ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Krisenkommunikation bei Cyberangriff

Erste-Hilfe-Kasten für Kommunen

Fraunhofer SIT

EDITH GERMANY
Enabling Digital Innovation & Technology in Hesse

FORSCHUNGSFÖRDERUNG CYBERSICHERHEIT HESSEN
Hessisches Ministerium des Innern, für Sicherheit und Heimatschutz

Infos und Materialien

IT-Vorfälle, sei es ein Cyberangriff auf die eigenen IT-Systeme oder ein technischer Ausfall – sind eine reale Gefahr für Kommunen. Digitale Services für Bürgerinnen und Bürger, interne digitale Kommunikation, digitalisierte Arbeitsabläufe, auch Telefonsysteme – alles kann Ziel einer Attacke sein und lahmgelegt werden, bis zur völligen digitalen Handlungsunfähigkeit der kommunalen Verwaltung.

In dieser Broschüre finden Sie Werkzeuge, Formulierungshilfen sowie Anlaufstellen für die Zeit vor und während einer solchen Krise.

Diese Information finden Sie auch auf unserer Website:

cybersicherheit-fuer-kommunen.de

1 – Vor der Krise

Für einen IT-Vorfall kann man sich wappnen. Auch Kommunen mit vergleichsweiser geringer finanzieller Ausstattung können mit guter Vorbereitung und clever eingesetzten Tools dafür sorgen, dass sie im Ernstfall noch handlungs- und kommunikationsfähig sind. Denn je nach Schwere des Vorfalls kann es zu einem Totalausfall aller elektronischen Systeme kommen – selbst VoiP-Telefonsysteme funktionieren dann nicht mehr.

Hier sind Schritte aufgelistet, die Sie zur Vorbereitung der Krisenkommunikation bei einem IT-Vorfall durchgehen sollten. Eine umfassende Vorbereitung sollte durch ein Business-Continuity-Management-System erfolgen.
In Hessen unterstützt das Hessische Cyberabwehr Ausbildungszentrum Land/Kommunen https://hessen3c.de/unsere-leistungen/cyberabwehr-ausbildungszentrum (HECAAZ L/K) die Kommunen dabei.

Hessen3C hilft unter der 24/7 erreichbaren Notfallhotline: 0611 353 9900

Kommunikationsverantwortliche Person benennen
Wenn nicht die kommunale Leitung selbst, dann Person in engster Zusammenarbeit mit der Leitung, Mitglied des Krisenstabs

- **Aufgabe: Zentrale Koordination der Krisenkommunikation.** Hier laufen alle Infos zusammen, von hier aus gehen alle Infos raus
- im Vorfeld möglichst Medientraining für die Person
- Grundregeln der Kommunikation und des Umgangs mit der Presse verinnerlichen → 2 – Sicherheit im Kontakt mit Medien

Alternativen Kontaktverteiler erstellen

- Alternative Mailadressen/Telefonnummern/Kontaktmöglichkeiten von wichtigen Kontakten der Kommune (intern und extern) sammeln, damit auch im Fall eines Totalausfalls alle erreicht werden können. → 3 – Checkliste interne und externe Kontakte
- Wichtig: Listen aktuell halten, Listen zugänglich halten, auch wenn IT ausfällt (z. B. als Ausdruck)

Mitarbeiterinnen und Mitarbeiter im Vorfeld für den Fall eines Cyberangriffs sensibilisieren

- Kommunikationsverhalten: Es wird einheitlich und nur von der verantwortlichen Person (s.o.) kommuniziert, keine Gerüchte/Spekulationen
- Mitarbeiterinnen und Mitarbeiter ermuntern, Auffälliges an kommunikationsverantwortliche Person zu melden
- Über alternative Kommunikationskanäle informieren, damit Mitarbeiterinnen und Mitarbeiter wissen, wo sie sich informieren können

Monitoring-Dienste einrichten: für eigene digitale Dienste oder die eigene Webseite kann man sich Benachrichtigungen schicken lassen, wenn diese nicht mehr online sind → 8 – Wie erfahre ich von der Krise

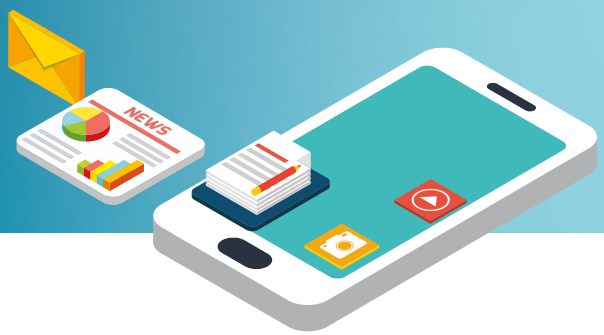
Social-Media-Kanäle einrichten

- als alternativer Kommunikationskanal nach außen
- als Monitoring-Möglichkeit
- als Anlaufstelle für Fragen v.a. von extern → 8 – Wie erfahre ich von der Krise

Software-Alternativen einrichten, auf die im Notfall zurückgegriffen werden kann. Sprechen Sie mit Ihrem IT-Dienstleister. Hessen3C bietet ein Set von Notfall-Laptops für akut betroffene Kommunen an.

Eine Fallback-Seite/Darksite für die kommunale Webseite einrichten (lassen) → 9 – Checkliste Darksite

2 – Sicherheit im Kontakt mit Medien Grundregeln der Kommunikation



1. **Unterscheiden Sie nicht zwischen interner und externer Kommunikation.**
   Alle internen Aussagen, die in größerem Kreis getroffen werden, sind quasi öffentlich und dringen früher oder später nach draußen.

2. **Erreichbarkeit der Verantwortlichen**
   Während der Krise ist es unabdingbar, dass der gesamte Krisenstab zeitnah erreichbar ist.

3. **Halten Sie sich an die festgelegten Kernbotschaften.**
   Die Einheitlichkeit und Klarheit aller Statements der Kommune sorgt für Vertrauen. Widersprüchliches verwirrt.

4. **Mitarbeiterinnen und Mitarbeiter zuerst**
   Wenn die IT-Strukturen der Kommune angegriffen werden, müssen zuerst die eigenen Mitarbeiterinnen und Mitarbeiter über den aktuellen Sachstand informiert werden. Es wirft ein schlechtes Licht auf die Leitung, wenn die Mitarbeitenden erst durch die Medien/Social Media oder anderen Quellen »von außen« von der Krise erfahren.

5. **Kein »Kein Kommentar« bei Gerüchten und Spekulationen**
   Wenn Sie mit Gerüchten und Spekulationen konfrontiert werden, sollten Sie sich zunächst über den Wahrheitsgehalt informieren, bevor Sie öffentlich kommunizieren. Sie sollten genau abwägen, welche Informationen für die Öffentlichkeit bestimmt sind und diese ggf. mit zuständigen Stellen abstimmen. Hier gilt: Erst informieren, dann kommunizieren!

6. **Gesprächspartnerinnen und -partner prüfen**
   Bitte achten Sie darauf, wem Sie Informationen anvertrauen und mit wem Sie diese teilen. Lassen Sie sich nicht auf Hintergrundgespräche oder »off-the-record-Statements« im kleinen Kreis ein. Der Konkurrenzdruck unter den Medien nimmt zu, alles wird geschrieben. Auch vertrauliche Aussagen, die ausdrücklich nicht für die Öffentlichkeit bestimmt sind, könnten dennoch veröffentlicht werden. Daher dringend den Einzelfall und mögliche Konsequenzen abwägen.

7. **Klare, einfache Sprache**
   (Verwaltungs-) Fachleute neigen dazu, Dinge in ihrer eigenen Fachsprache auszudrücken. Gerade in der Krisenkommunikation ist es aber wichtig, Informationen möglichst einfach und klar weiterzugeben, in der Sprache von Journalistinnen und Journalisten bzw. ihrer Leserinnen und Leser. Wichtige Aussagen stehen am Anfang und am Schluss eines Statements. Keine wortreichen Rechtfertigungen, sondern wichtige Fakten nennen.

8. **Online-Kommunikation**
   In der Krise zahlt sich Social-Media-Dialog aus. Die Reaktion muss auch außerhalb der Geschäftszeiten relativ rasch (innerhalb von 2 Stunden) erfolgen und für die verschiedenen Kanäle aufbereitet werden

3 – Checkliste interne und externe Kontakte

Die Leitung einer Kommune sollte über eine aktuelle Liste der internen Ansprechpartner und Ansprechpartnerinnen verfügen, die es ermöglicht, die wichtigsten Kontakte in der Stadt-/Kommunalverwaltung zu informieren und erste Informationen über Art und Umfang des Vorfalls zu beschaffen. Gleichzeitig sollten aktuelle Kontakte aller wesentlichen externen Ansprechpartner und Ansprechpartnerinnen aufgelistet sein.

Diese Listen müssen auch verfügbar sein, wenn aufgrund des IT-Vorfalls kein Online-Zugriff möglich ist!

Liste mit internen Ansprechpartnerinnen und Ansprechpartnern sollte enthalten:

- **Beauftragte** für Arbeits- und IT-Sicherheit, Beauftragte für Datenschutz
- **Verwaltungsleitung**, Mitglieder des Krisenstabs (sofern eingerichtet)
- **Pressestelle** bzw. Kommunikationsbeauftragte/Ansprechpartner und Ansprechpartnerinnen für Presseanfragen und Medienkontakte
- Mitarbeiterinne und Mitarbeiter

Liste mit externen Ansprechpartnerinnen und Ansprechpartnern sollte enthalten

- **Ermittlungsbehörden:** örtliche Polizei, LKA ZAC (Zentrale Ansprechstelle Cybercrime des hessischen Landeskriminalamts)
- Meldepflicht bei **Datenschutzaufsichtsbehörde** (HBDI – Hessischer Beauftragter für Datenschutz und Informationsfreiheit)
- **Politik** und Parteien
- Lokale und regionale **Medien**
- **Nachbarkommunen und Landkreise**
- Möglicherweise betroffene **kommunale Unternehmen**
- **IT-Dienstleister**
- **Hessen CyberCompetenceCenter (Hessen3C, Ansprechpartner für Cybersicherheit in Hessen):** https://hessen3c.de/unsere-leistungen/fuer-kommunen

  NOTFALLHOTLINE 0611 353 9900

- **Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität** (ZIT), Außenstelle der Generalstaatsanwaltschaft Frankfurt am Mai). Im Fall eines laufenden Ermittlungsverfahrens hat diese Stelle die Pressehoheit inne
- Falls vorhanden: die eigene **Cyber-Versicherung**

4 – Proaktiv informieren: Haltestatements

Haltestatements sollen proaktiv eine Position einleiten und eine kurze, allgemeine Stellungnahme zum Sachverhalt geben. Damit beugen Sie Spekulationen vor und gewinnen Zeit, bis alle relevanten Fakten recherchiert sind und eine vollständige Stellungnahme abgegeben werden kann.

Für die Anfangsphase

Ein Haltestatement sollte demnach nur in der Anfangsphase bzw. während der Recherchephase in einer Krisensituation eingesetzt werden.

Haltestatements sollten, wie alle Krisenkommunikationsmittel, immer mit den betroffenen Stellen (Presseabteilungen, Verwaltungsleitung, ggf. Fachleute für IT-Sicherheit und Datenschutz, ggf. Aufsichts- und Ermittlungsbehörden) **abgestimmt** werden, bevor sie verwendet werden können.

W-Fragen abarbeiten

- **Was** ist passiert?
- **Wo** ist es passiert?
- **Wer** ist involviert?
- **Wie lange** dauert der Vorfall noch an?
- Evtl. Wann ist es passiert? (vorsichtig nutzen, kein Täterwissen verbreiten)
- Ggf. Wie ist es passiert? (vorsichtig, meist Spekulation)

Interesse und Wunsch nach Aufklärung respektieren

Nicht zu Details äußern, die Spekulationen zulassen

Das Statement kann sowohl an Presse als auch intern an Mitarbeiterinnen und Mitarbeiter, an Aushänge in den Gemeinden, Newsletter, auf der Darksite (→ 9 – Darksite) etc. herausgegeben werden.

Musterformulierung für ein Haltestatement

Aktuell kommt es zu Störungen beim Dienst XY/im Bereich XY aufgrund eines IT-Vorfalls. Wir sind dabei, aufzuklären, was genau passiert ist und wie lange die Störung dauern wird. Wir haben die zuständigen Behörden sowie IT-Expertinnen und -Experten hinzugezogen [nur wenn dies der Fall ist]. Bitte haben Sie Verständnis dafür, dass wir zurzeit keine weiteren gesicherten Aussagen treffen können. Sobald wir mehr wissen, werden wir Sie informieren.

Für weitere Fragen steht Ihnen unser Kontakt XY zur Verfügung.

Musterformulierung für ein Haltestatement auf Social Media:

Der Dienst XYZ/Die Serviceplattform XYZ/Unsere Webseite… ist momentan nicht erreichbar. Wir sind auf der Suche nach der Ursache und bitten um etwas Geduld. Sobald wir mehr wissen, bzw. sobald der DienstXYZ wieder online ist, gibt es ein Update.

Musterantworten bei ersten Anfragen von Medienvertretenden

- Derzeit liegen uns noch keine weiteren Erkenntnisse vor, bitte lassen Sie uns Zeit zur Recherche. Wir werden Sie informieren, sobald wir etwas Genaueres erfahren.
- Bitte lassen Sie uns Zeit zur Untersuchung der Fehlerursache, unsere Expertinnen und Experten sowie externe Ermittlungsbehörden prüfen den Fall.
- Die Untersuchungen laufen, wir müssen die Ergebnisse abwarten. Zu den laufenden Ermittlungen dürfen wir uns nicht äußern. Wir werden Sie informieren, sobald uns Erkenntnisse vorliegen.
- Aus jetziger Sicht kann man zu den Ursachen des ... keine Aussagen treffen. Wir untersuchen den Fall. Bitte haben Sie Verständnis dafür, dass wir das Ergebnis der Untersuchungen erst abwarten.

5 – Rechercheplläne: Fragenkatalog für die interne Bestandsaufnahme

Dieser Fragenkatalog dient zunächst nur der internen Aufklärung in akuten Krisenfällen und als Grundlage für erste Überlegungen sowie als Einstufungshilfe für kommunale Cybersicherheitsvorfälle. Die Fragen müssen fallspezifisch angepasst werden.

Es sind jedoch auch typische Fragen, wie sie in Krisenfällen von Presse und interessierter Öffentlichkeit gestellt werden können. Viele dieser Informationen sollten jedoch nicht zur Kommunikation nach außen gegeben werden, vor allem, solange die Untersuchungen noch laufen.

In einem zweiten Schritt kann deshalb auf Grundlage Ihrer Vorarbeiten ein Fragen-/Antworten-Katalog zur Vorbereitung auf Interviews und Pressekonferenzen erstellt werden, bzw. auch eine Pressemitteilung formuliert werden.
→ 7 – Checkliste Presseinformation.

Geplante Veröffentlichungen zum Vorfall immer vorab mit der involvierten Polizeibehörde und/oder Datenschutzaufsichtsbehörde abstimmen.

Fragenkatalog

Allgemeine Angaben

- **Wichtigste Daten zur Einrichtung**: Anschrift, Zahl der Mitarbeiterinnen und Mitarbeiter
- **Angaben zu Vorfall**
  - Was ist geschehen? (Handelt es sich z.B. um eine IT-Störung, die bspw. durch einen technischen Defekt oder einen Stromausfall verursacht wurde, um einen Datenschutzvorfall oder einen Cyberangriff durch externe Akteure?)
  - Wann ist der Vorfall/die Störung (vermutlich) eingetreten?
  - Wann wurde der Vorfall entdeckt und gemeldet?
  - Ist der Vorfall andauernd oder bereits behoben?
  - Mit welchen Einrichtungen/Behörden wird bei der Behebung zusammengearbeitet? (Polizei, Datenschutzaufsichtsbehörde, BSI, LandesCERT, IT-Dienstleister, andere Kommunen)

Zur Strukturierung der Herangehensweise bei der Einordnung des Vorfalls und dessen Auswirkungen sowie daraus resultierende Datenschutzverletzungen kann es hilfreich sein, entlang der Cybersicherheits-Schutzziele der Vertraulichkeit, Verfügbarkeit und Integrität von Daten und Systemen zu arbeiten.

Verfügbarkeit

- **Technisch**: Welche Systeme oder Daten sind nicht verfügbar (bestimmte Datenbanken, Webseite, E-Mail-Server etc.)?
- **Organisatorisch**: Welche Leistungen und Funktionsbereiche sind durch die Nicht-Verfügbarkeit? Welche konkreten Dienste, Verfahren oder Handlungen können nicht oder nur eingeschränkt durch Mitarbeiterinnen und Mitarbeiter der Kommune oder Bürgerinnen und Bürger durchgeführt werden?
- **Örtlich**: Welcher Standort ist von der Nicht-Verfügbarkeit betroffen?

Vertraulichkeit

- **Welche Arten von Daten** sind von der Störung der Vertraulichkeit potenziell betroffen?
  - » Personenbezogene Daten (Personaldaten von Mitarbeiterinnen und Mitarbeitern oder Abgeordneten, Daten von Bürgerinnen und Bürgern -> wenn möglich Eingrenzung aus welchem Bereich)
  - » Verschlusssachen
  - » andere Arten von Daten
- **Welche Bereiche** sind von der Verletzung der Vertraulichkeit betroffen?
  - » **Technisch**: welche Systeme, IT-Anwendungen oder Datenbanken?
  - » **Organisatorisch**: welche Fachbereiche oder Ämter?
  - » **Örtlich**: welche Standorte
- Durch wen war ein unbefugter Zugriff möglich (Mitarbeiterinnen und Mitarbeiter innerhalb der Organisation, die zu weitgehende Berechtigungen hatten, Angreifer im Rahmen eines Cyberangriffs, ggf. sogar Veröffentlichung erbeuteter Daten im Darknet)?
- War ein unbefugter Zugriff nur grundsätzlich möglich oder gibt es Hinweise, dass der Zugriff auch tatsächlich stattgefunden hat?

Integrität

(Vollständigkeit und Korrektheit von Daten und die korrekte Funktionsweise eines Systems)

- Welche Systeme oder Daten sind von der Verletzung der Integrität betroffen (technisch, organisatorisch, örtlich)?
- Um welche Form bzw. Art der Störung der Integrität handelt es sich?

Auswirkungen und Abhilfemaßnahmen aus der internen Perspektive

- Hat das Ereignis Auswirkungen auf die Umgebung, wie bspw. Landkreise?
- Was wird von wem gegen den Vorfall / die Störung unternommen (Maßnahmen)?
- Welche Auswirkungen hat der Vorfall auf Bürgerinnen und Bürger bzw. ortsansässige Betriebe?
- Liegt eine meldepflichtige Datenschutzverletzung vor?
- Liegt eine Datenschutzverletzung vor, bei der auch betroffene Personen benachrichtigt werden müssen?
- Welche Risiken entstehen ggf. für betroffene Personen in Folge der Verletzung des Schutzes von personenbezogenen Daten? (bspw. durch missbräuchliche Verwendung der Daten wie Identitätsdiebstahl, Phishing)
- Liegen aktuell bereits Hinweise auf eine missbräuchliche Verwendung vor?
- Welche Abhilfe- bzw. Schutzmaßnahmen wurden für betroffene Personen eingeleitet?
- Welche Abhilfemaßnahmen bzw. Vorkehrungen können betroffene Personen selbst treffen, um sich vor Auswirkungen zu schützen?
- Wie lange ist die erwartete Dauer der Störung bzw. wie lange ist der Dienst voraussichtlich nicht erreichbar?
  - » Wenn Dienste erst nach und nach wiederhergestellt werden: Wie werden diese priorisiert? Was wird schnell wiederhergestellt, wo wird es länger dauern?
- Gibt es Alternativen oder Ausweichmöglichkeiten für betroffene Dienste/Standorte?
- Muss die Arbeit eingestellt werden?
  - » Ganz/teilweise/bis wann?
  - » Ist mit Schadensersatzansprüchen zu rechnen?
- Wodurch ist das Schadensereignis eingetreten? VORSICHT! Keine vorschnelle Schuldübernahme, bevor nicht alle Fakten geklärt sind

6 – Checkliste Presseinformation

Grundlage für Presseinformationen sind die geklärten Fragen aus → 5-Fragenkatalog. Bei einer ersten Presseinformation können ungeklärte Sachverhalte problemlos als solche ausgewiesen werden. Dabei gilt: Schnelligkeit vor Vollständigkeit, Richtigkeit vor Schnelligkeit. Formulierungen aus einem Muster-Haltestatement (→ 4-Proaktiv-informieren) können für die erste Presseinformation genutzt werden. Grundsätzlich gilt: Sobald belastbare neue Erkenntnisse da sind, sollten diese nachgereicht und ergänzt werden durch Fakten zu eingeleiteten Maßnahmen. (→ 2-Sicherheit im Umgang mit Medien). Achtung: Nicht für jede neue Information muss eine Presseinformation erstellt und verschickt werden, alternativ können die Medien auch in einem Pressegespräch oder anderen PR-Formaten informiert werden. Es müssen auch nicht zwingend drei Presseinfos erstellt werden.

Warnhinweise

Es ist nicht empfehlenswert, mit KI-Werkzeugen wie ChatGPT eine Pressemitteilung zu generieren. Falls Sie dies dennoch tun, achten Sie bitte unbedingt darauf, dass alle genannten Fakten und Formulierungen stimmen – lesen Sie den Text gründlich durch. (→ Praxistest KI für Texte)

Keine Schuldeingeständnisse – erst wenn Fakten klar sind, mit den Hausjuristen abstimmen und erst dann in die Kommunikation gehen

Cyberkriminelle nutzen Presse- und Medienberichterstattung zu Marketingzwecken. Die Kommunikation von Namen der verantwortlichen Gruppierungen sollte daher wohlüberlegt erfolgen.

Mit Datenschutzverantwortlichen, Ermittlungsbehörden, Kommunikationsstelle abstimmen

Erste Meldung

- Was ist passiert?
- Welche Dienste sind betroffen?
- Wer hilft/unterstützt?
- Welche Maßnahmen wurden bzw. werden getroffen?
- (eventuell: Wann ist es passiert? --> hier aber mit Ermittlungsbehörden abstimmen, könnte Täterwissen sein)

Zweite Meldung (wenn es neue Erkenntnisse gibt)

- Reichert die erste Meldung um Details bzw. neue Erkenntnisse an
- Schildert weitere Maßnahmen, gibt weitere Auskünfte über Art, Umfang und ggf. Konsequenzen
- Gibt ggf. an, was der Bevölkerung geraten wurde

Dritte Meldung

- Berichtet über die Situation vor Ort (Rathaus, Verwaltungsleitung)
- Gibt Einzelheiten über den Prozess
- Gibt Einzelheiten über die Verwendung des Dienstes
- Bringt Stellungnahmen von Experten und Expertinnen
- Beschreibt ggf. Verhalten gegenüber der Bevölkerung (weitere Warnung oder Entwarnung)
- Bringt Einschätzung der Gesamtsituation, Konsequenzen, zukünftige Verbesserungen in Bezug auf IT-Sicherheit

7 – Checkliste Infos für Mitarbeiterinnen und Mitarbeiter

Die Information der Mitarbeiterinnen und Mitarbeiter hat zum Ziel, das Vertrauen der Belegschaft zu sichern/schaffen sowie Spekulationen und Gerüchten sowie damit einhergehender übertrieben negativer Berichterstattung Einhalt zu gebieten.

Grundsatz I: Mitarbeiterinnen und Mitarbeiter vor Presse

MA müssen spätestens mit den Medienvertretern dieselben Informationen erhalten, besser vorher.

Grundsatz II: Nicht zwischen interner und externer Kommunikation unterscheiden

Alles, was MA wissen, sollte auch später an die Presse weitergegeben werden können.

Vor einer Krise

- Bekanntmachen, wo sich MA im Fall einer Krise informieren können – über Aushänge, alternative E-Mail-Adressen, Intranet (wenn dies noch funktioniert), Messengerdienste, etc…
- Alternative Kontaktmöglichkeiten (Diensthandynummern, Fax, …) möglichst aller Mitarbeiterinnen und Mitarbeiter sammeln und dies aktuell halten sowie jederzeit verfügbar halten (zur Not als Ausdruck → 3 Checkliste interne und externe Kontakte)
- Mitarbeiterinnen und Mitarbeiter sensibilisieren: keine öffentlichen Spekulationen, es gibt seitens der Kommune EINE Ansprechperson für die Presse, bei der alle Infos und Anfragen zusammenlaufen und die auch nach außen kommuniziert
  - » Sensibilisieren, dass es womöglich disziplinarische Konsequenzen haben kann, falls konkrete Kommunikationswege nicht eingehalten werden
  - » Auch privat nicht in Social Media spekulieren

Während einer Krise

- Mitarbeiterinnen und Mitarbeiter über vorher bekannt gegebene Kanäle informieren, sonst auch über: Aushänge, alternative E-Mail-Adressenliste, Intranet, Messengerdienste, …
- Die MA-Vertretung informieren, sofern vorhanden
- Info an MA sollte enthalten (→ 4-Proaktiv informieren):
  - » Was ist passiert?
  - » Wer ist involviert?
  - » Was ist zu tun, bzw. was wird getan?
  - » Was sollen Mitarbeitende in den nächsten Tagen/Wochen beachten?
  - » Evtl. Wann ist es passiert? Hier vorsichtig sein und kein Täterwissen verbreiten

Grundsätzlich gilt: auch interne Kommunikation muss, sobald Ermittlungen aufgenommen werden, mit Polizei/Staatsanwaltschaft abgestimmt werden!

Musterformulierung

Liebe Mitarbeiterinnen und Mitarbeiter,
in unseren Systemen ereignete sich ein IT-Vorfall/Zurzeit sind unsere Dienste X, Y und Z ausgefallen. Wir sind dabei, aufzuklären, was genau passiert ist, wer und was alles betroffen ist und wie es dazu kommen konnte. Wir bemühen uns also um Aufklärung, wollen aber Spekulationen und eventuelle Fehlinfos vermeiden und bitten Sie alle deshalb, selbst keine Aussagen gegenüber der Presse oder in sozialen Medien dazu zu treffen. Sobald wir mehr wissen, werden wir Sie zuerst über die bekannten Kanäle [benennen] informieren. Wenn Sie weitere Fragen haben oder Sie uns etwas mitteilen möchten, wenden Sie sich an XYZ, unsere Ansprechperson für alle Kommunikationsfragen.

8 – Monitoring: Wie erfahre ich von der Krise?

Um schnell und kompetent auf einen IT-Vorfall reagieren zu können, müssen Kommunal-Verantwortliche möglichst frühzeitig davon erfahren. Es gibt hier verschiedene Möglichkeiten, einen IT-Vorfall oder eine Kommunikationskrise mitzubekommen.

Über Monitoring-Dienste

für eigene digitale Dienste oder die eigene Webseite bzw. bestimmte URLs kann man sich digitale Benachrichtigungen schicken lassen, wenn diese nicht mehr online sind. Dann gibt es eine Warn-E-Mail. (Diese sollte auch an eine alternative Mailadresse als die Dienst-Mail gehen).

Über Social-Media-Kanäle

Wenn eine Kommune noch keine Social-Media-Präsenz aufgebaut hat, ist es unter anderem für die Krisenkommunikation empfehlenswert, dies zu tun (→ 1 – Vor der Krise). Über diese Kanäle können Bürgerinnen und Bürger sehr niedrigschwellig und jederzeit schreiben, wenn etwas nicht funktioniert („Hallo @GemeindeXYHessen, euer Bürgerportal ist ausgefallen!“ oder ähnliches). Man kann sich auch entsprechende Kanal-Aktivitäts-Benachrichtigungen an eine E-Mail schicken lassen, wenn man nicht jeden Tag in die Kanäle selbst reinschaut.

Ein weiterer Vorteil von Social-Media-Präsenz: über diese Kanäle kann man selbst bei einem Totalausfall der eigenen Systeme noch aktiv kommunizieren und Mitarbeiterinnen und Mitarbeitern, Bürgerinnen und Bürgern sowie der Presse Neuigkeiten senden.

WICHTIG: Die Zugänge zu den Social-Media-Kanälen sollten außerhalb der eigenen IT-Infrastruktur noch an einem alternativen Ort sicher aufbewahrt werden, damit man sich auch im Krisenfall noch einloggen kann. Benachrichtigungen über Kanal-Aktivitäten per E-Mail schicken lassen – hier sollte eine gewählt werden, die auch bei einem IT-Ausfall noch funktioniert.

Über einen **Alert-Servicedienst** (beispielsweise Google Alerts, Talkwalker Alerts, Socialmention oder Hootsuite, alles kostenlose Dienste): Hierüber lassen sich Alerts zu bestimmten Stichwörtern oder Stichwortkombinationen einrichten. Beispielsweise mit den Stichwörtern „BürgerdienstXY GemeindeZ“ oder ähnliches bekommt man aktuelle Nachrichten-Snippets und Meldungen aus Social Media hierzu als Mail geschickt. Auch hier bedenken, dass eine alternative Mailadresse als die dienstliche angegeben wird.

Sonderfall Fake News/Desinformation

Auf Social Media sind falsche Informationen, die bewusst irreführend sind, ein großes Problem. Sollte Ihre Kommune hier in den Fokus geraten und falsche Gerüchte im Umlauf sein, erfahren Sie es am schnellsten über die einzelnen Kanäle selbst und können hier über den kommunalen offiziellen Account gezielt dagegenhalten und Richtigstellungen verbreiten. Oft ist es sinnvoll, ein einzelnes Statement an den eigenen Kanal zu „pinnen“ und stehen zu lassen, evtl. mit einem Link zu weiteren Infos auf einer Webseite, wenn nötig.

9 – Darksite

Was ist eine Darksite?

Eine Darksite ist eine vorbereitete Internetseite, über die im Krisenfall schnell wichtige Informationen online gestellt werden können. Die Darksite ermöglicht es, schnell und aus erster Hand Fragen von Betroffenen, der allgemeinen Öffentlichkeit oder den Medien zu beantworten.

Um die Darksite zeitnah online zu schalten, sollten Sie diese im Vorfeld vorbereiten. Dazu gehört:

- Klärung Technik:
  - » Wo liegt die Darksite?
  - » Wer schaltet die Darksite wie frei? Ggf. mit externem IT-Dienstleister klären
- Bereiten Sie Textbausteine vor, um die Darksite schnell und einfach zu erstellen
- Die Gestaltung sollte übersichtlich sein

Elemente einer Darksite

Inhalte

- Aktuelle Informationen zum Geschehen, wie z. B. Pressemitteilungen
- Verhaltenshinweise für die Betroffenen
- Kontaktdaten von Ansprechpersonen, wie z. B. der Pressestelle oder dem/der Beauftragten für Datenschutz
- Bürger-Hotline (wenn vorhanden)
- Häufig gestellte Fragen (FAQ) und deren Antworten
- Links zu bzw. direkte Einbindung von weiteren wichtigen Informationsquellen (Social Media, etc.)
- Impressum / Datenschutzinformation

Bei laufenden Ermittlungen gilt: Inhalte immer mit den Ermittlungsbehörden (Polizei, Staatsanwaltschaft) abstimmen!

Design und Technik

- Die Darksite sollte so gestaltet sein, dass sie **einfach und schnell lädt** (keine großen Bilder etc.)
- Betroffene sollten sich gut darauf zurechtfinden, die wichtigsten Daten sollten **übersichtlich** platziert werden.
- Beim Design sollte man darauf achten, dass es auch **für mobile Endgeräte optimiert** ist.
- Außerdem ist es wichtig, dass die Darksite auf einem leistungsstarken **Server außerhalb der eigenen kommunalen Infrastruktur** gehostet wird und Backups vorhanden sind, um sicherzustellen, dass sie jederzeit verfügbar ist, selbst wenn der primäre Server ausfällt.

10 – Szenario-Matrix für die Öffentlichkeitsarbeit

Für die Kommunikation im Fall einer Cyberkrise ist es wichtig, die Auswirkungen der Krise auf verschiedene Bezugsgruppen einzuschätzen. Eine Szenario-Matrix dient dazu, die Interessen und Sichtweisen von Kommunikationspartnerinnen und -partnern systematisch zu reflektieren und zielgerichtete Botschaften für die unterschiedlichen Zielgruppen zu definieren.

Ein Planspiel kann bei der Vorbereitung helfen: Diskutieren Sie die Szenarien mit 2-5 Personen und tragen Sie Ihre Ergebnisse stichpunkt- artig in die Matrix ein. Das ausgefüllte Beispiel zeigt, wie eine bearbeitete Version aussehen kann, stellt aber keine Musterlösung dar, denn die Ergebnisse sind oft von konkreten Gegebenheiten vor Ort abhängig.

Mögliche Szenarien für eine Cyber-Krise sind zum Beispiel:

1. Ransomware-Attacke: Alle/viele Rechner/Dienste im Rathaus sind nicht mehr zugänglich
2. IT-Dienst der Stadt/Kommune wurde gehackt und steht nicht mehr zur Verfügung.
3. Personenbezogene Daten von Bürgern sind im Darknet aufgetaucht.
4. Die Webseite der Gemeinde wird durch Unbekannte kontrolliert, die städtischen Informationen werden manipuliert.
5. DDoS Angriff
6. Stromausfall – mit verschiedenen Schwerpunkten (wenn/wo)
7. Sicherheitslücke wird bekannt – was muss ich bedenken
8. SPAM-Versand über offizielle Accounts
9. Infrastrukturausfall als Überpunkt zu Stromausfall / Telefon etc

THEMEN-Beispiel: Ransomware-Angriff

Ransomware-Angriff	Medien	Mitarbeitende	Politik	Bürgerinnen und Bürger	Kommunale Unternehmen	Nachbar-Kommunen und Landkreise
Reaktion der Zielgruppe	Lokale und regionale Medien berichten – Fokus auf Ausfällen	MA sind verunsichert und wissen nicht, wie sie auf Anfragen aus dem privaten Umfeld reagieren sollen	Vertreterinnen und Vertreter aus dem Bereich Politik haben ein Informationsbedürfnis, z. B. aufgrund von Medienanfragen. Politikvertreterinnen und -vertreter sowie Parteien möchten Informationen und bewerten den Vorfall bereits auf Basis von Hören-sagen.	Bürgerinnen und Bürger sind verärgert, weil gewisse Dienste gestört oder ausgefallen sind	Sind ggf. von Ausfällen direkt/indirekt betroffen, unsicher über Auswirkungen	Verunsicherung der Bürgerinnen/Bürger: Erhöhter Kommunikationsaufwand
Botschaft an die Zielgruppe	Die Stadt/Gemeindeverwaltung ist handlungsfähig, externe Unterstützung von Experten angefragt.	Dies ist eine Notfall-Situation: Haltung der MA ist besonders wichtig – Multiplikatoren. Verwaltungsleitung informiert regelmäßig asap.	Dies ist ein Notfall – Amtsleitung informiert asap - Unterstützung durch besonnene Reaktion.	Wir arbeiten gemeinsam daran, ausgefallene Services wieder in Betrieb zu nehmen und bieten Alternativen wo möglich.	Dies ist eine Notfallsituation. Klärung läuft, Informieren asap. Wichtiger Partner für die Kommunikation.	Brauchen Unterstützung (Räume, Dienste, etc.). Bieten Personal und ggf. andere Kompensation.
Mögliche Gegen-Maßnahme	Medien als Kommunikationspartner nutzen – Fortschritte auch über Presse kommunizieren	Vollversammlung im Rathaus, Telefonkonferenzen oder Telefonketten, Aushänge Messenger-Gruppe für MA	Einladung zu besonderem Briefing durch Leitung des Krisenstabs	Öffentl. Aushänge, Bekanntgabe von Notfall-Telefonnr.; Unterstützung durch Nachbar-kommunen, Social Media-Kommunikation	Besondere Ansprechpartner festlegen und kommunizieren.	Bürgermeister-Treffen organisieren: Unterstützungsmaßnahmen definieren.
Sonstiges						

Szenario-Matrix

THEMA:	Medien	Mitarbeitende	Politik	Bürgerinnen und Bürger	Kommunale Unternehmen	Nachbar-Kommunen und Landkreise
Reaktion der Zielgruppe						
Botschaft an die Zielgruppe						
Mögliche Gegen-Maßnahme						
Sonstiges						