BDO Academy

Forensik und Incident Response

Umgang mit Cyber Security Incidents

Jan Starke

BDO Cyber Incident Response & Crisis Center

Vorstellung

Dipl.-Ing. (BA)
Informationstechnik

Dipl.-Softwaretechnologe

Senior Consultant

Cyber Incident & Crisis Center

BDO Cyber Security GmbH

jan.starke@bdosecurity.de

+49 160 96633251

GIAC REVERSE ENGINEERING MALWARE GREM

Bundesamt für Sicherheit in der Informationstechnik
Vorfall-Experte

iSAQB
CPSA-F Foundation Level
1701-CPSAFL-120913-DE

Jan Starke

Senior Consultant

DFIR-Toolkit

ntdsextract2

dissect

TECHNISCHE UNIVERSITÄT DRESDEN

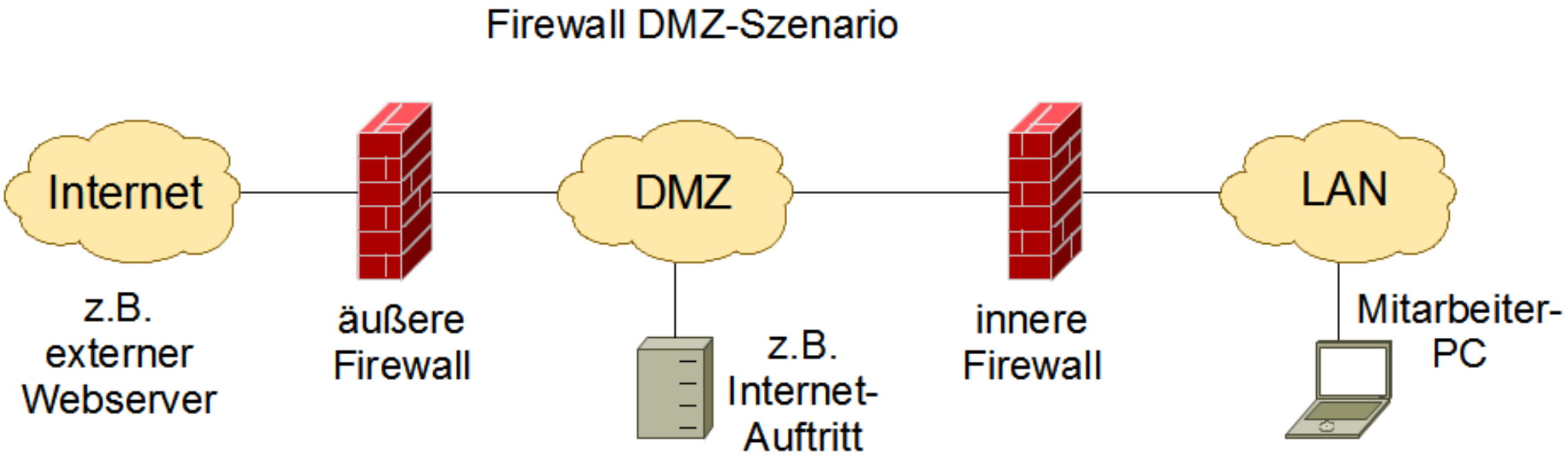
- Teil 1
  - Warum überhaupt Incident Response?
  - Die Bedrohungslage
  - Die Angreiferseite
  - Die Verteidigerseite
  - No-Go‘s im Incident Response
- Teil 2

Warum überhaupt Incident Response?

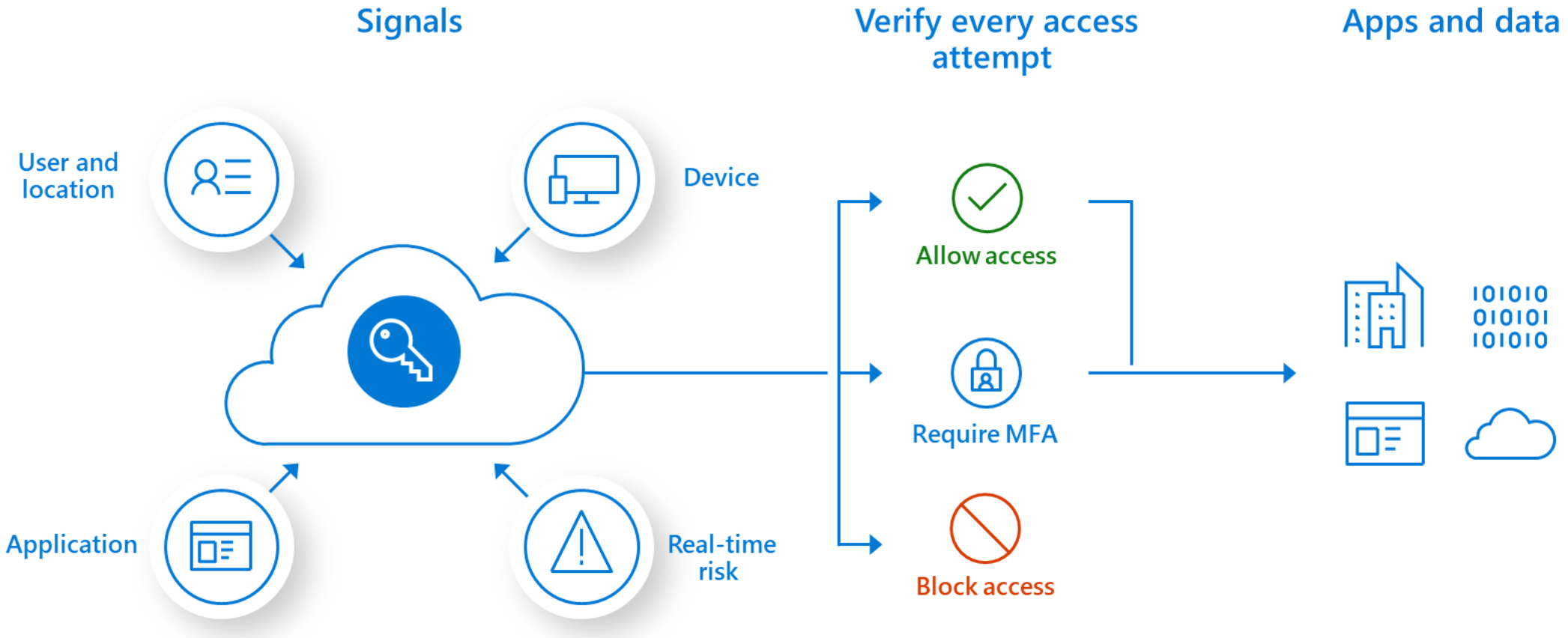
Prävention

Quelle: https://www.robl.de/pentagramm/kulturgeschichte/jericho.html

Prävention



Zero-Trust

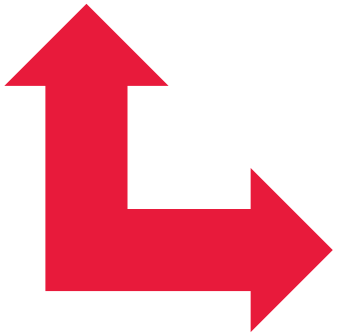


Quelle: https://www.microsoft.com/de-de/microsoft-365/blog/2019/09/18/why-banks-adopt-modern-cybersecurity-zero-trust-model/

Robustheit vs. Resilienz

Robustheit

aka die „Fähigkeit, zu widerstehen“



Resilienz

von lateinisch resilire ‚abprallen‘ oder ‚zurückspringen‘

aka die Fähigkeit, sich zu erholen

„Resilienz bedeutet auch in diesem Kontext, dass ein [Unternehmen] nach einem negativen Schock […] weiter existiert und wieder auf das Ausgangsniveau vor dem Schock zurückfindet“ (https://de.wikipedia.org/wiki/Resilienz_(Betriebswirtschaftslehre))

Ziel des Workshops

Resilienz: Fähigkeit zur Isolation und Regeneration

Die Bedrohungslage

Informationsaustausch

Das Traffic Light Protocol (TLP)

First Traffic Light Protocol 2.0 (https://www.first.org/tlp)	TLP: CLEAR	TLP: GREEN	TLP: AMBER	TLP: AMBER+STRICT	TLP: RED
Persönlich, nur für bekannte Empfänger	✓	✓	✓	✓	✓
Eingeschränkte interne Weitergabe	✓	✓	✓	✓	×
Eingeschränkte interne und organisationsübergreifende Weitergabe	✓	✓	✓	×	×
Organisationsübergreifende Weitergabe	✓	✓	×	×	×
Unbegrenzte Weitergabe	✓	×	×	×	×

Bedrohungslage: Informationsquellen

- Bundesamt für Sicherheit in der Informationstechnik (BSI) → https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html
- Bundeskriminalamt (BKA) → https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2023.html
- Warn- und Informationsdienst CERT Bund → https://wid.cert-bund.de/portal/wid/start
- Statista → https://de.statista.com/themen/2371/internetkriminalitaet-in-deutschland/#topicOverview
- Microsoft Digital Defense Report → https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023
- …

Motivation von Angreifern

- Geld
- Politische Ziele
- Militärische Ziele
- Wirtschaftliche Ziele (Konkurrenz)
- Rache
- Reputation

Quelle: https://cyberscoop.com/russian-cybercrime-raids-cryptex-uaps/ (02.10.2024)

Kategorisierung von Angreifern

- Cyber-Aktivistinnen und Cyber-Aktivisten
- Cyber-Kriminelle
- Konkurrenzausspähung/Industriespionage im Cyber-Raum
- Staatliche Nachrichtendienste im Cyber-Raum
- Staatliche Akteure im Cyber-War
- Cyber-Terroristinnen und Cyber-Terroristen
- Hobbyisten/Skript-Kiddies
- Innentäterinnen und Innentäter
- IT-Sicherheitsforscherinnen und IT-Sicherheitsforscher

Motivation von Angreifern

Wichtig!

Cyber-Sicherheitsvorfälle sind keine Naturereignisse!

Cyber-Sicherheitsvorfälle werden *bewusst* und *planvoll* herbeigeführt!

(unter Berücksichtigung Ihrer Schutzmaßnahmen)

Average cost of a data breach worldwide from May 2020 to February 2024, by industry (in million U.S. dollars)

Average total cost per data breach worldwide 2020-2024, by industry

	May 2020 - Mar 2021	Mar 2021 - Mar 2022	Mar 2022 -Mar 2023	Mar 2023 -Feb 2024
Healthcare	9.23	10.1	10.93	9.77
Financial	5.72	5.97	5.9	6.08
Pharmaceuticals	5.04	5.01	4.82	5.1
Technology	4.88	4.97	4.66	5.45
Energy	4.65	4.72	4.78	5.29
Professional services	4.65	4.7	4.47	5.08
Industrial	4.24	4.47	4.73	5.56
Global average	4.24	4.35	4.45	4.88
Research	3.6	3.88	3.63	3.54
Education	3.79	3.86	3.65	3.5
Consumer	3.7	3.86	3.8	3.91
Entertainment	3.8	3.83	3.62	4.09
Communications	3.62	3.62	3.9	4.09
Transportation	3.75	3.59	4.1	

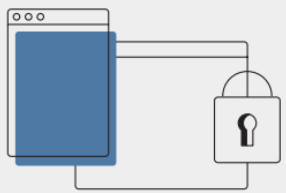
Description: Between March 2022 and February 2024, the highest average cost of a data breach, nearly 9.77million U.S. dollars, was detected in the healthcare industry. The financial sector ranked second, with 6.08 million U.S. dollars on average per breach. The global average data breach cost in the measured period was 4.88 million U.S. dollars. Data breaches in the public sector cost relatively low, an average of 2.55 million U.S. dollars during the measured period. Read more
Note(s): Worldwide; May 2020 to February 2024
Source(s): IBM; Ponemon Institute

Die Lage der IT-Sicherheit in Deutschland 2023 im Überblick

Ransomware

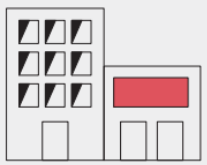
ist weiterhin die größte Bedrohung.

2 **Ransomware-Angriffe** auf Kommunalverwaltungen oder kommunale Betriebe wurden durchschnittlich pro Monat bekannt.



68 erfolgreiche **Ransomware-Angriffe auf Unternehmen** wurden bekannt.

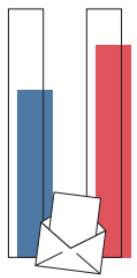
15 davon richteten sich gegen **IT-Dienstleister**.



Mehr als **2.000** **Schwachstellen** in Software-Produkten **(15 % davon kritisch)** wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein **Zuwachs von 24 %.**

Eine Viertelmillion
neue **Schadprogramm-Varianten** wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.

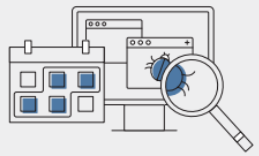
66%
aller **Spam-Mails** im Berichtszeitraum waren Cyberangriffe:
34% Erpressungsmails,
32% Betrugsmails



84%
aller betrügerischen E-Mails waren **Phishing-E-Mails** zur Erbeutung von Authentisierungsdaten, meist bei Banken und Sparkassen.

Top 3-Bedrohungen je Zielgruppe:

Gesellschaft	Wirtschaft	Staat und Verwaltung
		
Identitätsdiebstahl Sextortion Phishing	***Ransomware*** Abhängigkeit innerhalb der IT-Supply-Chain Schwachstellen, offene oder falsch konfigurierte Online-Server	***Ransomware*** APT Schwachstellen, offene oder falsch konfigurierte Online-Server



Rund **21.000** **infizierte Systeme** wurden täglich im Berichtszeitraum erkannt und vom BSI an die deutschen Provider gemeldet.

Durchschnittlich rund **775** **E-Mails mit Schadprogrammen** wurden an jedem Tag im Berichtszeitraum in deutschen Regierungsnetzen abgefangen.

370 **Webseiten** wurden im Durchschnitt an jedem Tag des Berichtszeitraums für den Zugriff aus den Regierungsnetzen gesperrt. **Der Grund:** Die Seiten enthielten Schadprogramme.

6.220 (2022)
5.100 (2021)

7.120 Teilnehmer hatte die **Allianz für Cyber-Sicherheit** im Jahr 2023.

Deutschland **Digital•Sicher•BSI•**

Bedrohungslage

Bundeslagebericht Cybercrime 2023

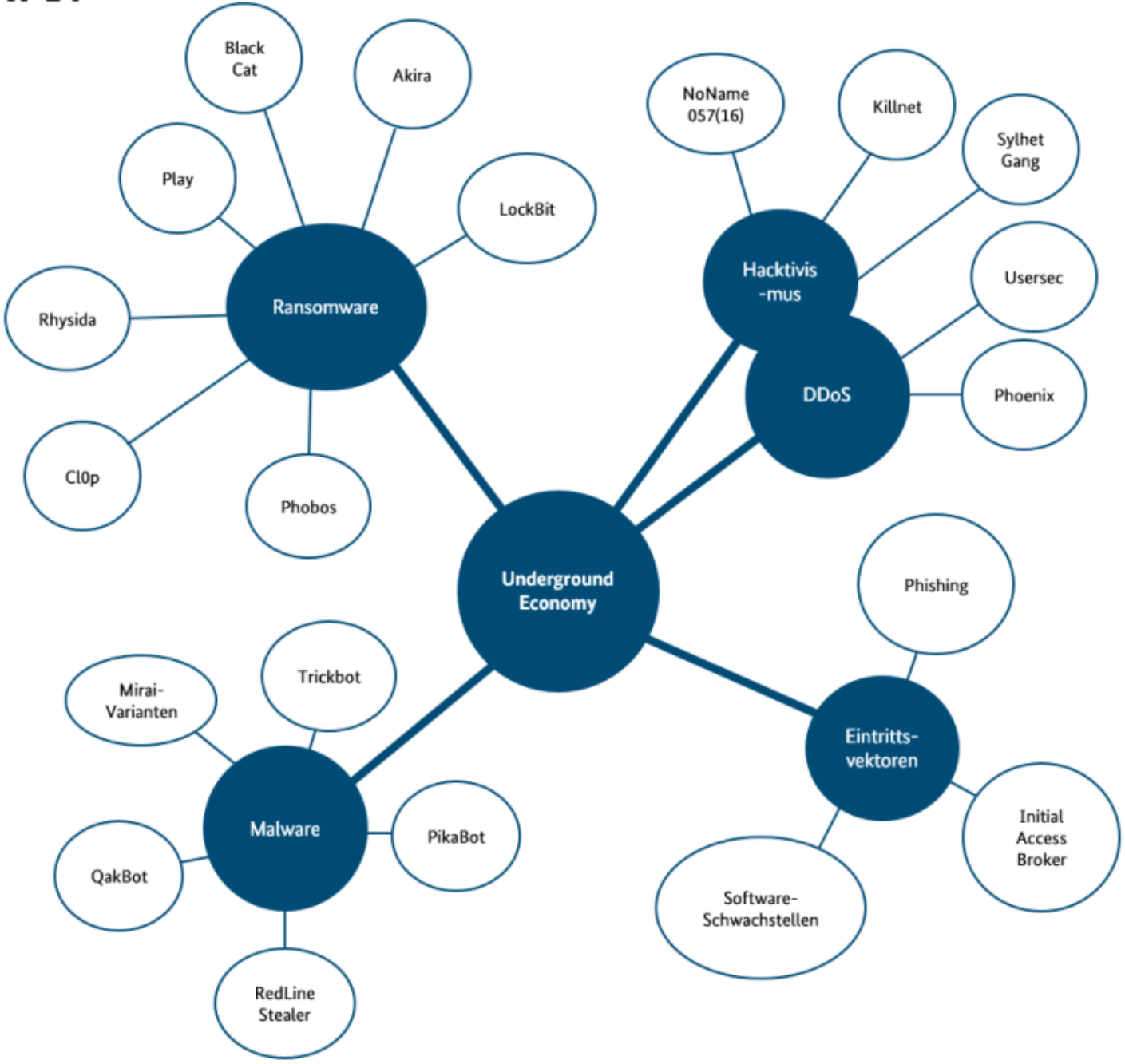
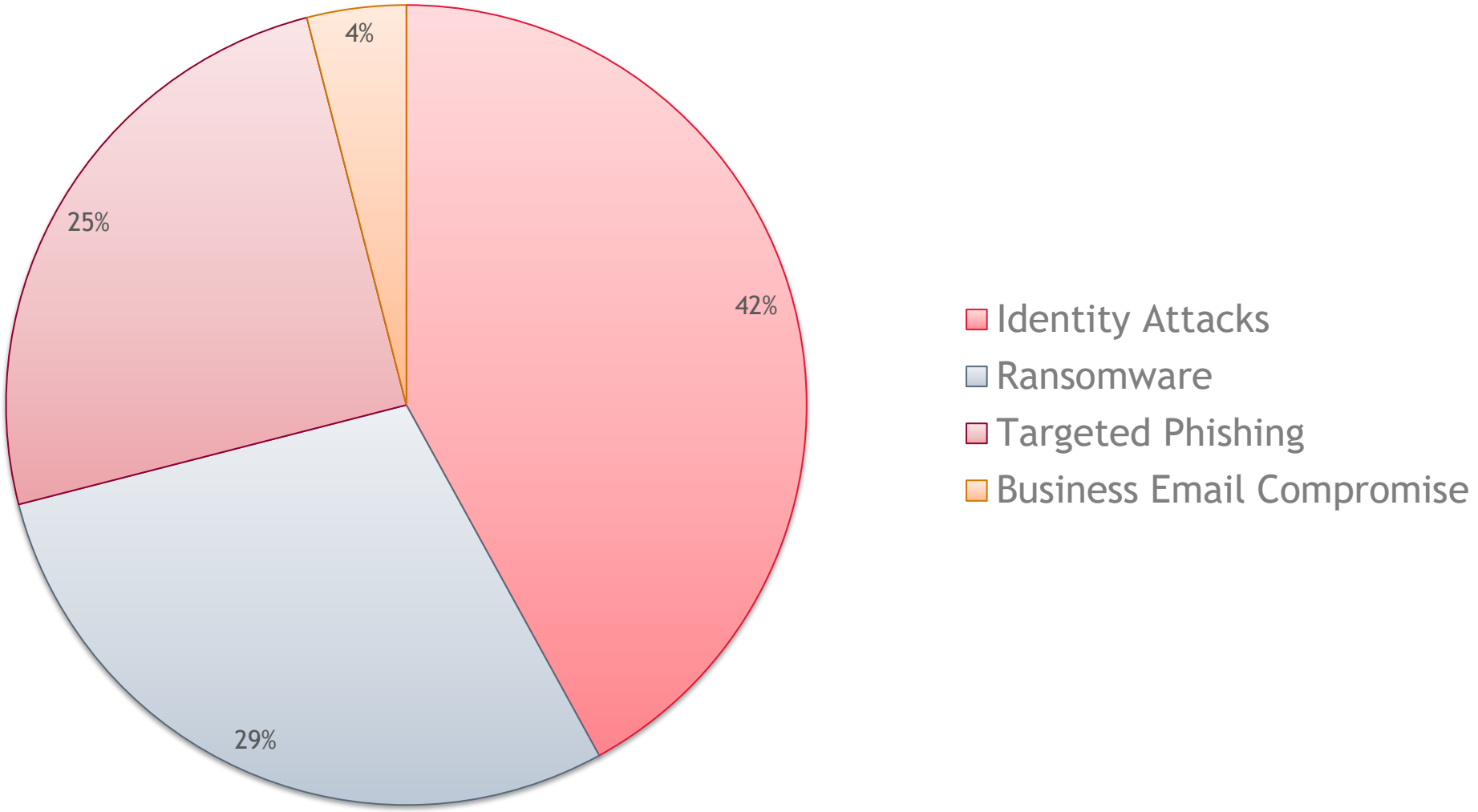


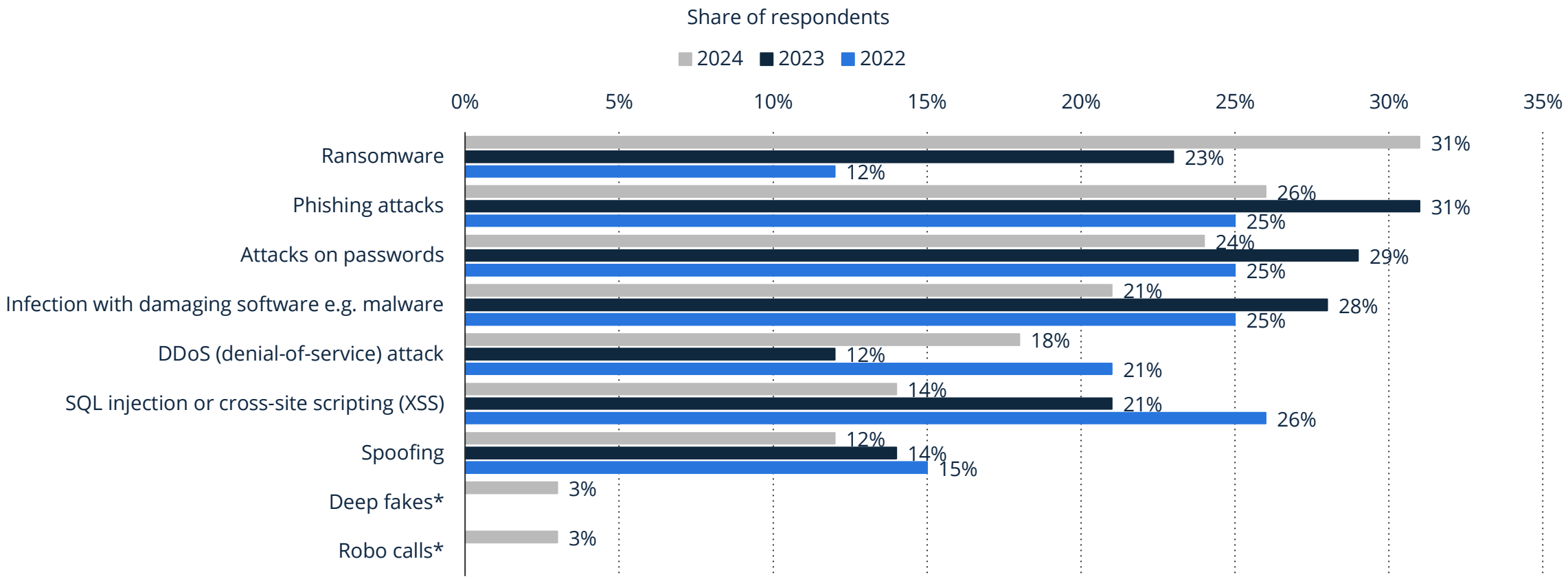
Abbildung 1: Relevante Bedrohungen der Cyberkriminalität 2023

Die häufigsten Angriffsvarianten (Quelle MDDR)



Cyberattacks companies have suffered in Germany from 2022 to 2024

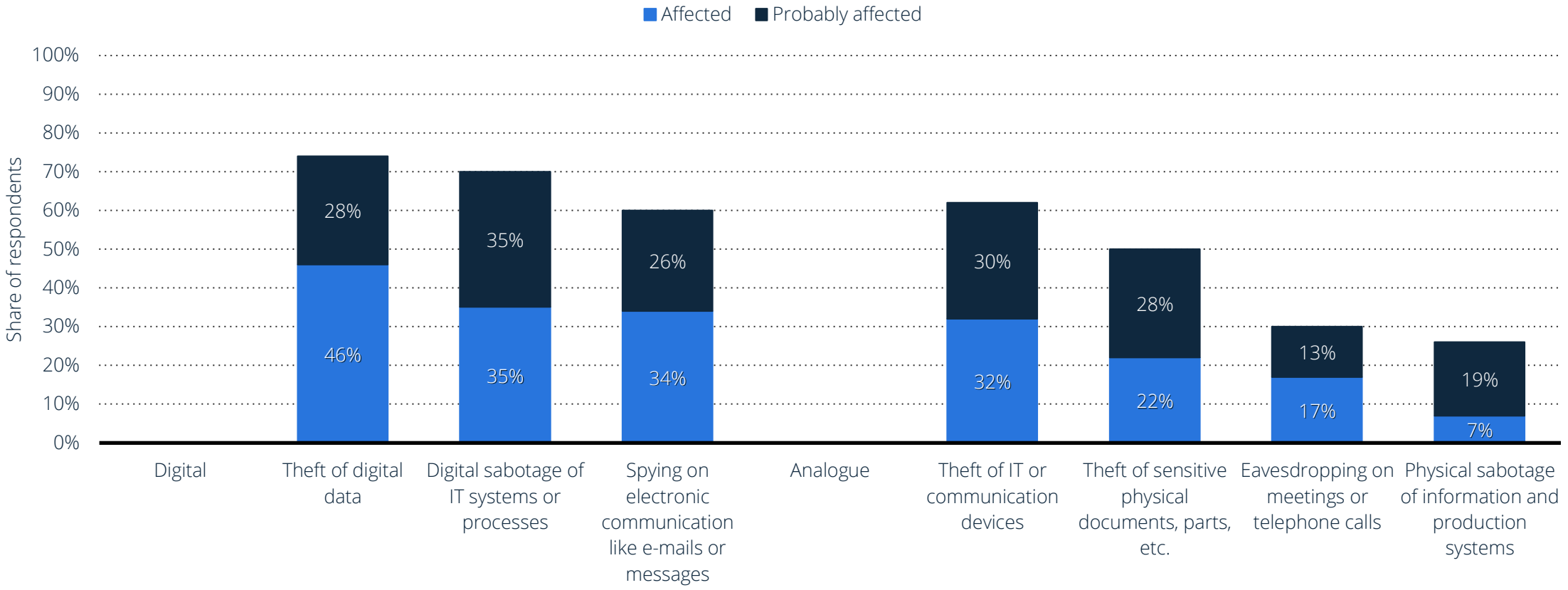
Cyberattacks companies have suffered in Germany 2022 to 2024



Description: In 2024, the most common cyberattacks against German companies were ransomware attacks, attacks on passwords and phishing attacks. Three percent of companies suffered deep fake attacks, which have become an easy scam for people to fall for since the development of AI. Read more
Note(s): Germany; CW 16 to CW 24, 2024; 1,003 respondents
Source(s): Bitkom

What types of security incidents concerning IT have you encountered in your company in the last year?

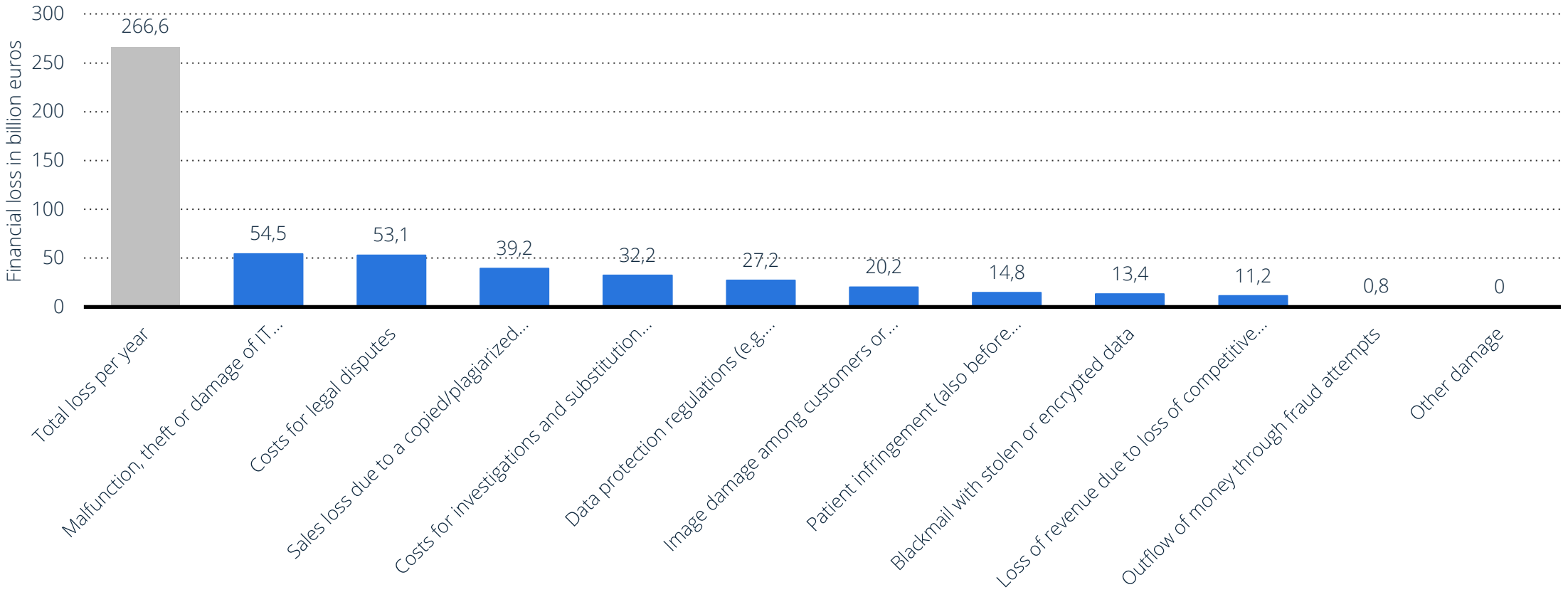
Types of cybercrime in companies in Germany 2024



Note(s): Germany; CW 16 to CW 24, 2024; 1,003 respondents
Further information regarding this statistic can be found on page 8.
Source(s): Bitkom; ID 429635

Financial damage from cybercrime in Germany in 2024 (in billion euros)

Financial loss from cybercrime in Germany 2024



Note(s): Germany; CW 16 to CW 24 2024; 1,003 respondents
Further information regarding this statistic can be found on page 8.
Source(s): Bitkom; ID 1360289

Threat Actors

Die 9 Säulen des Cyber Crime (BKA)

Foren und Jabber-Server

Bulletproofhosting & Proxyprovider

Marktplätze, Shops und Automated Vending Carts (AVC)

Malwareentwicklung & Coding

Malware Crypting & Obfuscation

Counter-Antivirus-Services (CAV)

Malware Delivery & Infection on Demand & PPI

Drops, Mules & Cashout

Exchanger - Die digitale Geldwäsche

Threat Actors

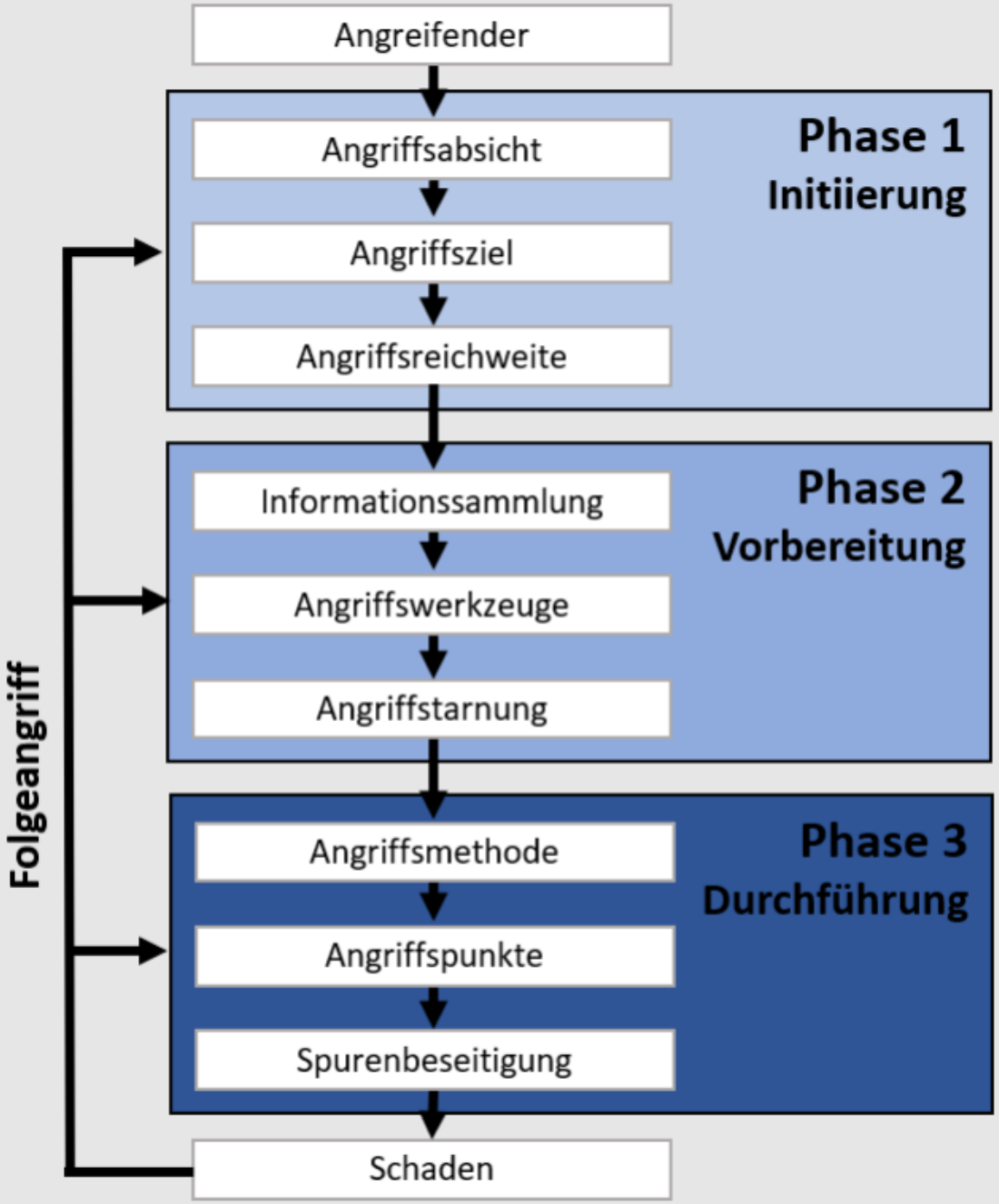
The Q3-2024 Ransomware Malicious Quartile

Figure 1: Top Threat Groups for Ransomware-as-a-Service Ecosystem

Quelle: https://www.halcyon.ai/raas-mq/power-rankings-ransomware-malicious-quartile-q3-2024

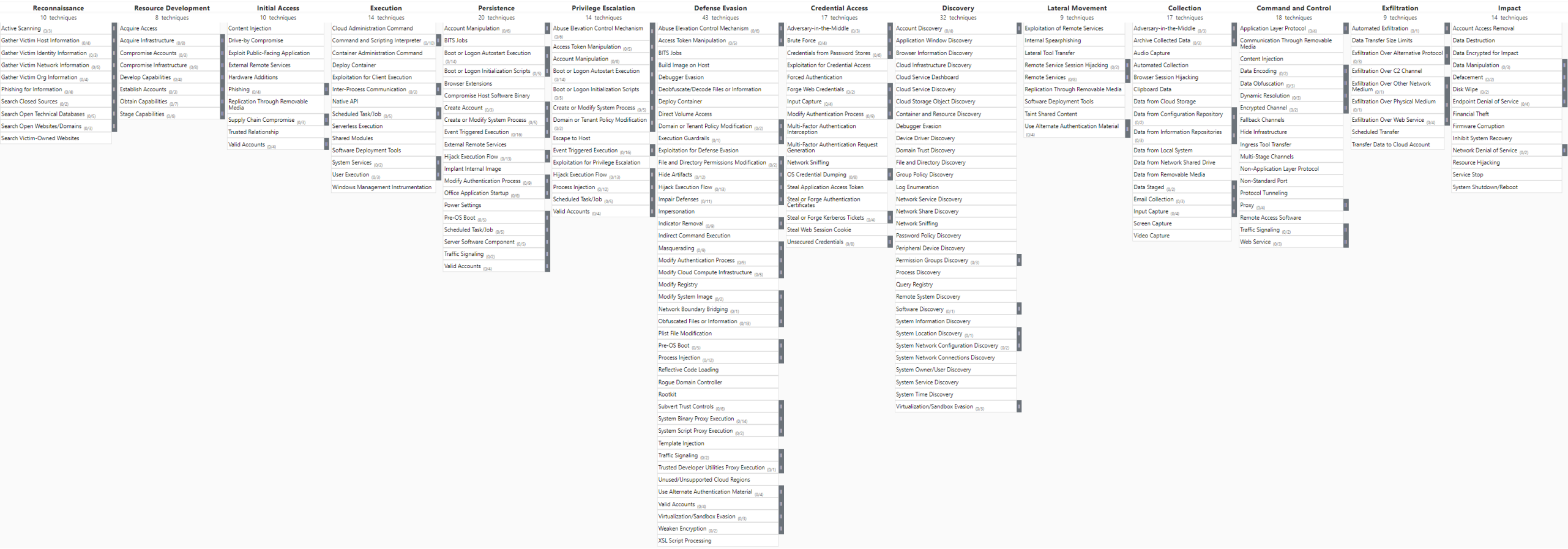
Phasen eines Cyber-Angriffs

Quelle: Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Vorfall-Praktiker und Vorfall-Experten



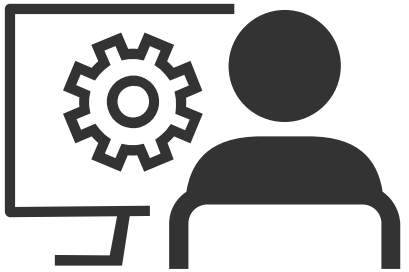
Phasen eines Angriffs

MITRE ATT&CK Matrix



Phasen eines Angriffs

- Reconnaissance
- Weaponization and Delivery
- Exploitation
- Installation
- Command and Control



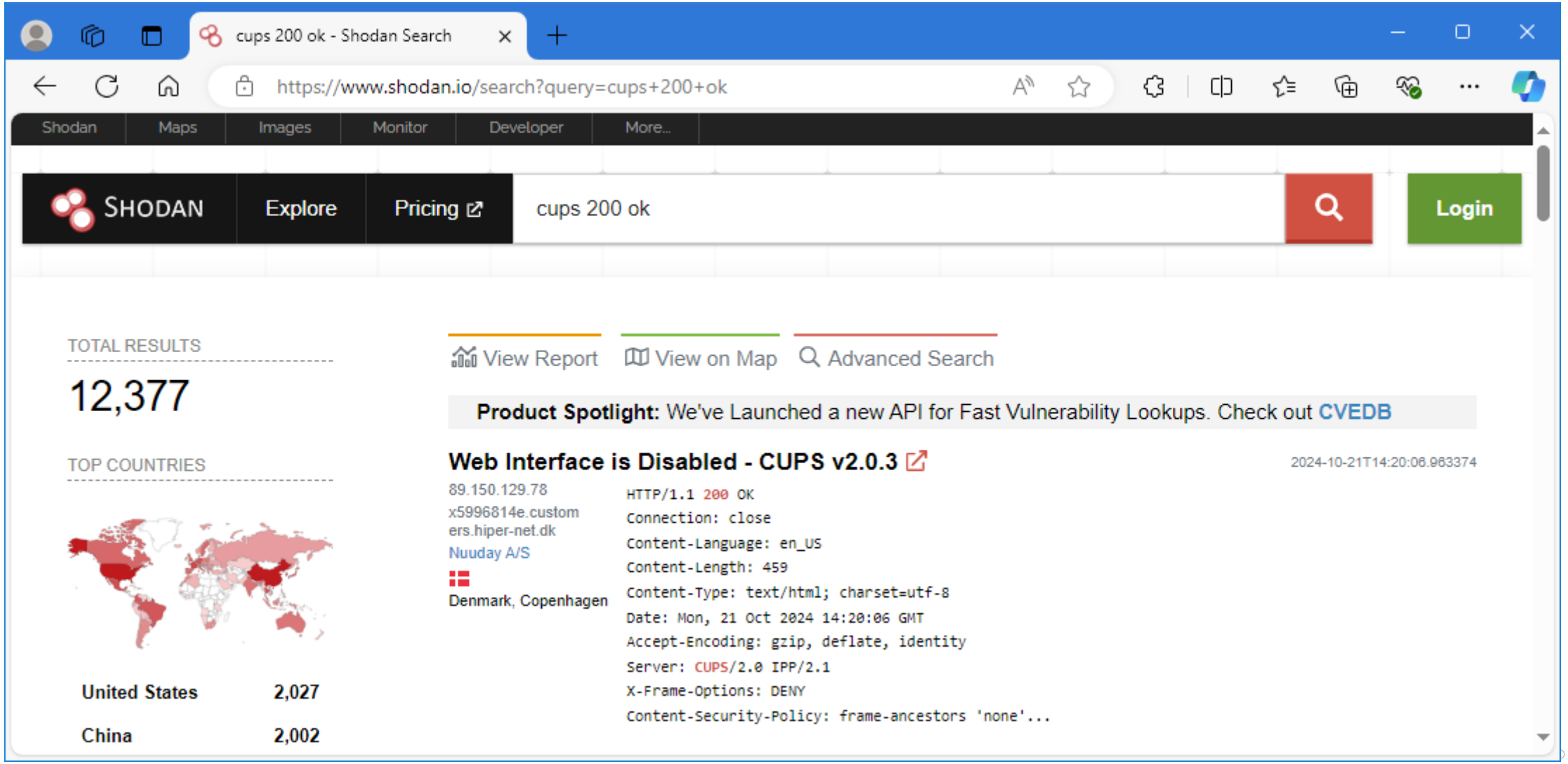
- Detection
- Isolation
- Emergency Operations
- Recovery
- Normal mode

Die Angreiferseite

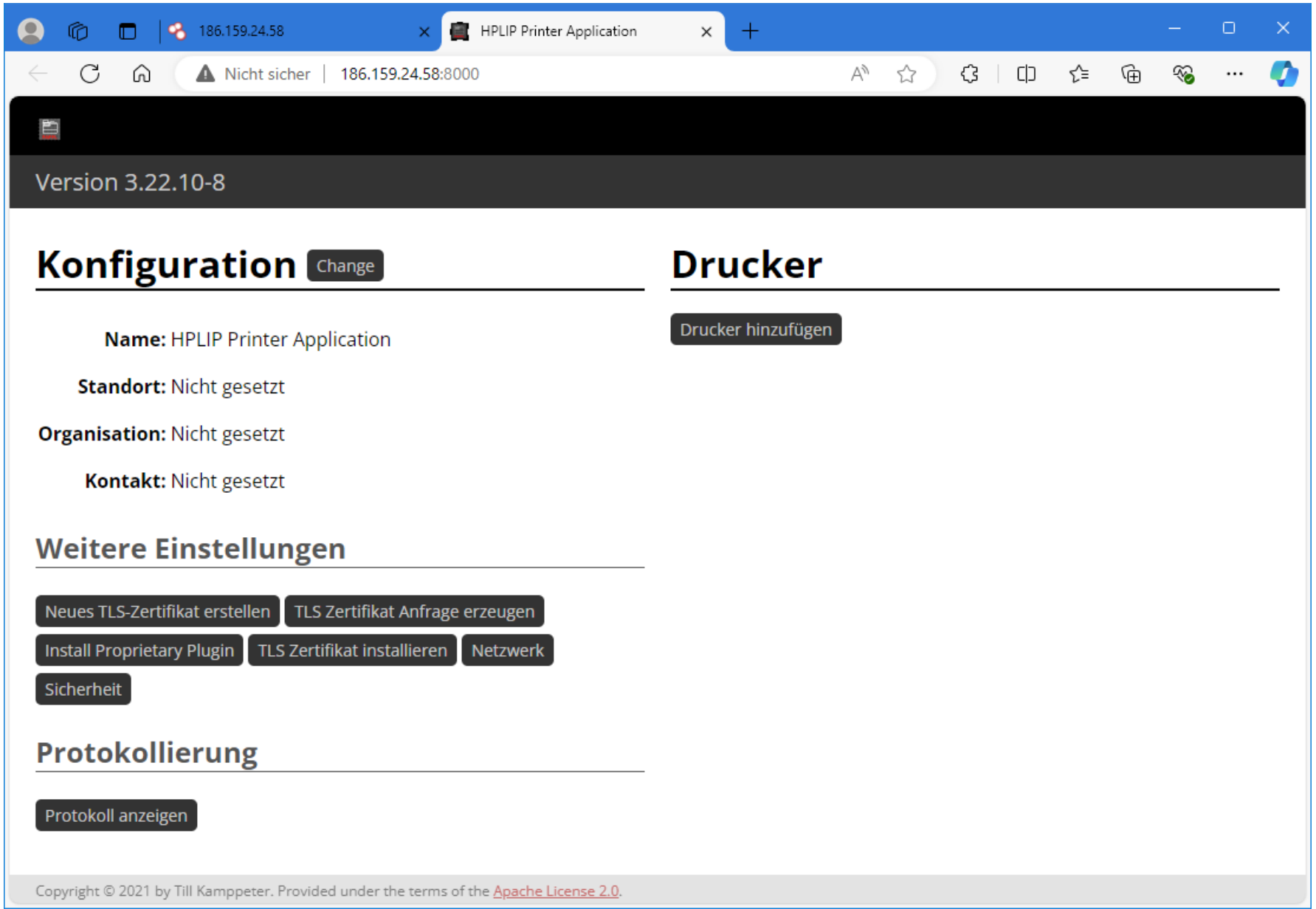
Reconnaissance

- Physischer Zugang
- Beeinflussbare Mitarbeiter (Bestechung, Erpressung)
- Mitarbeiter mit besonderen Rechten
- Exponierte Systeme
- Verwundbare Systeme
- Externe Dienstleister
- Jahresumsatz
- Verbindungen zu anderen Unternehmen

Reconnaissance

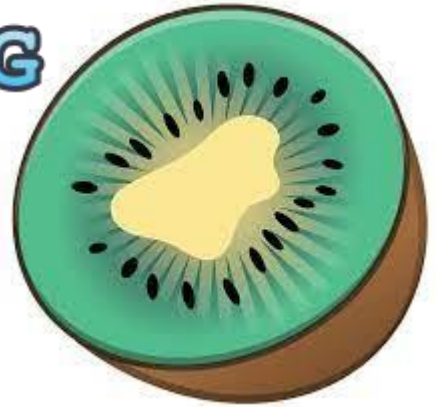


Reconnaissance



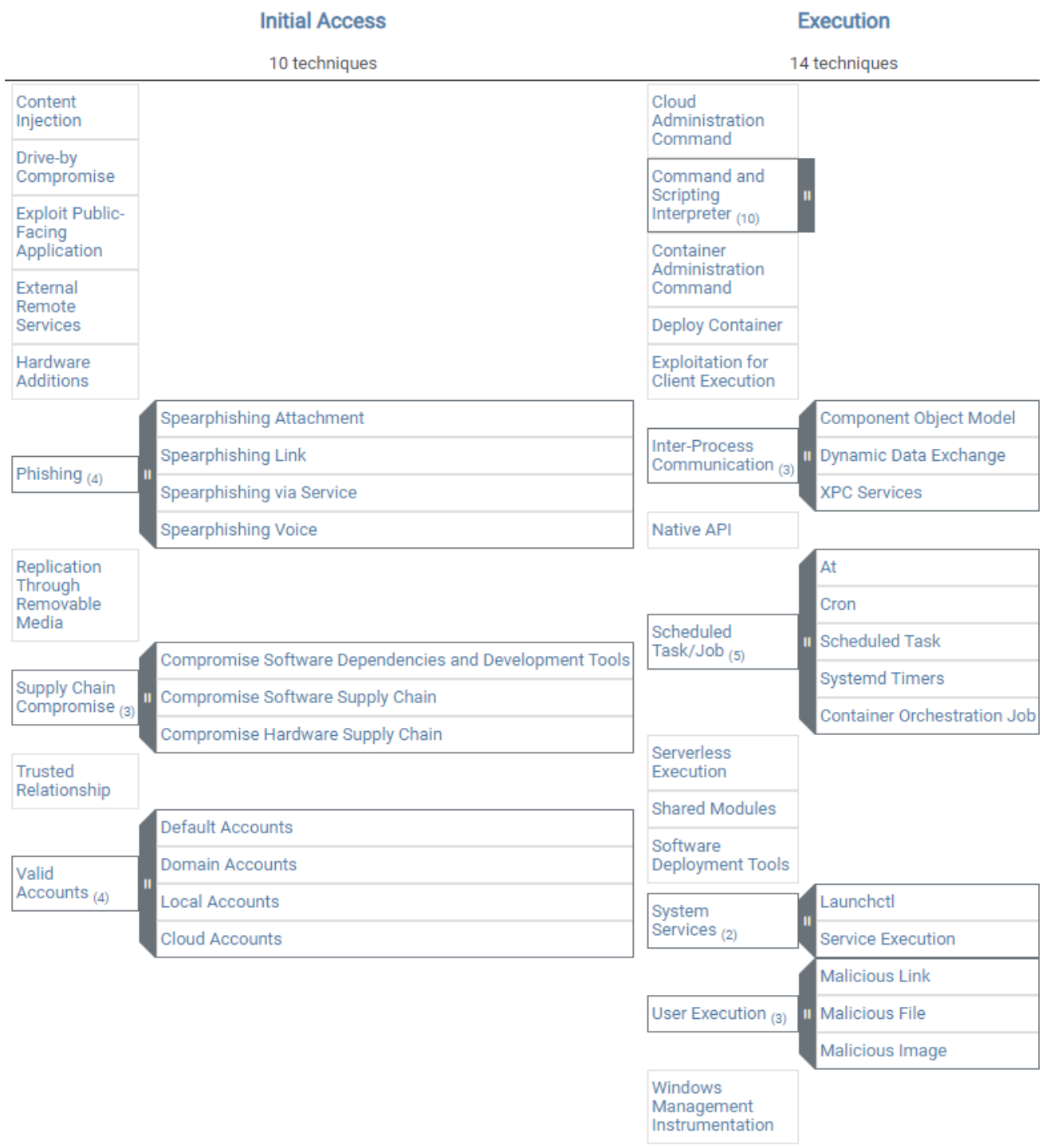
Weaponization and Delivery

Metasploit



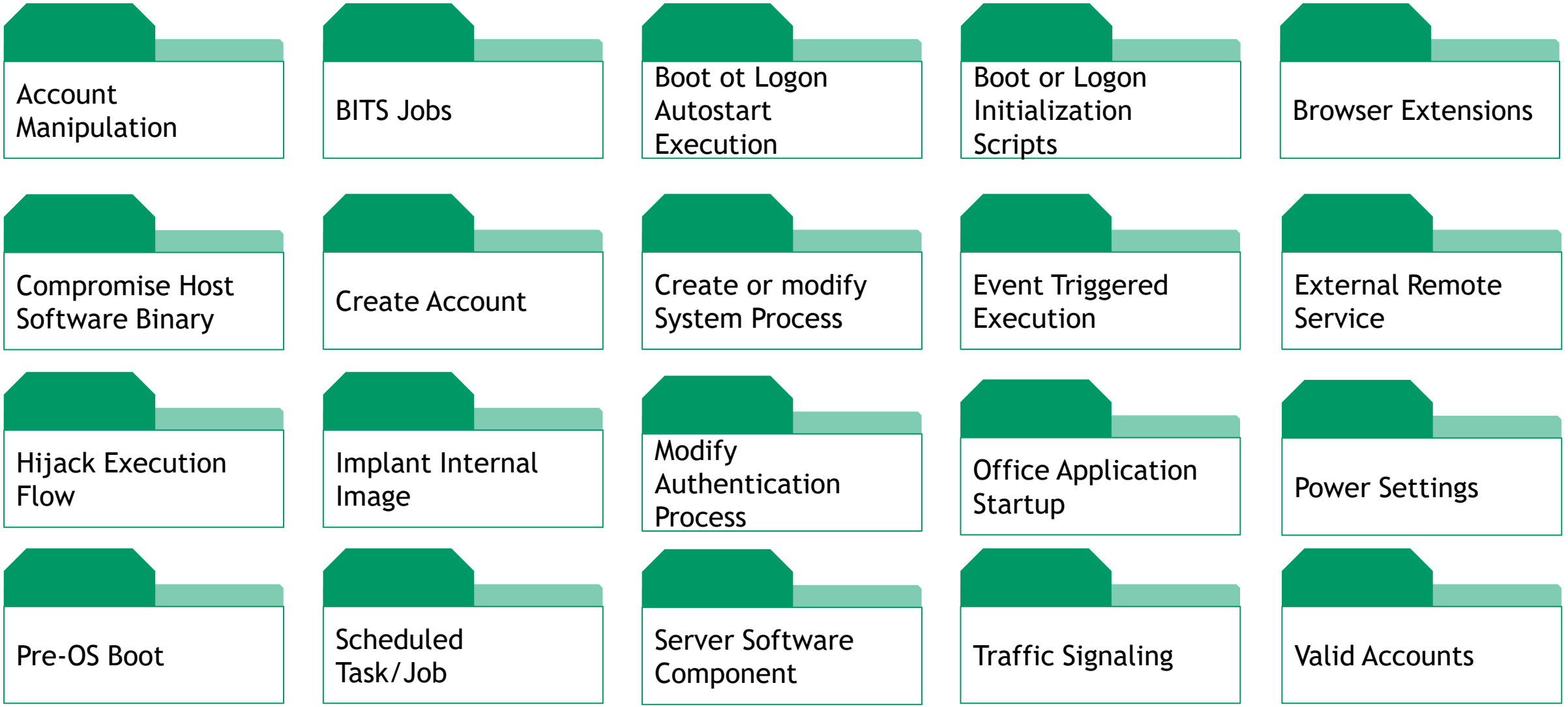
Exploitation

(MITRE ATT&CK

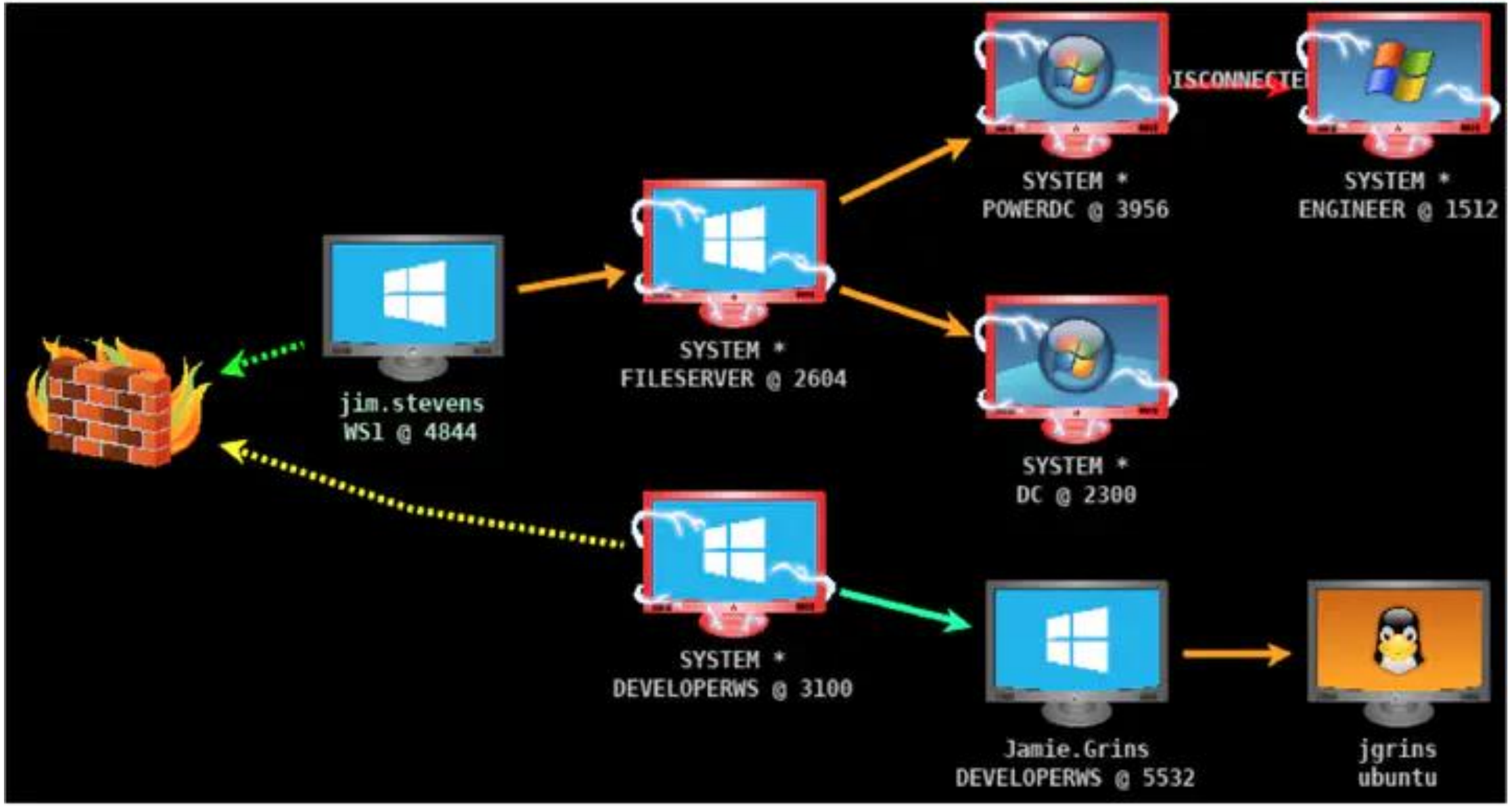


Installation

MITRE ATT&CK Persistence



Command and Control

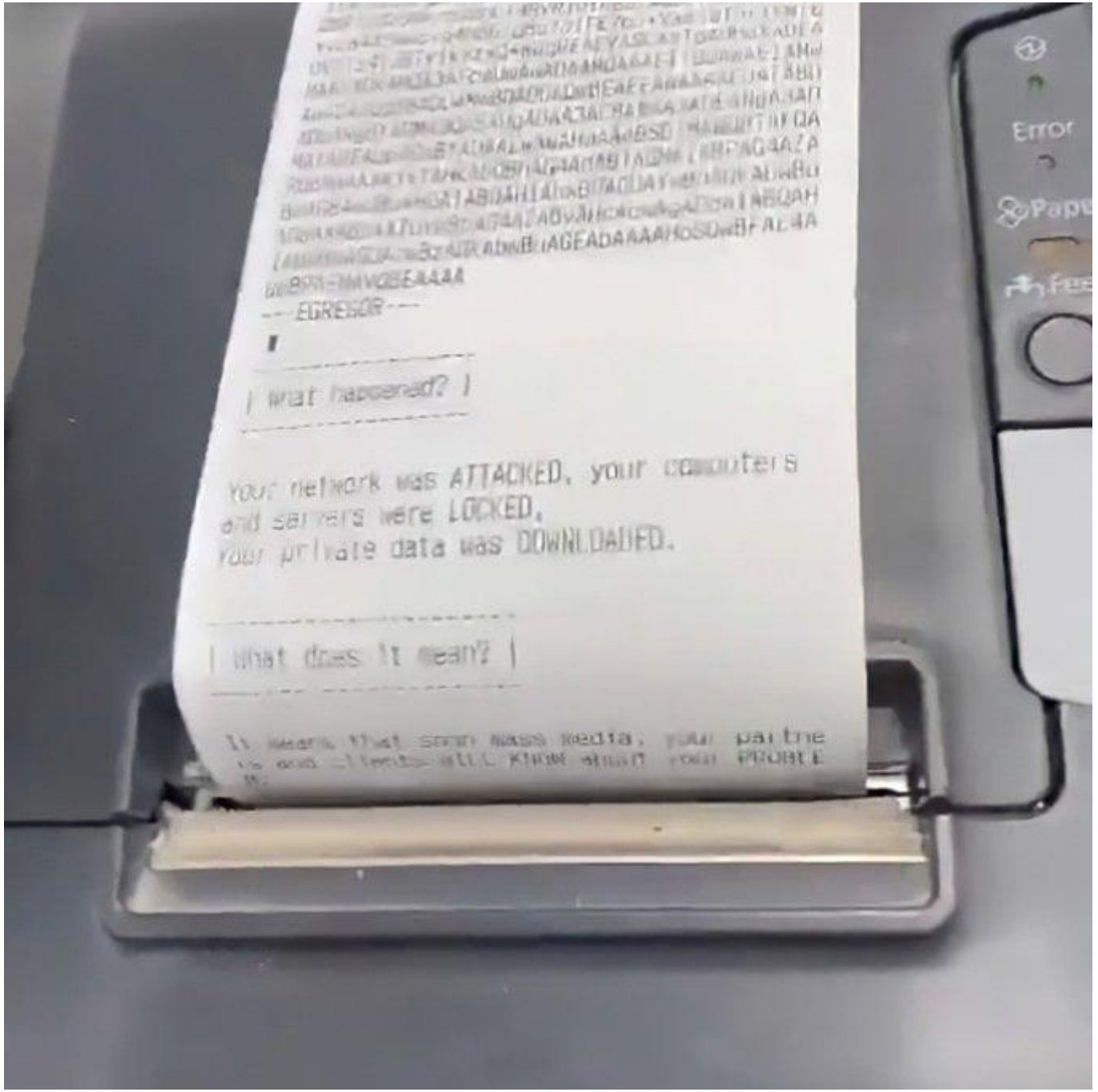


Command and Control

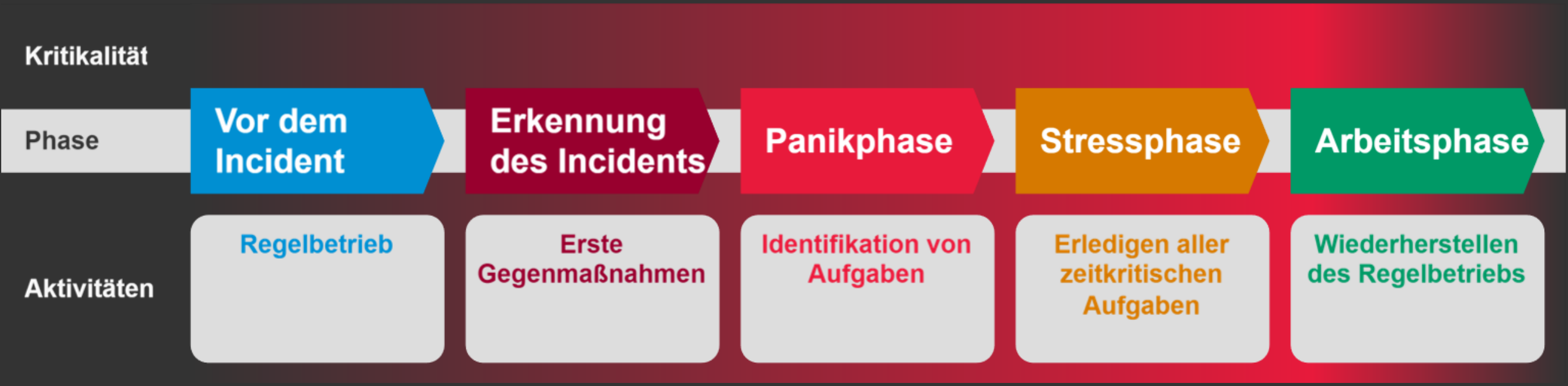
C2-Protokolle

Die Verteidigerseite

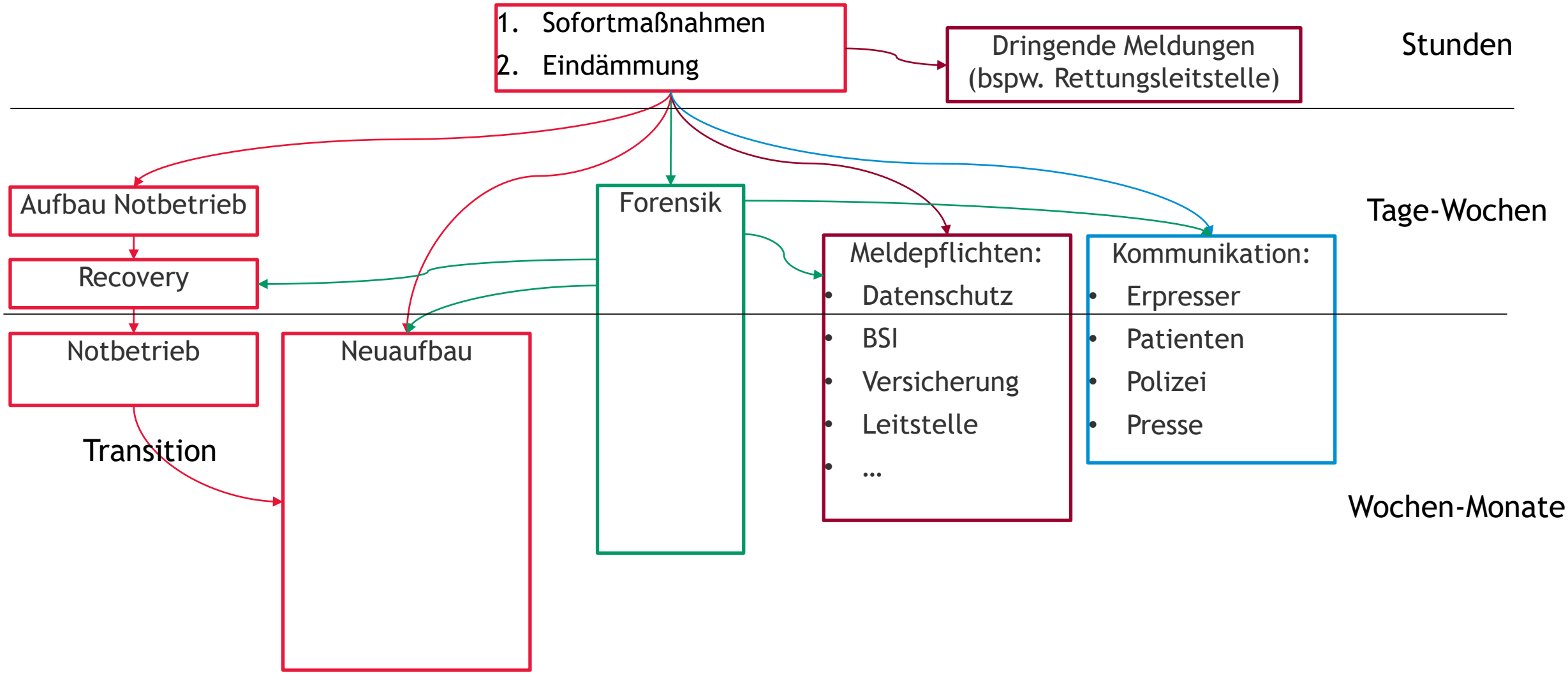
Das böse Erwachen



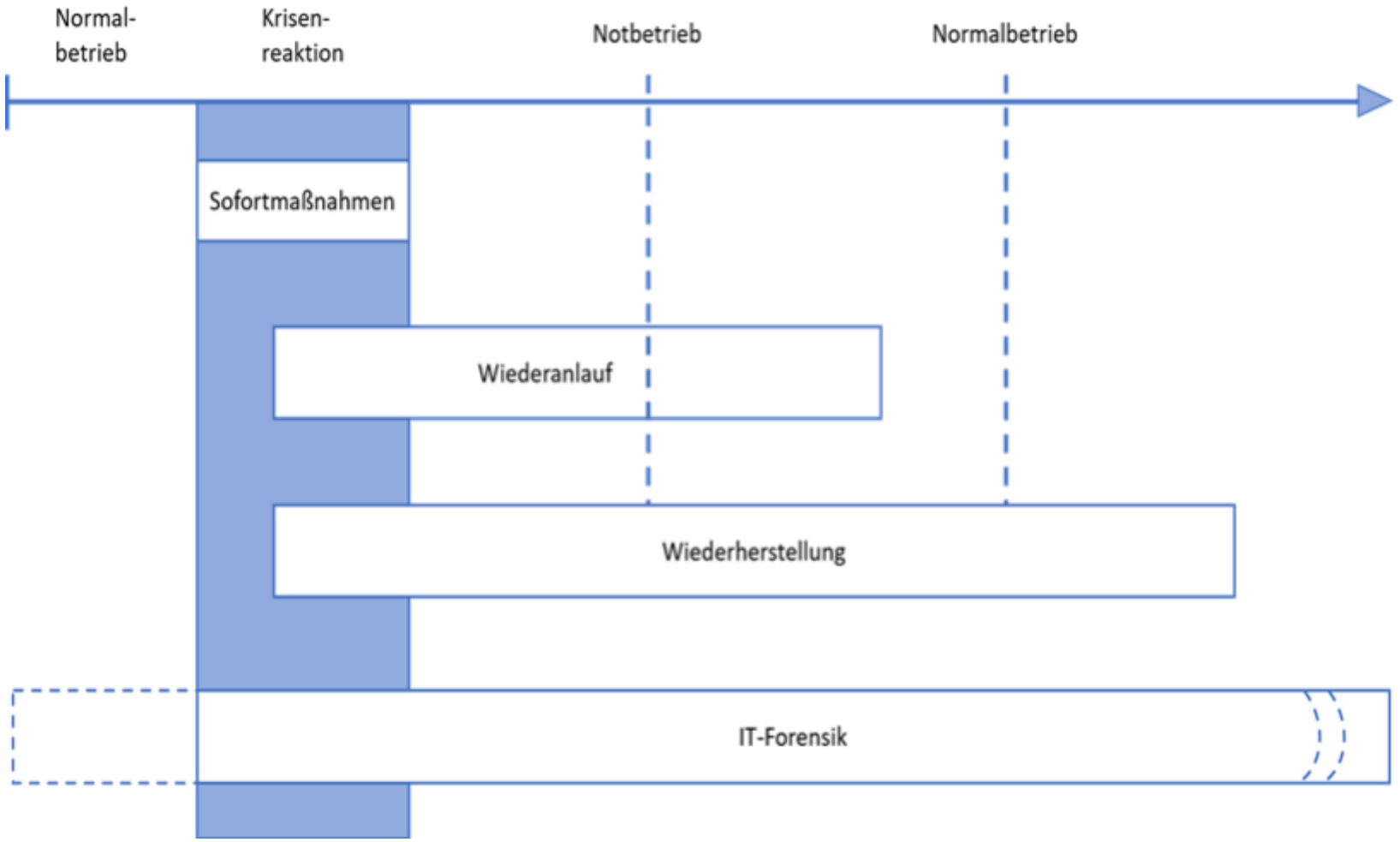
Security Incidents: Die Panikphase



Reaktion auf Vorfälle



Zeitliche Einordnung der Forensik



Quelle: Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Vorfall-Praktiker und Vorfall-Experten

Sofortmaßnahmen I

Ziele

- Eingrenzen des Schadens
- Minimierung der Betriebsunterbrechung

Sofortmaßnahmen II

Ziele

- Eindämmung

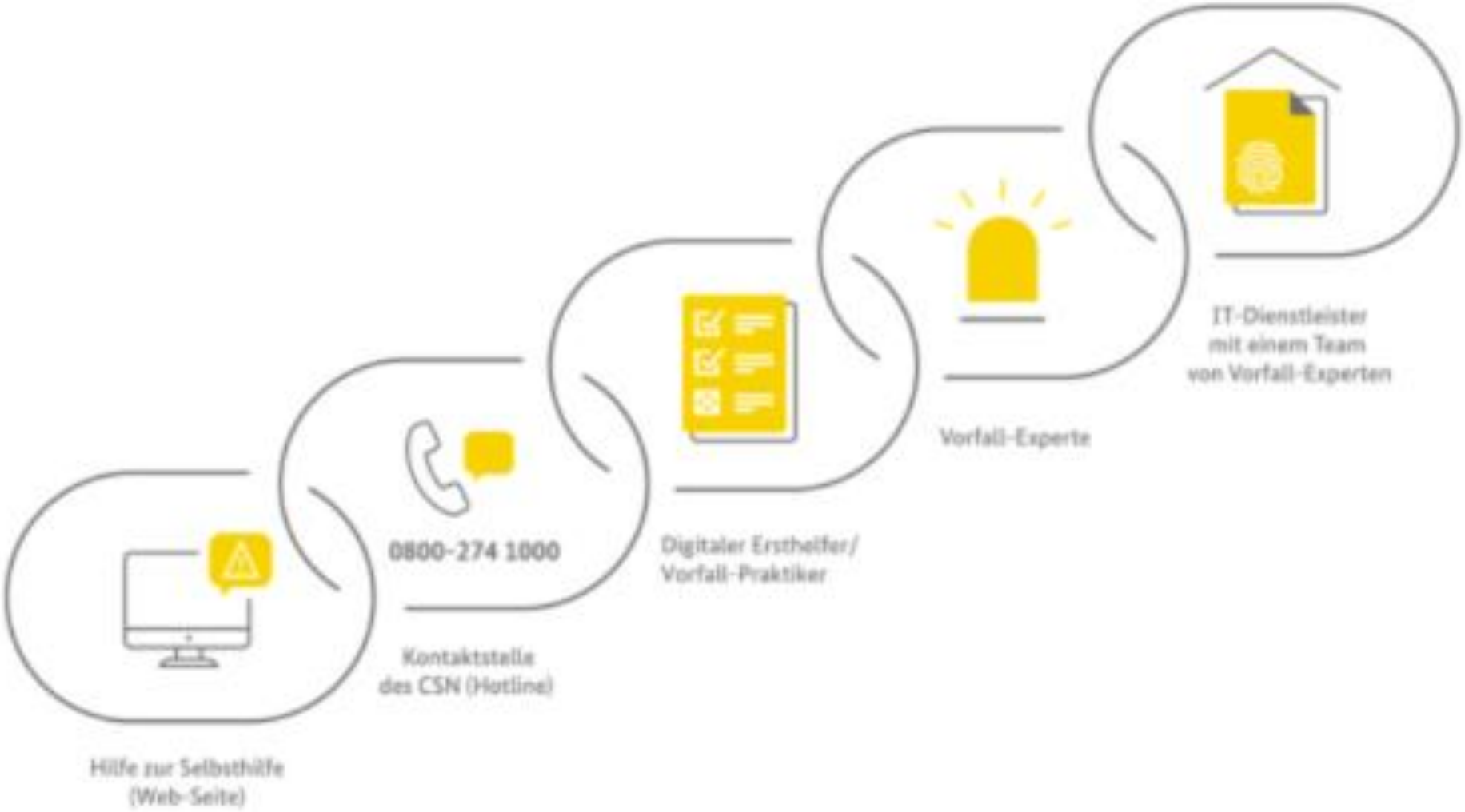
Eindämmung

aka **Einschränkung der Verfügbarkeit** aka **Betriebsunterbrechung**

- Benutzerkonten sperren
- Passwörter zurücksetzen
- VPN unterbrechen
- VLANs trennen
- FW-Regeln deaktivieren
- Server ausschalten
- Netzwerkkabel ziehen
- Stromversorgung unterbrechen
- …

Incident melden

Die digitale Rettungskette



Incident melden

(ohne Gewähr)

- Organisationsinterne Meldepflichten beachten!
- Versicherung
- Brand- und Katastrophenschutzamt bzw. IRLS (Anpassung Alarm- und Einsatzplan)
- Benachbarte Krankenhäuser

- Datenschutz
  - BDSG / PDSG → Meldung an DSB

- Kritische Infrastrukturen
  - KRITIS / NIS-2 → Meldung an BSI

- Weitere ?

Nächste Schritte

- Notfallplan aktivieren
- Beteiligte Akteure informieren
- Notfallkommunikation einrichten
- Status tracken
- Entscheidungen dokumentieren
- Durchgeführte Maßnahmen dokumentieren

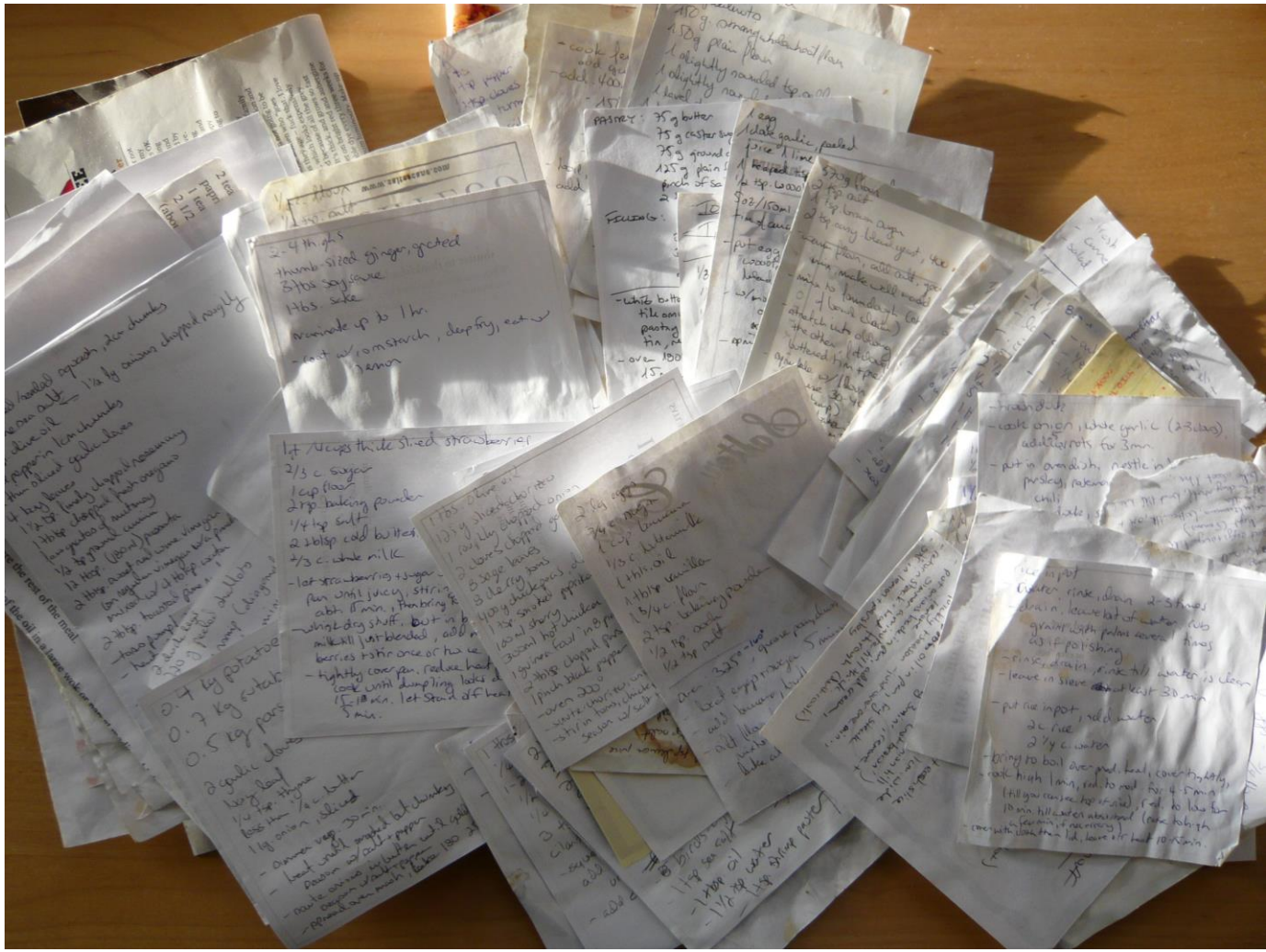
- Ursachen untersuchen → Forensik

No-Go‘s im Incident Response

Unzureichende Dokumentation

Zielgruppen der Dokumentation:

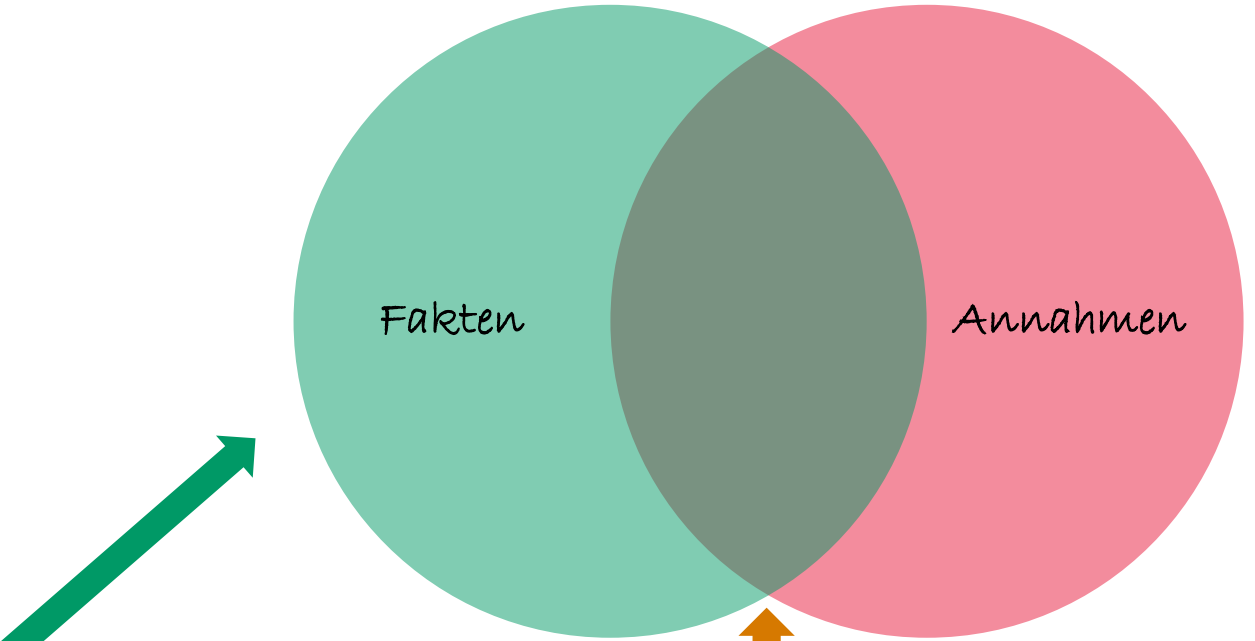
- Versicherung
- Polizei
- IT
- Forensik
- Incident Management
- Vertreter (Krankheit, Unfall, …)



Unzureichende Koordination

Ignorieren von Beweismitteln

Confirmation Bias



Beweise, die wir ignorieren

Beweise, die wir akzeptieren

Täuschung

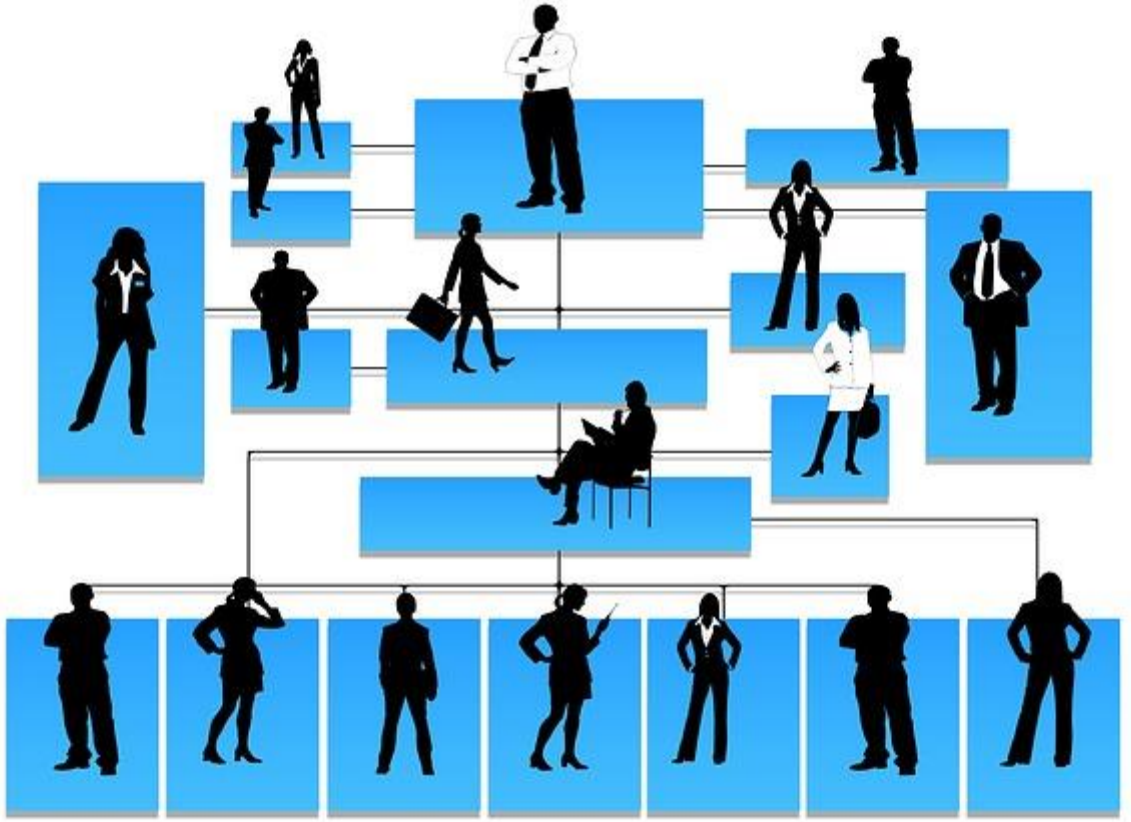
Schnelles Handeln ohne Analyse

Schnelles Handeln ohne Analyse

Beispiele:

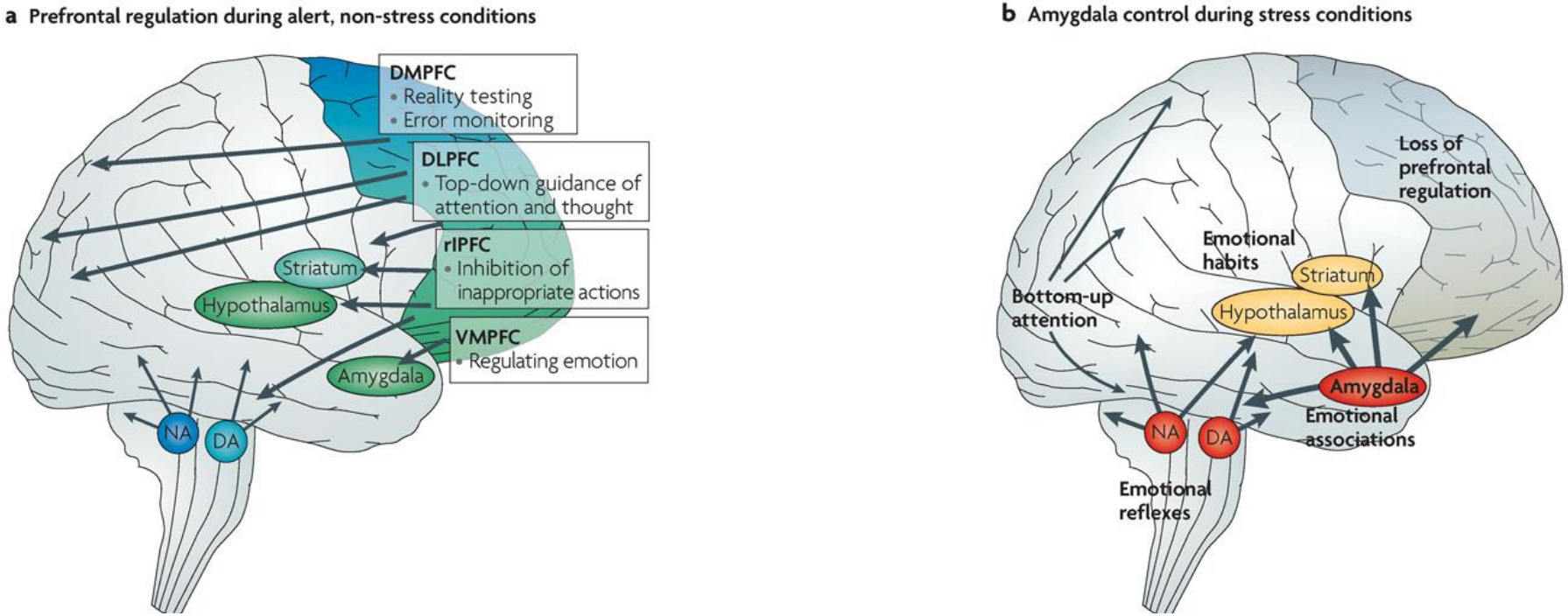
- Einspielen von Backups ohne Malware-Scan oder Entfernung von Backdoors
- Inbetriebnahme kompromittierter Systeme
- Ungeprüfte Übernahme von Systemen ins „grüne“ Netz
- Ausschalten von Systemen
- Nicht-Ausschalten von Systemen

Fehlende Einhaltung von Protokollen



Vertrauliche Informationen teilen

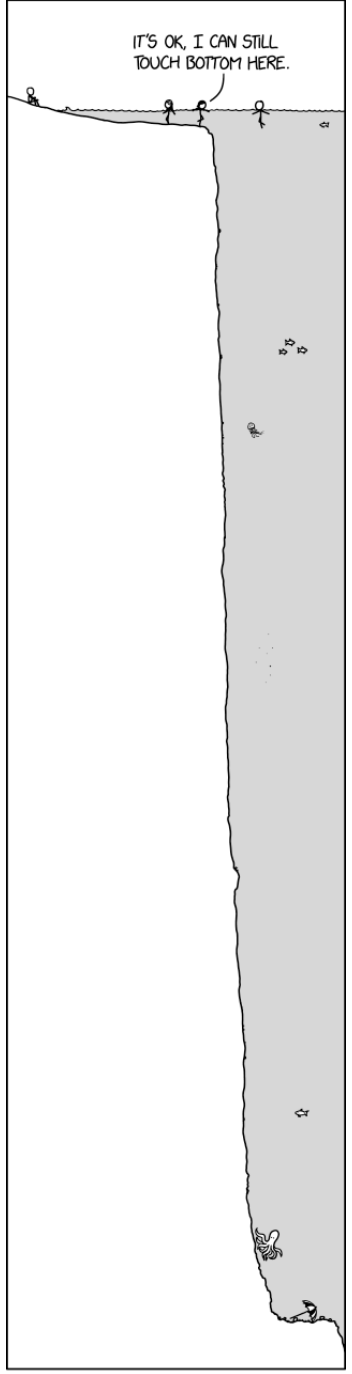
Emotionale Entscheidungen



Quelle: https://pmc.ncbi.nlm.nih.gov/articles/PMC2907136/

Unzureichende Einbeziehung von Experten

Falsche Einschätzung der Bedrohung



I LOVE SWIMMING, BUT OCCASIONALLY I REALIZE I DON'T KNOW HOW DEEP THE WATER UNDER ME IS AND IT FREAKS ME OUT.

Verzicht auf Post-Mortem-Analyse

(… aus Kostengründen)

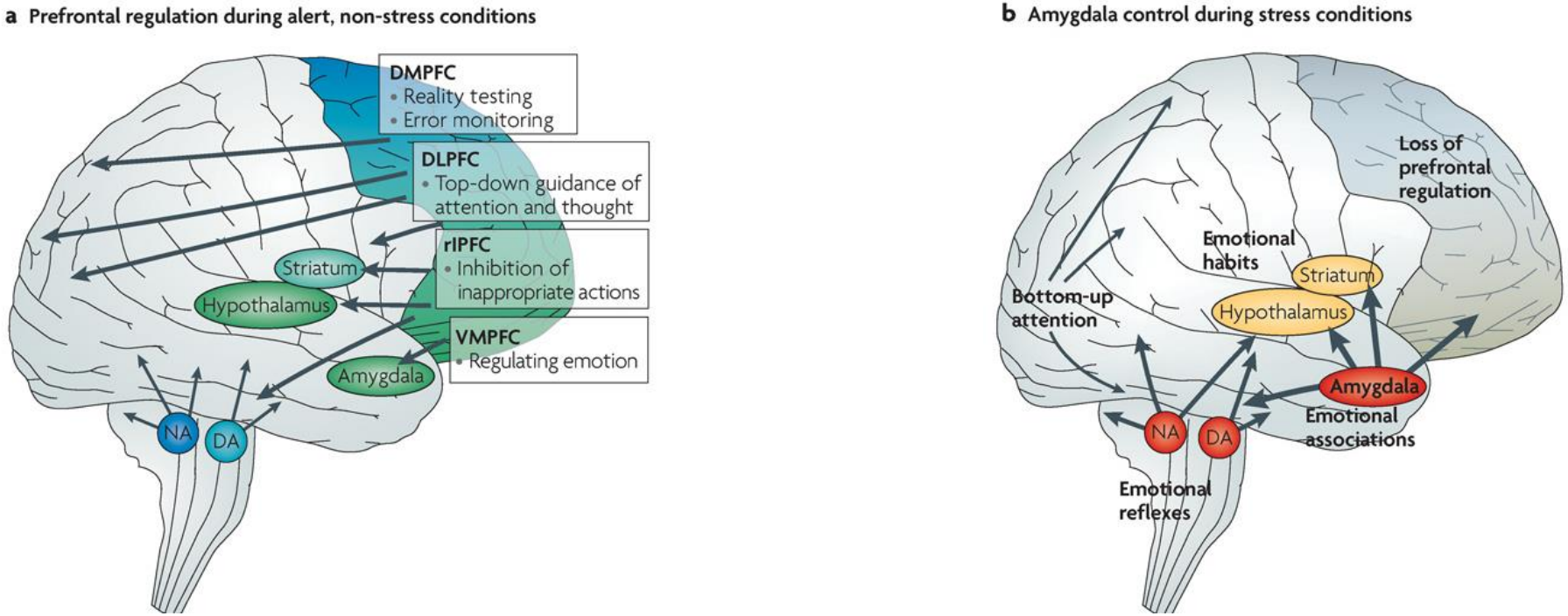
Quelle: https://www.saechsische.de/lokales/saechsische-schweiz-osterzgebirge/bad-gottleuba-berggiesshuebel/wie-gefaehrlich-ist-das-labyrinth-bei-langenhennersdorf-YR5P7GPXZ6Z52KSE4WN77FKJTI.html

Weitere Antipattern

- Immer jeden informieren
- Arbeitszeit mit Status-Calls füllen
- Diskussionen über die Schwere des Incidents
- Keine Eskalation an die Verantwortlichen

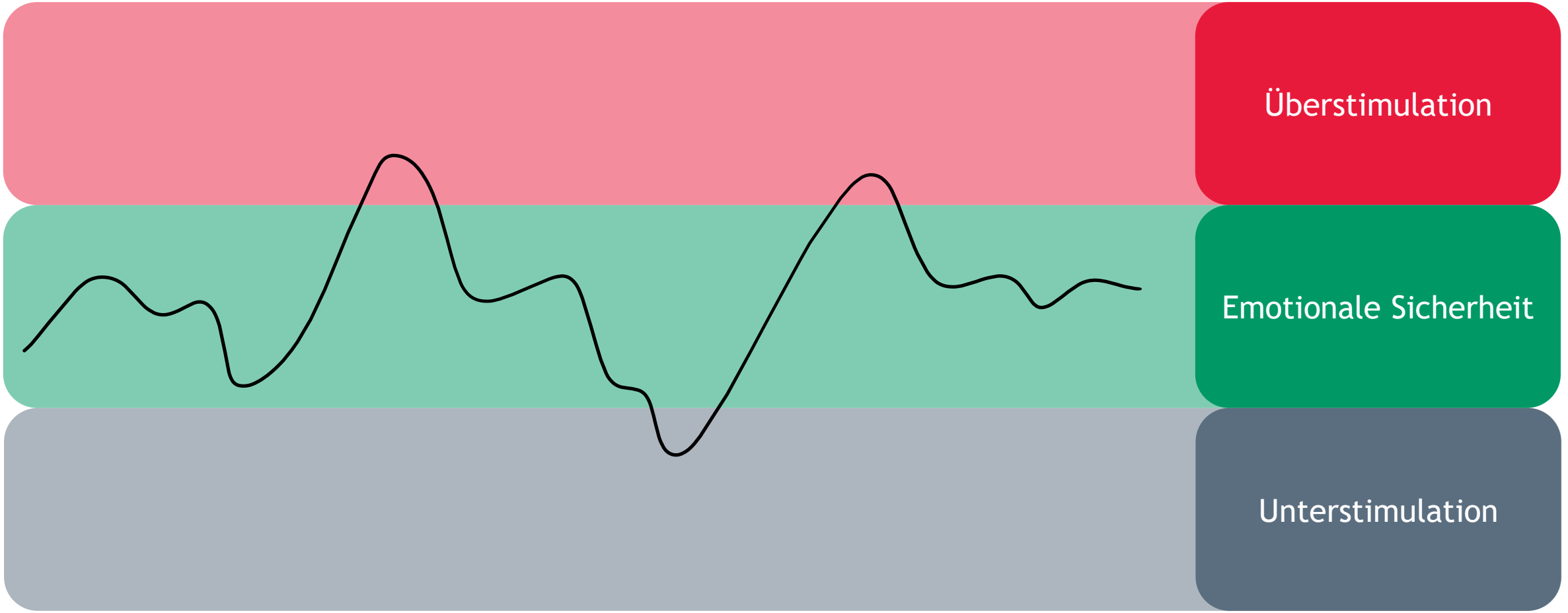
Kommunikation und Stress

Emotionale Entscheidungen

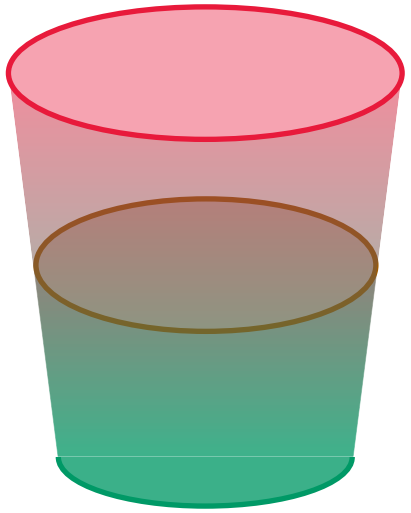


Quelle: https://pmc.ncbi.nlm.nih.gov/articles/PMC2907136/

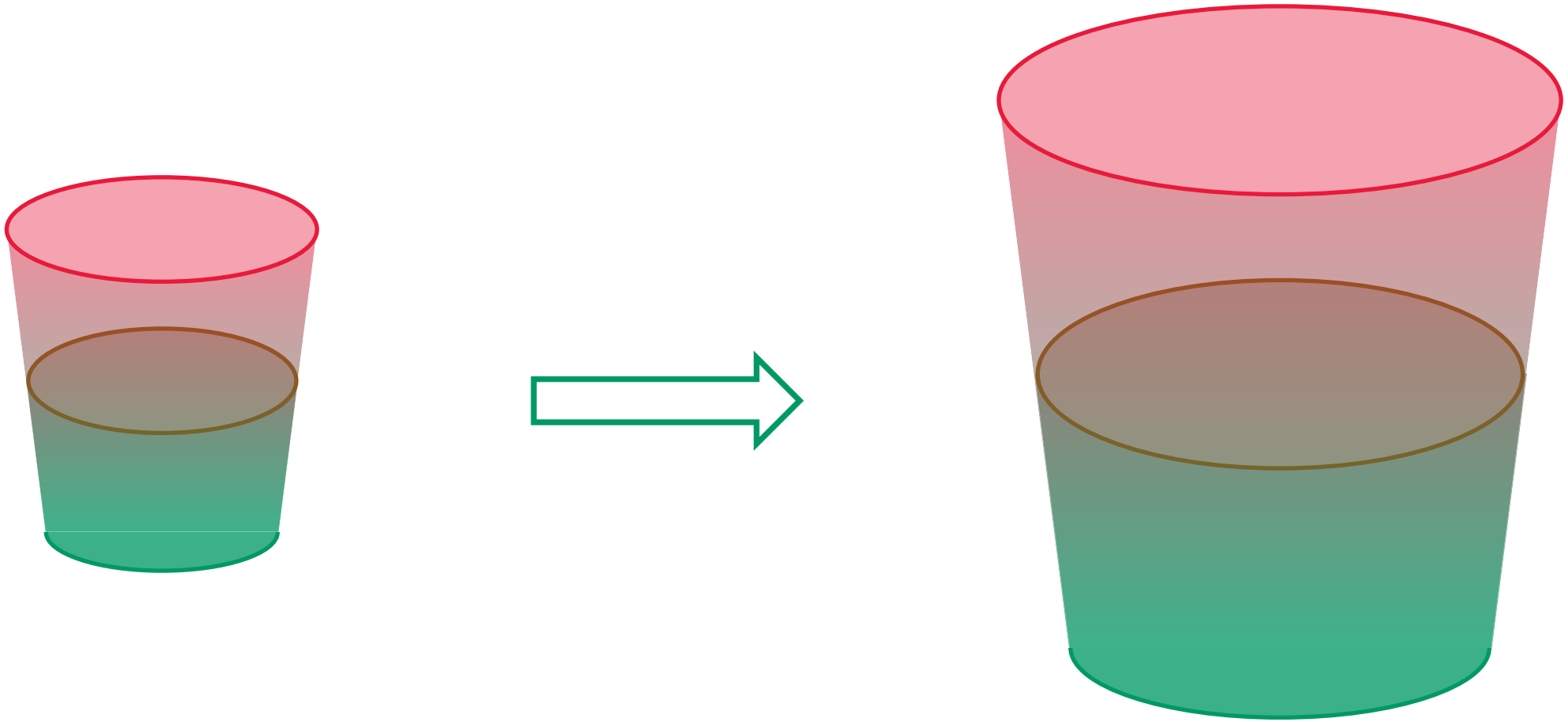
Stresstoleranzfenster



Stresstoleranz

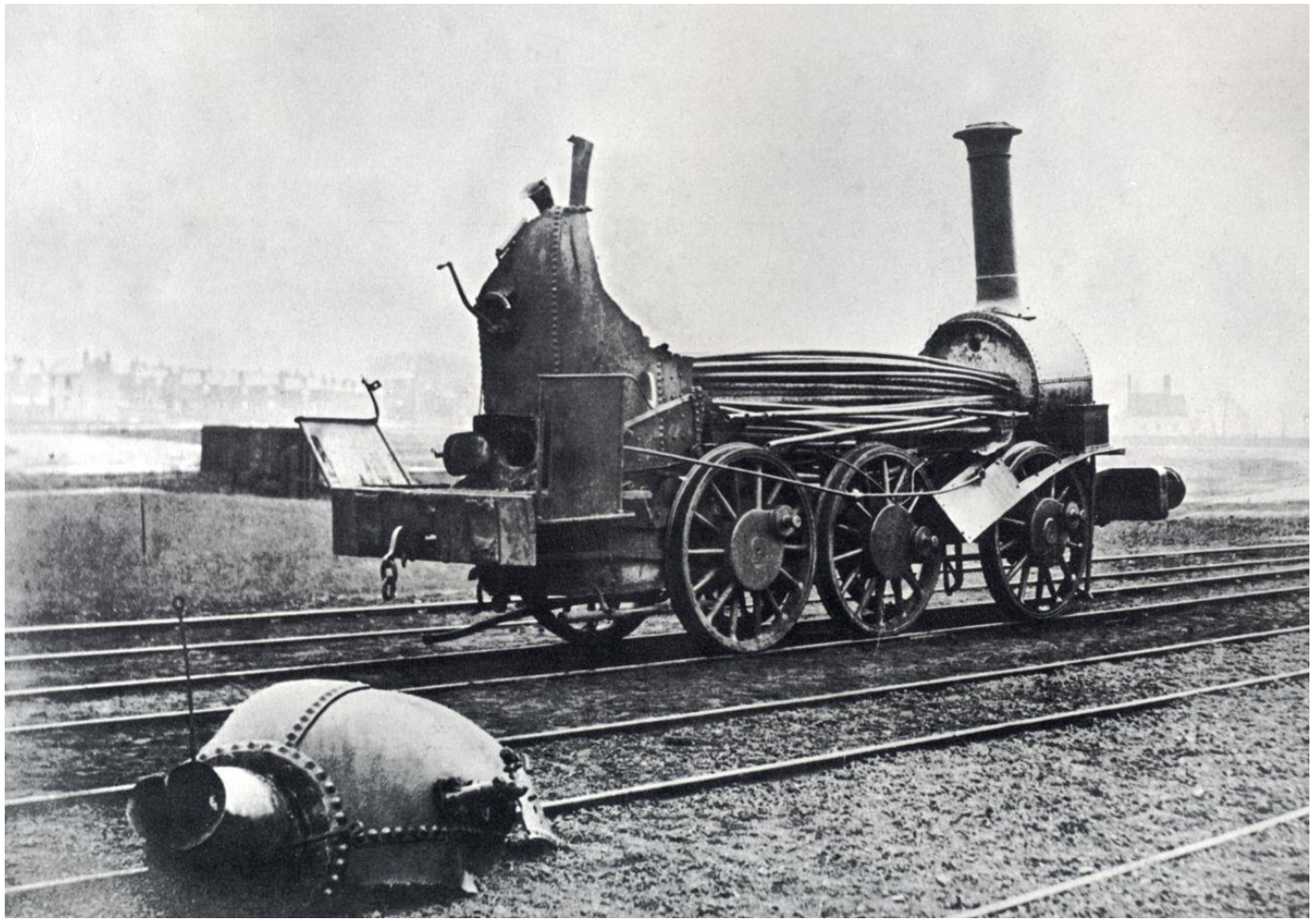


Stresstoleranz



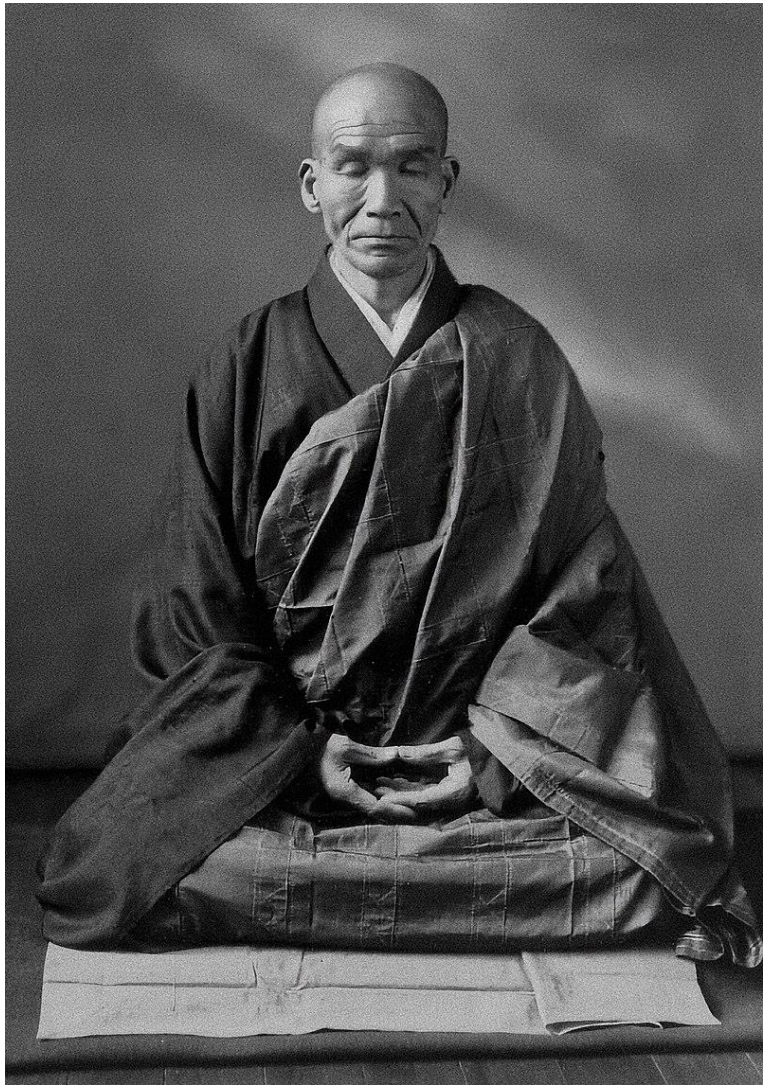
Techniken zur Stressbewältigung

Druck abbauen bevor es knallt



Techniken zur Stressbewältigung

Meditation / Yoga / Wandern / Musik hören / Theaterbesuch / …



Techniken zur Stressbewältigung

Zeitmanagement

- Getting Things Done (GTD)
  - Sammeln, Verarbeiten, Organisieren, Durchsehen, Erledigen
  - Listen: Aktionslisten, Projekteliste, Kalender, Warten-auf-Liste
- ALPEN
  - Aufgaben, Länge schätzen, Pufferzeiten einplanen, Entscheidungen treffen, Nachkontrolle durchführen
- The 7 habits of Highly effective people
  - Proaktiv sein
  - Schon am Anfang das Ende im Sinn haben
  - Prioritäten definieren
  - Win-Win denken
  - Erst verstehen, dann verstanden werden
  - Synergien schaffen
  - Die Säge schärfen
- …

Techniken zur Stressbewältigung

„Nein“ sagen

Es ist meine Aufgabe, mich glücklich zu machen.

Es ist nicht meine Aufgabe andere zu heilen / zu reparieren / zu verändern.

Ich habe das Recht, meine eigenen Gefühle zu haben.

Es macht nichts, wenn andere ärgerlich werden.

Ich bin ok, so wie ich bin.

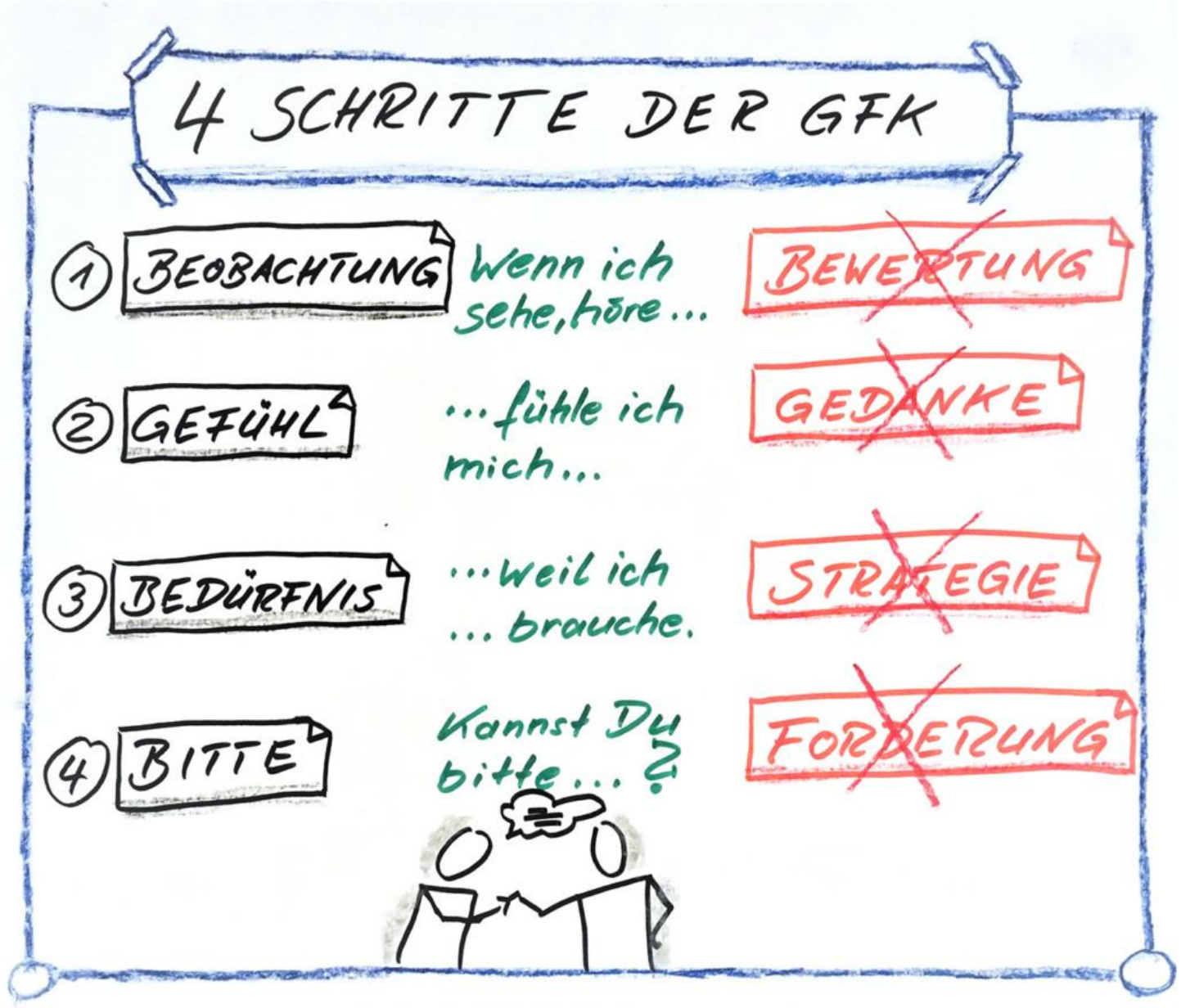
Es ist nicht mein Job Verantwortung für andere zu übernehmen.

Es ist ok „nein“ zu sagen.

Die Bedürfnisse andere muss ich nicht vorher erahnen.

Kommunikationstechniken

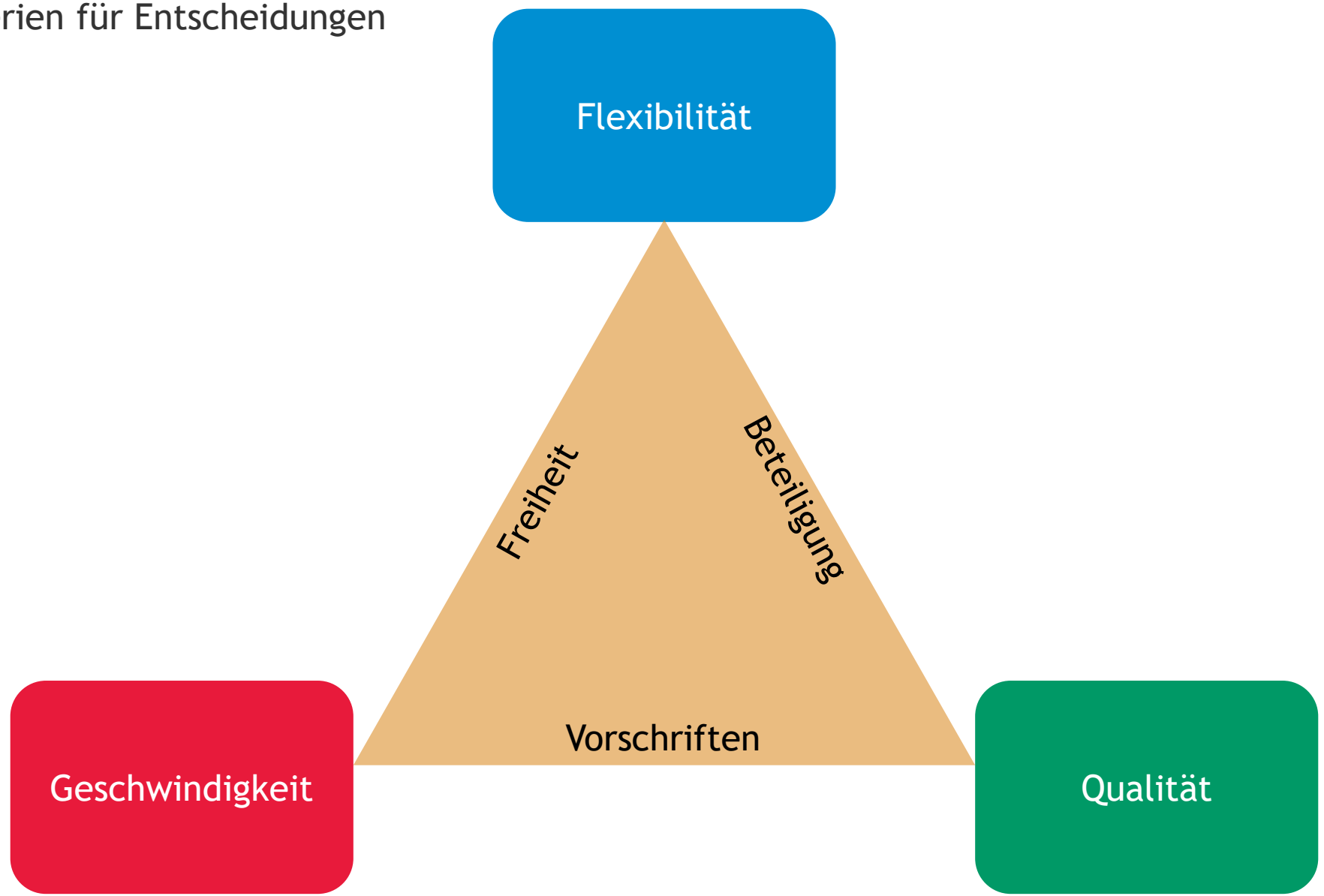
- Gewaltfreie Kommunikation



- Betzavta („Hurra, ein Konflikt!“ bzw. Gemeinsam – einen Konflikt in ein Dilemma verwandeln)

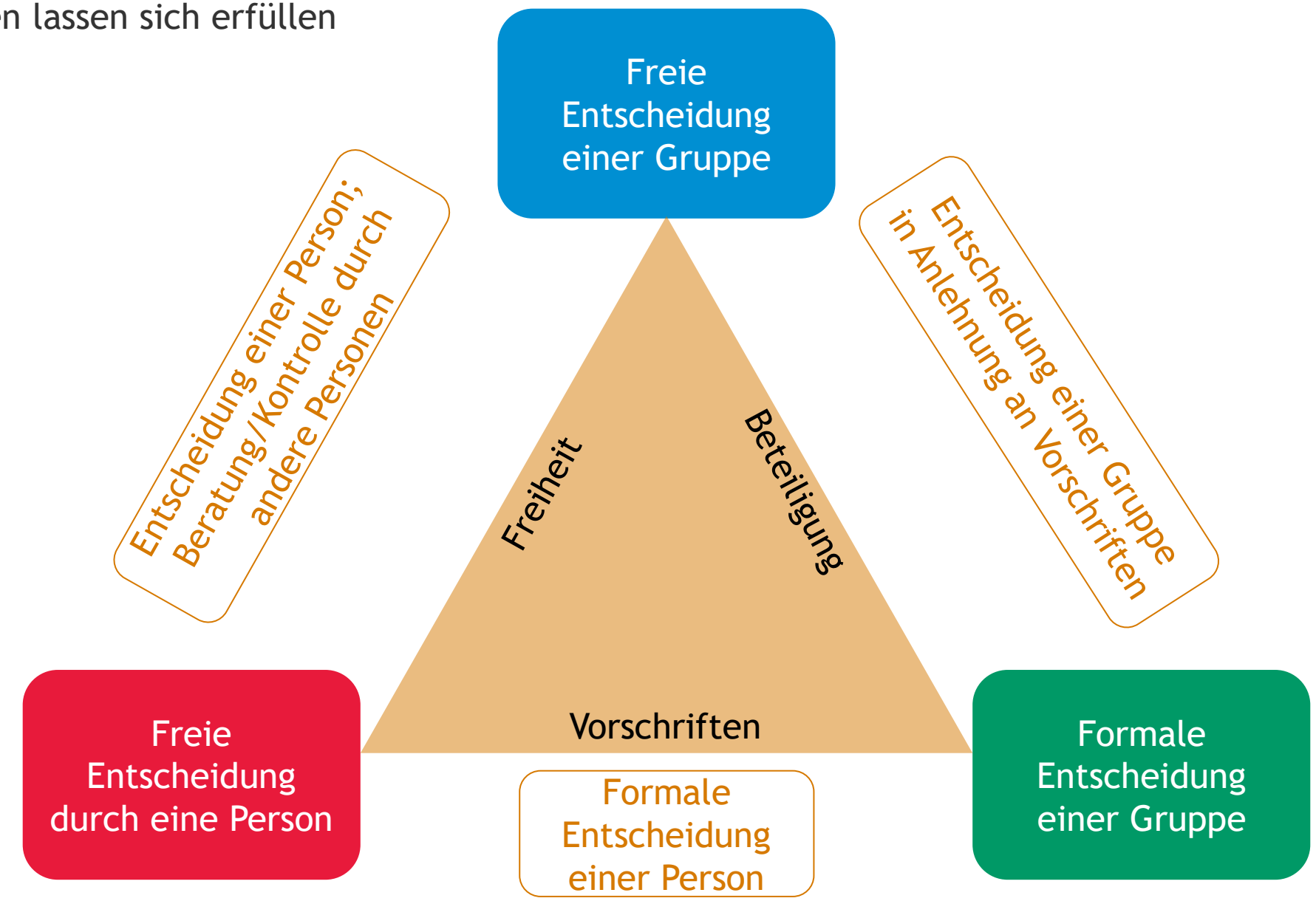
Methoden zur Entscheidungsfindung

Qualitätskriterien für Entscheidungen



Methoden zur Entscheidungsfindung

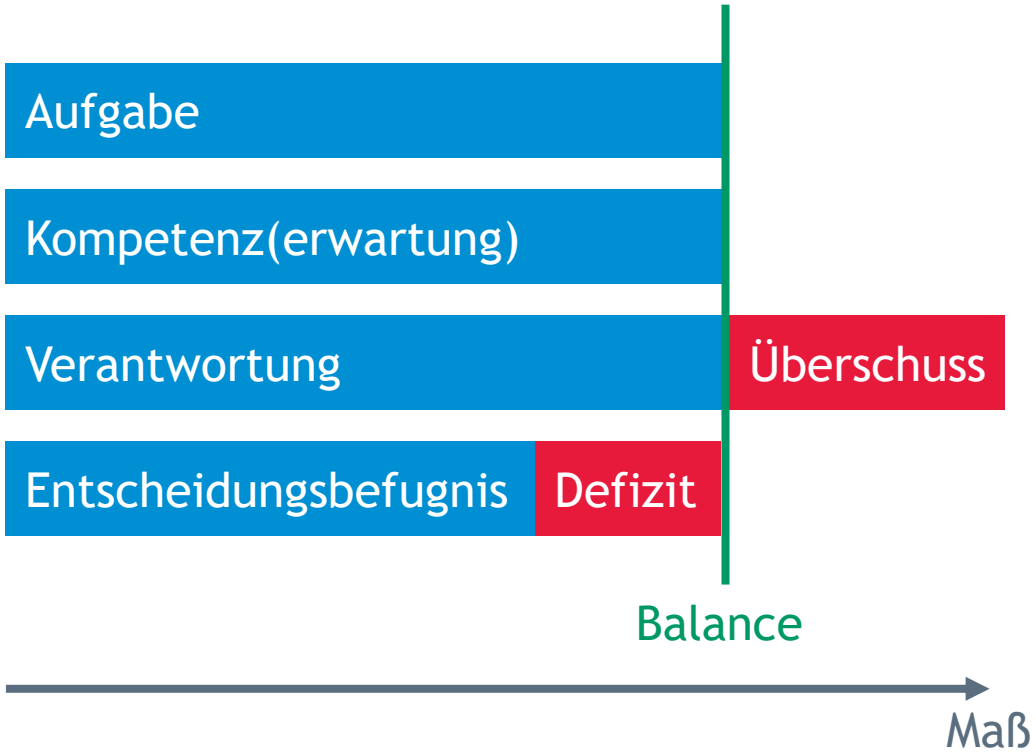
Zwei Kriterien lassen sich erfüllen



Methoden zur Entscheidungsfindung

Bekannte Schwierigkeiten

- Überregulation bzw. fehlende Richtlinien
- Verantwortungsdiffusion
- Angst vor Fehlentscheidungen
- Unreflektierter Konservatismus („So haben wir das schon immer gemacht!“)
- Zu hohe Risikobereitschaft
- Unmögliche Erwartungen



Kurze Pause

Vor Teil 2