BIGS ESSENZ

Brandenburgisches Institut für **Gesellschaft** und **Sicherheit**



WENN DIE VERWALTUNG OFFLINE IST: KRISENKOMMUNIKATION BEI IT-SICHERHEITSVORFÄLLEN IN KOMMUNALEN VERWALTUNGEN

Esther Kern

Die Studie untersucht die Krisenkommunikation kommunaler Verwaltungen bei IT-Sicherheitsvorfällen. Auf Basis eines abstrahierten Phasenmodells kommunaler IT-Sicherheitsvorfälle beginnend ab dem Einfallstor über die unmittelbare Reaktion zu Reflexion und Transfer werden die Maßnahmen der Krisenkommunikation analysiert. Dabei zeigt sich, dass das Thema Krisenkommunikation in Bezug auf IT-Sicherheitsvorfälle bei den Kommunen oftmals kaum bis wenig vorbereitet ist. So fehlen z. B. etablierte Meldeketten für Verdachtsmomente, auch alternative interne Alarmierungswege für den Ausfall regulärer IT-Kommunikation sind nicht vorbereitet.

Zum Abschluss gibt die Studie Handlungsempfehlungen: Vorbereitung der Krisenkommunikation und Klärung von Zuständigkeiten, Einbindung kommunikationsverantwortlicher Personen in den Krisenstab, Etablierung redundanter Melde- und Alarmierungsstrukturen sowie eine konsequente Abschlusskommunikation. Dabei sollten die Regeln der guten Krisenkommunikation beachtet werden.

Die vorliegende Kurzstudie wurde im Förderprogramm zivile Sicherheitsforschung des Bundesministeriums für Forschung, Technologie und Raumfahrt gefördert.

1 EINLEITUNG

Krisen werden maßgeblich durch ihre Krisenkommunikation geprägt. Das zeigt auch der aktuelle IT-Sicherheitsvorfall der Berliner Landesverwaltung. Informationen wurden nur reaktiv und scheibchenweise herausgegeben. Wie das Krisenmanagement wahrgenommen wird, unabhängig von seiner tatsächlichen Qualität, hängt stark mit der Krisenkommunikation zusammen. IT-Sicherheitsvorfälle unterscheiden sich dabei nicht von anderen Krisensituationen. Dennoch geraten übergeordnetes Krisenmanagement und Krisenkommunikation hier häufig aus dem Blick, weil eine ausgefallene IT zunächst als rein technische Angelegenheit erscheint. Doch die technische Bearbeitung eines IT-Sicherheitsvorfalls genügt nicht; es bedarf auch organisatorischer und kommunikativer Maßnahmen.

Die vorliegende Studie widmet sich explizit der Krisenkommunikation von kommunalen Verwaltungen bei IT-Sicherheitsvorfällen. Kommunale Verwaltungen sind oft wenig bis gar nicht auf diese Art von Vorfällen vorbereitet. Dies betrifft auch ihre interne wie externe Krisenkommunikation. Gerade im Bereich der Krisenkommunikation zeigt sich jedoch, dass mit begrenzten Ressourcen Abläufe angepasst und Prozesse eingeführt werden können, die dem Krisenmanagement insgesamt zugutekommen. Auf Basis von 17 semi-strukturierten Interviews mit bereits von IT-Sicherheitsvorfällen betroffenen kommunalen Verwaltungen analysiert die Studie die Krisenkommunikation in diesem Kontext. Zur Einordnung gibt sie zunächst einen Überblick über den Gegenstand der Krisenkommunikation, deren Besonderheiten in kommunalen Verwaltungen sowie die kommunikativen Anforderungen bei IT-Sicherheitsvorfällen. Abschließend werden Handlungsempfehlungen formuliert.

2 KRISENKOMMUNIKATION

Kommunikation ist ein elementarer Bestandteil des Krisenmanagements. Denn jede Krise stellt auch eine Kommunikationsherausforderung dar. Es ist eine Balance zwischen Schnelligkeit und Sorgfalt sowie zwischen Transparenz und dem Schutz sensibler Informationen, laufender Ermittlungsverfahren und Persönlichkeitsrechten erforderlich. Riecken (2014) stellt fest, dass „Kommunikation [trägt] neben dem tatsächlichen Response Management entscheidend dazu [bei], die Krise zu überstehen."[1] Die Verantwortlichen für Kommunikation sind daher ein wichtiger Teil des Krisenmanagementteams. Krisenkommunikation gilt es jedoch strategisch vorzubereiten und zu planen. Denn „[e]ine nicht vorbereitete oder fehlerhafte Krisenkommunikation kann die Situation unkontrolliert eskalieren lassen, das Vertrauen der Bevölkerung nachhaltig beeinträchtigen und somit die Glaubwürdigkeit verantwortlicher Stellen beschädigen."[2] Oder wie es im BSI-Standard 100-4 Notfallmanagement beschrieben ist „Krisenkommunikation ist einer der zentralen Erfolgsfaktoren des Krisenmanagements."[3]

Es ist zu unterscheiden zwischen Risiko- und Krisenkommunikation, die in einer engen Beziehung zueinanderstehen und sich wechselseitig beeinflussen. Alles, was vor dem Eintritt einer Gefahr, eines Schadens oder einer anderweitigen Krise passiert, ist dem Feld der Risikokommunikation zuzuordnen. Teil der Risikokommunikation sind die Vermittlung von „Informationen zu möglichen oder zu erwartenden Risiken sowie zum Umgang mit diesen (d. h. Entscheidungen, Maßnahmen, Pläne) vor Eintritt eines Schadensfalles."[4] Die Krisenkommunikation tritt hingegen dann in Kraft, wenn die Krise bereits eingetreten ist. Ihr Ziel ist es, das Schadensereignis möglichst effektiv zu bewältigen bzw. eine Kriseneskalation und den damit einhergehenden Vertrauensverlust zu verhindern. Krisenkommunikation übermittelt den verantwortlichen Akteuren die Informationen, die sie zum Handeln benötigen, und informiert zugleich alle relevanten Zielgruppen. Dies kann die eigene Belegschaft sein, Partner, Medien und die Bevölkerung. In der Praxis zeigen sich jedoch fließende Übergänge. Die folgende Studie fokussiert sich auf die Krisenkommunikation.

1 Riecken, Martin (2014): Erfolgskritische Faktoren der angewandten Krisenkommunikation, in: Thießen, Ansgar (2014): Handbuch Krisenmanagement, S. 323.
2 Bundesministerium des Innern (2014), Leitfaden Krisenkommunikation, S. 3.
3 Bundesamt für Sicherheit in der Informationstechnik (2008), BSI-Standard 100-4 Notfallmanagement, S. 76.
4 Tettenborn, Felix; Peters, Anja (2014): Leitfaden zur Risiko- und Krisenkommunikation in der Trinkwasserversorgung zur Verbesserung der Sicherheit in Hinblick auf CBRN-Bedrohungsszenarien: Kommunikation als vertrauensbildende Maßnahme und Handlungsempfehlungen zur Vorbereitung einer effektiven Krisenkommunikation, S. 13.

2.1 Krisenkommunikation in kommunalen Verwaltungen

Die Strategien, Maßnahmen und Best-Practices der Krisenkommunikation für die kommunale Verwaltung unterscheiden sich in der Praxis nur bedingt von denen privater Unternehmen oder anderer Organisationen. Die Bedingungen und Konsequenzen von Krisenkommunikation sind für staatliche Stellen jedoch andere.

Für ein Privatunternehmen kann eine Krisensituation im schlimmsten Falle in einer Insolvenz enden. Eine Kommune kann nicht vom „Markt" verschwinden, selbst wenn einzelne Personen aufgrund der Krise ihr Amt oder ihre Position verlieren. Wenn Krisenkommunikation in Kommunen schiefläuft, verliert die Kommune etwas anderes: die Glaubwürdigkeit, dass der Staat seiner Daseinsfürsorge nachkommt und handlungsfähig ist. Damit einher geht ein möglicher Vertrauensverlust in demokratische Strukturen.

Auf der anderen Seite sind private Unternehmen prinzipiell freier in ihrer Krisenkommunikation als Kommunen. Ob eine Auskunftsverweigerung sinnvoll ist, ist für Unternehmen Abwägungssache in der individuellen Krisensituation. In Kommunen gestaltet sich dies anders. Denn aufgrund der Informationsfreiheitsgesetze der Länder hat die Bevölkerung ein Recht auf Auskunft. Einschränkungen ergeben sich dann, wenn z. B. Persönlichkeitsrechte verletzt werden oder staatsanwaltschaftliche Verfahren laufen. In diesen Fällen kann die Kommune die Auskunft oder zumindest die Details zu bestimmten Vorgängen verweigern. Zudem geben die Presserechte der Länder den Medien ebenfalls einen gesetzlichen Anspruch auf Informationen, die zur Not auch eingeklagt werden können.[5]

Darüber hinaus agiert die Kommune im politischen Mehrebenensystem der Bundesrepublik Deutschland. Kommunen sind verfassungsrechtlich gesehen keine eigene Staatsebene, sondern gehören zu den Verwaltungseinheiten der Länder, wenn auch mit Selbstverwaltungsrechten. Aufgrund dessen ist die Kommune verpflichtet sogenannte Pflichtaufgaben durchzuführen. Hierzu gehören z. B. die Bereitstellung von Infrastrukturen wie u. a. Abwasserbeseitigung oder Schulhausbau, Sicherheit und Ordnung oder das Pass- und Meldewesen. Damit ist der Handlungsrahmen für kommunale Verwaltungen oftmals sehr eng gesteckt, gleichzeitig ist die Kommune die Ansprechperson für die Bevölkerung und ggf. auch Vermittlerin von staatlichen Maßnahmen, wie es z. B. während der COVID-19-Pandemie der Fall war.

In der Vergangenheit waren typische Krisenfälle für kommunale Verwaltungen vor allem Naturkatastrophen wie 2021 im Ahrtal oder das Hochwasser an der Elbe und weiteren Flüssen im Jahr 2013. Stark herausgefordert wurden die Kommunen auch ab 2020 durch den Beginn der COVID-19-Pandemie. Hinzu kam 2022 der Beginn der Vollinvasion auf die Ukraine und die damit entstandene Fluchtbewegung aus der Ukraine auch nach Deutschland und einer veränderten Sicherheitslage.

Mit dem steigenden Grad der Digitalisierung der Verwaltung bei gleichzeitig steigender Anzahl von Cyberangriffen, kommt es auch vermehrt zu Ausfällen von digitalen Infrastrukturen. Gleichzeitig dürften Klimaveränderungen und die damit einhergehende Zunahme von Naturkatastrophen vermehrt auch technische Ausfälle der IT-Infrastruktur verursachen. Dies zeigte sich schon im Sommer 2026 durch die Hitzewellen. So überhitzten beispielsweise zentrale Server im Rathaus der Stadt Schriesheim, so dass keine IT-unterstützten Leistungen mehr angeboten werden konnte und die telefonische Erreichbarkeit eingeschränkt war.[6]

Kommunikativ werden kommunale Verwaltungen in der Zukunft verstärkt herausgefordert durch neue Krisenformen sowie dem gleichzeitigen Auftreten multipler Krisen. Auch langanhaltende Krisenzustände wie die Pandemie fordern eine andere Art der Kommunikation als ein Ereignis welches nur für wenige Tage anhält. Dies zeigt auch die Analyse von Otten und Schophaus (2023). Auf bekannte Krisen fühlten sich die Kommunen vorbereitet, jedoch nicht auf neue und unvorhersehbare. Hierfür braucht es neue „kommunikative Modi."[7]

5 Latsch, Johannes (2025): Bürgermeister und Krisenkommunikation: Medien- und Öffentlichkeitsarbeit vom Alltagsstress zur Katastrophe, 2. Auflage.

6 Sperl-Hofmann, Heike (2026): Hitze legt Schriesheimer Rathaus-Server stundenlang lahm, in: Mannheimer Morgen, https://www.mannheimer-morgen.de/neckar-bergstrasse_artikel,-neckar-bergstrasse-hitze-legt-schriesheimer-rathaus-server-stundenlang-lahm-_arid,2384602.html, zuletzt abgerufen 05.08.2026.

7 Otten, Henrique Ricardo; Schophaus, Malte (2023): Krisenkommunikation in Kommunen: Organisation und Expertise in der Krisenkommunikation von Kommunalverwaltungen, Verwaltung & Management, 29 (5), S. 206.

2.2 Krisenkommunikation bei IT-Sicherheitsvorfällen

Combs et al. (2021) bezeichnen u. a. Datenschutzverletzungen und damit indirekt auch IT-Sicherheitsvorfälle als sogenannte „sticky crises", also zähe oder hartnäckige Krisen. Damit bezeichnen sie Krisensituationen, die sich von anderen durch ihre Komplexität und spezifischen Herausforderungen unterscheiden. Diese Krisen haben sich durch die Digitalisierung und das Aufkommen digitaler Kanäle verstärkt. Dabei gibt es nicht die hartnäckige Krise, sondern unterschiedliche Arten. Neben Datenschutzverletzungen, die bei den (potenziell) betroffenen Opfern ein starkes Gefühl der Vulnerabilität und direkten Betroffenheit hervorrufen, sind auch Gesundheitskrisen oder branchenweite Krisen mit entsprechenden Spillovereffekten solche Arten der Krise. Zudem können diese Krisen durch kontextbezogene Faktoren wie z. B. Desinformationen oder sozialen Fragen, die den Effekt für bestimmte Gruppen intensivieren, verstärkt werden. Davon betroffen ist vor allem die Krisenkommunikation, die situativ angepasst werden muss.[8]

Gerade in Fällen, in denen die Öffentlichkeit bzw. die betroffenen Stakeholdergruppen denken, dass die Organisation selbst verantwortlich für den IT-Sicherheitsvorfall ist, können emotionale Reaktionen wie Wut verstärkt werden.[9] Dabei können Verzögerungen in der Kommunikation oder der Versuch des Verschweigens einer Datenschutzverletzung dazu führen, dass die Verantwortlichkeit bei der Organisation gesucht wird.[10] Deswegen benötigen solche Vorfälle eine schnelle Reaktion, wenn nicht sogar eine fast sofortige, und eine immerzu angepasste Kommunikation und Reaktionsstrategie im Verlauf der Krise.[11] So z. B. wenn anfangs nicht klar ist, ob Daten durch die Angreifergruppe ins Darknet hochgeladen wurden und dies im Laufe der Ermittlung ersichtlich wird.

Relevant bei der Kommunikation ist auch, dass die Kommunikation präzise ist und die notwendigen Informationen enthält.[12] Dabei kann auch der Hinweis erfolgen, dass bestimmte Informationen noch nicht vorliegen, z. B. zu einem frühen Zeitpunkt. Knight und Nurse (2020) stellen fest, dass eine Balance zwischen Richtigkeit und Schnelligkeit benötigt wird, es jedoch wichtiger ist proaktiv zu kommunizieren als reaktiv auf eine Medienmeldung reagieren zu müssen.[13] Wichtig ist auch Verantwortung für den Vorfall zu übernehmen und dabei intern wie extern Empathie zu zeigen. Hinzu kommt, dass die Organisation zum Ausdruck bringt, dass sie wichtige und entscheidende Schritte übernimmt, um den Vorfall zu bewältigen und den Schaden soweit wie möglich zu begrenzen.[14] Dabei sollte eine Sprache gewählt werden, die verständlich ist und zu technische Begrifflichkeiten vermeidet.[15]

Die Kommunikation sollte über alle verfügbaren Kanäle erfolgen. Sollten Standardkanäle wie z. B. die Website einer Kommune zu dem Zeitpunkt nicht verfügbar sein, sollte überlegt werden welche möglichen Alternativkanäle es gibt.[16] Zudem sollte die Organisation im besten Fall die sozialen Medien wie auch klassischen Medien für Reaktionen auf die bisherige Kommunikation und den Vorfall monitoren.[17] In Zeiten des verstärkten Aufkommens von Desinformationen kann so auch frühzeitig auf mögliche Falschinformationen oder Gerüchte reagiert werden.

Im weiteren Verlauf sollte die Organisation kommunizieren inwiefern und in welchem Maße sie Maßnahmen ergreift, um das Level an Informationssicherheit zu verbessern.[18] Hier sollte kein Aufschluss über detaillierte Maßnahmen gegeben werden, die relevanten Stakeholdergruppen – bei kommunalen Verwaltungen die Bevölkerung – aber den Eindruck bekommen, dass sich der Status quo verbessern wird.

8 Coombs, Timothy; Holladay, Sherry J.; White, Rick (2021): Corporate Crises: Sticky Crises and Corporations, in: Jin, Yan; Reber, Bryan H.; Nowak, Glen J. (Hrsg.): Advancing Crisis Communication Effectiveness: Integrating Public Relations Scholarship with Practice, S. 35-51.
9 Syed, Romilla (2019): Enterprise reputation threats on social media: A case of data breach framing, in: The Journal of Strategic Information Systems, Volume 28 (3), S. 257-274.
10 Coombs, Timothy; Holladay, Sherry J.; White, Karen L. (2021): Situational Crisis Communication Theory (SCCT) and Application in Dealing with Complex, Challenging, and Recurring Crises, in: Jin, Yan; Reber, Bryan H.; Nowak, Glen J. (Hrsg.): Advancing Crisis Communication Effectiveness: Integrating Public Relations Scholarship with Practice, S. 165-180.
11 Reber, Bryan H.; Yarbrough, Richard; Nowak, Glen; Jin, Yan (2021): Complex and Challenging Crises: A Call for Solutions, in: Jin, Yan; Reber, Bryan H.; Nowak, Glen J. (Hrsg.): Advancing Crisis Communication Effectiveness: Integrating Public Relations Scholarship with Practice, S. 3-16.
12 Hytönen, Eveliina; Ruoslahti, Harris (2025): Crisis Communication Guidelines to Support Cyber Resilience, in: Lipps. Christoph; Han, Bin (2025): The Proceedings of the 24th European Conference on Cyber Warfare and Security, ECCWS 2025, S. 222-229.
13 Knight, Richard; Nurse, Jason R.C. (2020): A framework for effective corporate communication after cyber security incidents, in: Computers & Security, 99, 102036.
14 Hytönen, Eveliina; Ruoslahti, Harris (2025).
15 Knight, Richard; Nurse, Jason R.C. (2020).
16 Hytönen, Eveliina; Ruoslahti, Harris (2025).
17 Syed, Romilla (2019).
18 Bentley, Joshua; Ma, Liang (2020): Testing perceptions of organizational apologies after a data breach crisis, Public Relations Review, 46(5),101975.



Foto © iStock/Linda Wa

3 KRISENKOMMUNIKATION KOMMUNALER VERWALTUNGEN BEI IT-SICHERHEITSVORFÄLLEN

3.1 Datenerhebung und Methodik

Die empirische Grundlage dieser Studie bilden 17 semistrukturierte Expertinnen- und Experteninterviews zur digitalen Resilienz kommunaler Verwaltungen, die zwischen April 2025 und Mai 2026 durchgeführt wurden. Die befragten Personen kamen aus den Bereichen IT, Informationssicherheit, Digitalisierung und Verwaltungsleitung, und waren unmittelbar an der Prävention, Bewältigung oder Nachbereitung von IT-Sicherheitsvorfällen beteiligt. Ziel war es, vergangene Vorfälle aus Sicht der betroffenen Kommunen zu rekonstruieren und wiederkehrende technische, organisatorische sowie kommunikative Herausforderungen zu identifizieren.

Die Auswahl der Interviewpartner erfolgte auf Basis einer Recherche öffentlich dokumentierter IT-Sicherheitsvorfälle, insbesondere über kommunaler-notbetrieb.de[19] sowie den Suchmaschinen Google und DuckDuckGo. Anschließend wurden die betroffenen Kommunen schriftlich zur Teilnahme eingeladen. Berücksichtigt wurden Kommunen unterschiedlicher Größe und regionaler Verteilung sowie Vorfälle verschiedener Schweregrade. Die Stichprobe wurde bewusst fallorientiert und nicht zufallsbasiert zusammengestellt und erlaubt daher keine statistische Verallgemeinerung.

Die Auswertung erfolgte nach einem Grounded-Theory-informierten Vorgehen in Anlehnung an Strauss und Corbin. Ziel war die systematische Entwicklung von Kategorien sowie die Analyse von Zusammenhängen zwischen technischen, organisatorischen und kommunikativen Faktoren. Begriffe wie „die Mehrheit“, „viele“, „einige“ oder „vereinzelt“ beziehen sich ausschließlich auf die ausgewerteten Interviews und stellen keine statistische Verallgemeinerung dar.

19 Kommunaler Notbetrieb (o. J.): https://kommunaler-notbetrieb.de/, zuletzt abgerufen 09.10.2026.

Aus der Kodierung entwickelte sich ein abstrahiertes Sechs-Phasen-Modell kommunaler IT-Sicherheitsvorfälle:



Abbildung 1: Abstrahiertes Phasenmodell kommunale IT-Sicherheitsvorfälle, eigene Darstellung.

Im Mittelpunkt der vorliegenden Studie stehen die Erkenntnisse zur Krisenkommunikation bei IT-Sicherheitsvorfällen in kommunalen Verwaltungen. Die Analyse beginnt ab der Phase zwei des Phasenmodells.

3.2 Erkennungs- & Meldephase

Eine für die Reaktionsfähigkeit der Kommunen besonders relevante Phase liegt zwischen dem initialen Eindringen in das Netzwerk und der erstmaligen Entdeckung des Vorfalls. Je länger eine Kompromittierung unbemerkt bleibt, desto mehr Zeit steht den Angreifern grundsätzlich zur Verfügung, um sich innerhalb der Systeme weiterzubewegen, zusätzliche Zugänge einzurichten, Daten abzugreifen oder technische Schutzmaßnahmen zu umgehen. In dieser Phase sind einerseits technische Möglichkeiten zum Monitoring der Systeme wie z. B. des Netzwerks oder der Server wichtig. Andererseits ist es auch wichtig, dass Mitarbeitende sich melden, wenn ihnen Dinge verdächtig vorkommen oder sie auf einen Link geklickt haben, der ihnen im Nachgang doch unsicher erschien.

3.2.1 Vom ersten Verdachtsmoment zur Bestätigung des IT-Sicherheitsvorfalls

Aus kommunikativer Sicht stehen in dieser Phase vor allem die internen Meldewege im Vordergrund. In keinem der ausgewerteten Interviews wurde eine klar definierte und organisationsweit bekannte Meldekette für verdächtige Beobachtungen explizit beschrieben. Dieser Befund ist jedoch mit Vorsicht zu interpretieren: Die konkrete Ausgestaltung interner Meldewege bei Verdachtsmomenten wurde nicht in jedem Interview gesondert und mit gleicher Ausführlichkeit abgefragt. Aus dem Fehlen entsprechender Aussagen lässt sich daher nicht unmittelbar schließen, dass in allen Kommunen keinerlei Richtlinien bestanden.

Die Analyse der Antworten legt jedoch nahe, dass eine frühzeitige Meldung verdächtiger Beobachtungen in der Regel von der Aufmerksamkeit und Eigeninitiative Einzelner abhing. Dies ist besonders problematisch, wenn die betroffene Person zuvor selbst auf einen Link geklickt, Zugangsdaten eingegeben oder eine andere riskante Handlung ausgeführt hat. In solchen Situationen können Scham, Unsicherheit oder die Sorge vor persönlichen Konsequenzen zu verspäteter oder unterlassener Meldung führen – ein Befund, der mit der Sicherheitskultur der jeweiligen Behörde korreliert.

Dies zeigt sich exemplarisch auch an der folgenden Aussage einer interviewten Person:

Also ich würde auch sagen, wir waren bis zum Hack, (..) waren wir uns auch sicher, dass wir das gut gemacht haben, und ich glaube, der Mensch, über den das geschehen [ist], wenn er sich rechtzeitig gemeldet hätte, weil es ist ja nicht nur der dienstliche Zugang betroffen gewesen, sondern sein privater Zugang ja genauso (...). Wenn er sich rechtzeitig bei uns gemeldet hätte, dann hätten wir seinen Zugang geschlossen, und da wäre nichts passiert. (..) Aber es ist anders gelaufen. (.) Also da hat, ehrlich gesagt, dann auch der Meldeweg irgendwie, war vielleicht nicht bekannt, oder kam auf jeden Fall zu spät. (K13)“ [20]

20 Dieses Zitat sowie folgende wurden in Teilen redaktionell angepasst, um die Leserlichkeit zu verbessern. Die Originalaussage des Zitats wurde dabei nicht verfälscht.

Ob eine frühere Meldung den Vorfall tatsächlich vollständig verhindert hätte, lässt sich im Nachhinein nicht zweifelsfrei feststellen. Die Aussage verdeutlicht jedoch, welche Relevanz die interviewte Person einer zeitnahen internen Meldung für die potentielle Eindämmung des Vorfalls beimisst.

Technische Angriffserkennung und menschliche Meldungen sind dabei nicht als Alternativen, sondern als komplementäre Mechanismen zu betrachten: Technische Systeme erfassen nicht jede Auffälligkeit und ordnen diese nicht immer unmittelbar korrekt ein. Menschliche Meldungen wiederum hängen von der Wahrnehmung, Bewertung und Weitergabebereitschaft der Beschäftigten ab. Die Interaktion beider Ebenen ist somit essenziell.

3.2.2 Die formale Meldekette zur Eskalation

Sollte sich der Verdacht bestätigt haben, setzt aus kommunikativer Sicht die formale Meldekette zur Eskalation der Situation ein. Die Meldung einzelner Beobachtungen durch Beschäftigte (Abschnitt 3.2.1) ist von der formalen Vorfallsmeldung innerhalb der Organisation zu unterscheiden: Erstere dient der Sichtbarmachung einer Auffälligkeit, letztere bildet den Übergang von technischer Feststellung zu koordinierter organisatorischer Reaktion.

Spätestens mit begründetem Verdacht auf einen IT-Sicherheitsvorfall muss geklärt sein, welche internen Stellen zu informieren sind, wer die weitere Eskalation veranlasst und welche Entscheidungsbefugnisse bestehen. Je nach Art und Umfang des Vorfalls können neben der IT u. a. die Verwaltungsleitung, der Informationssicherheitsbeauftragte, der Datenschutzbeauftragte, die interne oder externe Kommunikation sowie betroffene Fachbereiche einzubeziehen sein.

Das Interviewmaterial ergibt kein einheitliches Bild vorab definierter Melde- und Eskalationsstrukturen. Die erste Weitergabe von Informationen hing teilweise davon ab, welche Person die Auffälligkeit feststellte, wen sie persönlich erreichen konnte und welche privaten oder dienstlichen Kontaktdaten verfügbar waren. Dadurch bestand das Risiko verspäteter, unvollständiger oder auf einzelne Personenkreise beschränkter Meldungen.

Eine belastbare Meldekette sollte daher mindestens folgende Punkte festlegen:

- welche Beobachtungen oder Verdachtsmomente eine Meldung auslösen,
- an welche Stelle die Erstmeldung gerichtet wird,
- welche Vertretung bei Nichterreichbarkeit zuständig ist,
- wer über weitere Eskalation und erste Maßnahmen entscheidet,
- welche internen und externen Stellen abhängig vom Vorfall einzubeziehen sind,
- wie die Meldung und daraufhin getroffene Entscheidungen dokumentiert werden.

Ebenso sollten Mindestangaben für eine Erstmeldung definiert werden: Zeitpunkt der Feststellung, beobachtete Auffälligkeiten, mutmaßlich betroffene Systeme, bereits eingeleitete Maßnahmen sowie Erreichbarkeit der meldenden Person. Eine Erstmeldung darf jedoch nicht davon abhängig gemacht werden, dass sämtliche technischen Zusammenhänge bereits abschließend geklärt sind.

Hier besteht ein Spannungsverhältnis zwischen Schnelligkeit und Bewertungssicherheit. Wird mit der Meldung gewartet, bis alle Zusammenhänge bekannt sind, geht wertvolle Zeit verloren. Gleichzeitig sollte eine unbestätigte Auffälligkeit nicht vorschnell als abschließend bewerteter Cyberangriff kommuniziert werden. Eine praktikable Lösung ist die ausdrückliche Einstufung als Verdachtsfall, der nach erster Prüfung bestätigt, herabgestuft oder geschlossen werden kann.

3.3 Unmittelbare Reaktion

In der nächsten Phase stehen zwei Aspekte im Vordergrund: Erstens die interne Alarmierung der Belegschaft und zweitens die Vorfallsmeldung an Dritte, wie z. B. Landes-CERT (Computer Emergency Response Team).

3.3.1 Interne Alarmierung

In keiner der interviewten Kommunen lag eine strukturierte Alarmierung aller Beschäftigten vor. Viele Kommunen stellten sich erst in der Krisensituation die Frage, wie sie die Belegschaft ohne die üblichen Kommunikationsmittel – Telefon, E-Mail, Intranet – erreichen können. Dies ist teils zeitkritisch: Gerade bei Ransomwarevorfällen kann es erforderlich sein, Computer gar nicht erst hochzufahren, um eine möglicherweise noch laufende Malware-Verbreitung zu stoppen.

Ohne Alltagskommunikation griffen Kommunen auf verschiedene alternative Instrumente zurück: Aushänge an Eingängen und Büros, private Telefonnummern und E-Mail-Adressen, teilweise noch funktionsfähige Intranets oder alternative Lösungen über z. B. das Intranet der örtlichen Feuerwehr. Zu späteren Zeitpunkten wurden vereinzelt Betriebsversammlungen einberufen.

Dabei waren die Kommunen mit zwei Problemen konfrontiert:

Erstens die möglichst zeitgleiche Erreichbarkeit der gesamten Belegschaft einschließlich Außenstellen, Zweitstandorte sowie kommunaler Einrichtungen wie Bauhöfe oder Kindergärten. Eine interviewte Person formulierte dies als Lesson Learned:

„Vorab war „die Linie nicht so vorgegeben […], dass auch klar war, wer welchen in welcher Zeit informiert. (..) Das muss ich auch sagen, im Nachgang, alle anrücken lassen, ab in großen Ratssaal, informieren und dann einheitlich, dass alle das Gleiche hören, wie damit umgegangen wird. […] Das war [auch] aufgrund der teilweise einfach fehlenden Kontaktdaten. Dann ging es an die privaten Verbindungen. Da wäre tatsächlich einfach eine gewisse Struktur im Vorfeld gut [gewesen]. (K04)“

Zweitens die Formulierung der Nachricht, insbesondere in schriftlicher Kommunikation: klar und verständlich, ohne Panik auszulösen. Dies gilt besonders für Anweisungen an die Beschäftigten, wie etwa den Computer nicht hochzufahren oder Daten auf einen USB-Stick zu übermitteln, um zu Hause weiterzuarbeiten.

Redundante interne Kommunikationswege erweisen sich gerade zu Krisenbeginn als wichtig. Die erste interne Ansprache setzt den Ton für die weitere Krisenkommunikation und prägt die Stimmung in der Organisation. Zudem trägt klare und verständliche Krisenkommunikation dazu bei, anfängliche Fehler zu vermeiden, die die Krise verstärken oder negativ beeinflussen.

Dies erfordert jedoch Vorbereitung: Es sollte vorab geklärt sein, wie Beschäftigte jenseits der Alltagskommunikation erreicht werden können – vor allem, aber nicht nur, Mitglieder des Krisenstabs. Eine Möglichkeit sind Alarmierungs-Apps; diese Wege müssen den Beschäftigten jedoch bekannt sein, damit Nachrichten entsprechend aufgenommen werden. Zweitens sollte die Kommunikation soweit möglich vorbereitet sein: Den Beschäftigten sollte vorab – vergleichbar mit Verhaltensregeln bei Brand – klar sein, wie sie sich bei einem IT-Sicherheitsvorfall zu verhalten haben.

3.3.2 Vorfallsmeldung an Dritte

Eine externe Vorfallsmeldung erfolgte in der Regel an die lokale Polizei, das Landeskriminalamt (LKA) und/oder die Zentrale Ansprechstelle Cybercrime (ZAC). Bei der großen Mehrheit wurde auch die Landesdatenschutzbehörde informiert. Darüber hinaus meldeten die Kommunen größere und teilweise auch kleinere Vorfälle an das Landes-CERT sowie weitere Landesbehörden. Je nach Anbindung wurden auch der kommunale Zweckverband und das kommunale Rechenzentrum eingebunden – insbesondere dann, wenn Fachverfahren nicht von der Kommune selbst gehostet, sondern z. B. über den Zweckverband bereitgestellt wurden. Kommunale Rechendienstleister sind zudem relevant, wenn sie die Anbindung an das Landesnetz gewährleisten, von dem die Kommune bei schwerwiegenden Vorfällen zwangsläufig getrennt werden muss. Diese Meldungen funktionierten überwiegend reibungslos, wenn teilweise auch verzögert.

Zu späteren Zeitpunkten erfolgten in einigen Fällen Meldungen an Partner oder weitere Dienstleister. Die Vorfallsmeldungen erfolgten nicht notwendigerweise zeitgleich an alle Stellen. Zudem bestand in einzelnen Fällen Unklarheit darüber, an wen die Kommune melden musste bzw. sollte und wo sie externe Unterstützung anfordern konnte. Dies ist auch abhängig vom Bundesland und den dort verfügbaren Unterstützungsleistungen. Diese müssen der Kommune aber erstmal bekannt sein.

3.4 Stabilisierung und Bewältigung



Foto © iStock/Dilok Klaisataporn

Bei IT-Sicherheitsvorfällen hat sich gezeigt, dass die befragten Kommunen standardmäßig bei den größeren Vorfällen extern kommuniziert haben, in einigen Fällen auch gezwungenermaßen. Die interne Kommunikation fiel jedoch oft hinten runter.

3.4.1 Interne Kommunikation

Die interne Kommunikation wurde oft vernachlässigt oder erfolgte nur auf Zuruf. Dies stuften einige Kommunen im Nachhinein als Fehler ein. Meist erfolgte sie reaktiv, ausgelöst durch konkrete Bedarfe, etwa die Anweisung, Computer nicht hochzufahren. Teilweise erhielten Beschäftigte Informationen erst aus zweiter Hand oder über die Presse, was die Stimmung in der Organisation belastete.

Auch im weiteren Verlauf erwies sich die Einhaltung eines einheitlichen Informationsstandes aller Beschäftigten als schwierig – besonders wenn die reguläre Kommunikation per E-Mail oder Intranet weiterhin ausfiel und nur Notlösungen zur Verfügung standen. Einige Kommunen führten Versammlungen durch, meist jedoch erst Tage nach Krisenbeginn. Zudem ist hier nicht garantiert, dass alle Beschäftigten vor Ort sind. Es ist auch eine Frage des Informationsflusses innerhalb der Behörde, dass z. B. die Leitungen von Geschäftsbereichen entsprechend durch den Krisenstab informiert werden und sich dann dafür verantwortlich fühlen, diese Informationen an ihre Mitarbeitenden weiterzugeben. Schlecht geführte interne Krisenkommunikation kann im schlimmsten Fall dazu führen, dass Beschäftigte die Kommune verlassen.

Auch bei kleineren Vorfällen sollte interne Kommunikation nicht unterschätzt werden, etwa um eine weitergehende Kompromittierung zu verhindern oder weitere Beschäftigte vor Social-Engineering-Angriffen – also die Manipulation von Personen durch das Ausnutzen menschlicher Eigenschaften wie z. B. Hilfsbereitschaft oder Vertrauen – zu schützen. Gerade bei Vorfällen, die sich innerhalb kürzester Zeit lösen ließen, spielte sie bei den befragten Kommunen jedoch kaum eine Rolle.

3.4.2 Externe Kommunikation

Die externe Kommunikation funktionierte in der Regel gut, wenn auch meist stark improvisiert. Keine Kommune hatte vorab geklärt, wie sie im Falle eines IT-Sicherheitsvorfalls kommunizieren und die Bevölkerung am besten erreichen möchte. Auch die Entscheidung, welche Partner zu informieren waren und an wen weitere Meldungen – ggf. freiwilliger Natur – erfolgen sollten, war in der Regel unvorbereitet.

Dabei nutzten die Kommunen unterschiedliche Wege. Neben Pressemitteilungen bzw. Mitteilungen in lokalen Zeitungen und Amtsblättern, erfolgte die Information gerade in kleineren Kommunen per Aushang am Rathaus. Darüber hinaus wurden Posts in den sozialen Medien sowie Alarmierungen über Katastrophen- und Gefahren-Apps wie KATWARN genutzt. Häufigkeit und Regelmäßigkeit der externen Kommunikation unterschieden sich erheblich von Kommune zu Kommune.

Eine weitere Schwierigkeit ergab sich daraus, dass Beschäftigte keinen Überblick mehr über anstehende Termine hatten. Das Standesamt etwa wusste nicht mehr, welche Eheschließungen zu welchem Zeitpunkt vereinbart waren – Termine, die grundsätzlich auch ohne IT weitergeführt werden können, deren Daten dann lediglich nachträglich digital zu dokumentieren wären. Eine Kommune löste dies, indem sie über die Pressestelle die Bevölkerung bat, proaktiv auf die Verwaltung zuzugehen.

Erneut zeigte sich zudem die Relevanz der Führungskultur: So gab es immer wieder Bürgermeister und Bürgermeisterinnen bzw. Landräte oder Landrätinnen, die nicht nach außen kommunizieren wollten. Bei kleineren Vorfällen mag dies noch möglich sein, wenn auch nicht unbedingt sinnvoll; bei größeren Vorfällen wird eine Nicht-Kommunikation sehr schnell untragbar. Es gab allerdings auch das Gegenteil und Situationen, in denen durch die Führung zu viel nach außen kommuniziert wurde, um sich entsprechend positiv darzustellen.

Eine dritte Schwierigkeit zeigte sich bei der Information von Betroffenen, wenn deren Daten im Darknet veröffentlicht wurden. So hatten die Kommunen teilweise Mühe zu identifizieren, von wem Daten dort zu finden waren und dies dann auch entsprechend zu kommunizieren. Besonders in der Bevölkerung löste dies Unverständnis aus.



Foto © Shutterstock/ Mo Photography Berlin

3.5 Wiederanlauf

Auch die Phase des Wiederanlaufs ist stark kommunikationsgeprägt. Für viele Beschäftigte signalisiert das Wiederinkrafttreten erster Fachverfahren häufig die Rückkehr zum Normalzustand. Hier bedarf es guter Kommunikation seitens des Krisenmanagementteams, da die dahinterstehende Doppelbelastung oft nicht wahrgenommen wird: Tickets für wieder lauffähige Fachverfahren werden eingereicht, neue Digitalisierungsprojekte in Anspruch genommen. Eine Person beschreibt die Phase der Doppelbelastung wie folgt,

„ab dem Zeitpunkt, wenn man etwas freigibt, muss man sich auch kümmern. Und das war wiederum schädlich. (….) Ich glaube, wir hätten klarer kommunizieren müssen, wir haben euch jetzt eure Anmeldung wieder zurückgegeben, euer Dokumentenmanagement, ihr könnt arbeiten, aber ihr dürft eigentlich jetzt keine Projekte starten, weil wir keine Zeit haben. Und mit jedem zusätzlichen Server, mit jedem zusätzlichen Dienst oder Fachverfahren steigen natürlich die Erwartungen. Dann gibt es wieder Störungstickets, dann gibt es wieder Anfragen, um die man sich auch kümmern muss. (K13)“

3.6 Reflexion und Transfer

Mit dem Übergang vom Notbetrieb zum Normalbetrieb, kommt auch die Phase der Reflexion und des Transfers. In den meisten Kommunen erfolgt diese Phase jedoch als fließender Übergang. Denn es fehlt oft an der Abschlusskommunikation – intern wie extern. Die Abschlusskommunikation ist jedoch ein wichtiger Bestandteil jeder Krisenkommunikation, denn damit wird symbolisiert, dass die Organisation die Krise überstanden hat.

Es zeigte sich in dieser Phase, dass die Anpassung bzw. Verbesserung von kommunikativen Maßnahmen nicht im Fokus der Kommunen standen. Stattdessen wurde sich vor allem auf technische Maßnahmen fokussiert wie z. B. die Einführung von Multi-Faktor-Authentifizierung, bessere Netzwerksegmentierung oder neue Backupkonzepte.

Kommunikativ wurde vor allem die Wissensvermittlung verstärkt: Viele Kommunen führten nach dem Vorfall Schulungskonzepte ein oder stellten sich in diesem Bereich neu auf. Einige berichteten zudem von einem Wissenstransfer mit anderen Kommunen. Eine Kommune gab an, einen extern gehosteten Mailservice eingerichtet zu haben, um diesen Kommunikationsweg zukünftig zu sichern.

Explizit berichtete keine Kommune, sich besser im Bereich der Krisenkommunikation aufgestellt zu haben. Dies schließt jedoch nicht aus, dass einzelne dies getan haben und der Interviewpartner dies etwa aufgrund fehlenden Zuständigkeitsbezugs nicht thematisierte. Möglicherweise blieben auch andere Maßnahmen bewusster im Gedächtnis, etwa die Einführung eines neuen Sicherheitskonzepts oder zusätzliches Budget für die Implementierung von technischen Sicherheitsmaßnahmen.

3.7 Handlungsempfehlungen

Aus den Beobachtungen aus der Praxis ergeben sich Handlungsempfehlungen an kommunale Verwaltungen zum kommunikativen Umgang mit einem IT-Sicherheitsvorfall.

1

Vorbereitung der Krisenkommunikation

Die Krisenkommunikation sollte vorab vorbereitet sein. Hierzu gehört u. a. die Klärung, wer in der Krise für die Kommunikation verantwortlich ist, die Vorbereitung bzw. Erstellung von Templates sowie die Erreichbarkeit von wichtigen internen und externen Personen zur Bewältigung der Krise.

Weiterführende Hilfe, siehe z. B.:

- Bundesministerium des Innern (2014), Leitfaden Krisenkommunikation, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/BMI08313-leitfaden-krisenkommunikation.pdf?__blob=publicationFile&v=10 (zuletzt abgerufen 09.10.2026).
- Dialog für Cybersicherheit (2024), Ergebnisbericht Cyberresilience-Framework. In IT-Krisen schneller agieren. (Kurz: RESI), https://www.dialog-cybersicherheit.de/storage/uploads/ws24-endprodukte/2024_Ergebnisbericht_RESI.pdf (zuletzt abgerufen 09.10.2026); hier vor allem Anlage B (Krisenkommunikation bei Cyberangriffen - Handreichung für Kommunen).
- Notfallkoffer von REDIKOM mit weiteren Vorlagen und Templates: https://www.redikom.org/notfallkoffer/ (zuletzt abgerufen 09.10.2026).

2

Kommunikationsverantwortliche Person als Teil des Krisenstabs

In vielen kommunalen Verwaltungen sind vorab definierte Krisenstäbe für einen IT-Sicherheitsvorfall immer noch nicht die Regel. Oftmals wird bei den Ad-hoc-Krisenstäben die Position der kommunikationsverantwortlichen Person vergessen. Es ist jedoch sinnvoll, dass diese Teil des Krisenstabs sind, damit in der Kommunikation nach innen und außen keine Fehler unterlaufen, z. B. bei der Darstellung der technisch getroffenen Maßnahmen, bei vorschneller Entwarnung bei möglichen Datenschutzverletzungen oder bei der Preisgabe von zu vielen Informationen.

Weiterführende Hilfe, siehe z. B.:

- Hofinger, Gesine; Heimann, Rudi (2022): Handbuch Stabsarbeit, Führungs- und Krisenstäbe in Einsatzorganisationen, Behörden und Unternehmen, 2. Auflage. (insbesondere Teil V).

3

Etablierung von Meldeketten bei Verdachtssituationen und zur Eskalation

Es zeigte sich, dass die Kommunen in aller Regel keine etablierten Meldeketten für Verdachtsmomente eingeführt hatten. Doch klar definierte Meldeketten sind erstens wichtig, um schnell eine verdächtige Situation einschätzen zu können. Zweitens sind diese bei der Eskalation wichtig, damit z. B. vorab geklärt ist, wer zuerst innerhalb des Hauses zu informieren ist, wer die zuständigen Behörden informiert und an welche ggf. dritte Stellen sich die kommunale Verwaltung bezüglich externer Unterstützung wenden kann.

Weiterführende Hilfe, siehe z. B.:

- IHK München (o. J.), Muster IT-Notfallplan, https://www.ihk-muenchen.de/ratgeber/digitalisierung/informationssicherheit/muster-it-notfallplan (zuletzt abgerufen 09.10.2026); hier vor allem Verifikation und Einschätzung der Meldung.
- Dialog für Cybersicherheit (2024), Anlagen zu den Handreichungen „Cyberresilience-Framework. In IT-Krisen schneller agieren. (Kurz: RESI)“: Merkblätter und Checklisten, https://www.dialog-cybersicherheit.de/storage/uploads/resi-ddos/2026_RESI_Checklisten_Listen.pdf (zuletzt abgerufen: 09.10.2026).

Etablierung von möglichen Wegen zur internen Alarmierung

4

Neben der Informierung der verantwortlichen Personen zur Bewältigung der Krise, ist es auch entscheidend sich vorab darüber Gedanken zu machen, auf welchen Wegen (und wie) die komplette Belegschaft über den Vorfall informiert wird. Insbesondere für den Fall, dass die normalen Kommunikationswege über E-Mail, Telefon oder Intranet nicht mehr verfügbar sind, ist zu prüfen, inwiefern alternative Kommunikationswege vorbereitet werden können.

Weiterführende Hilfe, siehe z. B.:

- Fraunhofer SIT (o. J.): Krisenkommunikation bei Cyberangriff, https://www.sit.fraunhofer.de/de/cyberkrisenkommunikation/ (zuletzt abgerufen 09.10.2026); hier vor allem Checkliste Infos und Darksite.

Abschlusskommunikation nicht vergessen

5

Viel zu oft wird die Krise kommunikativ nicht beendet. Das ist jedoch eine sinnvolle Maßnahme, um nach außen und nach innen zu signalisieren, dass die Krise überstanden ist und die getroffenen Maßnahmen erfolgreich waren. Sinnvollerweise wird im Zuge der Abschlusskommunikation auch erwähnt, inwiefern die Kommune aufgrund des Vorfalls Anpassungen vorgenommen hat (ohne dabei zu sehr in technische Details zu gehen).

Ein Beispiel für die Abschlusskommunikation ist in der Anlage B des Ergebnisberichtes von RESI (abrufbar unter https://www.dialog-cybersicherheit.de/storage/uploads/ws24-endprodukte/2024_Ergebnisbericht_RESI.pdf) zu finden.

Beachtung von Regeln der guten Krisenkommunikation

6

Im Generellen sollten die Regeln guter Krisenkommunikation beachtet werden, z. B.

- Schnelligkeit: Proaktive schnelle Reaktion, um nicht ständig reaktiv auf die Krise zu reagieren
- Wahrhaftigkeit: Ehrliche, sachliche und transparente Kommunikation (was nicht bedeutet, dass alles kommuniziert werden muss)
- Verständlichkeit: Klare Kommunikation ohne zu komplizierte Fachbegriffe
- Konsistenz: Einheitlich in der Botschaft über Kanäle und Personen hinweg.

Weiterführende Hilfe, siehe z. B.:

- Mayer, Aljoscha; Voss, Martin (2021): Risiko- und Krisenkommunikation: Ein Überblick, AKFS Report Nr. 4.

4 LITERATURVERZEICHNIS

Bentley, Joshua; Ma, Liang (2020): Testing perceptions of organizational apologies after a data breach crisis, Public Relations Review, 46(5),101975.

Bundesministerium des Innern (2014): Leitfaden Krisenkommunikation.

Bundesamt für Sicherheit in der Informationstechnik (2008): BSI-Standard 100-4 Notfallmanagement.

Coombs, Timothy; Holladay, Sherry J.; White Rick (2021): Corporate Crises: Sticky Crises and Corporations, in: Jin, Yan; Reber, Bryan H.; Nowak, Glen J. (Hrsg.): Advancing Crisis Communication Effectiveness: Integrating Public Relations Scholarship with Practice, S. 35-51.

Coombs, Timothy; Holladay, Sherry J.; White, Karen L. (2021): Situational Crisis Communication Theory (SCCT) and Application in Dealing with Complex, Challenging, and Recurring Crises, in: Jin, Yan; Reber, Bryan H.; Nowak, Glen J. (Hrsg.): Advancing Crisis Communication Effectiveness: Integrating Public Relations Scholarship with Practice, S. 165-180.

Hytönen, Eveliina; Ruoslahti, Harris (2025): Crisis Communication Guidelines to Support Cyber Resilience, in: Lipps. Christoph; Han, Bin (2025): The Proceedings of the 24th European Conference on Cyber Warfare and Security, ECCWS 2025, S. 222-229.

Knight, Richard; Nurse, Jason R.C. (2020): A framework for effective corporate communication after cyber security incidents, in: Computers & Security, 99, 102036.

Latsch, Johannes (2025): Bürgermeister und Krisenkommunikation: Medien- und Öffentlichkeitsarbeit vom Alltagsstress zur Katastrophe, 2. Auflage.

Otten, Henrique Ricardo; Schophaus, Malte (2023): Krisenkommunikation in Kommunen: Organisation und Expertise in der Krisenkommunikation von Kommunalverwaltungen, Verwaltung & Management, 29 (5), S. 206-218.

Reber, Bryan H.; Yarbrough, Richard; Nowak, Glen; Jin, Yan (2021): Complex and Challenging Crises: A Call for Solutions, in: Jin, Yan; Reber, Bryan H.; Nowak, Glen J. (Hrsg.): Advancing Crisis Communication Effectiveness: Integrating Public Relations Scholarship with Practice, S. 3-16.

Riecken, Martin (2014): Erfolgskritische Faktoren der angewandten Krisenkommunikation, in: Thießen: Handbuch Krisenmanagement, S. 319-332.

Sperl-Hofmann, Heike (2026): Hitze legt Schriesheimer Rathaus-Server stundenlang lahm, in: Mannheimer Morgen, https://www.mannheimer-morgen.de/neckar-bergstrasse_artikel,-neckar-bergstrasse-hitze-legt-schriesheimer-rathaus-server-stundenlang-lahm-_arid,2384602.html, zuletzt abgerufen 05.08.2026.

Syed, Romilla (2019): Enterprise reputation threats on social media: A case of data breach framing, in: The Journal of Strategic Information Systems, Volume 28 (3), S. 257-274.

Tettenborn, Felix; Peters, Anja (2014): Leitfaden zur Risiko- und Krisenkommunikation in der Trinkwasserversorgung zur Verbesserung der Sicherheit in Hinblick auf CBRN-Bedrohungsszenarien: Kommunikation als vertrauensbildende Maßnahme und Handlungsempfehlungen zur Vorbereitung einer effektiven Krisenkommunikation.

IMPRESSUM

Das Brandenburgische Institut für Gesellschaft und Sicherheit (BIGS) gGmbH ist ein unabhängiges, überparteiliches und nicht-gewinnorientiertes wissenschaftliches Institut, das zu gesellschaftswissenschaftlichen Fragen ziviler Sicherheit forscht. Das Institut publiziert seine Forschungsergebnisse und vermittelt diese in Veranstaltungen an eine interessierte Öffentlichkeit. Das BIGS entstand im Frühjahr 2010 in Potsdam und wird von der Universität Potsdam über ihre UP Transfer GmbH getragen, sowie von den Unternehmen IABG und W.I.S.. Alle Aussagen und Meinungsäußerungen in diesem Papier liegen in der alleinigen Verantwortung der Autor*innen.

Autorin:
Esther Kern

Titel:
Wenn die Verwaltung offline ist:
Krisenkommunikation bei IT-Sicherheitsvorfällen in kommunalen Verwaltungen

Gefördert durch:
Bundesministerium für Forschung, Technologie und Raumfahrt

Herausgeber:
Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH

Verantwortlicher im Sinne des Rundfunkstaatsvertrages:
Dr. Tim H. Stuchtey

SIFO.de

Das Projekt REDIKOM – Resilienz Digitaler Kommunen in Krisenzeiten hat es sich zum Ziel gesetzt, die digitale Handlungsfähigkeit kommunaler Verwaltungen zu stärken. Das Projekt wird vom Brandenburgischen Institut für Gesellschaft und Sicherheit koordiniert in Zusammenarbeit mit der Cybersicherheitsagentur Baden-Württemberg, dem Hasso-Plattner-Institut und der Landeshauptstadt Potsdam sowie mit weiteren assoziierten Partnern. Dabei wird im Rahmen von REDIKOM eine forensische, strukturelle und prozessuale Analyse durchgeführt, um das bestehende Defizit an quantitativen und qualitativen (Vorfalls-)Daten zu adressieren sowie praxiserprobte Handlungsempfehlungen zu erarbeiten und Playbooks daraus abzuleiten. Die Interviews, die die Grundlage für diese Studie darstellen, wurden zusammen mit dem Hasso-Plattner-Institut geführt.

REDIKOM wird vom Bundesministerium für Forschung, Technologie und Raumfahrt im Rahmen des zivilen Sicherheitsforschungsprogramms gefördert. Mehr Informationen unter www.sifo.de.

BIGS Essenz Nr. 25, Oktober 2026
ISSN 2191-6756

Förderkennzeichen: 13N17060

Copyright 2026 © Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH. Alle Rechte vorbehalten. Die Reproduktion, Speicherung oder Übertragung (online oder offline) des Inhalts der vorliegenden Publikaton ist nur im Rahmen des privaten Gebrauchs gestattet. Kontaktieren Sie uns bitte, bevor Sie die Inhalte darüber hinaus verwenden.

BIGS
BRANDENBURGISCHES INSTITUT für GESELLSCHAFT und SICHERHEIT

Brandenburgisches Institut für Gesellschaft und Sicherheit
Geschäftsführender Direktor: Dr. Tim H. Stuchtey

Dianastraße 46 . 14482 Potsdam
Tel.: +49-331-704406-0 . Fax: +49-331-704406-19
E-Mail: info@bigs-potsdam.org . www.bigs-potsdam.org



BIGS

BRANDENBURGISCHES INSTITUT
für GESELLSCHAFT und SICHERHEIT