

Schutz von Krisenkommunikation

Die entscheidende Rolle einer sicheren
Kommunikationsplattform im
Krisenmanagement

Wire Germany GmbH und Future Intelligence Group AG
März 2025

Krisenmanagement im digitalen Zeitalter



In unserer schnelllebigen und vernetzten Welt stehen Unternehmen ständig vor neuen Herausforderungen und unvorhersehbaren Ereignissen. Krisen wie Naturkatastrophen, Cyberangriffe oder Pandemien können jederzeit auftreten und den Geschäftsbetrieb massiv stören. Ein effektives Krisenmanagement und Business Continuity Management (BCM) sind daher unerlässlich, um die Resilienz eines Unternehmens zu gewährleisten und den Betrieb auch in Ausnahmesituationen aufrechtzuerhalten.

Die fortschreitende Digitalisierung und Vernetzung erhöht gleichzeitig die Verwundbarkeit von Unternehmen. Cyberangriffe werden immer ausgefeilter und können Geschäftsabläufe erheblich beeinträchtigen. Zudem führen die wachsende Abhängigkeit von Cloud-Diensten und mobilen Endgeräten zu neuen Risiken. Daher ist es wichtiger denn je, schon im Vorfeld Vorkehrungen zu treffen und ein umfassendes Krisenmanagementsystem einzuführen. Gerade in Krisensituationen ist eine sichere Kommunikation entscheidend. Damit geeignete Maßnahmen schnell und koordiniert ergriffen und Schäden minimiert werden können, muss ein reibungsloser Informationsaustausch zwischen allen Beteiligten gewährleistet sein. Herkömmliche Kommunikationswege sind oftmals anfällig für Ausfälle oder Sicherheitslücken – mit potenziell verheerenden Folgen im Ernstfall.



Was zeichnet gutes Krisenmanagement aus?

Erfolgreiches Krisenmanagement besteht nicht nur darin, im Ernstfall richtig zu reagieren, sondern auch in Prävention und Vorbereitung. Dazu gehört, potenzielle Risiken zu identifizieren, Krisenpläne zu erstellen und Mitarbeiterinnen und Mitarbeiter so zu schulen, dass sie im Ernstfall angemessen handeln.

Viele Unternehmen unterschätzen jedoch sowohl die Wahrscheinlichkeit als auch die möglichen Auswirkungen einer Krise. Nach einer Studie des Bundesamts für Sicherheit in der Informationstechnik (BSI) verfügen lediglich 43 % der befragten Unternehmen über einen aktuellen Krisenplan. Zudem beziehen viele Krisenpläne nicht alle relevanten Szenarien ein – von Naturkatastrophen über Pandemien und Cyberangriffe bis hin zu wirtschaftlichen und politischen Krisen, technischen Störungen oder Reputations- und Lieferkettenkrisen.

Fehlende Vorbereitung in der Krisenkommunikation führt dazu, dass im Notfall wichtige Informationen nicht rechtzeitig bei den richtigen Stellen ankommen. Bestehende Kommunikationsinfrastrukturen sind für Krisen häufig nicht ausgelegt und können zusammenbrechen.

Daher ist eine sichere Kommunikationsplattform in der Krisenplanung von essenzieller Bedeutung. Denn in kritischen Situationen muss bereits im Vorfeld sichergestellt sein, dass die Kommunikation intern wie extern schnell und zuverlässig funktioniert.

Was ist eine sichere Kommunikationsplattform?

Eine wirklich sichere Plattform bietet eine geschützte Umgebung, in der Unternehmenskommunikation selbst im Krisenfall weiterlaufen kann. Sechs zentrale Eigenschaften spielen dabei eine Schlüsselrolle:



Ende-zu-Ende-Verschlüsselung ohne Ausnahme

Eine Plattform sollte sämtliche Kommunikationsformen – Chat, Audio- und Videotelefonie, große Videokonferenzen, Dateiaustausch und Integrationen – konsequent Ende-zu-Ende verschlüsseln. Viele Lösungen versprechen Verschlüsselung, ohne diese in allen Bereichen durchgehend zu gewährleisten.



Zero-Trust- und Zero-Knowledge-Architektur

Zero Trust bedeutet, dass kein Nutzer, Gerät oder Dienst standardmäßig vertraut wird. Jeder Zugriff erfordert laufende Verifikation und Authentifizierung. Darüber hinaus muss eine Zero-Knowledge-Architektur greifen: Selbst wenn Server kompromittiert werden, darf es keinen „Masterzugang“ zu den Inhalten oder Metadaten der verschlüsselten Kommunikation geben.



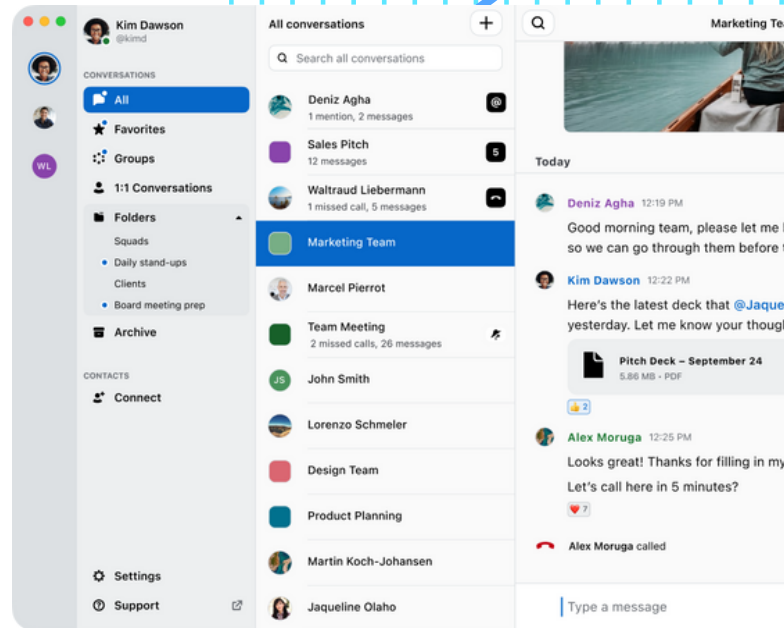
Post-Quantum-Ready

Mit dem Aufkommen des Quantencomputings wird es zunehmend wichtig, dass die Sicherheitsprotokolle einer Kommunikationsplattform zukunftsfähig bleiben. So sollte beispielsweise das Messaging Layer Protocol (MLS) oder ein vergleichbares Sicherheitskonzept eingesetzt werden, das eine flexible Anpassung der Verschlüsselungsverfahren ermöglicht.



Open Source

Ein essenzielles Prinzip von Zero Trust ist Transparenz auf allen Ebenen – bis hin zum Code. Eine Plattform, die auf Open Source setzt, schafft größtmögliche Nachvollziehbarkeit und Prüfbarkeit des Sicherheitsniveaus.



Datenhoheit

Unternehmen, die hohe Anforderungen an Datenschutz, Compliance mit lokalen Vorschriften und den Schutz vor Überwachung durch ausländische Staaten haben, benötigen eine Lösung, die sie auch On-Premises betreiben können. Nur so behalten sie die volle Kontrolle über ihre Daten.



Benutzerfreundlichkeit

Was auf den ersten Blick weniger nach einem Sicherheitsaspekt aussieht, ist in der Praxis essenziell. Fehlt es an einfacher Bedienung, nutzen Mitarbeitende womöglich „Schatten-IT“, beispielsweise WhatsApp. Dadurch entstehen gefährliche Sicherheitslücken. Eine sichere Plattform muss sich im Arbeitsalltag nahtlos integrieren lassen.

Warum sichere Kommunikation für das Krisenmanagement unverzichtbar ist



Schnelle Reaktionsfähigkeit

In Krisen zählt jede Sekunde. Mit Wire lassen sich alle relevanten Personen – von Mitarbeitenden über Führungskräfte bis zu externen Partnern – sofort per Messaging, Audio-/Videotelefonie und Dateiaustausch erreichen. So können Gegenmaßnahmen koordiniert und Schäden minimiert werden.



Zuverlässigkeit

Herkömmliche Kommunikationskanäle sind in Krisensituationen oft überlastet oder fallen aus. Wire hingegen wurde auf maximale Stabilität und Verfügbarkeit ausgelegt. Als einzige Plattform nutzt Wire vollständig das moderne Messaging Layer Security (MLS) Protokoll, das schnelle und sichere Gruppenkommunikation in großem Umfang ermöglicht – und das alles auch bei hoher Auslastung.



Vertraulichkeit und Integrität

Gerade sensible Daten, etwa Notfallpläne oder Finanzinformationen, müssen vor unbefugtem Zugriff geschützt sein. Dank Ende-zu-Ende-Verschlüsselung können nur autorisierte Personen die Nachrichten lesen. Wire wurde in Deutschland entwickelt, ist frei von Überwachungsstaats-Hintertüren (wie z. B. durch den Patriot Act) und bietet mit Open-Source-Code und On-Premises-Installationen volle Transparenz und Souveränität.



Effiziente Krisenkommunikation

In einer einzigen Plattform laufen alle Maßnahmen zusammen: Chatgruppen, Dateitransfers und Videokonferenzen sorgen für strukturierten Informationsfluss und klare Aufgabenverteilung. Zusätzlich erfolgt die starke Verschlüsselung automatisch im Hintergrund, sodass Anwenderinnen und Anwender keine manuellen Einstellungen vornehmen müssen.

Anwendungsbeispiele für eine sichere Plattform im Krisenmanagement

Ransomware-Angriff

Ein Krankenhaus wird von Ransomware befallen – ein gravierendes Beispiel ist das Universitätsklinikum Düsseldorf. Durch verschlüsselte Server ist der Betrieb stark eingeschränkt. Eine sichere Kommunikationsplattform, die selbst kompromittierte Server überstehen kann, ermöglicht eine koordinierte Reaktion und sichert die Patientenversorgung weitestgehend.

Ungewolltes Datenleck

Ein IT-Team speichert versehentlich sensible Kundendaten öffentlich zugänglich. So geschehen 2024 bei Cariad (VW-Tochter), als durch eine Fehlkonfiguration in der Amazon-Cloud Bewegungsdaten von 800.000 E-Autos mitsamt Personenbezug frei verfügbar waren. Mit einer sicheren Plattform können IT, PR und Management schnell reagieren, technischen und kommunikativen Schaden eindämmen und die Situation unter Kontrolle bringen.

Kompromittiertes Kollaborationstool

Ein Medienkonzern erleidet ein Datenleck in seiner Collaboration-Plattform (z.B. Microsoft Teams oder Slack), ähnlich wie ein umfassender Angriff auf Disneys Slack-Instanz mit Millionen internen Nachrichten. In solch einer Lage ist es entscheidend, rasch und sicher miteinander zu kommunizieren, um Begrenzung zu betreiben und IT- wie Compliance-Maßnahmen abzustimmen.





Globale, politische Unruhen

Ein internationaler Hersteller ist in einer politisch instabilen Region aktiv und fürchtet Lieferketten- und Produktionsausfälle. Beispielsweise führten Spannungen zwischen Indien und China zu Verzögerungen in Häfen und beim Nachschub. Eine sichere Plattform bietet einen vertraulichen Kommunikationskanal für lokale Mitarbeiter, Partner und Lieferanten und hält so den Betrieb aufrecht.

Führungskrisen

Ein Topmanager wird der illegalen Überwachung beschuldigt – der Ruf des Unternehmens steht auf dem Spiel. 2019 sorgte ein ähnlicher Fall bei der Credit Suisse für Aufsehen. Mit einer sicheren Plattform können Führungskräfte, Vorstand und Berater intern Informationen austauschen, die Situation bewerten, interne und externe Kommunikation koordinieren und rechtliche Risiken begrenzen.

Geschäftsentscheidungen mit hohem Risiko

Unternehmen sehen sich manchmal gezwungen, unpopuläre Maßnahmen zu ergreifen, etwa Stellenabbau oder die Schließung von Standorten. 2024 beendete Volkswagen (VW) den Beschäftigungsschutz mit IG Metall und erwog die Schließung deutscher Werke – eine höchst kontroverse Entscheidung mit entsprechendem Echo von Belegschaft und Öffentlichkeit. Eine sichere Plattform hilft, diese Entscheidungen intern abzustimmen und die unvermeidliche Außenkommunikation möglichst effektiv zu gestalten.

Wire + Future Intelligence: Eine umfassende Lösung für Krisenmanagement und sichere Kommunikation



Future Intelligence: Krisen und Business Continuity Management Future Intelligence entwickelt und implementiert auf Ihr Unternehmen zugeschnittene Krisenmanagementpläne, führt Übungen mit dem Krisenteam durch und schult Ihre Mitarbeitenden. Zudem gestaltet Future Intelligence Kommunikationsstrategien für unterschiedliche Krisenszenarien, richtet effiziente Kommunikationskanäle ein und unterstützt Sie in der Medienarbeit. Darüber hinaus geht Future Intelligence über das reine Krisenmanagement hinaus und ermittelt kritische Geschäftsprozesse, erstellt Notfallpläne und sorgt dafür, dass Ihr Betrieb auch im Krisenfall weiterlaufen kann.

Die Partnerschaft mit Wire Future Intelligence empfiehlt Unternehmen, die verschlüsselte Kommunikationsplattform Wire zu nutzen, um Datendiebstahl und Industriespionage gezielt vorzubeugen. Als hochsichere Lösung ist Wire ideal, um in Krisenzeiten vertrauliche Informationen auszutauschen. Mit Ende-zu-Ende-Verschlüsselung, Zero-Knowledge-Architektur und modernen Sicherheitsstandards gewährleistet Wire auch unter widrigsten Bedingungen die Vertraulichkeit und Integrität Ihrer Kommunikation.

Die Vorteile eines ganzheitlichen Ansatzes für Krisenmanagement, Business Continuity und sichere Krisenkommunikation

Wenn Organisationen integrierte Krisen- und Business-Continuity-Management-Pläne mithilfe sicherer Kommunikationslösungen entwickeln, bleiben sie auch in schwierigen Zeiten handlungsfähig und gehen gestärkt daraus hervor. Nachfolgend sind die wichtigsten Vorteile dieses ganzheitlichen Ansatzes aufgeführt:

Schutz von Vermögenswerten und Geschäftskontinuität

Krisenmanagement bewahrt die Assets eines Unternehmens – sei es im Fall von Naturkatastrophen, Cyberangriffen oder Wirtschaftskrisen. Parallel dazu stellt ein wirksames Business Continuity Management sicher, dass kritische Prozesse selbst in Krisensituationen weiterlaufen. Eine sichere Kommunikationsplattform bildet in allen Szenarien das Rückgrat für den reibungslosen Austausch von Informationen.

Reputation und Vertrauen

In Krisenzeiten ist eine transparente Kommunikation unverzichtbar, um Vertrauen bei Kunden, Partnern und Stakeholdern zu bewahren. Gleichzeitig erfordern brisante Themen besondere Vorsicht. Eine sichere Plattform schafft genau dafür den geschützten Rahmen, in dem die interne Abstimmung stattfinden kann – bevor das Unternehmen öffentlich kommuniziert.



Rechtliche und regulatorische Anforderungen

Mit Richtlinien wie NIS2 oder DORA steigen die Anforderungen an Unternehmen, v. a. bei kritischen Infrastrukturen. Sichere Kommunikationslösungen erfüllen wichtige Teile dieser Vorgaben und helfen, empfindliche Strafen zu vermeiden.

Wettbewerbsvorteil

Unternehmen mit starkem Krisenmanagement und BCM demonstrieren Widerstandsfähigkeit und können sich dadurch im Markt behaupten.

Mitarbeitersicherheit und Motivation

Gute Krisenstrategien schützen die Sicherheit und das Wohlbefinden der Belegschaft und schaffen Vertrauen. Wenn Mitarbeitende wissen, dass sie auf eine zuverlässige Infrastruktur zählen können, steigert das ihre Motivation und Identifikation mit dem Unternehmen.

Vermeidung finanzieller Verluste

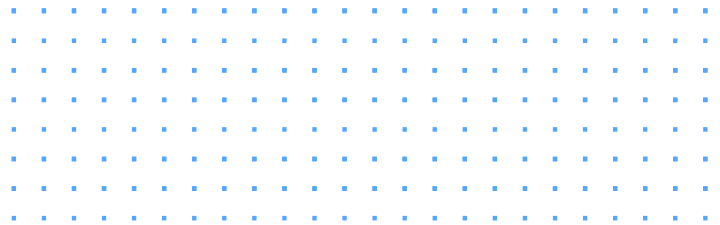
Je schneller eine Krisenreaktion abläuft, desto geringer sind mögliche Schäden. Eine effiziente Schadensbegrenzung, getragen von sicherer Kommunikation, senkt die finanziellen Folgen einer Krise erheblich.





Empfehlungen

Viele Unternehmen sind trügerisch beruhigt – frei nach dem Motto „Uns wird schon nichts passieren“. Diese Haltung kann im Ernstfall katastrophale Folgen haben. Die richtige Zeit zu handeln ist jetzt. Die folgenden sieben Schritte helfen beim Wechsel vom reaktiven zum proaktiven Krisenmanagement:



Sensibilisieren

Führungskräfte müssen für die Bedeutung von Krisenmanagement und sicherer Kommunikation sensibilisiert sein.



Analysieren

Mögliche Risiken und Schwachstellen sollten systematisch identifiziert werden.



Planen

Pläne müssen individuell sein, regelmäßig getestet und implementiert werden.



Kommunizieren

Eine durchdachte Krisenkommunikation darf nicht erst im Ernstfall konzipiert werden, sondern gehört von Anfang an zur Strategie.



Investieren

Eine sichere Kommunikationsplattform, die die oben genannten Kriterien erfüllt, ist eine entscheidende Investition in die Zukunftsfähigkeit des Unternehmens.



Falsche Annahmen erkennen

- „Wir kümmern uns später darum.“ Prävention ist nur wirksam, wenn sie frühzeitig umgesetzt wird.
- „Krisenmanagement ist zu teuer.“ Kurzfristiges Sparen kann langfristig weitaus höhere Kosten verursachen.
- „So etwas ist uns noch nie passiert.“ Die Welt verändert sich rasch, und Krisen kündigen sich selten lange vorher an.



Rechtliche Vorgaben einhalten

Neue EU-Richtlinien wie NIS2 und DORA drohen mit hohen Strafen, wenn Unternehmen keine angemessenen Sicherheitsmaßnahmen einführen.

Fazit

Im digitalen Zeitalter sind Krisenmanagement und sichere Kommunikation essenziell, um Reputationsschäden, finanzielle Einbußen und Betriebsunterbrechungen zu vermeiden. Wire und die Future Intelligence Group AG unterstützen Unternehmen dabei mit ganzheitlichen Lösungen für eine vorausschauende Krisenprävention.

Wenn Sie mehr über unsere Angebote erfahren möchten und wie wir Ihr Unternehmen krisenfest machen können, kontaktieren Sie uns gerne.

