
# VORSTELLUNG

RapidResponse

Uwe Grams und Vincent Rockenfeld

# INCIDENT-RESPONSE-EXPERTEN

**Uwe Grams**

- Krisenmanagement Spezialist mit > 12 Jahren Berufserfahrung in den Bereichen Krisenmanagement, Krisenkommunikation, Incident-Response (Projektleiter in >20 Fällen vor Ort),
- Schwerpunkt Krisenstabsaufbau, und Planung und Durchführung von Krisenstabsübungen, Notfallplanung und Business Continuity Management
- Co-Autor BSI Standard 200-4 Business Continuity Management

**Vincent Rockenfeld**

- IT-Security Spezialist mit > 7 Jahren Berufserfahrung in den Bereichen IT-Forensik (Schwerpunkt Großschadenslagen, Threathunting und Aufklärung staatlicher Angreifer/APT, Malware-Analyse) Incident-Response (Einsatzleitung in über 30 Fällen vor Ort)
- Wiederanlaufplanung, Unterstützung bei der Kommunikation mit Sicherheitsbehörden, Präventive Analyse von IT-Umgebungen zur Aufdeckung bestehender Cyberrisiken und Schwachstellen, Pentesting & Red-Teaming im KRITIS-Bereich und industrieller Kontrollsysteme.

RapidResponse

4 = sehr groß
3 = groß
2 = mittel
1 = klein

# REFERENZEN*

Landkreis Rechenzentrum
2x Großrechenzentrum
IT-Dienstleister
Versicherung
Versicherung
Versicherung
Arztpraxenverband
Uniklinikum
Arztpraxenverband
Uniklinikum
Information und Telekommunikation
Finanzen und Versicherungen
Gesundheits-wesen
Hotelkette
Handel
Webdesign
Großkanzlei
Dienstleistungen & Handel
Energie- und Wasserwirtschaft
Energieversorger
Hotelkette
Handel
Handel
Hotelkette
Online-Dienstleistung
Öffentliche Verwaltung
Reg.Partei
Produktion und Industrie
Stadtwerk
Stadtwerk
Produktionsunternehmen
Hochschule
Abfallverband
Rüstungsunternehmen
Forschungseinrichtung
2x Rüstungsunternehmen
5x Produktionsunternehmen
Öffentliche Verwaltung
Hochschule
3x Produktionsunternehmen

*begleitete Projekte beim alten Arbeitgeber HiSolutions AG

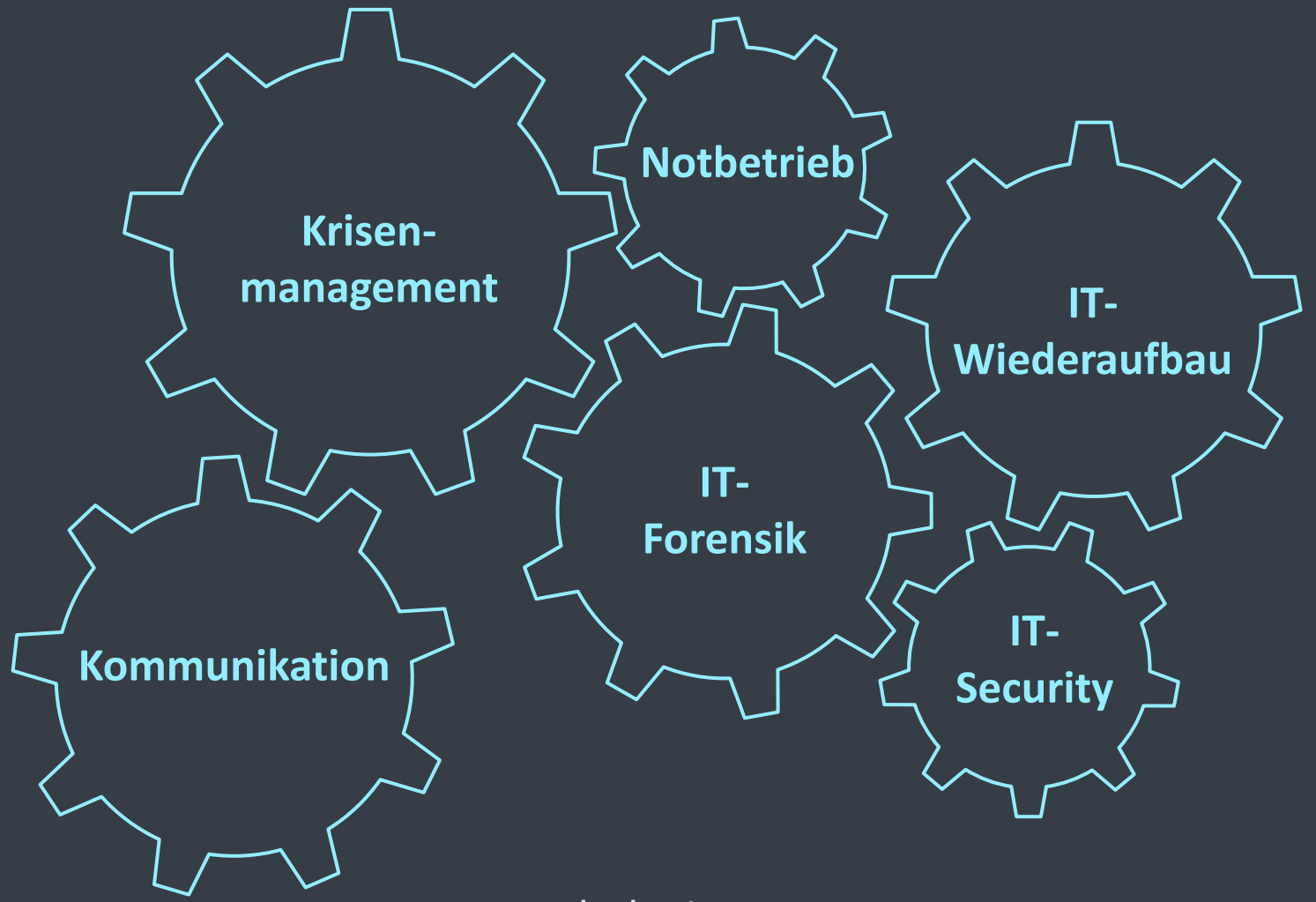
RapidResponse

# WAS MACHT EINE GUTE INCIDENT RESPONSE AUS?

Verhandlung

Datenschutz

Versicherungs-
kommunikation




DL-Steuerung

Lösegeldzahlung

Behörden-
kommunikation

Psychologie

RapidResponse

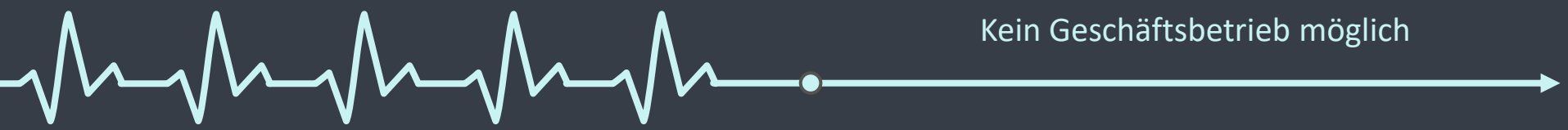
# VERSCHLÜSSELUNG LEGT BETRIEB LAHM


RapidResponse

# MAKROBETRACHTUNG

Normales Tagesgeschäft

Kein Geschäftsbetrieb möglich



Lieferanten

Eigenes UN

Kunden

Partner-UN

RapidResponse

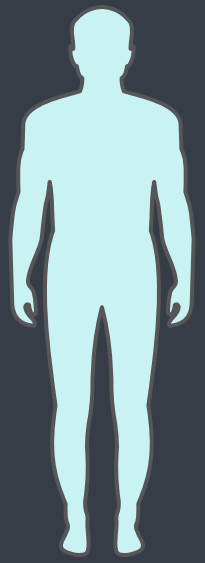
# MIKROBETRACHTUNG: FAKTOR MENSCH

Normales Tagesgeschäft

Kein Geschäftsbetrieb möglich

Angst

Unsicherheit



Stresswahrnehmung

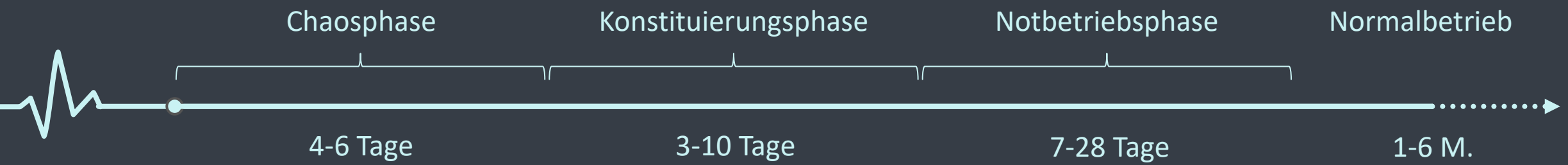
Kampf

Starre

Flucht

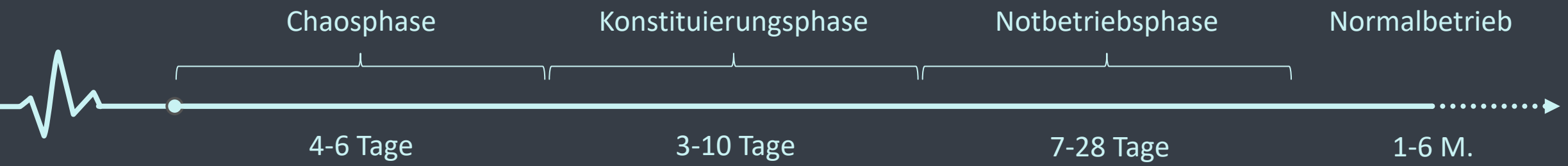
RapidResponse

# PHASEN DER BEWÄLTIGUNG



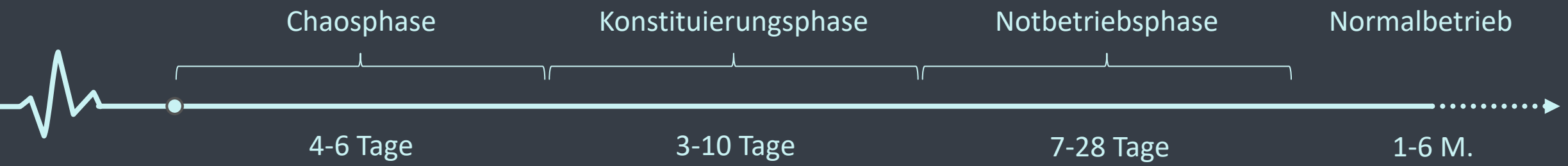

RapidResponse

# PHASEN DER BEWÄLTIGUNG: KRISENMANAGEMENT



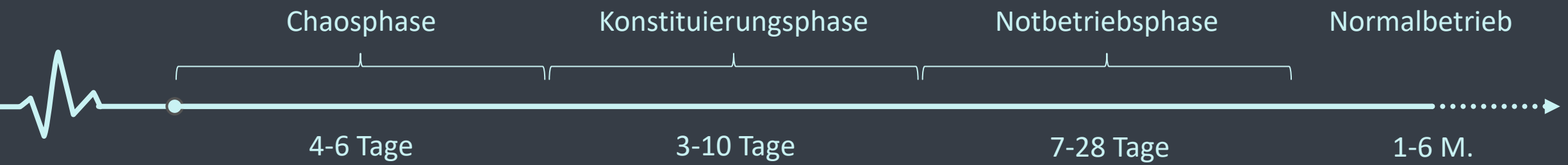

RapidResponse

# PHASEN DER BEWÄLTIGUNG: KRISENKOMMUNIKATION




RapidResponse

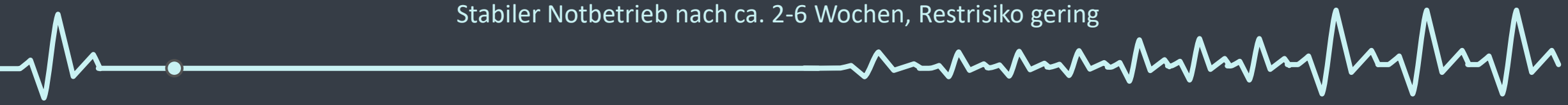
# PHASEN DER BEWÄLTIGUNG: IT-FORENSIK




RapidResponse

# EXKURS:
# IST ZAHLUNG DES LÖSEGELDS EINE ALTERNATIVE?

Stabiler Notbetrieb nach ca. 2-6 Wochen, Restrisiko gering



Entschlüsselung der Daten ca. 1,5 – 2,5 Wochen, Restrisiko hoch

- Lagesondierung
- DL-Beauftragung & Risikoabwägung der Lösegeldverhandlung
- Verhandlung mit Erpresser inkl. Test des Key / Abstimmung Versicherung
- Datensicherung erstellen
- Zahlungsabwicklung
- Key testen / analysieren
- Entschlüsselung der Daten

RapidResponse

# FRAGEN?


Uwe Grams
RapidResponse
CoFounder | Krisenmanager

grams@rapid-response.eu

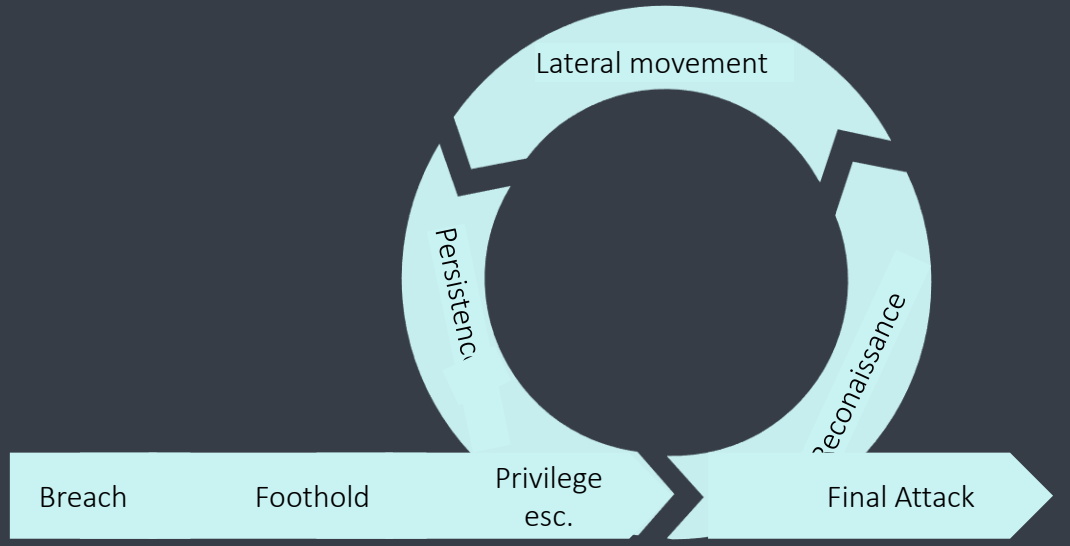
Vincent Rockenfeld
RapidResponse
CoFounder | IT-Forensiker

rockenfeld@rapid-response.eu

# BEISPIELABLAUF: RANSOMWAREVORFALL

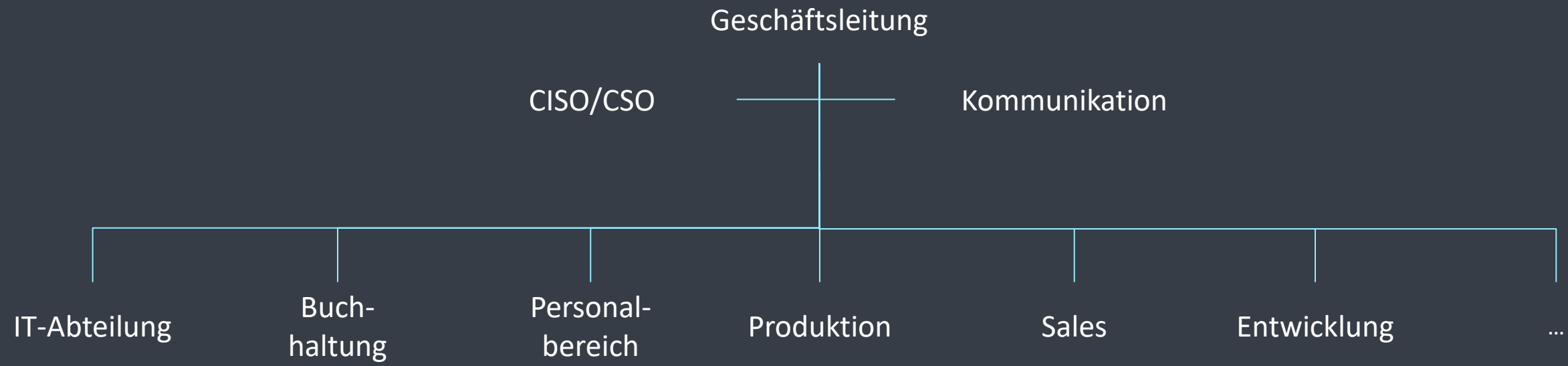
Normales Tagesgeschäft

- Ausnutzung der Schwachstelle
- Erlangung weitgehender Rechte
- Installation von Backdoors in eigenen und Fremdsystemen
- Deaktivieren Sicherheitsmechanismen
- Analysieren den Kunden
- Exfiltrieren Daten
- Löschen Backups
- Rollout des Verschlüsselungstrojaners




RapidResponse

# MIKROBETRACHTUNG: UNTERNEHMEN


RapidResponse

# EXKURS: GUTES INCIDENT RESPONSE IN DER REALITÄT

## BEISPIEL: PRODUKTIONSUNTERNEHMEN, 200 MITARBEITER, RANSOMWARE

| | Ideales Krisenmanagement | | Fehlerhaftes Krisenmanagement | |
|---|---|---|---|---|
| Phasen der Bewältigung | 4 Wo. | - | 10 Wo. | - |
| BU - Schäden | 1 Wo. | 150.000€ | 4 Wo. | 600.000€ |
| Dienstleisterkosten | - | 300.000€ | 1-2 Wo. | 400.000€ |
| Krisenmanagement & Kommunikation | | 80.000€ | | 35.000€ |
| IT-Forensik | | 120.000€ | | 75.000€ |
| IT-DL / Systemhaus | | 90.000€ | | 240.000€ |
| Juristische Beratung (DS, etc.) | | 10.000€ | | 50.000€ |
| Hard- und Softwarebeschaffung | - | 50.000€ | 1 Wo. | 100.000€ |
| Ergebnis | 4 Wo. | 500.000€ | 10 Wo. | 1.100.000€ |

RapidResponse

# SCHÄFER TRENNWANDSYSTEME GMBH (ÖFFENTLICH)

30.01.2020 – 23.04.2020

## Kurzbeschreibung Kunde

Die Schäfer Trennwandsysteme GmbH (Schäfer TWS) ist ein familiengeführter Produzent von Systemen für Umkleide- und Sanitäranlagen.

## Was war passiert?

Die gesamte IT-Infrastruktur (Server) wurde durch den PYSA-Verschlüsselungstrojaner unter Domain-administrativen Rechten verschlüsselt. Sämtliche Betriebsabläufe, einschließlich des vollautomatisierten Herstellungsprozesses waren schwer betroffen, nach wenigen Tagen war die Endmontage nicht mehr möglich.

RapidResponse

# SCHÄFER TRENNWANDSYSTEME GMBH (ÖFFENTLICH)

30.01.2020 – 23.04.2020

Die Erpresser forderten Lösegeld in BTC.

Die manuelle Produktion musste nach und nach eingeführt werden.

Was stand auf dem Spiel?
Existenz des Unternehmens.

Besonderheiten:

Vor allem durch das vollautomatische Plattenlager war die Produktion sehr IT-gebunden.

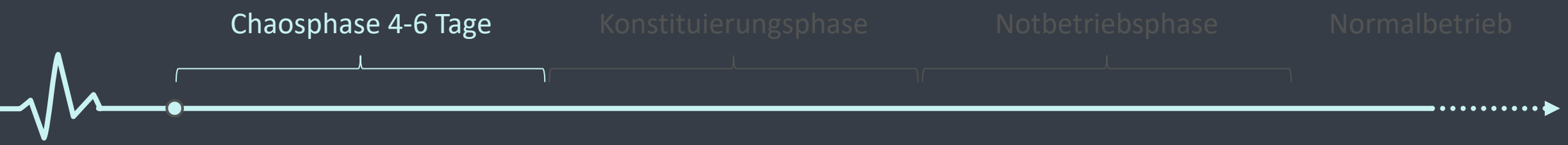
RapidResponse

# SCHÄFER TRENNWANDSYSTEME GMBH (ÖFFENTLICH)

https://www.youtube.com/watch?v=nJsWKezW6UE

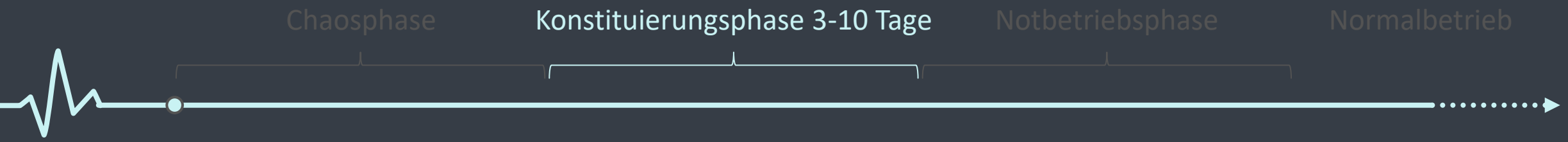
RapidResponse

# PHASEN DER BEWÄLTIGUNG: CHAOSPHASE



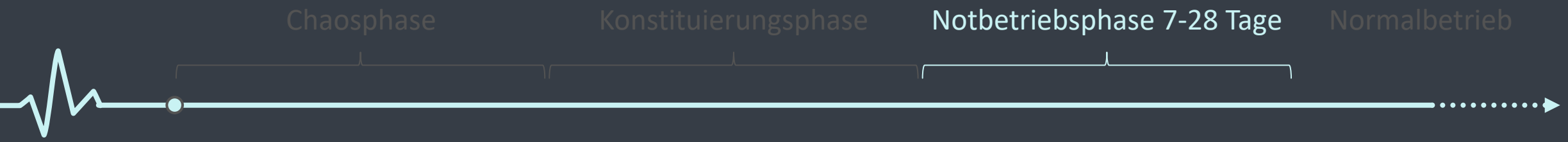

- Paralyse, Fassungslosigkeit, Lähmung, Verdrängung (Tag 1-2)
- Kommunikation als nachrangig betrachtet (Tag 1-2), ab Tag 3 eher adhoc (ggf. unüberlegt, intransparent und widersprüchlich)
- Backupsituation häufig ungenügend
- Fokussierung auf das wesentliche fällt schwer (was ist wirklich zeitkritisch?)
- Belegschaft hoch motiviert - Ressource Mensch wird jedoch außer Acht
- Erwartungen an IT-Forensik sind i.d.R zu hoch
- Fehlende Struktur führt zum Chaos (sinuskurvenartige Chaosphase)

# PHASEN DER BEWÄLTIGUNG: KONSTITUIERUNGSPHASE



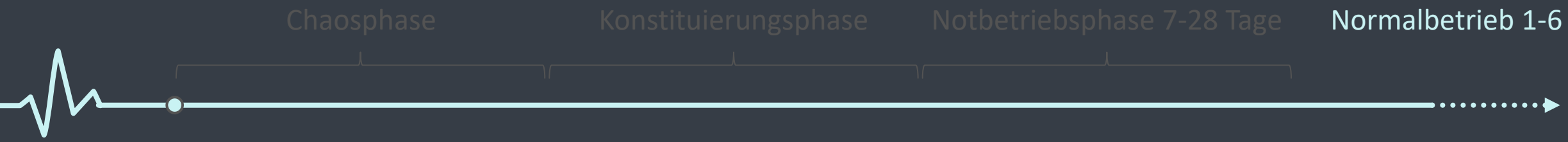

- Neuer Regelbetrieb setzt ein
- IT-Forensik liefert zunehmend weitere Ergebnisse
- Zeitkritische Prozesse nehmen zu
- Ermüdungserscheinungen nehmen zu
- Interessenskonflikte zwischen internen Parteien nehmen zu
- Notbetriebsprozesse werden initial aufgebaut

# PHASEN DER BEWÄLTIGUNG: NOTBETRIEBSPHASE




- Weitere Prozesse werden zeitkritisch, benötigen Notbetrieb
- Geduld von Partnern und Kunden nimmt ab
- Feinarbeiten und Details werden sichtbar
- Motivation abhängig von Erfolgen und vom Führungsstil
- Wiederaufbau der IT-Landschaft wird initiiert

# PHASEN DER BEWÄLTIGUNG: RÜCKF. NORMALBETRIEB




- Kleinarbeiten dauern i. d. R. mehrere Monate
- Daten aus den Notprozessen werden sukzessive zurückgeführt
- Fallabwicklung mit Partnern und Versicherung
- Hohe Lernkurve/Awareness über die eigene (IT-)Sicherheit und das Krisenmanagement

RapidResponse