

Notfallmanagement/Krisenmanagement Ist Ihr Rettungsanker aus
Papier oder Stahl?



Sicherheitsvorfall

The image shows a screenshot of a website with a dark blue header. On the left, the text "SICHERHEITSVORFALL" is displayed in white. The main navigation menu includes "HOCHSCHULE", "STUDIUM", "FORSCHUNG", "INTERNATIONAL", and "DIGITALISIERUNG". On the right, there are links for "BESCHÄFTIGTENPORTAL", "QUICKLINKS", and "ENGLISH". The main content area features a large blue background with a white exclamation mark and the headline "ANGRIFF AUF DIE IT-INFRASTRUKTUR". Below this, there are three distinct sections: a dark blue box with the text "Landkreis ruft bundesweit ersten Cyber-Katastrophenfall aus" and a Ferrari logo; a blue box with the headline "CYBERANGRIFF AUF DIE TU BERGAKADEMIE" and a sub-headline "Es gab einen Cyberangriff auf die IT-Infrastruktur der TU Bergakademie Freiberg. Der bisherige Webauftritt der Universität ist aktuell nicht erreichbar. Grundlegende Informationen zum Universitäts- und Studienbetrieb sowie Ansprechpersonen finden Sie auf dieser Seite. Wir bitten um Verständnis." followed by links for "Aktuelle Informationen des Rektorates" and "Informationen zum Studium auf www.studieren-in-freiberg.de"; and a photograph of a person using a laptop with a screen displaying a grid of numbers and letters over a building image.

SICHERHEITSVORFALL

HAW HAMBURG

HOCHSCHULE STUDIUM FORSCHUNG INTERNATIONAL DIGITALISIERUNG

BESCHÄFTIGTENPORTAL QUICKLINKS ENGLISH

ANGRIFF AUF DIE IT-INFRASTRUKTUR

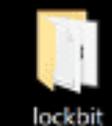
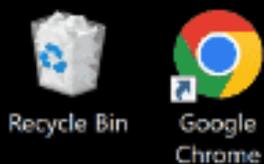
Landkreis ruft bundesweit ersten Cyber-Katastrophenfall aus

CYBERANGRIFF AUF DIE TU BERGAKADEMIE

Es gab einen Cyberangriff auf die IT-Infrastruktur der TU Bergakademie Freiberg. Der bisherige Webauftritt der Universität ist aktuell nicht erreichbar. Grundlegende Informationen zum Universitäts- und Studienbetrieb sowie Ansprechpersonen finden Sie auf dieser Seite. Wir bitten um Verständnis.

[Aktuelle Informationen des Rektorates](#)

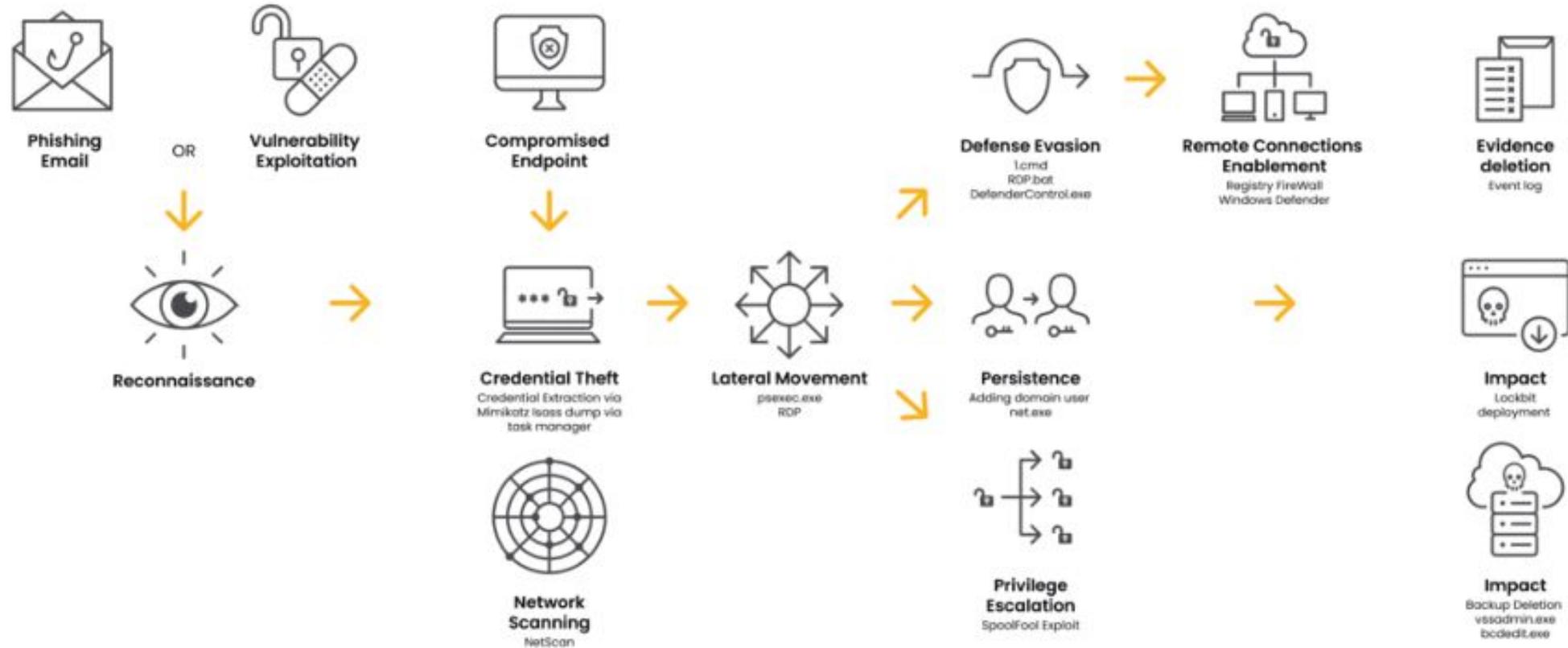
Informationen zum Studium auf www.studieren-in-freiberg.de



LockBit Black

**All your important files are stolen and encrypted!
You must find HLJkNskOq.README.txt file
and follow the instruction!**

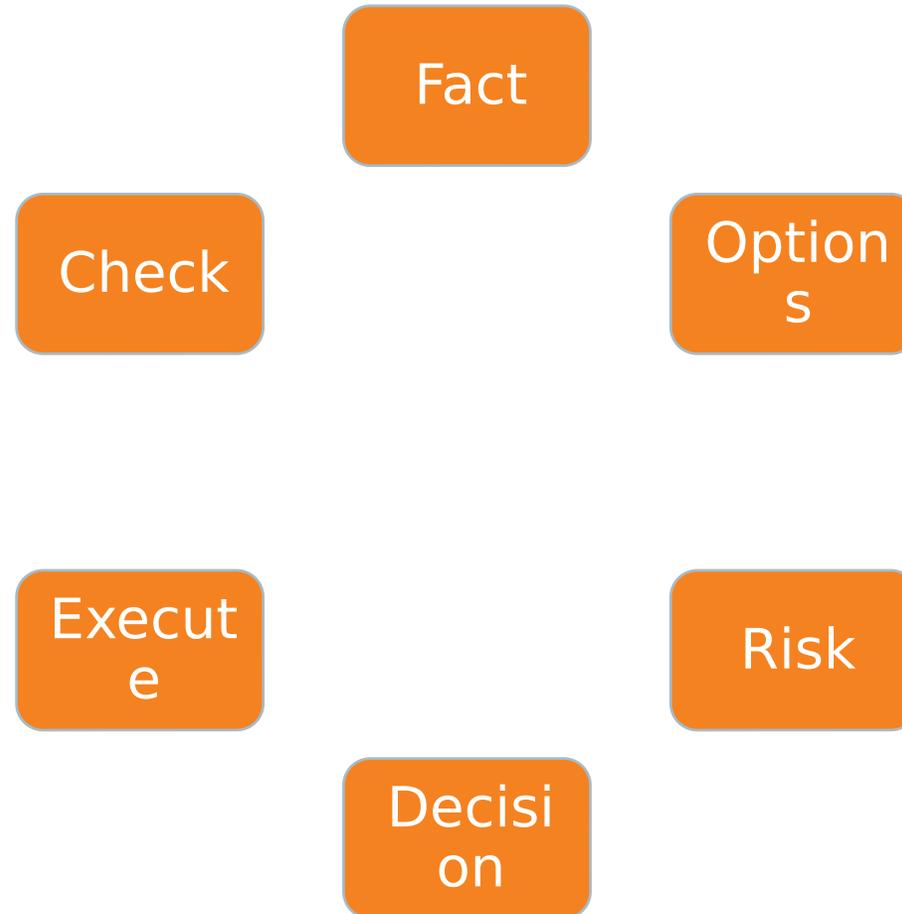
Ransomware



Quelle:

https://www.vx-underground.org/malware_defense.html

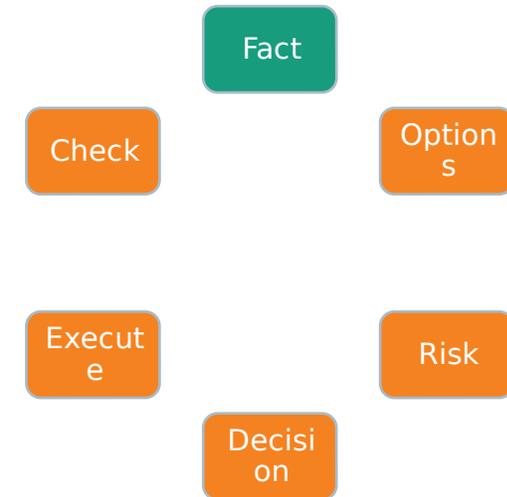
FORDEC-Modell



FORDEC-Modell

Fact

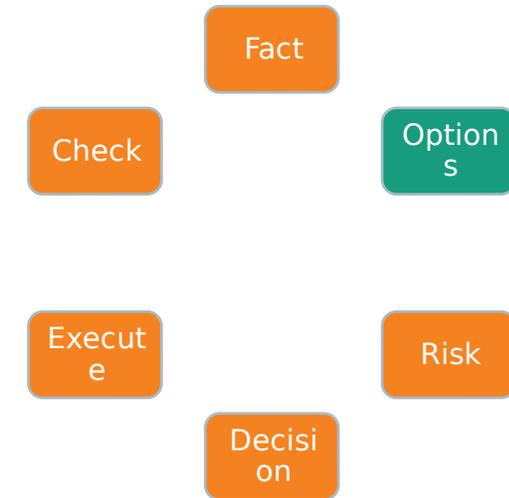
- Fakten sammeln
 - Fakten bezüglich der Ursachen
 - Fakten bezüglich der Auswirkungen
- Antworten auf folgende Fragen suchen:
 - Was ist passiert?
 - Wie ist es passiert?
 - Wann und wo ist es passiert?
 - Wer und welche Ressourcen sind betroffen?
 - Welche Maßnahmen wurden eingeleitet?
 - Welche Auswirkungen hat der Vorfall auf die Mitarbeiter/Kunden/Öffentlichkeit?



FORDEC-Modell

Option

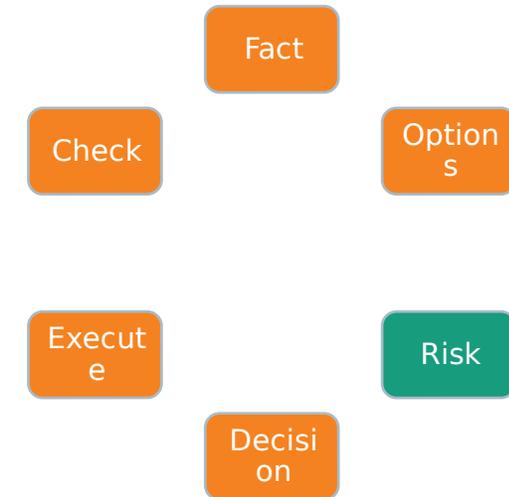
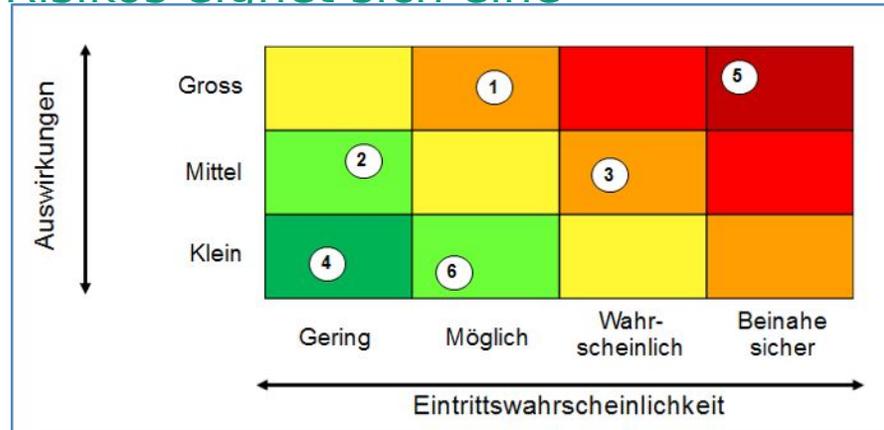
- Handlungsalternativen identifizieren
- z.B.
 - Ausfall der IT
 - Gibt es ein Backup-System? Kann nahtlos umgeschaltet werden?
 - Ausfall der Gebäudesteuerung
 - Gibt es alternative Locations? Können Büroräume kurzzeitig gemietet werden?



FORDEC-Modell

Risk

- Für jede Handlungsoption muss das Risiko und der Nutzen einer Entscheidung ermittelt werden.
- Zur Analyse des Risikos eignet sich eine Risikomatrix

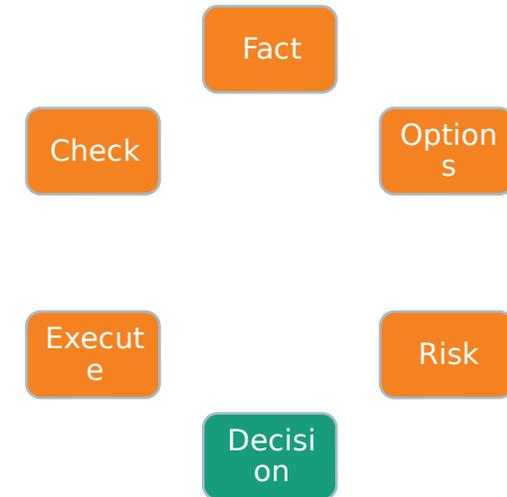


- Die Risiken jeder Entscheidungsoption sollten klar dokumentiert werden

FORDEC-Modell

Decision

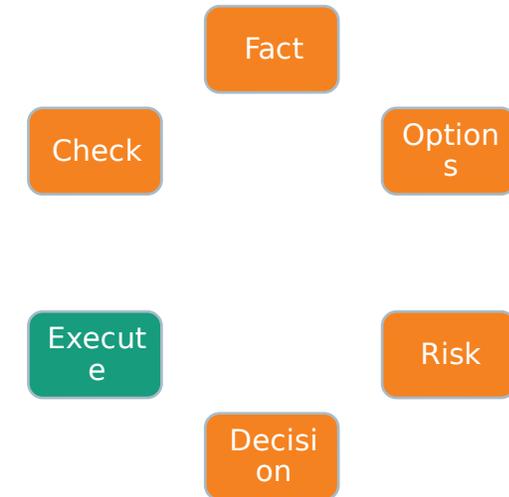
- Schnelle Entscheidung manchmal wichtiger als die richtige Entscheidung
- Jede Entscheidung sollte gut begründet werden können
- Risiko so gering wie möglich halten



FORDEC-Modell

Execute

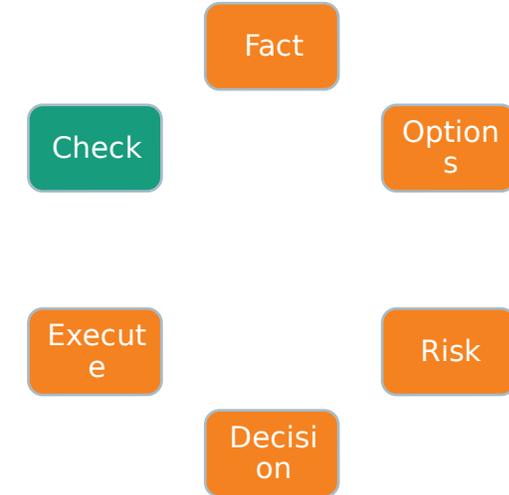
- Entscheidungsträger innerhalb des Krisenstabs geben die Ausführung einer Option frei
- Operative Mitarbeiter im Krisenstab setzen die Entscheidung um
- Checklisten können bei der Umsetzung helfen
- Achtung: vorgegebene Pläne nicht blind abarbeiten □ neue Krise möglich



FORDEC-Modell

Check

- Kontrolle der umgesetzten Maßnahme:
 - Wird das gewünschte Ergebnis erzielt?
 - Muss nachgesteuert werden?
- ggf. FORDEC-Kreislauf von vorne Starten und Fakten zur neuen Situation sammeln
- Ergebnisse detailliert dokumentieren!
 - Fakten aus Schritt 1 aufnehmen
 - Für welche Maßnahme wurde sich in Schritt 4 entschieden?
 - Wie wurde die Maßnahme umgesetzt?
 - Welche Auswirkungen konnte gemessen werden?



Krise

- Entscheiden ist nicht, ob und wie oft eine Krise eintritt, sondern in welcher Form und wie Sie damit umgehen
- Nicht immer sofort als Krise erkennbar
- Erzeugen einen hohen Informationsbedarf

Krise



Vier mögliche Konsequenzen:

- Krise beendet und positiv beigelegt
- Krise läuft weiter
- Krise endet mit einer negativen Lösung
- Krise endet in einer Katastrophe

Krise

Mögliche auslösende Ereignisse:



Naturereignisse



Technisches Versagen



Menschliches Versagen



Terrorismus

Krise

Cybercrime:



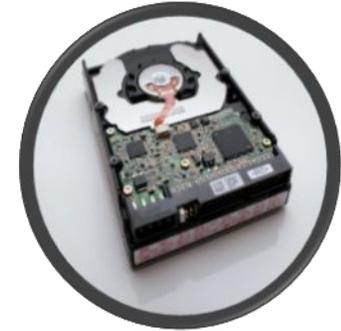
DDoS



Shitstorm /
Fake News



Schadsoftware



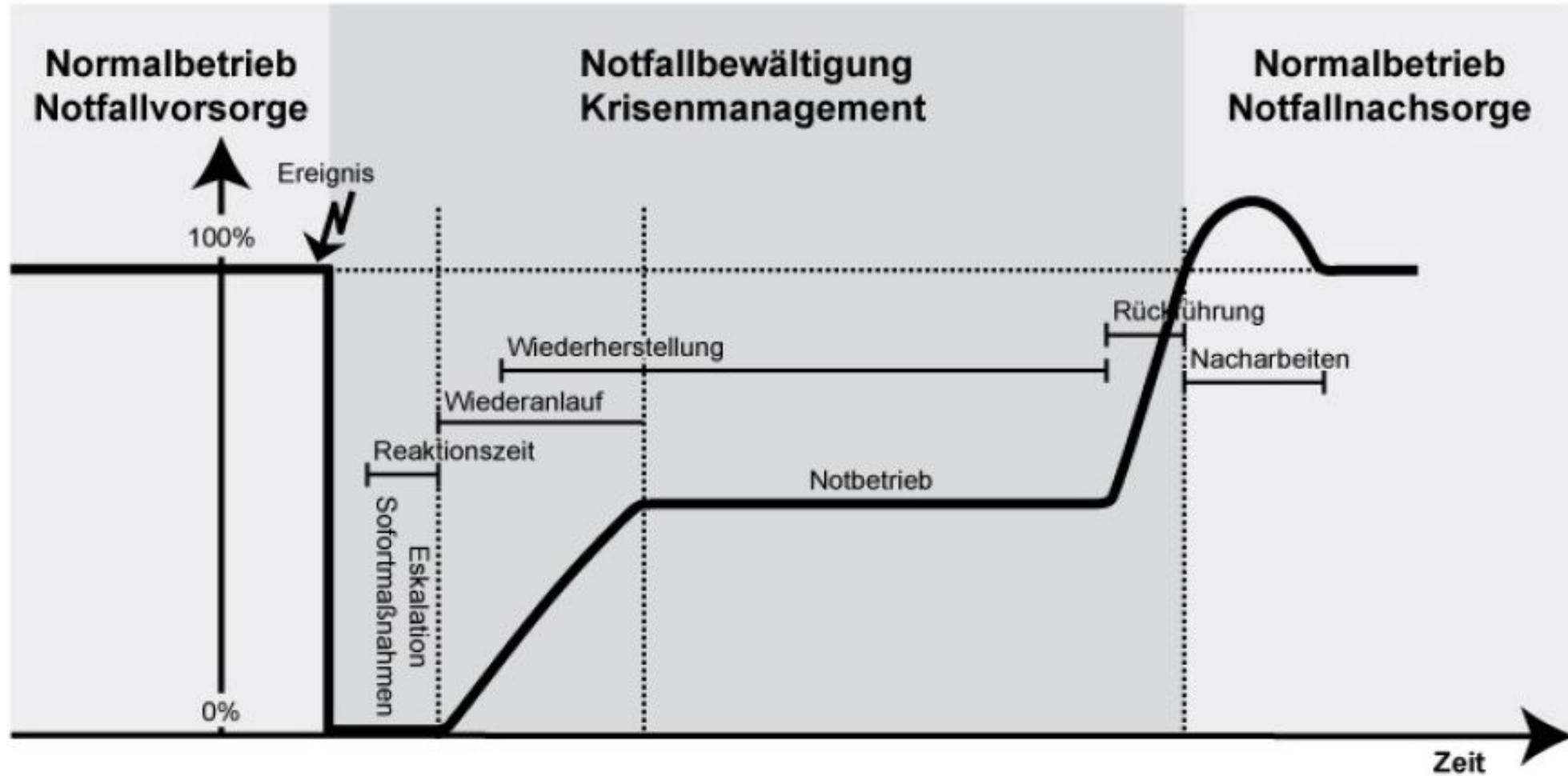
Datendiebstahl

Krise

Drei Phasen einer Krise:

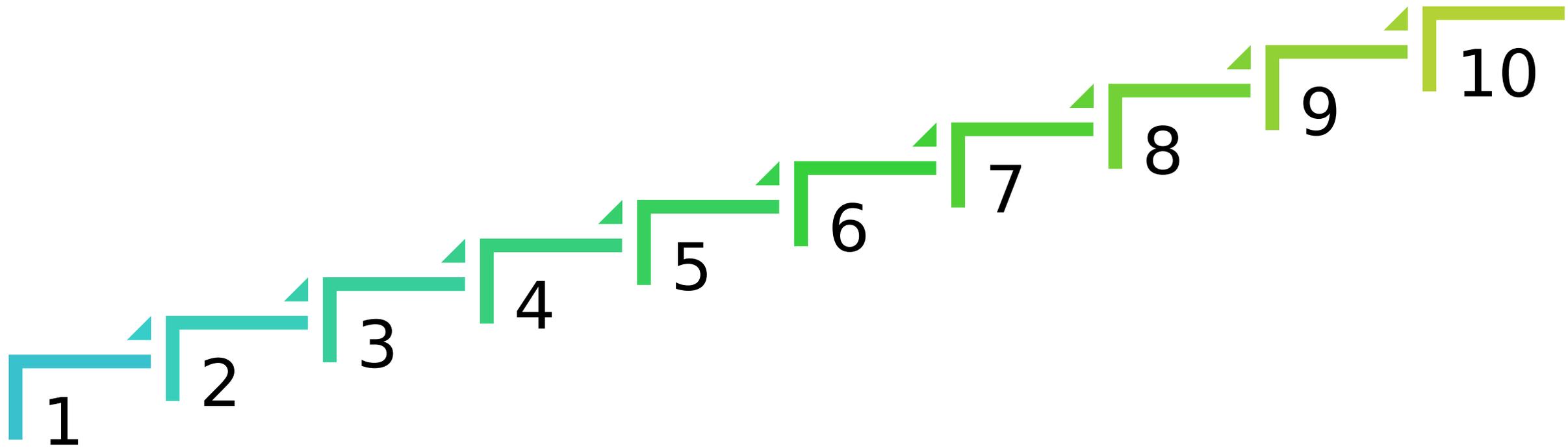


Krisenbewältigung



Krise

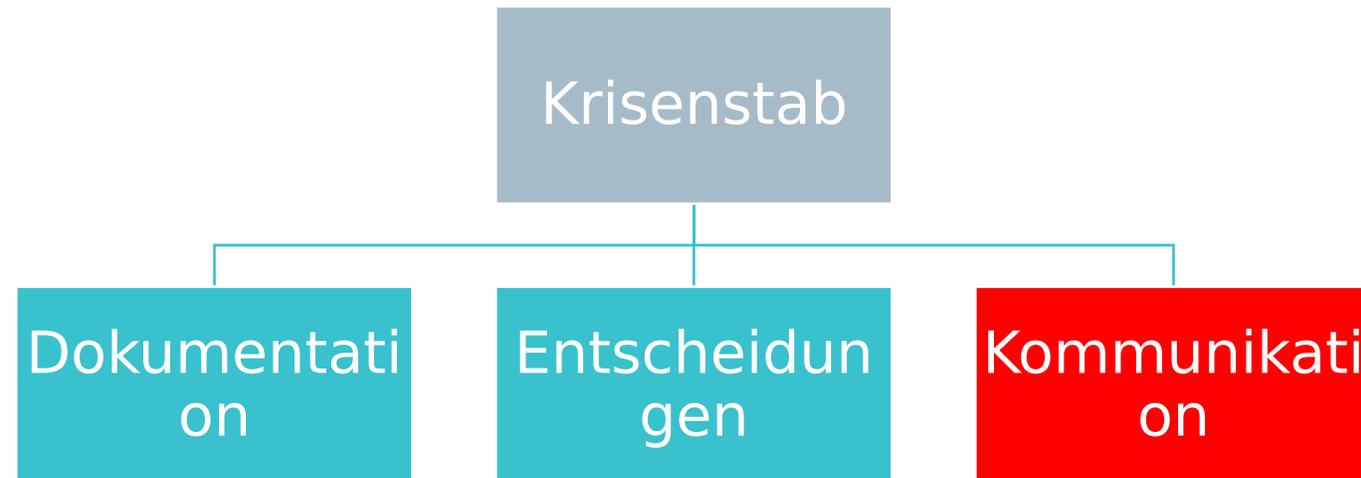
Eskalationsstufen



Krisenmanagement

Krisenstab

- wird innerhalb der Organisation gebildet und besitzt besondere Befugnisse
- koordiniert alle Beteiligten und stellt das Informationsmanagement sicher
- beurteilt die Lage und wägt Handlungsoptionen ab
- trifft Entscheidungen zur Bewältigung der Krise
- Informiert die Belegschaft, Partner, Behörden und Bevölkerung



Krisenmanagement

Krisenstab

- wird innerhalb der Organisation gebildet und besitzt besondere Befugnisse



Risikokommunikation vs. Krisenkommunikation

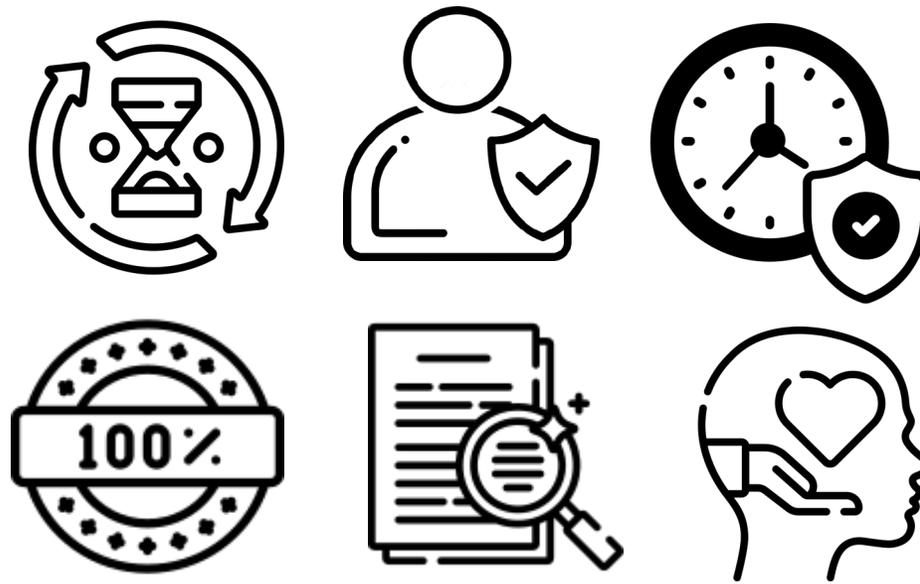
Risikokommunikation	Krisenkommunikation
Präventiv	Nachsorge
Anlassunabhängig	Anlassbezogen
Langfristig	Kurzfristig, zeitlich begrenzt
Vorbereitend auf Gefahren und Risiken	Reagierend auf eingetretene Krisen
Ziel ist es, Vertrauen aufzubauen	Ziel ist es, akut drohenden Schaden abzuwenden



Krisenkommunikation

Grundprinzipien

- Transparenz
- Wahrhaftigkeit
- Zuverlässigkeit
- Empathie
- Konsistenz
- Aktualität



□ **Besonders im Bereich IT zu nicht IT - Verständlichkeit !!**

- Organisatorische Vorkehrungen treffen, welche im Krisenfall schnell umgesetzt werden können
- Entscheidungsprozesse (Wie wird entschieden?)
- Organisatorischer Rahmen (Wer entscheidet?)
- Pragmatische Vorkehrungen (Was machen wir bei einem IT-Ausfall?)

Krisenkommunikation

Framing



Kontakt

B.Sc. Martin Klöden
IT-Forensik
Tel. +49 3727 58-1319
martin.kloden@fkie.fraunhofer.de
kloden@hs-mittweida.de

Hochschule Mittweida
Technikumplatz 17
09648 Mittweida
www.fkie.fraunhofer.de
www.hs-mittweida.de





Vielen Dank für Ihre
Aufmerksamkeit
