



Gemeinsame Krisenstabsübung

Aveniq & enersuisse

Ransomware-Angriff: «Multi Extortion»

Ihre heutigen Referenten

Wer wir sind und was Sie heute erwartet



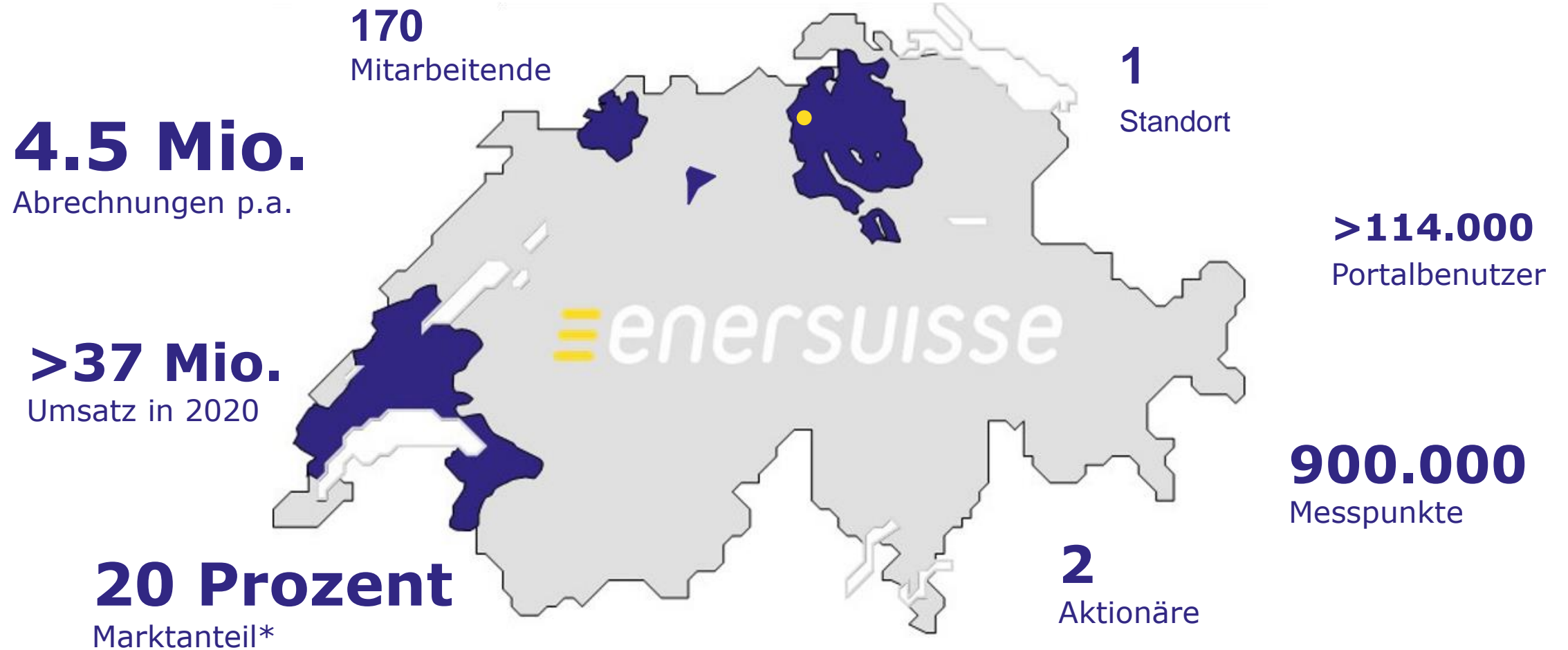
Alice Drifte
Professional Strategic Consultant
Aveniq



Gerhard Höchle
CIO
enersuisse

Ausgangslage

enersuisse – der führende Dienstleistungsanbieter im Schweizer Energiemarkt



Unser Leistungsportfolio

Modulprodukte

Plattformprodukte

Beratung

Publikationen zu einzelnen Produkten und Serviceleistungen siehe auch:

- [LinkedIn](#)
- [enersuisse.ch](#)



Inkasso



Output Management



Retourenbearbeitung



Billing



Chatbot



Abrechnung Wärme und ZEV



Kundenkommunikation im Kontext der Ostral-Vorgaben



Eichstelle



Multi Energy Billing



Kundendienst



Online Services



M2D Meter-to-Data



D2C Data-to-Customer



Methoden HCD & Lean



HCD User Research

Messwesen

Ablesung

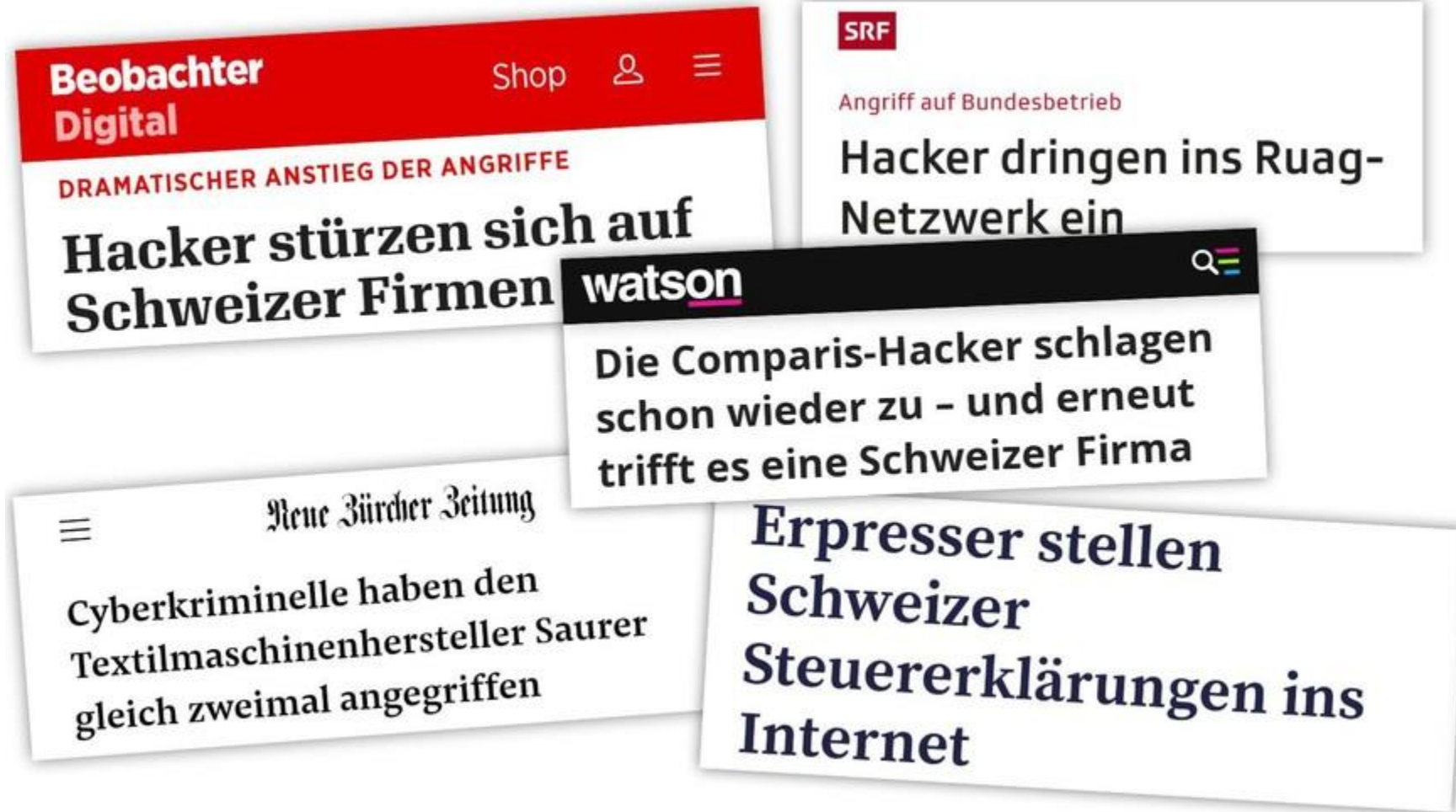
Abrechnung

Druck / Versand

Kundendienst

Ausgangslage

Zunehmende Cyber-Bedrohungen in der Schweiz



Ausgangslage

Zunehmende Cyber-Bedrohungen in der Schweiz

Meldungen an das NCSC im zweiten Halbjahr 2023 (pro Woche)

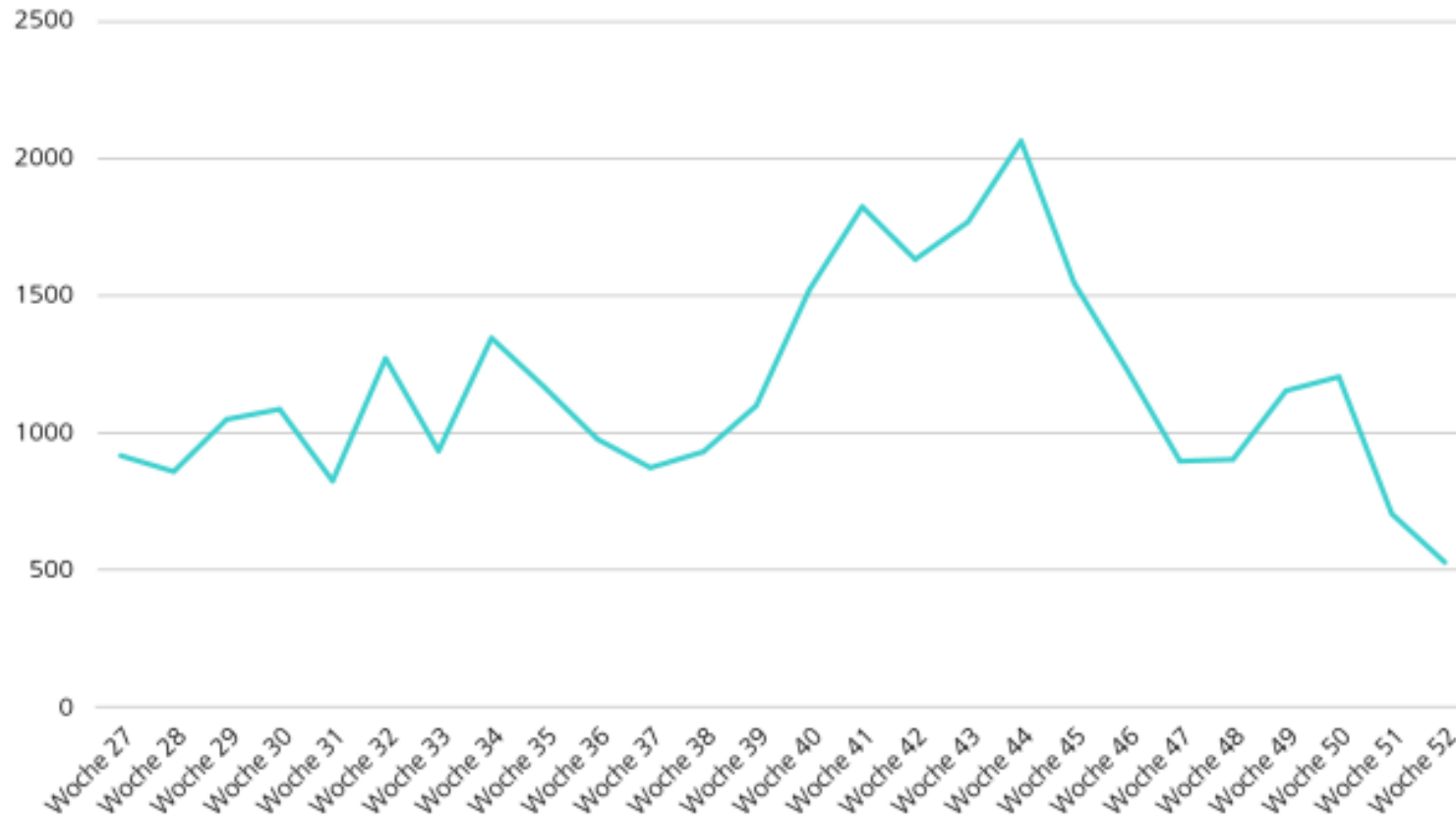


Abb. 1: Anzahl Meldungen pro Woche beim NCSC vom Juli bis Dezember 2023, siehe auch [Aktuelle Zahlen \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/aktuelle-zahlen).

Ausgangslage

Energiesektor



- NIS-Richtlinie umgesetzt**
- Bindende Cyber-Sicherheitsanforderungen für Stromsektor**
- Rechtliche Grundlagen für Umsetzung der NIS-Richtlinie geschaffen, aber noch nicht ausgearbeitet**
- Keine umfassenden und/oder verbindlichen Cyber-Sicherheitsrichtlinien für Stromsektor**



Aktuell gelten das Subsidiaritätsprinzip, Eigenverantwortung und rechtlich unverbindliche Empfehlungen (VSE-Grundsatz, IKS-Minimalstandard)

VERSCHLÜSSELUNG

Die Dateien, auf die Sie zugreifen wollen, sind durch unsere RANSOMWARE verschlüsselt.
Niemand kann die Dateien entschlüsseln, ohne unseren Entschlüsseler.
Ausserdem haben wir Ihre Daten gestohlen.

Deadline: 29.11.2023, 11:00 AM (CET)

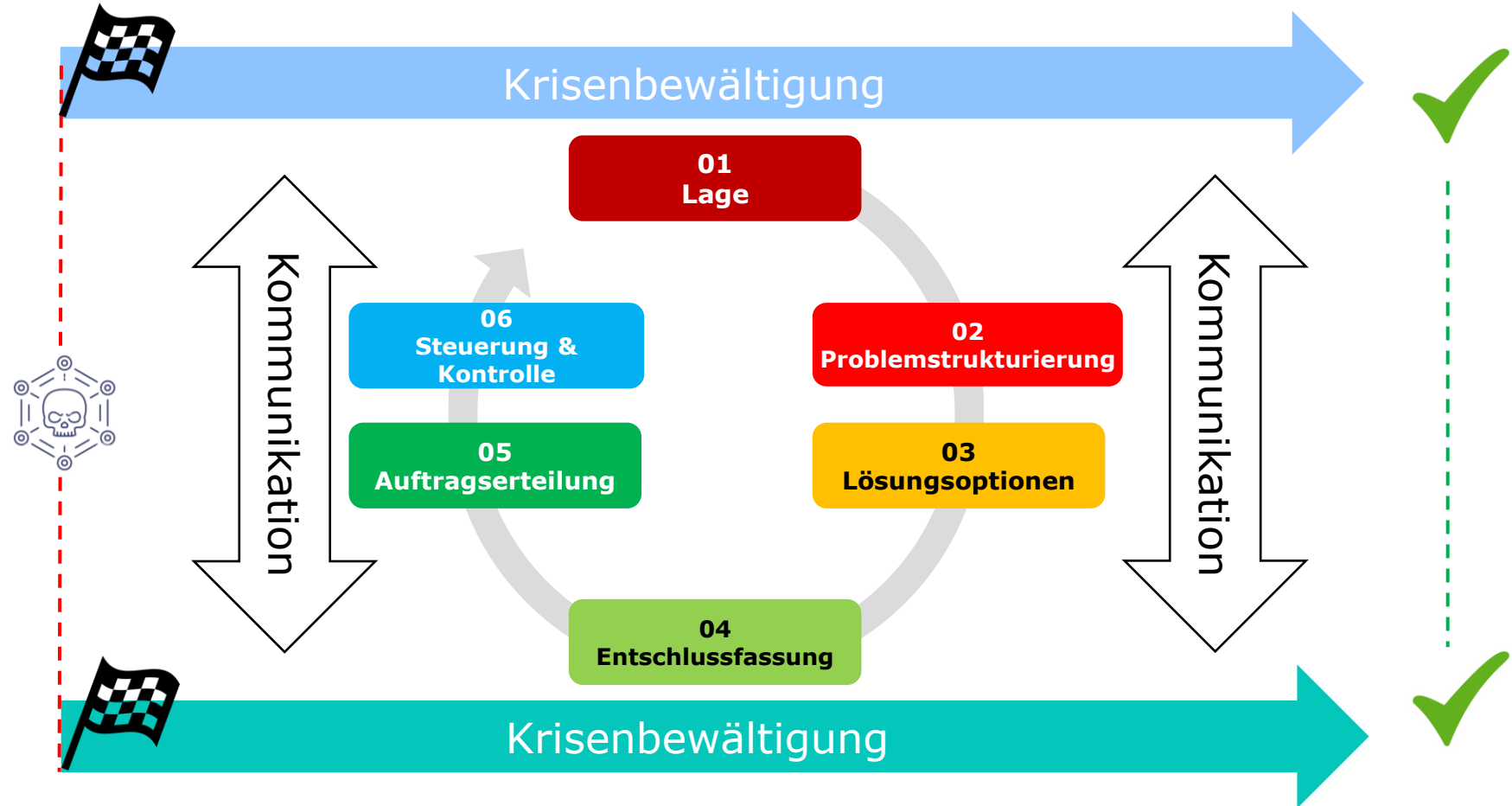
Lösegeld: 30.000.000 CHF

Sie haben bis zum Ende der Deadline Zeit, um das Lösegeld in Form der Crypto-Währung
MONERO auf das unten angegebene Wallet zu zahlen. Keine Sorge, nach dem
Zahlungseingang erhalten Sie den Entschlüsseler und können Ihre Daten wieder nutzen.
Wenn Sie nicht zahlen, bleibt die Verschlüsselung bestehen und wir werden Ihre sensiblen
Daten im Dark Web veröffentlichen.

Wallet-Adresse: 999tNkZrDNChErekiMxAPU4TRpe9Df99EPAukDyL4NcAniPbh2iQ1YDRk4LUXe1DaiKcQdhuMVrNf59nQlhxagDeyus9L

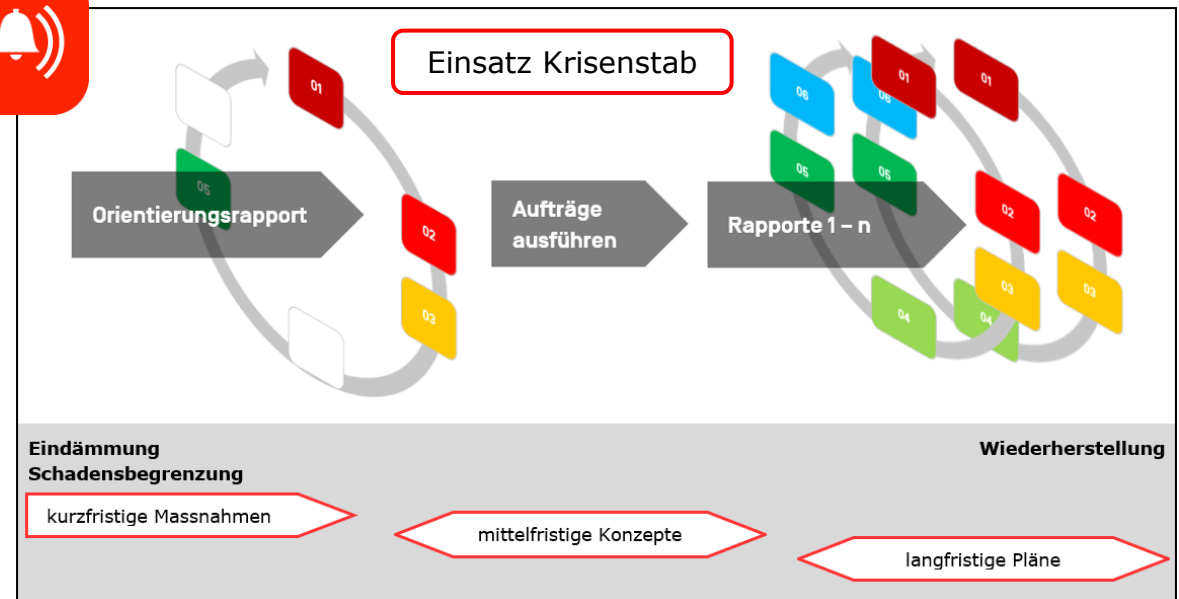
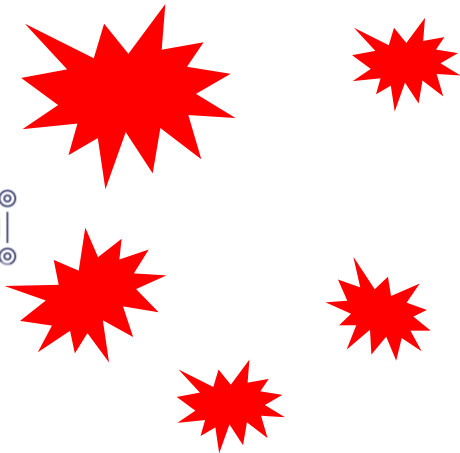
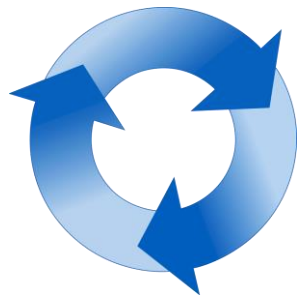
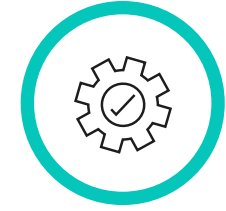
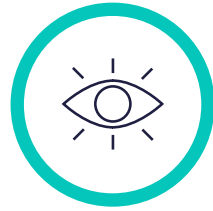
Ausgangslage

Ziele der Übung



Übungsvorbereitung

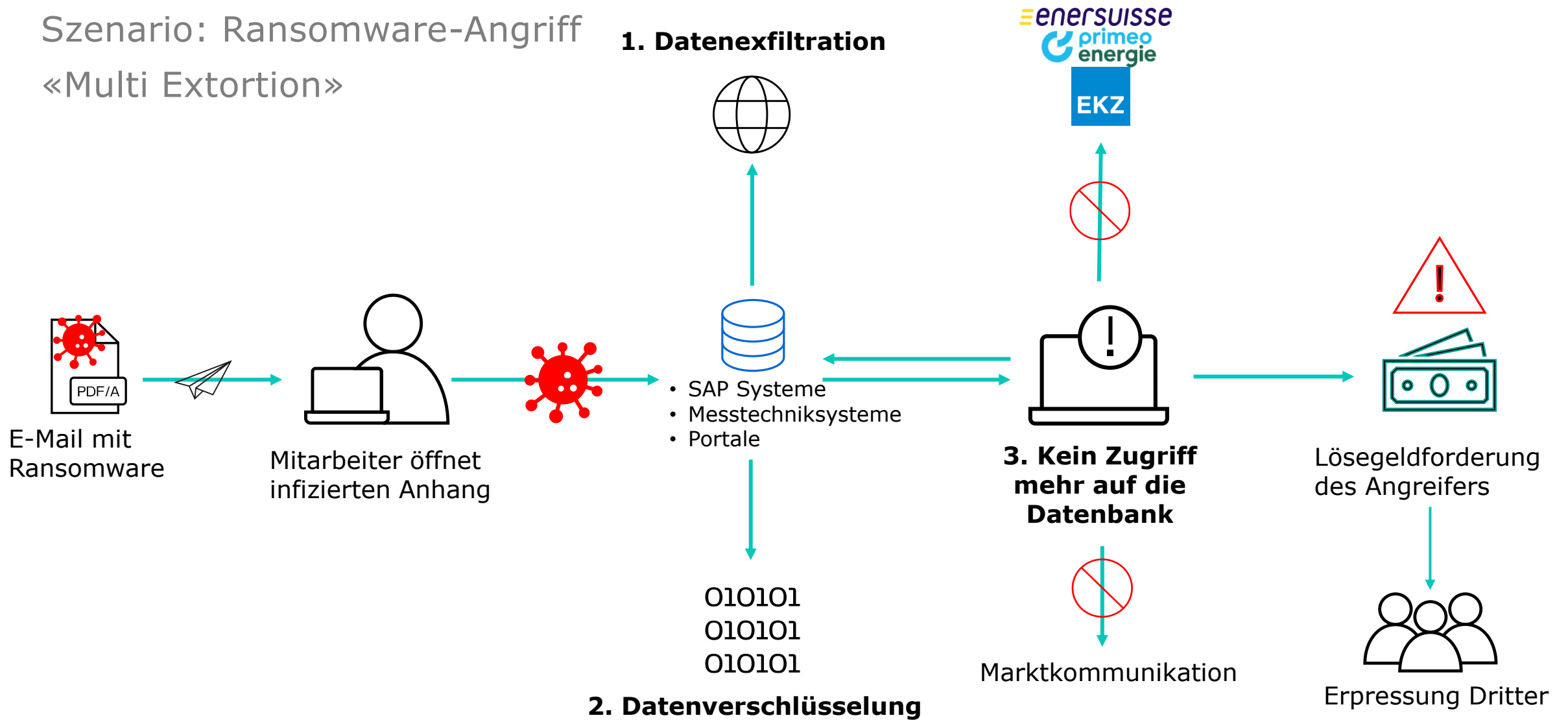
Implementierung eines Basis-Krisenmanagementsystems für enersuisse



Übungsvorbereitung

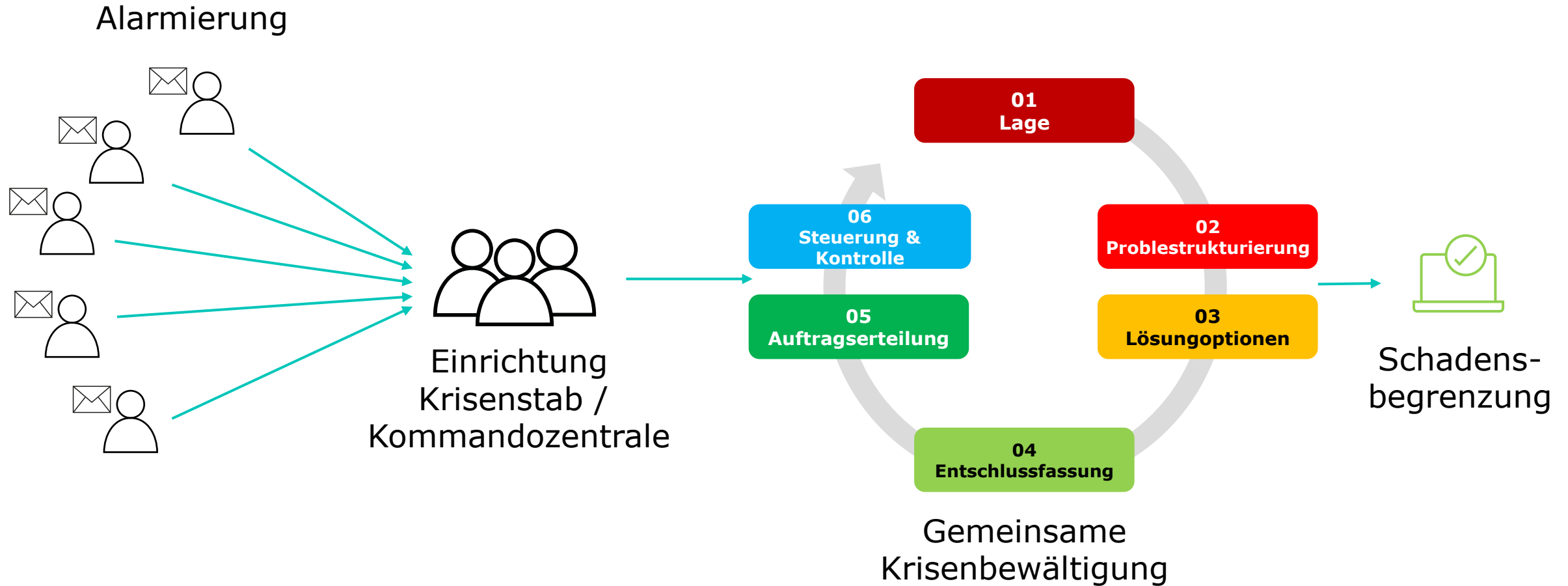
Szenario: Ransomware-Angriff

«Multi Extortion»



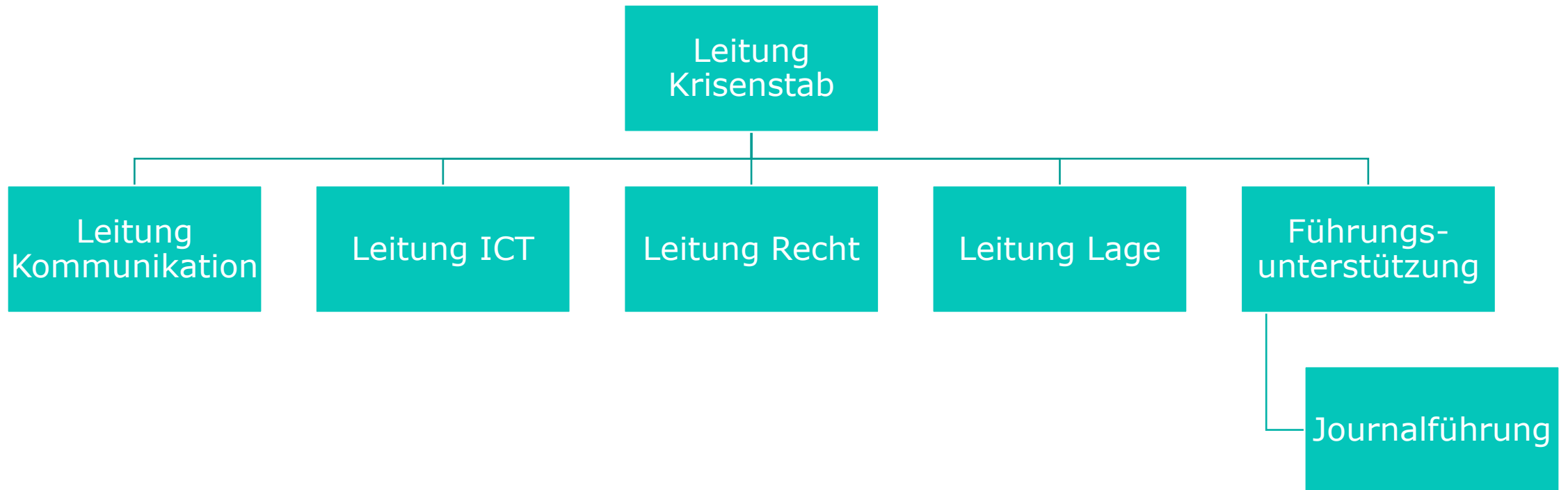
Übungsdurchführung

Von der Alarmierung zum Krisenstab



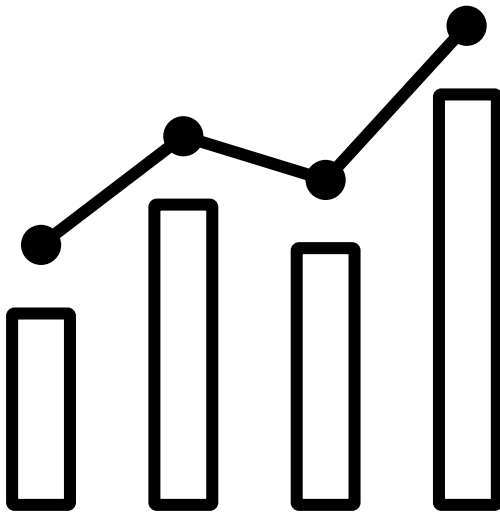
Übungsdurchführung

Rollen des Krisenstabs (enersuisse)



Lessons learned

Verbesserungspotenzial



Schnellere Synchronisation der beiden Krisenstäbe

Insbesondere am Anfang kann die Kommunikation proaktiver erfolgen, um eine gezielte Koordination gemeinsamer Massnahmen zu gewährleisten.

Problem- und Massnahmenstrukturierung

Prioritäre Problemfelder sollten besser erkannt und behandelt werden, um wichtige Massnahmen nicht zweitrangig zu behandeln. (Beispiel: Bedrohung CEO)

Rollenbesetzung und Fachwissen

Die Besetzung von Schlüsselrollen, wie die Leitung Recht und die Leitung Kommunikation, sollte mit Fachkräften erfolgen, um eine fundierte Unterstützung und Beratung zu gewährleisten.

Lagedarstellung

Die Hilfsmittel zur Lagedarstellung sollten optimiert werden, um ein übersichtliches Lagebild zu gewährleisten.

Weiteres Vorgehen

Kontinuierlicher Verbesserungsprozess



Feedback

Nach der Übung wurden die Teilnehmer*innen und Beobachter*innen befragt. Wie ist es den Teilnehmenden ergangen? Welche Herausforderungen gab es?



Krisenstab muss leben

Ein Krisenstab muss aktiv und dynamisch arbeiten. Er sollte ständig bereit sein, auf neue Entwicklungen zu reagieren und flexibel zu handeln.

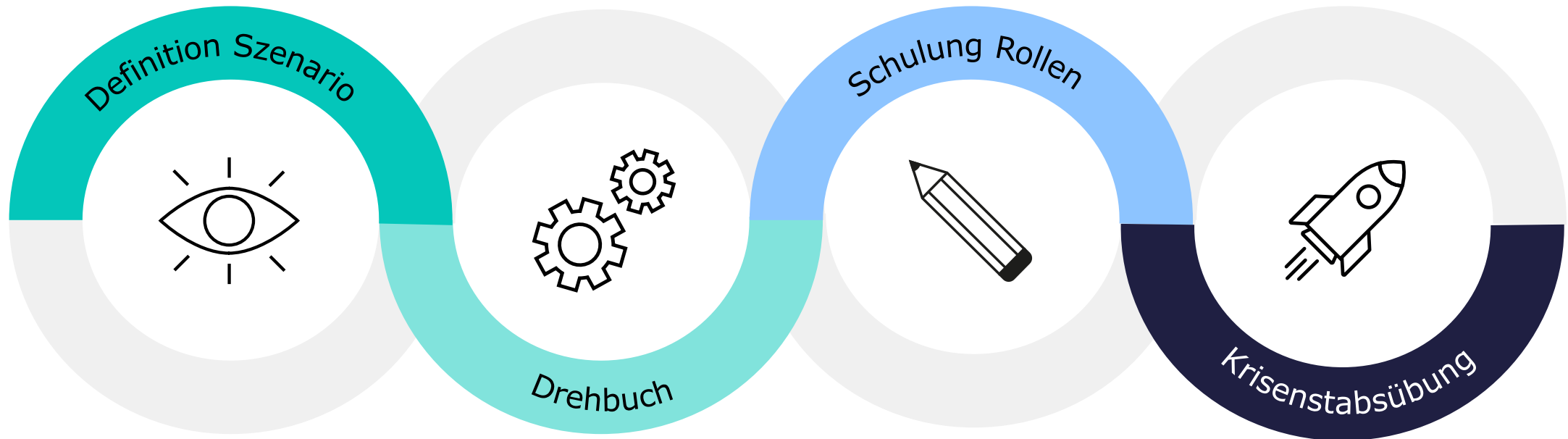


Regelmässige Übungen

Durch regelmässige Übungen können die Mitglieder des Krisenstabs ihre Rollen und Verantwortlichkeiten besser verstehen und ihre Fähigkeiten verbessern.

Weiteres Vorgehen

Krisenstabsübung 2024



AVENIQ

Haben Sie Feedback für uns?

Herzlichen Dank

