

# Incident Response Krisenmanagement

Nürnberg Digital

HiSolutions AG

Lorenz Egender

A long cable-stayed bridge spans across a body of water under a dramatic, cloudy sky at sunset. The bridge features a prominent central pylon and a series of smaller piers. The sun is low on the horizon, casting a warm glow across the scene.

# Agenda

1. Cyberkrisen

2. Cyberkrisenmanagement



## Lorenz Egender Managing Consultant | Krisenmanager

- Experte für Krisenmanagement und Incident Management
- Unterstützung von Krisenstäben und IT-Leitungen
  - Aufbau von Krisenstäben und Bewältigung von Cyberkrisen
  - Einrichtung eines Notbetriebs
  - Etablierung der Krisenkommunikation
- Schwerpunkt außerhalb von Incident Response Einsätzen:  
Präventive Vorbereitung auf Schadensereignisse  
(BCM, Krisenmanagement und Krisenkommunikation)

# Zahlen, Daten und Fakten



Langjährige Erfahrung  
Seit 1992 aktiv



Kompetentes Personal  
ca. 280 Mitarbeiter



Fallaufkommen 2021  
Ca. 800



Incident Response Team  
30 Mitarbeiter



Unsere Standorte

# 1. Cyberkrisen



1 Woche •  
Nach Cyberangriff auf Xplain  
Datenschutzbeauftragter eröffnet #Untersuchung gegen #Fedpol

"Die Bundesämter für #Polizei und für #Zoll und #Grenzschutz sind Gegenstand einer Untersuchung des Schweizerischen #Datenschutz- und Öffentlichkeitsbeauftragten. Hintergrund ist unter anderem der Hackerangriff auf Xplain. Beim IT-Dienstleister sind Daten der beiden Behörden gespeichert."



Datenschutzbeauftragter eröffnet Untersuchung gegen Fedpol  
swissinfo.ch • Lesedauer: 1 Min.

"42 % der Führungskräfte oder ihre Familienmitglieder vom einem Cyberangriff betroffen waren, dessen Folgen so schwerwiegend waren wie e ... mehr anzeigen



42 % der Führungskräfte waren in den letzten 2 Jahren Opfer eines schweren Cyberangriffs  
it-daily.net • Lesedauer: 2 Min.

let Medi seine Kunden sich Alternativen zu suchen  
lesen gerät immer häufiger in das...  
... mehr anzeigen



Nach Cyberangriff bittet t  
Büro Zonen auf Unterstützung  
... mehr anzeigen

"Zeitungen erscheinen nach Hackerangriff als Notausgaben  
Die Rheinische Post Mediengruppe hat warben mit den Folgen eines Cyberangriffs zu kämpfen: Zeitungen erscheinen heute als Notausgaben. Nachts ... mehr anzeigen



Cyberangriff Rheinische Post Mediengruppe bringt Notausgaben heraus  
... mehr anzeigen

Russischer Hacker-Angriff  
... Lesedauer: 2 Min.  
Gefällt mir

Als Barmer-Versicherter künftig erhöhte Vorsicht bei Kontobewegungen  
"Barmer informiert Versicherte über Cyberangriff  
Bei einem Cyberangriff auf einen externen Dienstleister könnten Ki ... mehr anzeigen



Kundendaten von Barmer-Versicherten gestohlen - jetzt Bankrott  
... mehr anzeigen



Cyberangriff Smart-Healthtech Berlin  
... Lesedauer: 1 Min.



Ein Krankenhaus in US-Bundesstaat Illinois wird am Freitag dieser Woche schließen und gibt einen Ransomware-Angriff als einen der Gründe an. Durch die Attacke wurden die Computersysteme des Hospitals 2017 lahmgelegt. ... mehr anzeigen

US-Krankenhaus schließt, erkrankte wegen eines Ransomware-Angriffs  
... Lesedauer: 1 Min.

# Angriffsmotivation

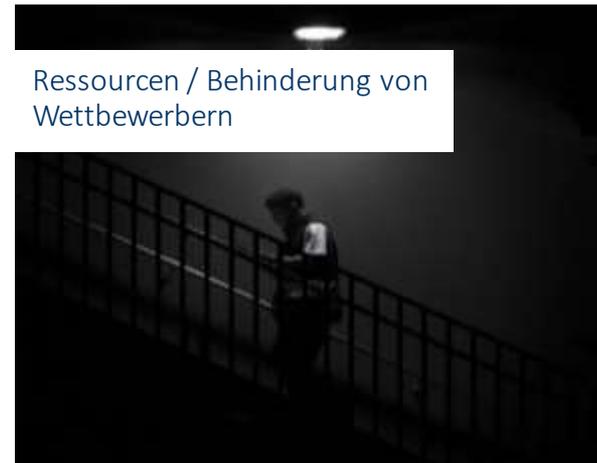
Erpressung – finanzielle Motivation



Spionage



Ressourcen / Behinderung von Wettbewerbern



Hacking aus Spaß und Neugier



Betrug – Onlinehandel oder CEO-Fraud



Frustration oder Rache – persönliche Motivation



## 2. Cyberkrisenmanagement

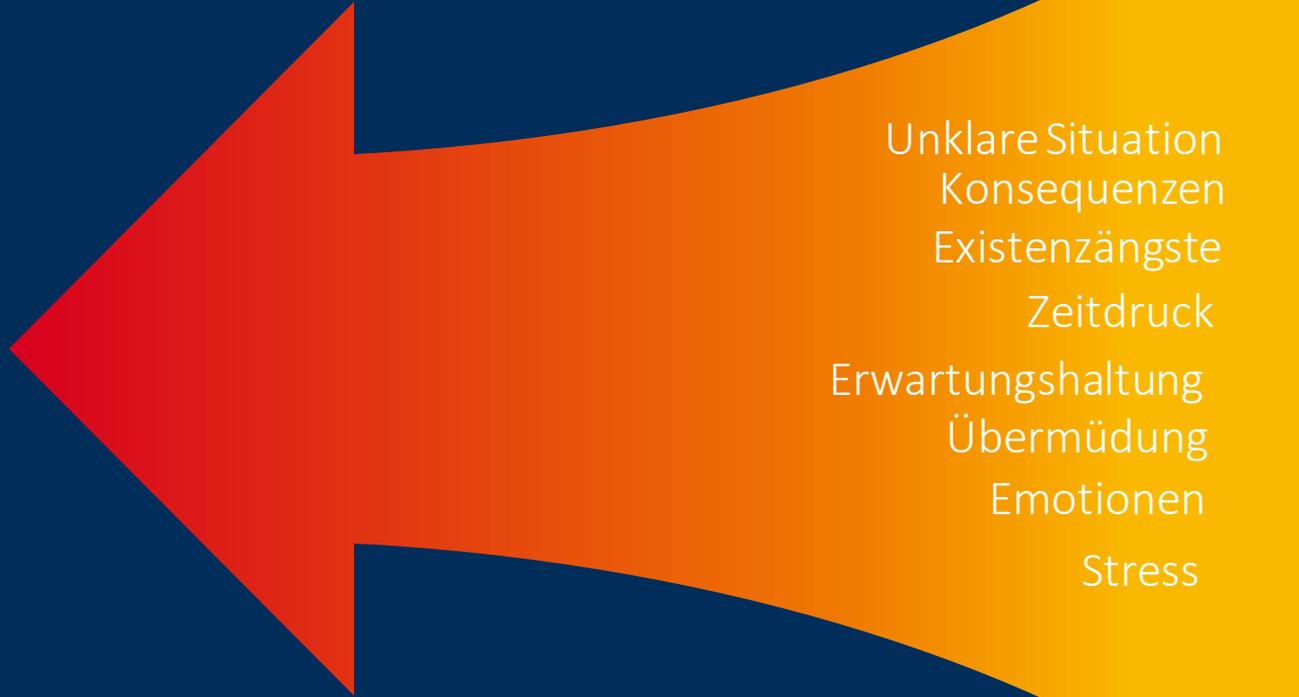
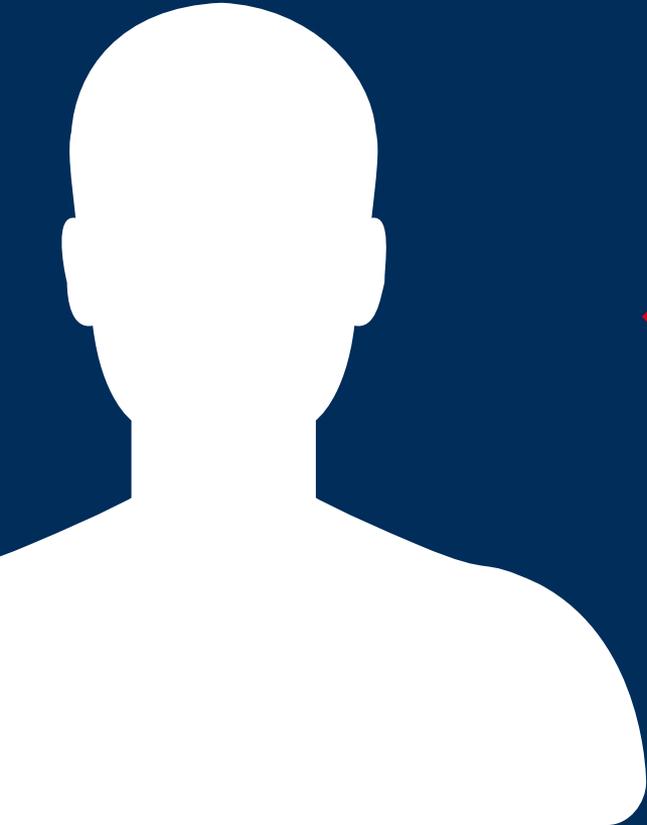


# Fachliche Herausforderungen eines Krisenmanagers

BCM  
KRITIS  
Krisenmanagement  
ISMS  
Datenschutz  
IT-NFM  
Forensik  
Kommunikation



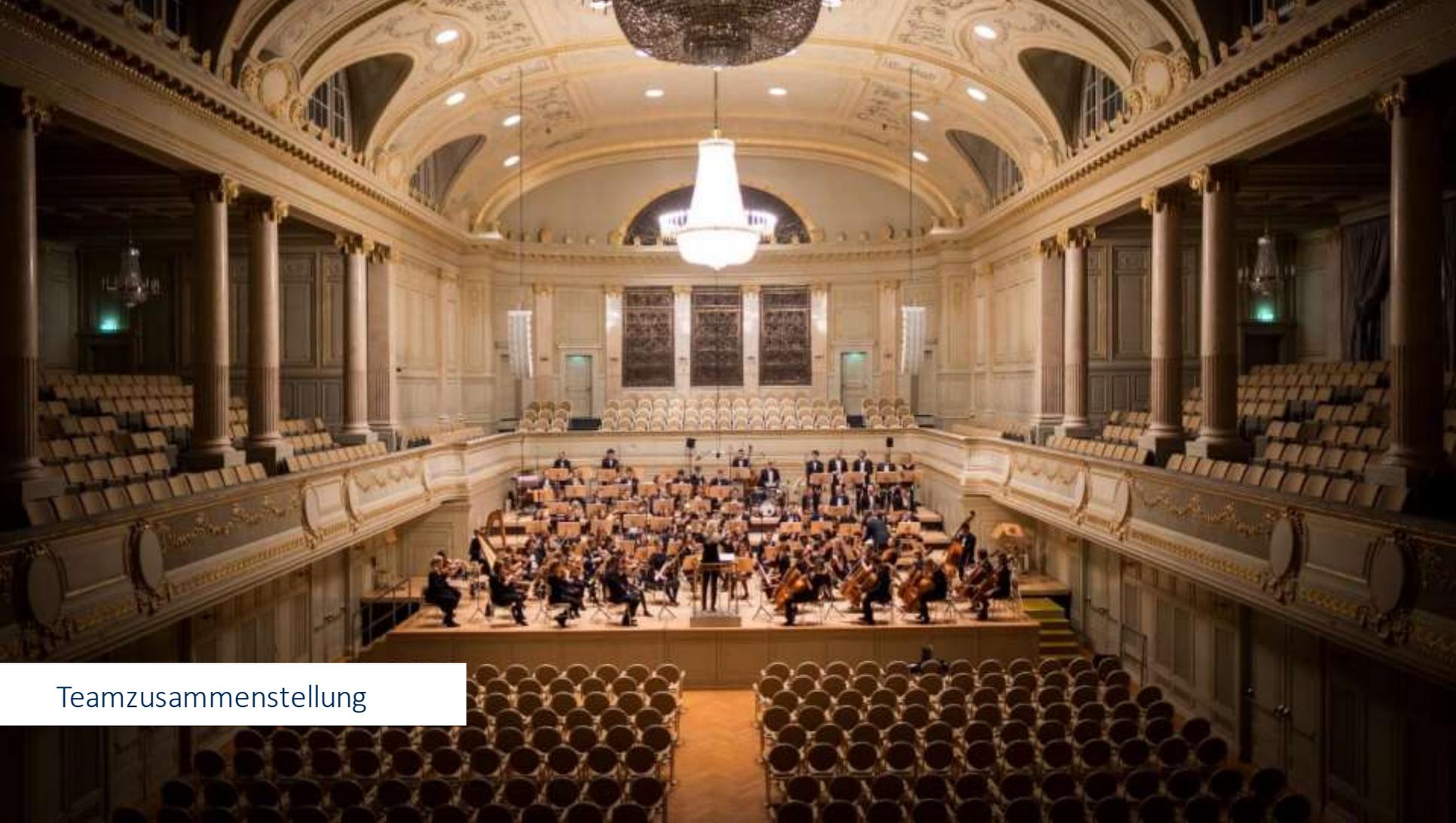
# Persönliche Herausforderungen eines Krisenmanagers



Unklare Situation  
Konsequenzen  
Existenzängste  
Zeitdruck  
Erwartungshaltung  
Übermüdung  
Emotionen  
Stress

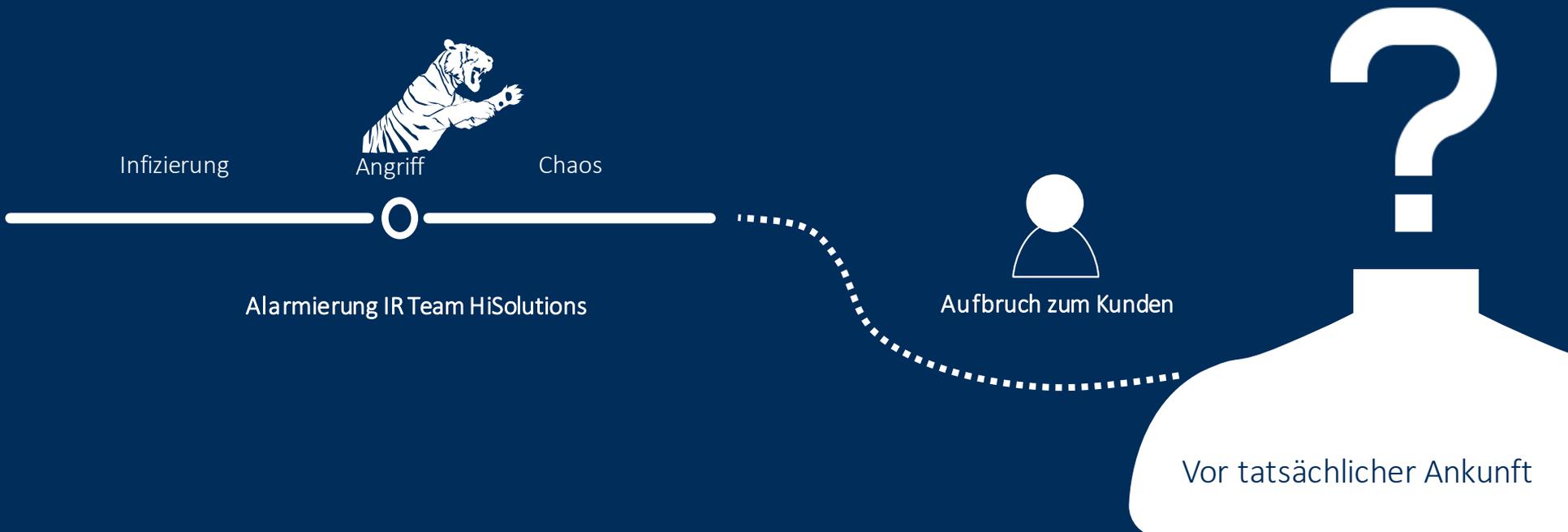


Anruf Hotline



Teamzusammenstellung

# Wissenstand nach Erstgespräch



# Phasen der Vorfallbewältigung



## Phase 0

Alarmierung IR Team HiSolutions

Phase 1 (Tage 1-2 beim Kunden)

Chaosphase & Soforthilfe

Phase 2 (Woche 1-2 beim Kunden)

Stabilisationsphase

Phase 3 (Woche 2+x beim Kunden)

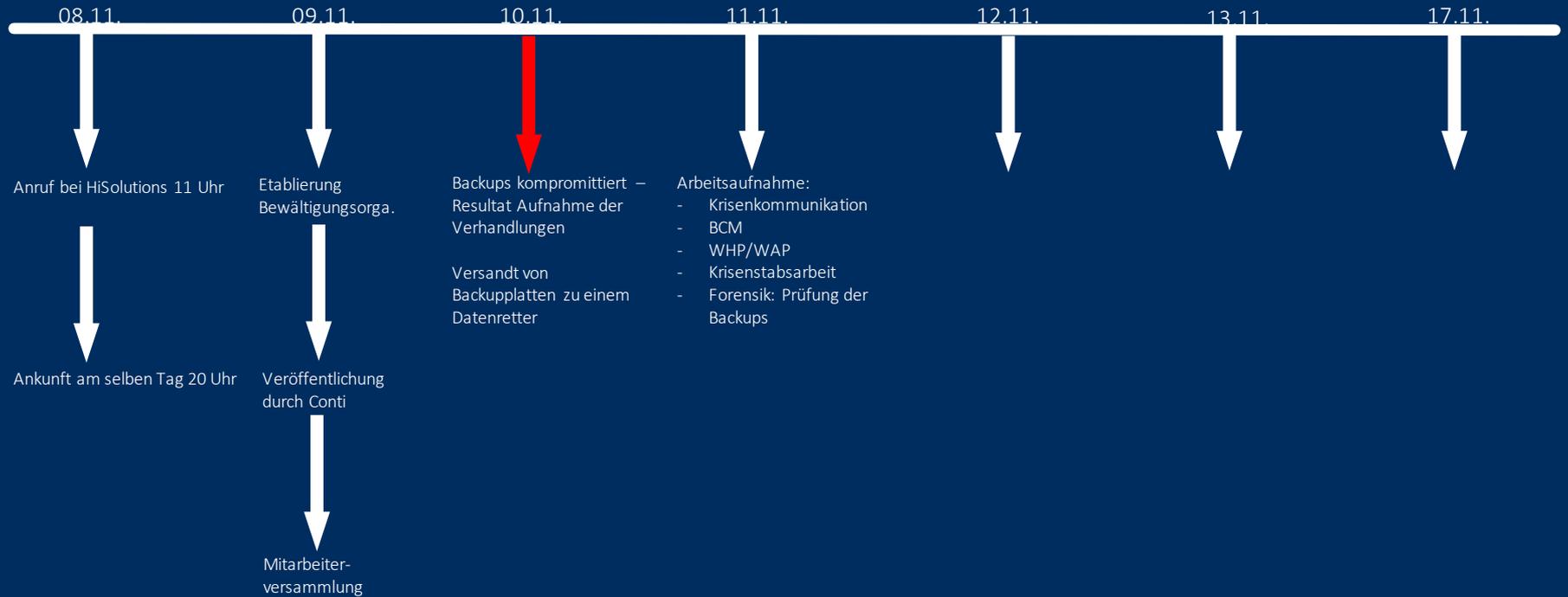
Notbetriebsphase

Phase 4

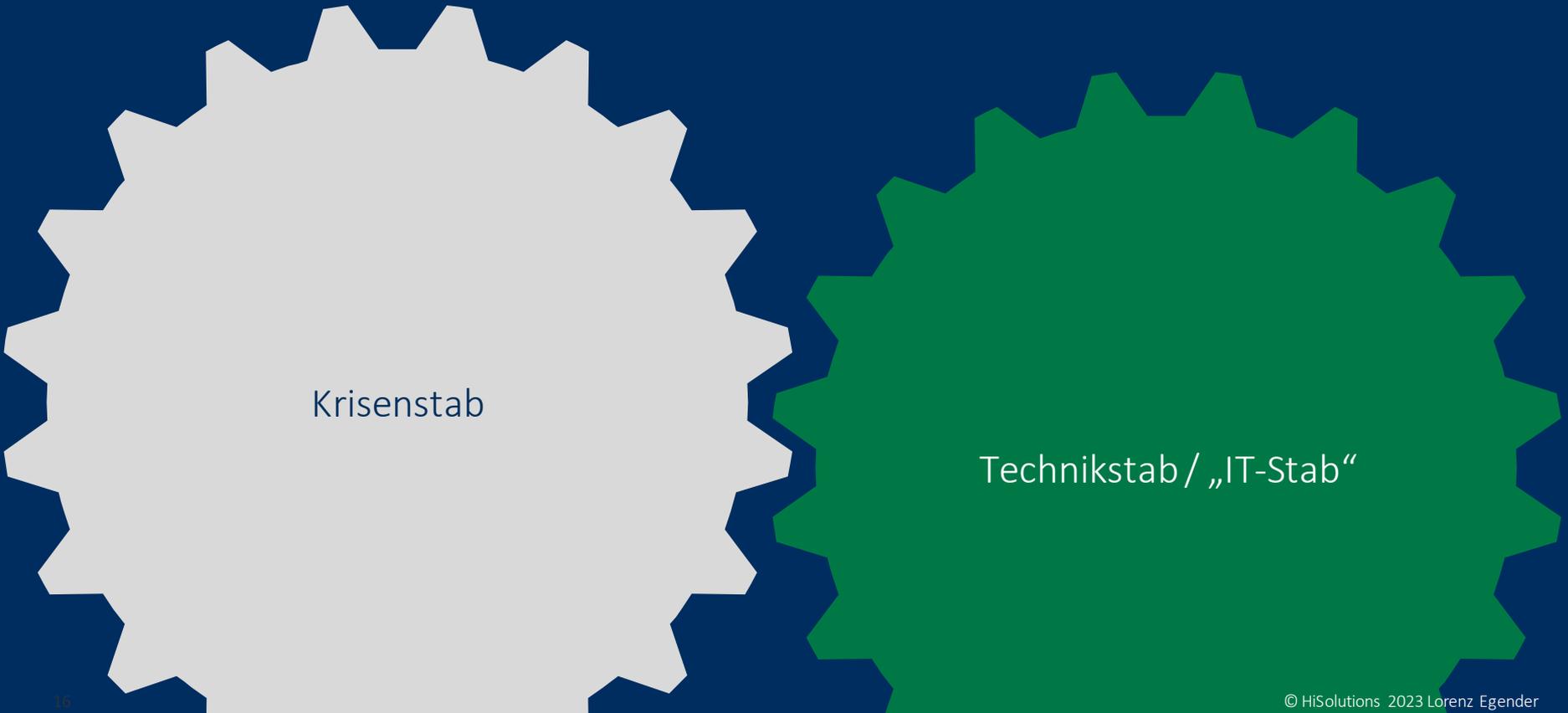
Nachbereitung



# Verlauf einer Schadensbewältigung



# Zweistabssystem

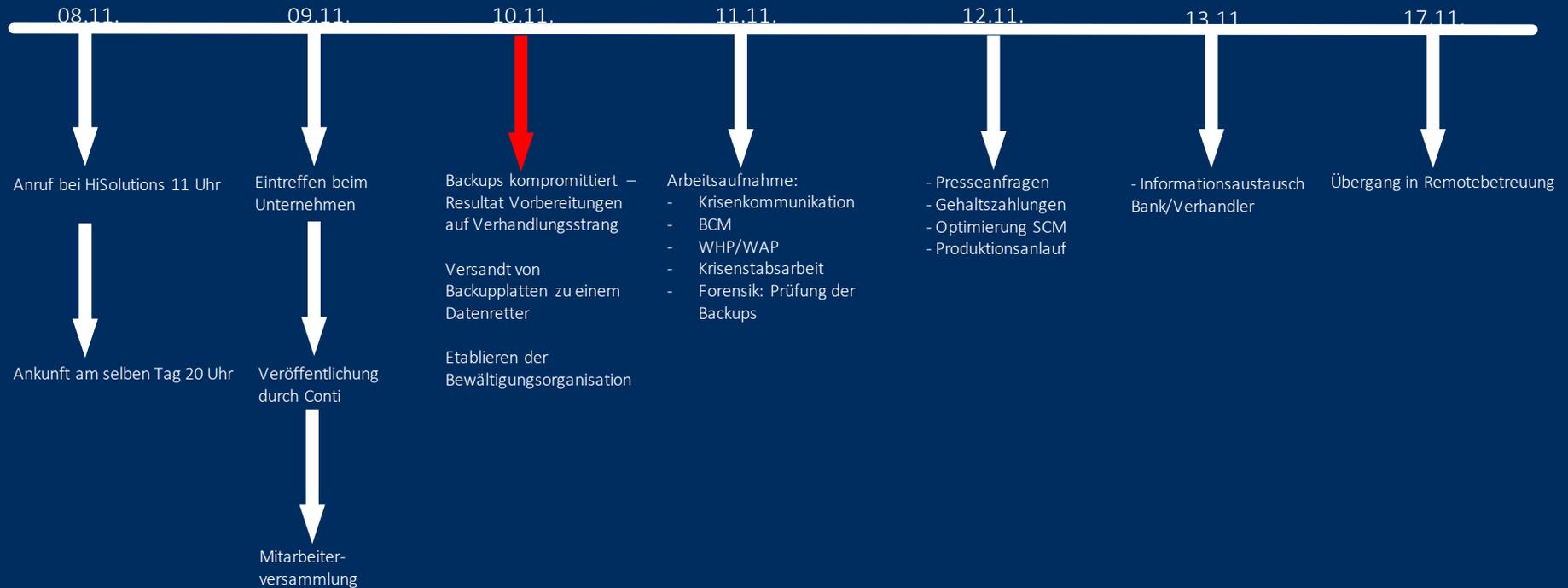


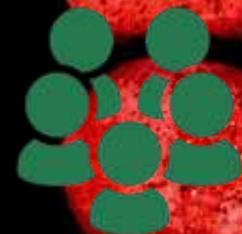
The diagram illustrates a two-staff system using two interlocking gears. The left gear is light gray and labeled 'Krisenstab'. The right gear is green and labeled 'Technikstab / „IT-Stab“'. The gears are positioned side-by-side, with their teeth meshing together, symbolizing the interaction and coordination between the crisis staff and the technical staff.

Krisenstab

Technikstab / „IT-Stab“

# Verlauf einer Schadensbewältigung





Irgendjemand hat immer einer zündende Idee

# After Action Review





Gemeinsam.



Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com