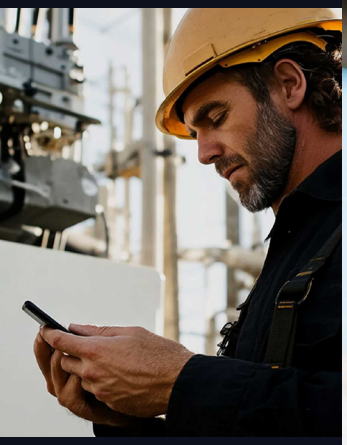
Checkliste:
5 praktische Schritte für eine krisensichere Kommunikation



teamwire

Für IT-Verantwortliche, CEOs, CISOs und Entscheider in Unternehmen, Organisationen und Behörden

Einführung

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

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

Krisenkommunikations-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?

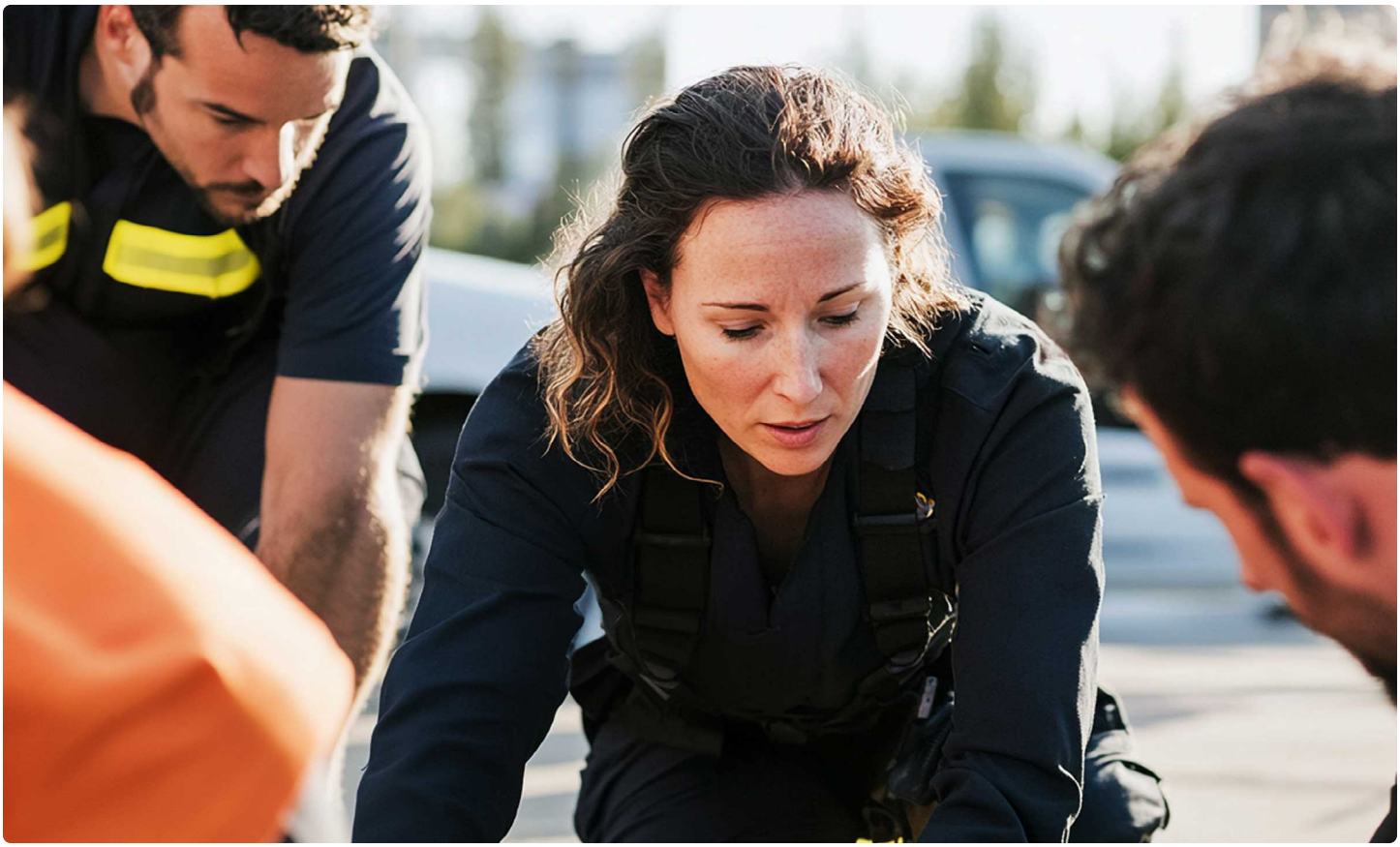
Schritt 3

Krisensichere Kommunikationstechnologie 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 Betriebskontinuitätsmanagements 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.

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?

Vor- und Nachbereitung entscheidet über den Erfolg in Krisensituationen

Krisensichere Kommunikation ist kein Luxus – sie ist essenziell für Behörden und Organisationen mit Sicherheitsaufgaben (BOS), KRITIS und Unternehmen mit hohen Sicherheitsanforderungen, das Gesundheitswesen und kommunale Verwaltungen.

Wer vorbereitet ist, schützt nicht nur Daten und Systeme, sondern auch seine Mitarbeitenden, seinen Kundenstamm und den Geschäftsbetrieb.

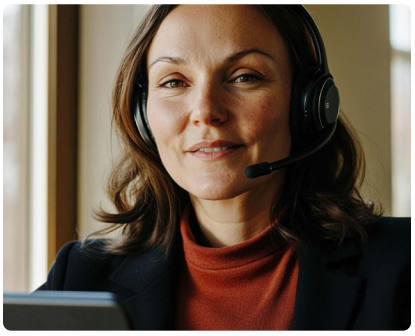
Wer vorbereitet ist, schützt nicht nur Daten und Systeme, sondern auch seine Mitarbeitenden, seinen Kundenstamm und den Geschäftsbetrieb.

Wer vorbereitet ist, schützt nicht nur Daten und Systeme, sondern auch seine Mitarbeitenden, seinen Kundenstamm und den Geschäftsbetrieb. Vertiefen Sie Ihr Wissen mit unseren praxisnahen Ressourcen rund um sichere Kommunikation. Unsere Leitfäden, die Sie unterstützen, Ihre Ziele zu erreichen, stehen Ihnen zum kostenlosen Download zur Verfügung.

Und in unseren zahlreichen Sucess-Stories können Sie entdecken, wie Teamwire unseren Kunden aus den verschiedenen Branchen in der Praxis hilft.

Hier finden Sie alle Leitfäden und Success-Stories.

Viel Freude beim Lesen!



Kontaktieren Sie uns für eine individuelle Beratung und Demo.

Kontaktieren Sie uns →

Impressum

Herausgeber
Teamwire GmbH Tittmoninger
Straße 11 81679 München

Website
teamwire.eu

E-Mail
info@teamwire.eu

Geschäftsführung
Tobias Stepan
Registergericht: Amtsgericht München
HRB 187102

Konzeption
Teamwire GmbH, teamwire.eu

Text
Stephanie Strohmeier, Tobias Stepan,
Teamwire GmbH, teamwire.eu

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

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

Alle Rechte vorbehalten – einschließlich der, welche die Vervielfältigung, Bearbeitung, Verbreitung und jede Art der Verwertung der Inhalte dieses Dokumentes oder Teile davon außerhalb der Grenzen des Urheberrechtes betreffen. Handlungen in diesem Sinne bedürfen der schriftlichen Zustimmung durch Teamwire. Teamwire behält sich das Recht vor, Aktualisierungen und Änderungen der Inhalte vorzunehmen. Sämtliche Daten und Inhalte, die auf Screenshots, Grafiken und weiterem Bildmaterial sichtbar sind, dienen lediglich zur Demonstration. Für den Inhalt dieser Darstellung übernimmt Teamwire keine Gewähr.

© Teamwire GmbH, 2026

teamwire