



Krisenmanagement ohne Konsequenzenmanagement ist wertlos

Gerald KORTSCHAK & Harald SCHENNER



Wir



DI KORTSCHAK Gerald

Vortragender FH St. Pölten
Vortragender WIFI Stmk
Vortragender Milkdo ST



DI SCHENNER Harald

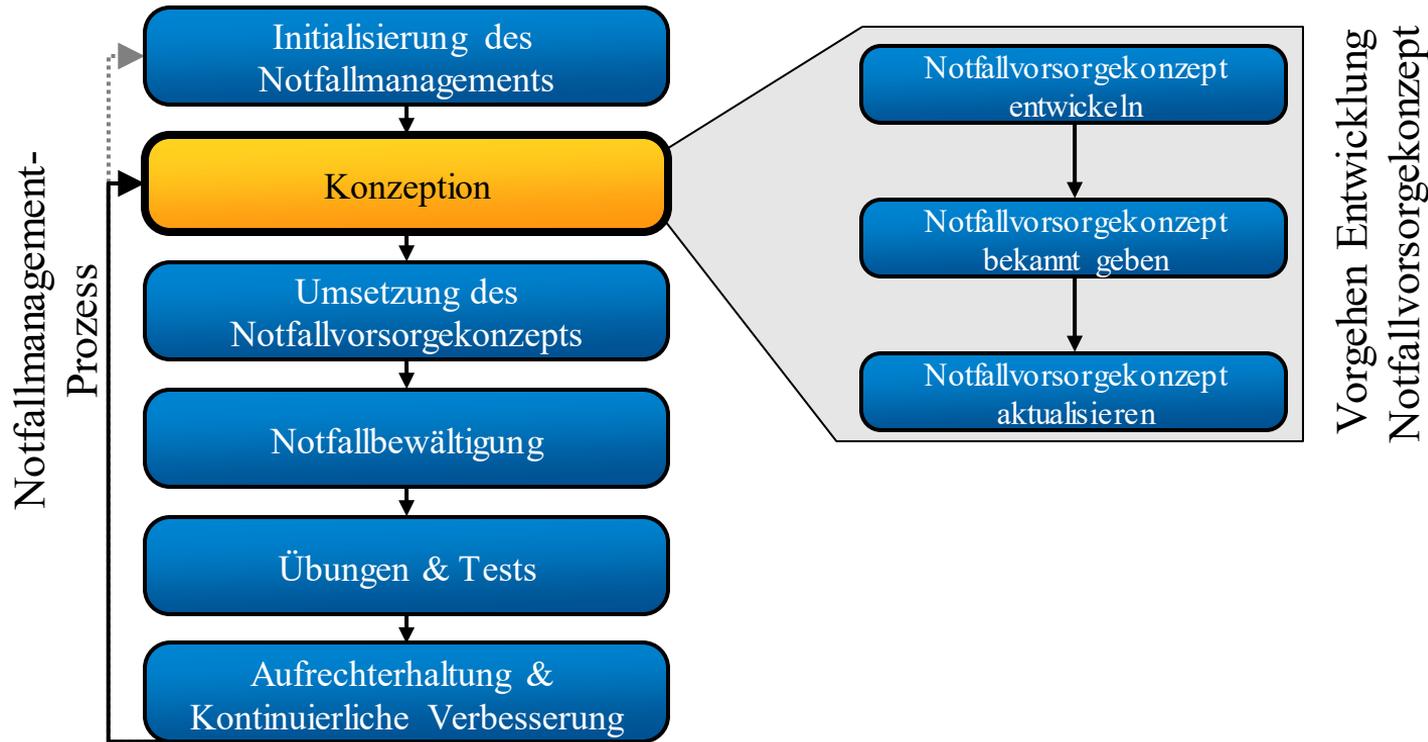
Vortragender FH St. Pölten
Vortragender WIFI Stmk
Vortragender FH CAMPUS02

Lust auf Bingo?

- Cyber Resilience
- Gen 5 Hacker
- Cyber Incident Response Plan (CIRP)
- Cyber Attack Information System (CAIS)
- Cyber Emergency Response Team (CERT)
- Cyber Defense Center (CDC)
- Cyber Incident Simulation (FMA)
- Cooperative Cyber Defence Center of Excellence
- Security Information and Event Management (SIEM)
- beliebig mit „advanced“ oder „next generation“ erweiterbar



Das Notfallvorsorgekonzept ist Teil der Konzeptionsphase des BSI 100-4 Prozess



Behandlung von Risiko / Restrisiko?

Eliminieren

- Systemwechsel
- Prozessänderung

Reduzieren

- Abwehrmaßnahmen
- Gegenmaßnahmen (Firewall, IPS, IDS, ...)

Akzeptieren

- "is so"
- Entscheidung der GF

Transferieren

- Risiko abwälzen (Versicherung)
- Risiko auslagern (Rechenzentrum)



STRATEGY

IDEA CONNECTION

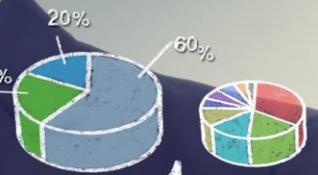
CREATIVITY

CONTENT

PEOPLE

RESEARCH INFORMATION GROWTH

TECHNOLOGY ANALYSIS



LIKE

SHARE

SOCIAL NETWORK

FRIENDS

ACCESS MANAGEMENT



GROUP



NETWORK



COMMUNITY

FEEDBACK



WHO

WHEN

SOLUTION

SECURITY



TEAMWORK

PLANNING



WHAT

WHY

SUCCESS



INNOVATION



VISION



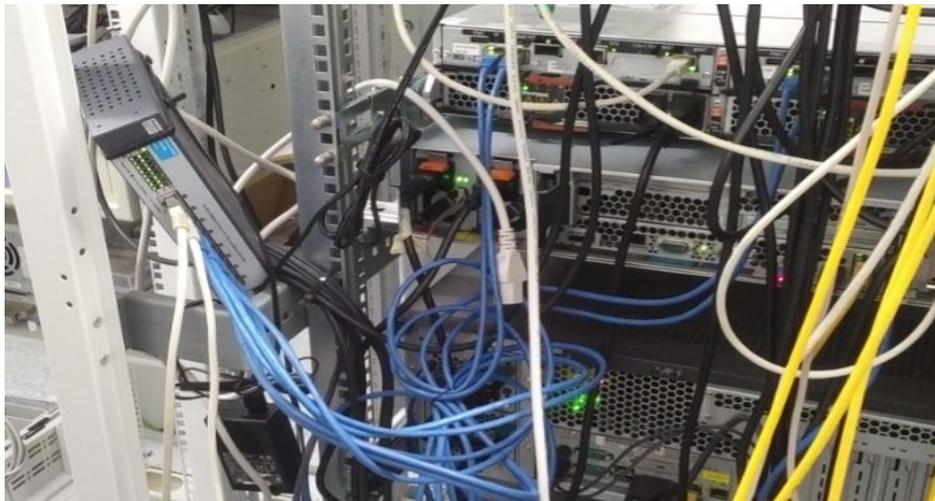
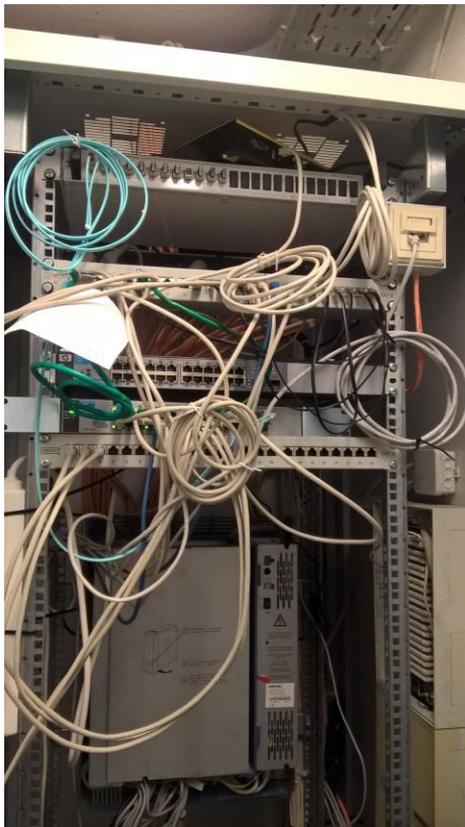
- MARKETING
- TARGET
- SKILLS

WHERE

HOW

GOAL





Die häufigsten Fehler

- Keine **smarten** LösungsZiele
- Lagebeurteilung != Lagefeststellung
- Mangelnde Information
- Teamführung
- Eindämmen statt lösen
- Symptom statt Ursache
- Kopf in den Sand
- „Das muss sofort wieder funktionieren“-Mentalität
- Kein eigenes Budget (24% bis 37%)



Die häufigsten Fehler

- verschwiegene Fakten
- falsche Lagebilder (Feststellung & Beurteilung)
- zu späte Entscheidungen = keine Entscheidung
- „Entschiedenes“ wird diskutiert
- kein Team-Rückhalt (= falsches Team)
- zu detaillierte Entscheidungen
- Kdt will Teamleader & Entscheider sein
- Kein Mut zur Lücke
- **Stressverletzte**



Die graue Theorie

Reaktiver Dienst

- Bereitstellung von Notfallteams, die bei Sicherheitsvorfällen zur Abwehr und Wiederherstellung von IKT-Systemen bereitgehalten werden (auch als CSIRT für Computer Security Incident Response Team bezeichnet).

Präventiver Dienst

- Die präventiven Aufgaben eines CERT sind die Entwicklung der IKT-Sicherheit, die Warnung und erkannten Angriffsmustern, die Untersuchung, die Schadensermittlung und die Erhöhung der Wirkungsbereich besonders durch Ausbildung.

Sicherheitsqualitätsmanagement

- Bereitstellen einer fachlichen Know-How-Basis, der Dokumentation und eines Lessons-Learned-Zyklus für den eigenen Wirkungsbereich.

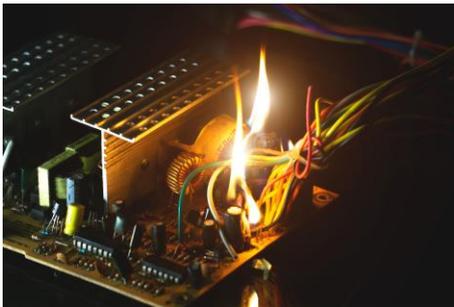


Konsequenzenmanagement als Lösung

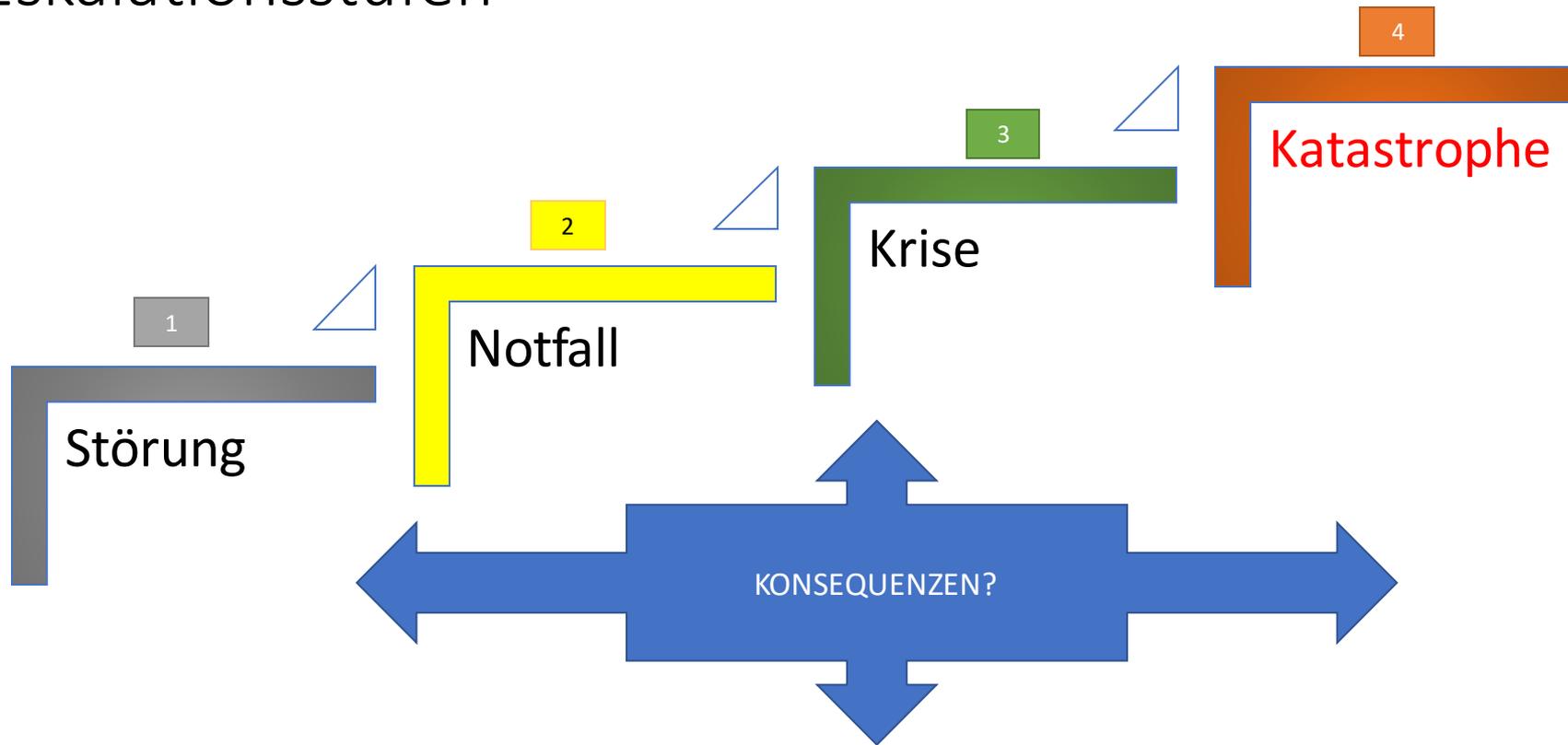


Was ist was?

- „Krise ist eine Situation die mit normalen Strukturen des Alltages nicht mehr bewältigt werden kann“ (Obst. Rudolf WABNEGG, MSD)
- Katastrophe ist die Eskalation der Krise im nicht mehr bewältigbaren Ausmaß inklusive der daraus folgenden Konsequenzen.



Eskalationsstufen

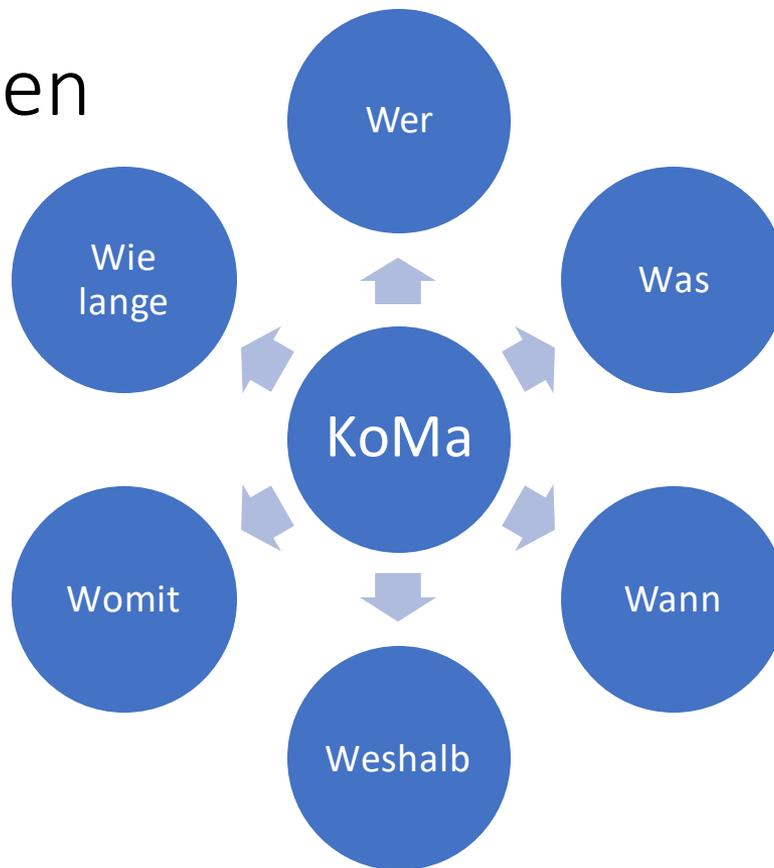


Was ist Konsequenzenmanagement?

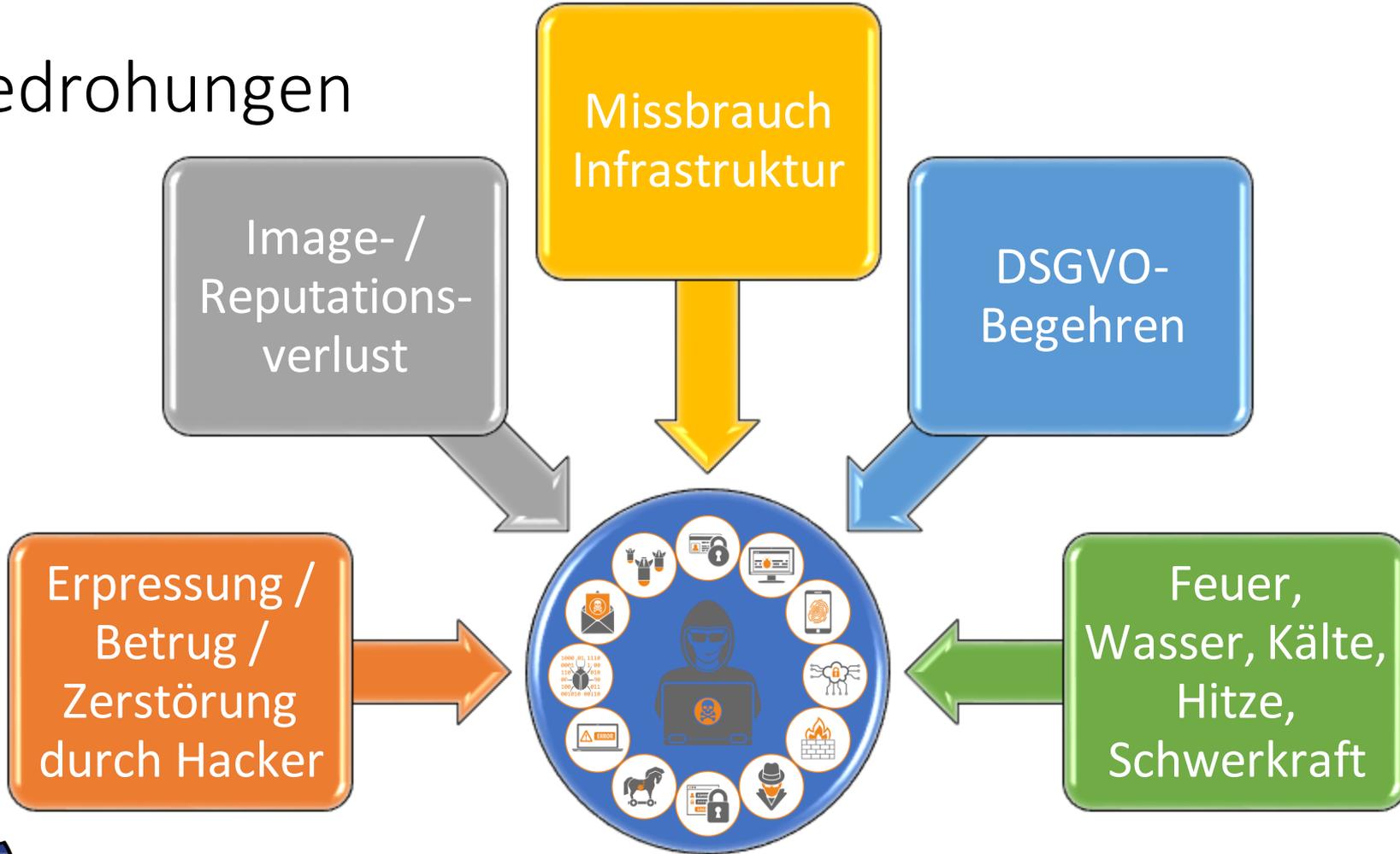
- Unmittelbare Reaktion zur Bewältigung von Auswirkungen
- Dazu muss man aber die Auswirkungen kennen!



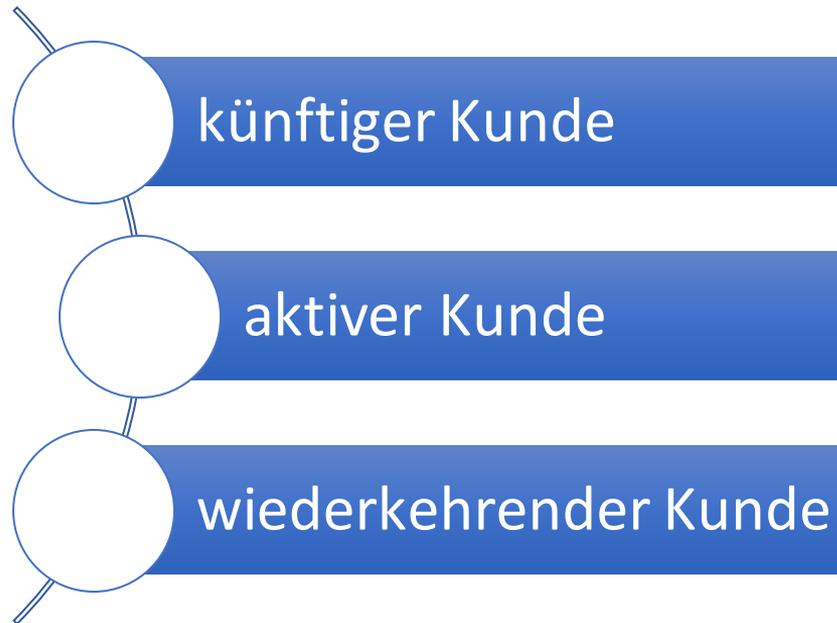
Auswirkungen



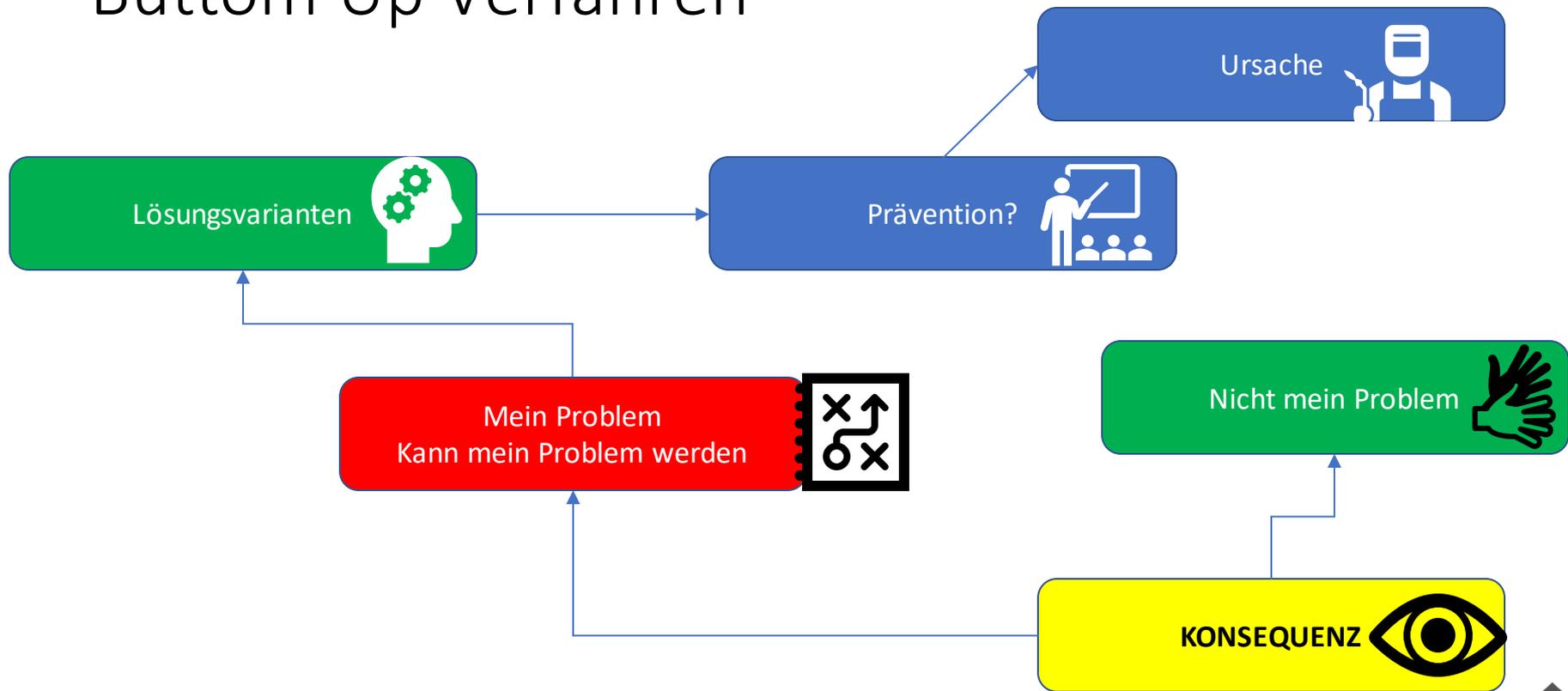
Bedrohungen



Wirkfelder



Buttom Up Verfahren



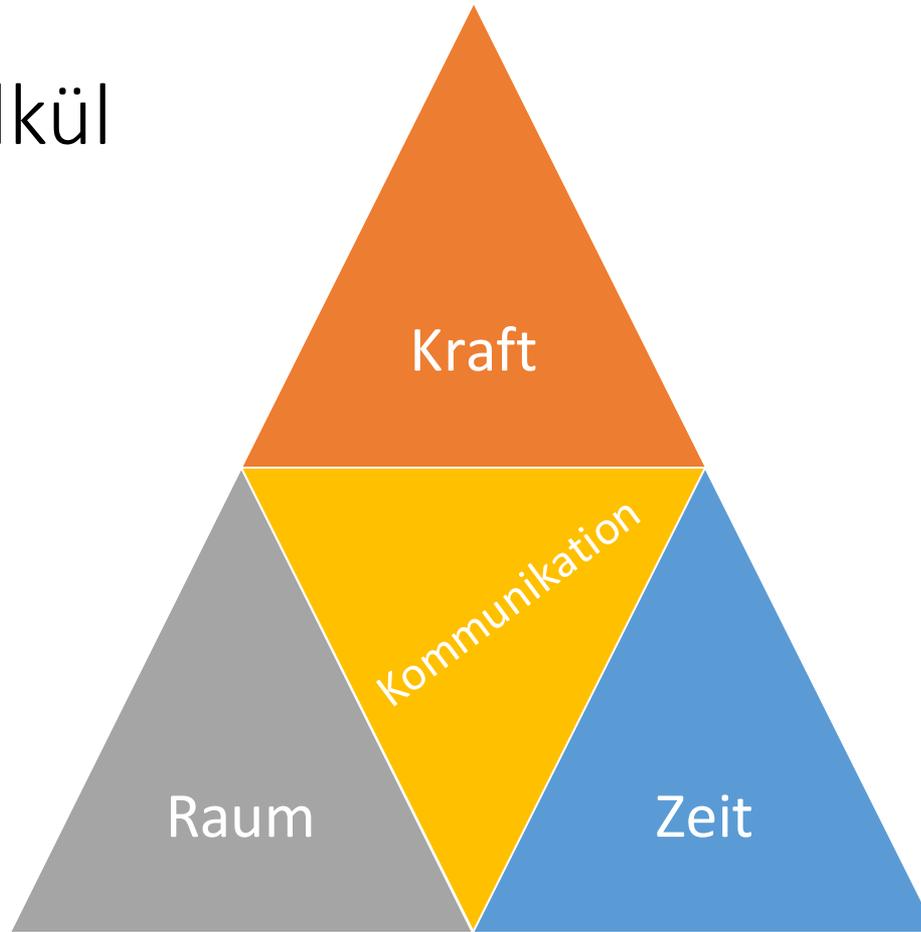
Nur eine nicht (rechtzeitig) getroffene
Entscheidung ist eine falsche
Entscheidung! **(golden hour)**

Oops...

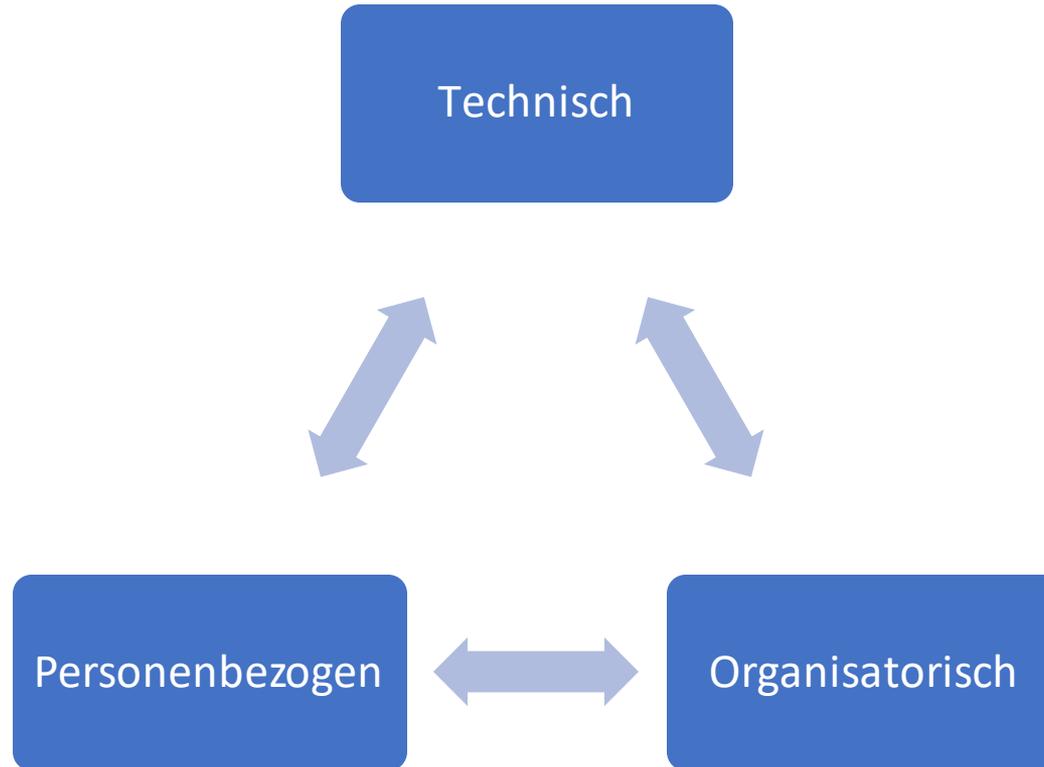
404 Page Not Found



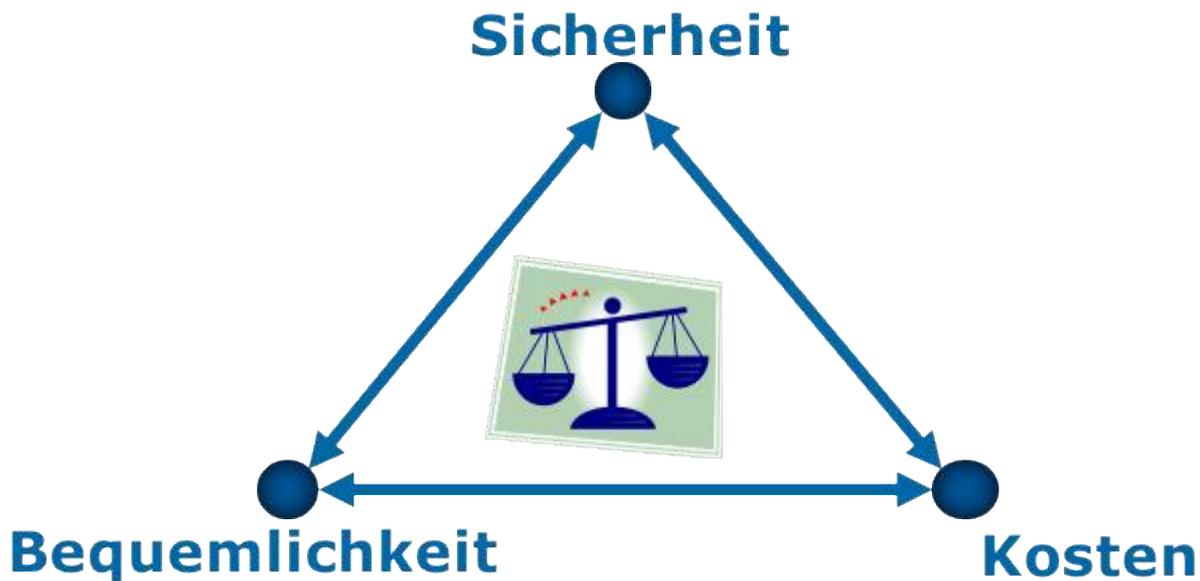
KRZK-Kalkül



TOP-Prinzip der Maßnahmen



Dreieck der Effektivität



Jede Krise ist ein kreativer Prozess



wenn man ihr den Beigeschmack
der Katastrophe nimmt!

e pluribus unum



>> www.sevian7.com

DI Gerald KORTSCHAK
Harald SCHENNER
+43 316 71 39 48

office@sevian7.com



Wir weisen ausdrücklich darauf hin, dass es sich bei den vorliegenden Unterlagen um ein unentgeltliches Service der Autoren handelt und die Informationen keine Unternehmensberatung darstellen. Jegliche Haftung für die Aktualität, Richtigkeit und Vollständigkeit der dargestellten Informationen wird ausgeschlossen.

Alle Rechte, insbesondere das Recht der Vervielfältigung und Verbreitung sowie der Übersetzung, vorbehalten. Kein Teil dieser PowerPoint-Präsentation darf in irgendeiner Form (durch Fotokopie, Mikrofilm oder ein anderes Verfahren) ohne schriftliche Genehmigung der Autoren reproduziert oder unter Verwendung elektronischer Systeme gespeichert, verarbeitet, vervielfältigt oder verbreitet werden.

Die für Schulen und Hochschulen vorgesehene freie Werknutzung „Vervielfältigung zum eigenen Schulgebrauch“ gilt für dieses Werk nicht, weil es seiner Beschaffenheit und Bezeichnung nach nicht zum Unterrichtsgebrauch bestimmt ist.

