontrollierte Selbstkritik und das Eingeständnis von Fehlern wirken vertrauensbildend. Schnelles, proaktives Handeln wird positiv bewertet. Ebenso Offenheit und Transparenz – zwei wichtige Parameter für die Öffentlichkeit, um sich ein Bild vom Störfall zu machen. Je nachvollziehbarer die Schilderung einer Störung und der eingeleiteten Gegenmaßnahmen ist, desto größer die Bereitschaft, an Schadensbegrenzung und die Bewältigung der Krise zu glauben.

2. Krisenfälle/ Szenarien für öffentliche IT-Dienstleister

Nicht jeder Störfall ist eine Krise. Von einer Krise ist erst zu sprechen, wenn dauerhafter Schaden eingetreten ist oder sich ankündigt, von dem nicht nur das Unternehmen selbst betroffen ist, sondern auch Kunden, die Öffentlichkeit und externe Verantwortliche (Aufsichtsrat, politische Entscheider usw.). Alle internen Vorfälle, die nicht innerhalb kurzer Zeit behoben werden können, und alle Vorfälle mit unmittelbaren Konsequenzen für Außenstehende sind als Krisenfälle zu begreifen und zu behandeln: sie müssen nach außen kommuniziert werden.

Im Folgenden zeigen wir einige **Krisenszenarien** auf, von denen öffentliche IT-Dienstleister betroffen sein können:

- Worst-Case-Szenario: Kompletter Stromausfall, Brand, Außenschäden am Rechenzentrum mit Evakuierung, Personenschaden, Pandemie, Explosion und so weiter. Hierbei muss davon ausgegangen werden, dass die gesamte technische

Infrastruktur im Rechenzentrum und in der Geschäftsstelle eines IT-Dienstleisters nicht mehr funktionsfähig oder zumindest in Teilen betroffen ist. Verkehrswege können unterbrochen sein, die IP-Telefonie gestört, auf das Inter- und Intranet kann nicht mehr zugegriffen werden. Dies hat zur Folge, dass auch alle externen Partner in Verwaltungen nicht mehr auf Daten und Dienste zugreifen können oder diese unter Umständen sogar verloren gegangen sind.

- Störung der Verfügbarkeit von Fachverfahren oder der IT-Infrastruktur: Durch einen Störfall, etwa einen Brand im Rechenzentrum, kann auf einzelne Fachverfahren oder Daten nicht mehr zugegriffen werden. Verwaltungsmitarbeiter können demzufolge nicht mehr ihre Aufgaben erfüllen und beispielsweise Kunden bedienen. Auch der Zusammenbruch einer Datenleitung mit Auswirkungen auf die Verfügbarkeit von Daten und Diensten oder der Ausfall von notwendigen Materiallieferungen fallen unter dieses Szenario. Es kommt daher zumindest zu einer zeitlichen Verzögerung von Diensten – solange bis der technische Schaden behoben worden ist

- Störung der Vertraulichkeit durch Datendiebstahl oder Datenverlust: Kommt es zu einem Datenverlust durch Datendiebstahl oder Hacking und werden zum Beispiel Meldedaten aus dem Melderegister im Internet veröffentlicht, so ist das Vertrauen der Öffentlichkeit in die technische Sicherheit von personenbezogenen Daten beim IT-Dienstleister ernsthaft beschädigt. Die öffentliche Sensibilität für den Datenschutz ist in diesem Szenario größer als bei einem Wirtschaftsunternehmen mit Datenleck. Die Messlatte für einen öffentlichen IT-Dienstleister hängt höher, wodurch umfangreiche vertrauensbildende Maßnahmen notwendig werden.

- Störung der Integrität (bspw. bei Korruption durch eigene Mitarbeiter): In diesem Szenario dringen interne Informationen oder Daten nach außen. Sei es, dass ein „Whistleblower“ die Presse über interne Missstände informiert oder ihr Datenbestände zugespielt. Oder sei es, dass Daten manipuliert werden,

beispielsweise Personalabrechnungen. In beiden Fällen hat die Integrität des Unternehmens im Ansehen der Öffentlichkeit Schaden erlitten oder ist zumindest gefährdet.

- Streik, Demonstrationen: Bei (angekündigten) Streiks und Demonstrationen ist unter Umständen ebenfalls von einem Krisenszenario zu sprechen – und zwar dann, wenn nicht genügend Personal für die Aufrechterhaltung des Geschäftsbetriebs zur Verfügung steht und die gewohnten Dienstleistungen nicht erbracht werden können.

- „Shitstorm" in Sozialen Medien: Hierbei bilden sich in sozialen Netzwerken (Facebook, StudiVZ etc.) oder den Social Media (Twitter, Youtube) Interessensgruppen, die einen tatsächlichen Fehler/Schaden publik machen oder Rufmord betreiben wollen. Es werden dann geeignete Kommunikationsmaßnahmen (im selben Medium!) notwendig, um den Imageschaden zu begrenzen.

In allen Szenarien ist es notwendig, einen **Krisenstab** einzuberufen, der aus Personen besteht, die den Betrieb aufrechterhalten können. In der Regel wird dies der Geschäftsführer oder Vorstand sein, ein technischer Leiter, einige Fachberater aus verschiedenen Abteilungen, ein Sprecher aus der Abteilung Öffentlichkeitsarbeit sowie weiteres zuarbeitendes Personal in der Telefonzentrale, Pressestelle und Rechenzentrumstechnik.

3. Betroffene und notwendige Infrastrukturen

Von einem Krisenfall kann die hausinterne technische Infrastruktur in unterschiedlichem Ausmaß betroffen sein. Auf der Basis einer spezifischen Fallanalyse muss zunächst bestimmt werden:

- Welche technischen Systeme sind ausgefallen beziehungsweise gefährdet? Welche funktionieren noch?

Es empfiehlt sich hierbei, Störfalle durch andere technische Abteilungen gegenprüfen zu lassen, um ein verlässliches Bild über das Ausmaß der Situation zu erhalten.

Beispielsweise können der gesamte Rechenzentrumsbetrieb in Mitleidenschaft gezogen sein, einzelne Fachverfahren nicht mehr funktionieren, die Datenverbindung zu den Kunden unterbrochen sein, oder – beim Worst-Case-Szenario –es kann zu einem Zusammenbruch aller IP-getriebenen Geräte kommen, einem Totalausfall. Bei einem Teil der LÜKEX-Übungen Ende 2011 ist dieses Szenario nachgestellt worden. Die „Länderübergreifende Krisenmanagement-Übung/EXercise“ konzentrierte sich besonders auf die Zusammenarbeit und Koordination mehrerer Organisationen. Damit stand die Krisenkommunikation im Mittelpunkt.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat bereits im Jahr 2008 den Grundschutzstandard 100-4 „Notfallmanagement“ herausgegeben. Darin wird ein systematischer Weg aufgezeigt, um ein Notfallmanagement in einer Behörde oder einem Unternehmen aufzubauen und die Kontinuität des Geschäftsbetriebs im Krisenfall sicherzustellen. Daran anlehnend haben viele öffentliche IT-Dienstleister ein Notfallhandbuch und einen Notfallkoffer mit den nötigsten Kommunikationsmedien gepackt.

Am Beispiel des Worst-Case-Szenarios lassen sich die notwendigen Vorüberlegungen gut schildern. Wenn die üblichen Kommunikationswege unterbrochen sind, stellt sich die Frage: Mittels welcher Ersatztechnologien kann die externe Kommunikation aufrechterhalten werden? Überlegenswert ist daher, sich folgende Infrastrukturen anzuschaffen:

- analoge Telefone (Posthauptanschlüsse)
- X400-Faxgeräte (analog), möglich zwei Geräte (in/out)
- Mobiltelefone, Smartphones, Tablet-PCs, ggf. Satellitentelefon
- UMTS-Schnittstellen/ Surfstick (Handy, PC)
- Dark Site (bei externem Dienstleister oder in anderen RZ-Standorten) als Ersatz für die ausgefallene eigene Website?
- ggf. BOS-Digitalfunk („Behörden und Organisationen mit Sicherheitsaufgaben“)

- Megafone, Batterien
- Materialien für Aushänge, Handzettel, Flyer, Plakate
- (geschlossene) Twitter-/ Facebook-Gruppen (interne und externe Kommunikation)
- Botendienste (Fahrradkuriere etc.)

Wenn nicht sämtliche technischen IP-Systeme ausgefallen sind, bietet sich durchaus auch Kommunikation über Videokonferenzsysteme (beispielsweise zwischen verschiedenen Firmenstandorten) an. Dieses Szenario wurde ebenfalls auf der LÜKEX-Übung 2011 durchgespielt und erwies sich als besonders geeignet für die Kommunikation zwischen mehreren betroffenen Krisenstäben, etwa in verschiedenen Bundesländern.

Da der Grund für den Krisenfall nicht immer zeitnah behoben werden kann und das Krisenteam möglicherweise länger mit der Lösungsfindung befasst ist, wird zusätzliche Infrastruktur erforderlich:

- Dienst- und Ablösepläne
- Catering-Service
- Arbeits- und Ruheräume (für Team, Presse, Verantwortliche)
- technischer Support (Computer-Notfallteams, CERT)
- PC-Arbeitsplätze im Notfall-Raum
- Ladegeräte für Mobiltelefone und PCs
- Flipchart, Büromaterialien
- Akkudrucker
- Notfallkoffer samt Notfallhandbuch mit Telefonnummern und E-Mail-Adressen der intern Zuständigen sowie der Partnerorganisationen (Verwaltungen etc.)
- Presseverteiler mit Telefonnummern und E-Mail-Adressen von überregionalen, regionalen und lokalen Medien

Die letzten beiden Punkte in dieser Liste müssen regelmäßig aktualisiert werden, damit die Kontaktangaben auf dem neuesten Stand bleiben. In der Praxis bewährt hat sich die halbjährliche Datenpflege und Überprüfung der Kontaktadressen.

4. Krisenkommunikationsplan

Krisenkommunikation bezeichnet die Öffentlichkeitsarbeit von Organisationen in einer Krisensituation und erfordert eine klare Verteilung von Zuständigkeiten und Verantwortlichkeiten. Sie umfasst die umgehende Information aller direkt oder indirekt betroffenen Gruppen.

Hierbei ist zwischen interner und externer Krisenkommunikation zu unterscheiden. Die interne Krisenkommunikation ist die Kommunikation innerhalb des Krisenstabs beziehungsweise unter den Verantwortlichen in Rechenzentrum, Behörden und Politik. Die externe Krisenkommunikation richtet sich die Öffentlichkeit. Ziel ist es, die Krise möglichst effektiv zu bewältigen und eine Eskalation zu vermeiden. Vertrauen, Glaubwürdigkeit und Akzeptanz sollen so schnell wie möglich (wieder) hergestellt werden.

Vor allem die Kommunikation mit Presse und Öffentlichkeit (in Form von Informationen, Hinweisen, Erklärungen, Warnungen, Entschuldigungen, Verhaltensregeln und Maßnahmenbeschreibungen) muss unverzüglich geschehen: sachgerecht, umfassend, wahrheitsgetreu und transparent. Nach außen gerichtete Informationen müssen widerspruchsfrei, verständlich und verifizierbar sein.

Ein **Krisenkommunikationsplan** ist das zentrale Dokument für den Ernstfall, er ist im Vorfeld zu erstellen und soll schnelles Handeln garantieren. Als eine Art Handlungskatalog mit Regieanweisungen für die in der Krisenkommunikation agierenden Mitarbeiter beschreibt der Krisenkommunikationsplan im Detail die PR-relevante Vorgehensweise während eines Krisenfalls:

- Festlegung der Kommunikationsstrategie (Wer soll angesprochen werden?)
- Festlegung des inhaltlich und argumentativ einheitlichen Auftretens (Was soll gesagt werden?)
- Definition der qualitativen (etwa Imageverlust vorbeugen) und quantitativen Kommunikationsziele (Festlegung der Zeitabstände zwischen Meldungen)
- Start der Meldeketten und Priorisierung von anzusprechenden Zielgruppen und Personen (Politik - Medien - Kunden)

- Auflistung der verfügbaren Instrumente für die Krisenkommunikation (Welche analogen und digitalen Medienkanäle stehen zur Verfügung?)
- Zuweisung von Rollen, Zuständigkeiten und Verantwortlichkeiten (Sprecher, „Krisengesicht“, Zuarbeiter, Entscheider)
- Entwicklung eines Handlungskatalogs für die Krisenkommunikation („Regieanweisungen“, Sprachregelungen, Pressemeldungen, Recherche von Sach- und Fachfragen, Produktion von O-Tönen)
- Konzept zur Einbindung der Medien in die Krisenarbeit (Fernsehen, Rundfunk, Printpresse, Online-Medien, Soziale Medien)
- Konzept zur Medienbeobachtung (Wie wird berichtet, und wie lässt sich die Berichterstattung gegebenenfalls korrigieren?)
- Wichtig: Umfassende Dokumentation des Krisenverlaufs durch minutiöse Protokolle (Krisen-Logbuch); Aufzeichnungen der nach außen gegebenen Informationen (Bild, Ton, Text).

5. Kommunikationsregeln

Die Hauptregel im Krisenfall lautet: **Nur einer spricht!** Auch wenn mehrere Ressorts oder Organisationen (IT-Dienstleister und Verwaltung) involviert sind, sollte die Kommunikationsarbeit bei nur einem Sprecher liegen, dem „Krisengesicht“. Auf diese Weise können Widersprüche vermieden werden für den Fall, dass die Presse nachrecherchiert und mit weiteren Personen in Kontakt tritt.

In vielen Fällen wird das „Krisengesicht“ ein Vorstandsmitglied oder der Geschäftsführer sein. Überlegenswert ist jedoch auch, einen Pressesprecher solange „an die Front“ zu schicken, bis eine Lösung gefunden wurde und das Ende der Krise in Sicht ist. Dies verkündet dann der Vorstand oder ein Politiker. Ein solches Vorgehen erfordert naturgemäß eine präzise Abstimmung darüber, welche Informationen nach außen gelangen und welche nicht.

- In der Praxis sollten beim Telefonieren unterdrückte Nummern verwendet werden, damit immer nur eine Person zu erreichen ist: der offizielle Sprecher.

Die Autorisierung von Informationen, Pressemitteilungen, Hinweisen für die Dark Site usw. erfolgt durch den Leiter des Krisenstabes, der selbst nicht als Sprecher auftritt. Nur der Sprecher gibt Informationen nach außen. Weitere Mitarbeiter unterliegen einer Schweigepflicht oder befolgen einen Gesprächsleitfaden, was insbesondere hinsichtlich Rückfragen durch die Presse vorteilhaft ist. Interne Sprachregelungen und Textschablonen können via Intranet und Mail verbreitet werden – sofern diese noch funktionieren. Ansonsten gehören sie in das Krisenhandbuch.

Falls es sich der Geschäftsführer oder ein Vorstand nicht nehmen lassen will, der Öffentlichkeit Rede und Antwort zu stehen, sollte er sich darauf konzentrieren, Lösungen zu verkünden und das Vertrauen in das Unternehmen zu stärken. Währenddessen konzentriert sich ein Pressesprecher auf die Probleme und Schwierigkeiten in der Krise.

- Wichtig dabei: Niemals allein auftreten, eine Begleitperson, die auf Fehler oder Versprecher aufmerksam macht und als eine Art Zeuge agiert, sollte stets dabei sein.

Des Weiteren gelten folgende Regeln:

- Offen, ehrlich und transparent informieren (aber nicht immer vollständig)
- Nur Fakten kommunizieren! Den Sachstand zusammenfassen, das Geschehen erklären, die Folgen aufzeigen, die Ursachen (sofern bekannt) benennen.
- Fehler eingestehen, nicht verschieben
- Sachverhalte klären, nicht Schuldige suchen
- Den Sprachduktus der Zielgruppe anpassen und allgemein verständlich sprechen. Vorsicht mit vielen technischen Fachtermini!
- Verantwortliche gemäß Priorität informieren: Vorstand, Mitarbeiter, Gesellschafter/Politik, Datenschutzbeauftragter, Kunden, Öffentlichkeit

- Proaktive und möglichst zeitnahe Kommunikation (30-60 Minuten nach Schadensfall)
- Informationsfluss aufrechterhalten: nach der Erstmeldung neue Informationen ohne Verzögerung weitergeben. Dabei immer die zeitliche Entwicklung klarstellen („Heute um 12.30 Uhr…“)
- Falls eine Pressekonferenz notwendig erscheint, sollte sie innerhalb 24 Stunden einberufen werden.

6. Umgang mit Presse- und Medienvertretern

Medienvertreter interessieren sich vor allem für Antworten auf folgende fünf Fragen:

- Was ist passiert?
- Was sind die Gründe für die Krise?
- Welche Maßnahmen zur Krisenbewältigung sind eingeleitet worden oder geplant?
- Wer ist verantwortlich?
- Kann sich die Krise wiederholen?

Auf diese Fragen muss man vorbereitet sein, am Besten in Form eines regelmäßigen **Medientrainings**, bei dem ein Krisenfall simuliert und die dazugehörige Krisenkommunikation geübt wird. Videokonferenzsysteme eignen sich dazu gut, aber auch allgemeines Training vor der Kamera und dem Mikrofon. Das „Krisengesicht“ soll glaubwürdig, vertrauensvoll und authentisch „rüberkommen“. Je geübter ein Sprecher (oder Geschäftsführer) darin ist, umso leichter fällt es, in der Krisensituation souverän zu agieren.

Einen guten **Umgang mit Presse- und Medienvertretern** zeichnen darüber hinaus folgende Punkte aus:

- frühzeitiger Aufbau und kontinuierliche Pflege eines Netzwerks mit lokalen, regionalen und überregionalen Medienvertretern und Journalisten

- dauerhafte Netzwerkarbeit durch Medienpartnerschaften oder Kontaktgespräche
- Handlungsempfehlungen/„Regieanweisungen“ und Sprachregelungen für den Erstkontakt mit Medienvertretern bei einem Krisenereignis
- frühzeitiges Auftreten und Präsenzzeigen von Entscheidungsträgern
- Bereithalten von Hintergrundinformationen (Bilder, Grafiken, Texte, Statistiken oder Aufgabenbeschreibungen)
- Vorbereitung von Sprechzetteln, Pressemitteilungen, Fragen und Antworten, Argumentationsketten
- Sammlung wertvoller Erfahrungen im Umgang mit Presse- und Medienvertretern durch eine kontinuierliche Presse- und Öffentlichkeitsarbeit (zum Beispiel Durchführung von Interviews, Pressekonferenzen)

7. Spezialfall: Social Media

Einen Spezialfall der Krisenkommunikation bilden die Sozialen Medien. Wann immer sich ein sogenannter „Shitstorm“, das heißt ein rhetorischer Angriff im Web 2.0 ereignet, heißt es: Schnell handeln! Das Problem bei Sozialen Medien ist, dass sich die Zahl der kritischen oder diffamierenden Stimmen binnen kürzester Zeit rasend schnell vermehren kann. Die Kommunikationsstrategie muss hier besonders sorgfältig sein, da Rede und Gegenrede unmittelbar und sichtbar aufeinander folgen. Zudem haben soziale Medien wie Facebook, Twitter und Blogs schnell eine relevante Reichweite erlangt, so dass die Themen von etablierten Print- und Online-Medien aufgegriffen werden. Denen wäre es jedoch lieber, direkt informiert zu werden – entsprechend argwöhnisch kann ihre Reaktion ausfallen.

Folgende Punkte sind im Umgang mit Sozialen Medien zu beachten:

- **Geschwindigkeit:** Krisenkommunikation im Netz muss schnell sein. Zumindest das Eingeständnis eines Fehlers oder einer Störung sollte sofort erfolgen. Im

Anschluss ist es wichtig, transparent über weitere Entwicklungen zu berichten, so dass sich verärgerte Kunden und Kritiker ernst genommen fühlen.

- **Konfrontationen:** Die Hausanwälte in Stellung zu bringen, weil im Netz Verleumdungen verbreitet werden, ist keine gute Idee und der Online-Reputation nicht zuträglich – auch wenn man im Recht sein mag. Besser ist es, argumentativ vorzugehen und Fakten sprechen zu lassen.
- **Relevanz:** Bevor auf negative Kritik reagiert wird, muss deren Relevanz bewertet werden. Wie ist der Kritiker vernetzt, welche Reichweite kann er entfalten? Manchmal ist ignorieren besser als vorschnell handeln. Sollte die Kritik jedoch berechtigt sein, muss reagiert und der Beitrag kommentiert werden.
- **Persönlichkeit:** Im Web 2.0 geht es um Menschen. Die Akteure möchten mit Ihren Anmerkungen und Kommentaren ernst genommen werden. Für Unternehmen ist es daher wichtig, „Gesichter" im Social Web zu etablieren. Konflikte lassen sich sehr viel häufiger sachlich und objektiv ausdiskutieren, wenn echte Menschen miteinander kommunizieren.
- **Überraschung:** Krisenkommunikation im Web 2.0 beginnt vor der Krise: Eine relevante Reichweite erreicht man nicht über Nacht. Unternehmen müssen vorab Präventivstrategien entwickeln und Menschen in den sozialen Medien an sich binden, um im Krisenfall „Fürsprecher" zu haben.
- **Strategien:** Durch Echtzeit-Monitoring lassen sich Krisenherde meist schon frühzeitig identifizieren. Wichtig ist in den sozialen Medien die richtige Tonalität und Ansprache: Krisen-PR muss „auf Augenhöhe" geschehen. Zudem sollten Mitarbeiter im Umgang mit Kritik geschult und „Social Media Guidelines" definiert werden, um Missverständnisse zu vermeiden.
- **Erfolg:** Der Erfolg der eigenen Krisen-PR bemisst sich daran, wie viel Bedeutung einer Krise nach einer gewissen Zeit noch zugemessen wird (per Google-Suche, Social-Media-Monitoring). Überwiegen wieder positive Botschaften in den sozialen Netzwerke und der Google-Suche, tritt das Krisenereignis in den Hintergrund - man war erfolgreich.

8. Checklisten

In einem vom Bundesministerium des Innern (BMI) im Jahr 2008 herausgegebenen Handbuch „Krisenkommunikation – Leitfaden für Behörden und Unternehmen“ (siehe „Links“, Kapitel 10) finden sich im Anhang B eine Reihe nützlicher und detaillierter Checklisten für die Krisenkommunikation. Sie können leicht dem eigenen Bedarf angepasst und dem eigenen Krisenhandbuch zugefügt werden. Darüber hinaus eignen sich die Checklisten gut dafür, sich mit dem Ausmaß einer Krisensituation vertraut zu machen und alle Möglichkeiten zu durchdenken.

Die Checklisten betreffen folgende Themenfelder:

1. Konzeptionelle Präventivmaßnahmen (Ziele und Leitlinien)
2. Früherkennung/Frühwarnsysteme (Identifikation krisenanfälliger Bereiche)
3. Alarmierung (Priorisierung der zu benachrichtigenden Personen)
4. Personelle Aspekte (Zuweisung von Verantwortung)
5. Technisch organisatorische und logistische Aspekte (verfügbare Medienkanäle)
6. Krisenkommunikationsarbeit im Krisenstab (Aufgabenverteilung)
7. Kommunikation mit den Mitarbeitern (interne Krisen-PR)
8. Kommunikation mit den Medien/ der Öffentlichkeit (externe Krisen-PR)
9. Kommunikation mit der Bevölkerung (externe Krisen-PR)
10. Sonstige Zielgruppen (externe Krisen-PR)
11. Lessons Learned (interne Evaluation und Nachbereitung der Krise)
12. Krisennachsorge (externe Nachbereitung in Veröffentlichungen, Seminaren)
13. Aus- und Fortbildung (von Mitarbeitern)

Instrumente der Krisenkommunikation

geeignet zur		
	Information	**Kommunikation**
Alarmierung über Schneeballsystem	X	
Analoges Telefonnetz	X	X
Aushänge an zentralen Plätzen und Gebäuden	X	
Behördeneigene Telefonnetze	X	X
Dark Site	X	
Durchsagen über Lautsprecherwagen	X	
Festnetz über Vorrangschaltung	X	X
Flugblätter	X	
Flyer	X	
Handzettel	X	
Informationsbroschüren	X	
Meldegänger	X	X
Mobilfunk über Vorrangschaltung	X	X

Öffentliche Fernsprecher/Münztelefone		X
Plakate	X	
Presseinformation über E-Mail-Verteiler	X	
Pressekonferenz über Internet		X
Pressemeldungen über E-Mail-Verteiler	X	
Radiodurchsagen	X	
Schaukästen	X	
Selbstalarmierung	X	
Sirenensignale	X	
Telefonkonferenz über Satellitentelefon	X	X
„Tür-zu-Tür“-Information	X	
Unternehmenseigene Telefonnetze	X	X
Videokonferenz über Internet	X	X
Zeitungen	X	
Zentrale Anlauf- bzw. Informationsstellen	X	X

9. Textschablonen

Folgende Textschablonen/Templates können als Beispiele dienen, wie Mitarbeiter im Krisenfall kommunizieren sollten beziehungsweise wie Medien zu informieren sind. Sie können leicht dem eigenen Bedarf angepasst werden:

Telefonzentrale (Standardsatz, nicht durchstellen):

„Die Situation ist uns bekannt. Sobald nähere Informationen vorhanden sind, werden wir die Öffentlichkeit sofort unterrichten."

Vorstandssekretariat (Standardsatz, nicht durchstellen):

„Der Vorstand ist über die Situation informiert. Wenn Sie wichtige Informationen/ Anliegen haben, werde ich diese an die zuständigen Personen weiterleiten. Sobald uns weitere Informationen vorliegen, werden wir Sie davon unterrichten."

Krisensprecher (erste Verlautbarung):

„Wir wissen von der Situation und bedauern sie sehr. Augenblicklich sind wir dabei, uns einen Überblick über die Lage zu verschaffen. Sobald uns konkrete Informationen vorliegen, werden wir Sie informieren."

„Soweit möglich haben wir erste notwendige Vorkehrungen getroffen, um die Schäden so gering wie möglich zu halten. Wir werden Sie über alle weiteren Vorkommnisse unterrichten."

Erste Pressemeldung/ Website-Text:

„Ort, Datum. Beim Unternehmen XYZ in Ort hat sich heute, gegen 0.00 Uhr ein Brand ereignet, bei dem das Rechenzentrum in Mitleidenschaft gezogen wurde. Detaillierte

Informationen über den Grad der Beschädigung liegen noch nicht vor – eine Gefährdung der Datensicherheit kann aber (nicht) ausgeschlossen werden. Eine Untersuchung des Vorfalls läuft gegenwärtig. Genauere Erkenntnisse über die Ursachen liegen uns noch nicht vor. „XYZ“ unternimmt alle Anstrengungen, um zur Aufklärung beizutragen und die Datensicherheit nicht zu gefährden. Über den aktuellen Stand der Vorkommnisse werden wir Sie weiter auf dem Laufenden halten.“

Weitere Formulierungen:

„Wir bedauern den Vorfall und nehmen ihn sehr ernst...“

„Wir werden alles Notwendige unternehmen, um einen vergleichbaren Vorfall in Zukunft zu verhindern. Ein Datendiebstahl (o.ä.) in diesem Ausmaß war bislang nicht vorstellbar...“

„Wir haben alle Maßnahmen getroffen, um weiteren Schaden abzuwenden...“

„Wir haben die betroffenen Systeme unmittelbar nach Bekanntwerden der Vorfälle vom Netz genommen beziehungsweise abgeschaltet, um eine weitere Gefährdung der Daten zu verhindern...“

10. Links:

- Wikipedia-Eintrag: „Krisenkommunikation“
  http://bit.ly/IO3mQJ

- BSI-Standard 100-4 „Notfallmanagement“:
  http://bit.ly/HNY1ZZ (PDF)

- Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS Strategie):
- http://bit.ly/HHz9Nu (PDF)

- Bundesinnenministerium: „Krisenkommunikation (Leitfaden für Behörden und Unternehmen)“
  http://bit.ly/HCgwMg (PDF)

Der Leitfaden Krisenkommunikation ist im Rahmen der Vitako-Arbeitsgruppe Öffentlichkeitsarbeit entstanden, an der Holger Förster (Dataport), Hans-Peter Mayer (AKDB), Frank Schuckelt (KIVBF) und Bernd-Hendrik Nissing (ekom21) teilgenommen haben.