# DOK FORUM | ICT TRENDS 2025

F24

## Unternehmerische Krisen- und Ausnahmesituationen in Echtzeit beherrschen

ICT BUSINESS & TECHNOLOGY CONSULTING

DOK SYSTEME

**Sebastian Bolle**

Head of Partnerchannel DACH

Montag, 24. November 2025

*Public*

F24


**Sebastian Bolle**

Head of Partner Channel DACH

+49 151 58242449

sebastian.bolle@f24.com

# F24 – Ihr Partner mit globaler Reichweite im Bereich Resilienz

**#1** Europas führender Software-as-a-Service (SaaS) Alarmierungs-, Incident- und Krisenmanagement

**25** Jahre Erfahrung

**1** Erster und einziger europäischer Anbieter im **Gartner** Report für EMNS und von **Forrester** unter den Top-10-CEM Anbietern gelistet

**280+** Mitarbeiter weltweit

**71.4 m** EUR Umsatz (FY2024[1])

[1] pro-forma

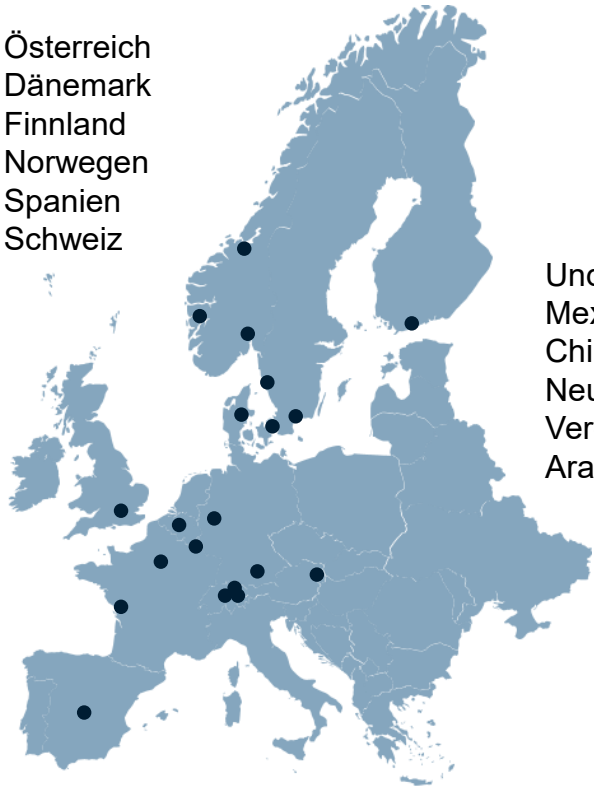
**5,500+** Kunden weltweit

DAX40 Anteil
**53%**

STOXX Europe 50 Anteil
**38%**

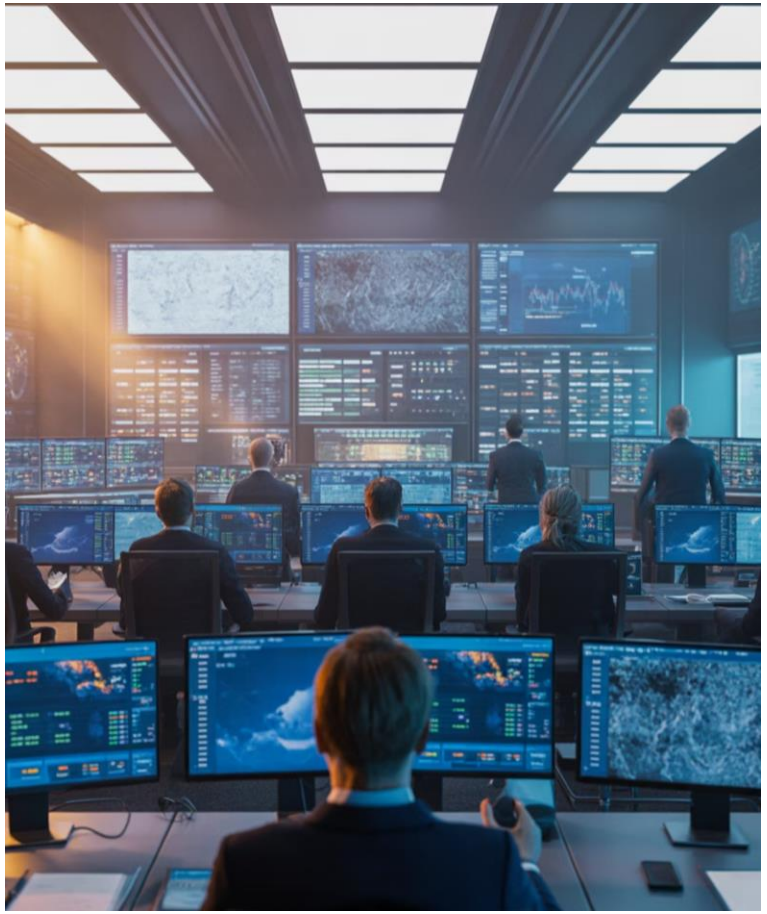
**20+** Standorte in Europa

Deutschland (HQ)
Belgien
Frankreich
Luxemburg
Großbritannien
Schweden
Österreich
Dänemark
Finnland
Norwegen
Spanien
Schweiz



Und auch in:
Mexiko
Chile
Neuseeland
Vereinigte Arabische Emirate

# Unternehmerische Krisen- und Ausnahmesituationen in Echtzeit beherrschen



- Globale Vernetzung, Cyberbedrohungen, Lieferkettenrisiken und regulatorische Anforderungen erhöhen die Komplexität

**NIS 2** **KritisDachG** **B3S**
**DORA** **ISO 27001** **ISO 22301**

haben klare Anforderungen an Strukturen für **Detektion**, **Alarmierung**, **Eskalation**, **Krisenmanagement** und **Notfallkommunikation**

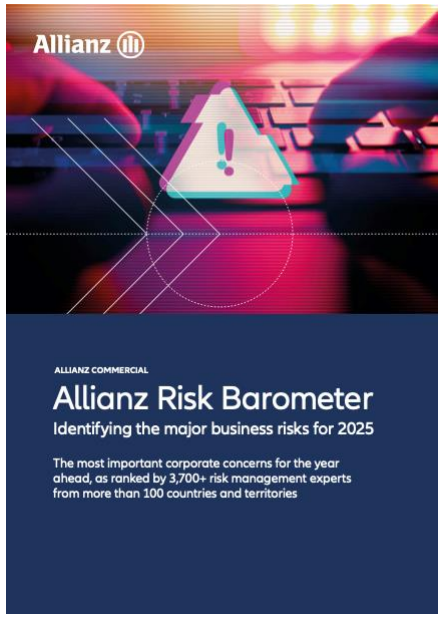
- Organisationen müssen in Echtzeit reagieren – unabhängig von IT-Systemen, Standorten oder Personen
- Krisenkommunikation ist heute keine Kür, sondern Voraussetzung für Resilienz und Compliance
- **Krisen lassen sich nicht verhindern – aber sie lassen sich beherrschen**

**Es ist die richtige Mix aus Organisation, Verantwortung und Technologie, die über Erfolg oder Misserfolg entscheidet.**

# Risikobetrachtung

## Risiken in der Praxis

Die Allianz hat **451 Unternehmen in Deutschland** befragt, welche **Risiken** sie als die **größten Bedrohungen für ihre Organisation** sehen.




**Cyberrisiken / IT-Ausfälle** **47%**
Ransomware-Angriffe, Datenlecks und gezielte Cyberattacken bedrohen die digitale Infrastruktur von Unternehmen Systemausfälle, Cloudprobleme und Netzwerkstörungen führen zu erheblichen Betriebsunterbrechungen

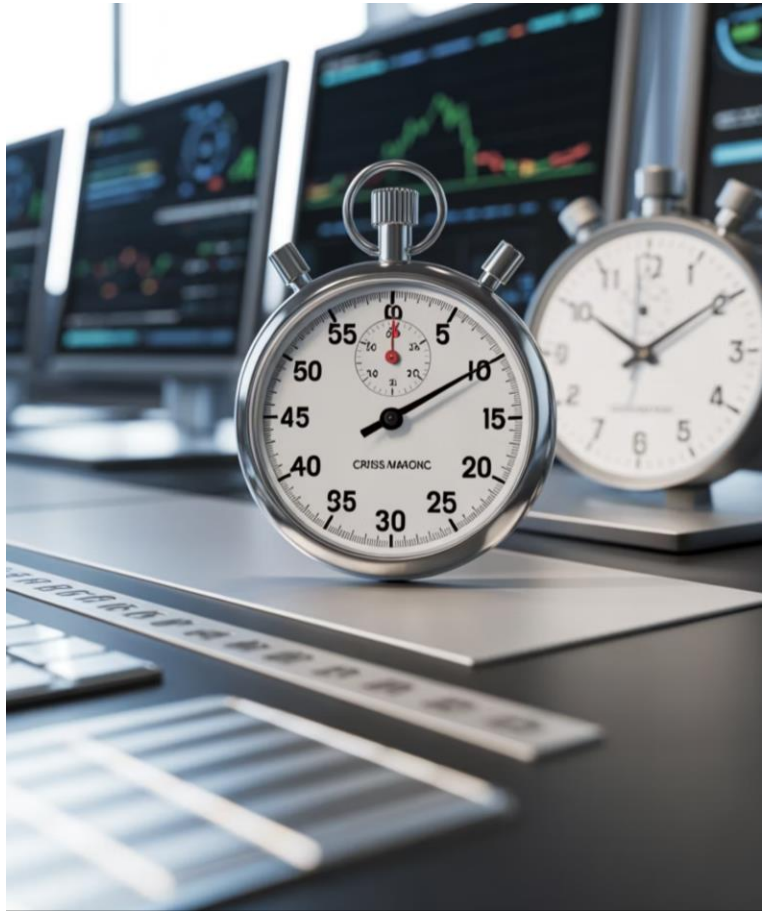
**Betriebsunterbrechungen** **46%**
Lieferkettenprobleme, Produktionsausfälle und Infrastrukturschäden beeinträchtigen die Geschäftskontinuität

**Rechtliche Risiken** **19%**
Regulatorische Anforderungen, Compliance-Verstöße und Haftungsfragen steigen kontinuierlich

**Ob IT-Ausfall, Stromstörung oder Cyberangriff – die ersten Minuten entscheiden über den Verlauf**

Genau deshalb sprechen wir heute über den Faktor Zeit, über Alarmierung, Krisenkommunikation und warum beides nicht dasselbe ist.

# Der Aspekt Zeit
## entscheidender Erfolgsfaktor

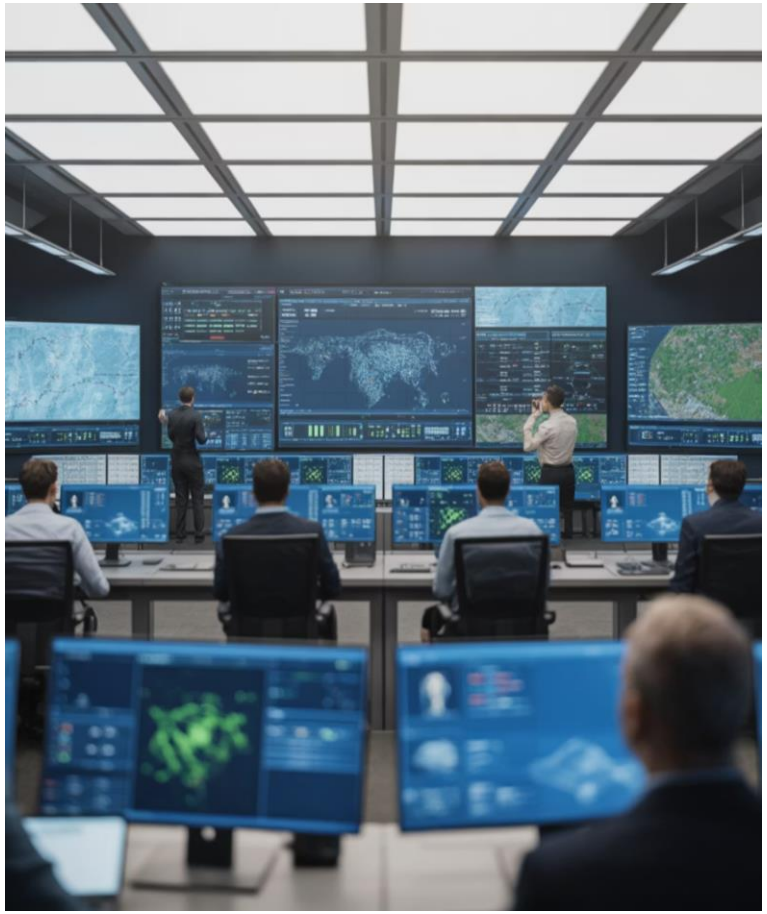


- **Zeitgewinn entscheidet über Verlauf und Auswirkung einer Krise**
- je früher Informationen fließen und Entscheidungen getroffen werden, desto besser lässt sich eine **Eskalation verhindern**


- Zeit ist keine technische, sondern eine organisatorische Ressource

# Alarmierung ist nicht Krisenmanagement

## Planbar vs. Situativ



### Alarmierung
**ist ein Prozess**

- Vorbereitet und strukturiert
- Prozessgetrieben nach definierten Szenarien
- Automatisierte Abläufe
- Wer wird wann wie informiert?
- Auslösung nach Regeln

**Es ist planbar**

### Krisenmanagement
**ist Führung**

- Alles ist Dynamisch
- Lagegetrieben
- Entscheidungen unter Unsicherheit
- Steuerung im Echtbetrieb
- Was wird wie kommuniziert?
- Wer kommuniziert?

**Es ist Situativ**

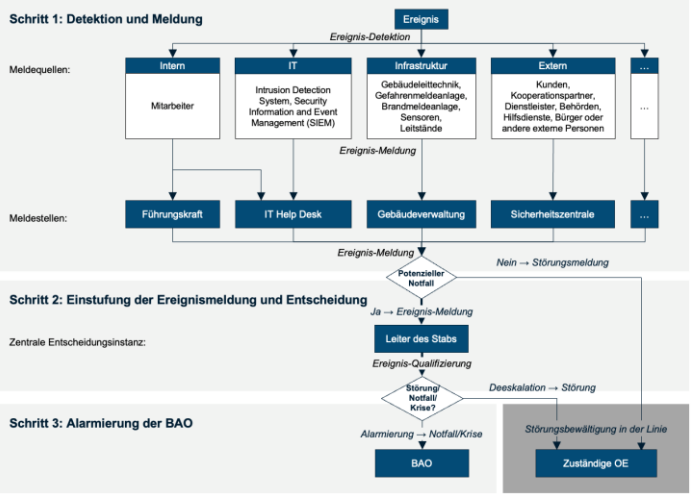
**Erst die Verbindung beider Ebenen schafft echte Handlungsfähigkeit:**

- **Geschwindigkeit** ohne Orientierung führt zu Aktionismus
- **Orientierung** ohne Geschwindigkeit führt zu Stillstand

# Hilfestellung: BSI-Standard 200-4

## Detektion, Alarmierung, Eskalation

**Der BSI-Standard 200-4 beschreibt die strukturierte Abfolge vom Ereignis bis zur Krisenorganisation**




- **Schritt 1: Detektion & Meldung** über interne Quellen (IT-Systeme, Infrastruktur, Mitarbeiter) **oder** externe Quellen (Kunden, Dienstleister, Behörden)
  → **Meldung erfolgt an definierte Stellen** (z. B. IT Help Desk)
- **Schritt 2: Einstufung & Entscheidung**
  ***Zentrale Entscheidungsinstanz prüft:*** Störung oder potenzieller Notfall?
  ***Qualifizierung:*** Störung / Notfall / Krise. Wenn es unklar oder gravierend ist
  → **Einberufung Krisenstab zur Lagebewertung**
- **Schritt3: Alarmierung BAO** Bei bestätigtem Notfall/Krise
  → **Alarmierung der besonderen Aufbauorganisation**

In jedem Fall sollte sichergestellt werden, dass Schadensereignisse und Störungen mit Notfallpotenzial an eine zentrale Entscheidungsinstanz gemeldet werden.

Zusätzlich **muss** für den Alarmierungs- und Eskalationsprozess technisch sichergestellt sein, dass die **Kommunikations- und Alarmierungstechnik auch in einem Not- oder Krisenfall zur Verfügung steht**.

Es sollten außerdem **Kommunikationskanäle zur Verfügung stehen, die unabhängig von der IT der Institution funktionieren**.

F24

**Wie kann ich so etwas technisch umsetzen?**

# Lokale Alarmserver

## Mit klaren Grenzen

Traditionelle lokale Alarmserver können anfällig für Störungen, die ihre Funktionsfähigkeit in kritischen Situationen stark einschränken können. Diese Abhängigkeiten stellen ein erhebliches Risiko für die Krisenfestigkeit dar.

**Abhängigkeit von lokaler Stromversorgung und IT-Infrastruktur**

Ein Ausfall der lokalen Stromversorgung oder der IT-Infrastruktur legt den Server lahm und macht ihn unbrauchbar

**Risiko durch Naturereignisse, Brände oder Cyberangriffe**

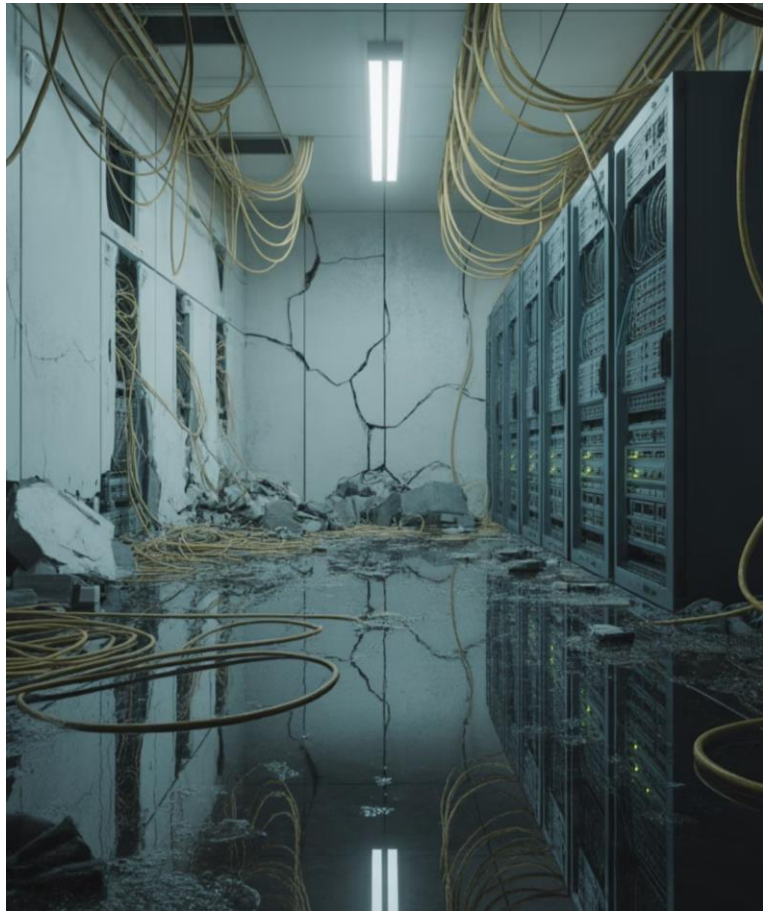
Physische Gefahren oder Cyberangriffe können lokale Systeme direkt zerstören oder blockieren

**Redundanz vor Ort ≠ Krisenfestigkeit**

Selbst redundante Systeme am gleichen Standort sind bei einem umfassenden Ausfall des Standorts nutzlos

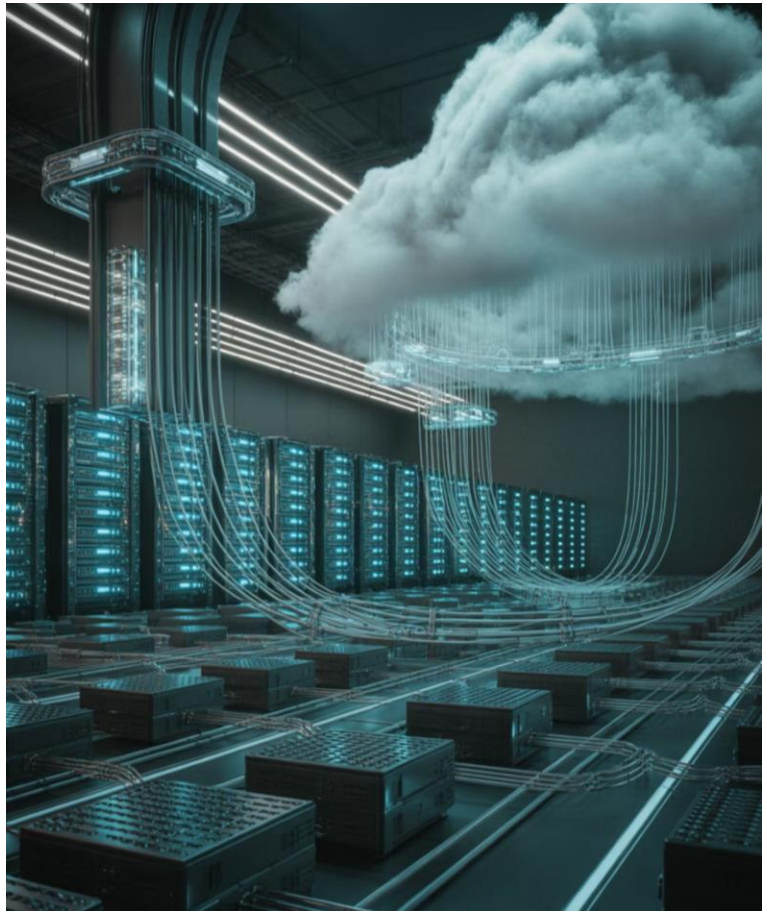
**Kommunikation endet am Standort**

Bei einem Ausfall des lokalen Netzwerks oder Servers ist eine Kommunikation über den Standort hinaus nicht mehr möglich



# Cloud-basierte Alarmserver

## Die bessere Lösung?



### IT-Infrastrukturunabhängigkeit

Cloud-Lösungen sind unabhängig von lokaler IT-Infrastruktur und extern redundant ausgelegt.

### Durchgängige Kommunikation

Kommunikation bleibt auch bei lokalen Systemausfällen am Standort bestehen.

### Keine echte Anbindung an lokale Systeme

Typischerweise basieren diese auf IP-basierten Eingängen (REST, Webhooks, Mail, SMS). Ohne ein durchgängiges Integrationskonzept bleibt die Kopplung an lokale Gefahrenmelde-, IT- und TK-Systeme brüchig – insbesondere bei Leitungs- oder Standortausfällen

### Fehlende lokale Integration

Integration in lokale Infrastruktur ist ohne komplexe Workarounds nicht möglich.

# Hybrid
## der logische Weg

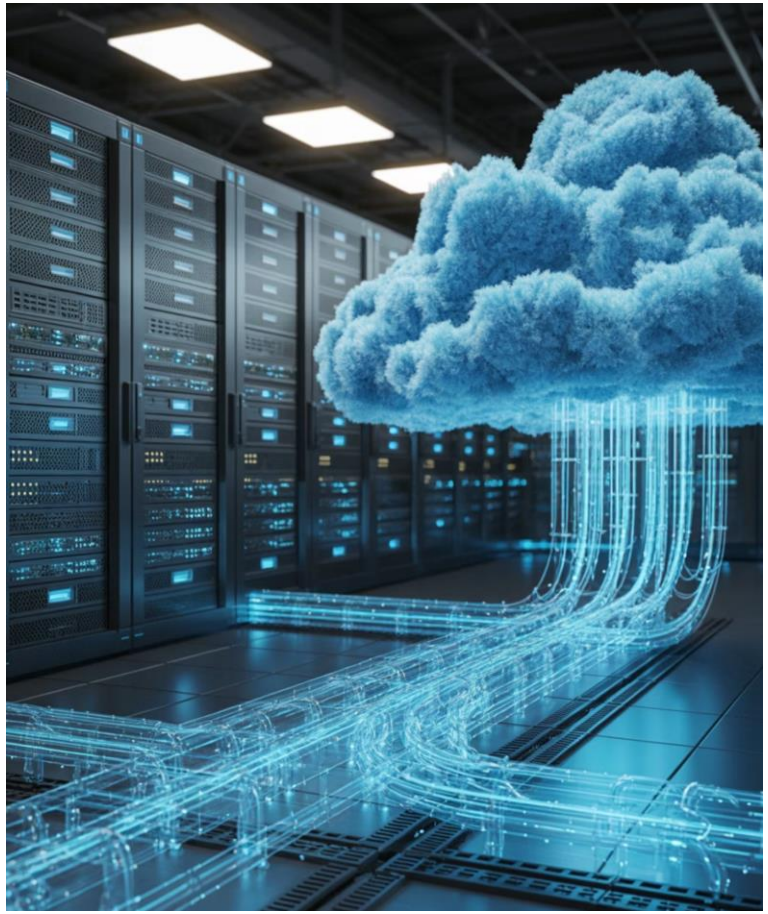
FACT24

### Lokale Plattform + SaaS-Lösung als Gesamtsystem
Die Kombination aus einer lokalen Alarmierungsplattform und einer SaaS-Lösung schafft ein robustes Gesamtsystem für höchste Anforderungen.

### Durchgängige Kommunikation: Lokal & Extern
Beide Kommunikationswege – lokal (z.B. Telefon, DECT) und extern (Massen-Anrufe, SMS, E-Mail, Push, etc.)

### Echtzeit-Alarmierung auch bei Teilausfällen
Diese hybride Architektur gewährleistet eine durchgängige Echtzeit-Alarmierung und Handlungsfähigkeit, selbst bei teilweisen Infrastrukturausfällen.

### Maximale Resilienz und verkürzte Reaktionswege
Getrennte, aber nahtlos vernetzte Ebenen sichern jederzeit die Handlungsfähigkeit und verkürzen durch parallele Nutzung die Reaktionswege erheblich.

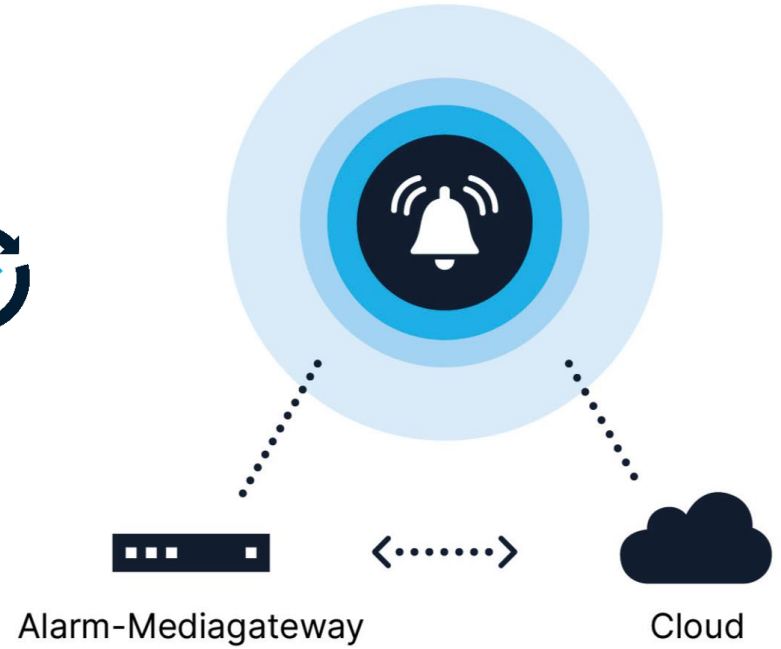


# Bausteine für ein professionellen Notfall- und Krisenmanagements

FACT24

**99,99%**

garantierte Verfügbarkeit für Alarmierungsservices und 99,50% für alle anderen Services




Alle Daten sind durch umfassende technische und organisatorische Maßnahmen

**DSGVO-konform**

geschützt

**ISO zertifiziert**

F24 wird unter einem Managementsystem entwickelt und betrieben, das nach **ISO/IEC 27001 und 22301 zertifiziert** ist

**Unsere Lösungen verbinden Alarmierung, Incident-Management und Krisenmanagement in einer Plattform**
**Das sorgt dafür, dass alle Bausteine nicht isoliert stehen, sondern ineinandergreifen**

# Praktisches Beispiel: Cyberangriff

# IT-Security in der Praxis

## Wenn 3 Uhr morgens die SMS kommt

### Typische Vorbereitungen

- ✓ Organisationen kaufen Tools – SIEM, SOAR, EDR, MDR, XDR, UEBA
- ✓ Eine ISO 27001 wird vorbereitet
- ✓ Dann kommt der Auditor
- ✓ Dokumentation ist geschrieben
- ✓ Zertifikat wird ausgestellt
- ✓ Alle sind zufrieden

**Übungen?**
**Einmal im Jahr, Dienstag 10 Uhr – angekündigt!**
**„Wir simulieren Ransomware.“**

### Dann kommt der Ernstfall

- 3 Uhr nachts. Systeme schlagen Alarm (SMS/Mail) – aber niemand reagiert.
- Production Server ist down.
- Vermutung: Ransomware.
- Wer liest die Nachrichten?
- Wer eskaliert?
- Wer entscheidet?
- Wie ist der Asset-Owner zu dieser Zeit erreichbar?

**Das ist der Moment, in dem man merkt:**

- Compliance ist nicht Sicherheit
- Ohne zuverlässige Alarmierung und Eskalation ist ein SOC im Ernstfall praktisch nicht handlungsfähig

# BSI-Standard 200-4 BCM

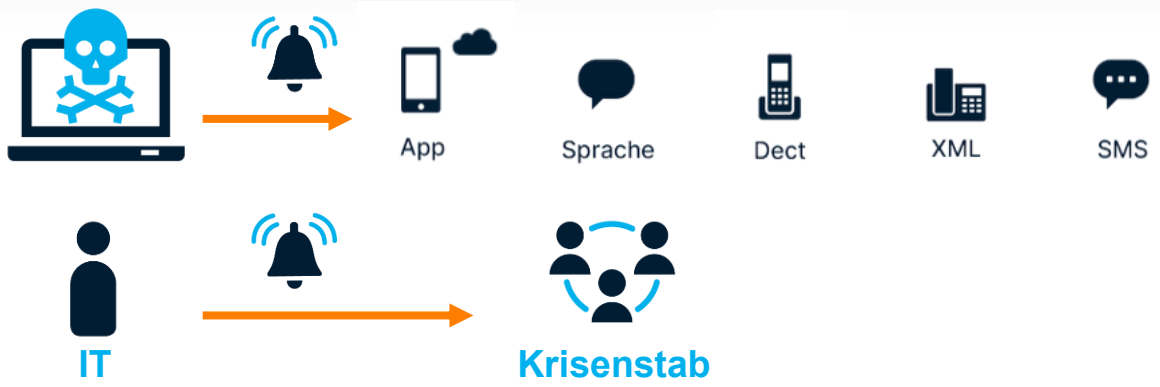
## Schritt 1: Detektion und Meldung
## Integration in die bestehende Infrastruktur

FACT24 ENS+


**Nahtlose Integration**

FACT24 ENS+ lässt sich in bestehende IT-Sicherheitsinfrastrukturen integrieren

- **Integration in IT-/EDR-/SIEM-Systeme** zur Auslösung automatisierter Alarmierungsprozesse
- **Kalenderanbindung zur Einbindung** von Bereitschaften und Verfügbarkeiten
- **Multimedialer Kommunikationsmix** (Telefon, SMS, App, Konferenz) für 24/7-Erreichbarkeit
- **IT-Teams werden binnen Sekunden informiert und alarmiert**



# BSI-Standard 200-4 BCM

## Schritt 2: Einstufung der Ereignismeldung und Entscheidung
## Kommunikation innerhalb des Krisenstabs

FACT24 ENS+

### Einfache Aktivierung

Über das Smartphone, das Webinterface oder einen Telefonanruf

### Priorisierte Alarmierungslisten

Die wichtigsten Stakeholder zuerst benachrichtigen (Entscheidungsträger & Wissensträger)

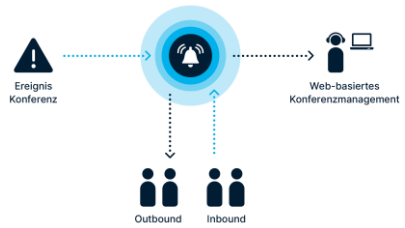
### Direkte Kommunikationskanäle (IT-Infrastukturunabhängig)

Alarmierungen über mehrere Kanäle wie Telefonanrufe, SMS und mobile Apps

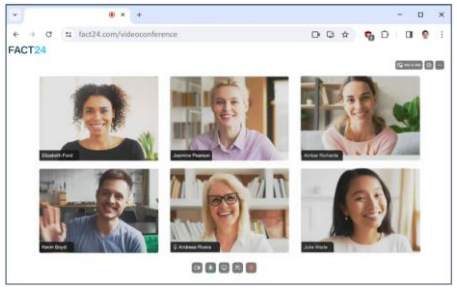
### Kollaborative Entscheidungsfindung

teilen und gemeinsame Entscheidungen treffen

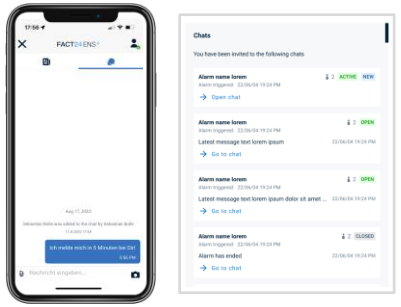
### Audio-Konferenzen



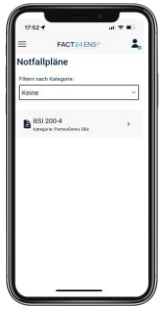

### Video-Konferenzen




### Chats



### Notfallpläne




### Echtzeit-Informationen und Updates

Entscheidungsträger laufend mit aktuellen und relevanten Informationen versorgen

### Dokumentation und Nachverfolgung

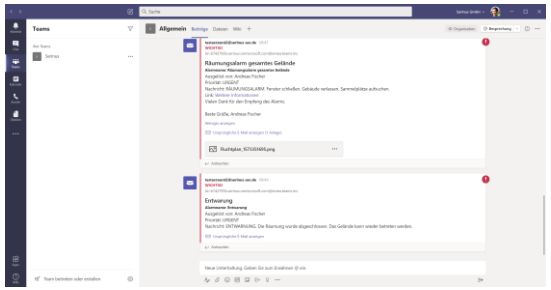
Revisionssichere Aufzeichnung aller Aktivitäten und Entscheidungen

# BSI-Standard 200-4 BCM

## Schritt 3: Alarmierung der BAO

## Erreichbarkeit von Internen und Externen

FACT24 ENS+



**Primäre Kanäle** (für z.B. Mitarbeiter)

- **Sprachanruf**
- **Smartphone App**
- **PC-Client**
- **Chat**
- Microsoft Teams, und andere UCC-Lösungen

(Unter Berücksichtigung von Skills, Dienstplänen und Verfügbarkeit)

**Sekundäre Kanäle** (für z.B. Externe)

- **SMS**
- **E-Mail**
- **Fax**

# Kommunikation in der Krise

## Der entscheidende Erfolgsfaktor

### In der Krise entscheidet Kommunikation über Erfolg oder Misserfolg.

- **Multi-Kanal-Fähigkeit**
  Jeder Kanal hat seine Berechtigung. **Hybride Redundanz schaffen Sicherheit** und stellensicher, dass kritische Nachrichten ankommen.

- **Führung durch Kommunikation**
  Ein Kristenstab muss kommunizieren können.
  Kommunikation sorgt dafür, dass alle Beteiligten das gleiche Lagebild haben, koordiniert handeln können, das Mitarbeiter angewiesen und Kunden informiert werden.

- **Koordiniertes Handeln**
  Effektive Krisenkommunikation synchronisiert Teams, vermeidet Doppelarbeit und stellt sicher, dass Ressourcen optimal eingesetzt werden.

> **Kommunikation ist kein Nebenaspekt des Krisenmanagements – sie ist das zentrale Steuerungsinstrument**
> Ohne klare Kommunikation gibt es keine koordinierte Reaktion.

# Informationsverteilung

## mit zeitkritischen Hintergrund

## wenn es um Menschen oder Werte geht

FACT24 ENS+

### Alarmierung

- Rufbereitschaft
- Massenalarmierung
- Patientenalarme
- Krisenstäbe einberufen

### Technische Alarmierung

- IT-Alarmierung
- OT-Alarmierung
- Smart Building
- REST-API

### Arbeitsschutz

- Alleinarbeits-platzschutz
- Ersthelfer-Notruf
- Stiller Alarm
- Räumungs- und Evakuierungsalarm

### Krisenmanagement

- Incident Management
- BCM / IT-Notfall-management
- Amok & Terror
- Info-Hotline

F24

Die Frage ist längst nicht mehr, ob oder wann eine Krise kommt, sondern –

# Wie gut sind wir vorbereitet?