

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

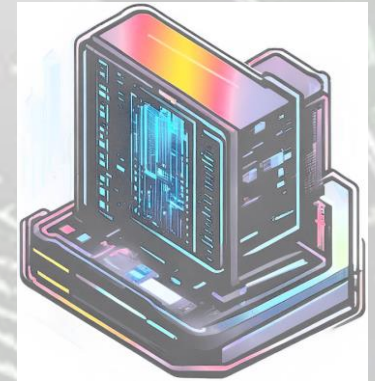
+49 160 96633251

Jan Starke

Senior Consultant



DFIR-Toolkit



ntdextract2



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

Jericho war die erste Stadt, die das Volk Israel im gelobten Land Kanaan eroberte.

Nachdem die Israeliten die Stadt 7 Tage lang umzingelt hatten, bliesen die Priester auf Befehl Josuas in die Widderhörner und Posaunen, das Kriegsvolk hub ein Geschrei an und siehe:

Die Mauern der Stadt stürzten in sich zusammen und die Israeliten drangen in die Stadt...

(Buch Josua, Kap. 6, 1-27)

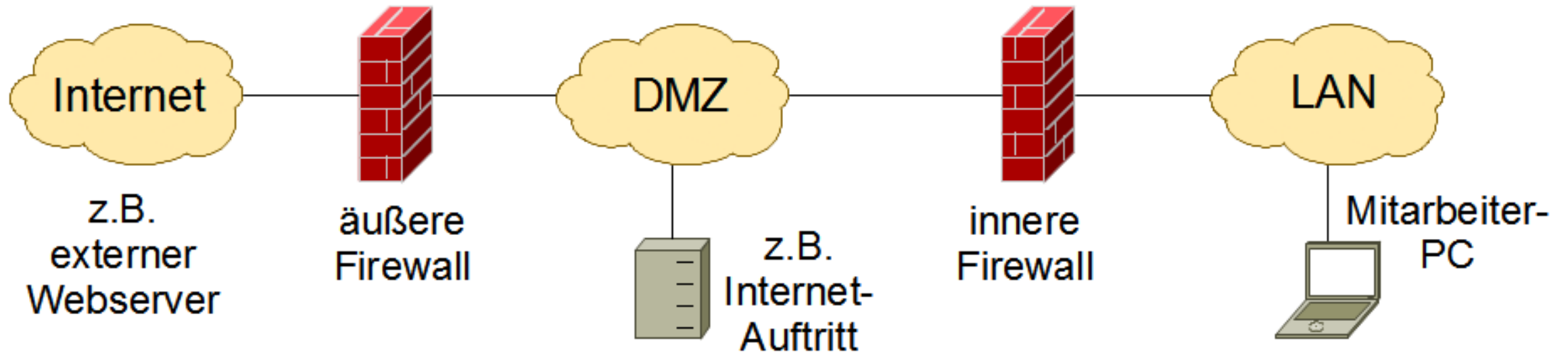


Jericho zum Ende der Bronzezeit

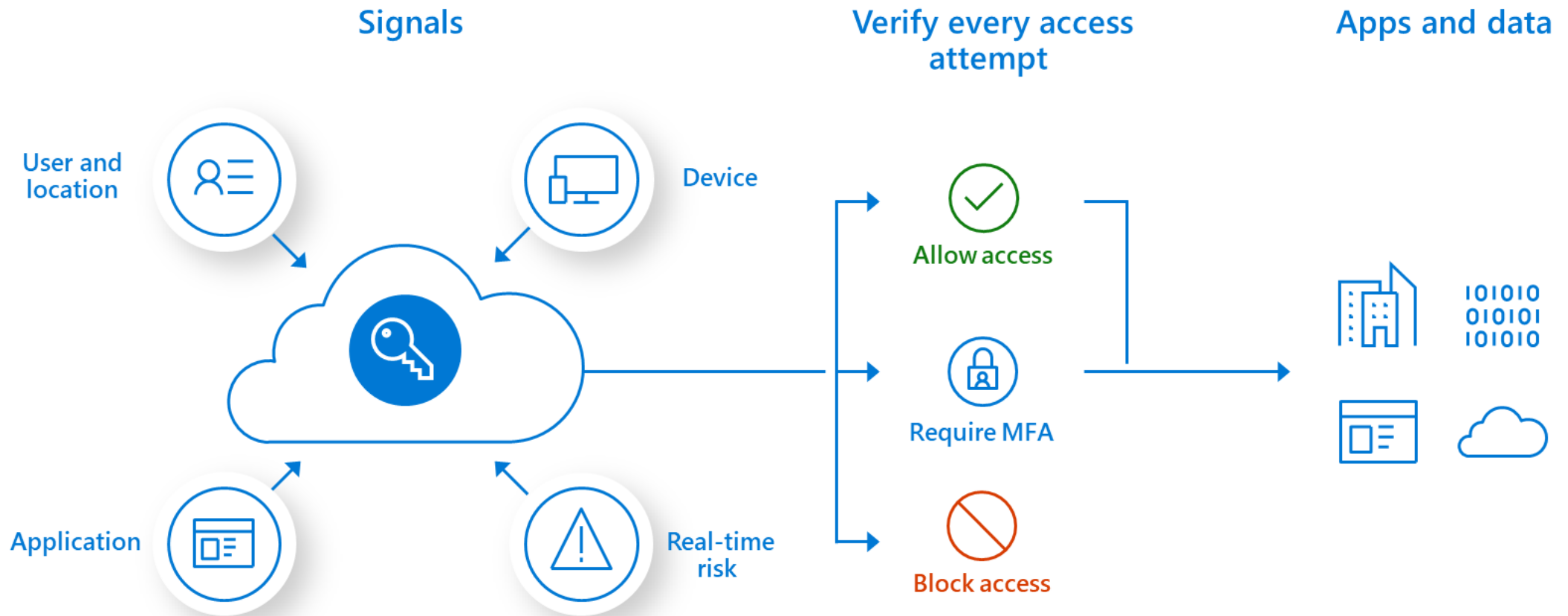
Quelle: <https://www.robl.de/pentagramm/kulturgeschichte/jericho.html>

Prävention

Firewall DMZ-Szenario



Zero-Trust

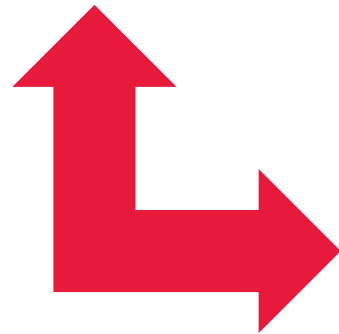


Quelle: <https://www.microsoft.com/de-de/microsoft-365/blog/2019/09/18/why-banks-adopt-modern-cybersecurity-zero-trust-model/>

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_\(Betriebswirtschaftslehre\)](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!

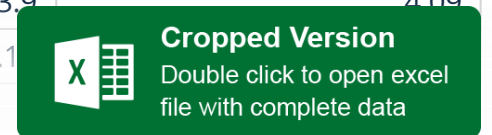
Cyber-Sicherheitsvorfälle werden *bewusst* und *planvoll* herbeigeführt!

(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 | |

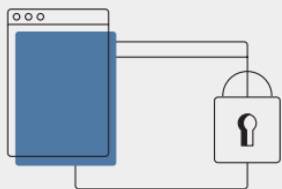


Die Lage der IT-Sicherheit in Deutschland 2023 im Überblick

Ransomware

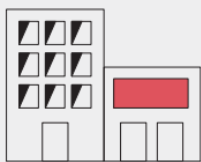
ist weiterhin die größte Bedrohung.

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 %.

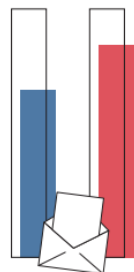


Eine Viertelmillion neue Schadprogramm-Varianten wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.



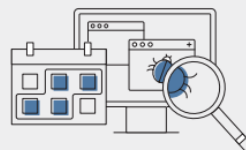
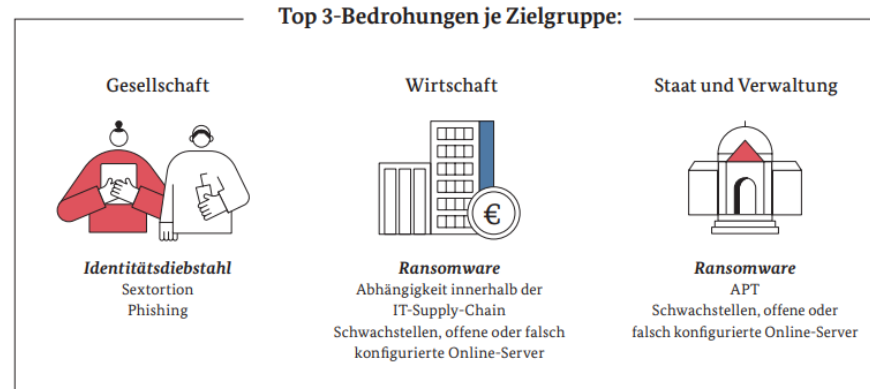
66%

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



84%

aller betrügerischen E-Mails waren Phishing-E-Mails zur Erhebung von Authentisierungsdaten, meist bei Banken und Sparkassen.



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



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

Deutschland
Digital•Sicher•BSI

Bedrohungslage

Bundeslagebericht Cybercrime 2023

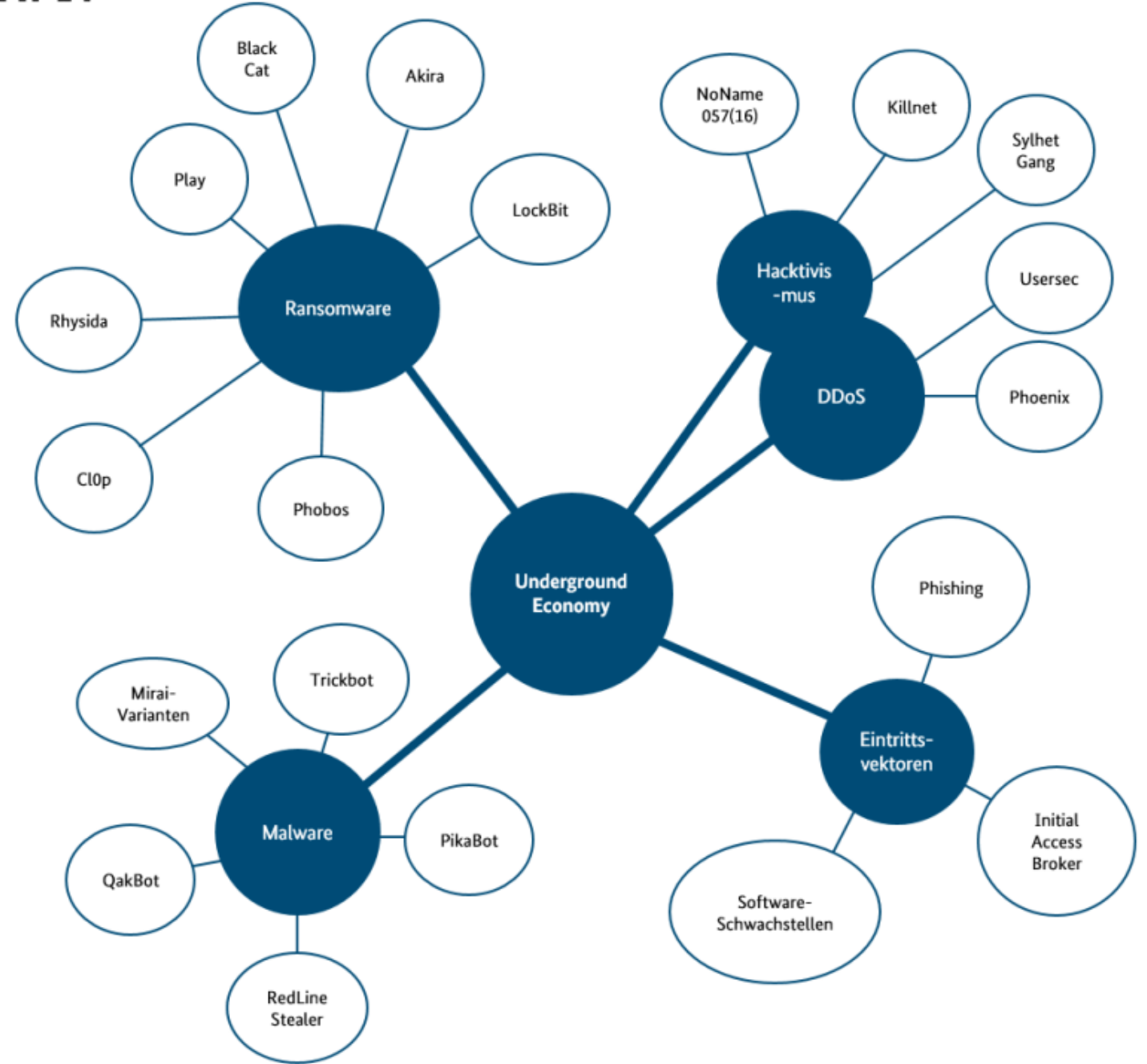
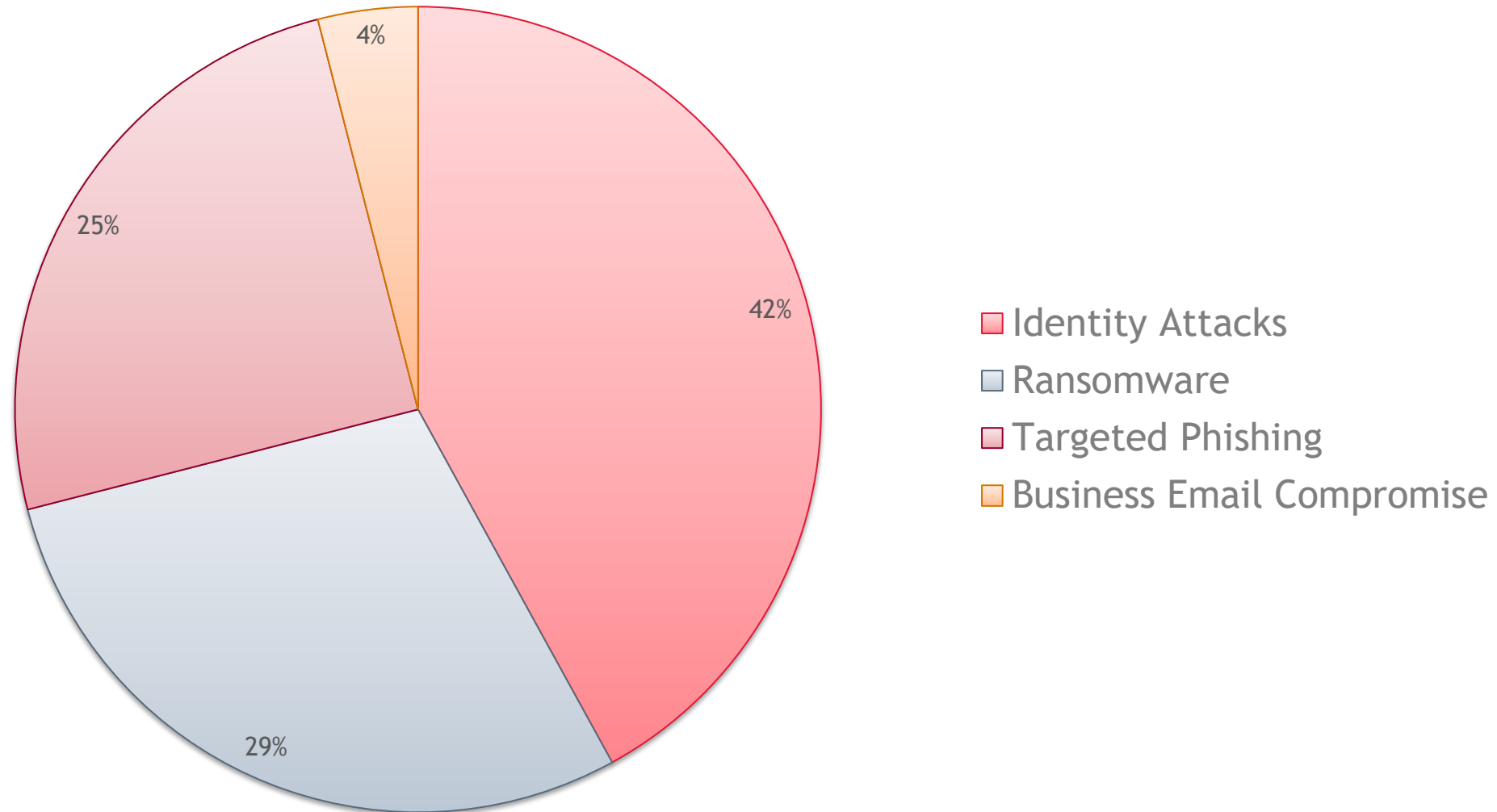


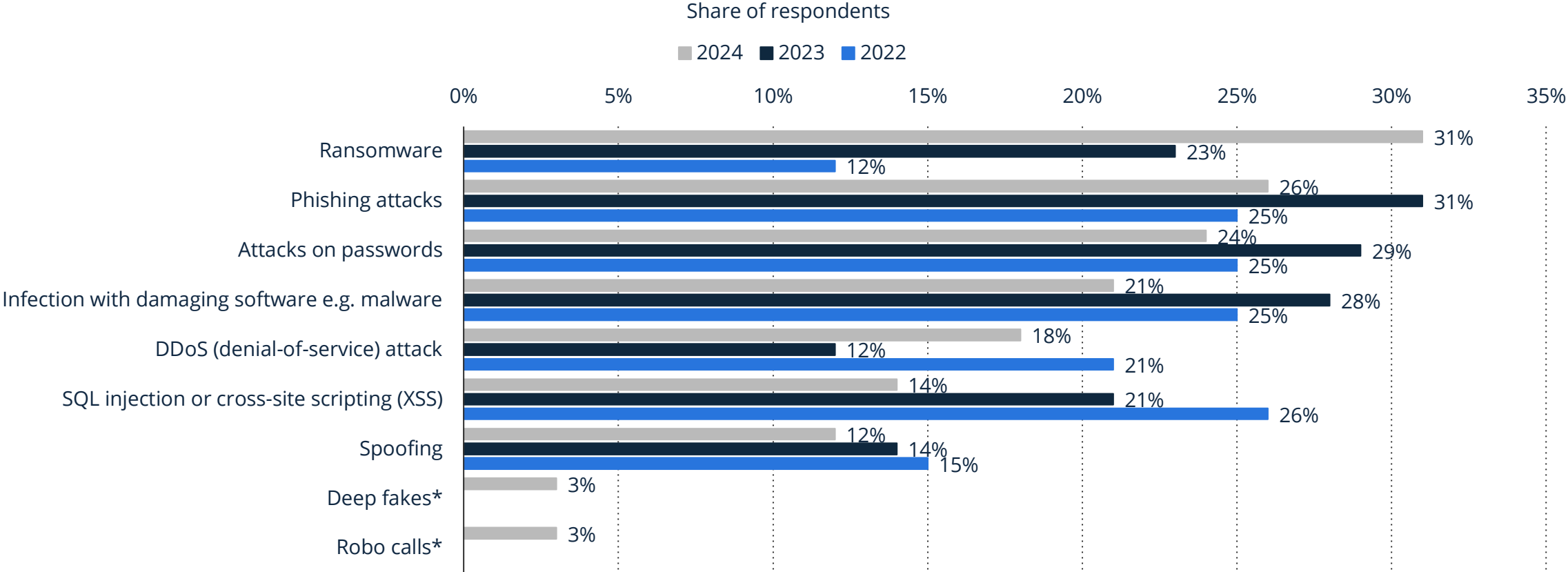
Abbildung 1: Relevante Bedrohungen der Cyberkriminalität 2023

Die häufigsten Angriffsvarianten (Quelle MDDR)



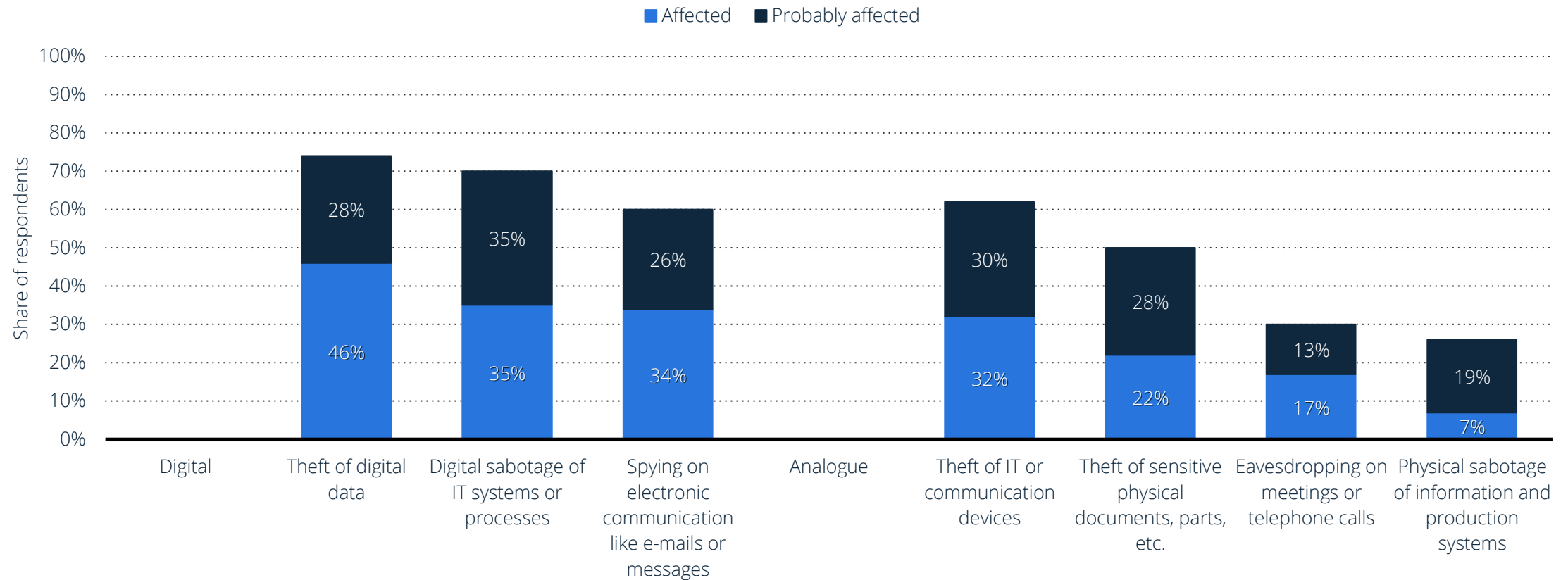
Cyberattacks companies have suffered in Germany from 2022 to 2024

Cyberattacks companies have suffered in Germany 2022 to 2024



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

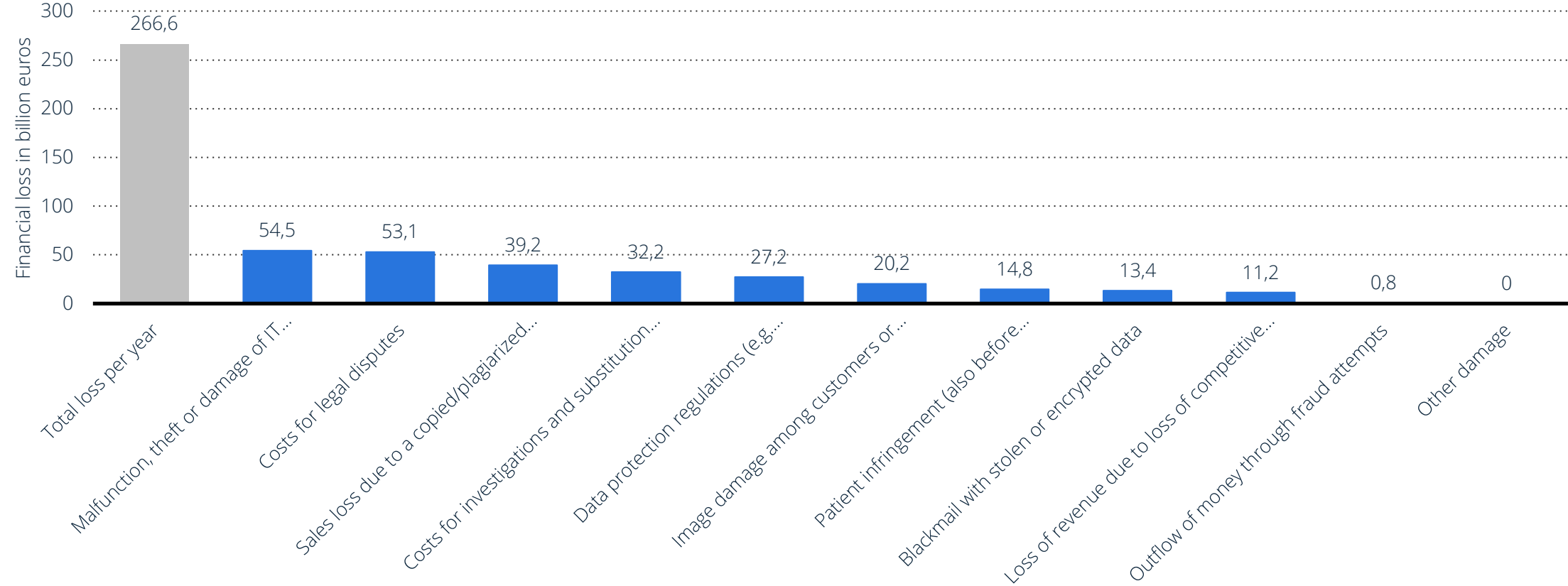
Types of cybercrime in companies in Germany 2024



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

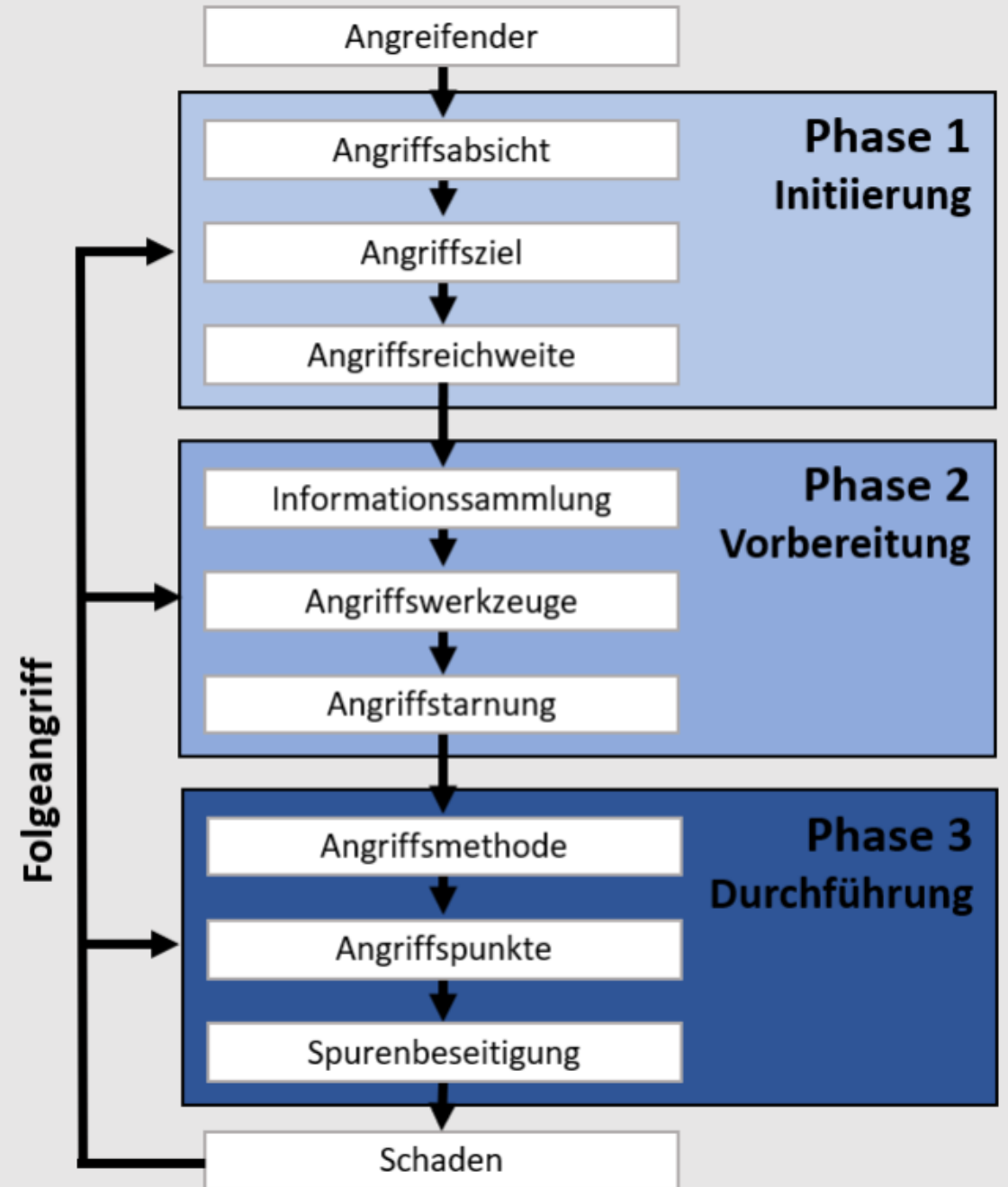
The Q3-2024 Ransomware Malicious Quartile

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



Phasen eines Cyber-Angriffs

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

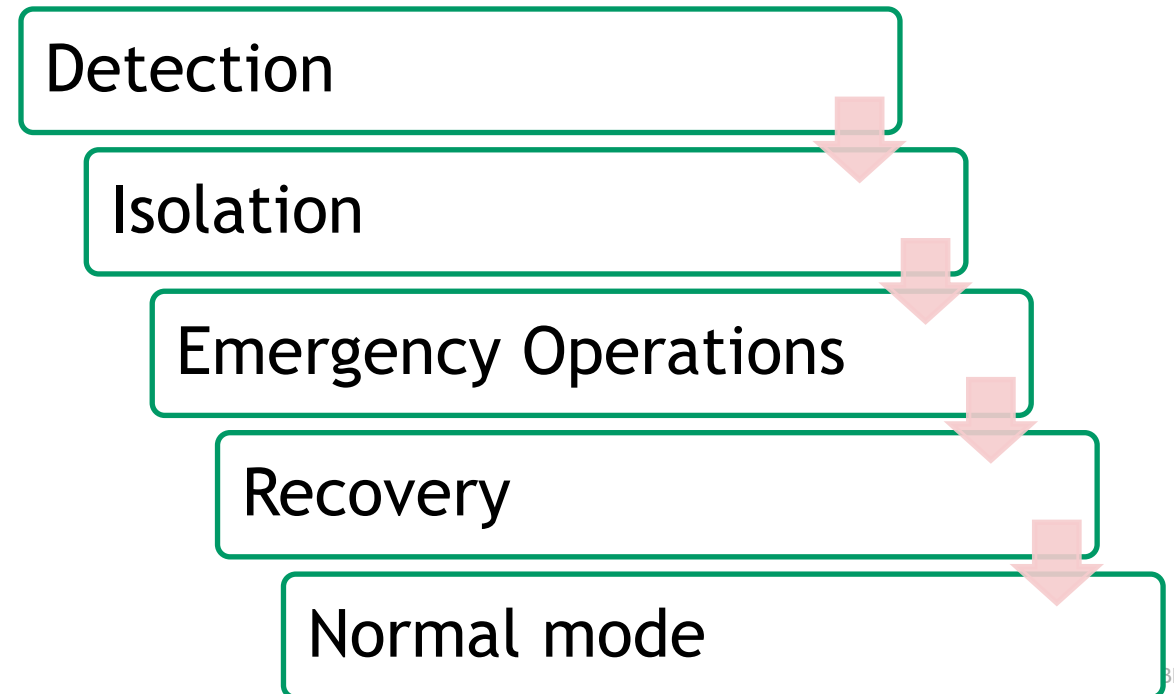
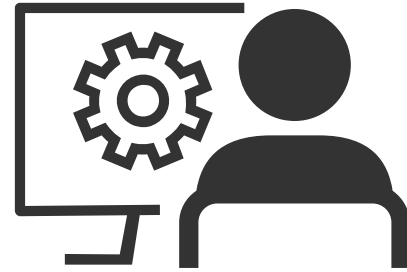
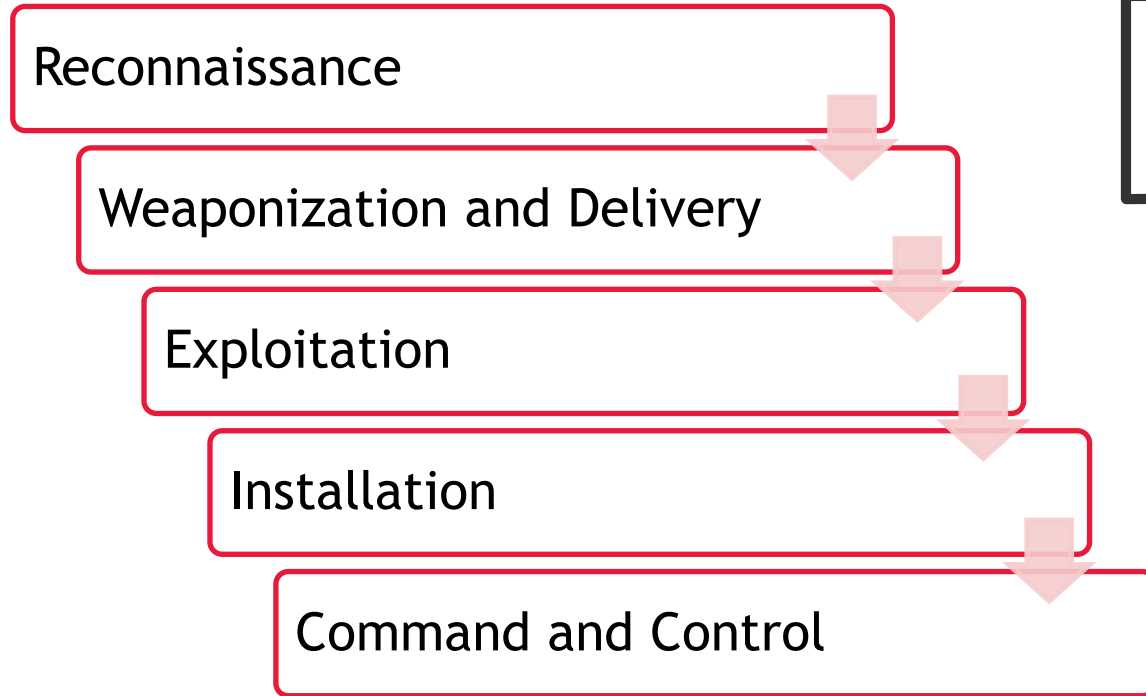


Phasen eines Angriffs

MITRE ATT&CK Matrix

| Reconnaissance | Resource Development | Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|--|---------------------------------|-------------------------------------|--|---|---|---|--|--|---|--|--|--|----------------------------------|
| Active Scanning (0.3) | Acquire Access | Content Injection | Cloud Administration Command | Account Manipulation (0.9) | Abuse Elevation Control Mechanism (0.9) | Abuse Elevation Control Mechanism (0.9) | Adversary-in-the-Middle (0.3) | Account Discovery (0.4) | Exploitation of Remote Services | Adversary-in-the-Middle (0.3) | Application Layer Protocol (0.4) | Automated Exfiltration (0.1) | Account Access Removal |
| Gather Victim Host Information (0.4) | Acquire Infrastructure (0.8) | Drive-by Compromise | Command and Scripting Interpreter (0.10) | BITS Jobs | Access Token Manipulation (0.5) | Access Token Manipulation (0.5) | Brute Force (0.4) | Application Window Discovery | Internal Spearphishing | Archive Collected Data (0.3) | Communication Through Removable Media | Data Transfer Size Limits | Data Destruction |
| Gather Victim Identity Information (0.3) | Compromise Accounts (0.3) | Exploit Public-Facing Application | Container Administration Command | Boot or Logon Autostart Execution (0.14) | Account Manipulation (0.9) | BITS Jobs | Credentials from Password Stores (0.6) | Browser Information Discovery | Lateral Tool Transfer | Audio Capture | Content Injection (0.3) | Exfiltration Over Alternative Protocol | Data Encrypted for Impact |
| Gather Victim Network Information (0.6) | Compromise Infrastructure (0.8) | External Remote Services | Deploy Container | Boot or Logon Initialization Scripts (0.14) | Boot or Logon Autostart Execution (0.14) | Build Image on Host | Exploitation for Credential Access | Cloud Infrastructure Discovery | Remote Service Session Hijacking (0.2) | Automated Collection | Debugger Evasion (0.3) | Exfiltration Over C2 Channel | Data Manipulation (0.3) |
| Gather Victim Org Information (0.4) | Develop Capabilities (0.4) | Hardware Additions | Exploitation for Client Execution | Browser Extensions | Boot or Logon Initialization Scripts (0.14) | Debugger Evasion | Forced Authentication | Cloud Service Dashboard | Remote Services (0.8) | Browser Session Hijacking | Deobfuscate/Decode Files or Information | Exfiltration Over Other Network Medium (0.1) | Defacement (0.2) |
| Phishing for Information (0.4) | Establish Accounts (0.3) | Phishing (0.4) | Inter-Process Communication (0.3) | Compromise Host Software Binary | Boot or Logon Initialization Scripts (0.14) | Deobfuscate/Decode Files or Information | Forge Web Credentials (0.2) | Cloud Service Discovery | Replication Through Removable Media | Clipboard Data | Domain or Tenant Policy Modification (0.2) | Exfiltration Over Physical Medium (0.1) | Disk Wipe (0.2) |
| Search Closed Sources (0.2) | Obtain Capabilities (0.7) | Replication Through Removable Media | Native API | Create Account (0.3) | Create or Modify System Process (0.5) | Deploy Container | Input Capture (0.4) | Cloud Storage Object Discovery | Software Deployment Tools | Data from Cloud Storage | Encrypted Channel (0.2) | Exfiltration Over Web Service (0.4) | Endpoint Denial of Service (0.4) |
| Search Open Technical Databases (0.5) | Stage Capabilities (0.6) | Supply Chain Compromise (0.3) | Scheduled Task/Job (0.5) | Create or Modify System Process (0.5) | Domain or Tenant Policy Modification (0.2) | Direct Volume Access | Modify Authentication Process (0.9) | Container and Resource Discovery | Taint Shared Content (0.4) | Data from Configuration Repository (0.2) | Fallback Channels | Exfiltration Over Web Service (0.4) | Financial Theft |
| Search Open Websites/Domains (0.3) | Trusted Relationship | Serverless Execution | Serverless Execution | Event Triggered Execution (0.18) | Escape to Host | Execution Guardrails (0.1) | Multi-Factor Authentication Interception | Debugger Evasion | Use Alternate Authentication Material (0.4) | Data from Information Repositories (0.3) | Hide Infrastructure | Scheduled Transfer | Firmware Corruption |
| Search Victim-Owned Websites | Valid Accounts (0.4) | Software Deployment Tools | Shared Modules | External Remote Services | Event Triggered Execution (0.18) | Exploitation for Defense Evasion | Multi-Factor Authentication Request Generation | Device Driver Discovery | | Data from Local System | Ingress Tool Transfer | Transfer Data to Cloud Account | Inhibit System Recovery |
| | | System Services (0.2) | Software Deployment Tools | Hijack Execution Flow (0.13) | Exploitation for Privilege Escalation | File and Directory Permissions Modification (0.2) | Network Sniffing | Domain Trust Discovery | | Data from Network Shared Drive | Multi-Stage Channels | | Network Denial of Service (0.2) |
| | | User Execution (0.3) | System Services (0.2) | Implant Internal Image | Hijack Execution Flow (0.13) | Hide Artifacts (0.12) | OS Credential Dumping (0.8) | File and Directory Discovery | | Data from Removable Media | Non-Application Layer Protocol | | Resource Hijacking |
| | | Windows Management Instrumentation | User Execution (0.3) | Modify Authentication Process (0.9) | Process Injection (0.12) | Hijack Execution Flow (0.13) | Steal Application Access Token | Group Policy Discovery | | Data Staged (0.2) | Non-Standard Port | | Service Stop |
| | | | Power Settings | Office Application Startup (0.9) | Scheduled Task/Job (0.5) | Impair Defenses (0.11) | Steal or Forge Authentication Certificates | Network Service Discovery | | Email Collection (0.3) | Protocol Tunneling | | System Shutdown/Reboot |
| | | | Pre-OS Boot (0.5) | Power Settings | Valid Accounts (0.4) | Impersonation | Steal or Forge Kerberos Tickets (0.4) | Network Share Discovery | | Input Capture (0.4) | Proxy (0.4) | | |
| | | | Scheduled Task/Job (0.5) | Pre-OS Boot (0.5) | Indicator Removal (0.9) | Indicator Removal (0.9) | Steal Web Session Cookie | Network Sniffing | | Screen Capture | Remote Access Software | | |
| | | | Server Software Component (0.5) | Process Injection (0.12) | Indirect Command Execution | Masquerading (0.9) | Unsecured Credentials (0.8) | Password Policy Discovery | | Traffic Signaling (0.2) | Web Service (0.3) | | |
| | | | Traffic Signaling (0.2) | Reflective Code Loading | Modify Authentication Process (0.9) | Modify Authentication Process (0.9) | | Peripheral Device Discovery | | | | | |
| | | | Valid Accounts (0.4) | Rogue Domain Controller | Modify Cloud Compute Infrastructure (0.5) | Modify Cloud Compute Infrastructure (0.5) | | Permission Groups Discovery (0.3) | | | | | |
| | | | | Rootkit | Modify Registry | Modify Registry | | Process Discovery | | | | | |
| | | | | Subvert Trust Controls (0.8) | Modify System Image (0.2) | Modify System Image (0.2) | | Query Registry | | | | | |
| | | | | System Binary Proxy Execution (0.14) | Network Boundary Bridging (0.11) | Network Boundary Bridging (0.11) | | Remote System Discovery | | | | | |
| | | | | System Script Proxy Execution (0.2) | Obfuscated Files or Information (0.13) | Obfuscated Files or Information (0.13) | | Software Discovery (0.1) | | | | | |
| | | | | Template Injection | Plist File Modification | Plist File Modification | | System Information Discovery | | | | | |
| | | | | Traffic Signaling (0.2) | Pre-OS Boot (0.5) | Pre-OS Boot (0.5) | | System Location Discovery (0.1) | | | | | |
| | | | | Trusted Developer Utilities Proxy Execution (0.1) | Process Injection (0.12) | Process Injection (0.12) | | System Network Configuration Discovery (0.2) | | | | | |
| | | | | Unused/Unsupported Cloud Regions | Reflective Code Loading | Reflective Code Loading | | System Network Connections Discovery | | | | | |
| | | | | Use Alternate Authentication Material (0.4) | Rogue Domain Controller | Rogue Domain Controller | | System Owner/User Discovery | | | | | |
| | | | | Valid Accounts (0.4) | Rootkit | Rootkit | | System Service Discovery | | | | | |
| | | | | Virtualization/Sandbox Evasion (0.3) | Subvert Trust Controls (0.8) | Subvert Trust Controls (0.8) | | System Time Discovery | | | | | |
| | | | | Weaken Encryption (0.2) | System Binary Proxy Execution (0.14) | System Binary Proxy Execution (0.14) | | Virtualization/Sandbox Evasion (0.3) | | | | | |
| | | | | XSL Script Processing | System Script Proxy Execution (0.2) | System Script Proxy Execution (0.2) | | Weakens Encryption (0.2) | | | | | |
| | | | | | Template Injection | Template Injection | | XSL Script Processing | | | | | |

Phasen eines Angriffs



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

The screenshot shows a web browser window with the Shodan search engine interface. The search query is 'cups 200 ok'. The page displays 12,377 total results. A 'Product Spotlight' banner promotes a new API for vulnerability lookups. The main result is titled 'Web Interface is Disabled - CUPS v2.0.3' and includes a world map showing top countries: United States (2,027) and China (2,002). The result details include IP address 89.150.129.78, location in Denmark, and various HTTP headers.

Browser tabs: cups 200 ok - Shodan Search

Browser address bar: <https://www.shodan.io/search?query=cups+200+ok>

Navigation: Shodan, Maps, Images, Monitor, Developer, More...

SHODAN Explore Pricing ↗ cups 200 ok [Search] [Login]

TOTAL RESULTS
12,377

TOP COUNTRIES

| | |
|---------------|-------|
| United States | 2,027 |
| China | 2,002 |

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)

Web Interface is Disabled - CUPS v2.0.3 ↗ 2024-10-21T14:20:06.963374

89.150.129.78
x5996814e.customers.hiper-net.dk
[Nuuday A/S](#)
Denmark, Copenhagen

HTTP/1.1 200 OK
Connection: close
Content-Language: en_US
Content-Length: 459
Content-Type: text/html; charset=utf-8
Date: Mon, 21 Oct 2024 14:20:06 GMT
Accept-Encoding: gzip, deflate, identity
Server: CUPS/2.0 IPP/2.1
X-Frame-Options: DENY
Content-Security-Policy: frame-ancestors 'none'...

Reconnaissance

186.159.24.58 x HPLIP Printer Application x +

Nicht sicher | 186.159.24.58:8000

Version 3.22.10-8

Konfiguration [Change](#)

Name: HPLIP Printer Application

Standort: Nicht gesetzt

Organisation: Nicht gesetzt

Kontakt: Nicht gesetzt

Drucker

[Drucker hinzufügen](#)

Weitere Einstellungen

[Neues TLS-Zertifikat erstellen](#) [TLS Zertifikat Anfrage erzeugen](#)

[Install Proprietary Plugin](#) [TLS Zertifikat installieren](#) [Netzwerk](#)

[Sicherheit](#)

Protokollierung

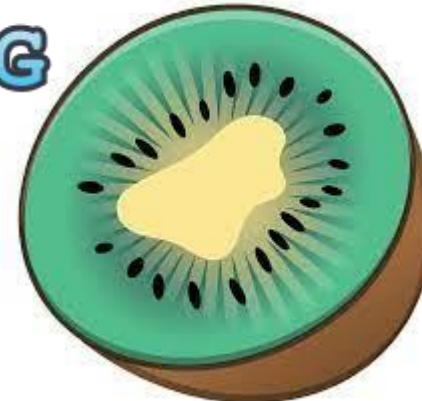
[Protokoll anzeigen](#)

Copyright © 2021 by Till Kampeter. Provided under the terms of the [Apache License 2.0](#).

Weaponization and Delivery

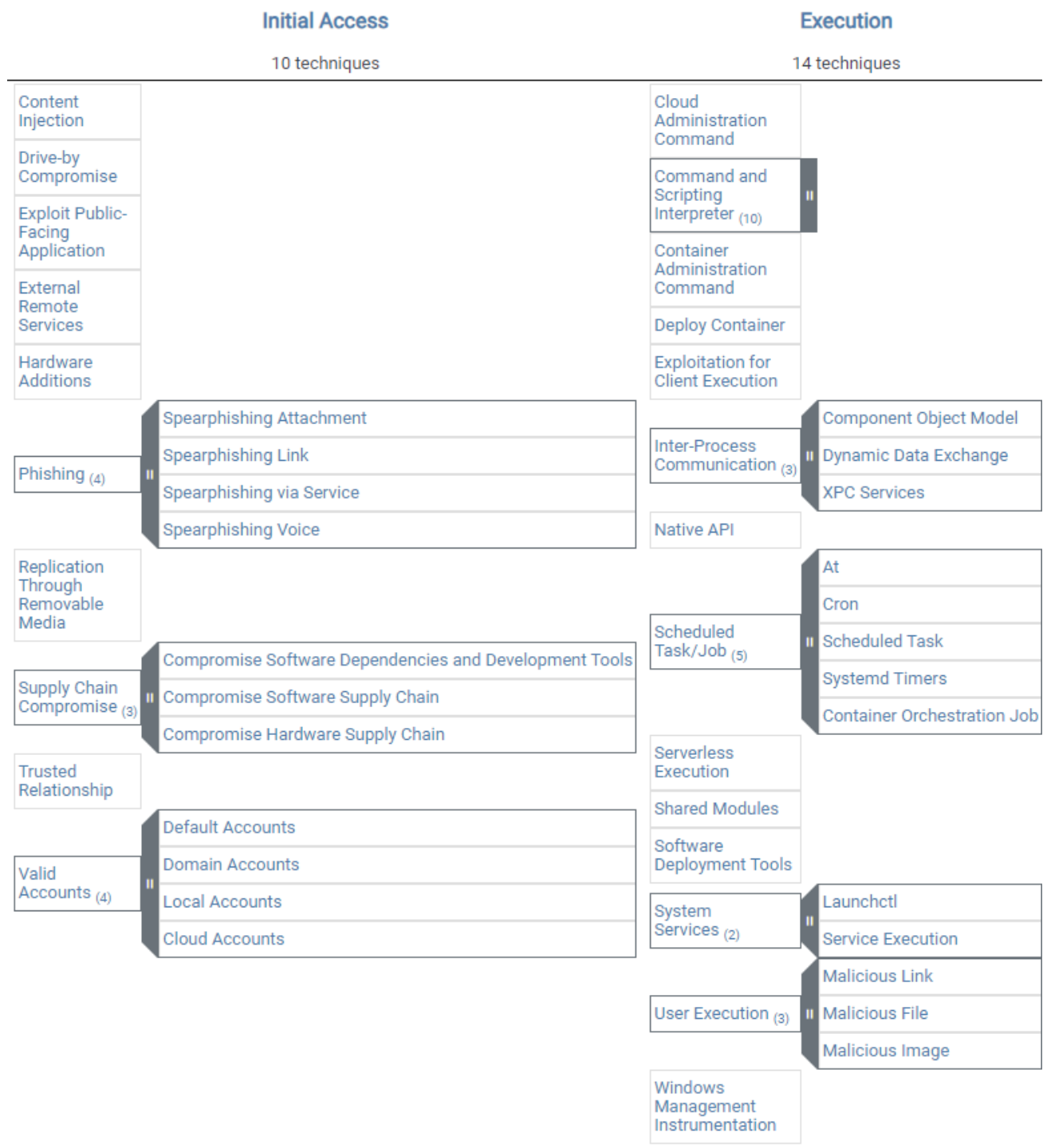


Metasploit



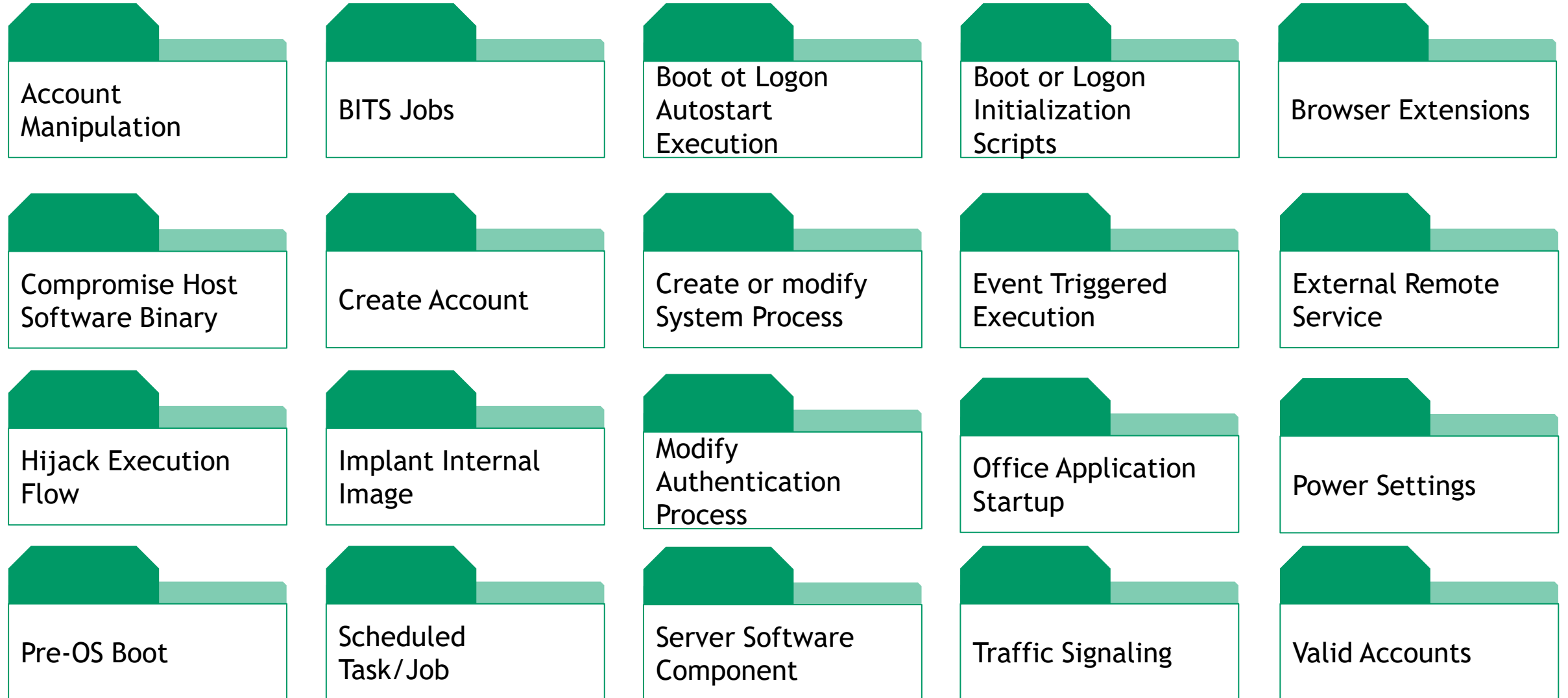
Exploitation

(MITRE ATT&CK)

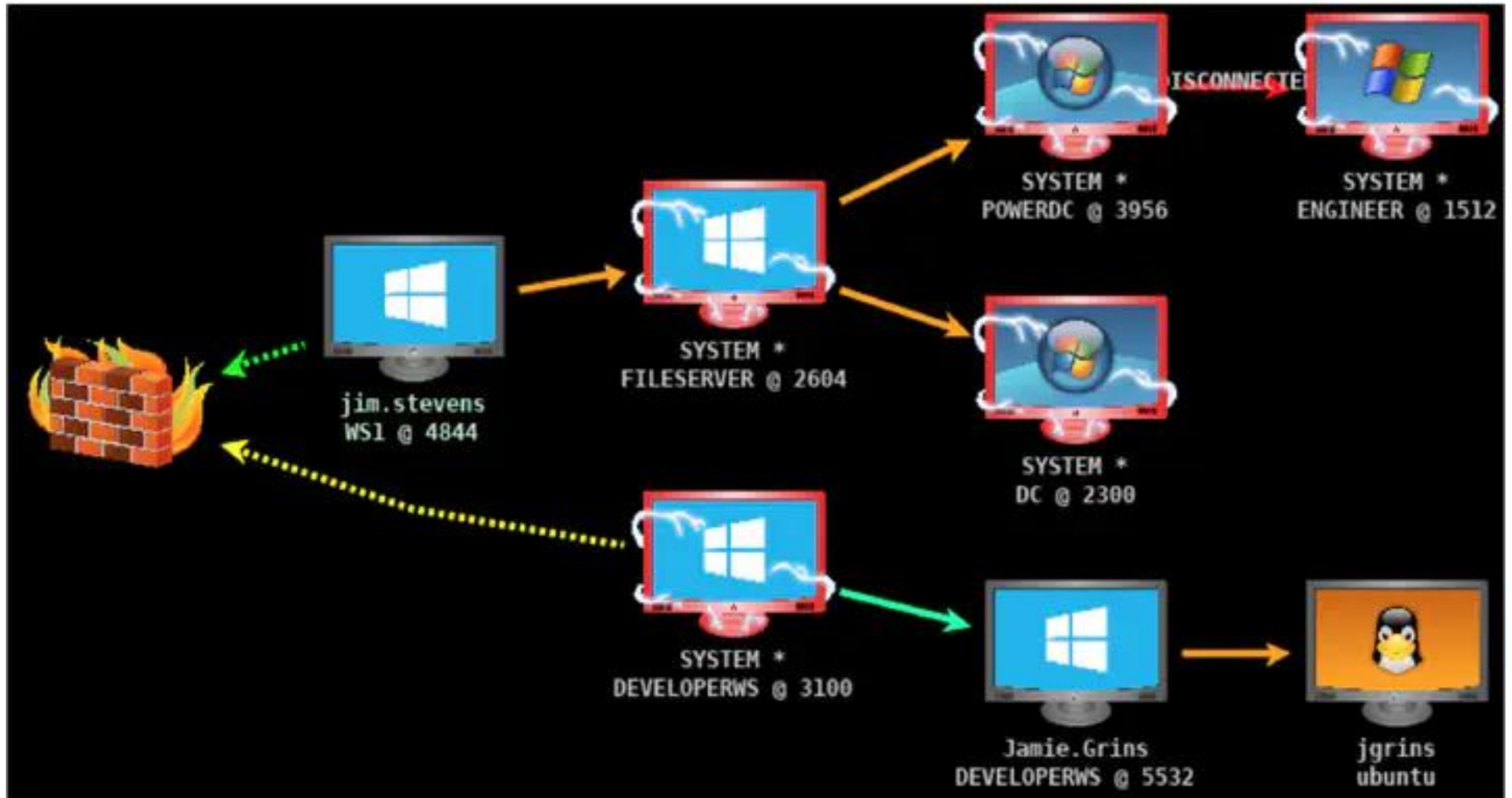


Installation

MITRE ATT&CK Persistence

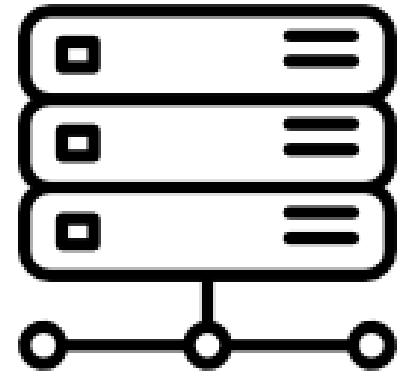
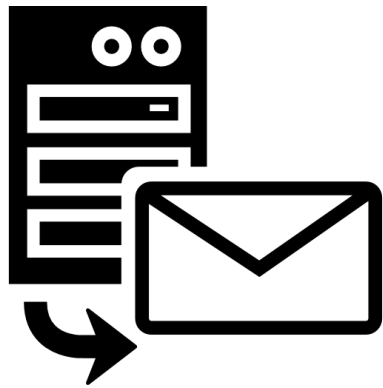


Command and Control



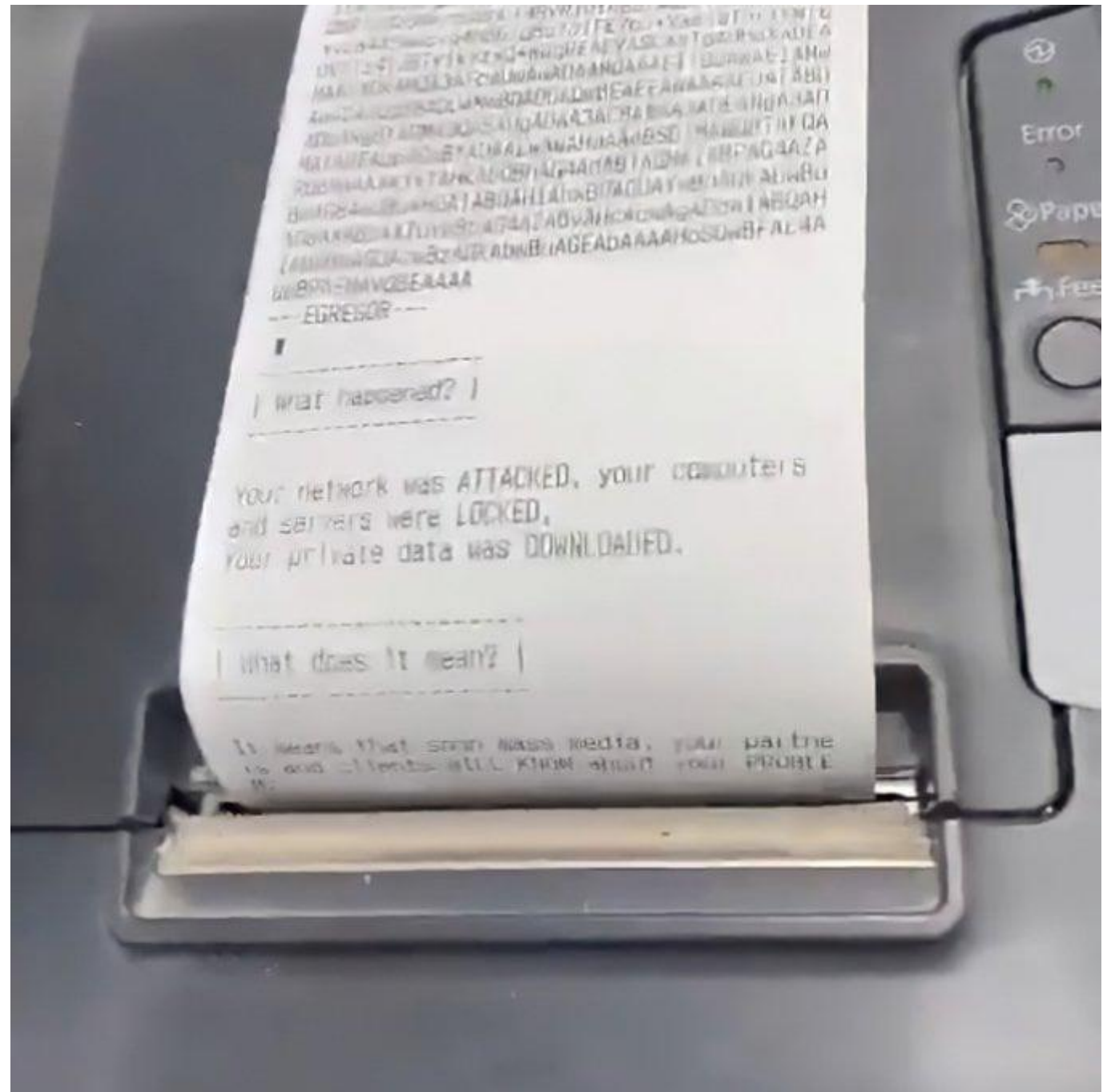
Command and Control

C2-Protokolle

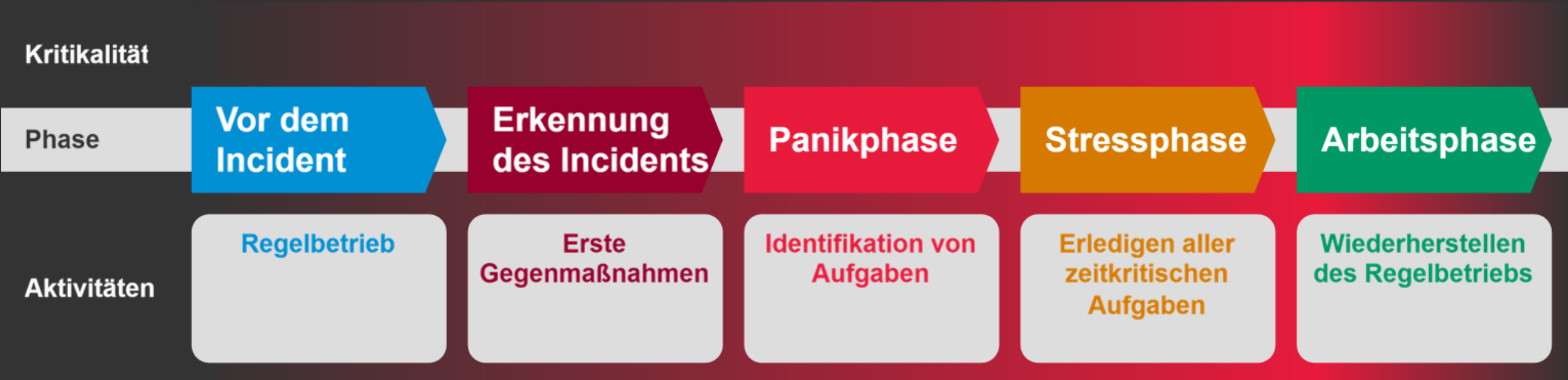


Die Verteidigerseite

Das böse Erwachen



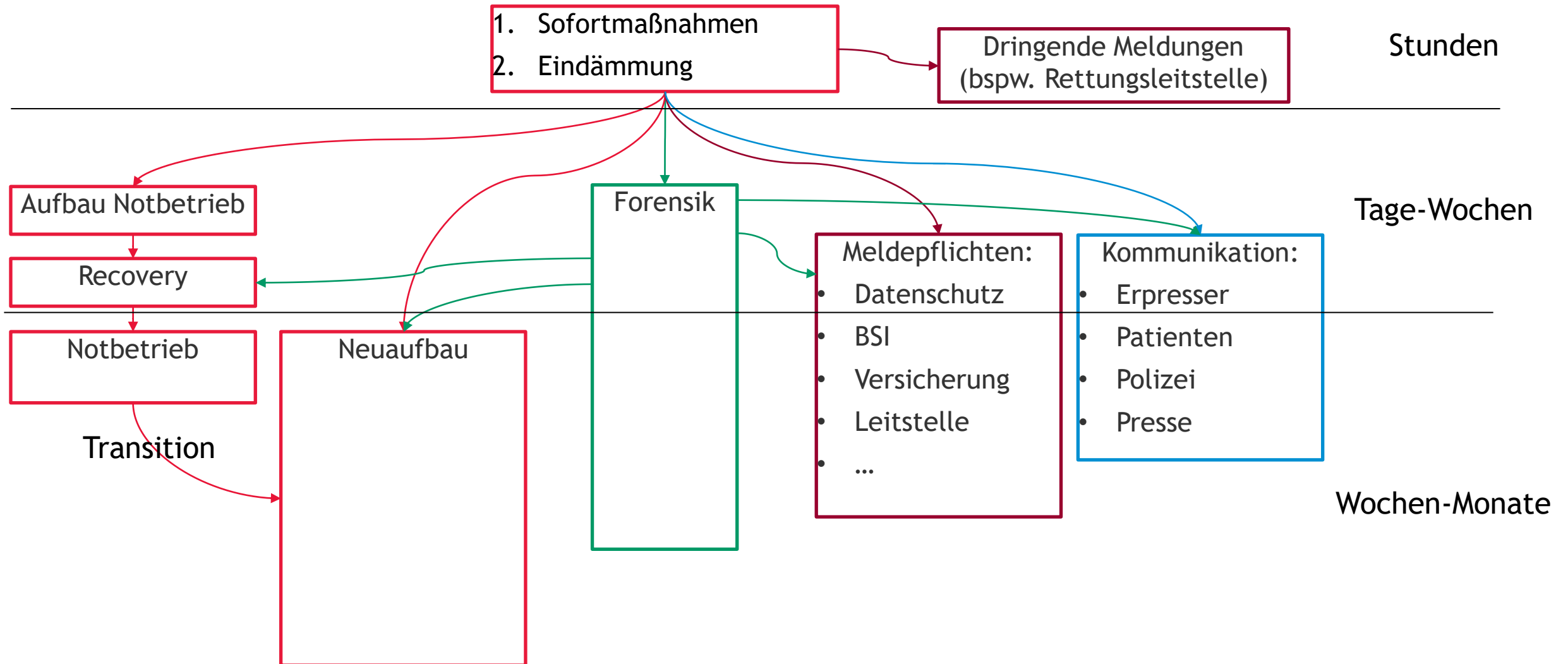
Security Incidents: Die Panikphase



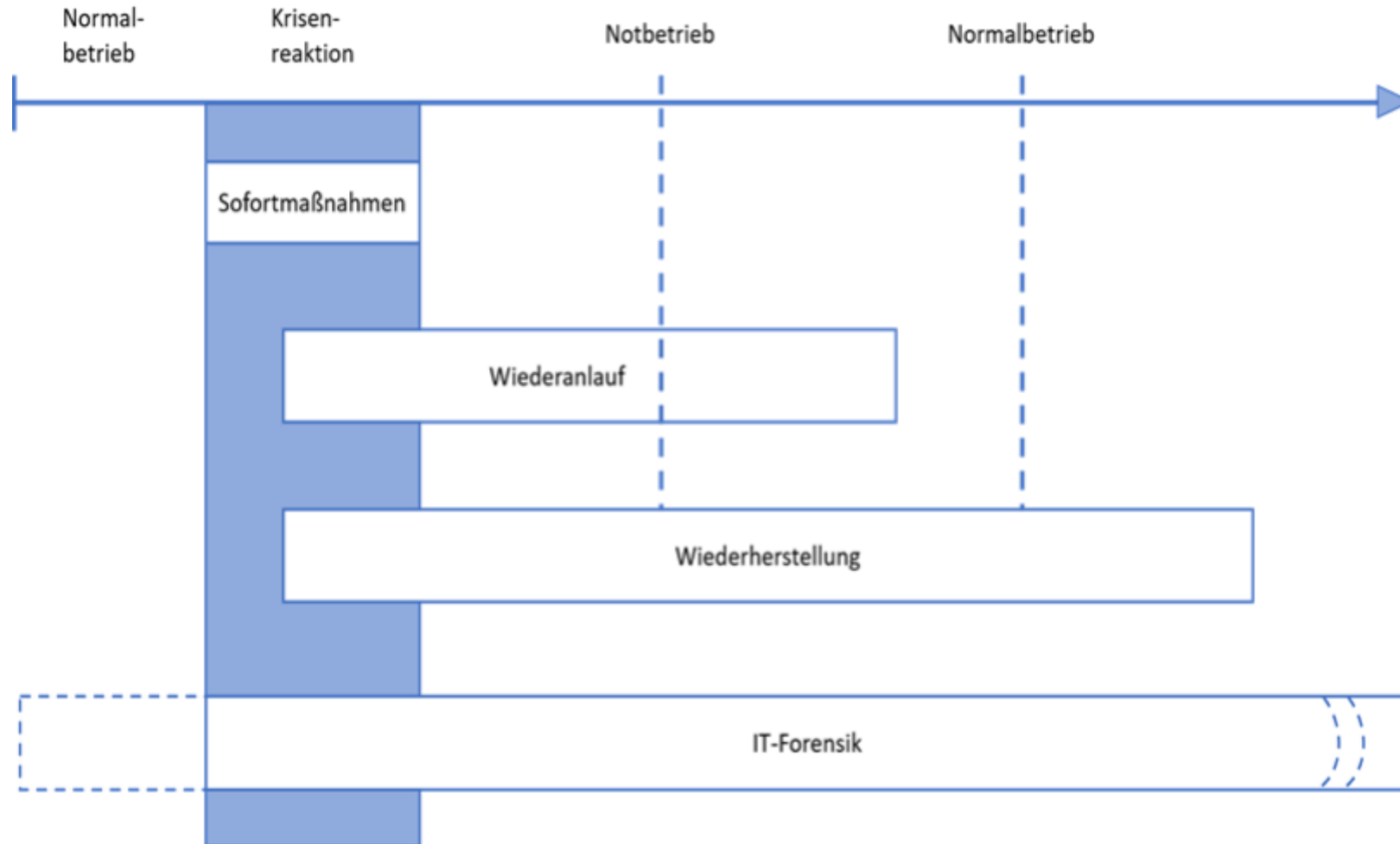
BDO Cyber Security GmbH, eine Gesellschaft mit beschränkter Haftung deutschen Rechts, ist eine rechtlich selbständige Konzerngesellschaft der BDO AG Wirtschaftsprüfungsgesellschaft. BDO AG Wirtschaftsprüfungsgesellschaft, eine Aktiengesellschaft deutschen Rechts, ist Mitglied von BDO International Limited, einer britischen Gesellschaft mit beschränkter Nachschusspflicht, und gehört zum internationalen BDO Netzwerk voneinander unabhängiger Mitgliedsfirmen.

BDO ist der Markenname für das BDO Netzwerk und für jede der BDO Mitgliedsfirmen. © BDO

Reaktion auf Vorfälle



Zeitliche Einordnung der Forensik



Sofortmaßnahmen I

Ziele

- Eingrenzen des Schadens
- Minimierung der Betriebsunterbrechung



Sofortmaßnahmen II

Ziele

- Eindämmung



Eindämmung

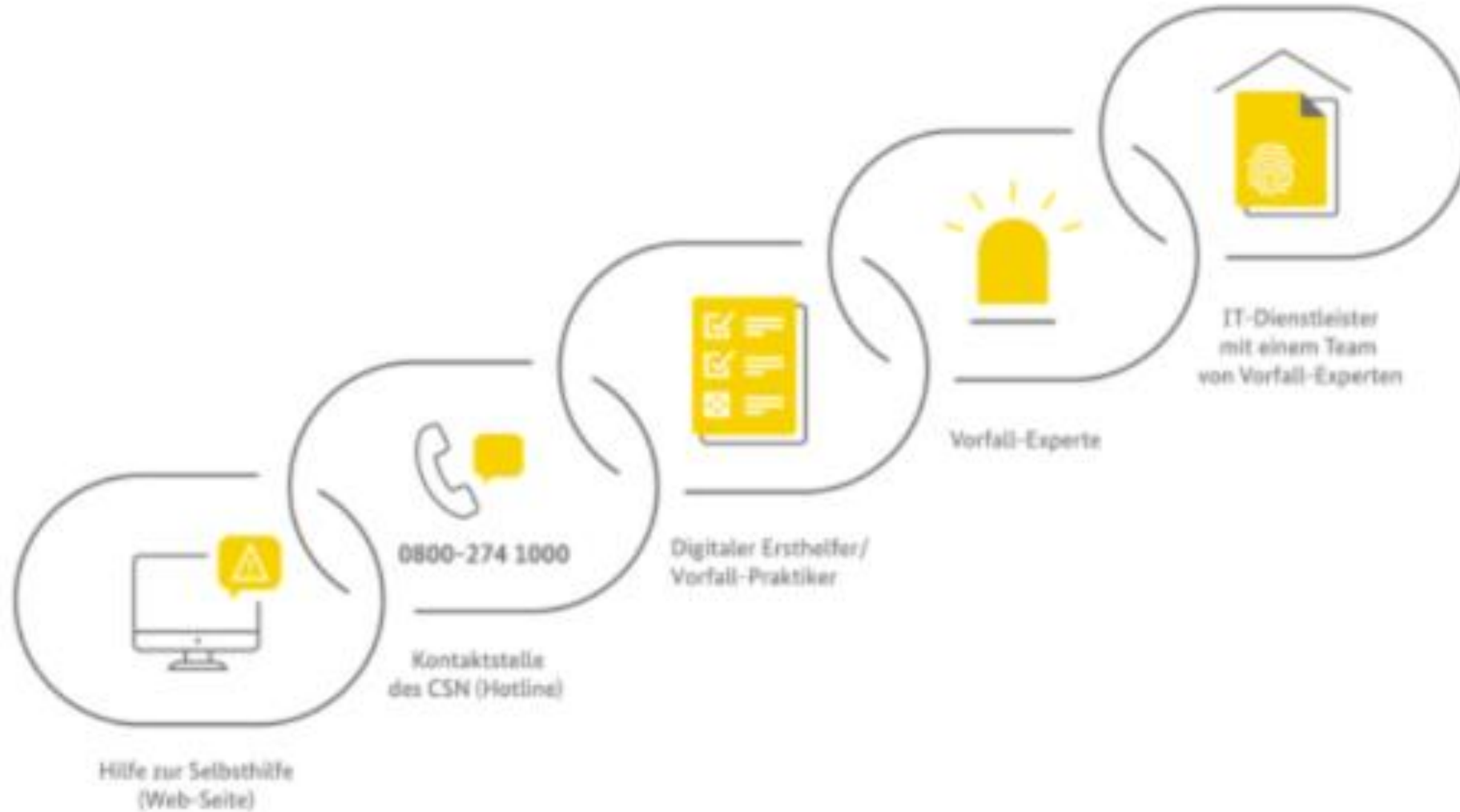
aka Einschränkung der Verfügbarkeit aka Betriebsunterbrechung

- Benutzerkonten sperren
- Passwörter zurücksetzen
- VPN unterbrechen
- VLANs trennen
- FW-Regeln deaktivieren
- Server ausschalten
- Netzkabel 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

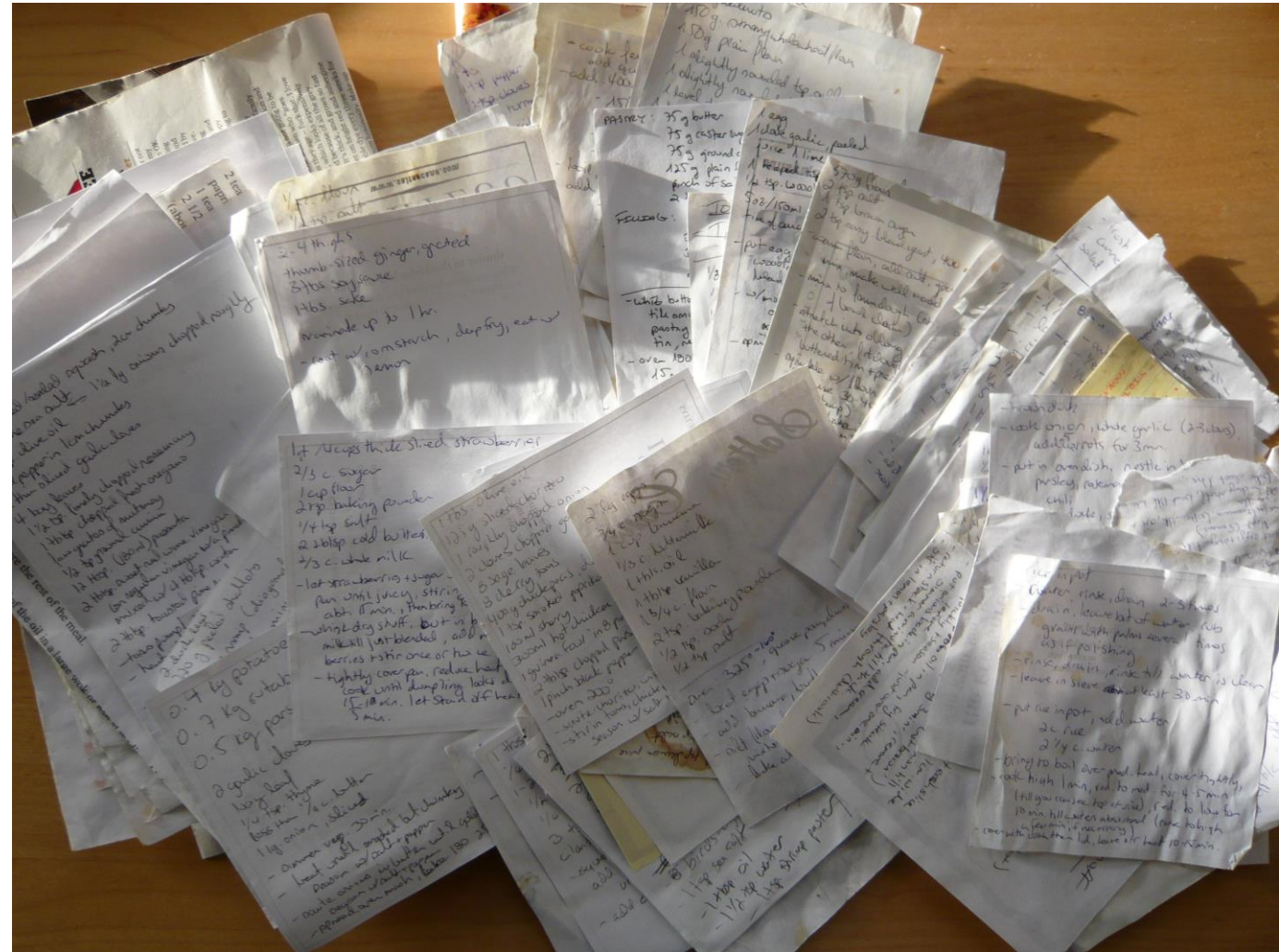


No-Go's im Incident Response

Unzureichende Dokumentation

Zielgruppen der Dokumentation:

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

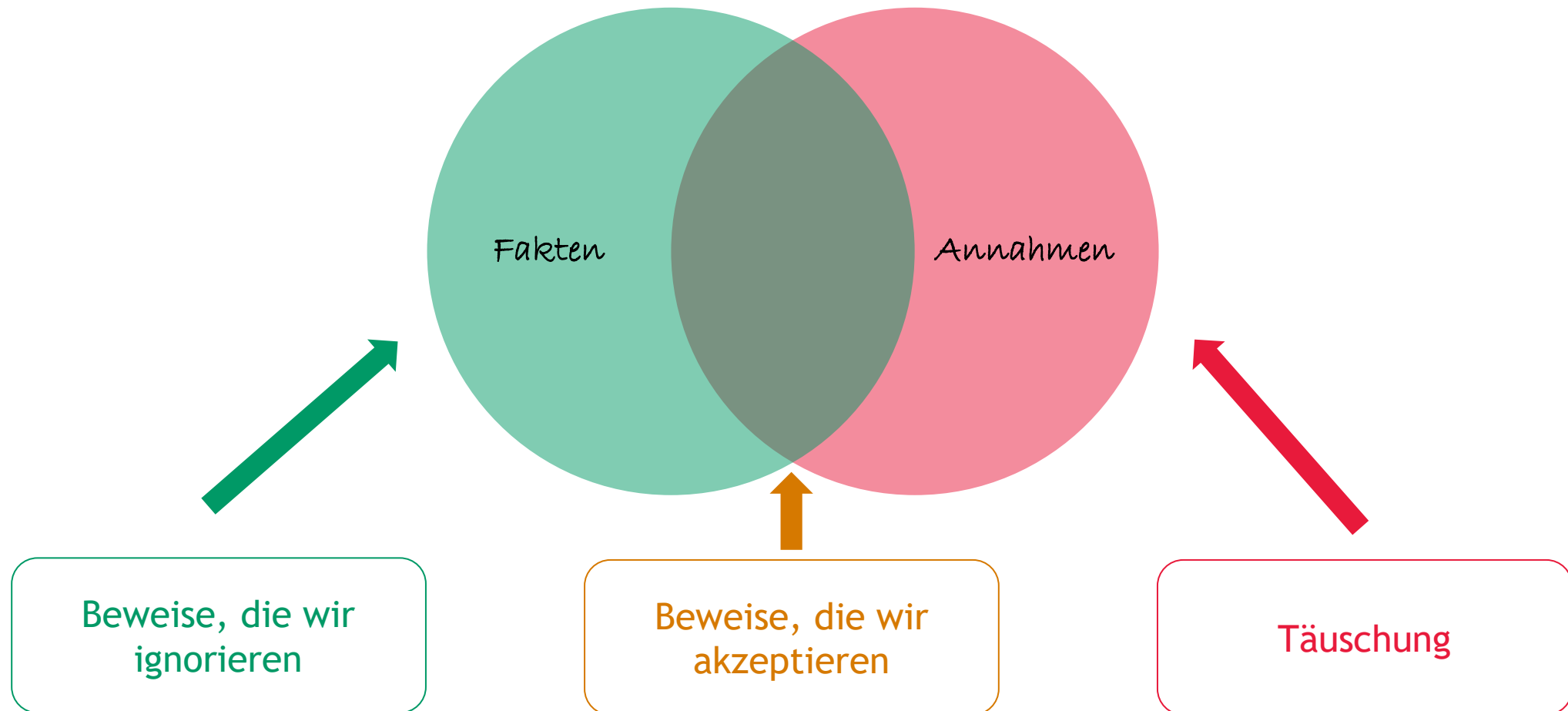


Unzureichende Koordination



Ignorieren von Beweismitteln

Confirmation Bias



Schnelles Handeln ohne Analyse

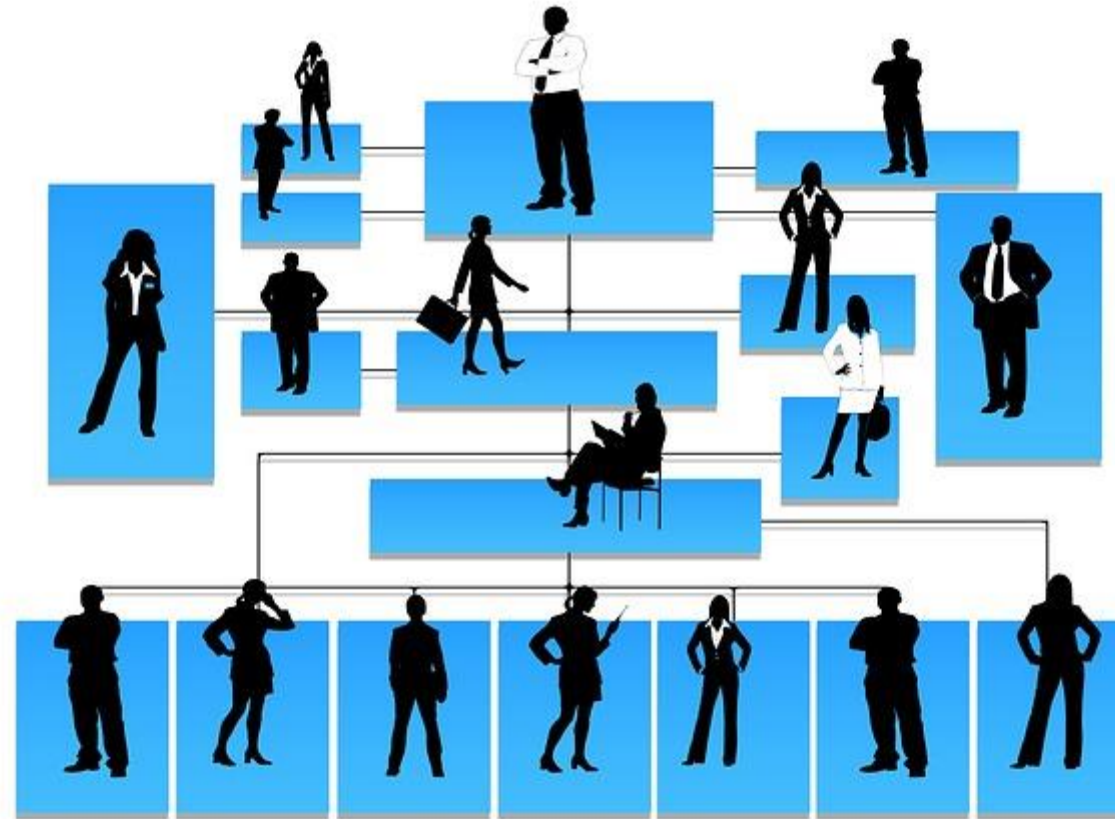
Schnelles Handeln ohne Analyse

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



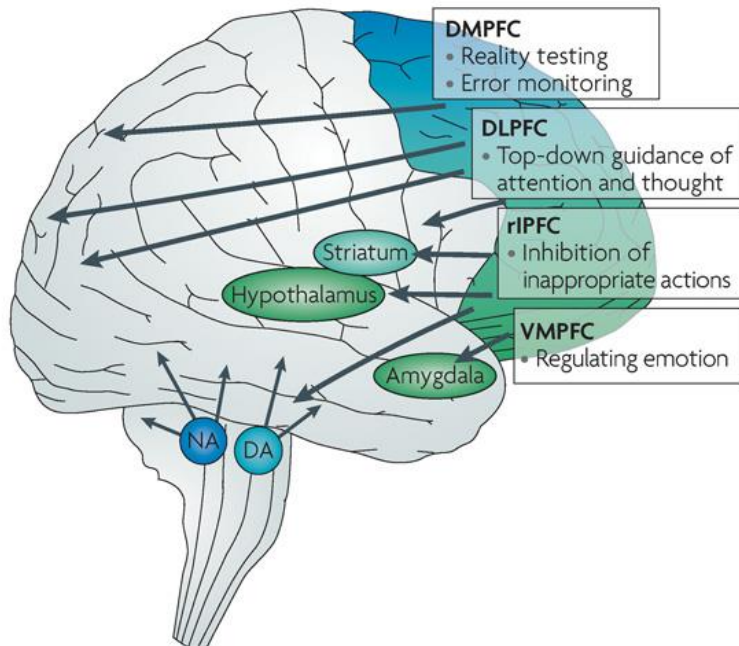
Vertrauliche Informationen teilen



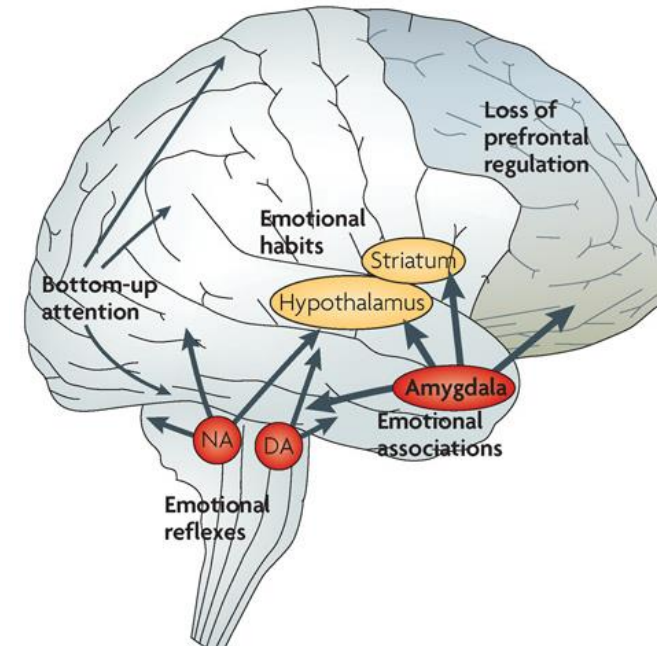
Emotionale Entscheidungen

NO PANIC

a Prefrontal regulation during alert, non-stress conditions



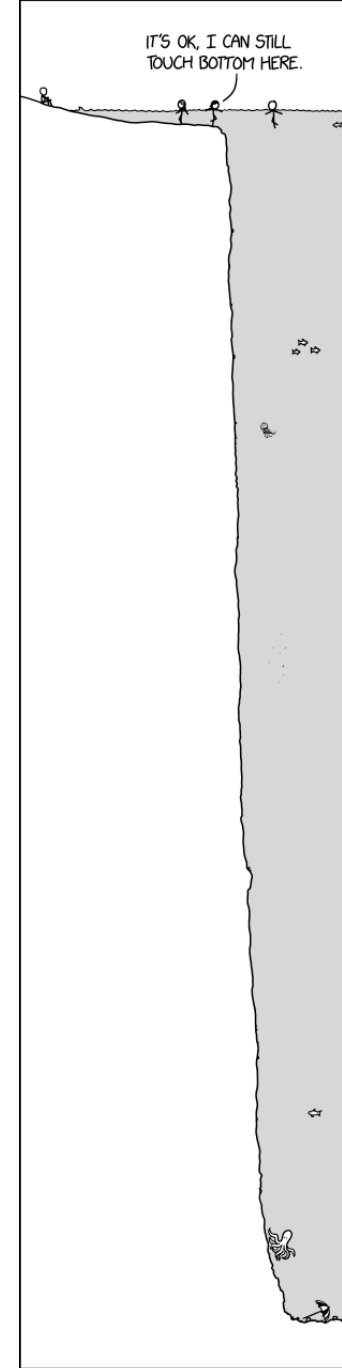
b Amygdala control during stress conditions



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

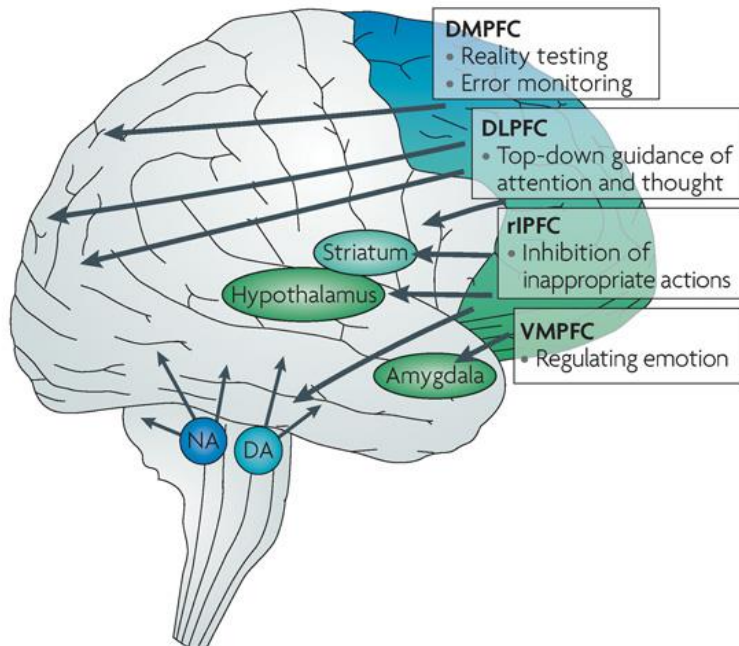
- Immer jeden informieren
- Arbeitszeit mit Status-Calls füllen
- Diskussionen über die Schwere des Incidents
- Keine Eskalation an die Verantwortlichen

Kommunikation und Stress

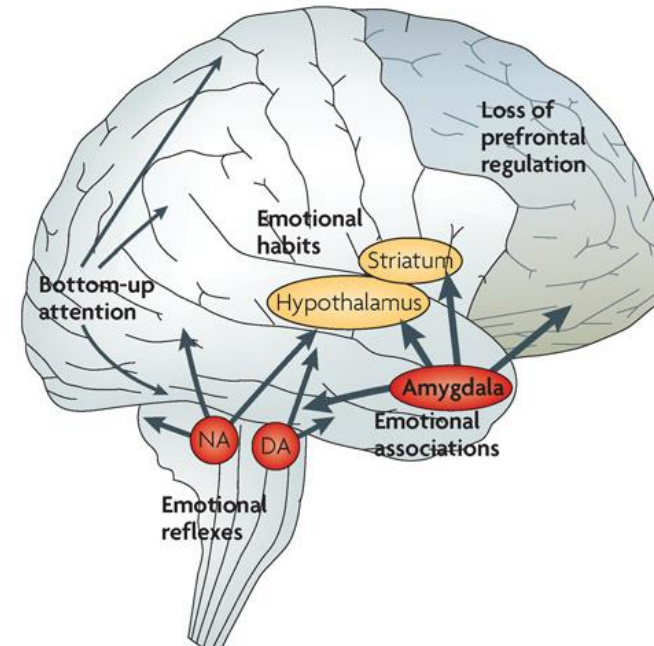
Emotionale Entscheidungen

NO PANIC

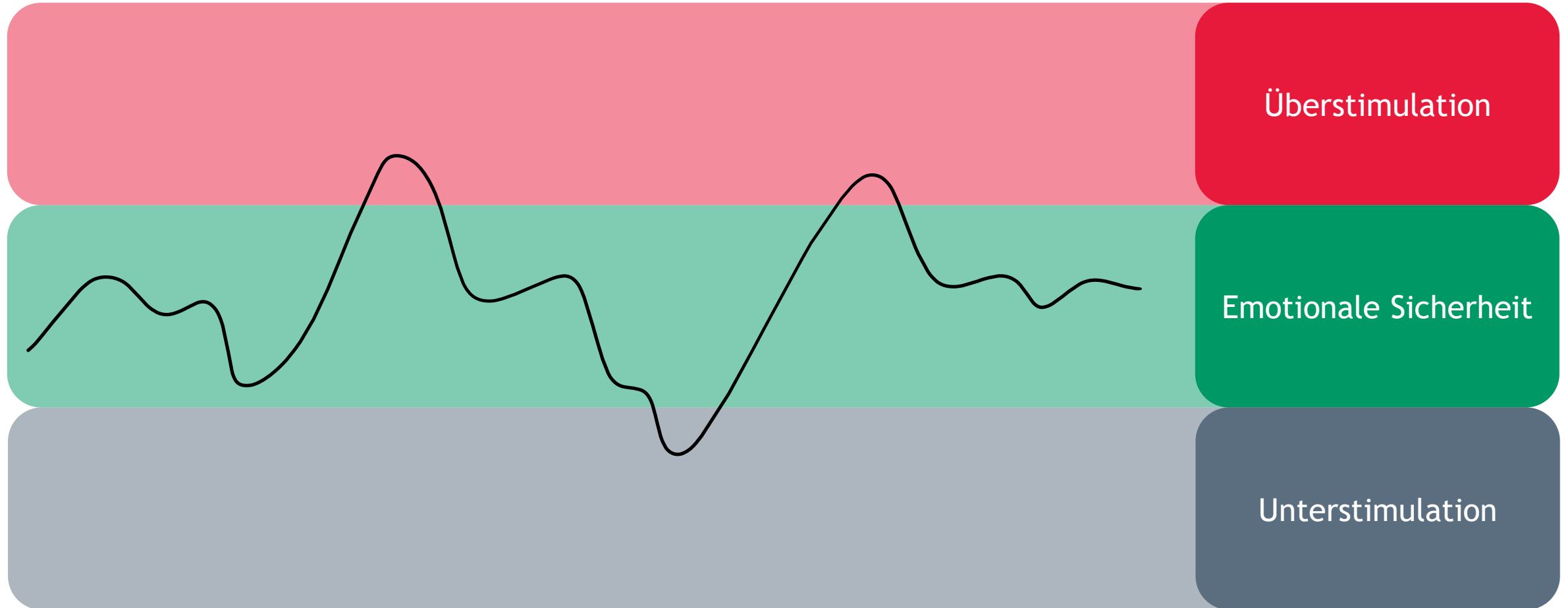
a Prefrontal regulation during alert, non-stress conditions



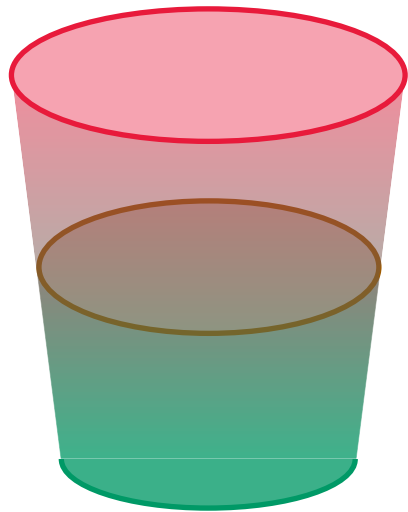
b Amygdala control during stress conditions



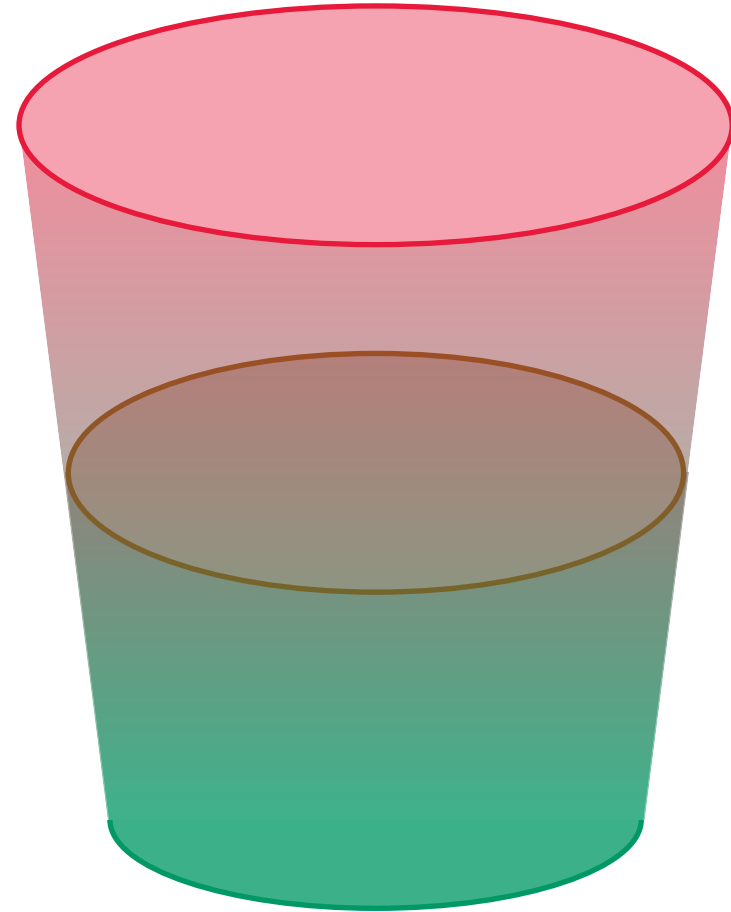
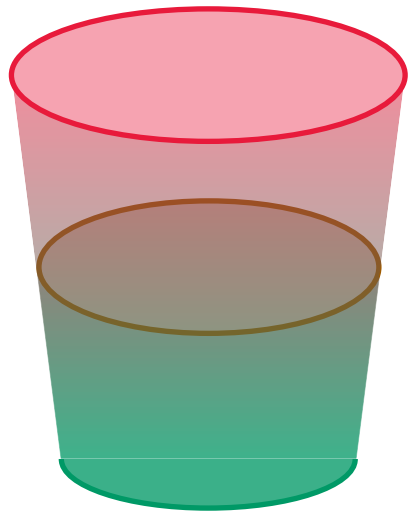
Stresstoleranzfenster



Stresstoleranz

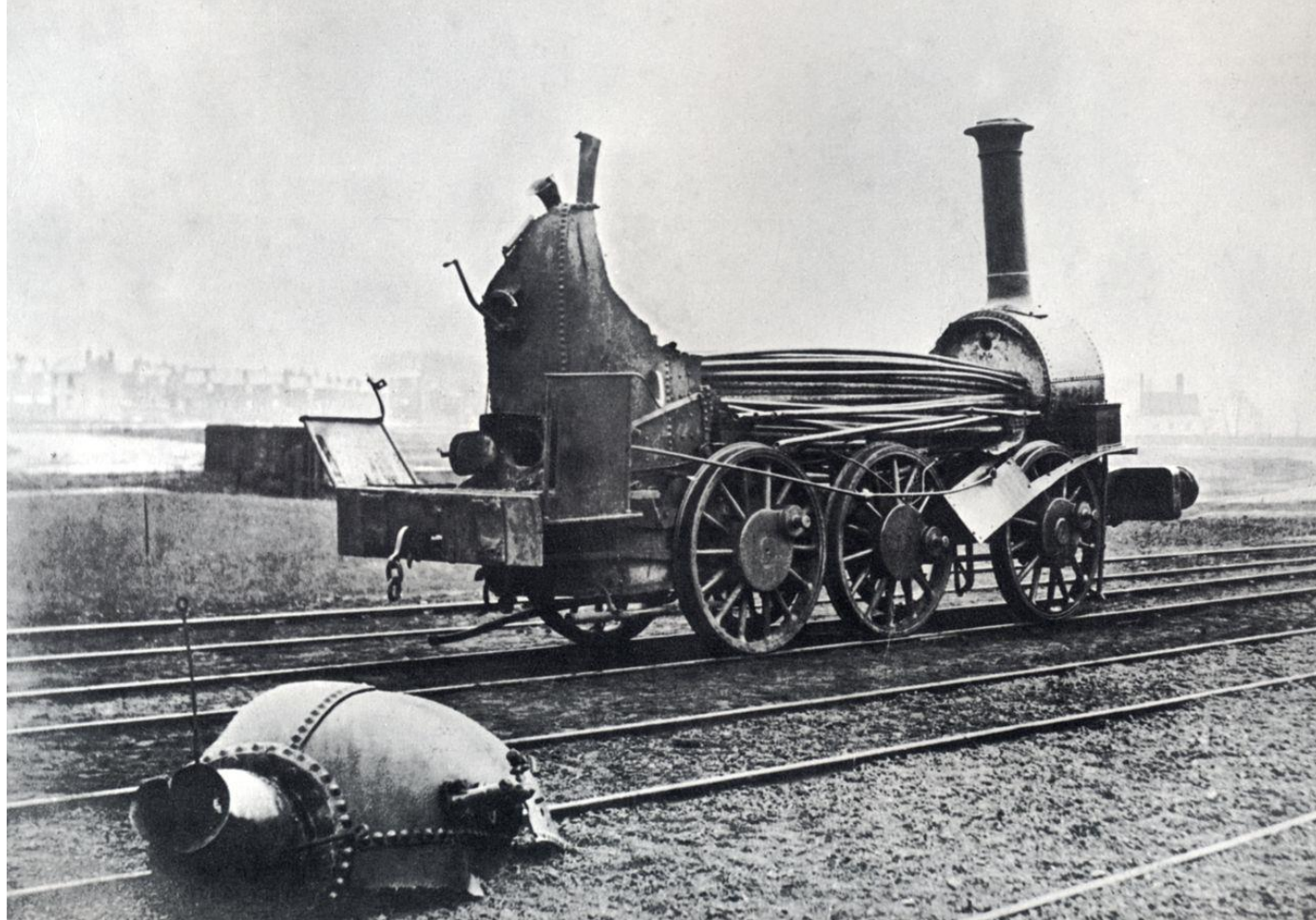


Stresstoleranz



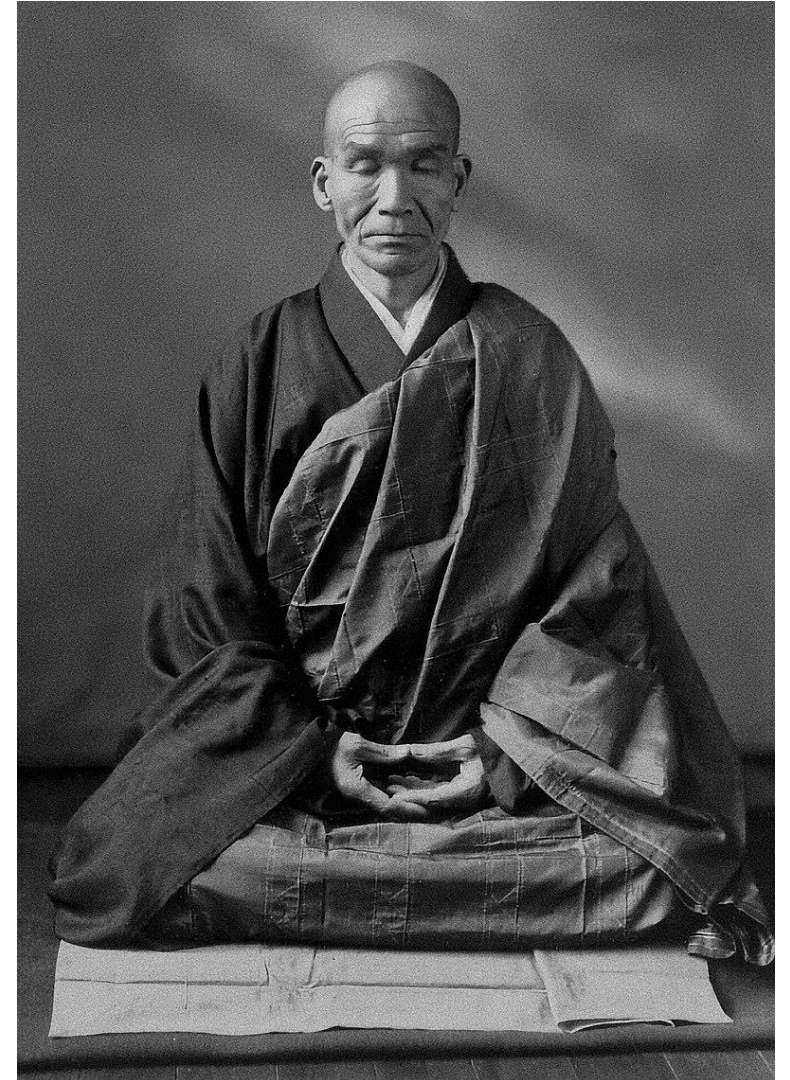
Techniken zur Stressbewältigung

Druck abbauen bevor es knallt



Techniken zur Stressbewältigung

Meditation / Yoga / Wandern / Musik hören / Theaterbesuch / ...



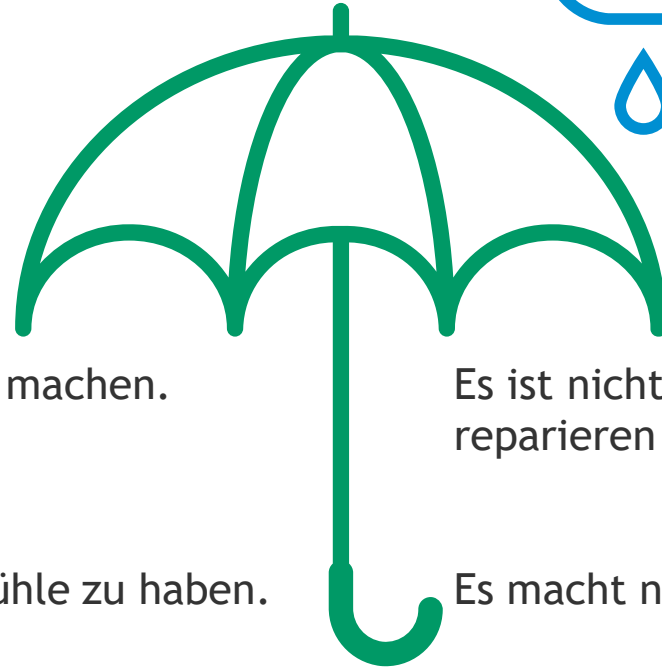
Techniken zur Stressbewältigung

Zeitmanagement

- Getting Things Done (GTD)
 - Sammeln, Verarbeiten, Organisieren, Durchsehen, Erledigen
 - Listen: Aktionslisten, Projektliste, 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.

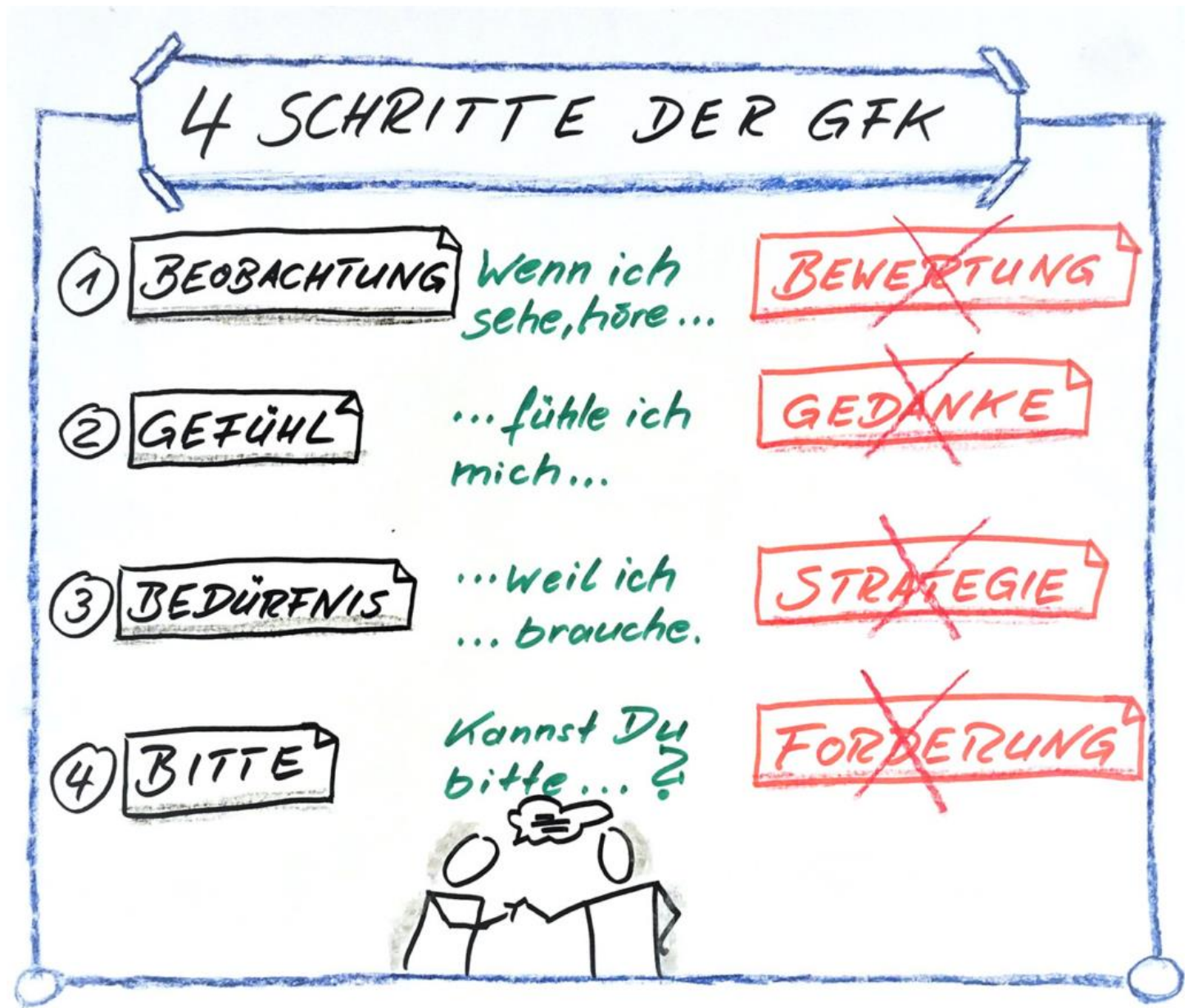
Es ist nicht mein Job Verantwortung für andere zu übernehmen.

Es ist ok „nein“ zu sagen.

Die Bedürfnisse andere muss ich nicht vorher erahnen.

Kommunikationstechniken

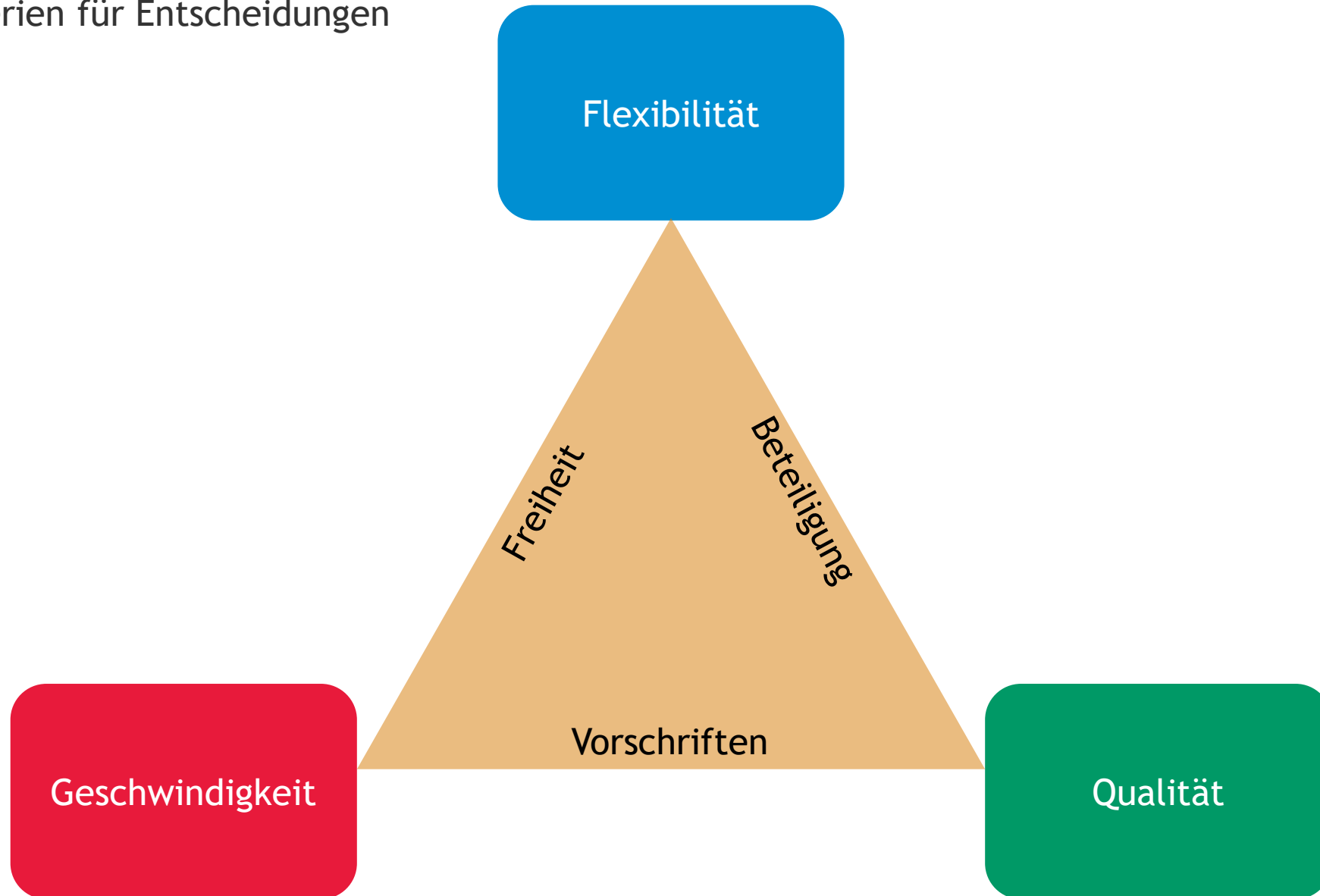
- Gewaltfreie Kommunikation



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

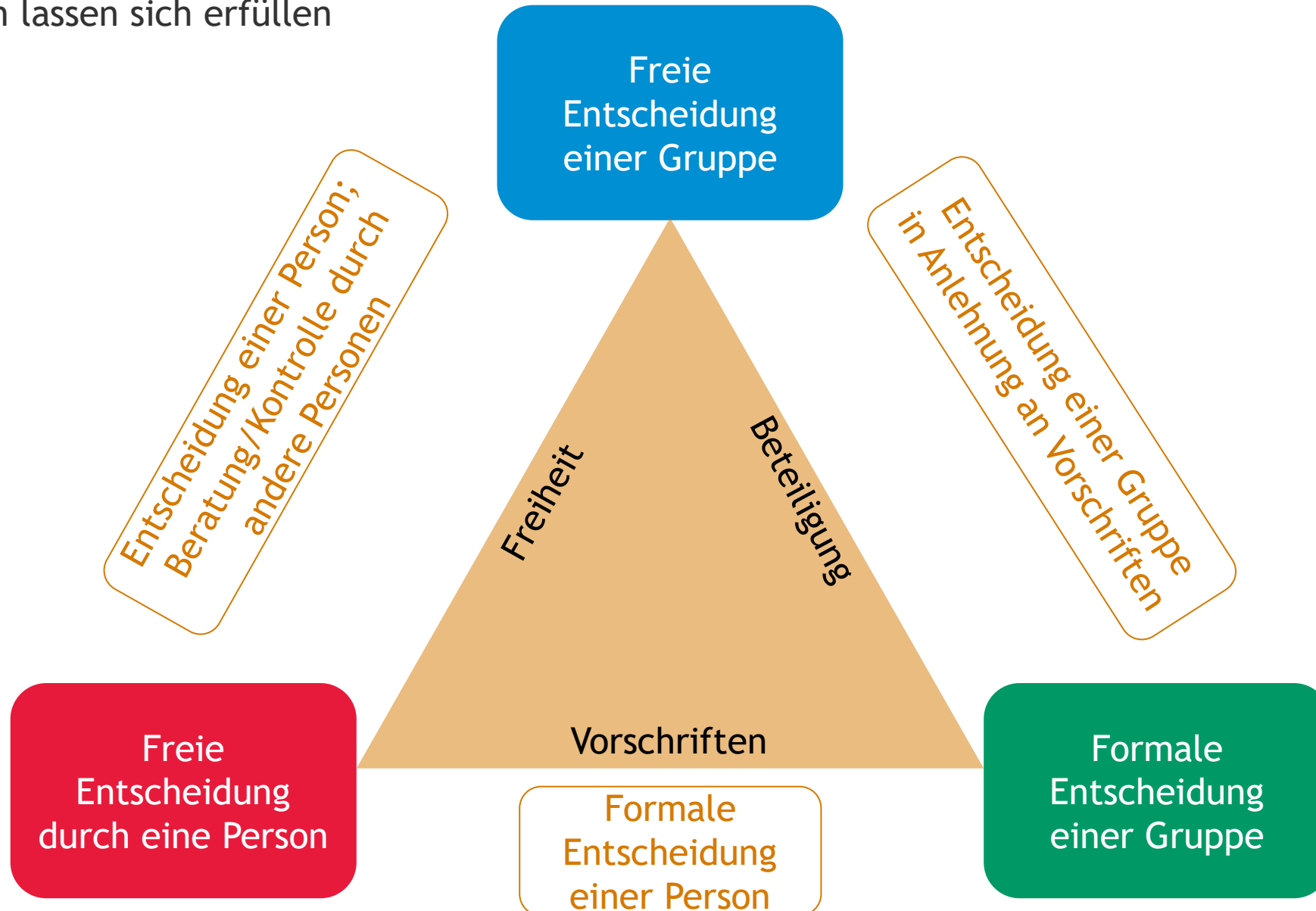
Methoden zur Entscheidungsfindung

Qualitätskriterien für Entscheidungen



Methoden zur Entscheidungsfindung

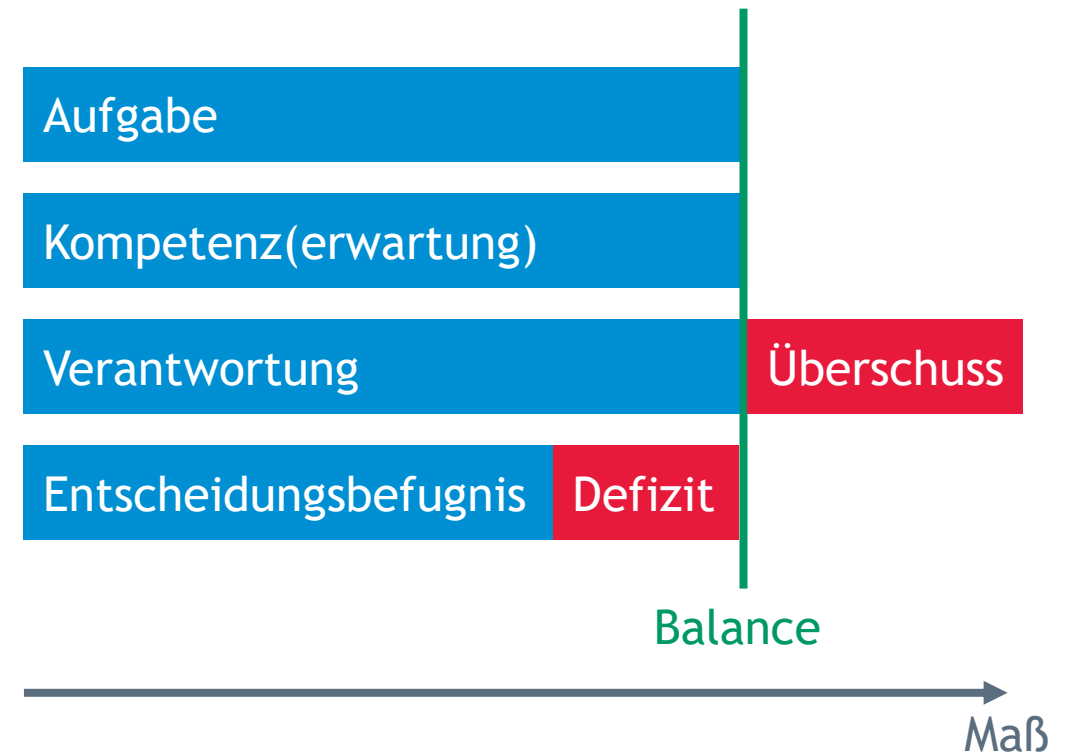
Zwei Kriterien lassen sich erfüllen



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