LEITFADEN

Krisenkommunikation für Städte und Gemeinden

Wie Sie bei Cyberangriffen, IT-Ausfällen und kommunalen Notlagen handlungsfähig bleiben – auch wenn Standardkommunikation versagt [inkl. 5-Schritte-Checkliste]

teamwire

Vorwort

Kommunikation als Teil der kommunalen Handlungsfähigkeit

Städte und Gemeinden tragen eine besondere Verantwortung. Sie sichern nicht nur die Versorgung ihrer Bürgerinnen und Bürger – von Straßenbeleuchtung über Bauhof bis hin zu öffentlicher Sicherheit und Ordnung – sondern müssen auch in Ausnahmesituationen handlungsfähig bleiben. In Krisensituationen zeigt sich, wie belastbar diese Verantwortung tatsächlich abgesichert ist.

Wenn Informationen nicht zuverlässig fließen oder vorgesehene Kommunikationsmittel selbst betroffen sind, verlieren auch ausgefeilte Notfallpläne an Wirksamkeit.

Ob Cyberangriff, IT-Ausfall, Extremwetterphänomene oder großflächige Netzstörung: Solche Szenarien sind längst keine Ausnahme mehr. Sie treffen kommunale Verwaltungen oft unerwartet, unter hohem Zeitdruck und mit unmittelbaren Auswirkungen auf den laufenden Betrieb. In genau diesen Momenten entscheidet nicht allein die technische Infrastruktur darüber, wie handlungsfähig eine Organisation bleibt, sondern vor allem die Kommunikation.

Denn ein Krisenstab ist nur so handlungsfähig wie seine Kommunikation. Wenn Informationen nicht zuverlässig fließen oder vorgesehene Kommunikationsmittel selbst betroffen sind, verlieren auch ausgefeilte Notfallpläne an Wirksamkeit. Die zentrale Frage lautet:

Wie lassen sich Rathaus, Ordnungsamt, Bauhof, IT, Krisenstab und externe Partner koordinieren, wenn

E-Mail, Telefon oder Kollaborationstools nicht mehr verfügbar oder vertrauenswürdig sind?

Viele Städte und Gemeinden verlassen sich im Alltag auf Standardkommunikationslösungen oder Consumer-Messenger wie WhatsApp. Im Ernstfall jedoch zeigen diese Systeme ihre Schwächen: Sie sind häufig an die eigene IT gekoppelt, nicht priorisiert, nicht zentral steuerbar und nicht darauf ausgelegt, unter Krisenbedingungen zuverlässig zu funktionieren. Improvisierte Lösungen – etwa private Messenger wie WhatsApp oder Telefonketten – schaffen kurzfristig Reichweite, erhöhen jedoch die Risiken hinsichtlich Datenschutz, Nachvollziehbarkeit und Steuerbarkeit.

Improvisierte Lösungen – etwa private Messenger wie WhatsApp oder Telefonketten – schaffen kurzfristig Reichweite, erhöhen jedoch die Risiken hinsichtlich Datenschutz, Nachvollziehbarkeit und Steuerbarkeit.

Dieser Leitfaden beleuchtet, warum krisenfeste Kommunikation für Städte und Gemeinden ein zentraler Bestandteil der kommunalen Handlungsfähigkeit ist. Er zeigt typische Krisenszenarien aus dem kommunalen Umfeld auf, analysiert die Schwachstellen klassischer Kommunikationswege und macht deutlich, welche Anforderungen eine Kommunikationslösung erfüllen muss, um in Behörden und kommunalen Betrieben tatsächlich belastbar zu sein.

Ziel ist es, Verantwortlichen in Städten, Gemeinden und Landkreisen eine klare Entscheidungsgrundlage zu geben: für eine Krisenkommunikation, die auch dann funktioniert, wenn Standardwege versagen – und die Organisation handlungsfähig hält, wenn es wirklich darauf ankommt. Zum Schutz der Bürger.

01.

Warum Krisenkommunikation systemrelevant ist

Städte und Gemeinden gehören zur kritischen Infrastruktur. Ihre Aufgabe endet nicht beim stabilen Betrieb von Ämtern und Einrichtungen, sondern umfasst auch die Fähigkeit, in Ausnahmesituationen handlungsfähig zu bleiben. Genau hier rückt die Kommunikation in den Mittelpunkt. Und zwar nicht als unterstützende Funktion, sondern als operatives Steuerungsinstrument.

Ende 2024 legte ein Hackerangriff z.B. die gesamte IT der Stadt Aschaffenburg lahm. Weder interne noch externe Kommunikation war möglich. Das Rathaus war geschlossen, die Mitarbeitenden mussten zu Hause bleiben. Die Anliegen der Bürger konnten tagelang nicht bearbeitet werden. Sie waren quasi abgeschnitten von der Außenwelt, die Arbeit blieb liegen. Kurzum: Die Business Continuity war nicht gesichert.

In Krisensituationen verdichtet sich Zeit. Entscheidungen müssen schneller getroffen, Maßnahmen unmittelbar umgesetzt und Informationen zuverlässig verteilt werden. Gleichzeitig steigt die Komplexität: IT, Netzbetrieb, Leitstelle, Bereitschaftsdienste, Geschäftsführung und externe Partner müssen koordiniert handeln – oft parallel, oft unter hohem Druck. Ohne funktionierende Kommunikation verliert selbst eine technisch robuste Infrastruktur ihre Wirksamkeit.

Ein zentrales Problem vieler kommunaler Verwaltungen besteht darin, dass ihre Kommunikationsfähigkeit eng an den Normalbetrieb gekoppelt ist. E-Mail-Systeme, Kollaborationsplattformen oder Telefonanlagen sind in der Regel Teil derselben IT-Landschaft, die im Krisenfall selbst betroffen sein kann. Fällt diese Infrastruktur aus – etwa durch einen Cyberangriff oder einen großflächigen IT-Fehler –, bricht nicht nur der Informationsfluss ab, sondern auch die Führungs- und Steuerungsfähigkeit der Organisation.

Das Problem: Standardkommunikation ist nicht krisenfest. Keine priorisierte Alarmierung, keine Quittierungen, keine gezielte Steuerung großer Gruppen. Die Konsequenz sind Notlösungen wie Telefonketten oder private Messenger – kurzfristig wirksam, langfristig riskant. Datenschutz, Dokumentation und Kontrolle bleiben dabei oft auf der Strecke.

Beispiel aus der Praxis: Die Stadt Kleve setzt Teamwire erfolgreich im Alltag und bei besonderen Lagen wie Großveranstaltungen, Bombenentschärfungen und kommunalen Notfällen ein. Die sichere, datenschutzkonforme Kommunikation ermöglicht schnelle Reaktionen – auch wenn herkömmliche Kanäle ausgelastet oder nicht verfügbar sind.

„Teamwire ermöglicht uns eine schnvelle, sichere und flexible Kommunikation – sowohl im Alltag als auch bei außergewöhnlichen Ereignissen wie Bombenentschärfungen oder Großveranstaltungen."

Ben Viethen,
Digitalisierung Stadt Kleve

→ Hier die gesamte Success-Story lesen

Für Städte und Gemeinden ist das besonders kritisch. Als Teil der öffentlichen Daseinsvorsorge unterliegen sie erhöhten regulatorischen Anforderungen wie NIS-2 und IT-SiG 2.0 und stehen im Ernstfall nicht nur operativ, sondern auch rechtlich und reputational unter Beobachtung. Eine ungeplante, unkontrollierte Kommunikation kann hier zusätzliche Schäden verursachen – unabhängig vom eigentlichen Auslöser der Krise.

Anfang 2026 war die Stadtverwaltung Heinsberg in Nordrhein-Westfalen betroffen. Zahlreiche weitere Beispiele für Cyberattacken auf Stadtverwaltungen listet das Portal KonBriefing.

Krisenkommunikation muss daher unabhängig vom Normalbetrieb gedacht werden. Sie benötigt einen eigenen, entkoppelten Kommunikationskanal, der auch dann weiterhin verfügbar bleibt, wenn zentrale IT-Systeme ausfallen oder kompromittiert sind. Dieser Kanal muss es ermöglichen, Informationen schnell, sicher und zielgerichtet zu verteilen, Rückmeldungen einzuholen und Maßnahmen zu koordinieren – über alle Abteilungen und Betriebe hinweg.

Richtig aufgesetzt, wird Kommunikation damit zu einem stabilisierenden Faktor in der Krise. Sie schafft Orientierung, reduziert Unsicherheit und ermöglicht es Verantwortlichen, auch unter außergewöhnlichen Bedingungen handlungsfähig zu bleiben. Für Städte und Gemeinden ist das kein „Nice-to-have", sondern ein wesentlicher Bestandteil moderner Daseinsvorsorge und organisatorischer Resilienz.

02.

Typische Krisenszenarien in Städten und Gemeinden und warum Standard-kommunikation hier versagt

Krisen in kommunalen Verwaltungen entstehen meist plötzlich, entwickeln sich dynamisch und betreffen mehrere Ebenen gleichzeitig: Rathaus, Ordnungsamt, Bauhof, Bereitschaftsdienste, IT–Abteilung und externe Partner. In solchen Situationen zeigt sich, ob Kommunikationsstrukturen wirklich belastbar sind oder zum Risiko werden.

Was viele Kommunen erleben: Kommunikationskanäle versagen genau dann, wenn sie am dringendsten benötigt werden. Das ist kein theoretisches Risiko, es ist eine reale Herausforderung im Verwaltungsalltag. Die Folgen sind Verzögerungen, Unsicherheiten und operative Risiken, die vermeidbar wären, wenn die Kommunikation unabhängig, priorisiert und steuerbar wäre.

Cyberangriffe und IT-Ausfälle

Cyberangriffe gehören zu den größten Herausforderungen für Städte und Gemeinden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt in seinem Lagebericht zur IT-Sicherheit in Deutschland ausdrücklich davor, dass die IT-Sicherheitslage weiterhin auf angespanntem Niveau bleibt. Kommunale Verwaltungen geraten zunehmend ins Visier von Angreifern. Schadsoftware, Ransomware oder gezielte Angriffe auf zentrale IT-Systeme können dazu führen, dass E-Mail-Server, Kollaborationsplattformen oder Telefonie nicht mehr verfügbar sind oder vorsorglich abgeschaltet werden müssen.

Genau in solchen Momenten ist klare, koordinierte Kommunikation besonders wichtig: Krisenstab, Ordnungsamt, Bauhof, externe Dienstleister und Mitarbeitende müssen schnell auf denselben Informationsstand gebracht werden. Klassische Kommunikationsmittel sind hierfür jedoch häufig ungeeignet, weil sie Teil derselben IT-Infrastruktur sind, die gerade ausfällt.

Das Ergebnis sind improvisierte Notlösungen: private Messenger, E-Mails über externe Accounts oder Telefonketten. Diese schaffen zwar kurzfristig Reichweite, führen aber zu unkontrollierten, schwer steuerbaren Informationsflüssen und erhöhen die Risiken in Bezug auf Datenschutz, Compliance und Nachvollziehbarkeit. Für kommunale Verwaltungen ist das besonders kritisch, weil regulatorische Vorgaben wie NIS-2, IT-SiG 2.0 und DSGVO die Aufrechterhaltung sicherer Kommunikationswege sowie die Revisionssicherheit vorschreiben.

„Die mobile Kommunikation via WhatsApp entsprach leider nicht mehr den gesetzlichen Anforderungen. Eine DSGVO-konforme, sichere und für die Nutzer attraktive Lösung musste her."

Richard Lippmann,
IT-Leiter der Stadt Zirndorf

→ Hier die gesamte Success-Story lesen

Unwetter, Extremwetter und Katastrophenschutz

Extremwetterereignisse wie Stürme, Hochwasser oder anhaltende Hitzeperioden stellen kommunale Verwaltungen vor besondere Herausforderungen. Sie betreffen häufig mehrere Versorgungsbereiche gleichzeitig, erschweren den Zugang zu Einsätzen und binden personelle Ressourcen über längere Zeiträume. Bauhof, Feuerwehr, Ordnungsamt und Krisenstab müssen koordiniert handeln.

In solchen Lagen ist es entscheidend, mobile Einsatzteams zuverlässig zu erreichen und zu koordinieren – unabhängig davon, wo sie sich befinden. Gleichzeitig müssen Lageinformationen laufend aktualisiert und an unterschiedliche Personengruppen verteilt werden: operative Teams, Krisenstab und gegebenenfalls externe Stellen wie Polizei, THW oder Katastrophenschutzbehörden.

Standardkommunikation ist hierfür oft zu träge oder zu fragmentiert. Informationen werden mehrfach weitergegeben, gehen verloren oder erreichen falsche Empfänger. Eine zentrale, mobile Kommunikationsplattform schafft hier Abhilfe, indem sie Lageinformationen bündelt, Einsatzteams zielgerichtet informiert und Rückmeldungen strukturiert erfasst.

Großveranstaltungen und besondere Lagen

Ob Stadtfest, Wahl, Bombenentschärfung oder großflächige Baustelle, in solchen Situationen müssen viele Akteure gleichzeitig koordiniert werden. Ordnungsamt, Feuerwehr, technische Dienste und externe Sicherheitsdienstleister benötigen schnelle Abstimmungswege und ein gemeinsames Lagebild. Die Erfahrung zeigt: Wer hier auf einen improvisierten Kommunikationsmix setzt, verliert wertvolle Zeit und riskiert Missverständnisse.

Augmented Reality zur Lageerkennung, Live-Standorte und Broadcast-Funktionen ermöglichen in solchen Situationen ein klares, aktuelles Lagebild – auf Knopfdruck, für alle Beteiligten.

Weitere Herausforderungen im kommunalen Betrieb

Ein weiterer zentraler Punkt: Die Kommunikations-herausforderungen sind im kommunalen Betrieb nicht isoliert, sondern über mehrere Ebenen verteilt. Mitarbeitende arbeiten an unterschiedlichen Orten – im Bürgerbüro, im Bauhof, im Außendienst oder im Homeoffice. Zudem müssen Fachbereiche, kommunale Betriebe und externe Dienstleister zusammenarbeiten. Gleichzeitig gelten strenge Vorgaben für Datenschutz, Revisionssicherheit und Compliance.

Standardlösungen erfüllen diese Anforderungen oft nicht: Sie sind entweder nicht entkoppelt vom Normalbetrieb, bieten keine priorisierte Alarmierung oder lassen sich nicht revisionssicher dokumentieren. Hinzu kommt das Risiko durch US-basierte Tools: Kommunikationsdienste wie Microsoft Teams, Slack oder WhatsApp unterliegen dem US CLOUD Act und sind weder DSGVO- noch NIS-2-konform – für Kommunen ein erhebliches Compliance-Risiko.

Machen Sie jetzt den NIS-2-Check:

Erfüllt Ihre Krisenkommunikation die neuen Anforderungen? 8 Fragen, 2 Minuten – finden Sie heraus, wie Ihre Organisation aufgestellt ist und wo Handlungsbedarf besteht.

→ Jetzt Selbsttest starten

Gemeinsamkeiten aller Szenarien

Unabhängig vom Auslöser – ob Cyberangriff, Unwetter, Großveranstaltung oder IT-Ausfall – gilt: Städte und Gemeinden benötigen Kommunikationswege, die zuverlässig, steuerbar und unabhängig vom Alltagsbetrieb sind. Nur so bleibt die Organisation handlungsfähig, wenn es wirklich darauf ankommt.

03.

Der Krisenstab: Kommunikation unter Druck

Wenn in einer Stadt eine Krise eintritt, ist der Krisenstab das zentrale Steuerungsorgan. Hier laufen Informationen zusammen, hier werden Prioritäten gesetzt und Entscheidungen getroffen, die unmittelbare Auswirkungen auf den Versorgungsbetrieb, die Mitarbeitenden und die Öffentlichkeit haben. Die Leistungsfähigkeit dieses Gremiums hängt jedoch weniger von formalen Zuständigkeiten ab als von einem häufig unterschätzten Faktor: der Kommunikation.

In der Praxis zeigt sich, dass viele Krisenstäbe zwar organisatorisch definiert sind, ihre Kommunikationsfähigkeit jedoch eng an den Normalbetrieb geknüpft bleibt. E-Mail, Telefon oder Kollaborationstools werden auch im Ernstfall weiter genutzt – selbst dann, wenn diese Systeme instabil, überlastet oder Teil der Störung sind. Das führt dazu, dass Informationen verzögert eintreffen, unvollständig bleiben oder dass im Krisenstab unterschiedliche Wissensstände entstehen.

Wenn Kommunikation zum Engpass wird

Krisenstäbe arbeiten unter hohem Zeitdruck. Lage-einschätzungen müssen laufend aktualisiert, Maßnahmen koordiniert und Entscheidungen dokumentiert werden. Gleichzeitig müssen Informationen aus unterschiedlichen Bereichen zusammengeführt werden: Ordnungsamt, Bauhof, IT, Bereitschaftsdienste, externe Dienstleister oder Behörden.

Ohne einen zentralen, priorisierten Kommunikationskanal entstehen dabei schnell typische Probleme:

- Parallele Kanäle führen zu Informationssilos, sodass Informationen nicht alle relevanten Personen gleichzeitig erreichen.
- Fehlende Quittierungen sorgen für einen unklaren Wissensstand, da Rückmeldungen aus dem operativen Bereich unstrukturiert sind oder verloren gehen.
- Fehlende Priorisierung: Entscheidungen basieren auf veralteten oder unvollständigen Lagebildern.
- Fehlende zentrale Dokumentation führt zu fehlender Nachvollziehbarkeit: Zuständigkeiten und Eskalationswege werden unklar.

Besonders kritisch wird dies, wenn mehrere Kommunikationskanäle parallel genutzt werden. Telefonate, einzelne Messenger-Gruppen und E-Mails führen zu einem fragmentierten Informationsfluss, der sich kaum noch überblicken oder nachvollziehen lässt. Für einen Krisenstab bedeutet das: Zeitverlust, Unsicherheit und erhöhte Fehleranfälligkeit.

Anforderungen an die Krisenkommunikation im Stab

Damit ein Krisenstab seine Aufgabe erfüllen kann, braucht er eine Kommunikationsbasis, die speziell für Ausnahmesituationen ausgelegt ist. Diese muss deutlich mehr leisten als die klassische Alltagskommunikation.

Zentral ist zunächst die Unabhängigkeit vom Normalbetrieb. Die Kommunikation des Krisenstabs darf nicht von denselben IT-Systemen abhängen, die im Krisenfall selbst betroffen sein können. Nur so bleibt die Führungsfähigkeit erhalten, auch wenn zentrale Anwendungen oder Infrastrukturen ausfallen.

Ebenso wichtig ist die gezielte Steuerung von Informationen. Nicht jede Information ist für alle Beteiligten gleichermaßen relevant. Ein Krisenstab benötigt die Möglichkeit, Inhalte priorisiert zu verteilen, bestimmte Personengruppen gezielt anzusprechen und Rückmeldungen strukturiert einzuholen. Alarmierungen, Quittierungen und Statusmeldungen sind hierfür essenziell.

Darüber hinaus spielt die Nachvollziehbarkeit von Entscheidungen eine zentrale Rolle. Gerade für kommunale

Behörden ist es entscheidend, dass Informationsflüsse dokumentiert und Entscheidungen später rekonstruierbar sind:

- Wer wurde wann informiert?
- Welche Maßnahmen wurden beschlossen?
- Welche Rückmeldungen lagen vor?

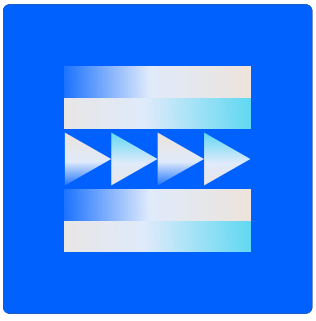
Eine unstrukturierte Kommunikation erschwert diese Transparenz erheblich.

Kommunikation zwischen Krisenstab und operativen Teams

Der Krisenstab agiert nicht isoliert. Seine Wirksamkeit hängt maßgeblich davon ab, wie gut die Kommunikation mit den operativen Einheiten funktioniert. Einsatzteams im Bauhof, Bereitschaftsdienste im Ordnungsamt oder externe Partner benötigen klare Anweisungen, aktuelle Lageinformationen und die Möglichkeit, relevante Rückmeldungen schnell zurückzuspielen.

Ohne einen gemeinsamen Kommunikationskanal kommt es hier häufig zu Medienbrüchen. Informationen werden telefonisch weitergegeben, später per E-Mail zusammengefasst oder in separaten Systemen dokumentiert. Diese Verzögerungen wirken sich direkt auf die Reaktionsgeschwindigkeit aus.

Eine zentrale mobile Kommunikationslösung schafft hier eine durchgängige Verbindung zwischen dem Krisenstab und dem operativen Betrieb. Sie ermöglicht es, Lagebilder zu teilen, Maßnahmen zu koordinieren und Rückmeldungen aus dem Feld unmittelbar in die Entscheidungsfindung einzubeziehen – unabhängig vom Aufenthaltsort der Beteiligten.



Krisenstabsarbeit braucht klare Kommunikationsstrukturen

Ein leistungsfähiger Krisenstab benötigt mehr als nur einen Besprechungsraum und einen Notfallplan. Er braucht Kommunikationsstrukturen, die auch unter extremen Bedingungen funktionieren. Dazu gehört ein klar definierter Zweitkanal, der regelmäßig genutzt, geübt und in die organisatorischen Abläufe integriert ist.

Nur wenn Kommunikation auch im Alltag etabliert ist, kann sie im Ernstfall ihre stabilisierende Wirkung entfalten. Für Städte und Gemeinden bedeutet das: Krisenkommunikation ist keine Aufnahmefunktion, sondern ein fester Bestandteil moderner Führungs- und Resilienzkonzepte.

04.

Anforderungen an eine krisenfeste Kommunikations-lösung für Städte und Gemeinden

In Kapitel 02 und 03 haben wir die Relevanz von Kommunikation im Krisenfall sowie die strukturellen Mängel klassischer Lösungen analysiert. Jetzt stellt sich die Frage:

Welche Eigenschaften muss eine Kommunikationslösung haben, damit sie in den beschriebenen Szenarien tatsächlich funktioniert – und den Anforderungen von Städten und Gemeinden gerecht wird?

Kommunale Verwaltungen stehen unter besonderer Beobachtung: Neben der operativen Herausforderung zählt auch die regulatorische Compliance, etwa im Rahmen von NIS-2, IT-SiG 2.0 und DSGVO. Kommunikation muss deshalb nicht nur schnell und zuverlässig, sondern auch sicher, kontrollierbar und auditierbar sein.

1. Ausfallsicherheit und Unabhängigkeit von der Alltags-IT

Eine krisenfeste Kommunikationslösung darf nicht dieselben Systeme nutzen, die im Krisenfall ausfallen können – wie E-Mail-Server, Kollaborationsplattformen oder unternehmensinterne Telefonanlagen. Sie muss unabhängig funktionieren, auch wenn zentrale IT-Komponenten nicht verfügbar sind oder abgeschaltet werden müssen.

Kernanforderungen:

- Unabhängiger Kommunikationskanal, der nicht an E-Mail, Telefon oder Standard-IT gebunden ist
- Mobile Erstkommunikation mit Push-Funktionalität auch bei eingeschränktem Netz
- Kurzfristige Alarmierung aller relevanten Beteiligten ohne Medienbrüche

Eine krisenfeste Kommunikationslösung darf nicht dieselben Systeme nutzen, die im Krisenfall ausfallen können.

2. Echtzeitkommunikation und zielgerichtete Informationsverteilung

In Krisen zählt jede Minute. Informationen müssen sofort, transparent und zielgerichtet verteilt werden – an den Krisenstab, das Ordnungsamt oder den Bauhof. Daher sind Funktionen erforderlich, die über einfache Chats hinausgehen: Broadcast-Nachrichten, priorisierte Alarme, Quittierungen und klar strukturierte Gruppenkommunikation.

Wichtige Merkmale:

- Gruppenchats, Broadcast-Listen und Verteilergruppen für schnelle, klare Reichweite
- Priorisierte Alarme, die auch Stummschaltungen durchbrechen
- Quittierungspflicht für empfangene Informationen
- Klare Rollen- und Zielgruppensegmentierung für Informationsverteilung

„Im Winterdienst müssen wir sicherstellen, dass Alarme auch nachts zuverlässig ankommen und Rückmeldungen direkt dokumentiert werden können. Mit Teamwire haben wir eine Lösung gefunden, die unsere Einsatzplanung flexibel und effizient unterstützt."

Andrea Rennebarth,
Geschäftsführerin Zweckverband Bauhof TKS

→ Hier die geasmte Success-Story lesen

3. Standort- und Einsatzdaten in Echtzeit

Bei operativen Störungen müssen Einsatzteams nicht nur informiert, sondern auch koordiniert werden. Live-Standorte, Augmented Reality (AR) und Kartenfunktionen erhöhen die situative Transparenz und verkürzen Entscheidungsschleifen – entscheidend bei Großveranstaltungen, Unwetterlagen oder Bombenentschärfungen.

Das umfasst:

- Echtzeit-Standortdaten von Bauhofteams, Ordnungsdienst und Einsatzfahrzeugen
- AR-Unterstützung zur Visualisierung von Einsatzorten, Zufahrten und Sammelpunkten
- Übersicht über Ressourcen und Maßnahmen auf einer interaktiven Karte

4. Sicherheit, Compliance und Datensouveränität

Kommunale Verwaltungen tragen Verantwortung für sensible Bürger- und Verwaltungsdaten. Diese dürfen nicht über unkontrollierte oder datenschutzrechtlich problematische Kommunikationskanäle laufen. Compliance-Anforderungen wie NIS-2, DSGVO und IT-SiG 2.0 verlangen Kontroll- und Nachweisbarkeit.

Anforderungen an die Lösung:

- 100 % Erfüllung von NIS-2 und IT-SiG 2.0
- 100 % DSGVO-Konformität, Hosting in Deutschland oder der EU
- Zertifizierungen wie ISO 27001 oder das BSI C5-Testat und volle Unterstützung regulatorischer Vorgaben
- Verschlüsselung nach modernsten Sicherheitsstandards
- Zero-Trust-Sicherheitsmodell
- Revisionssichere Speicherung und Auditfähigkeit
- 100 % Datensouveränität ohne US-Zugriff oder Abhängigkeit von Diensten in Drittstaaten wie den USA (US CLOUD Act)

5. Bedienbarkeit und breite Nutzbarkeit

Der Vorteil einer professionellen Lösung liegt nicht nur in Sicherheitsstandards, sondern auch in der intuitiven Bedienung selbst unter Stressbedingungen. Insbesondere mobile Teams im Außendienst oder Bauhof müssen schnell und ohne Schulungsbarrieren reagieren können.

Anforderungen an die Lösung:

- Intuitive Benutzeroberfläche auf Smartphone, Tablet und Desktop
- Multiplattform-Unterstützung (iOS, Android, Windows, Linux, macOS, Web)
- Synchronisierte Echtzeitkommunikation über alle Geräte hinweg
- Apple CarPlay-Unterstützung für mobile Teams im Fahrzeug

Lesetipp

Digitale Souveränität: Warum sie für Behörden und KRITIS in Europa unverzichtbar ist

Zum Artikel

„Der Clou ist, dass die Dokumentation via Teamwire auf dem Mobilgerät erfolgen kann und sich dann problemlos in der Desktop-App weiterbearbeiten und versenden lässt."

Richard Lippmann,
IT-Leiter der Stadt Zirndorf

→ Hier die gesamte Success-Story lesen

6. Zentrale Administration und Integrationsfähigkeit

Damit eine Lösung in den bestehenden Betriebs- und Sicherheitsprozess eingebettet werden kann, muss sie sowohl administrativ steuerbar als auch technisch integrierbar sein. Dazu gehören zentrale Nutzer- und Rechteverwaltung sowie Schnittstellen zu bestehenden IT-Systemen.

Anforderungen an die Lösung:

- Zentrales Administrations-Dashboard
- Integration in MDM/EMM/UEM-Systeme über AppConfig
- LDAP- und Active-Directory-Anbindung für automatische Synchronisation
- API-Schnittstellen für Systemautomatisierung
- Föderationsfähigkeit für Zusammenarbeit mit externen Partnern wie Nachbargemeinden, Landkreisen oder anderen Behörden

Zwischenfazit: Was eine krisenfeste Lösung leisten muss

Die genannten sechs Anforderungen bilden das Fundament für Kommunikation, die auch unter Extrembedingungen funktioniert. Sie sind keine theoretischen Idealvorstellungen, sondern praktische Notwendigkeiten im kommunalen Betrieb.

Die zentrale Frage für Städte und Gemeinden lautet:

Erfüllt unsere aktuelle Lösung diese Anforderungen vollständig? Oder verlassen wir uns auf Kompromisse, die im Ernstfall zum Risiko werden?

Warum eine spezialisierte Lösung wie Teamwire diese Anforderungen erfüllt

Teamwire wurde nicht als Alltagschat entwickelt, sondern als Kommunikationsplattform, die auch bei Ausfällen, Störungen oder Cybervorfällen Handlungsfähigkeit garantiert – genau dort, wo andere Systeme versagen.

Nahtlose Kommunikation zwischen Rathaus, Außendienst und Krisenstab: Alle Akteure in einer sicheren Plattform vereint

Teamwire verbindet Rathaus, Bauhof, Ordnungsamt, Krisenstab und Management auf einer gemeinsamen, sicheren Kommunikationsplattform. Informationen, Warnungen und Einsatzdaten fließen in Echtzeit – ohne Umwege, Verzögerungen oder Medienbrüche.

- Einfach wie WhatsApp – aber sicher
- 1:1- & Gruppenkommunikation
- Sprach- & Videokonferenzen
- Farbige Statusmeldungen mit Lesebestätigungen
- Live-Standorte und Augmented Reality

Zum Weiterlesen

Weitere Details zu allen Funktionen finden Sie hier.

Mehr erfahren

Optimale Erweiterung zu E-Mail: Digitale Inhalte in Sekunden teilen und bearbeiten

Teamwire ergänzt bestehende Kommunikationskanäle wie E-Mail oder Funk durch eine moderne, mobile Plattform für Echtzeitkommunikation. So können Rathaus, Bauhof und Krisenstäbe Informationen sofort teilen, visualisieren und dokumentieren – sicher, nachvollziehbar und DSGVO-konform.

- Digitale Inhalte teilen (Fotos, Video, Dokumente etc.)
- Bilder schnell und unkompliziert bearbeiten
- Schnelle Umfragen erstellen

Zum Weiterlesen

Weitere Details zu allen Funktionen finden Sie hier.

Mehr erfahren

Effektive Krisenkommunikation mit integrierten Notfallfunktionen: Reagieren, bevor die Lage eskaliert

Ob Stromausfall, Unwetter, Bombenentschärfung oder Cyberangriff – in der kommunalen Verwaltung müssen alle Beteiligten in Sekunden reagieren können. Mit Teamwire bleiben Krisenstäbe, Ordnungsamt und Bauhof auch bei IT-Ausfällen oder Netzproblemen handlungsfähig. Die Plattform bietet integrierte Notfallfunktionen und unterstützt den Schutz von Mitarbeitenden, die täglich draußen unterwegs sind.

- Notfallalarmierung & Panik-Button für Notfälle
- Live-Standorte & Augmented Reality
- Push-to-Talk & Broadcast
- Einfache Kartenbearbeitung

Datensouveränität und Compliance garantiert: Kommunikation nach höchsten EU-Sicherheitsstandards

In der kommunalen Verwaltung gilt Datenschutz als oberstes Gebot. Teamwire schützt die gesamte interne und externe Kommunikation nach europäischen Sicherheitsrichtlinien – vollständig verschlüsselt, DSGVO- und NIS-2-konform, speziell entwickelt für die Anforderungen öffentlicher Einrichtungen.

- Mehrschichtige Verschlüsselung
- Volle Datensouveränität
- Privacy by Design & Default
- Zero-Trust-Sicherheitsmodell
- Individuelle Aufbewahrungsrichtlinien
- Zertifizierte Sicherheit (ISO 27001, BSI C5-Testat)

Ausfallsicherheit auch bei IT-Störungen: Bleiben Sie handlungsfähig, wenn andere Systeme versagen

In der Krisenmomenten zählt Verfügbarkeit mehr als alles andere. Teamwire bleibt auch dann betriebsbereit, wenn zentrale IT-Systeme oder Netzwerke ausfallen – sei es durch Wartung, technische Störung oder Cyberangriff. So bleibt Ihre Behörde jederzeit handlungsfähig und kommunikationsfähig – intern wie extern. Zum Schutz Ihrer Bürger und Ihrer Mitarbeiter.

- Höchste Verfügbarkeit
- Souveränes Hosting On-Premise, Private oder Public Cloud
- Skalierbare Architektur
- Permanente Backups
- Vollständige Zugriffskontrolle

Zum Weiterlesen

Weitere Details zu allen Funktionen finden Sie hier.

Mehr erfahren

Professionelle Nutzerverwaltung: Alle Nutzer und Geräte einfach zentral steuern

Verabschieden Sie sich von unübersichtlichen Tools und dezentralen Strukturen: Mit Teamwire verwalten Sie alle Nutzer, Geräte und Berechtigungen zentral – effizient, transparent und revisionssicher. So behalten Sie die volle Kontrolle über Ihre Kommunikationsumgebung, ganz gleich, ob im Rathaus, im Bauhof oder in anderen kommunalen Organisationen.

- Zentrales Administrationsportal & Revisionssicherheit
- Umfassendes Mobile Application Management
- Verfügbar für alle Geräte und gängigen Betriebssysteme

Zusammen ergibt das eine Kommunikationslösung, die nicht nur die operativen Anforderungen im Krisenfall erfüllt, sondern zugleich die Compliance- und Sicherheitsanforderungen abdeckt, die Städte und Gemeinden heute erwarten.

Zum Weiterlesen

Weitere Details zu allen Funktionen finden Sie hier.

Mehr erfahren

CHECKLISTE

5 praktische Schritte für eine krisensichere Kommunikation

In Krisensituationen zählt jede Sekunde. Verzögerungen oder Kommunikationsausfälle können erhebliche Schäden verursachen. Diese umfassende Checkliste hilft Ihnen, eine robuste, ausfallsichere interne Krisenkommunikation zu etablieren.

teamwire

Schritt 1

Risikoanalyse: Welche Krisen können eintreten?

Beginnen Sie damit, mögliche Krisen- und Notfallsituationen, die Ihr Unternehmen betreffen könnten, zu identifizieren und zu analysieren. Ob Hackerangriffe, Fehler in der Produktion, Lieferkettenprobleme, Mitarbeiterunfälle, Streiks, Naturkatastrophen oder Terroranschläge – eine gründliche Analyse dieser Szenarien hilft Ihnen, die spezifischen Anforderungen für Ihre Krisenkommunikation zu verstehen.

Ziel: Mögliche Krisenszenarien identifizieren und die Auswirkungen auf die interne Kommunikation bewerten.

☐ Mögliche Krisenszenarien definieren

- Cyberangriffe (z. B. Ransomware, DDoS, Datenlecks)
- IT-Ausfälle (z. B. Cloud-Dienste offline, Netzwerkstörungen)
- Naturkatastrophen (z. B. Überschwemmungen, Brände, Stromausfälle)
- Notfälle mit Personengefahr (z. B. Terrorlagen, Amokläufe, Bombendrohungen)
- Interne Störungen (z. B. technische Defekte, Sabotage, menschliche Fehler)

☐ Betroffene Kommunikationskanäle analysieren

- Welche internen Tools und Dienste könnten ausfallen? (z. B. E-Mail, Microsoft Teams, Telefon)
- Gibt es Alternativen oder Backup-Kanäle?
- Wie lange könnte ein Ausfall dauern und was bedeutet das für die Organisation?

☐ Sensible Abhängigkeiten identifizieren

- Gibt es zentrale Kommunikationssysteme, die bei einem Ausfall alles blockieren?
- Welche internen und externen Stellen müssen im Notfall dringend informiert werden?

Schritt 2

Krisen-kommunikations-strategie festlegen

Erstellen Sie auf Basis der definierten Szenarien detaillierte Notfallpläne. Diese sollten klare Richtlinien, Handlungsanweisungen und Verantwortlichkeiten beinhalten, damit Sie in einer Krisensituation effektiv kommunizieren und handeln können. Stellen Sie sicher, dass der Plan den Informationsaustausch mit allen Mitarbeitenden – unabhängig von ihrem Standort oder ihrer Arbeitssituation – berücksichtigt.

Ziel: Verantwortlichkeiten und Kommunikationswege für verschiedene Krisenszenarien im Voraus definieren.

☐ Krisenteam benennen

- Wer trägt die Verantwortung für die Kommunikation? (z. B. IT-Sicherheitsverantwortliche, Krisenstab)
- Wer ist Back-up, falls der Hauptverantwortliche ausfällt?

☐ Kommunikationsketten und Eskalationsstufen festlegen

- Wer informiert wen und in welcher Reihenfolge?
- Welche Meldungen sind für alle, welche nur für bestimmte Gruppen relevant?

☐ Sichere Kommunikationswege definieren

- Welche Tools dürfen in der Krise genutzt werden? (z. B. Teamwire statt WhatsApp)
- Welche Kanäle sind ausfallsicher und erreichbar, auch bei Netzproblemen?

☐ Rollen und Zuständigkeiten klar regeln

- Wer koordiniert, wer informiert, wer dokumentiert?
- Welche Mitarbeitenden müssen sofort kontaktiert werden?

☐ Vorgaben für Datenschutz und Sicherheit beachten

- Ist die gewählte Notfallkommunikation DSGVO-konform?
- Wie werden sensible Informationen sicher übermittelt?

Schritt 3

Krisensichere Kommunikations-technologie implementieren

Wählen Sie eine geeignete und gesicherte Lösung für die Krisenkommunikation, die den Anforderungen Ihres Unternehmens entspricht. Dabei sollten vor allem die individuellen Pflichten eines Betriebskontinuitäts-managements berücksichtigt werden. Vermeiden Sie Standardkommunikationstools, die für alltägliche Unternehmenskommunikation angeschafft wurden und dort im Einsatz sind, da diese oft nicht die nötigen Funktionen für Krisenkommunikation bieten.

Schritt 3

Ziel: Eine technische Infrastruktur aufbauen, die auch im Krisenfall zuverlässig funktioniert.

☐ Unabhängige, ausfallsichere Kommunikationsplattform bereitstellen

- Keine Abhängigkeit von Cloud-Diensten mit potenziellen globalen Ausfällen
- Keine Abhängigkeit von Cloud-Systemen, die nicht DSGVO- konform sind
- Lokale oder hybride Lösungen mit hoher Verfügbarkeit nutzen

☐ Datenschutzkonforme Messenger einsetzen

- Kein WhatsApp oder andere unsichere Consumer-Apps
- Sichere Lösungen wie Teamwire mit Verschlüsselung und Notfall-Features nutzen

☐ Alternative Kommunikationsmethoden einrichten

- Push-to-Talk für Sofortnachrichten in Notfällen
- Broadcast-Funktion für schnelle Updates an große Gruppen
- Statusmeldungen zur Lageeinschätzung in Echtzeit
- Live-Standort für bessere (Einsatz-)Koordination
- Relevante Gruppenchats für Notfälle

Schritt 3

☐ Offline- und Notfallkontaktlisten führen

- Wichtige Telefonnummern und Ansprechpartner auch analog verfügbar halten
- Klare Anweisungen für den Fall eines IT- oder Netzausfalls bereitstellen

☐ Notfall-Warnsysteme aktivieren

- Automatische Benachrichtigungen und Alarme bei kritischen Vorfällen
- Smarte Eskalationsmechanismen einrichten

Schritt 4

Regelmäßige Tests und Schulungen durchführen

Schulen Sie Ihre Mitarbeitenden in der Anwendung der Tools und stellen Sie sicher, dass jeder versteht, wie es in einer Krisensituation zu nutzen ist. Es ist wichtig, dass die Lösung intuitiv zu bedienen ist und in die tägliche Kommunikation integriert wird, damit sie im Ernstfall vertraut und sofort einsatzbereit ist.

Einen solchen Ernstfall sollten Sie vorab in unternehmensweiten Übungen erproben. Überwachen Sie dabei die Kommunikation und passen Sie gegebenenfalls die Abläufe an, um im Ernstfall optimal zu reagieren und Schäden so gering wie möglich zu halten.

Ziel: Die Notfallkommunikation regelmäßig erproben und die Mitarbeitenden vorbereiten.

- [ ] **Regelmäßige Krisensimulationen durchführen**
  - Ernstfälle nachstellen: z. B. Cyberangriff-Simulation oder Stromausfall-Szenarien
  - Überprüfung, ob alle Kommunikationswege und Notfallmaßnahmen greifen
- [ ] **Schulungen und Trainings für alle relevanten Mitarbeitenden**
  - Wie und wann wird das Krisenteam informiert?
  - Welche Kanäle sind wann von Nutzen?
  - Wie wird eine Krise gemeldet und eskaliert?
- [ ] **Dokumentation der Krisenübungen & Lessons Learned**
  - Protokollieren, was gut funktioniert und wo Optimierung nötig ist
  - Maßnahmen zur Verbesserung ableiten
- [ ] **Awareness-Maßnahmen für Mirabeitende etablieren**
  - Schulungen zu Cybersecurity und zu sicherem Verhalten in Krisen
  - Praktische Übungen mit realistischen Szenarien

Schritt 5

Nach der Krise evaluieren und verbessern

Jede Krise oder Übung bietet die Chance, besser zu werden. Nehmen Sie sich Zeit, Prozesse zu analysieren, Feedback einzuholen und Ihre Krisenstrategie zu optimieren. Nur so kann Ihre Organisation langfristig resilient bleiben.

Ziel: Aus jeder Krise oder Übung lernen und Prozesse kontinuierlich optimieren.

- [ ] Krisenverlauf und Kommunikation analysieren
  - Was hat gut funktioniert?
  - Wo gab es Verzögerungen oder Missverständnisse?
- [ ] Feedback der Beteiligten einholen
  - Hat sich die eingesetzte Technologie bewährt?
  - Wurden alle relevanten Personen schnell informiert?
- [ ] Krisenkommunikationsstrategie anpassen
  - Notfallpläne aktualisieren
  - Verantwortlichkeiten nachjustieren
- [ ] Technische Infrastruktur regelmäßig überprüfen
  - Sind alle eingesetzten Kommunikationslösungen noch sicher und aktuell?
  - Sind neue Technologien oder Features erforderlich?
- [ ] Langfristige Verbesserungen etablieren
  - Ist eine bessere Integration mit bestehenden IT-Systemen möglich?
  - Sollte das Krisenteam weiter ausgebaut oder geschult werden?

Jetzt testen:

Sie können auch einen schnellen, kostenlosen Selbsttest auf unserer Webseite durchführen:

Funktioniert Ihre Kommunikation auch, wenn die IT ausfällt? Prüfen Sie in wenigen Schritten, ob Ihre Kommunikation im Ernstfall zuverlässig weiterläuft.

→ Hier der Selbsttest starten

Vor- und Nachbereitung entscheidet über den Erfolg in Krisensituationen

Krisensichere Kommunikation ist kein Luxus – sie ist essenziell für Städte und Gemeinden. Wer vorbereitet ist, schützt nicht nur Daten und Systeme, sondern auch seine Mitarbeitenden, die Bürger und den Geschäftsbetrieb.

Übrigens: In unseren zahlreichen Success-Stories können Sie entdecken, wie Teamwire unseren Kunden aus den verschiedenen Branchen in der Praxis hilft.

→ Hier finden Sie alle Success-Stories.

06. Fazit und Ausblick

Resilienz beginnt mit Kommunikation

Krisen lassen sich nicht verhindern – ihre Auswirkungen jedoch sehr wohl begrenzen. Für Städte und Gemeinden entscheidet sich die Handlungsfähigkeit im Ernstfall nicht allein an der technischen Robustheit von Verwaltungsinfrastrukturen, sondern maßgeblich an der Qualität der Kommunikation. Sie ist das verbindende Element zwischen Krisenstab, IT, Ordnungsamt, Bauhof, Einsatzteams und externen Partnern.

Krisenfeste Kommunikation ist kein isoliertes IT-Projekt, sondern ein integraler Bestandteil moderner Daseinsvorsorge.

Die Praxis zeigt: Standardkommunikation reicht in Ausnahmesituationen nicht aus. Systeme, die im Alltag gut funktionieren, sind im Krisenfall häufig selbst betroffen, nicht priorisierbar oder organisatorisch ungeeignet. Improvisierte Ausweichlösungen schaffen kurzfristig Reichweite, erhöhen jedoch langfristig Risiken – operativ, regulatorisch und reputational.

Krisenfeste Kommunikation muss deshalb bewusst vom Normalbetrieb entkoppelt gedacht werden. Sie benötigt einen eigenen, ausfallsicheren Kanal, der auch dann funktioniert, wenn zentrale IT-Systeme oder Cloud-Dienste nicht verfügbar sind. Gleichzeitig muss sie den besonderen Anforderungen kommunaler Verwaltungen gerecht werden: klare Steuerbarkeit, schnelle Alarmierung, sichere Informationsverteilung, Nachvollziehbarkeit sowie vollständige DSGVO- und NIS-2-Konformität.

Dieser Leitfaden hat gezeigt, dass krisenfeste Kommunikation kein isoliertes IT-Projekt ist, sondern ein integraler Bestandteil moderner Daseinsvorsorge. Sie unterstützt nicht nur die operative Bewältigung von Krisen, sondern schafft Orientierung, reduziert Unsicherheit und stärkt das Vertrauen von Mitarbeitenden, Partnern und Bürgern.

Für Städte und Gemeinden bedeutet das: Wer heute in belastbare Kommunikationsstrukturen investiert, handelt nicht reaktiv, sondern verantwortungsvoll und vorausschauend. Kommunikation wird damit zu einem strategischen Faktor der Resilienz und zu einer zentralen Voraussetzung dafür, auch in Ausnahmesituationen handlungsfähig zu bleiben und den Versorgungsauftrag zuverlässig zu erfüllen.

Es ist Zeit, Ihre kommunale Verwaltung krisensicher zu machen

Krisenfeste Kommunikation entsteht nicht durch Zufall, sondern durch bewusste Entscheidungen. Für Städte und Gemeinden bedeutet das, Kommunikationsstrukturen regelmäßig zu prüfen, Schwachstellen zu identifizieren und gezielt abzusichern – bevor der Ernstfall eintritt.

Wie steht es um Ihre Krisenkommunikation?

Wir unterstützen Sie dabei, Schwachstellen zu identifizieren und eine krisenfeste Kommunikationsstruktur aufzubauen – individuell auf Ihre Gemeinde oder Stadtverwaltung zugeschnitten:

Teamwire jetzt kostenlos testen →

Live-Demo jetzt anfordern →

Impressum

Herausgeber
Teamwire GmbH
Tittmoninger Straße 11
81679 München, Deutschland

Website
teamwire.eu

E-Mail
info@teamwire.eu

Geschäftsführung
Tobias Stepan
Registergericht: Amtsgericht München
HRB 187102

Konzeption
Teamwire GmbH, teamwire.eu

Text
Stephanie Strohmeier,
Teamwire GmbH, teamwire.eu

Layout & Grafik
Pilar Sabogal, Salva González, Teamwire GmbH, teamwire.eu

Die Inhalte des Leitfadens wurden mit größter Sorgfalt erstellt. Für die Richtigkeit, Vollständigkeit und Aktualität können wir jedoch keine Gewähr übernehmen.


teamwire