# Spotlight Cyber-Versicherung – Neue Risiken und neue Herausforderungen

Hamburg, 28.04.2025

1 Definition Cyber

2 Risikosituation

3 Schadenbeispiele

4 Cyber Versicherung

5 Prävention

# Definition Cyber

# Industrie 4.0 versus Bedrohungsszenarien

**Industrie 4.0**

Digitalisierung

Smart Products

Smart Mobility

Internet der Dinge

Software as a Service

Smart Factory

**Bedrohungsszenarien**

Payment Diversion Fraud

Fake President

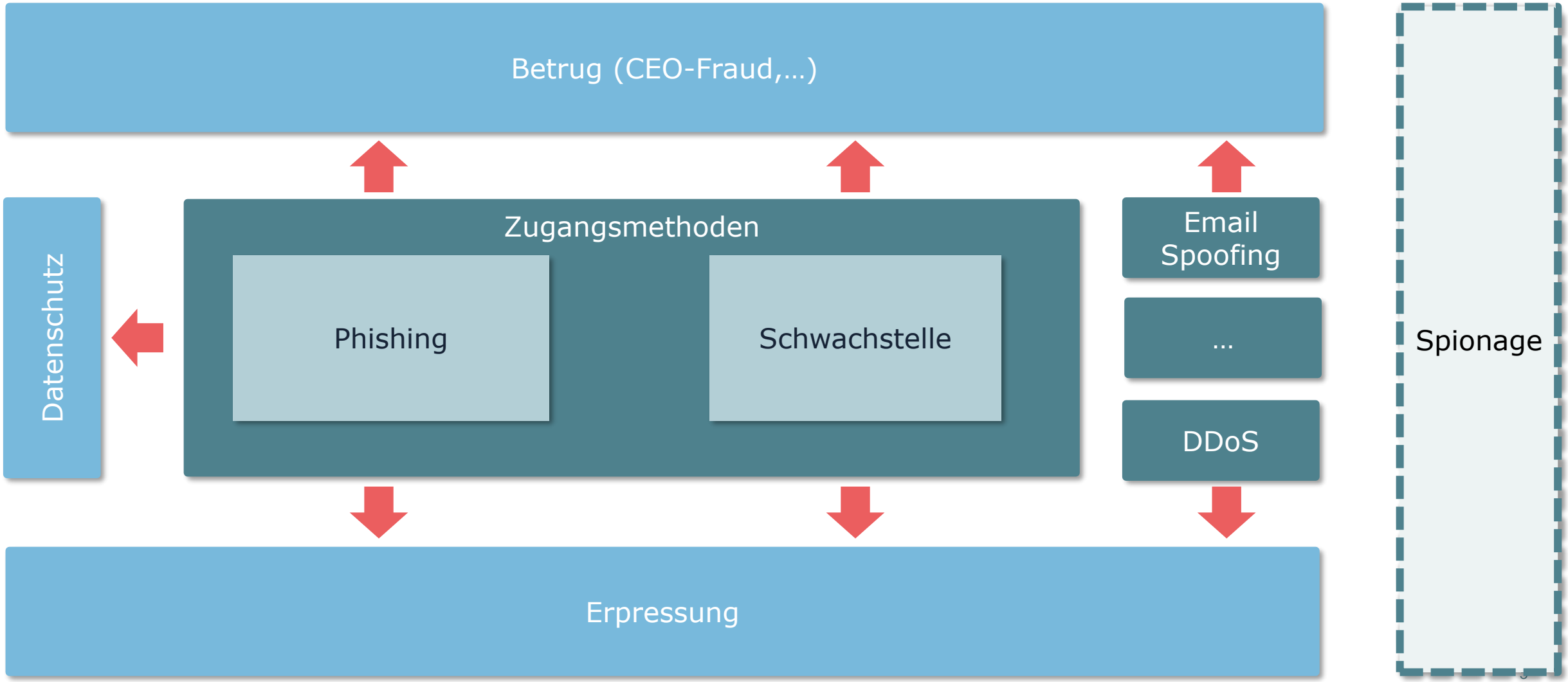
Ransomware

Denial of Service Angriff (DOS)

Crime as a Service

Social Engineering

# Definition Cyber-Kriminalität



# Risikosituation

# Allianz Risikobarometer 2025

Quelle: Allianz-Risk-Barometer-2025-Appendix.pdf

- Cyber auch 2025 Top Risiko
  - Global
  - national
- Als mögliche Auslöser auch indirekt in weitern Risiken enthalten

## Top 10 risks in Germany

*Source: Allianz Commercial.* Figures represent how often a risk was selected as a percentage of all responses for that country.
Respondents: 451. Figures don't add up to 100% as up to three risks could be selected

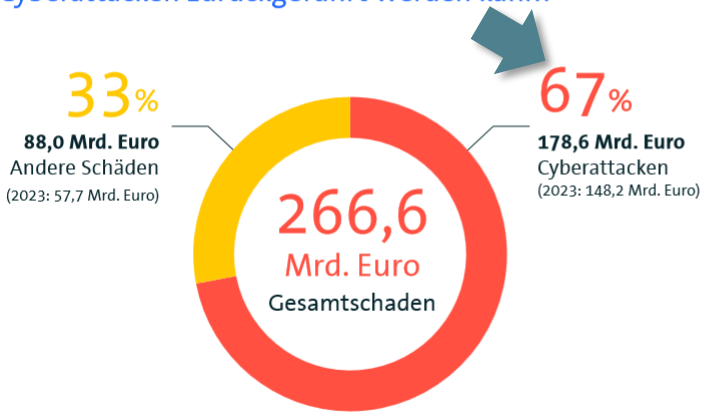
| Rank | | Percent | 2024 rank | Trend |
|---|---|---|---|---|
| 1 | Cyber incidents *(e.g., cyber crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)* | 47% | *1 (44%)* | → |
| 2 | Business interruption *(incl. supply chain disruption)* | 40% | *2 (37%)* | → |
| 3 | Natural catastrophes *(e.g., storm, flood, earthquake, wildfire, extreme weather events)*[1] | 29% | *5 (20%)* | ↑ |
| 4 | Changes in legislation and regulation *(e.g., new directives, protectionism, environmental, social, and governance, and sustainability requirements)* | 29% | *3 (23%)* | ↓ |
| 5 | Fire, explosion | 18% | *8 (16%)* | ↑ |
| 6 | Political risks and violence *(e.g., political instability, war, terrorism, coup d'état, civil unrest, strikes, riots, looting)*[2] | 17% | *8 (16%)* | ↑ |
| 7 | Climate change *(e.g., physical, operational, financial and reputational risks as a result of global warming)* | 17% | *6 (19%)* | ↓ |
| 8 | Shortage of skilled workforce | 15% | *4 (20%)* | ↓ |
| 9 | Market developments *(e.g., intensified competition / new entrants, M&A, market stagnation, market fluctuation)* | 13% | NEW | ↑ |
| 10 | Critical infrastructure blackouts *(e.g., power disruption)* or failures *(e.g., aging dams, bridges, rail tracks)* | 12% | NEW | ↑ |

1 Natural catastrophes ranks higher than changes in legislation and regulation based on the actual number of responses.
2 Political risks and violence ranks higher than climate change based on the actual number of responses.

# Bitkom Studie Wirtschaftsschutz 2024

## Cyberattacken verursachen zwei Drittel der Schäden

Wie hoch ist der prozentuale Anteil des entstandenen Gesamtschadens, der auf Cyberattacken zurückgeführt werden kann?




13 Basis: Unternehmen, die in den letzten 12 Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=812) | Quelle

## Schaden steigt auf 266,6 Milliarden Euro

Welche Schäden sind Ihrem Unternehmen im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

| Schaden durch... | Schadenssummen in Mrd. Euro (2024) | Schadenssummen in Mrd. Euro (2023) | Schadenssummen in Mrd. Euro (2022) |
|---|---|---|---|
| **Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen** | 54,5 | 35,0 | 41,5 |
| **Kosten für Rechtsstreitigkeiten** | 53,1 | 29,8 | 16,2 |
| **Umsatzeinbußen durch nachgemachte Produkte bzw. Plagiate** | 39,2 | 15,3 | 21,1 |
| **Kosten für Ermittlungen und Ersatzmaßnahmen** | 32,2 | 25,2 | 10,1 |
| **Datenschutzrechtliche Maßnahmen, z.B. durch Behörden** | 27,2 | 12,4 | 18,3 |
| **Imageschaden bei Kunden oder Lieferanten, Negative Medienberichterstattung** | 20,2 | 35,3 | 23,6 |
| **Patentrechtsverletzungen, auch vor Anmeldung** | 14,8 | 10,4 | 18,8 |
| **Erpressung mit gestohlenen Daten** | 13,4 | 16,1 | 10,7 |
| **Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen** | 11,2 | 21,5 | 41,5 |
| **Geldabfluss durch Betrugsversuche** | 0,8 | 3,9 | - |
| **Sonstige Schäden** | 0 | 1,1 | 0,9 |
| **Gesamtschaden pro Jahr** | **266,6** | **205,9** | **202,7** |

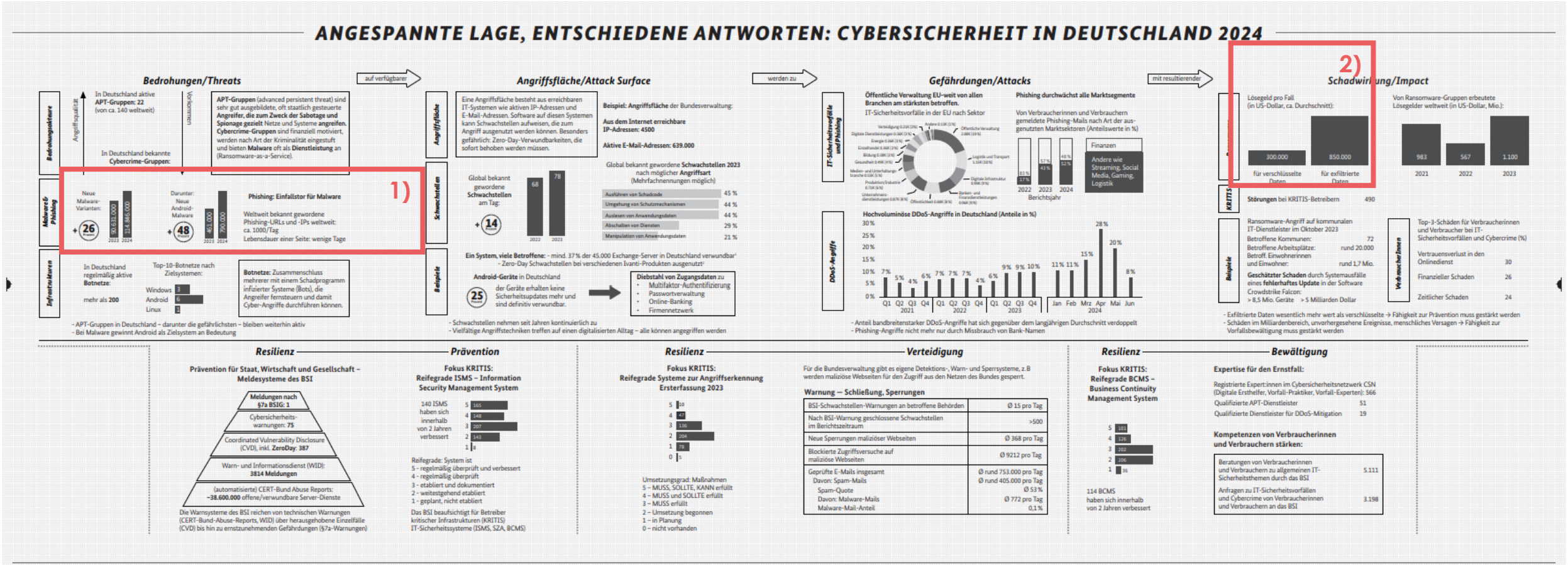
4 Basis: Alle Unternehmen (n=1.003) | Mehrfachnennungen möglich | rundungsbedingt kann die Summe der Einzelschäden vom Gesamtschaden abweichen. | Quelle: Bitkom Research 2024

bitkom

Quelle: https://www.bitkom.org/Bitkom/Publikationen/Studie-Wirtschaftsschutz

# Die Lage der IT-Sicherheit in Deutschland 2024

## Grafische Doppelseite, Quelle: BSI




1) +26% Maleware-Varianten und 1.000 Phishing-URLs pro Tag

2) Höhere Lösegelder pro Fall für exfiltrierte, als für verschlüsselte Daten

# Wer sind die Angreifer

## Festgestellte Cybercrime Beziehungen im Jahr 2020

Staatliche Auftraggeber

Serivceportale im Darknet

Geschäftsmodell

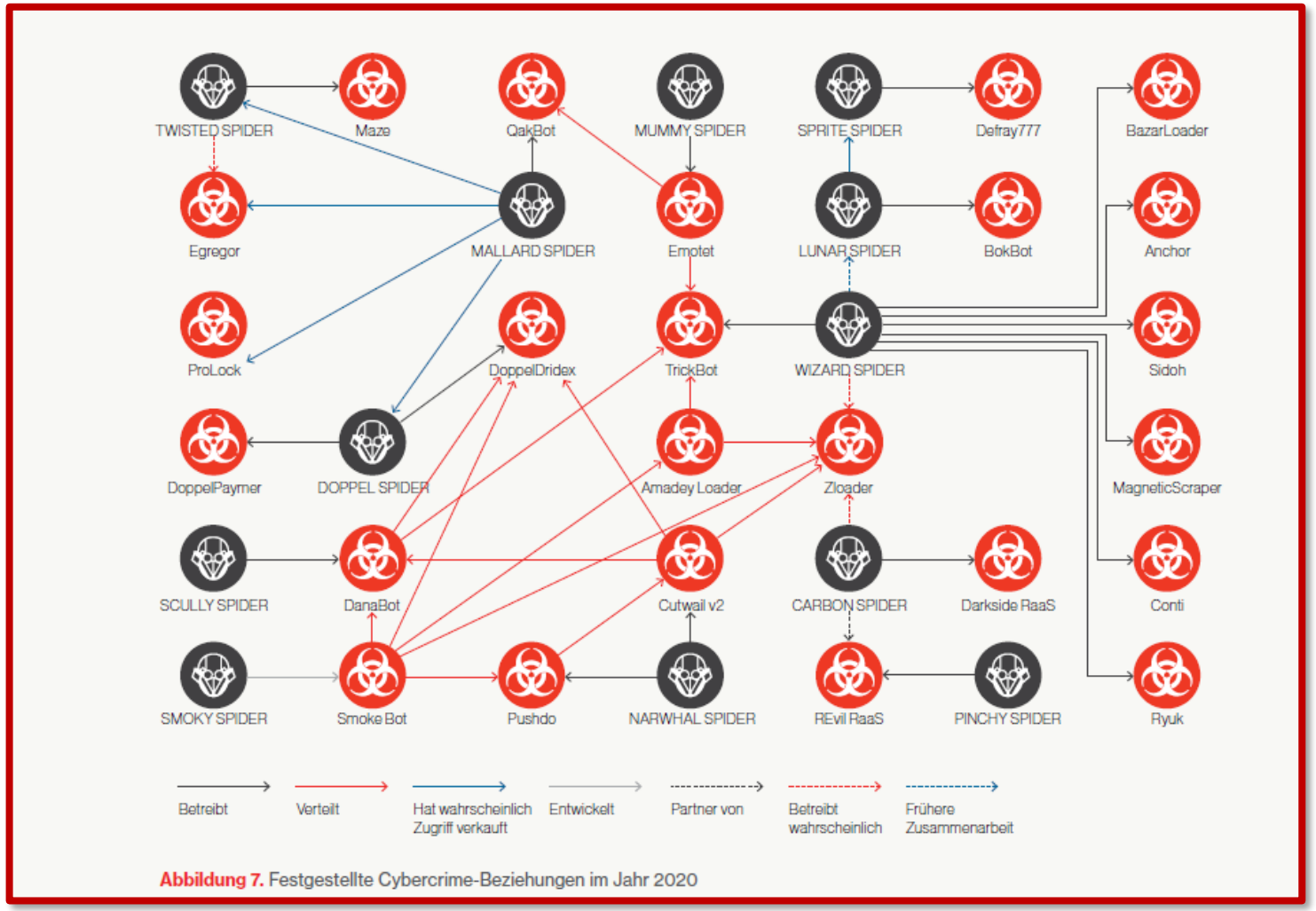



**Abbildung 7.** Festgestellte Cybercrime-Beziehungen im Jahr 2020

Spezialisierte Anbieter

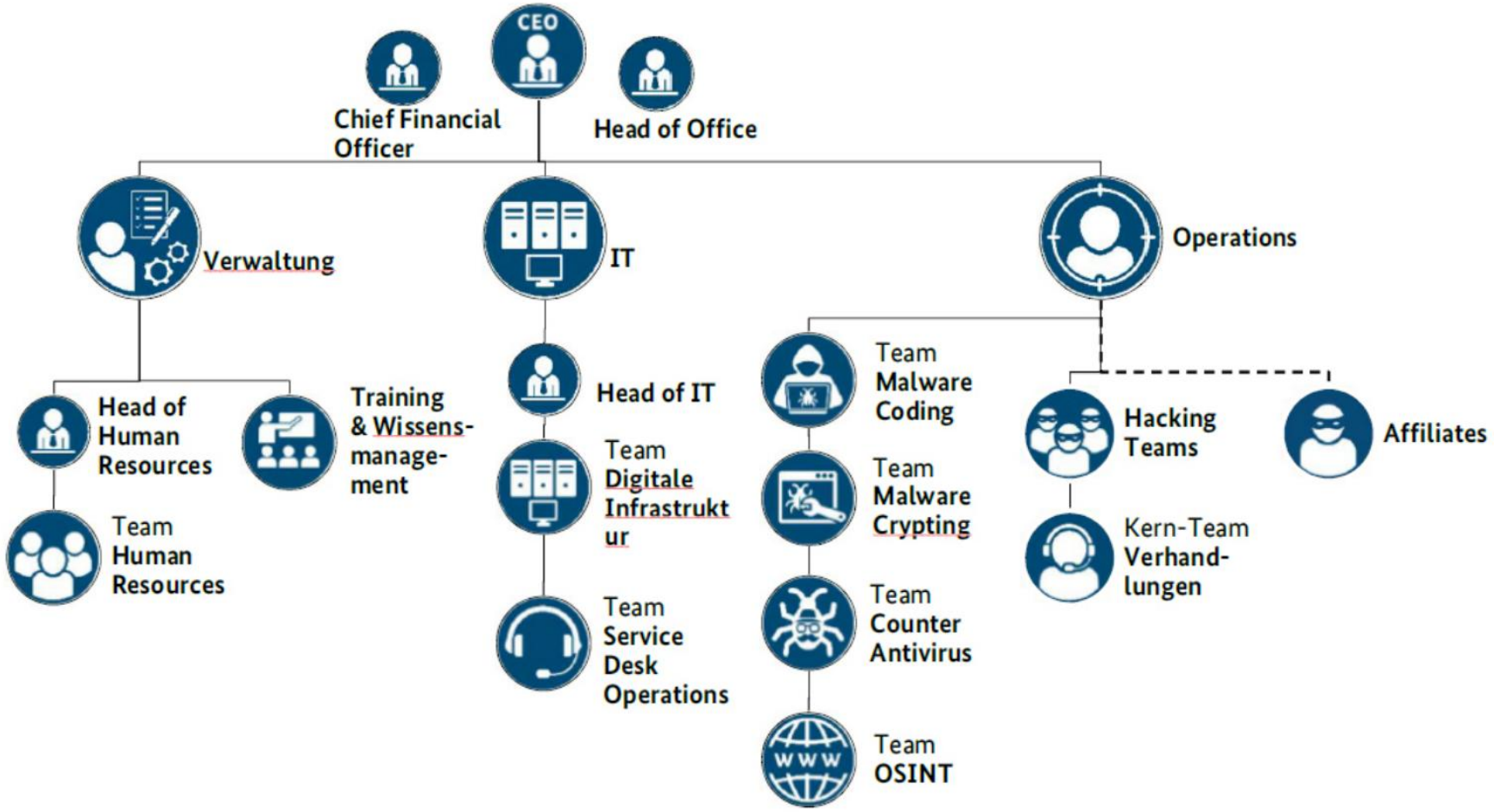
Crime as a service

Internationale Kooperationen

Quelle: Crowdstrike – Global Threat Report 2021

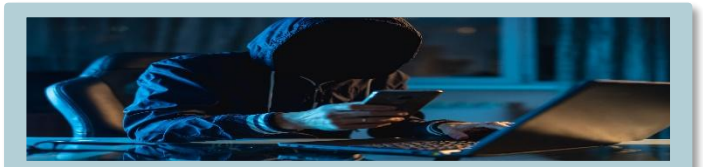
# Wie arbeiten Cyberkriminelle

Hoch professionelle Organisationen - Arbeitsteilung innerhalb einer RaaS-Gruppierung analog der Struktur eines mittelständischen Unternehmens mit ca. 30 - 100 Mitarbeitern




Quelle: BKA - Cybercrime Bundeslagebild 2022

# Motivation der Angreifer

| |  Spionage |  Bereicherung |  Krieg |
|---|---|---|---|
| Ziel | Betriebsgeheimnisse | Finanzmittel | Zerstörung |
| Organisation | Geschäftsmodell | Geschäftsmodell | staatl. motiviert |
| Ausbreitung | punktuell | begrenzt | unbegrenzt |
| Schaden-auswirkung | indirekt bzw. verzögert | direkt spürbar | direkt spürbar |
| Besonderheit | unerkannt und unbemerkt | Angriff muss „gut“ ausgehen | Zerstörung |

# NIS 2 - Network and Information Systems Directive

## Überblick

### Hintergrund

- EU-Richtlinie
- Umsetzung bis 17.10.2024
- Ziel: Stärkung der Netzwerk- und Informationssicherheit in der EU

Quellen:

BSI - FAQ zu NIS-2

### Betroffene

- Betreiber kritischer Anlagen
- Wichtige Einrichtungen
- 18 Wirtschaftssektoren
- ab 50 Beschäftigte / 10. Mio. EUR Jahresumsatz

Überprüfung:

BSI - NIS-2-Betroffenheitsprüfung - NIS-2-Betroffenheitsprüfung

### Auswirkungen

- Melde und Berichtspflichten
- Risikoanalyse „Cyberrisiken“
- Sicherheitsmaßnahmen
- Vorsorge für den Notfall
- Verschärfte Haftung des Managements
- Bußgelder

# Schadenbeispiele

# Schadenpressespiegel

**Artivon**

Am 21.11.2024 meldet einer der führenden Hersteller von Geräten für die Herzchirurgie, Opfer einer Ransomware-Attacke geworden zu sein. Die Auswirkungen sind so, dass sich das Unternehmen gezwungen sieht, eine Adhoc-Mitteilung (Form 8-K) gegenüber der SEC abzugeben.

csoonline.com, dailysecurityreview.com

**HCRG Care Group**

Im Februar 2025 ist der Presse zu entnehmen, dass die Ransomware-Bande Medusa behauptet, mehr als 2.000 sensible Datensätze erbeutet zu haben. HCRG ist in UK einer der größten Anbieter von Gesundheits- und Pflegediensten. Die Lösegeldforderung soll bei 2. Mio. USD liegen.
Dass es einen Vorfall gibt wird durch HCRG und den British National Health Service bestätigt.

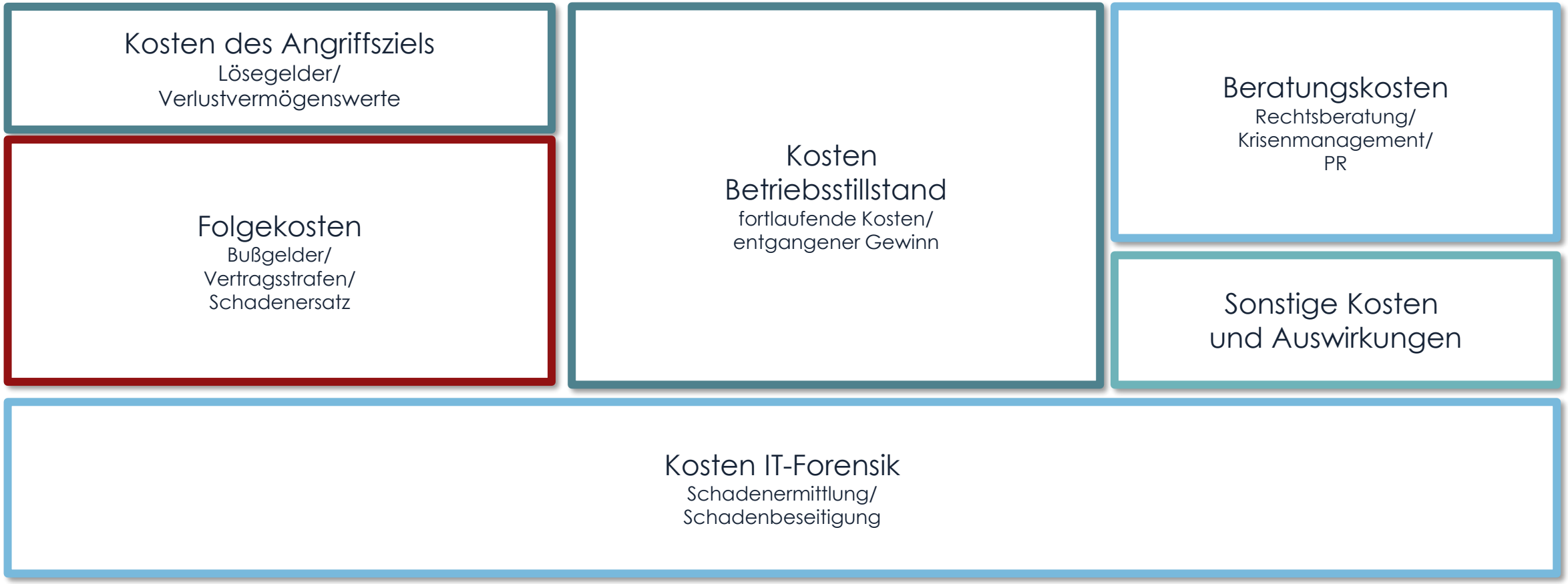
csoonline.com
cybersecurityintelligence.com

**Crowdstrike**

Im Juli 2024 führt ein fehlerhaftes Update de IT-Securitysoftware Falcon des Hersteller Crowdstrike dazu, dass weltweit Rechner stillstehen und nur durch einen manuellen Eingriff wieder in Gang gesetzt werden können. Dadurch dass das Update 76 min später verfügbar war wird der Schaden auf ca. 300. Mio. EUR geschätzt.

heise.de

# Auswirkungen von Cyber-Vorfällen




Darstellung ohne Maßstab

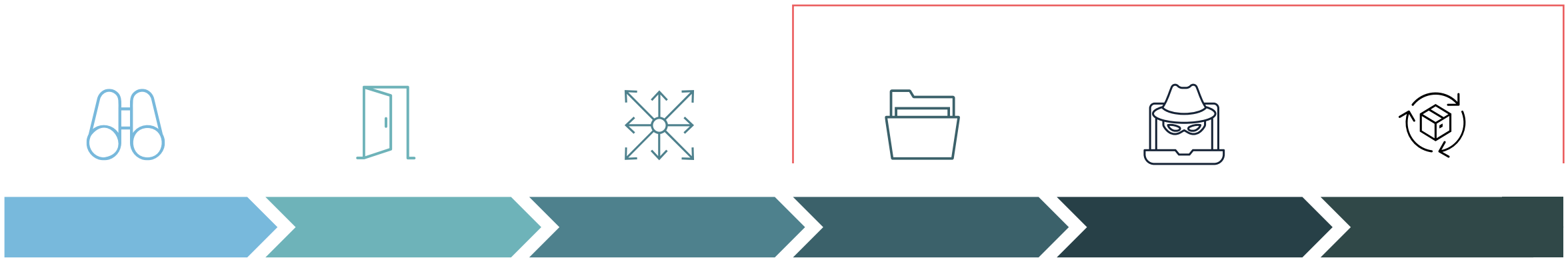
# Wie finden die Angreifer ihre Ziele?

## Schwachstellen bleibt selten unentdeckt

**Annahme**

**Realität**

# Ablaufplan Ransomware-Angriff



Phishing

Zutritt

Ausbreitung

Archivierung

Erpressung

Wiederanlauf

Schwachstelle

Krisenmanagement

# Ransomware-Angriff – Wie lange stehen wir?

## Gute Vorbereitung – Schnelle Reaktion

- Frühzeitige Reaktion
- Verfügbarkeit Dienstleister
- Analysebedarf
- Verfügbarkeit Backups
- Wiederanlauffähigkeit der Infrastruktur

# KI und Cyber

Erkennung

Täuschung

# Technologiefortschritt - Künstliche Intelligenz

Quelle: https://www.nzz.ch/feuilleton/deepfakes-wenn-der-papst-ploetzlich-wie-ein-rapper-aussieht-ld.1732304


Im März 2023 tauchte ein Video von Wolodymyr Selenskyj auf, in dem der ukrainische Präsident seine Streitkräfte scheinbar dazu aufrief, ihre Waffen niederzulegen und sich der russischen Armee zu ergeben. Dabei handelte es sich jedoch um ein Deepfake-Video. (© https://www.youtube.com/watch?v=X17yrEV5sl4; Screenshot; 08.11.2023)

Quelle: https://www.bpb.de/lernen/digitale-bildung/werkstatt/542670/deepfakes-wenn-man-augen-und-ohren-nicht-mehr-trauen-kann/

## Videokonferenz voller KI-Klone: Angestellter schickt Betrügern 24 Millionen Euro

Bislang werden im Rahmen der "Chef-Masche" Angestellte zumeist von einer Person überzeugt, Geld herauszugeben. Ein Fall in Hongkong hat nun eine neue Qualität.

191

(Bild: fizkes/Shutterstock.com)

Quelle: https://www.heise.de/news/Videokonferenz-voller-KI-Klone-Angestellter-schickt-Betruegern-24-Millionen-Euro-9618064.html

Quelle: https://www.watson.ch/digital/kuenstliche-intelligenz/838459952-erkennst-du-die-ki-generierten-fake-fotos-hier-kannst-du-dich-testen

# Ablauf Zahlungsumleitungsbetrug





## Geschäftsvorfall

- z.B. Instandsetzung durch Werkstatt

## 1. Rechnung

- per Email
- vollständig richtig

## 2. Rechnung

- wenig später
- per Email
- Korrektur der 1. Rechnung
- neues Konto

## Zahlung

- der 2. Rechnung
- Kostenerstattung

## Mahnung

- Werkstatt erinnert an die Zahlung

# Cyber-Versicherung

# Cyber-Versicherung

## Deckungsinhalt

### Haftpflicht

- Datenschutzverletzungen
- Vertraulichkeitsverletzungen

Jeder Ransomware-Vorfall ist auch ein DSGVO-Vorfall und innerhalb von 72 medepflichtig (§ 33 DSGVO)

### Eigenschäden

- Wiederherstellungskosten Daten
- Ertragsausfall durch Umsatzverluste
- Cyber-Erpressung

Kostentreiber Betriebsunterbrechung

### Assistance

- Rechtsberatung
- PR-Berater
- IT-Forensik
- Information betroffener Daten-inhaber nach Datenschutzvorfall

Aktive Unterstützung im Schadenfall 24/7 erreichbar.

# Der Weg zur Cyber-Versicherung

**Vorbereitende Fragen:**

Welcher Vertriebsweg?

- Ausschreibungsplattformen
- Versicherer direkt
- Versicherungsmakler

Weiterer Beratungsbedarf?

**Zu klärende Fragen (Auswahl):**

- Welche Deckungssummen
- Welche Deckungsbausteine
- Welche Selbstbeteiligung

# Abgrenzung zu anderen Versicherungssparten

**Deckung für Schäden aus Verletzung der Informationssicherheit**

Assistance, Eigenschäden, Drittschäden.

**Cyber**

**Sach/ Elektronik**

**Keine Überschneidung**

Deckung für Sachschäden und daraus resultierende Ertragsausfälle

Daten sind keine Sachen

**Versichert sind Ansprüche Dritter aufgrund der beruflichen Tätigkeit**

I.d.R. Keine Eigenschäden, keine Assistance.

**Berufs-Haftpflicht**

**Vertrauens-schaden**

**Fließender Übergang, bei zielgerichtetem Vorgehen auch Überschneidung**

Deckung für Vermögensschäden durch vorsätzliche, strafbare und gezielte Handlungen

# Wichtige Klauseln

## Auflagen / Vorbehalte Obliegenheiten

- Fristen
- Konsequenzen der Nichteinhaltung
- Auflistung konkreter Maßnahmen
- Stand der Technik

## Repräsentanten

Wie weit wird der Kreis gezogen

- Geschäftsführer
- Vorstände
- Partner
- IT-Leiter

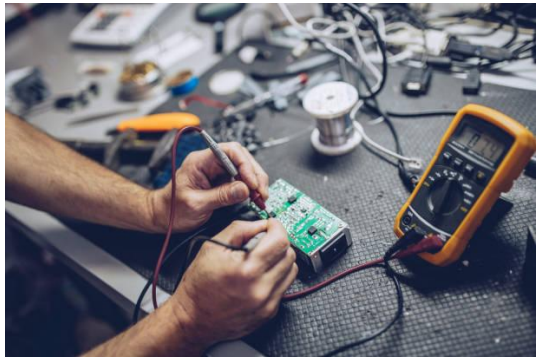
## Deckungserweiterung

- Cyberkriminalität
- Prävention
- technische Probleme

## Ausschlüsse / Sublimite

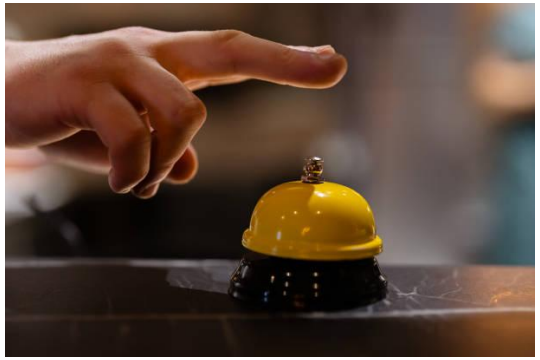
- Ransomware
- Lieferkettenschäden
- Kriegsausschluss
- IT-Dienstleister
- Cyber-Erpressung
- Erfüllungsanspruch
- Produkthaftung

# Wann lohnt sich eine Cyber-Versicherung



IT-Sicherheit
kein DIY


Bedarf
Risikotransfer



Kundenwunsch

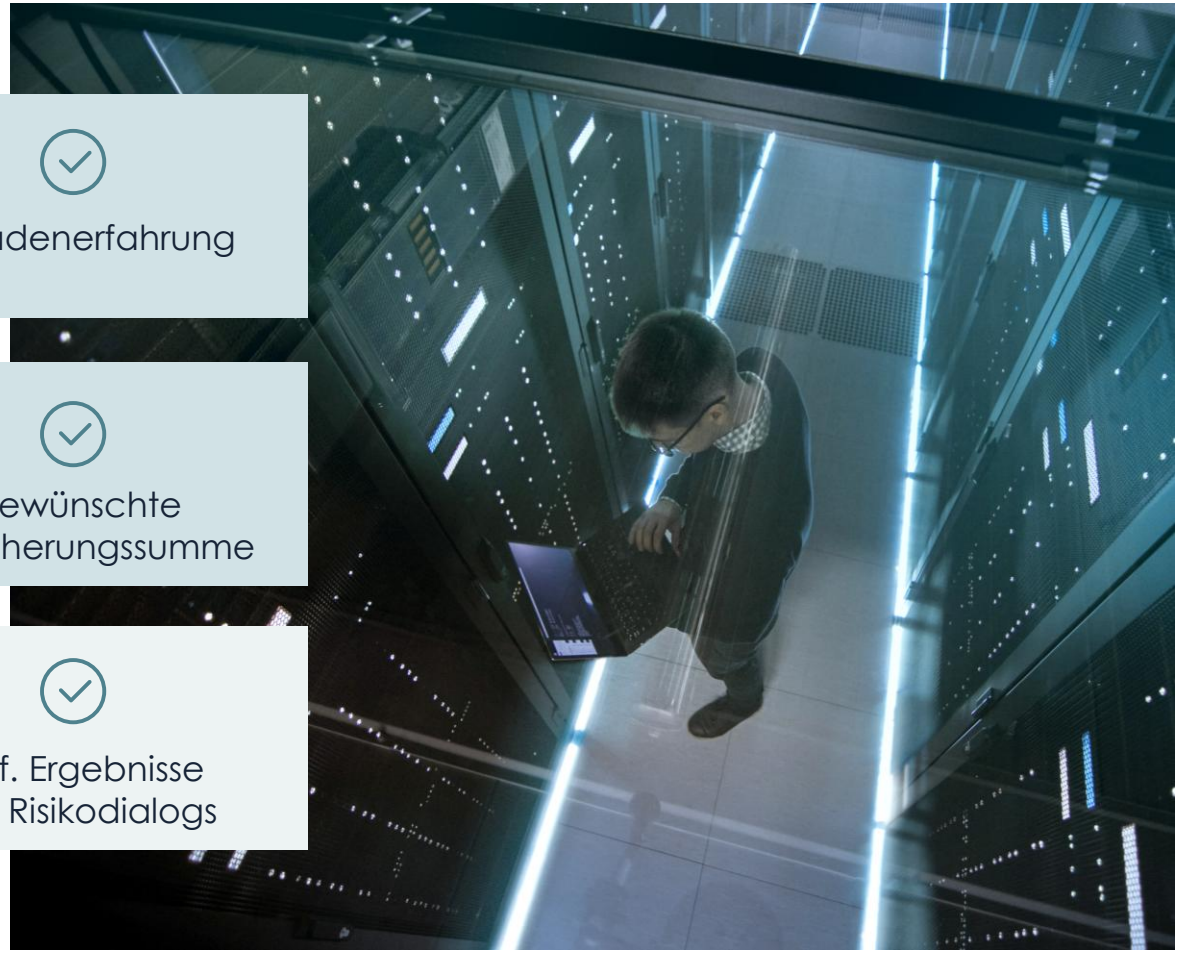

Gesetzliche oder
Regulatorische
Anforderungen

# Versicherungsanbieter

# Prämienkalkulation Cyberversicherung

## Berücksichtigte Faktoren der Versicherer

- Branche
- Umsatz
- Schadenerfahrung
- Risikoinformationen aus Fragebogen
- Zeichnungsrichtlinien des Versicherers
- gewünschte Versicherungssumme
- Selbstbeteiligung
- ggf. Zuschläge für Deckungserweiterungen
- ggf. Ergebnisse des Risikodialogs



# IT-Sicherheit

Empfehlungen basierend auf Schadenerfahrungen

- Multi Faktor Authentifizierung
- Offline Backups
- Altsysteme
- Patch-management
- Privileged Access Management
- Endpoint Protection
- Restore Tests
- Verantwortung
- Berechtigungs-konzept
- Pentest
- Notfallplan
- Keine privaten Geräte
- Awareness
- SIEM/SOC
- Segmentierung

# Prävention von Zahlungsmittelumleitungsbetrug

## Eigentlich ganz einfach

- 4 Augen-Prinzip konsequent umsetzen
- keine Zahlungen auf Zuruf
- Awareness-Schulungen
- keine Zahlung ohne Kommunikation oder schriftliche Anweisung
- Vertrauen ist gut, Kontrolle auch

# Ihre Fragen

Vielen Dank für Ihre Aufmerksamkeit

# Ihr Kontakt bei GGW


**Jan Kempermann**

Leiter Geschäftsbereich Wirtschaftskriminalität

+ 49 40 23768090 381

+49 178 240 7884

jan.kempermann@ggw.de

GGW GmbH
Chilehaus B – Fischertwiete 1 20095 Hamburg