die Mobiliar

Fachreferat zum Thema Cyber

Simon Seebeck, Kompetenzzentrum Cyber Risk
AM Suisse, 13.08.2025

Agenda

1. Intro
2. Bedrohungslage von heute und morgen
3. Wer steht im Visier der Cyberkriminellen?
4. Ausführungen zum aktuellen Markt
5. Welche Methoden verwenden Cyberkriminelle, um Menschen zu hacken?
6. Klassische Cyber-Schadenbilder
7. Präventionsmassnahmen

"Cybercrime" als eigene Volkswirtschaft?!

Wahrscheinlichkeit eines Gebäude- vs. Cyber-Schadens

Alle ***48 Minuten***

brennt es.

Alle ***8,5 Minuten***

ereignet sich ein Cybervorfall.

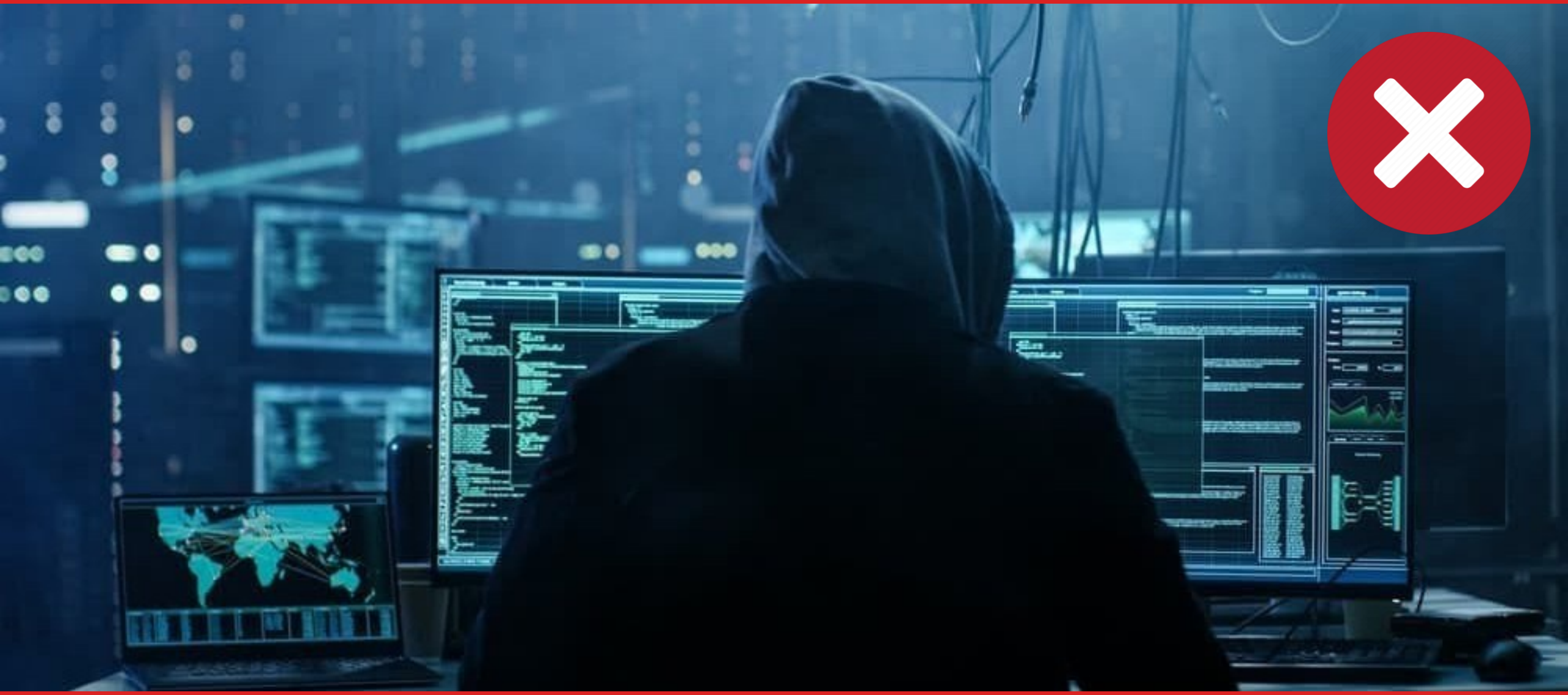
Quelle: Beratungsstelle für Brandverhütung BFB, Jahresdurchschnitt 2004-2023

Quelle: **Bundesamt für Cybersicherheit** BACS, 07.11.2024

Bei einer Cyber-Attacke haben viele ein Problem

Bedrohungslage heute und morgen

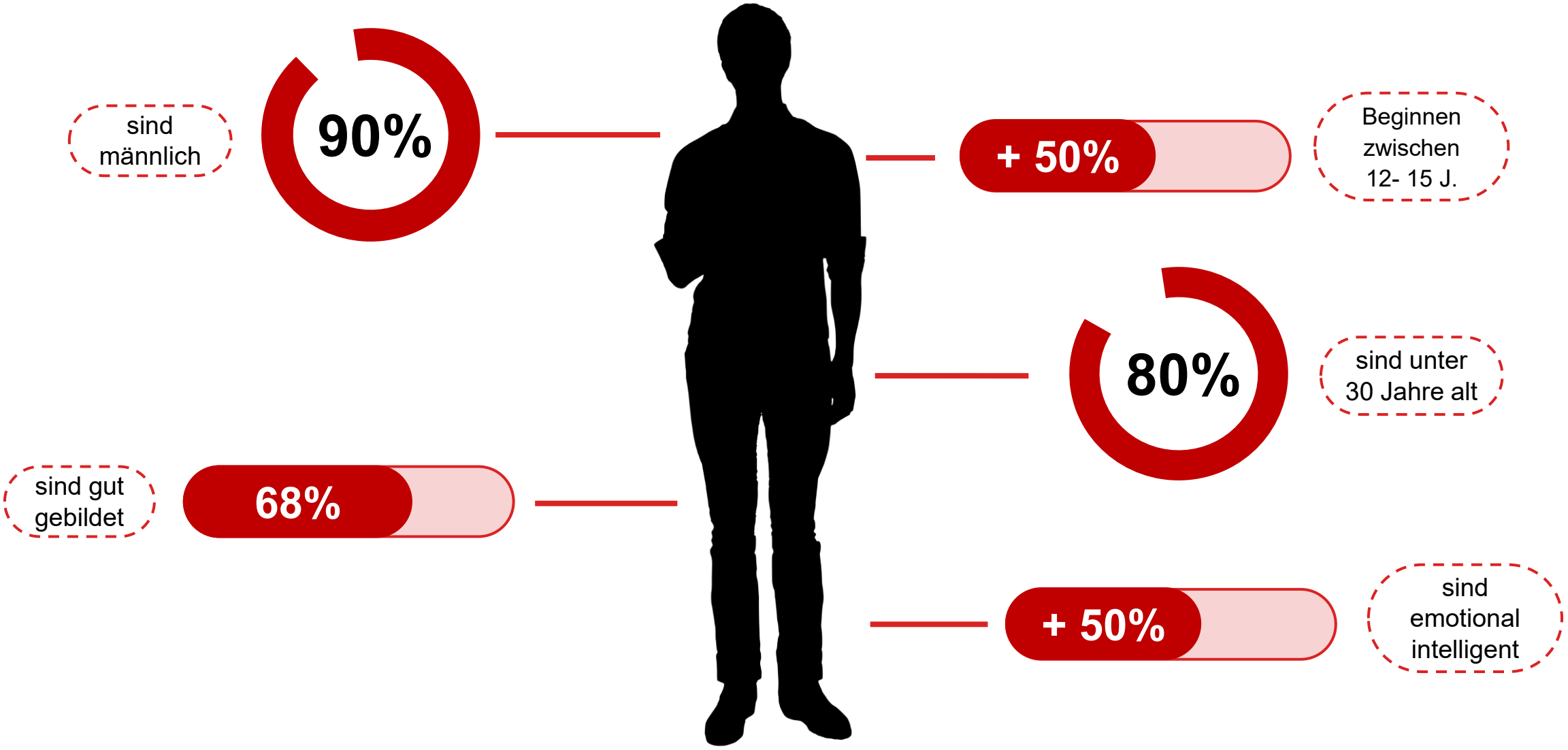
Wie man sich Hacker vorstellt




Wana Decrypt0r 2.0
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/15/2017 16:32:52
Time Left
02:23:59:49
Your files will be lost on
5/19/2017 16:32:52
Time Left
06:23:59:49
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

Wer Hacker in Wirklichkeit sind

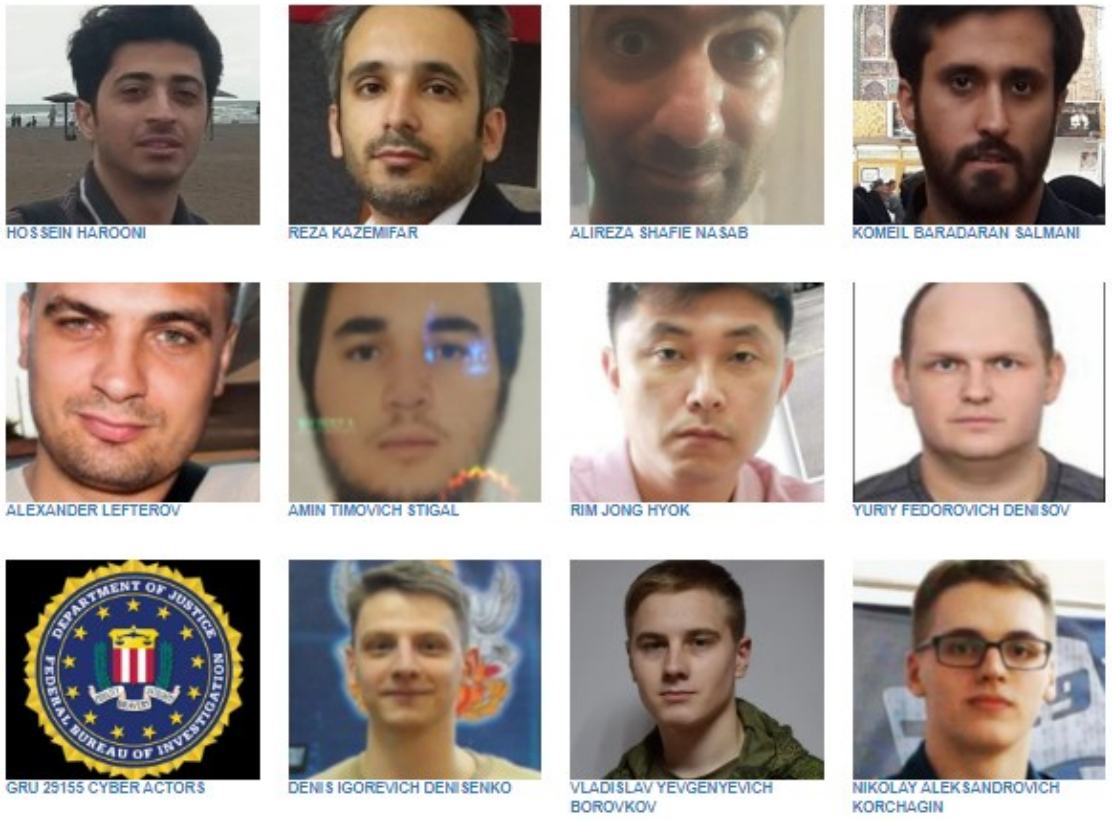
Anatomie eines Hackers



Digitale Technologie: Chancen und Gefahren

Chancen: digitale Vernetzung Industrie 4.0

Gefahr: Cyber-Kriminalität



Quelle: https://www.fbi.gov/investigate/cyber/most-wanted 2024

Wer steht im Visier der Cyberkriminellen?

Wir alle stehen im Visier der Hacker !

Nutzung von E-Mail und Office-Palette

On-Premise Data Center

Steuerungssysteme wie Boardcomputer etc.

Nutzung von WLAN und Telefonie / Voice over IP

Cloud-Dienste

Datenverlust

Identitätsdiebstahl

Datenmissbrauch

Datenklau

Stellen Sie sich die folgenden Fragen?

Risiko-Einschätzung

- Wie gravierend ist der **Ausfall aller internetverbundenen Geräte** (z.B. Computer, Telefonie, Maschinen, Webshop)?
- Wie schlimm ist der **Verlust oder die Unwiederherstellbarkeit sämtlicher** Kunden-, Auftrags-, Lieferanten- und Lohn**daten**?

Cyber-Schadenfall

- Ist Ihr **IT-Dienstleister** bereit, **für eine Pauschale** in der Höhe der Versicherungsprämie (ca. CHF 850) **für sämtliche Kosten** (BU, Neuinstallation der IT-Infrastruktur, etc.) einzustehen?
- Haben Sie einen **Partner** mit Erfahrung einer Bewältigung eines Cyber-Angriffs?

Ausführungen zum aktuellen Markt

Die Gefahr nimmt jede Minute zu!

- **80% der Angriffe** zielen auf den Menschen
- **569 % weltweite Erhöhung der Anzahl von Phishing E-Mails** (2021- 2022)
- **20'872 erkannter Phishing-Webseiten (+108% ggü. Vorjahr)** – Bundesamt für Cybersicherheit 2024
- **Ausgefeilteres und skalierfähiges Social Engineering** – GenKI* als Treiber

**Generative künstliche Intelligenz*

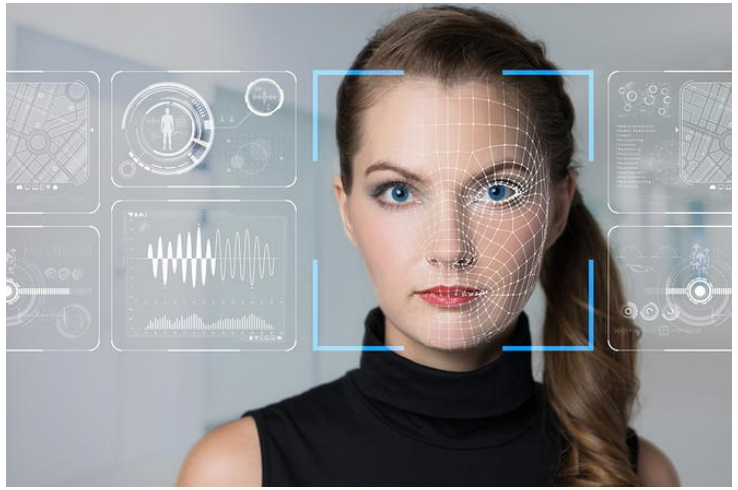
Quellen: Enisa Top Threats 2025, "State of Cybersecurity Trends 2023", PurpleSec Okt 2022, Dark Reading März 2023, Anti-Phishing Bericht 2024 & Cybersecurity Ventures.com

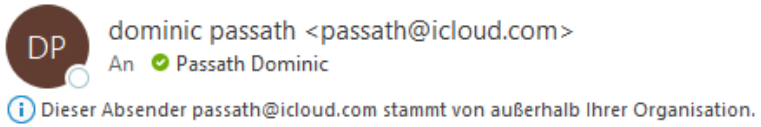
"Amateure hacken Systeme, Profis hacken Menschen"

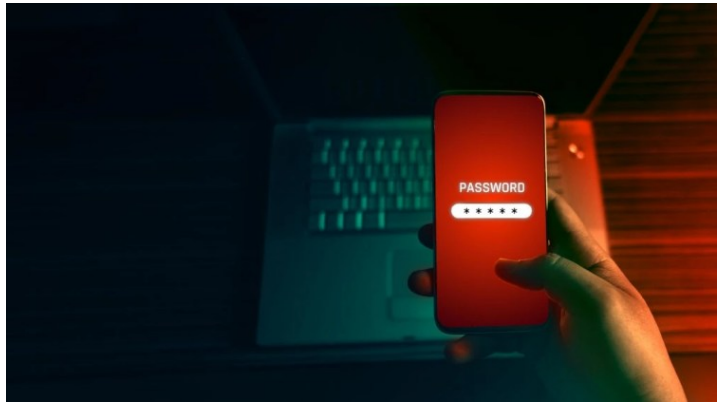
Zitat: Bruce Schneider (US-amerikanischer Experte für Kryptographie & Computersicherheit)

Welche Methoden verwenden Cyberkriminelle, um Menschen zu hacken?

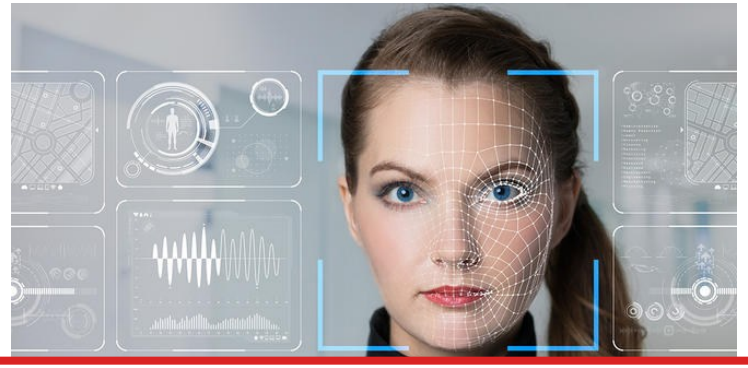
Was für Möglichkeiten haben Hacker und was bedeutet dies für uns?



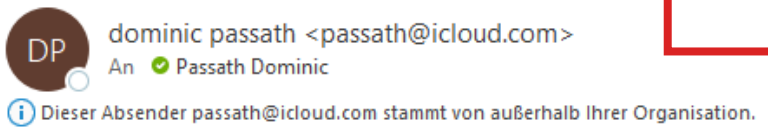


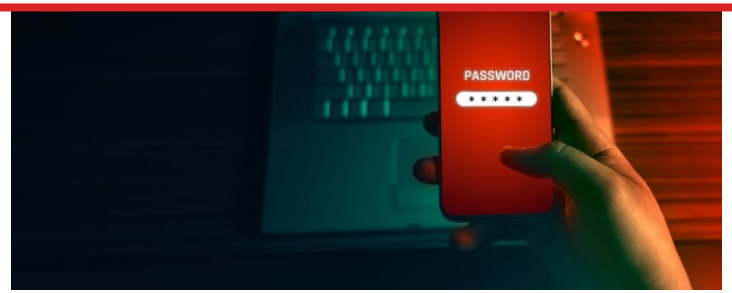


Was für Möglichkeiten haben Hacker und was bedeutet dies für uns?



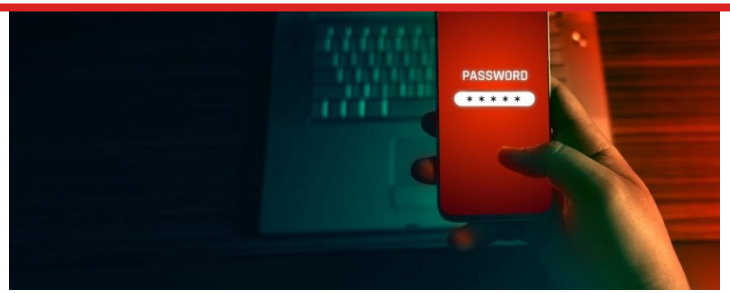
CEO-Fraud



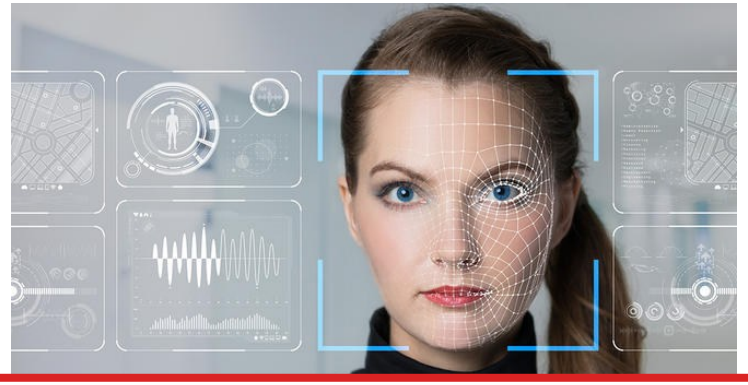


Was für Möglichkeiten haben Hacker und was bedeutet dies für uns?

Betrug

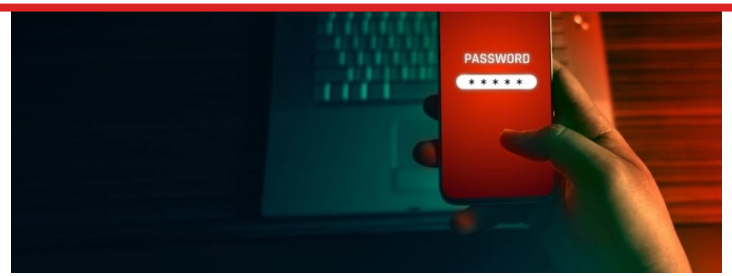


Was für Möglichkeiten haben Hacker und was bedeutet dies für uns?



Phishing – i.d.R. Angriff

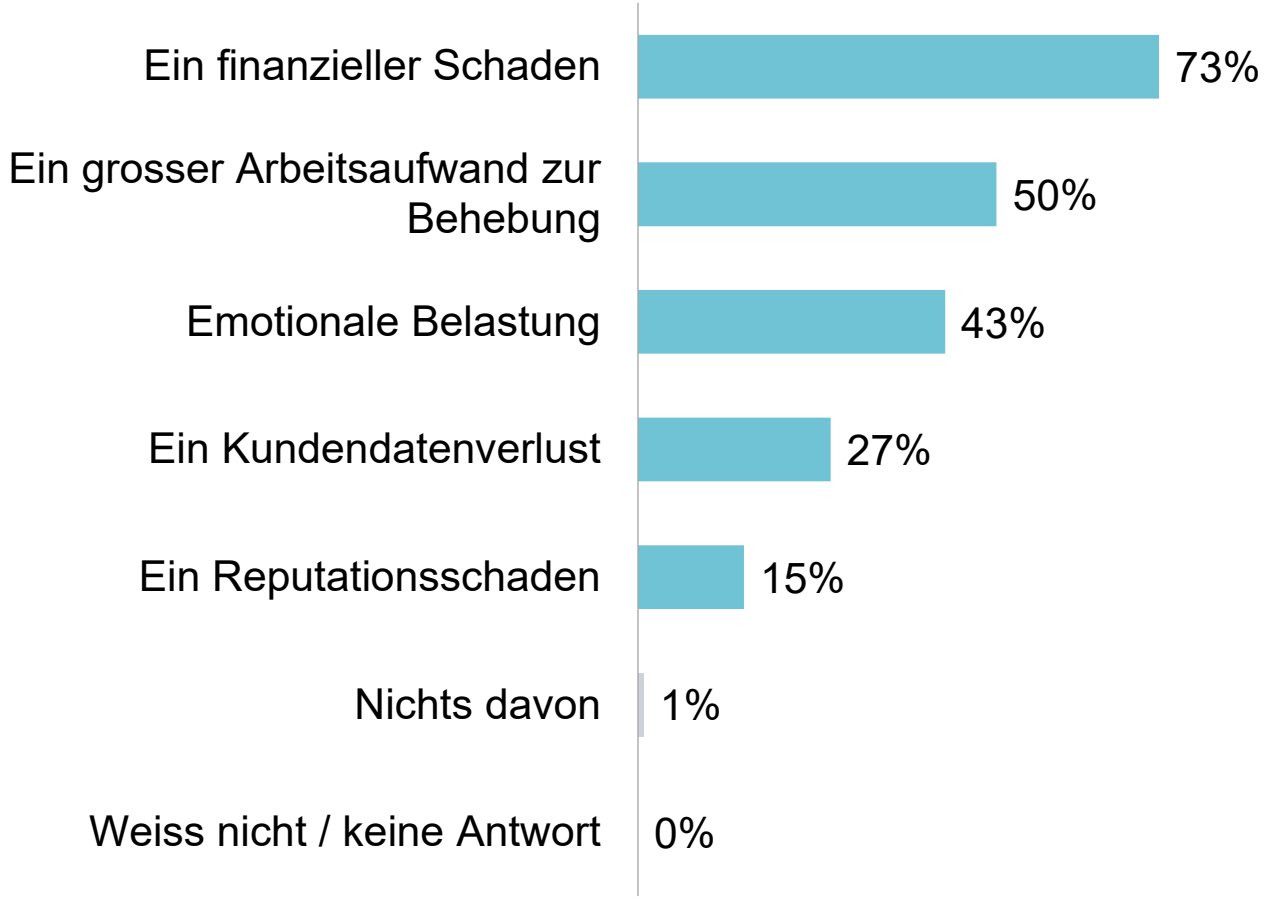
Ransomware



Klassische Cyber-Schadenbilder

Welche zusätzlichen Schäden können entstehen?

Cyber Risk ist **vielschichtig, betrieblich und eigenverantwortlich**!



Quelle: https://www.mobiliar.ch/studie/cybersicherheit-schweiz

Der Schadenfall aus der Optik des Kunden bzw. der Kundin

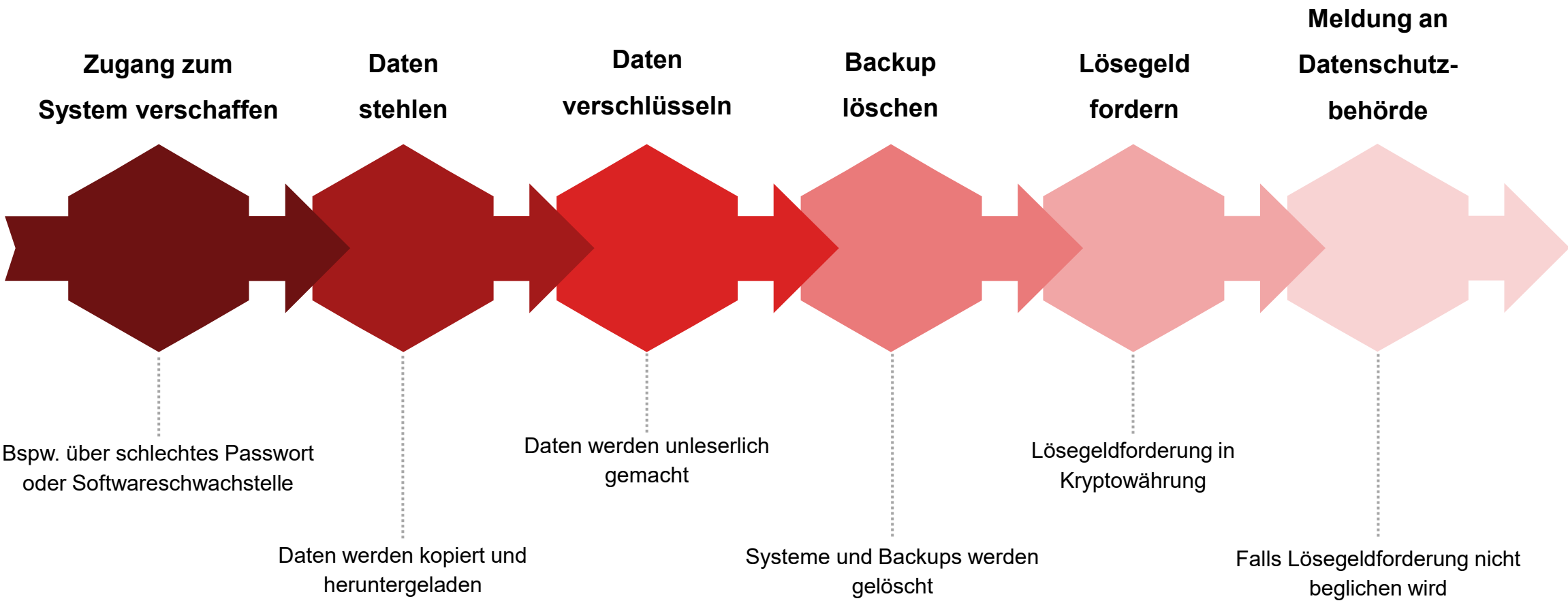
Was beobachten wir bei unseren Kunden?

2 Schadenbilder

Erpressung

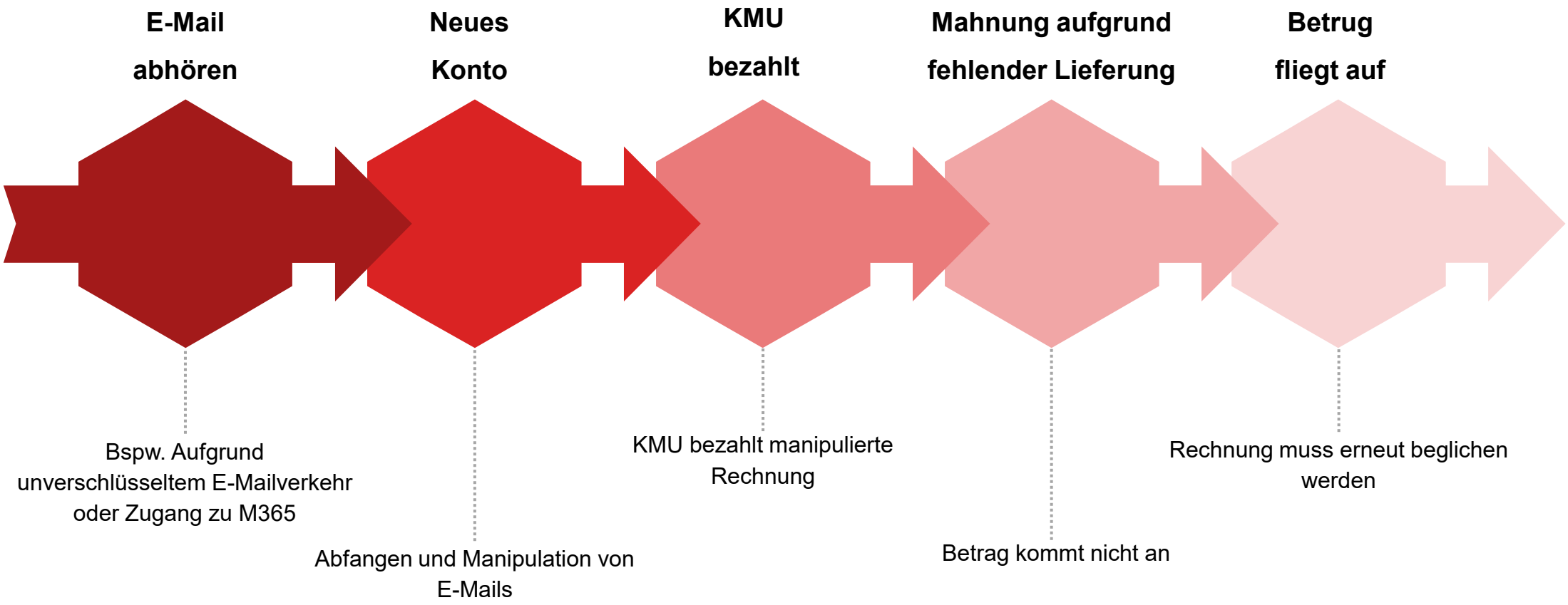
Betrug

Typische Cyber-Schadenbilder – wie gehen **Erpresser** vor?



Die Lösegeldforderung steht i.d.R. im Verhältnis zum Umsatz

Typische Cyber-Schadenbilder – wie gehen **Betrüger** vor?



Der Umfang des Betrugs hängt von diversen Faktoren ab (z.B. der Höhe der wiederkehrenden Rechnungen)

Angriff auf eine Landtechnik-Werkstatt

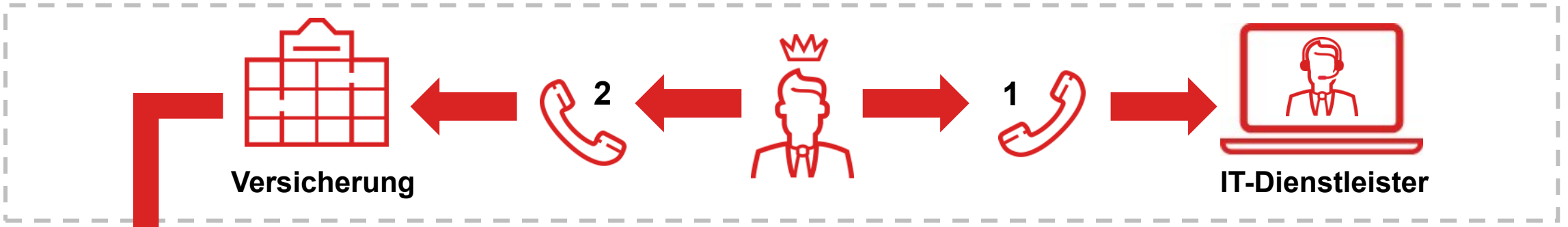
Ausgangslage: Eine kleine Landtechnik-Werkstatt betreibt ein digitales System zur Verwaltung von Kundendaten, Reparaturaufträgen und Ersatzteilen. Cyberkriminelle dringen in das Netzwerk ein, stehlen sensible Informationen, verschlüsseln alle betrieblichen Dateien und löschen die vorhandenen Backups. Anschliessend stellen sie eine Lösegeldforderung in Form von Kryptowährung, um die Daten wiederherzustellen und die Entschlüsselung zu ermöglichen. Sollte die Lösegeldforderung nicht beglichen werden, so werden alle sensiblen Kundendaten im Darkweb veröffentlicht.

Entstandener Schaden:

- Ertragsausfall infolge eines Stillstands im Betrieb (kein Umsatz für mehrere Tage)
- Kosten für externe IT-Fachleute, die den Angriff analysieren und versuchen, die Systeme wiederherzustellen
- Kosten für Forensiker und Experten für Lösegeldverhandlungen
- Kosten für PR-Massnahmen, um das Vertrauen der Kunden und Geschäftspartner trotz des Vorfalls aufrechtzuerhalten

Der Schadenfall aus der Optik des Versicherers

Nach dem Schadenereignis



Cyber Schaden-Inspektor:Innen

Partner Netzwerk

Analyse Sachverhalt, Sofortmassnahmen, Incident Response & Forensik
(ergänzend zu IT-Dienstleister des VN)

Krisenmgmt & Kommunikation

Datenrettung

Partnernetz Anwälte (Datenschutz)

Das Angebot der Versicherer im Schadenfall

Partnernetzwerk:

- Datenrettung
- Wiederherstellung
- Abwehr von Angriffen
- Krisenbewältigung
- Kommunikation
- …

Landtechnik-Werkstatt

- Datenrettung ✓
- Kosten für Analyse ✓
- IT-Dienstleister ✓
- Eigenleistungen ✓

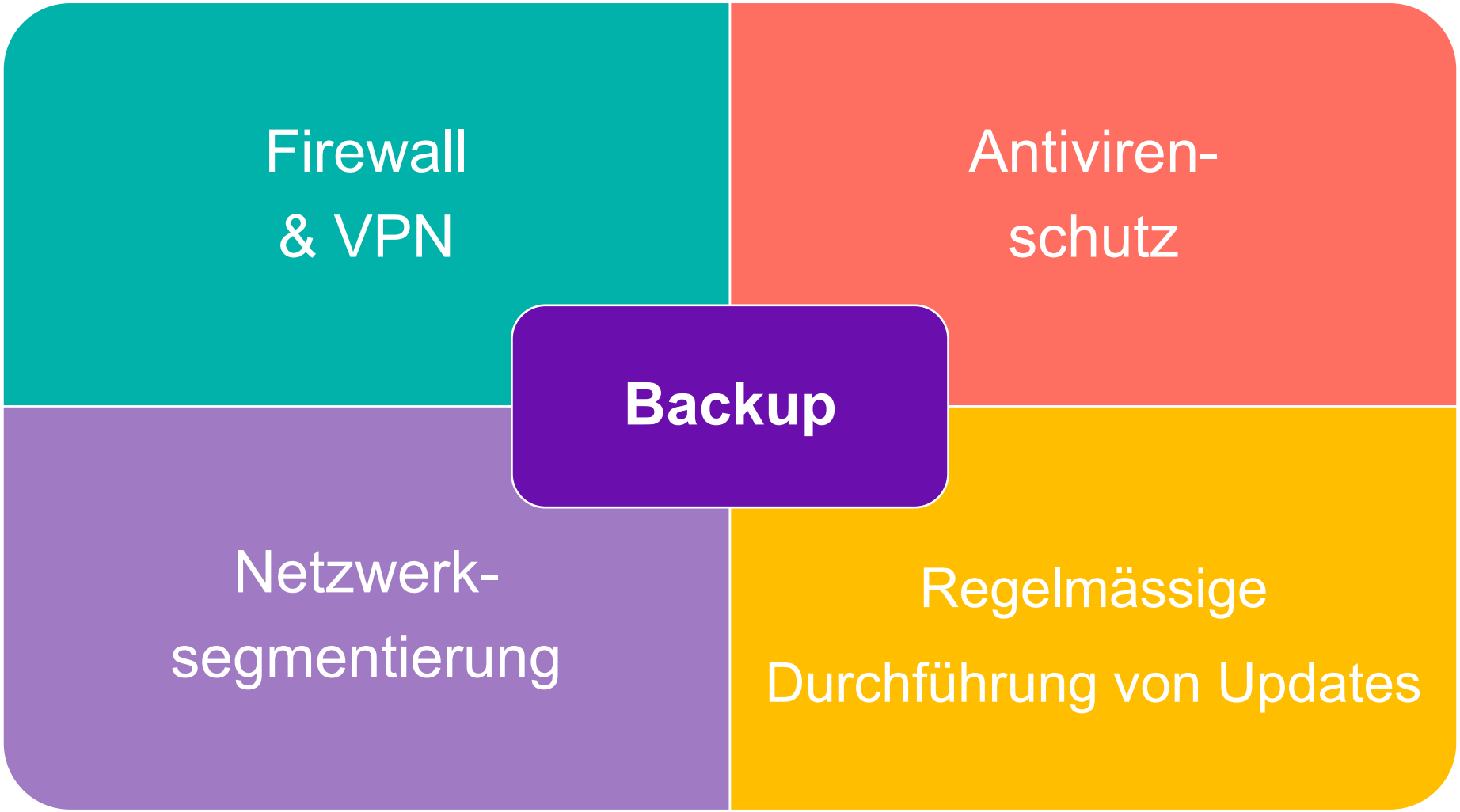
Kostenübernahme:

- Daten - Wiederherstellung
- Wiederherstellung Systeme
- Ertragsausfall
- Krisen, PR-Management
- Internet – Betrug
- Haftpflichtansprüche

Präventionsmassnahmen

Technologische Massnahmen

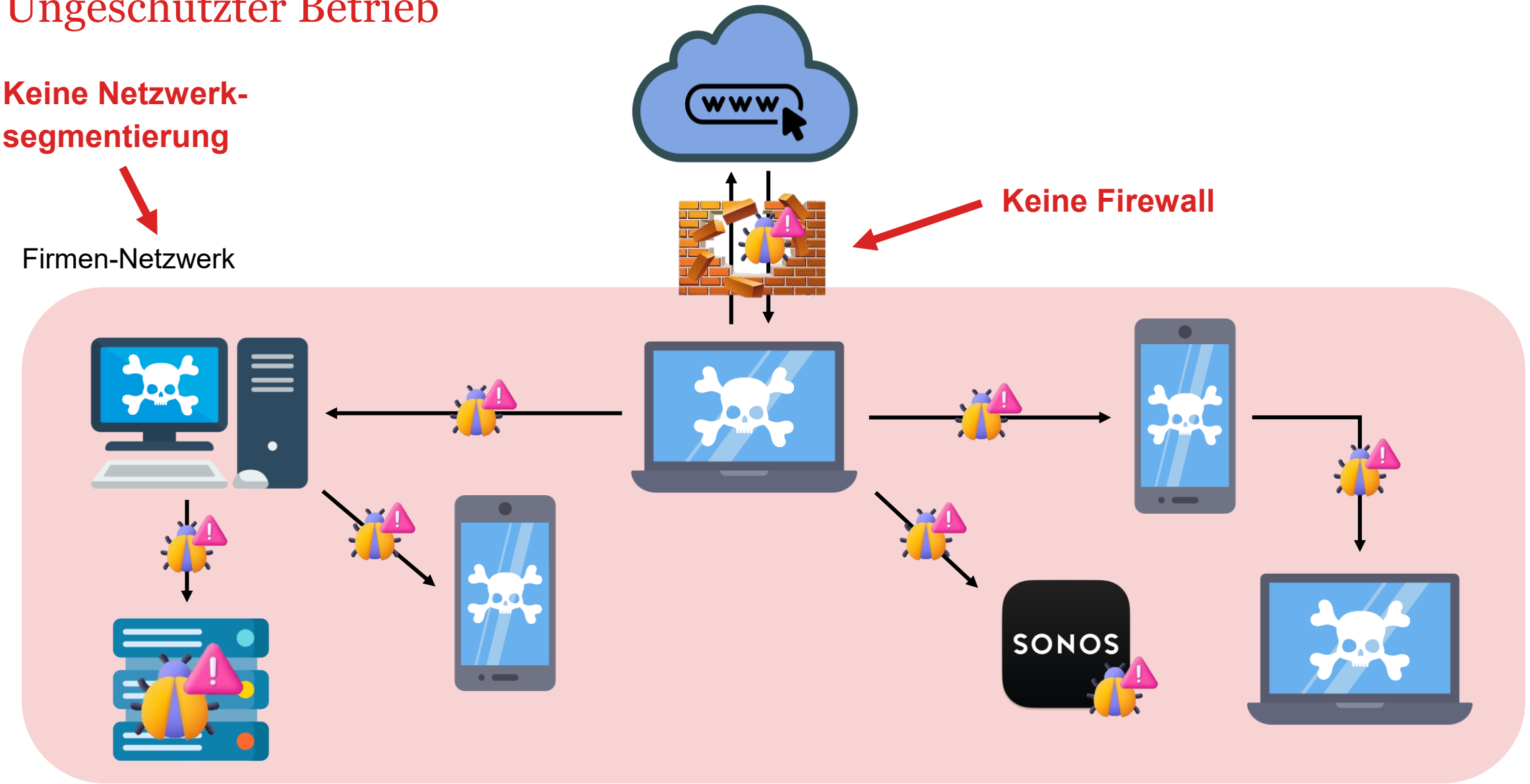
Überblick über die wichtigsten technologischen Massnahmen



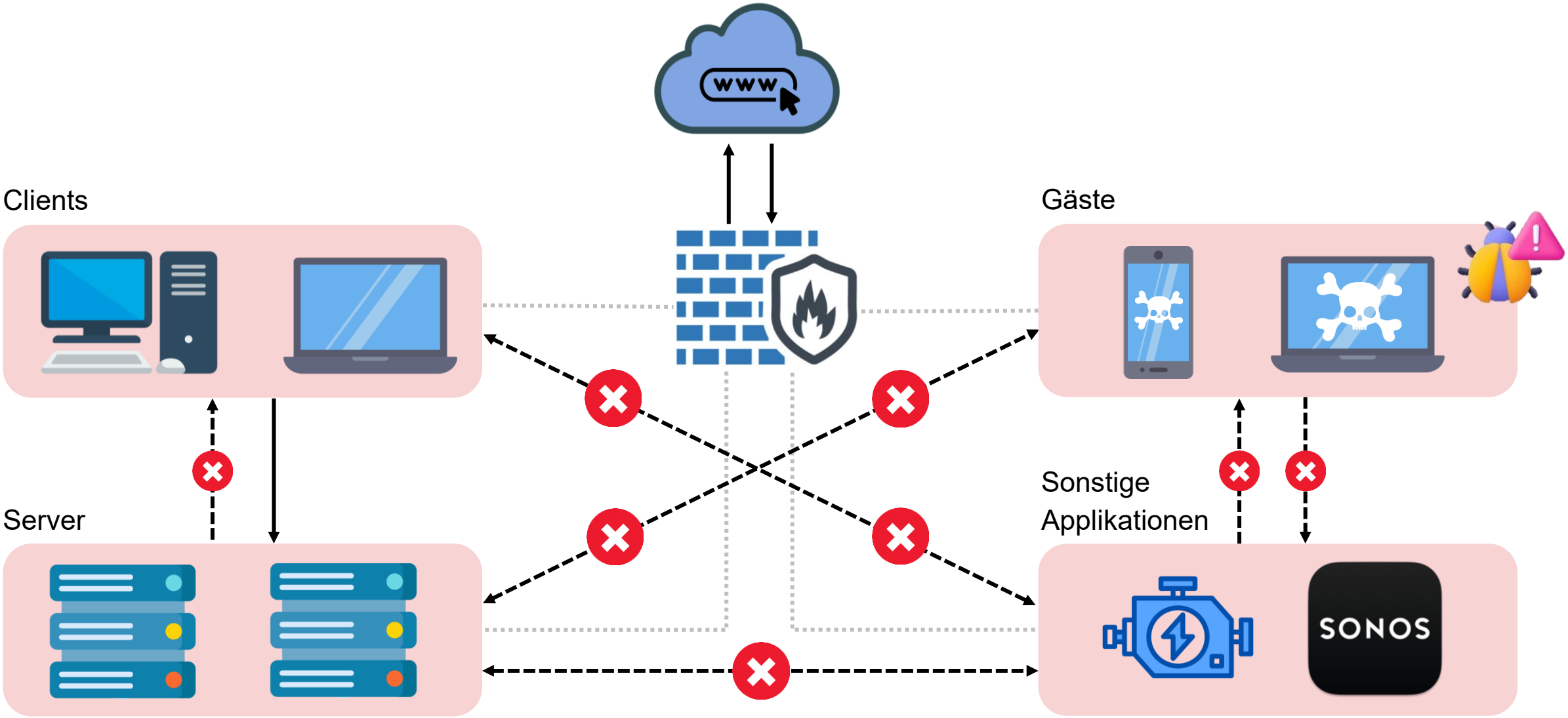
Ungeschützter Betrieb

Keine Netzwerk-segmentierung

Firmen-Netzwerk



Netzwerksegmentierung & Firewall

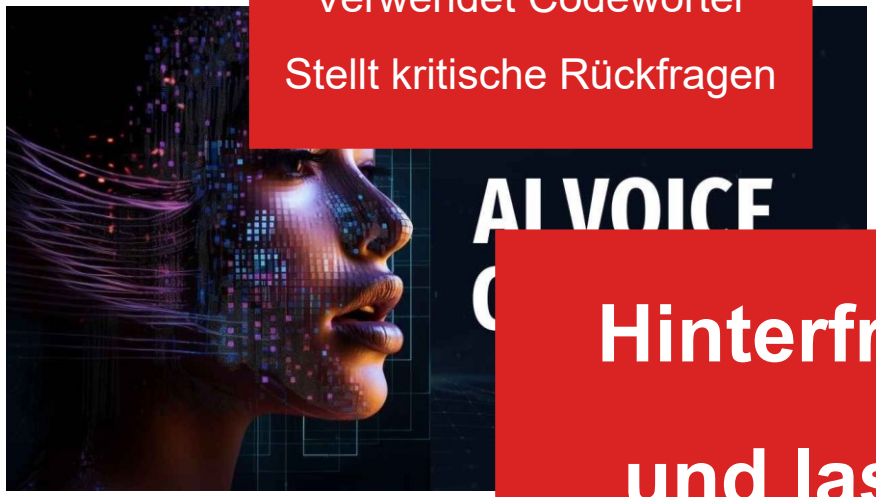


Menschliche Massnahmen

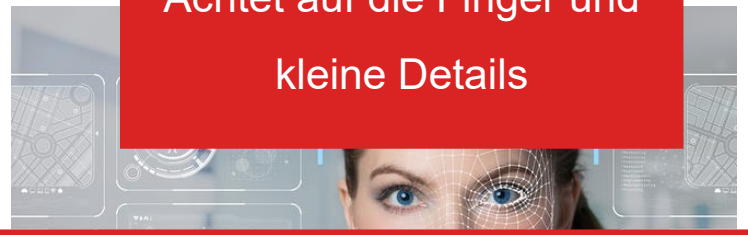
Überblick über die wichtigsten menschlichen Massnahmen

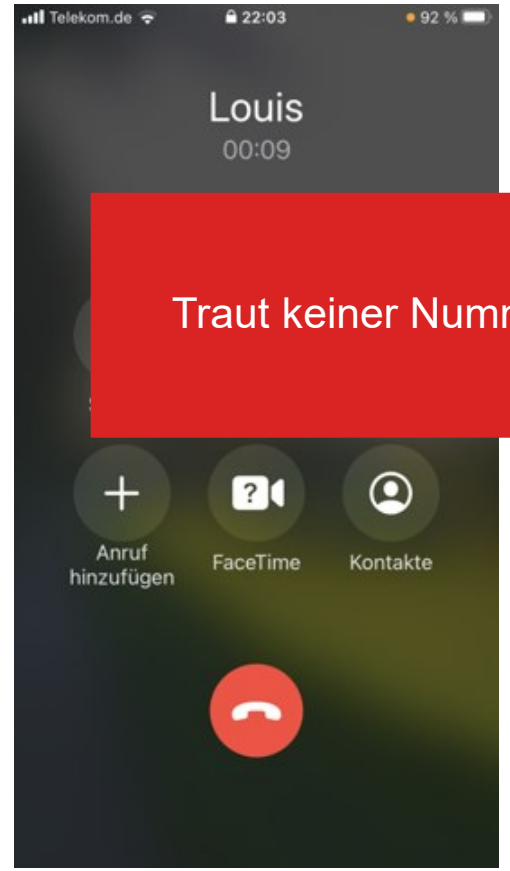
Verwendet Codewörter

Stellt kritische Rückfragen



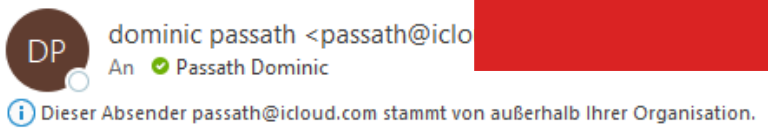
Achtet auf die Finger und kleine Details



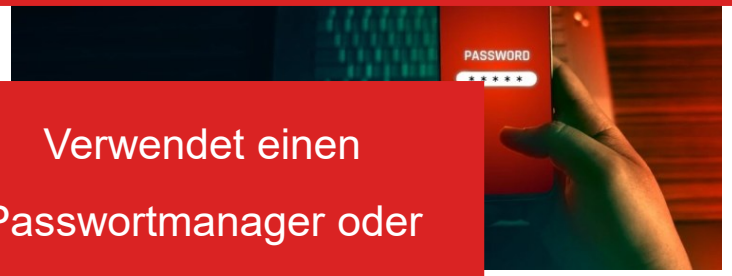


Traut keiner Nummer

Hinterfragt den Sachverhalt und lasst euch nicht unter Druck setzten



Achtet auf den Absender



Verwendet einen Passwortmanager oder lange Passwörter

Vielen Dank für eure Aufmerksamkeit

Anhang

Überblick über die wichtigsten menschlichen Massnahmen

Passwortsicherheit

Komplexe Passwörter oder Passwortmanager und MFA verwenden.

Schulung & Sensibilisierung

Cyber-Sensibilisierungstraining durchführen, um sich mit den aktuellen Bedrohungen und Schutz-massnahmen vertraut zu machen.

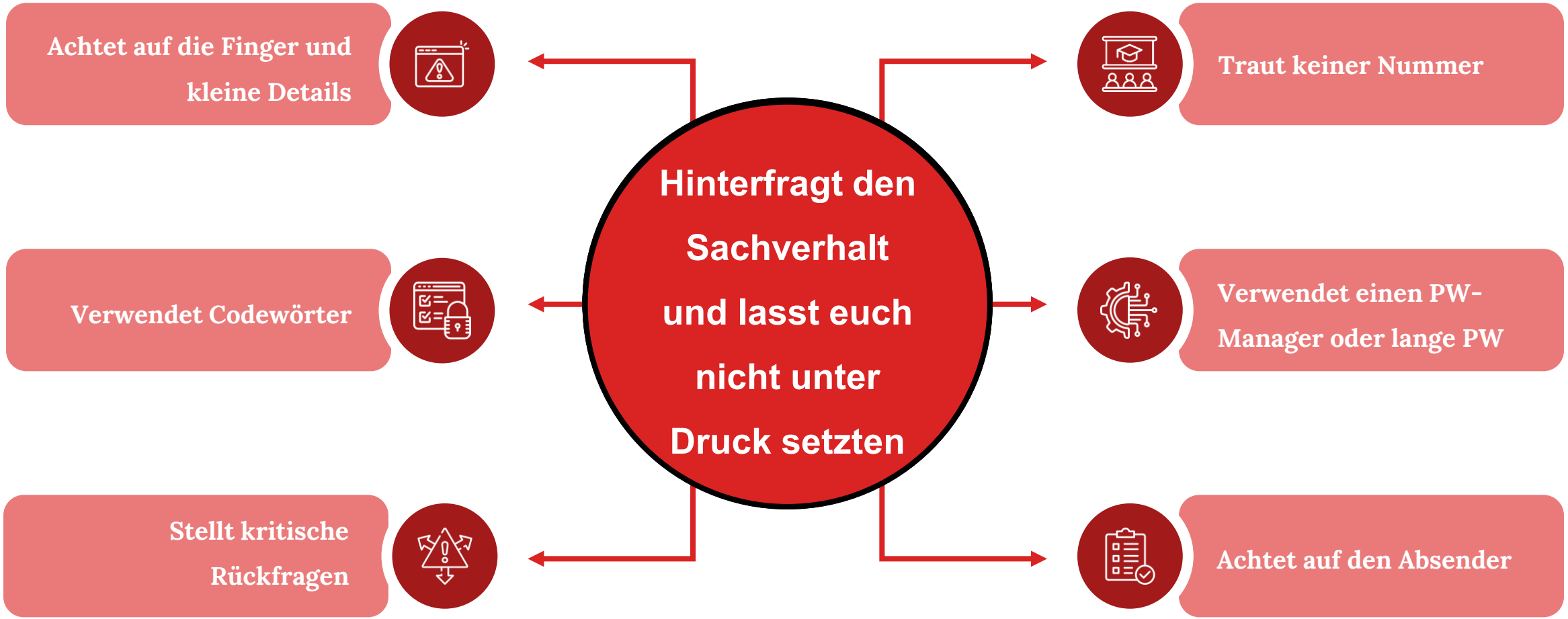
Datensparsamkeit

Vorsicht beim Teilen von Informationen.

Online-Privatsphäre

Überprüfen Sie die Privatsphäre-Einstellungen in sozialen Netzwerken.

Weitere Tipps



Wie erstellt man ein sicheres Passwort?

Entwurf

Ich arbeite seit 15 Jahren bei der AM Suisse.

las15JbdAS

I,as15J,bdA,S,

Netflix

ix.I,as15J,bdA,S,.Ne

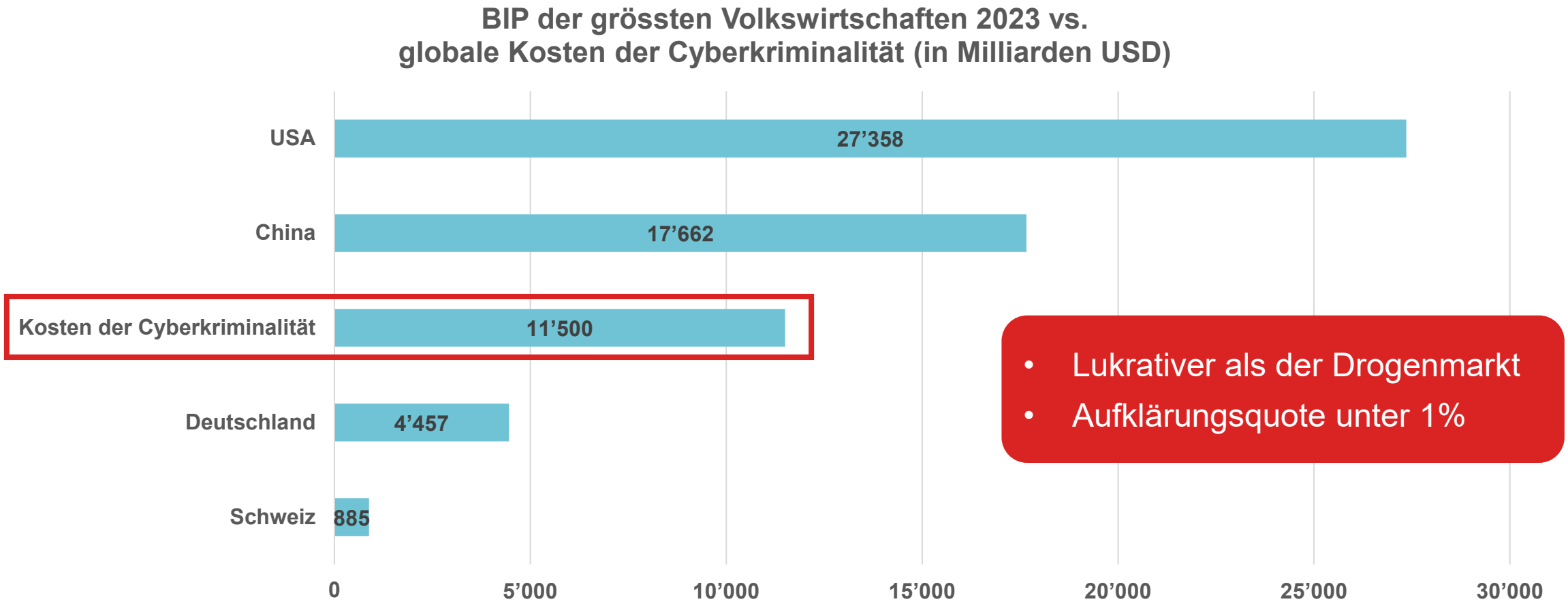
10 Min. 10 Zeichen

A1& Verschiedene Zeichen

Aa Gross- & Kleinschreibung

 Eselsbrücke

"Cybercrime" als eigene Volkswirtschaft?!



Quelle: Statista 2024 und WEF Annual Meeting 2024

Bedrohungslage von Morgen – eine Prognose

Nutzer

resp. unsere KundInnen => weitere Exponierung

- **Zunehmende digitale Vernetzung:** Nutzung von Cloud und mit dem Internet vernetzten Geräte (IoT)
- Weitere **Fragmentierung der Wertschöpfungskette**

Cyber-Kriminelle

- **Ausnutzung von Schwachstellen**
  - Schnittstellen in der Lieferkette
  - Schlecht geschützte, immer verfügbare Produktionsanlagen (evtl. mit IoT)
- **Nutzung der Technologie GenKI**
  - Ausgefeilteres Social Engineering
  - Automatisierung und Skalierung machen Cyber-Angriffe zum Massenphänomen (Crime-as-a-Service)
- **Verwundbarere Cyber-Angriffe mit Datendiebstahl**
  - Zunahme von Ransomware-Attacken (Lösegelderpressungen): Meldepflichten oder ein geübter "Notfall- inkl. Kommunikationsplan" rücken in den Vordergrund
  - Zunahme von Haftpflichtfälle, da Risiko der Veröffentlichung von Kunden-, Mitarbeiter-, Lieferanten-daten steigt: Cyber-Versicherung mit Partnernetzwerk wird wichtiger

Abkürzungen:
IoT = Internet of Things
GenKI = generative Künstliche Intelligenz;

Was sind die Auswirkungen auf das Tagesgeschäft (wird dies gedeckt)?

- Teils Konventionalstrafen
- Betriebsunterbruch
- Verlorene Daten, welche aufgearbeitet werden müssen
- Stress und emotionale Belastung