

Krisenkommunikation bei Cyberangriffen – Handreichung für Kommunen

Cyberresilience-Framework.
In IT-Krisen schneller agieren.
(Kurz: RESI)



Inhaltsverzeichnis

Krisenkommunikation bei Cyberangriffen.....	2
1. Einleitung.....	2
2. Bewertung und Entscheidungsfindung	3
3. Grundlagen der Krisenkommunikation.....	4
4. Hauptaufgaben der Kommunikationsverantwortlichen	5
5. Kommunikationsstrategie, -plan und -maßnahmen	5
5.1. Kommunikationsstrategie	5
5.2. Kommunikationsplan.....	6
5.3. Kommunikationsmaßnahmen	7
6. Leitfragen.....	8
7. Interne Kommunikation	9
8. Externe Kommunikation	10
8.1. Bürgerinnen und Bürger.....	10
8.2. Medien.....	11
8.3. Partner/Lieferanten und Behörden	12
9. „New Normal“	12

Krisenkommunikation bei Cyberangriffen

1. Einleitung

Trotz aller organisatorischen und technischen Sicherungsmaßnahmen können Organisationen Opfer von Cyberangriffen werden. Die Auswirkungen können sich auf interne Bereiche beschränken, aber auch weitreichende externe Folgen haben. In allen Fällen besteht aufgrund der hochsensiblen Daten, die betroffen sein können, eine große Verantwortung im Umgang mit der Situation. Um in dieser Ausnahmesituation schnell handlungs- und sprechfähig gegenüber allen relevanten Anspruchsgruppen zu werden, soll diese Handreichung Empfehlungen zur Krisenkommunikation geben.

Zielsetzung guter Krisenkommunikation ist es, nicht nur operativ, sondern auch kommunikativ schnell und angemessen auf die Krise zu reagieren, durch transparente und zeitnahe Informationen Unsicherheiten zu minimieren und so das Vertrauen interner und externer Anspruchsgruppen bestmöglich zu bewahren. Durch gezielte Informationsweitergabe kann verhindert werden, dass Gerüchte und Fehlinformationen verbreitet werden (intern und extern).

In größeren Kommunen/Organisationen kann in der Krise auf bestehende Strukturen und Prozesse zurückgegriffen bzw. darauf aufgebaut werden. In kleineren Organisationen werden einige Herausforderungen situativ gelöst werden müssen. Diese Handreichung versucht, diesem Umstand Rechnung zu tragen, indem sie überwiegend praxisnahe, schnell anwendbare Tipps und einfach umsetzbare Maßnahmen bietet. Daher werden in diesem Dokument nicht alle Szenarien und entsprechenden Kommunikations-Optionen dargestellt.

Zusammen mit dieser Handreichung erhalten Sie einige Vorlagen für Kommunikationsmaßnahmen. Diese sind als Vorschläge und Textbausteine zu verstehen, die

je nach Ausmaß und Folgen des Angriffs sowie zeitlicher Entwicklung auf die jeweilige konkrete Situation angepasst werden müssen. Alle Statements sollten inhaltlich mit den Zuständigen des jeweiligen Fachbereichs (z. B. Datenschutz, Compliance, Recht) abgestimmt werden. Insgesamt berücksichtigt diese Handreichung nicht nur akute Maßnahmen, sondern auch Aspekte der vorgelagerten und nachgelagerten Resilienz.

Ausführlichere Informationen zum Thema Krisenkommunikation finden Sie u. a. in folgenden Dokumenten:

Leitfaden Krisenkommunikation / BMI

<https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/leitfaden-krisenkommunikation.html>

„Ransomware: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall Version 1.2“ / BSI

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.html

Online-Kurs „Notfallmanagement“ / BSI

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-Notfallmanagement/online-kurs-notfallmanagement_node.html

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-Notfallmanagement/7_Notfaellebewaeltigen/3_Krisenkommunikation/Krisenkommunikation_node.html

2. Bewertung und Entscheidungsfindung

Die Schnittstellen zum Krisenstab ergeben sich aus den weiteren Dokumenten, die Ihnen im Rahmen dieser Handreichung zur Verfügung gestellt werden.¹

Im Akutfall geht es darum, Verantwortliche für die einzelnen Workstreams/Aufgaben möglichst schnell zu definieren (sofern nicht vorab festgelegt). Hierfür muss auch die Verantwortlichkeit der Rolle „Krisenkommunikation“ definiert werden (im Folgenden: Kommunikationsverantwortliche), die für die Koordination und Durchführung aller Kommunikationsmaßnahmen während der Krisensituation verantwortlich ist. Sofern sich diese nicht durch interne Ressourcen (Pressestelle, sonstige Verantwortliche für Regelkommunikation) besetzen lässt oder diese zu stark gefordert ist, kann (zeitliche begrenzte) externe Expertise hinzugezogen werden.

Abhängig von den vorab definierten Krisenstrukturen und -prozessen sowie Meldewegen und Eskalationsstufen Ihrer Organisation müssen die Kommunikationsverantwortlichen gemeinsam mit weiteren Mitgliedern des Krisenstabs beraten und entscheiden, ab wann eine interne und eine externe Kommunikation als notwendig erachtet werden und in welchem Umfang/zeitlichen Intervallen diese erfolgen. Gibt es hierzu keine vorab definierten Entscheidungsgrundlagen, muss diese Einschätzung situativ getroffen werden. Eine Einbeziehung der Rechtsabteilung (sofern diese nicht Mitglied des Krisenstabs ist) stellt sicher, dass alle rechtlichen Anforderungen erfüllt werden.

Leitfragen

¹ Der Begriff Krisenstab bezeichnet in diesem Dokument alle Formen von Gremien, in denen Informationen zur Lage bewertet sowie operative und kommunikative Entscheidungen getroffen werden.

Für die Entscheidungsfindung bezüglich einer aktiven Kommunikation an externe Anspruchsgruppen können folgende Leitfragen zum Vorfall bzw. seinen Auswirkungen hilfreich sein:

- Besteht eine Gefahr für die Aufrechterhaltung der Sicherheit und Gesundheit der Bevölkerung bzw. kann es dazu kommen (Funktionsfähigkeit Notrufe/Leitstellen, Erreichbarkeit und Arbeitsfähigkeit von Sicherheitsbehörden)?
- Ist das Angebot der kritischen Verwaltungsleistungen sowie der grundlegenden Dienstleistungen zur Daseinsvorsorge (basierend auf Fachverfahren) eingeschränkt bzw. kann es dazu kommen?
- Gibt es bereits Medienanfragen oder sind diese absehbar?
- Bestehen Berichts- oder Veröffentlichungspflichten gegenüber Behörden (z. B. Abfluss bzw. Veröffentlichung personenbezogener Daten)?
- Gibt es externe Parteien (Partner, Lieferanten), die von dem Vorfall betroffen sind und informiert werden müssen?

Beispielhafter Entscheidungsablauf

1. **Ereignisbewertung:** Einschätzung des Vorfalls sowie potenzieller Auswirkungen und Risiken durch Kommunikationsverantwortliche
2. **Rechtliche Prüfung:** Sicherstellung der Einhaltung aller gesetzlichen Anforderungen
3. **Entscheidung:** Vorstellung der Kommunikationsstrategie im Krisenstab, Freigabe durch Leiter:in des Krisenstabs bzw. zuständige Leitungsfunktion
4. **Durchführung:** Umsetzung der Kommunikationsmaßnahmen gemäß dem festgelegten Plan

Alle Lagebilder und Entscheidungen des Krisenstabs müssen durch eine definierte Rolle vollständig, schnell auffindbar und unveränderbar dokumentiert/protokolliert werden.

Diese Dokumentation ist strikt von der Rolle der Kommunikation zu trennen und muss nicht durch diese gepflegt werden. Es ist darauf zu achten, dass ggf. vertrauliche Informationen nicht nach außen gegeben werden.

3. Grundlagen der Krisenkommunikation

Durch den Cyberangriff kann Vertrauen bei den internen und externen Anspruchsgruppen verloren gehen, welches es zurückzugewinnen gilt. Dies gelingt, indem die Organisation planvoll handelt – eine verlässliche Kommunikation ist ein starker Indikator für planvolles Handeln.

Folgende Grundsätze bilden die Basis erfolgreicher Krisenkommunikation:

- **Frühzeitiges Erkennen des Krisenpotenzials:** Bildung von Szenarien: Was ist der Worst Case? Wie wird dann operativ gehandelt und kommuniziert? Sowohl bei der internen als auch der externen Kommunikation muss differenziert werden, welche Anspruchsgruppen und welche Arbeitsbereiche direkt und indirekt betroffen sind bzw. betroffen sein werden.
- **Kommunizieren Sie zeitnah, aber nicht überstürzt.** Planen Sie Zeit für Abstimmungs- und Freigabeprozesse mit ein. Ggf. kann die Übersetzung von Kommunikationsmaßnahmen in andere Sprachen notwendig sein – planen Sie auch hierfür Zeit ein.
- **Faktenbasiert und empathisch:** Richten Sie Ihre Kommunikationsmaßnahmen an sachlicher Recherche und einer nüchternen Analyse der Lage aus. Zeigen Sie

dennoch Empathie und Verständnis für die Sorgen und Belange der Anspruchsgruppen und versuchen Sie, diese möglichst gut zu antizipieren.

- **Einheitlichkeit sicherstellen:** Achten Sie darauf, dass alle Kommunikationsmaßnahmen aufeinander abgestimmt und einheitlich sind. Nutzen Sie Redundanzen, bspw. Formulierungen in Wordings für interne und externe Anspruchsgruppen, FAQ etc.

4. Hauptaufgaben der Kommunikationsverantwortlichen

In Sondersituationen kommt auf Kommunikationsverantwortliche eine hohe Arbeitsbelastung zu: Unter zeitlichem Druck und bei oftmals unklarer Faktenlage müssen teilweise hochrelevante Entscheidungen an eine Vielzahl von Anspruchsgruppen kommuniziert werden. In solchen Situationen ist inhaltliche Klarheit ein hohes Gut: Kommunikationsverantwortliche müssen deshalb bei der Einholung der für ihre Aufgaben erforderlichen Informationen in Krisenstäben so lange aktiv und gezielt nachfragen, bis sie wirklich alle technischen und organisatorischen Details verstanden haben. Nur wenn alle Sachverhalte wirklich verstanden wurden, können die aktuelle Lage, Prognosen, Einschränkungen und Fortschritte korrekt an die entsprechenden Zielgruppen kommuniziert werden.

Zu den wichtigsten Aufgaben von Kommunikationsverantwortlichen zählen folgende:

- **Teilnahme an Krisenstab-Sitzungen- zwingend notwendig:** Beschaffen von Grundlagen, Fakten und Daten für die Krisenkommunikation, Lieferung des aktuellen kommunikativen Lagebilds auf Basis von Medienbeobachtung sowie Bündelung/Analyse häufig gestellter Fragen
- **Zielgruppen-Analyse:** Definition der Betroffenheit (intern und extern), Analyse des jeweiligen Informationsbedarfs, Erstellung von neuen/Ergänzung von bestehenden Kontaktlisten/Verteilern (z. B. zu Medien)
- **Entscheidung über Kommunikationsstrategie/kommunikative Grundhaltung, Erstellung eines Kommunikationsplans, Umsetzung der Kommunikationsmaßnahmen**
– siehe Folgekapitel
- **Aufsetzen bzw. Ausweiten der Medienbeobachtung:** Online, Print, TV/Hörfunk. Wenn bis dato nicht vorhanden, schnellstmöglich aufsetzen (z. B. über kostenpflichtigen Anbieter oder Google/Talkwalker Alerts, mit Stichwörtern wie „Gemeinde XY“)
- **Dokumentation:** alle aktiv verbreiteten Informationen, alle eingehenden schriftlichen und ggf. mündlichen Anfragen/Auskunftserteilungen/Hilfeersuchen sowie die Antworten darauf müssen dokumentiert werden. Diese Dokumentation ist der Gesamtdokumentation des Krisenmanagements zuzuführen.
- **Beratung zur Erstellung von Informationsschreiben an weitere Anspruchsgruppen:** z.B. Kommunikation mit weiteren HVB, DSGVO-Meldungen an LDI und ggf. Mitarbeitende und Bevölkerung, Anzeigenerstattung bei Polizei/LKA etc.
- **Abklärung verfügbarer finanzieller Ressourcen:** z.B. zur ad-hoc-Beauftragung von Medienbeobachtungs-Dienstleistern, Hinzuziehung externer Kommunikationsverantwortlicher etc.

5. Kommunikationsstrategie, -plan und -maßnahmen

5.1. Kommunikationsstrategie

Ob eine aktive oder reaktive Kommunikation ratsam ist, kann sich in Einzelfällen unterscheiden. Eine reaktive Kommunikationsstrategie zeichnet sich durch eine

zurückhaltende Informationspolitik aus und eignet sich nur in solchen Krisen, in denen eine Behörde mit geringer öffentlicher Aufmerksamkeit rechnet.

Aktive Kommunikationsstrategie: Beim hier skizzierten Szenario eines Cyberangriffs mit großen Auswirkungen ist die Organisation i.d.R. direkt und sichtbar von der Krise betroffen. Daher empfiehlt sich eine aktive Kommunikationsstrategie, die die direkten und indirekten Ursachen und Auswirkungen der Krise adressiert. Der Vorteil dieser aktiven Kommunikation ist, dass die Informationsbedürfnisse von externen Anspruchsgruppen bedient werden und sich auch die Gefahr einer fehlerhaften Berichterstattung verringern lässt. Im Rahmen einer aktiven Kommunikation müssen Sie kontinuierlich und in regelmäßigen Intervallen kommunizieren – siehe [Kommunikationsplan](#).

„Intern vor Extern“: Ihre Mitarbeiter:innen sollten immer zuerst informiert werden, bevor eine öffentliche Kommunikation beginnt. Zudem sollte abgewogen werden, welche Details notwendig sind, um Transparenz zu gewährleisten, ohne sensible Informationen preiszugeben. Rechnen Sie damit, dass alle Informationen, die Sie intern verbreiten, relativ zügig nach außen gelangen werden, und berücksichtigen Sie dies bei Ihrer internen Kommunikation.

Prozesskommunikation und Zeitpläne: Alle Betroffenen benötigen dringend eine zeitliche Perspektive für die kommenden Tage und Wochen – auch wenn diese ggf. noch nicht verlässlich verfügbar ist. Hier sollte mit Bedacht kommuniziert werden, um keine falschen Versprechungen zu machen, die dann nicht eingehalten werden können. Im Rahmen einer Prozesskommunikation können (Zwischen-)Ziele in groben Zeitrastern sowie erste Meilensteine benannt werden. Erfragen Sie für diese Prozesskommunikation in den Krisenstabsitzungen grobe Zeitpläne. Benennen Sie klar, welche Schritte erreicht wurden, welcher Teilschritt als Nächstes ansteht und mit welchem Ergebnis wann zu rechnen ist. Geben Sie damit einen aktuellen Überblick, welche öffentlichen Dienstleistungen in Ihrer Kommune aktuell funktionieren, welche nur mit Einschränkungen verfügbar sind und welche derzeit nicht funktionieren.

Unwissen und Nichtwissen kommunizieren: Vermitteln Sie ausschließlich faktenbasierte Informationen, die auf belegbaren Tatsachen beruhen. Verbreiten Sie Planungsstände, aber keine Mutmaßungen. Kommunizieren Sie auch Unsicherheit und Nichtwissen, und lieber etwas zu pessimistisch als mit zu ambitionierten Zielsetzungen und Zeitrahmen („Wann Prozess XY wieder läuft, ist derzeit noch nicht absehbar.“, „Das untersuchen wir gerade noch intern und geben Ihnen dann Bescheid“).

Verständlich kommunizieren: Bedenken Sie, dass Sie zum Großteil Menschen informieren, die mit Ihnen geläufigen Strukturen, Prozessen und Fachbegriffen nichts anfangen können. Versetzen Sie sich in die Lage der wichtigsten Anspruchsgruppen, empfinden Sie deren Erwartungen und enttäuschte Erwartungen nach (Auto ummelden, Auszahlung von Wohngeld/Sozialhilfe, An-/Abmeldung von Wohnsitz, Ausstellung von Passdokumenten etc.) und geben Sie die entsprechenden Informationen in einfacher, klarer Sprache wieder. Erläutern Sie alternative/improvisierte Lösungswege so klar wie möglich.

5.2. Kommunikationsplan

Die Erstellung eines Kommunikationsplans muss zeitnah erfolgen und die Frage beantworten: Wer kommuniziert wann was an wen über welchen Kanal?

Legen Sie fixe Kommunikationszeitpunkte fest und halten Sie diese ein – auch wenn es nichts Neues gibt. Teilen Sie den jeweiligen Anspruchsgruppen mit, wann sie das nächste Mal von Ihnen hören oder lesen. Die Regel lautet: so häufig und regelmäßig wie möglich, um zeitaufwändige Rückfragen zu reduzieren und Ressourcen freizuhalten.

Wichtig: Kommunikationspläne (Intervalle, Umfang & Inhalt der Kommunikation) können angepasst werden, die kommunikative Grundhaltung/Kommunikationsstrategie (aktiv) sollte aber beibehalten werden.

Beispiel für einen Kommunikationsplan:

Alle Betroffenen² erhalten jeden Tag zur gleichen Zeit/jede Woche am gleichen Tag ein Update, in dem informiert wird:

- Was bis jetzt unternommen/erreicht wurde
- Was der aktuelle Stand ist
- Was für die kommende Woche geplant ist

Das Update kann aus zwei Teilen bestehen:

1. einem allgemeinen Teil (für alle gleich)
2. einem spezifischen Teil (für die wichtigsten Betroffenen individuell ergänzt / an spezifische Anspruchsgruppen angepasst)

Das Update kann folgende Kerninformationen enthalten:

- Status der Wiederherstellung (Infos werden geliefert durch IT)
 - Art und Zahl der technischen Geräte (Desktops, Laptops, Server etc.), die wieder im Betrieb sind
 - Art und Zahl der Software-Systeme/Fachverfahren, die wieder in Betrieb sind
- Arbeitsfähigkeit (Infos werden geliefert durch IT-Teams)
 - Anteil (Prozent) der wiederhergestellten Arbeitsfähigkeit der gesamten Kommune
 - Anteil (Prozent) der wiederhergestellten Arbeitsfähigkeit bereichsspezifisch

Das Update kann situativ ergänzt werden um Highlights, wie z.B. die vollständige Wiederinbetriebnahme eines Bereiches oder eines Software-Systems/Fachverfahrens. Im Falle von Rückschritten sollte eine Begründung ergänzt werden.

5.3. Kommunikationsmaßnahmen

- **Intern:** Mitarbeiter-Informationen, FAQ, Sprechzettel/inhaltliche Zulieferung für Arbeitsbereiche (Krisen-Hotline, Sammel-Mailadresse etc.) – [siehe Folgekapitel](#)
- **Extern:**
 - Bürgerinnen und Bürger: Bürger-Informationen & FAQ – direkt über Website/Darksite/Notfallseite, Amtsblätter, Aushänge, Social-Media-Postings, indirekt über Medien – [siehe Folgekapitel](#)
 - Medien: Holding Statement, Presseinformationen, Statements zur Beantwortung von Medienanfragen, Interviews und Hintergrundgespräche, FAQ, ggf. Pressekonferenzen – [siehe Folgekapitel](#)

Beispiele für die genannten Kommunikationsmaßnahmen werden Ihnen als Vorlage zur Verfügung gestellt.

² Die Intervalle können sich für intern und extern sowie Teil der Zielgruppen unterscheiden.

6. Leitfragen

Kommunikationsverantwortliche müssen durch die Fachbereiche so instruiert werden, dass sie in der Lage sind, auch komplexe technische Probleme zielgruppenspezifisch und verständlich aufzubereiten und zu präsentieren. Nur wenn sie die technischen und organisatorischen Sachverhalte umfassend verstehen, können sie die aktuelle Lage sowie Prognosen, Einschränkungen und Fortschritte sachlich richtig und verständlich an die entsprechenden Zielgruppen kommunizieren.

Um alle wichtigen Informationen im Krisenstab einzuholen und sie in der Folge für das Verfassen von Kommunikationsmaßnahmen nutzen zu können, sind folgende Leitfragen zum Vorfall bzw. seinen Auswirkungen für Kommunikationsverantwortliche hilfreich:

- Was konkret ist vorgefallen/was ist es für ein Angriff?
- Wann wurde der Angriff bemerkt? Seit wann läuft er?
- Welche Folgen hat der Angriff im informationstechnischen System ausgelöst, und warum kann er nicht innerhalb kurzer Zeit behoben werden?
- In welchem Ausmaß ist die Arbeitsfähigkeit der Mitarbeitenden eingeschränkt? Bis wann?
- Welche Systeme bzw. Daten sind derzeit nicht verfügbar (Server, Telefonie, Mailverkehr, Webseite, etc.)?
- Welche Fachverfahren und angeschlossenen Dienstleistungen sind dadurch nur eingeschränkt oder gar nicht verfügbar?
- Welche weiteren Auswirkungen haben der Angriff und seine Folgen auf Bürgerinnen und Bürger?
- Welche Auswirkungen haben der Angriff und seine Folgen auf die Zusammenarbeit mit Partnern/Dienstleistern?
- Wie lange sind die Dienste voraussichtlich nicht verfügbar?
- Gibt es Workarounds/Behelfslösungen für betroffene Dienstleistungen? Wie sind diese konkret zu nutzen?
- Sind Backups verschlüsselt/nutzbar?
- Sind Daten abgeflossen? Wenn ja, welche Art von Daten?
- Liegt eine meldepflichtige Datenschutzverletzung vor?
- Liegt eine Datenschutzverletzung vor, bei der auch betroffene Personen benachrichtigt werden müssen?
- Was können potenziell betroffene Personen tun, um sich jetzt vor den Auswirkungen des Angriffs zu schützen?
- Was konkret wird aktuell sowie kurzfristig unternommen, um den Angriff abzuwehren und seine Folgen einzudämmen?
- Mit welchen Einrichtungen/Behörden und externen Experten wird zusammengearbeitet, um den Angriff abzuwehren und seine Folgen einzudämmen?
- Wenn Dienste erst nach und nach wiederhergestellt werden: Wie und durch wen werden diese priorisiert? Wie ist der antizipierte Zeitrahmen?

Die Antworten auf diese Fragen müssen Kommunikationsverantwortliche je nach aktueller Lage bzw. fortschreitender Lageentwicklung zusammenfassen und in einfach verständlicher, nicht-technischer Sprache an die entsprechenden Zielgruppen übermitteln. Hierbei ist zu

beachten, dass sensible Informationen aus den hier genannten Leitfragen lediglich dem fachlichen Verständnis dienen und nicht nach außen gegeben werden dürfen. Generell ist eine Prüfung von Informationen, die nach außen gehen, durch Jurist:innen angebracht.

7. Interne Kommunikation

Die Arbeitsfähigkeit der Mitarbeiter:innen ist bei einem Cyberangriff üblicherweise stark eingeschränkt, was viele Fragen aufwirft: 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 ggf. in anderen Bereichen unterstützen? Wie werden Arbeitszeiten, Urlaubstage, Krankheitsausfall oder die Überstunden zur Krisenbewältigung in der IT erfasst? Werden Gehälter pünktlich ausgezahlt? Die interne Kommunikation zielt vor allem darauf ab, den Mitarbeiter:innen diese und weitere zentrale Informationen zu ihrem Arbeitsbereich zu beantworten.

Alle Mitarbeiter:innen sollten im Krisenfall vor externen Anspruchsgruppen oder mindestens zeitgleich mit diesen informiert werden – sowohl in betroffenen als auch nicht betroffenen Bereichen. Personen in leitenden Positionen (Führungskräfte und Amtsleitungen) können als Multiplikatoren in den jeweiligen Ämtern fungieren. Je mehr Infos schnell und proaktiv vermittelt werden, umso weniger Rückfragen werden an alle Beteiligten herangetragen.

Gleichzeitig sind die Mitarbeiter:innen zu sensibilisieren, was die Weitergabe von Informationen angeht. Da Beschäftigte einer angegriffenen Organisation im privaten Bereich für Außenstehende verlässliche Informationslieferanten und damit eine wichtige Dialog- und Multiplikatoren-Gruppe darstellen, müssen sie wissen, welche Informationen sie weitergeben dürfen – und welche nicht. Bitten Sie aktiv darum, auf Spekulationen in privaten Gesprächen oder auf Social-Media-Kanälen zu verzichten. Weisen Sie darauf hin, dass alle offiziellen Anfragen ausschließlich vom Kommunikationsverantwortlichen und nicht durch einzelne Mitarbeiter:innen beantwortet werden. Nur so können Sie sicherstellen, dass Ihre Organisation nach außen einheitlich kommuniziert.

Entsprechend des von Ihnen aufgestellten Kommunikationsplans müssen auch Informationen an Mitarbeiter:innen kontinuierlich verschickt werden, so dass diese jederzeit auf dem aktuellen Stand sind. Hierbei ist Rücksprache mit dem Personalmanagement zu halten.

Folgende Kommunikationsinhalte sind hilfreich:

- Beschreibung der aktuellen Lage und damit verbundener Einschränkungen
- Prognose zu weiterer Szenario-Entwicklung und damit verbundener Arbeitsfähigkeit
- Kontinuierliche Aktualisierungen der Informationen über den Fortschritt und aktuelle Maßnahmen
- FAQ, welche die wichtigsten Fragen beantworten (fortlaufend zu ergänzen)
- Hinweis auf neu etablierte Kommunikationskanäle und definierter Kanal für Rücklauf von Fragen und Feedback
- Verhaltensregeln und Sprachregelungen zu Anfragen Externer bzw. im Familien- und Freundeskreis
- Förderung von Engagement und Initiative der Mitarbeiter:innen (z.B. Möglichkeiten zur Unterstützung in anderen Abteilungen oder Bereichen)

Die konkreten Kommunikationsinhalte ergeben sich aus den Antworten auf die o.g. [Leitfragen](#).

Je länger die Situation mit all ihren Auswirkungen anhält, umso mehr müssen auch psychologische/emotionale Aspekte bei der Kommunikation berücksichtigt werden: Je nach

Grad der Involviertheit in die Krisenbewältigung kann die Arbeitsbelastung und damit auch der hohe Druck für Ihre Mitarbeiter:innen enorm ansteigen. Berücksichtigen Sie dies in der Mitarbeiterkommunikation, indem Sie den Beteiligten für ihren Einsatz danken und ggf. auch organisatorische/operative bzw. psychologische Unterstützung anbieten.

→ Vorlagen für solche Informationsschreiben (Erst- und Folgeinformation, FAQ) an Mitarbeiter:innen finden Sie im Abschnitt „[Interne Kommunikation](#)“. Auch hier können Sie sich Redundanzen zunutze machen: Verwenden Sie Bausteine aus den externen FAQ in der Mitarbeiterkommunikation und stellen Sie so auch die Einheitlichkeit der Botschaften sicher.

Kanäle

Bei einem Ausfall Ihrer gewohnten Kanäle (Mail, Intranet) müssen Sie ggf. mit Behelfslösungen arbeiten. Dies können browserbasierte Tools sein, die über Chatfunktionen verfügen und ggf. auch das Teilen von Dokumenten erlauben (Slack, Teams). Als Behelfslösungen haben sich auch Messenger-Dienste bewährt. Ggf. können wichtige interne Informationen auch über Aushänge kommuniziert werden.

8. Externe Kommunikation

Die externe Kommunikation über den Vorfall und die getroffenen Maßnahmen zielt darauf ab, die Öffentlichkeit (Bürgerinnen und Bürger) und die Medien schnell und umfassend über die Situation zu informieren und so Gerüchte/Fehlinformationen zu minimieren. Neben den genannten Anspruchsgruppen können auch Dienstleister und Partner sowie Politiker und Verbände zu den Zielgruppen der externen Kommunikation gehören. Beantworten Sie externe Anfragen zeitnah unter Verwendung der einheitlichen FAQ.

8.1. Bürgerinnen und Bürger

Für die Bürger:innen hat das skizzierte Szenario eines Cyberangriffs unter Umständen direkte und drastische Auswirkungen: Durch die Verschlüsselung von Servern und Daten sind wichtige Fachverfahren nicht mehr verfügbar, und grundlegende Dienstleistungen können nicht mehr angeboten werden. Hierüber müssen die Betroffenen zeitnah informiert werden – ebenso wie über Workarounds und Behelfslösungen, sobald diese etabliert wurden.

Folgende Kommunikationsinhalte sind hilfreich:

- Beschreibung der aktuellen Lage und damit verbundener Einschränkungen
- Prognose zu weiterer Szenario-Entwicklung und damit verbundenen Dienstleistungen
- Kontinuierliche Aktualisierungen der Informationen über den Fortschritt und aktuelle Maßnahmen
- FAQ inkl. Antworten, welche die wichtigsten Fragen beantworten (fortlaufend zu ergänzen)
- Hinweis auf neu etablierte Kommunikationskanäle und definierter Kanal für Rücklauf von Fragen/Feedback (Hotline, Sammel-Mailadresse)
- Verhaltensregeln und -ratschläge zu Behelfslösungen

Die konkreten Kommunikationsinhalte ergeben sich aus den Antworten auf die o.g. [Leitfragen](#).

→ Vorlagen für [Informationen an Bürger:innen](#) (Erst- und Folgeinformation) sowie für [externe FAQ](#) finden Sie in diesem Dokument.

Kanäle

Bei einem Ausfall Ihrer gewohnten Kanäle (Website, Mail) müssen Sie ggf. mit Behelfslösungen arbeiten. Etablieren Sie zügig eine Notfall-Website mit allen wichtigen Informationen und Kontaktdaten. Ggf. können wichtige externe Informationen auch über Aushänge kommuniziert werden. Eine Krisen-Hotline kann, sofern die technischen und personellen Ressourcen verfügbar sind, als Sammelstelle für Rückfragen dienen. Sofern Sie Social-Media-Kanäle nutzen, können auch hierüber Informationen verbreitet werden. Mitarbeitende, die diese Kanäle (Hotline, Social Media) betreuen, benötigen Sprechzettel/FAQ, um eingehende Fragen einheitlich und jeweils nach dem aktuellen Kenntnisstand beantworten zu können. Über diesen Kanal werden auch weitere Themen/Fragen gesammelt, die dann wieder Eingang in die FAQ finden müssen.

8.2. Medien

Je intensiver die Krise und je größer ihre Auswirkungen, desto stärker und brisanter entwickelt sich die Berichterstattung der Medien. Daher wird eine aktive Kommunikationsstrategie empfohlen, auf Basis derer verfügbare Informationen offensiv verbreitet werden (siehe [Kapitel 4](#)).

Verantwortlicher für Medienanfragen: Sollte noch kein/e Ansprechpartner:in für Medien existieren, benennen Sie diesen für die Dauer der Krise und bitten Sie darum, alle Anfragen schriftlich sowie ausschließlich an diese Rolle zu richten. Wenn Ihre Mailsysteme nicht mehr funktionsfähig sind, richten Sie hierfür ggf. eine neue/externe Mailadresse ein (z.B. presse_kommuneXY@posteo.de), von der aus sie die Medienarbeit zentral steuern.

Medienverteiler: Sofern Sie Medienverteiler nutzen, prüfen Sie, ob wirklich alle Empfänger:innen mit den Informationen versorgt werden sollen, oder ob die aktuellen Updates lediglich für einen Teil dieser Zielgruppe relevant sind (siehe [Kommunikationsplan](#)). Sollten Sie keine Medienverteiler besitzen, recherchieren Sie die Adressen Ihrer wichtigsten Lokalmedien (Zeitung, Online-Portale, Radio-/TV-Sender) und versenden Sie Ihre Informationen an diese Redaktionen. Hier zählt Geschwindigkeit unter Umständen mehr als Vollständigkeit: Keine Sorge, wenn Sie keine vollständige Kontaktliste haben – die Journalisten werden sich im Fall eines Cyberangriffs auf Ihre Kommune ziemlich sicher von sich aus bei Ihnen melden.

Holding Statement/Erst-Information: Ein Holding Statement ist eine vorläufige Erklärung, die grundlegende Informationen liefert und verspricht, weitere Details so schnell wie möglich bereitzustellen. Mit einem solchen Statement können Sie schnell und angemessen auf Anfragen von Medien, Partnern oder der Öffentlichkeit reagieren, noch bevor detailliertere Informationen verfügbar sind.

Presseinformationen: Im Szenario Ransomware sollten Sie – aufgrund Ihrer eingeschränkten Arbeitsfähigkeit – die lokalen Medien nutzen, um wichtige Informationen an die Bürger:innen zu übermitteln. Veröffentlichen Sie deshalb immer dann eine Presseinformation, wenn es neue, relevante Informationen gibt. Basis hierfür sind die Informationen zur jeweils aktuellen Lage, die Sie aus dem Krisenstab mitnehmen. Denken Sie daran, die Presseinformationen immer intern (HVB, Datenschutzverantwortliche) sowie ggf. auch extern (Ermittlungsbehörden) abzustimmen.

Statements/Interviews/Hintergrundgespräche: Je nach zeitlicher Verfügbarkeit können Sie als Kommunikationsverantwortliche oder andere Mitarbeiter:innen (z.B. Bürgermeister) auch für Hintergrundgespräche und Interviews zur Verfügung stehen, um über die Presseinfos hinaus ein inhaltliches und emotionales Verständnis für die Lage zu schaffen. Geben Sie zitierfähige Antworten an Journalist:innen nur in schriftlicher Form und nach Freigabe durch den Krisenstab/Verantwortliche, es sei denn, Sie sind dazu befugt und fähig.

→ Vorlagen für [Holding Statements](#), [Presseinformationen](#) sowie für [externe FAQ](#) finden Sie in diesem Dokument.

Kanäle

Bei einem Ausfall Ihrer gewohnten Kanäle (Website, Mail) müssen Sie ggf. mit Behelfslösungen arbeiten. Etablieren Sie – wie bereits im Kapitel [Bürgerinnen und Bürger](#) erwähnt – zügig eine Notfall-Website mit allen wichtigen Informationen und Kontaktdaten und nutzen Sie ggf. oben beschriebene externe Mailadressen.

8.3. Partner/Lieferanten und Behörden

Bedenken Sie auch, dass Unternehmen und Organisationen, die mit Ihrer Organisation zusammenarbeiten, sowie übergeordnete staatliche Stellen Informationen benötigen. Diese können Sie aus den externen FAQ generieren.

9. „New Normal“

Nach dem hier beschriebenen Szenario eines Ransomware-Angriffs wird Ihre Organisation – je nach Dauer und Ausmaß des Vorfalls und seiner Folgen – ggf. nicht mehr die alte sein, sondern noch für eine geraume Zeit mit dem Makel „Cyberangriff“ in Verbindung gebracht und wahrgenommen werden. Dies gilt es auch bei der Kommunikation zu berücksichtigen: Bewerten Sie Ihre Folgekommunikation daher immer aus der Sicht von kritischen, weil direkt betroffenen und in ihrer eigenen Handlungsfähigkeit eingeschränkten Zielgruppen. Sie müssen keine Fehler eingestehen, die Sie nicht begangen haben – aber etwas Zurückhaltung kann helfen, die öffentliche Wahrnehmung und Reputation Ihrer Organisation zu verbessern.

Sobald alle kritischen Verwaltungsleistungen und Dienstleistungen wieder uneingeschränkt angeboten werden können, ist eine Veröffentlichung einer abschließenden Presseinformation möglich, in der die ergriffenen Maßnahmen aufgelistet werden können. Sofern ein forensischer Abschlussbericht erstellt wurde, wird sich die Frage nach der Veröffentlichung der Ergebnisse stellen. Eine allgemeingültige Empfehlung zum Umgang mit internen, sicherheitsrelevanten Erkenntnissen ist nicht möglich. Im Sinne der Transparenz und Hilfestellung für andere Kommunen kann dieser in internen Kreisen komplett oder in Auszügen besprochen werden. Es ist aber ebenso legitim, die Ergebnisse lediglich intern auszuwerten.

Um die Wirksamkeit Ihrer Krisenkommunikation zu überprüfen und Verbesserungsmöglichkeiten für die Zukunft zu identifizieren, sind eine Nachbereitung und Evaluation der Strategie und ergriffenen kommunikativen Maßnahmen ratsam. Hierfür kann internes Feedback eingeholt und analysiert werden. Die Rückmeldung der Beteiligten kann zur Verbesserung der Prozesse für die Zukunft beitragen. Eine Dokumentation und Archivierung aller relevanten Informationen für potenzielle zukünftige Krisen wird empfohlen. Diese Dokumentation sollte auch offline verfügbar sein, so dass sie bei einem eventuellen weiteren Vorfall uneingeschränkt zugänglich ist.

Mögliche Evaluierungsmaßnahmen

- Interne Feedback-Runden und Umfragen: Einholen von Rückmeldungen der Mitarbeiter zur Verbesserung der Kommunikationsstrategie
- Evaluierung der Medienberichterstattung: Analyse der Medienresonanz zur Bewertung der Öffentlichkeitsarbeit

Anpassung des Kommunikationshandbuchs basierend auf den gewonnenen Erkenntnissen: Überarbeitung und Aktualisierung des Handbuchs zur Optimierung der Krisenkommunikation