Notfall- und Krisenmanagement

Am Beispiel einer Kritischen Infrastruktur (KI)

17. September 2024 Jolanda M. Walker, MSc DAS

Agenda

Ziel und Grundlagen

Um was geht es?

Modus Operandi

Konkret...

Erfahrung im Krisenmanagement im Ausland als Delegierte des IKRK

Ziel des Krisenmanagements

Schnellstmögliche Wiederherstellung des **ordentlichen** Betriebes

Reputation schützen

Miteinander aus Krisen lernen

Grundlagen

Dokumente

- Konzept Notfall- und Krisenmanagement (Folien und in Papier)
- Handbuch Notfall- und Krisenmanagement
- Folien Notfall- und Krisenmanagement (int. & ext. Version)
- Rollenbeschriebe Krisenstab ("wer macht was bis wann"?)
- Quick Guide Manager on Duty (Notfallmanagement)
- Telefonverzeichnis (analog und digital)

Planung

- Ausbildungskonzept auf Jahresbasis mittels Roadmap
- Mtl. Fachausbildungen mit Fokusthema (zB. 45' Inhalt/15' Austausch)
- Jahresplanung der Trainings (angeleitet mittels Trainer)
- Jahresübung (ohne Anleitung mit Auswertung für Fokusthemen)

Um was geht es?

Herausforderungen bei einer ICT Firma

Anzahl Security Alerts

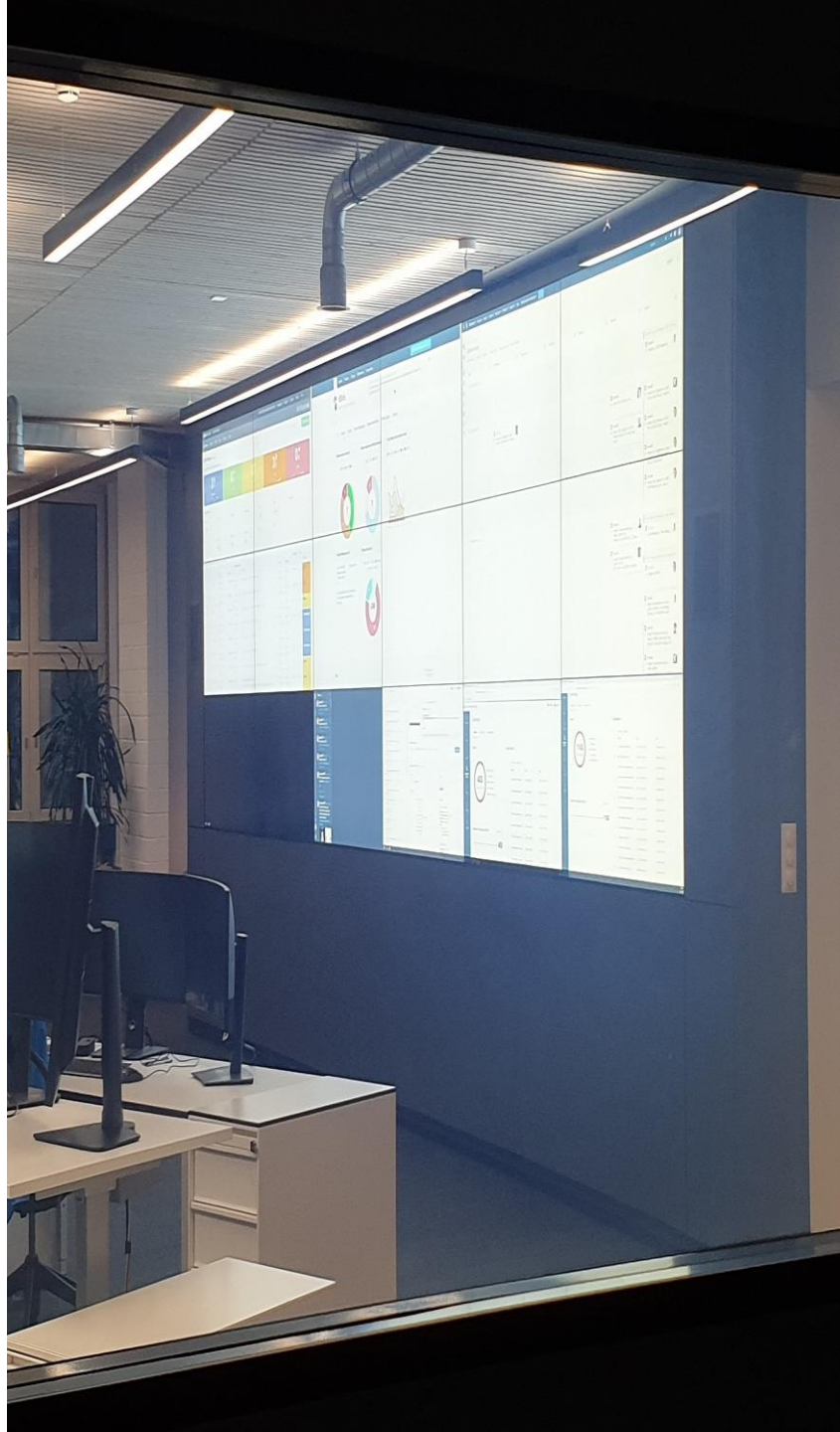
Mangel an Security Analysten

Heterogene Infrastrukturen

Lange MTTR-Zeiten

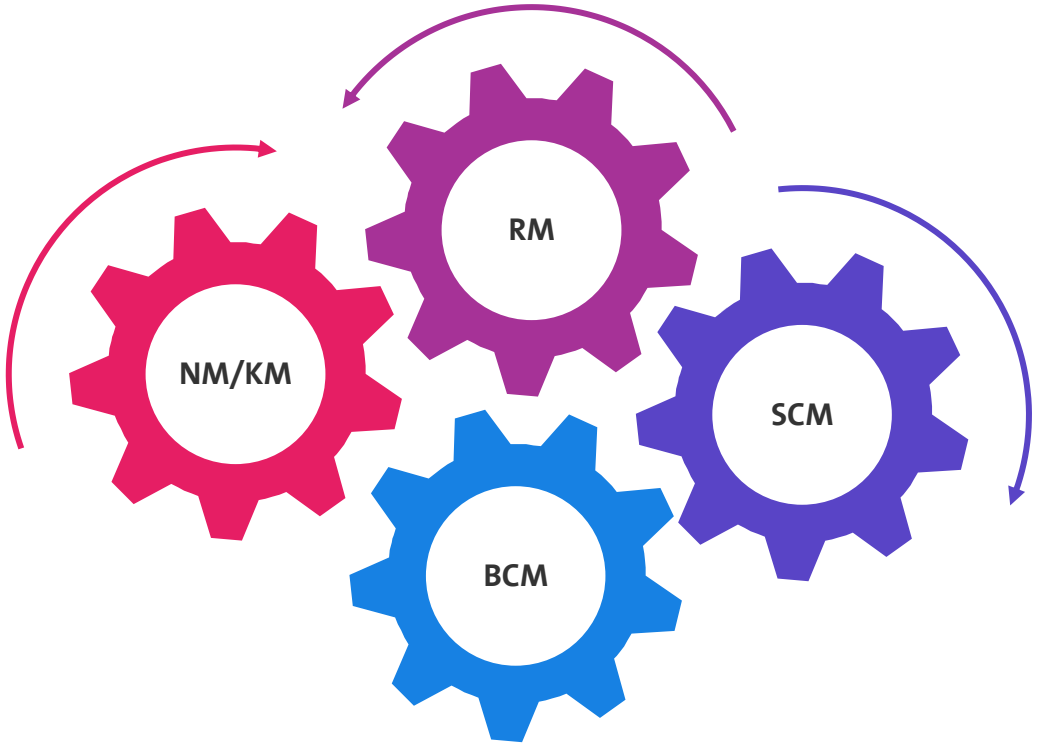
Komplizierte Prozesse

Eingeschränkte Visibilität




Wie schützen?

Interdisziplinäre Zusammenarbeit



Notall-/Krisenmanagement

- Regelt den systematischen Umgang mit Notfall- und Krisenlagen

→ Handlungsfähigkeit sicherstellen
→ Koordination der Einheiten
→ (Sofort-)Massnahmen zu ergreifen
→ Auswirkungen zu minimieren und Normalbetrieb wiederherzustellen

Risk Management

- Identifikation von Risiken und Bewertung derselben nach Eintrittswahrscheinlichkeit und Auswirkungen

→ Massnahmen zur Risikominderung/ -kontrolle (inkl. Entscheidung bez. Risikoakzeptanz) zu ergreifen

Service Continuity Mgmt (SCM)

- Prozess zur Wiederherstellung der Services/ Systeme nach einer Unterbrechung

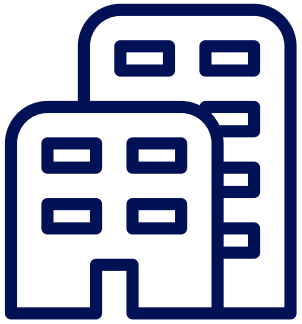
→ Service Continuity Plänen entwickeln, Tests durchführen
→ SCM unterstützt des Business Continuity Management beim IT-Ausfall

Die vier Säulen des Business Continuity Management Systems

Die Säulen des BCM spiegeln die Ressourcen wider, auf die sich Swisscom bei der Durchführung geschäftskritischer Aktivitäten und bei der Bewältigung von Krisen stützt.

Personal

Menschen sind der Eckpfeiler, die es uns ermöglichen, unsere geschäftskritischen Aktivitäten durchzuführen.



Gebäude

Swisscom ist auf eine Vielzahl von Gebäuden angewiesen, um den Betrieb geschäfts-kritischer Aktivitäten sicherzustellen.

Lieferanten

Die geschäftskritischen Aktivitäten von Swisscom sind auch von externen Lieferanten abhängig.

IT

Die Plattformen, Netzwerke, Konnektivität und Hardware, die Swisscom für ihre geschäftskritischen Aktivitäten einsetzt.

Es kommt nicht darauf an, die Zukunft vorauszusagen, sondern darauf, auf die Zukunft vorbereitet zu sein.

Perikles (um 500 - 429 v. Chr.), Griechischer Politiker und Feldherr

Definitionen

Reden wir vom Gleichen - verstehen wir uns?

Notfall

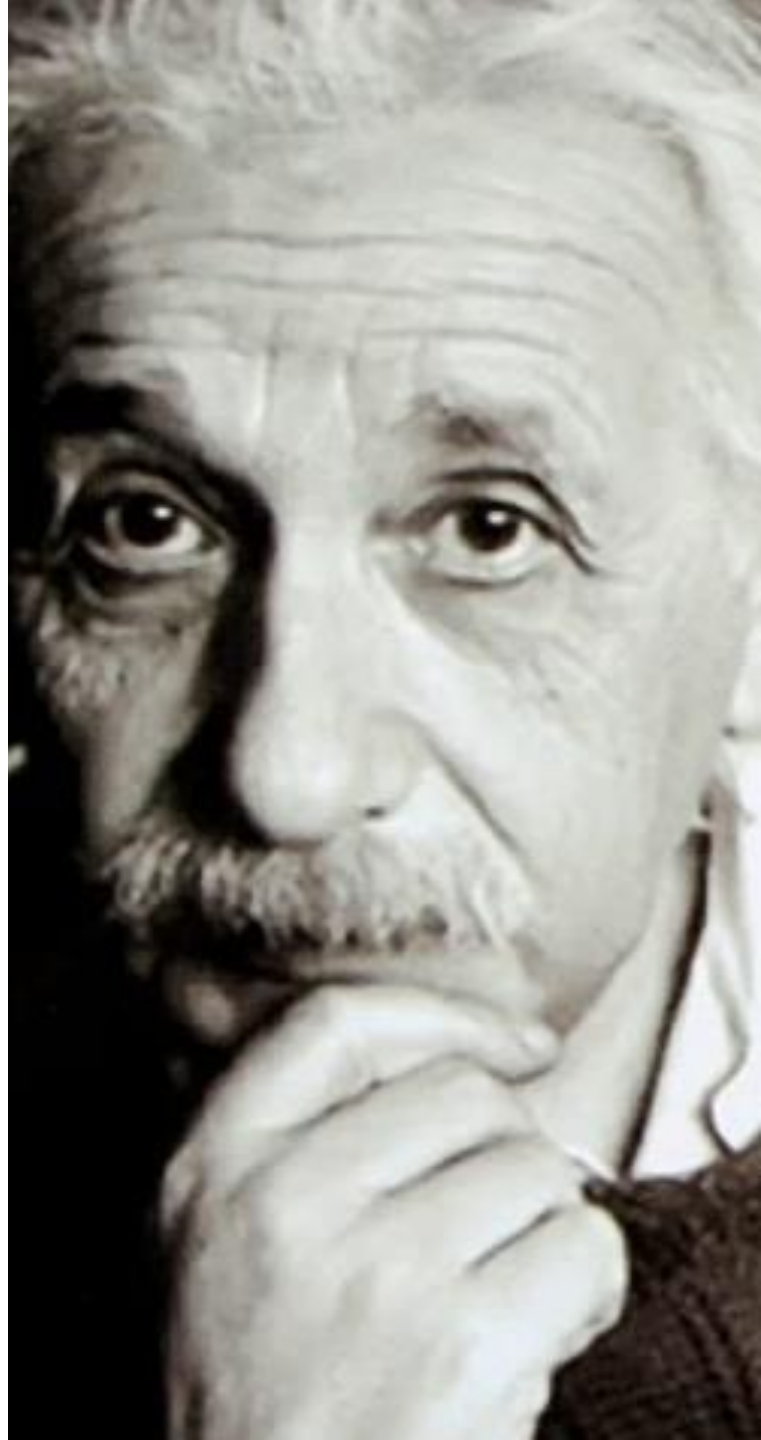
Plötzlich auftretende, ausserordentliche Lage mit Auswirkung auf die betroffene Organisationseinheit begrenzt. Das Ereignis kann grösstenteils mit den Mitteln und Ressourcen der betroffenen Organisations-einheiten bewältigt werden.

Krise

(Plötzlich) auftretendes Ereignis mit Auswirkungen auf die Reputation, die Handlungsfreiheit oder die Existenz der Unternehmung. Die Ereignis-bewältigung erfordert koordinierte, horizontal und vertikal vernetzte, ausserordentliche Massnahmen, da die normale Organisationsstruktur, die Entscheidungswege und die Ressourcen nicht mehr genügen.

Im Notfallmanagement steht die **Handlungsfähigkeit** im Vordergrund und im Krisenmanagement ist die **Entscheidungsfähigkeit** zentral

Quelle: Praxishandbuch Krisenmanagement; Sartory, Senn, Zimmermann, Mazumder, Midas Verlag



Erkennen und auslösen einer Krise

Operative Stufe	Taktische Stufe	Strategische Stufe	Strategische Stufe
Erkennung/erste Reaktionen	Manager on Duty der OE (Notfallmanagement)	Krisenmanagement	Katastrophe (Bund) wir dienen zu

Ereignis tritt ein
- Ereignis wird in der Linie erkannt
- Verantwortung der Bearbeitung verbleit in der Linie

Eskalation zu Notfallmanagement der OE
- Linie erkennt, das Ereignis übersteigt die Möglichkeiten
- Das Notfallmanagement ist das stärkste Mittel der Bereichsleitung
- Eskalation zum Notfallmanagement, gespiesen durch MoD
- Der MoD der Linie übernimmt die Führung und koordiniert bei Bedarf mit anderen MoD des Konzerns

Eskalation zu Krisenmanagement Konzern
- Der MoD der Linie kann das Ereignis **nicht** bewältigen
- Eskalation zu Entscheidungsträger Krisenstab Konzern
- Bei Auslösung des Krisenstabes übernimmt der Krisenmanager
- Das Krisenmanagement ist das stärkste Mittel des CEO

Das Eskalationsmodell

Wer macht was bis wann...

Die Eskalationsstufe ist abhängig von der Kundenauswirkung

Kriterien

Escalated Major Incident	• Business-Kritikalität sehr hoch • Reputation akut gefährdet
Major Incident	• Business-Kritikalität hoch • Ethische Gründe • Reputationsschaden möglich
Escalated Incident	• Business-Kritikalität mittel
Incident	• Business-Kritikalität niedrig
Prevented Incident	• Verhinderung von Service- und Kunden-Impact, Redundanzverlust oder Kapazitätsengpässe

Business-Kritikalität	• 1-n Services nicht oder nur teilweise verfügbar • Arbeiten nicht möglich oder Prozesse stark eingeschränkt • Unzumutbarer, inakzeptabler Zustand, z. B. Workaround • Mehrere Standorte eines Kunden betroffen • Behebungszeit inakzeptabel oder massiv überschritten
Ethik	• Geographisches Gebiet betroffen, z. B. ein Dorf, ganze Regionen oder ein Tal • Leben gefährdet • Existenz von Unternehmen gefährdet
Reputation	• Vertrauensverlust, Ansehen, Erscheinungsbild oder Reputation gefährdet • Hohe Medienrelevanz zu erwarten oder bereits vorhanden • Finanzieller Schaden zu erwarten

Link auf Wiki IT Service Management System/Incident Management

Angriffe auf kritische Infrastrukturen in der Ukraine

2014	**Annexion der Krim**
2015	BlackEnergy3 (Sandworm)
2016	Industroyer (Sandworm)
2017	NotPetya
2021	> 2'000 Angriffe gegen Regierungssysteme und kritische Infrastrukturen
2022	**Einmarsch Russland in der Ukraine** Whispergate DDoS Angriffe Defacements ViaSat Sabotage Industroyer 2 Wiper Killnet & Co ...

Was hilft…

Kultur – um was geht es?

Quelle: 1207 kulturaspekte.pdf (memecon.de)

Umgang

...wer eignet sich...

Umgangsformen

- Haltung
- Anstand
- Erdung
- Reflexion
- Flexibilität
- Mut
- Hilfsbereitschaft
- Verschwiegenheit
- Pragmatismus
- Wiederstandfähigkeit

Fachspezialist

Durchhaltefähigkeit

Sozialkompetenz

Kognitive Fähigkeiten

- Strukturiertes Denken
- Vernetztes Denken
- Synthesefähigkeit
- Ausdruck in Wort und Schrift
- Visualisieren – "ein Bild vor Augen führen"
- (Erfahrung)

Arbeitskultur

...miteinander reden...

Zielgruppe – Flughöhe
Was will ich bewirken?
Was ist die Körnigkeit des Inhaltes?

Fakten versus Annahmen oder Tatsachen und Meinungen
Rahmen setzen (BABS: Natur, Technik, Gesellschaft)
Quellen (NZZ, Economist, Bund, Blick, Social Media etc.)
Datum vermerken, die Lage ändert
Prüfung der Fakten (Facts and Figures)

Was kenne ich, was kann ich besonders gut?

Arbeitskultur

warum die erste Idee oft nicht die Beste ist

- Versteifung auf das Offensichtliche
- Einfluss von Emotionen
- Prägung durch Charakter und Persönlichkeit
- Vorurteile und Wahrnehmungsfehler

Was uns hilft...

- Train as you fight
- Struktur für die Grundstabilität
- Regelmässig trainieren
- Fachreferate/Ausbildungen (60')
- Achten auf die Fachkenntnisse im Krisenstab
- Themen entlang der Risikomatrix des Konzerns

Konkret…

Denken – um was geht es?

Simple Systeme – (ordentliche Lage) Tagesgeschäft

Dunkelheit – Lichtschalter

Komplizierte Systeme – (besondere Lage) Notfall

Raddefekt – Radwechsel

Mono-kausal und linear

Komplexe Systeme – (ausserordentliche Lage) Krise

Was ist die Grundursache?

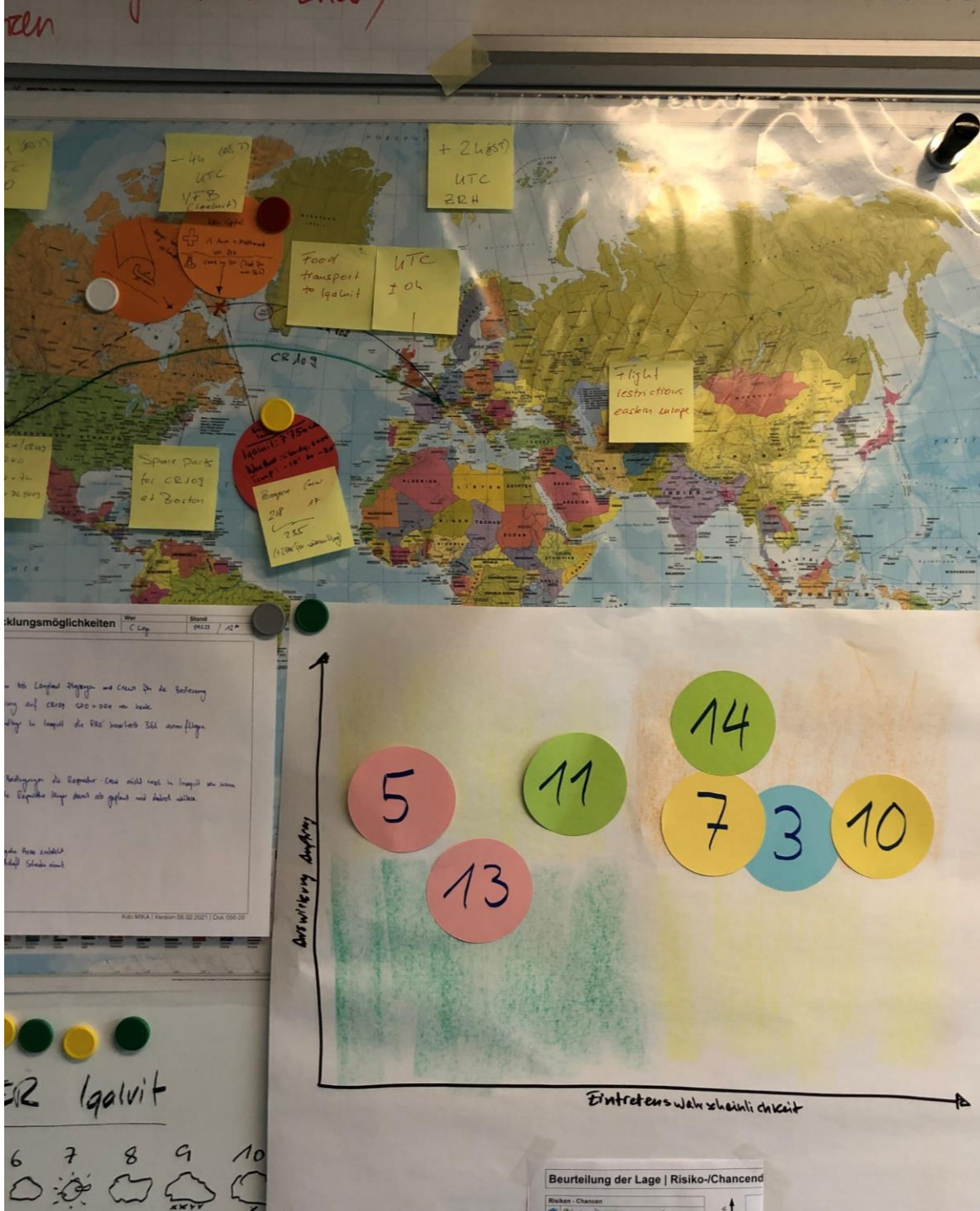
Wie ist das Problem vernetzt?

Wie sind die Abhängigkeiten?

Womöglich wechselwirkende Abhängigkeiten?

Wie kann ich das Problem (e) verstehen?

Wer kann helfen?



Gesamtlage mehrstufig verstehen

Problemerfassung seitens Krisenmanager mit Hilfe des Stabschefs

- Die PE wird nach dem Orientierungsrapport und **vor dem 1. Lagerapport erstellt** und visualisiert zugänglich gemacht.
- Um die ausserordentliche Lage unter Zeitdruck zu verstehen, ist eine Problemerfassung (PE) immer innert **90 Minuten zu erstellen.**
- Die Problemerfassung dient der **Entscheidungsgrundlage**.
- Die Problemerfassung wird je nach Faktenlage **korrigiert.**
- Zu berücksichtigende Aspekte sind die **Natur, die Technik und die Gesellschaft.**

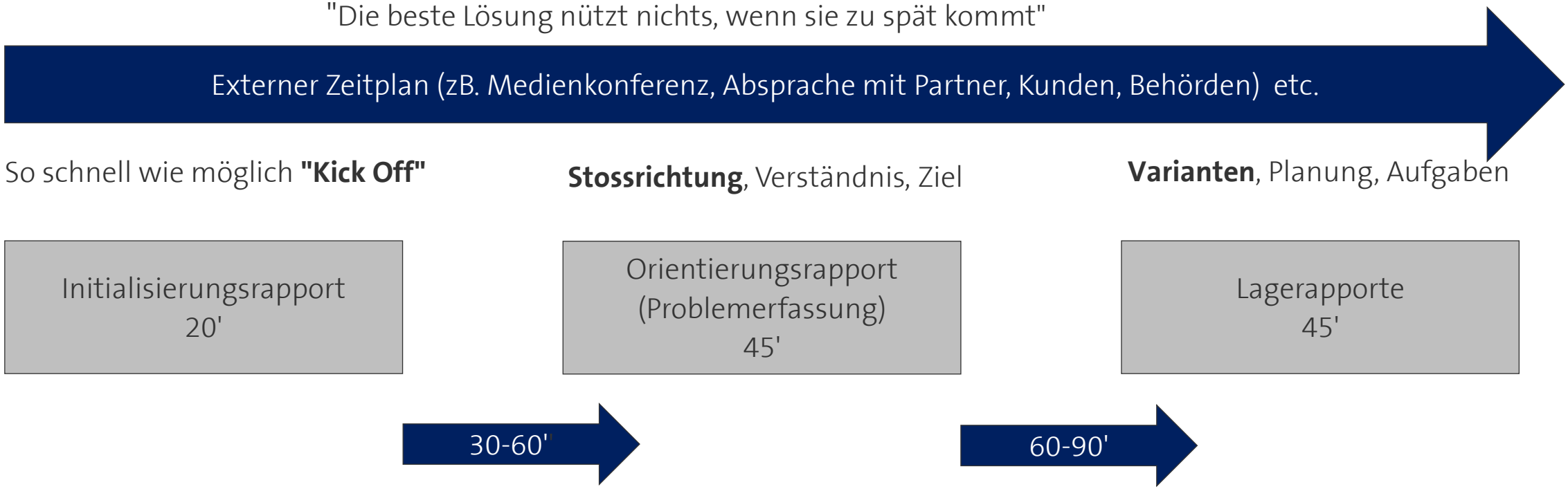
Problemerfassung		Wer	Stand
Problemdarstellung /-entdeckung			
Problemklärung	Teilaufgaben		
	Aufgabenumschreibung		
	Handlungsrichtlinien		
	Produkte		
Problem-beurteilung	Prioritäten		
	Stabsgliederung		

Um erste Gedanken zu ordnen, eignet sich das Raster, bevor visualisiert wird.

Der Führungsrhythmus

Zeitverhältnisse

"Die beste Lösung nützt nichts, wenn sie zu spät kommt"



- Der **Initialisierungsrapport** findet asap statt, auch wenn noch nicht alle vor Ort sind. Mit wenigen Informationen und unklarem Auftrag wird gestartet, der Rahmen wird gesetzt. Das Lageteam sammelt erste Fakten und erstellt eine rudimentäre Übersicht. Die W-Fragen helfen, es gilt: "besser wenig als nichts erfassen".
- Die **Problemerfassung** wird schnellstmöglich erstellt und laufend geprüft, sie wird im **Orientierungsrapport** präsentiert.
- Die **Lagerapporte** dienen der verbindlichen Planung sowie der Kontrolle der Arbeiten und Absprachen.

Was ist relevant...?

Drei Punkte

- Es kommt meistens anders als wir **denken**… Wir haben frühkindliche Prägungen (Bauchgefühl)
- Jeder ist **ersetzbar**…Redundanzen schaffen (BCM)
- **Übung** macht den Meister…Ansonsten haben wir Blockaden (Kleinhirn), wir haben Angst

Dwight D. Eisenhower, 34. Präsident der USA

..." Was ist wichtig - was ist dringend"...?

Eisenhower-Prinzip – Wikipedia

...es gibt nichts Gutes, ausser man tut es!

Beispiele aus der Praxis