

Cyber Crisis Management

23. September & 2. Oktober 2025



Cyber Crisis Management

Albert Hilgenberg

CISO / Lead Security Assurance Services

hilgenberg@avantec.ch

Warum Cyber Crisis Management heute unverzichtbar ist



Cyberangriffe zählen weltweit zu den grössten Geschäftsrisiken – zusammen mit Betriebsunterbrechungen und Naturkatastrophen.



Cyberangriffe treffen alle Branchen, von Finanzinstituten, Spitälern, Industrie, Behörden und KMU



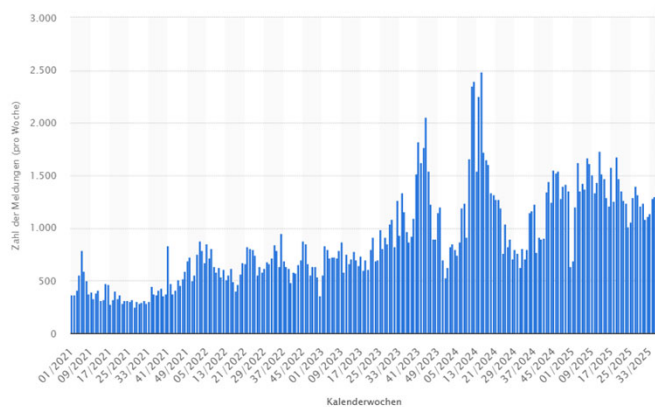
Regulatoren und Versicherungen fordern klare Prozesse



Reputation und Vertrauen entscheiden über Überleben



Es ist keine Frage ob, sondern wann



«In der Krise ist nicht die Technik entscheidend, sondern wie gut die Organisation reagiert.»

Cyber Crisis Management

23. September & 2. Oktober 2025

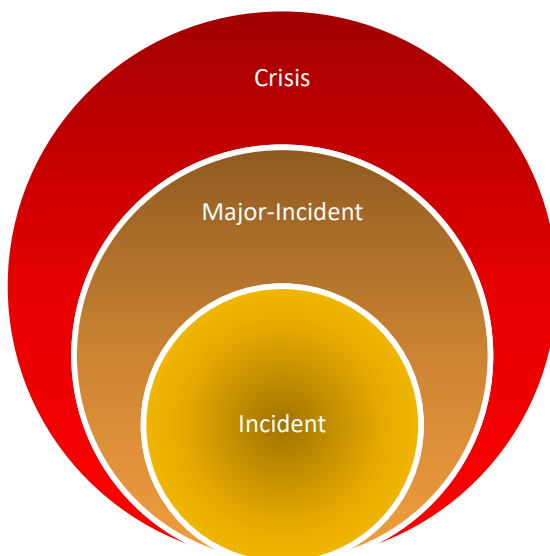
Was erwartet Sie in den nächsten 45 Minuten?



Agenda

-  **Grundlagen & Kernkomponenten** – Rollen, Prozesse, Bausteine
-  **Vorbereitung & Prozesse** – Szenarien, Playbooks, Teams
-  **Recovery & Lessons Learned** – Wiederanlauf, Nachbereitung, Verbesserung
-  **Kommunikation** – Stakeholder, Prinzipien, Strategie
-  **Diskussion & Q&A** – Takeaways, Fragen

Was ist eine Cyber-Krise?



Crisis:

Existenzielle Bedrohung, hohe Unsicherheit, strategische Entscheidungen nötig

Major Incident:

Kritischer Service betroffen, Management muss informiert werden

Incident:

Lokal, technisch lösbar, minimale Auswirkungen

Cyber Crisis Management

23. September & 2. Oktober 2025

Merkmale einer Cyber-Krise



Unerwartet, hoher **Zeitdruck**, fehlende Infos

Technisch **und** organisatorisch **komplex**

Bedrohung für Geschäft, Reputation, Compliance

Hoher **Entscheidungsdruck** auf allen Ebenen



Eine Cyber-Krise ist mehr als ein IT-Problem – sie ist eine Unternehmenskrise

Auswirkungen einer Cyber-Krise



Finanziell

- Umsatzverlust, Betriebsunterbrechungen, Vertragsstrafen

Reputation

- Vertrauensverlust bei Kunden und Partnern
- Negative Medienberichterstattung

Regulatorisch

- Geldbussen, Meldepflichten, behördliche Prüfungen

Operationell

- Unterbrechung kritischer Geschäftsprozesse
- IT-Ausfälle, reduzierte Leistungsfähigkeit

Strategisch

- Verlust von Marktanteilen
- Einschränkung zukünftiger Geschäftsmöglichkeiten



Diese potenziellen Risiken zeigen, wie entscheidend effektives Crisis Management für den Schutz von Geschäft, Reputation und Compliance ist.

Cyber Crisis Management

23. September & 2. Oktober 2025

Kernkomponenten im Cyber Crisis Management



Cyber Crisis Management Team

- **Steuert die Krise zentral** – Koordination aller Beteiligten und Prozesse
- **Trifft schnelle & fundierte Entscheidungen** – reduziert Risiken und Verzögerungen
- **Schützt Geschäft, Reputation & Vertrauen** – intern wie extern

Technische & organisatorische Resilience

- Systeme, Netzwerke und Prozesse
- Notfall-Infrastruktur, Backups, Redundanzen
- Fachliche Expertise & Einsatzbereitschaft

Governance & Policy

Governance & Policy

- Verantwortlichkeiten, Entscheidungsbefugnisse, Freigaben
- Rechtliche und regulatorische Anforderungen
- Struktur, Compliance und Verbindlichkeit

Prozesse & Playbooks

- Vorgefertigte Handlungsanweisungen für Szenarien
- Klare Rollen, Eskalationswege und Kommunikation
- Schnelle, koordinierte Reaktion ermöglichen

Technische & organisatorische Resilience

Prozesse und Playbooks

Cyber Crisis Management Team



Kernfunktion des Cyber Crisis Management Teams



Operative Steuerung

- Massnahmen priorisieren, Risiken bewerten, Entscheidungen dokumentieren

Koordination

- Abteilungen & externe Stakeholder abstimmen, Informationsfluss sichern

Kommunikation

- Interne & externe Botschaften steuern, Vorlagen nutzen, konsistent informieren

Psychologische Entlastung

- Rollen & Eskalationswege klar, externe Experten unterstützen



Schnell handeln, Risiken bewerten, Massnahmen koordinieren.

Cyber Crisis Management

23. September & 2. Oktober 2025

Rollen & Verantwortung



Geschäftsleitung

- Strategische Entscheidungen, Budget & Kommunikation

Teamleiter

- Operative Koordination, Lagebesprechungen

Security Lead

- Analyse, Eindämmung, Behebung

IT/Infrastruktur

- Systeme steuern, Wiederherstellung sichern

Kommunikationsbeauftragter

- Konsistente interne & externe Kommunikation

Legal / Compliance

- Meldungen, Behördenkontakt, rechtliche Beratung

Externe Berater

- Spezialwissen, Entlastung, regulatorische Anforderungen



Klare Rollen und abgestimmte Verantwortlichkeiten

Krisenreaktion: Stellen Sie sich diese Fragen



- Wer sollte im Cyber Crisis Management Team sein?
- Welche externen Experten benötigen wir?
- Wie arbeitet unser Cyber Crisis Management Team, wenn die Kernsysteme ausfallen?
- Wo treffen wir uns, wie versorgen wir das Team, wie organisieren wir die Schichten?
- Wie greifen wir auf das Cyber Crisis Playbook zu?
- Wie gehen wir mit Lösegeldforderungen um? Was ist die rechtliche Lage?
- Wann Polizei, Behörden und regulatorische Stellen informieren?
- Wann informieren wir Kunden? Welche Kunden? Ehemalige Kunden? Wie? Wer ist dafür verantwortlich?
- Wie kommunizieren wir, wenn die üblichen Kanäle (E-Mail, Webseite, Teams etc.) ausfallen?

Cyber Crisis Management

23. September & 2. Oktober 2025

Cyber Crisis Playbook



Vermeidet Chaos:

- In der Krise zählt jede Minute – ein Playbook reduziert Improvisation.

Beschleunigt Entscheidungen:

- Klare Rollen, Prozesse und Eskalationswege schaffen Handlungssicherheit.

Erhöht Effektivität:

- Abstimmung zwischen IT, Security, Legal & Kommunikation wird erleichtert.

Reduziert Stress:

- Checklisten und Vorlagen entlasten das Team unter Druck.

Sichert Konsistenz:

- Einheitliche Botschaften und regulatorische Vorgaben werden zuverlässig eingehalten.



Viele Themen, eine Struktur – so bleibt das Team handlungsfähig.

Struktur & Inhalte



Rollen & Verantwortlichkeiten

Entscheidungsprozesse

Lagebesprechungen

Checklisten

- **Vorbereitend:** Systeme prüfen, Kontaktdaten aktualisieren, Trainingsplan, Playbook-Zugriff sichern
- **Akut:** Lagebewertung, technische Sofortmassnahmen, Kommunikation, regulatorische Meldungen
- **Nachbereitend:** Dokumentation, Lessons Learned, Wiederherstellung & Tests

Kommunikationspläne

Regulatorische Anforderungen

2. Cyber Crisis Management Checkliste

Die nachfolgende Checkliste bildet die Basis für die Lagebesprechungen:

ID	Aufgabe	Ref.
1	Prüfung der Anwesenheit aller notwendigen Teilnehmer	A.1
2	Bestimmung der Leitung des CCMT	A.2
3	Bestimmung des Entscheidungskaders	A.3

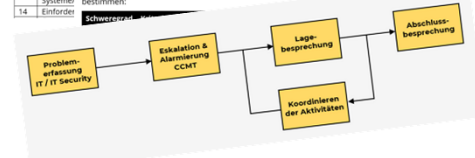
Appendix B - Definition & Kriterien für eine Cyber Krise

Eine Cyber Security Krise wird dann ausgerufen, wenn ein Security Incident den Schweregrad 'High' oder 'Critical' erreicht hat. Dies wird auch Major Incident genannt. Die Schweregrade von Security Vorfällen sind folgendermassen definiert:

Schweregrad	Definition Schweregrad
Low	Keine unmittelbare Schädigung bzw. Bedrohung von Schutzziele (Verfügbarkeit, Integrität, Vertraulichkeit) kritischer Aktiven.
Medium	Unmittelbare Schädigung bzw. Bedrohung von Schutzziele (Verfügbarkeit, Integrität, Vertraulichkeit) kritischer Aktiven.
High	Schutzziele (Verfügbarkeit, Integrität, Vertraulichkeit) kritischer Aktiven sind erheblich geschädigt bzw. bedroht.
Critical	Umfangreiche und länger anhaltende Schäden an Schutzziele (Verfügbarkeit, Integrität, Vertraulichkeit) kritischer Aktiven vorhanden bzw. erwartet.

Tabelle 5 Definition Schweregrad eines Security Vorfalls

Die nachfolgenden Kriterien sollen helfen, den Schweregrad eines Security Vorfalls zu bestimmen:



Cyber Crisis Management

23. September & 2. Oktober 2025

Vorbereitung auf eine Cyber Krise



- 1 Analyse**
- BIA – Auswirkungen auf Geschäftsprozesse
 - Crisis Management Check – Strukturen & Prozesse
 - Reputationsrisiko – Image & Stakeholder

- 2 Planung**
- Szenarioplanung – mögliche Cybervorfälle
 - Cyber Crisis Playbook – Abläufe & Verantwortlichkeiten
 - Krisenkommunikation – intern & extern

- 3 Simulation**
- Playbook Briefing – Einführung
 - Crisis Simulation – Szenario-Übung
 - Rollentraining – gezielte Aufgaben

- 4 Lessons Learned**
- Feedback & Review – Erkenntnisse aus Übungen und Vorfällen
 - Optimierung – Pläne und Prozesse anpassen

Kommunikation als Erfolgsfaktor in Cyber-Krisen



In einer Cyber-Krise entscheidet **Kommunikation** über Erfolg oder Misserfolg.

Sie formt die Wahrnehmung von Kunden, Partnern, Mitarbeitenden und Behörden, erhält **Vertrauen** und Reputation und beeinflusst direkt die Handlungsfähigkeit. Klare, proaktive und konsistente Kommunikation ermöglicht es dem Unternehmen, die Krise **effizient zu steuern** und die Bewältigung aktiv zu kontrollieren.

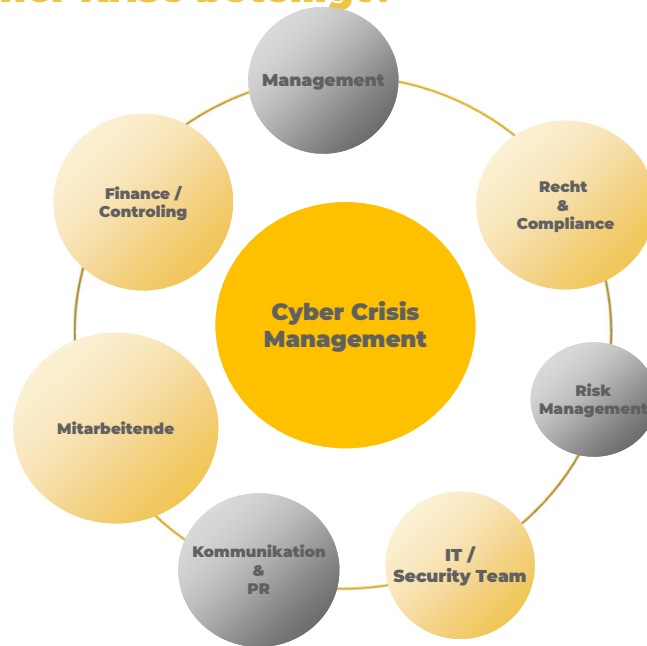
intern & extern



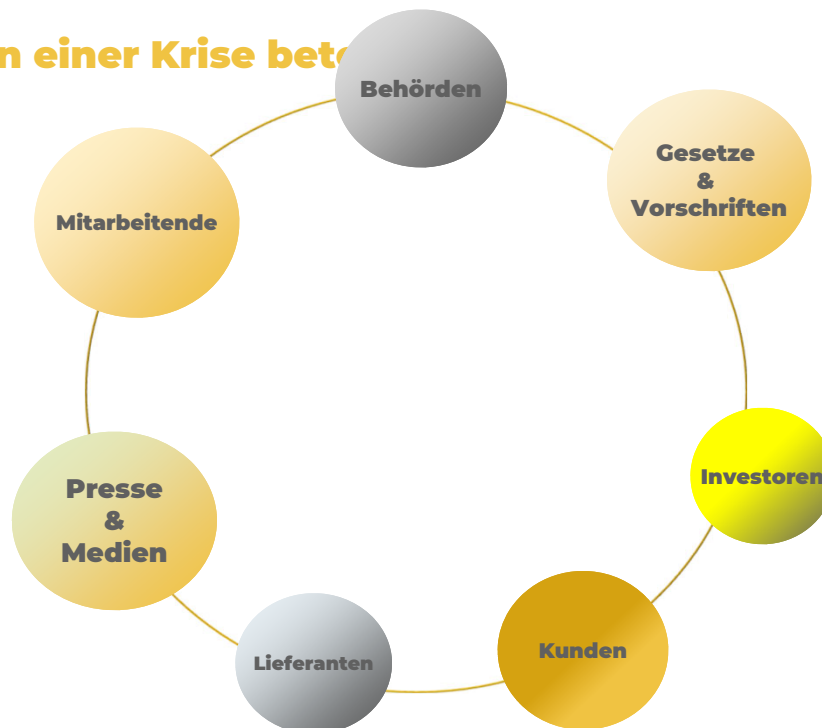
Cyber Crisis Management

23. September & 2. Oktober 2025

Wer ist in einer Krise beteiligt?



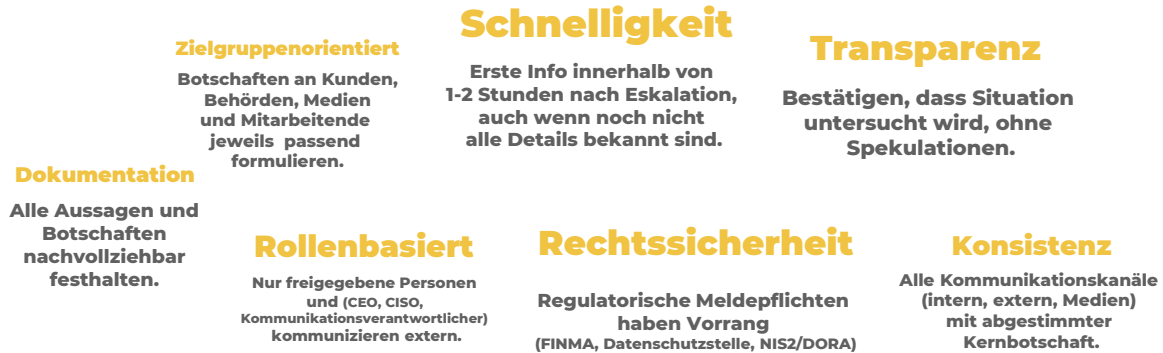
Wer ist in einer Krise beteiligt?



Cyber Crisis Management

23. September & 2. Oktober 2025

Generische Kommunikationsprinzipien



Kommunikationskanäle & Kanal-Strategie



Kommunikationskanäle & Tools

- **Intern:** Intranet, Mail, Chat-Tools (z. B. Teams), Telefonketten, Townhalls.
- **Extern:** Website (Notfallseite vorbereitet), Kundenmails, Callcenter-Skripte, Social Media Accounts, Pressemitteilungen.
- **Fallback:** Alternativkanäle bei IT-Ausfällen (z. B. externe Provider, Notfall-Website).

Kanal	Typ	Ziel	Ton / Sprachregelung	Risiken / Hinweise
Pressemitteilung	Einseitig	Öffentlichkeit, Medien	Sachlich, faktenbasiert, kontrolliert	Keine spekulativen Aussagen
Website / Notfallseite	Einseitig	Kunden, Partner	Klar, transparent, Handlungsorientiert	Regelmässige Updates notwendig
E-Mail an Kunden	Einseitig	Kunden	Vertrauensbildend, präzise, kurze Handlungsanweisungen	Keine technischen Details, die Kriminelle nutzen könnten
Intranet-News	Einseitig / bidirektional	Mitarbeitende	Aktiv, klar, direkt	Feedbackkanal schaffen (z. B. Helpdesk)
Townhall / Videokonferenz	Bidirektional	Mitarbeitende, Management	Beruhigend, transparent, kontrolliert	Fragen filtern, klare Moderation
Callcenter / Hotline	Bidirektional	Kunden	Einheitliche Antworten, vorgefertigte FAQ	Schulung der Mitarbeitenden, Eskalation definieren
Social Media	Bidirektional	Öffentlichkeit, Kunden	Kontrollierte Statements, Monitoring	Realtime Monitoring notwendig, Reputationsrisiko bei ungeplanten Posts

Cyber Crisis Management

23. September & 2. Oktober 2025

Situationsmatrix



Eskalationsstufe	Beispiel-Szenario	Kommunikationsfokus	Adressaten	Verantwortlich
Stufe 1: Verdacht	Ungewöhnliche Aktivitäten, interne Abklärungen laufen	Nur interne Kommunikation, keine externe Aktivität	Mitarbeitende im betroffenen Bereich	CISO / IT Security
Stufe 2: Bestätigter Vorfall	Eingeschränkter Datenabfluss, Angriff im CDC bestätigt	Frühe Information an Management & kritische Stakeholder, Vorbereitung externer Meldungen	Management, CISO, Behörden (z. B. Datenschutzstelle, FINMA)	CISO + Krisenstab
Stufe 3: Kritischer Vorfall	Relevante Kundendaten oder Geschäftsprozesse betroffen	Proaktive externe Kommunikation, transparente Lageeinschätzung, Schadensbegrenzung	Kunden, Medien, Behörden, Partner	CEO + Kommunikation
Stufe 4: Öffentlichkeitswirksam	Vorfall bereits in Medien / Social Media	Aktive Medienarbeit, konsistentes Messaging, Krisen-PR	Medien, Öffentlichkeit	CEO + Kommunikation

Sprachleitfaden für Cyber Crisis Kommunikation



Unternehmen 1 (hilflos):

- „Wir sind seit Donnerstag von einem Cyberangriff betroffen. Unsere Systeme sind ausgefallen. Heute (Samstag) ist ein spezielles Incident Team vor Ort und untersucht den Fall.“

Unternehmen 2 (stark):

- „Wir haben am Donnerstag einen Cyberangriff festgestellt und die Systeme vorsorglich isoliert, um Risiken zu minimieren. Seitdem arbeiten unsere internen und externen Spezialisten daran, die Services strukturiert wiederherzustellen.“

Don'ts

- Passiv („wir sind betroffen“, „unsere Systeme sind ausgefallen“)
- Hilflosigkeit andeuten („wir mussten“, „wir hoffen“)
- Schulduweisungen („wir wurden angegriffen und lahmgelegt“)
- Spekulationen („vermutlich, möglicherweise“)

Do's

- Aktiv formulieren („Wir haben entschieden...“)
- Proaktivität betonen („vorsorglich“, „bewusst“)
- Kontrolle signalisieren („unter definierten Prozessen“, „strukturiert“)
- Schutz betonen („zum Schutz unserer Kunden“)



Bereiten Sie sich vor: Ein klarer **Kommunikationsplan** ist entscheidend, um eine Cyber-Krise zu steuern – und Ihre Reputation steht dabei auf dem Spiel.

Cyber Crisis Management

23. September & 2. Oktober 2025

Zentrale Regeln für Kommunikation



- Berücksichtigen Sie alle beteiligten Stakeholder (intern wie extern)
- Halten Sie stetige Kommunikation mit allen Beteiligten aufrecht
- Verwenden Sie die richtige Sprache («Informationsinhalt») für jede Zielgruppe
- Planen Sie so viel wie möglich! – Sie haben noch keinen Plan? Dann entwickeln Sie welche!

Was Sie mitnehmen sollten



- Cyber-Krise = mehr als ein IT-Vorfall – betrifft ganze Organisation
- Die ersten Stunden sind kritisch – Klarheit, Geschwindigkeit, Kommunikation
- Haben wir ein benanntes Cyber Crisis Team mit Stellvertretern?
- Gibt es ein strukturiertes Playbook?
- Vorbereitung entscheidet – Szenarien, Übungen
- Sind Behördenkontakte & externe Partner vorbereitet?
- Zusammenarbeit mit Partnern – Behörden vorab klären

Cyber Crisis Management

23. September & 2. Oktober 2025

Wie geht es weiter?



„Viele Organisationen erkennen nach solchen Sessions, dass sie zwar wissen, **was** sie tun müssten – aber unsicher sind, **wie** sie es konkret umsetzen.“

Wir unterstützen mit:



Cyber Defense Center (CDC)

Sorgt dafür, dass Bedrohungen früh erkannt und behoben werden.



24/7 Monitoring & Erkennung



Schnelle Analyse und Reaktion



Risikominimierung & Sicherheitsverbesserung



Cyber Crisis Readiness

Fundament für handlungsfähige CCM-Teams im Krisenfall.



Cyber Readiness Workshop (Risiko & Kommunikationsanalyse)



CCM-Playbook und Walkthrough



Jährlicher Cyber Crisis Drill



Cyber Crisis Advisory

Flexible Krisenreaktion genau dann, wenn sie gebraucht wird.



Crisis Support und Coordinator (24/7 Reaktionsbereitschaft)



Beratend bei technischen Massnahmen und Executive-Entscheidungsunterstützung



Koordiniert zwischen IT, Management, Behörden und SOC

Fragen?



Cyber Crisis Management

23. September & 2. Oktober 2025



Danke

