WEIHRICH
INFORMATIK

die Mobiliar

Stärkung der Cyber Widerstandsfähigkeit

Thomas Weihrich, Weihrich Informatik GmbH

Christoph Clavadetscher, Mobiliar Kompetenzzentrum Cyber Risk

23. Oktober 2025 in Kreuzlingen

Vorstellung der Referenten

Thomas Weihrich
Inhaber und Geschäftsführer, Weihrich Informatik

Christoph Clavadetscher
Cyber Risk Experte, die Mobiliar

Wahrscheinlichkeit eines Gebäude- vs. Cyber-Schadens

Alle ***48 Minuten***

brennt es.

Alle ***8,5 Minuten***

ereignet sich ein Cybervorfall.

Quelle: Beratungsstelle für Brandverhütung BFB, 2024

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

Cyber-Attacke, was nun?

Was kostet mich dieser Vorfall?

Wer ist meine "Cyber Feuerwehr"?

Wie informiere ich meine Kunden und Geschäftspartner?

Wie funktioniert mein Notbetrieb?

Eigenverantwortung

Was ist mein Plan im Umgang mit Medien?

Muss ich die Behörden informieren?

Was sage ich meinen Mitarbeitenden?

Wie kann ich mein Tages-geschäft weiterführen?

Oops – was ist auf dem Backup und funktioniert das Einspielen?

Aktuelle Lage – bei einer Cyber-Attacke haben Viele ein Problem

watson 8°

Schweiz International Wirtschaft Sport Leben Spass Digital Wissen Blogs Quiz Videos

DIGITAL-NEWS

Schweizer Firmen fallen bei Cybersicherheit zurück – 80 Prozent ungenügend geschützt

Die Verteidungsfähigkeit von Schweizer Firmen gegen Cyberangriffe ist laut dem Technologie-Unternehmen Cisco schlechter geworden. Rund 80 Prozent sind nicht ausreichend gegen Cyberangriffe geschützt.

6

07.05.2025, 18:30 07.05.2025, 18:30

Zu diesem Schluss kommt der am Mittwoch veröffentlichte Cybersecurity Readiness Index 2025 von Cisco.

Quelle: Watson, 07.05.2025

Agenda

1. Wie sieht die **aktuelle Cyber-Bedrohungslage** aus?

2. Was ist ein **typisches Cyber-Schadenbild** und dessen **Auswirkungen**?

3. **Wie** steht es um **Ihr Unternehmen** und wie können **Sie sich schützen**?

4. Was ist die **Rolle des Managed IT-(Security-)Dienstleisters**?

5. Was ist **die Rolle des Versicherers**?

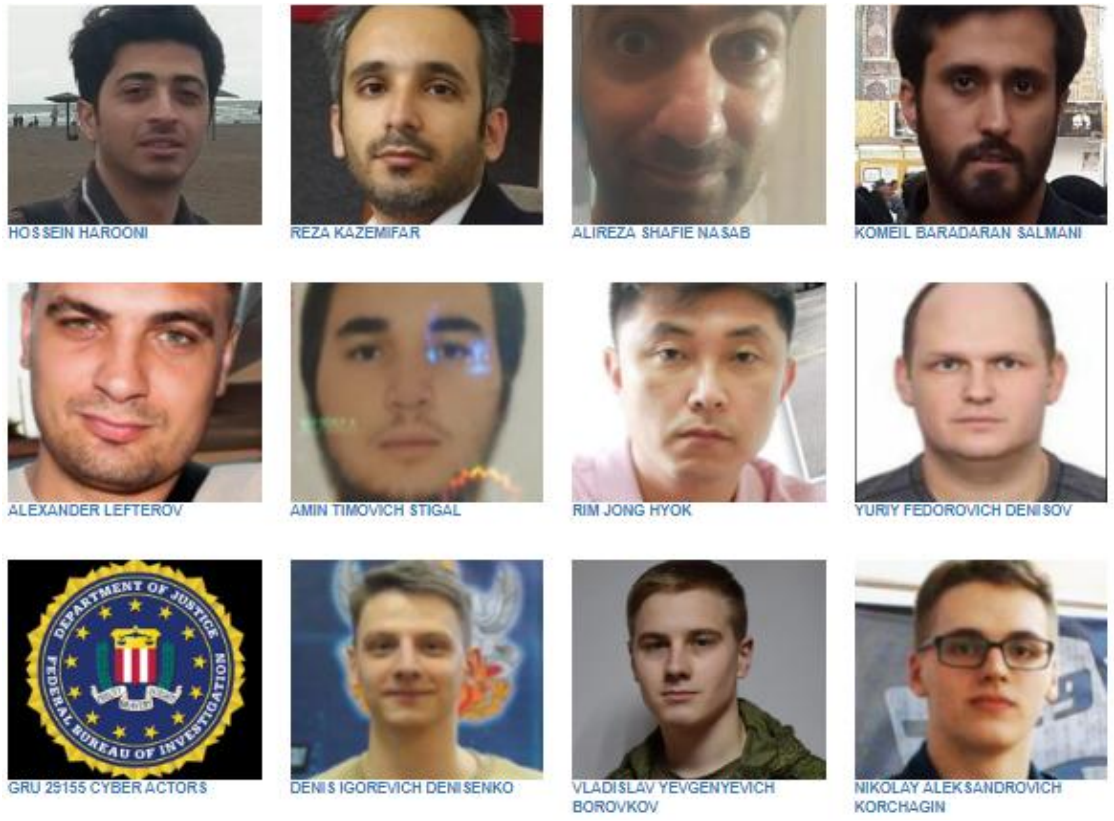
6. **Praktische Tipps** zur Umsetzung

Wie sieht die aktuelle Cyber-Bedrohungslage aus?

Wer die digitalen Technologien nutzt, steht im Risiko

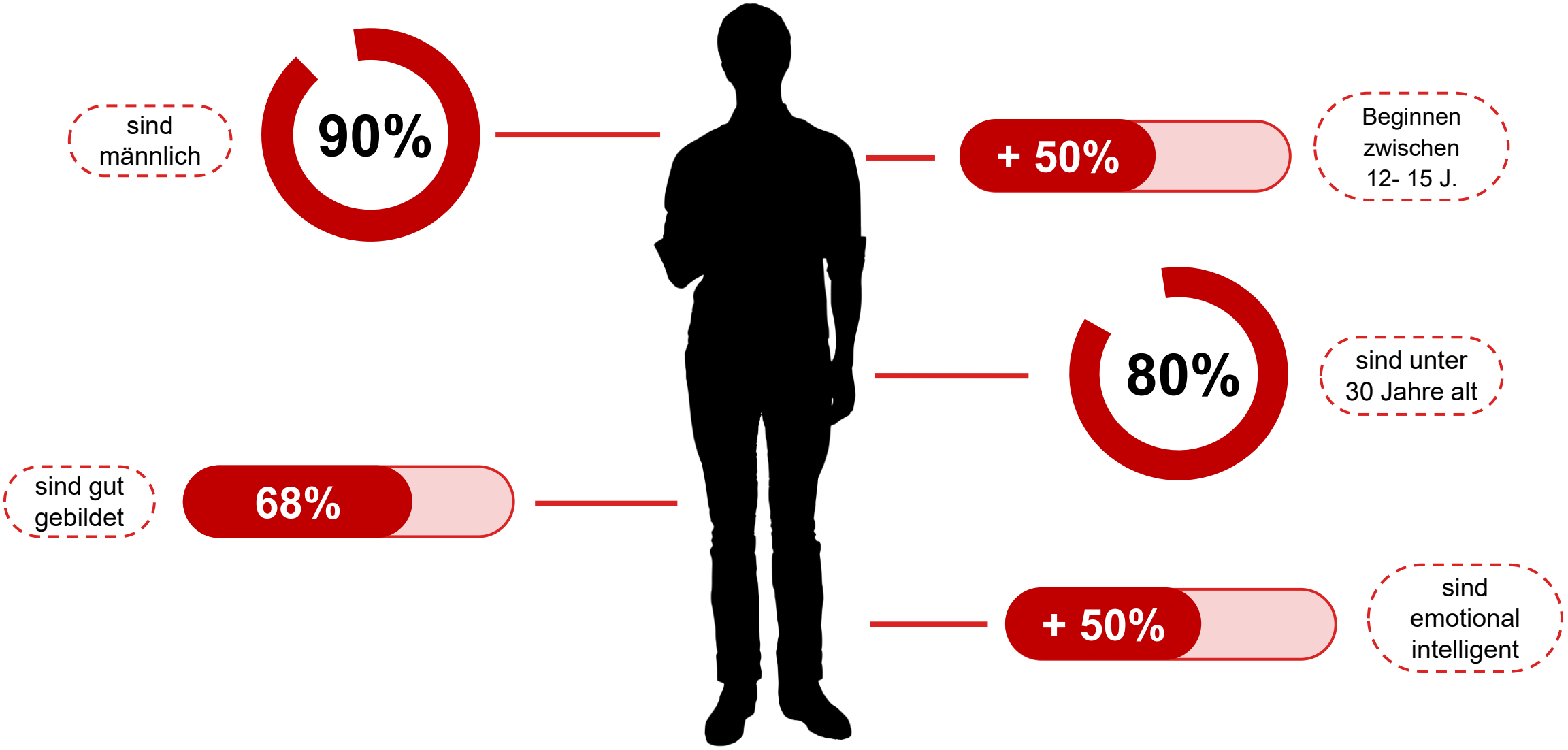
Zunehmende digitale Vernetzung durch Industrie 4.0

Neue Gefahr durch Cyber-Vandalismus, -Aktivismus, -Kriminalität und -Terrorismus



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

Anatomie eines Hackers



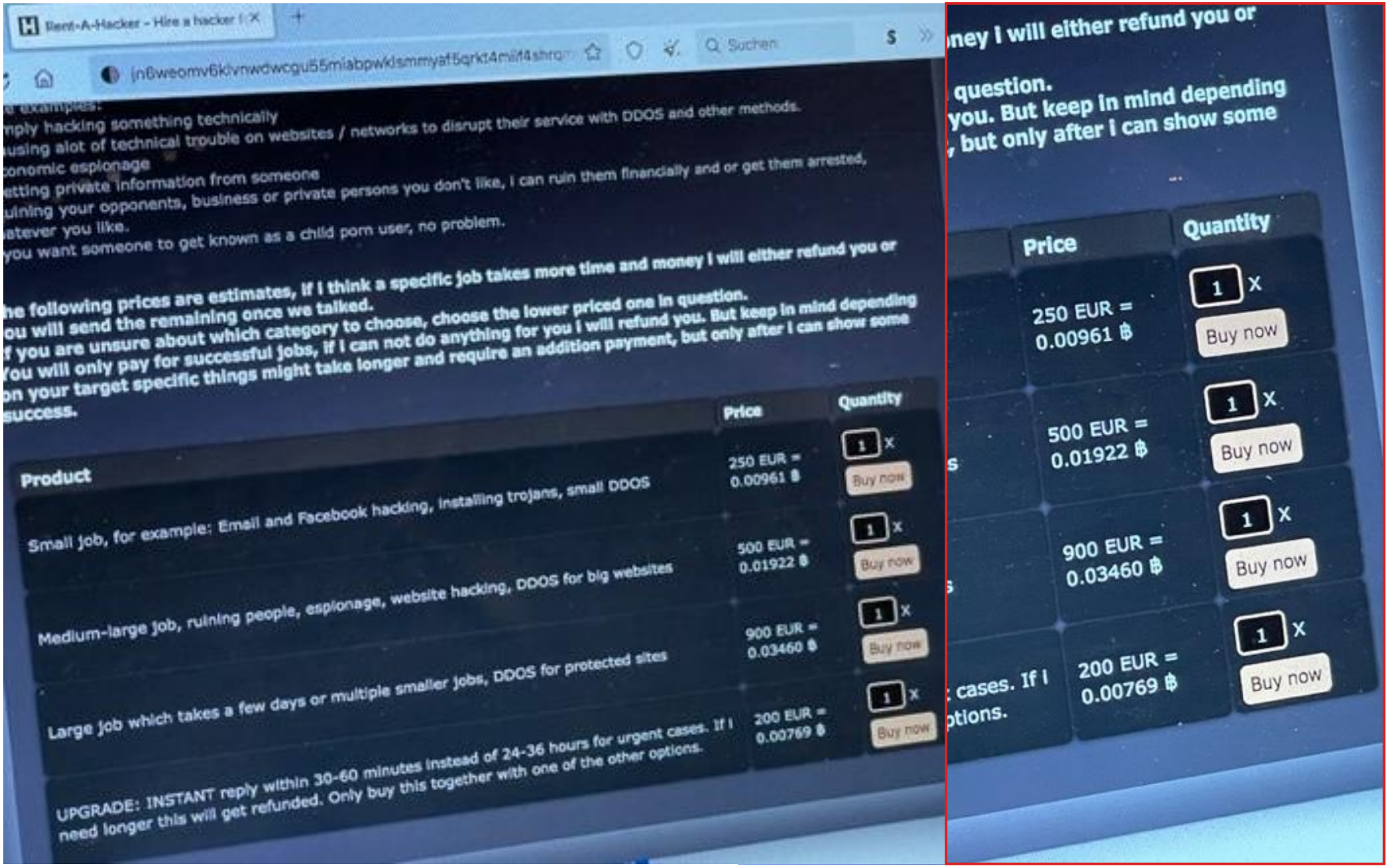
Darknet – Cyberkriminalität ist ein neues Geschäftsfeld

CYBERCRIME PRICE LIST

ATTACK TOOLS	MALWARE	$200	REMOTE ACCESS TROJAN
		$50	PASSWORD STEALER
	RANSOMWARE	200	SOPHISTICATED LICENSE FOR WIDESPREAD ATTACKS
		$50	UNSOPHISTICATED LICENSE FOR TARGETED ATTACKS
		$1	PC MALWARE INSTALLATION
		$400	1 MILLION MALICIOUS SPAM
	SOFTWARE	$100	REMOTE DESKTOP CONTROL TOOL
		$700	DISTRIBUTED DENIAL OF SERVICE ATTACK SOFTWARE
	PAYMENT & LOG-IN INFO	$5	CREDIT/DEBIT CARD FOR ONLINE USE
		$10	CREDIT/DEBIT CARD INFO THAT CAN BE CLONED ON PLASTIC
		$5	BANK ACCOUNT LOG-IN (USERNAME AND PASSWORD)
		$25	BANK ACCOUNT LOG-IN WITH ACCESS TO EMAIL, SECURITY ANSWERS, ETC.
		$1	EXISTING PAYPAL ACCOUNT
DATA	PERSONAL INFORMATION	$3	SOCIAL SECURITY AND DATE OF BIRTH VERIFICATION
		$150	CREDIT REPORT 750+ CREDIT SCORE
	DATABASE RECORDS	$25	1 MILLION COMPROMISED EMAIL/PASSWORDS
SERVICES	HACKING	$100	EMAIL ACCOUNT
		$100	SOCIAL MEDIA ACCOUNT
		$300	CMS WEBSITE (WORDPRESS, ETC.)
	USER OBFUSCATION	$150	BULLETPROOF HOSTING IN A LAX JURISDICTION (CHINA, EASTERN EUROPE, ETC.)
		$20	VIRTUAL PRIVATE NETWORK (VPN)
	MALWARE	$1	PC MALWARE INSTALLATION
		$25	MALICIOUS FILE ENCRYPTION
	SPAM	$20	500 SMS (FLOODING)
		$400	500 MALICIOUS EMAIL SPAM
		$20	500 PHONE CALLS (FLOODING)
		$200	1 MILLION EMAIL SPAM (LEGAL)
	FAKE DOCUMENTS	$25	DIGITAL COPY OF FAKE CREDIT/DEBIT CARD
		$25	DIGITAL COPY OF FAKE DRIVER'S LICENSE OR PASSPORT
		$15	DIGITAL COPY OF FAKE UTILITY BILL OR SOCIAL SECURITY CARD

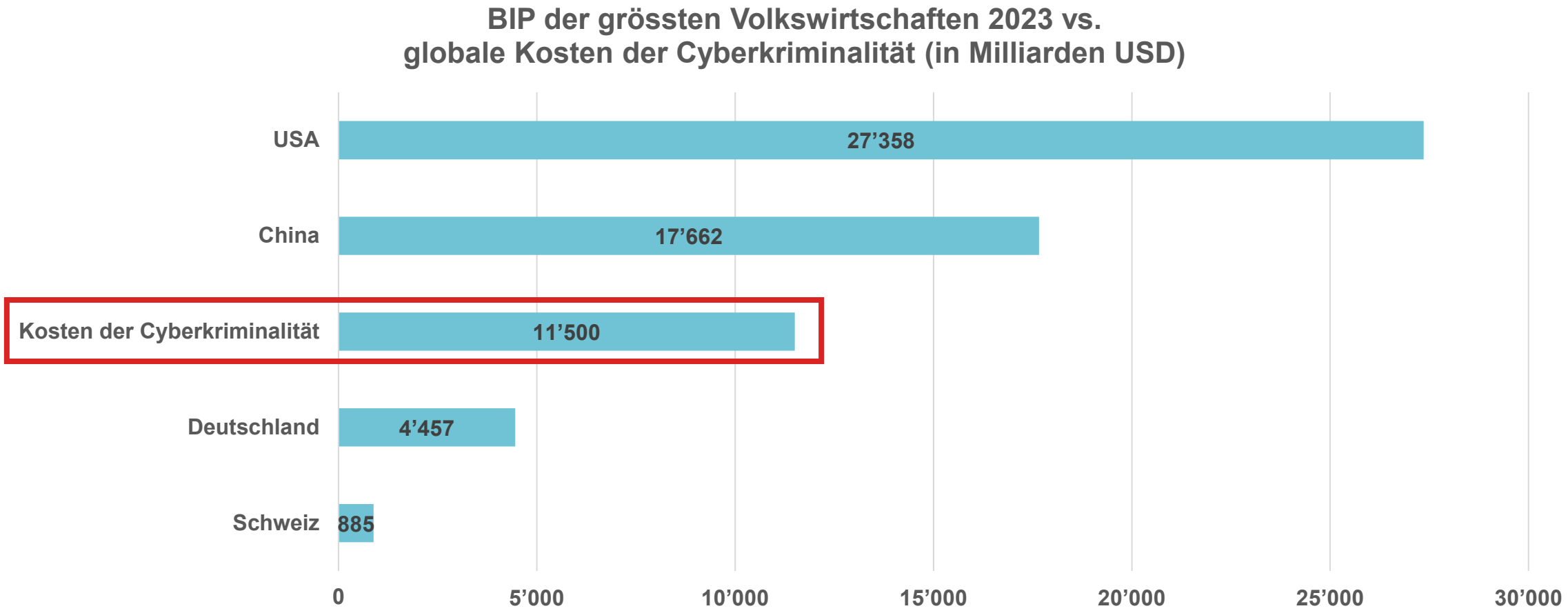
FORTUNE MAGAZINE
SOURCE: RECORDED FUTURE

[5] Quelle: FORTUNE Magazine, A Hacker's Tool Kit, Oktober 2017


Rent-A-Hacker - Hire a hacker
Suchen
mply hacking something technically
using alot of technical trouble on websites / networks to disrupt their service with DDOS and other methods.
conomic espionage
etting private information from someone
uining your opponents, business or private persons you don't like, i can ruin them financially and or get them arrested,
atever you like.
you want someone to get known as a child porn user, no problem.
he following prices are estimates, if i think a specific job takes more time and money i will either refund you or
ou will send the remaining once we talked.
f you are unsure about which category to choose, choose the lower priced one in question.
You will only pay for successful jobs, if i can not do anything for you i will refund you. But keep in mind depending
on your target specific things might take longer and require an addition payment, but only after i can show some
success.
Product
Price
Quantity
Small job, for example: Email and Facebook hacking, installing trojans, small DDOS
250 EUR = 0.00961 ฿
Buy now
Medium-large job, ruining people, espionage, website hacking, DDOS for big websites
500 EUR = 0.01922 ฿
Buy now
Large job which takes a few days or multiple smaller jobs, DDOS for protected sites
900 EUR = 0.03460 ฿
Buy now
UPGRADE: INSTANT reply within 30-60 minutes instead of 24-36 hours for urgent cases. If i need longer this will get refunded. Only buy this together with one of the other options.
200 EUR = 0.00769 ฿
Buy now
ney i will either refund you or
question.
you. But keep in mind depending
, but only after i can show some
Price
Quantity
250 EUR = 0.00961 ฿
Buy now
500 EUR = 0.01922 ฿
Buy now
900 EUR = 0.03460 ฿
Buy now
cases. If i
ptions.
200 EUR = 0.00769 ฿
Buy now

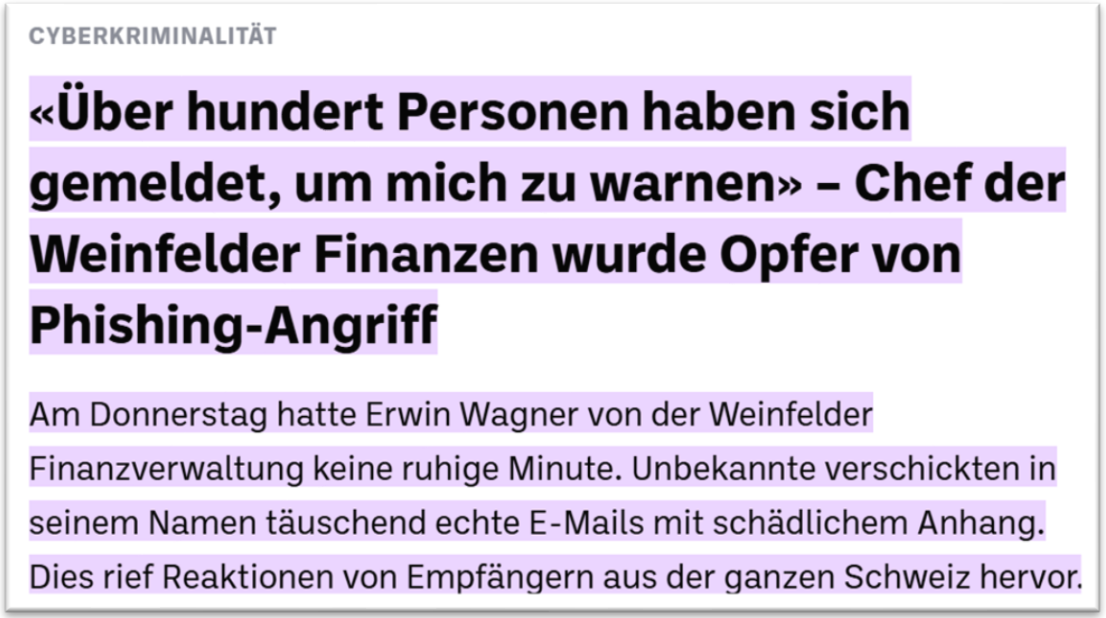

Wana Decrypt0r 2.0
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. 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

"Cybercrime" als eigene Volkswirtschaft?!



Quelle: Statista 2024 und WEF Annual Meeting 2024

Cyber-Angriffe sind in jeder Region angekommen, um zu bleiben…



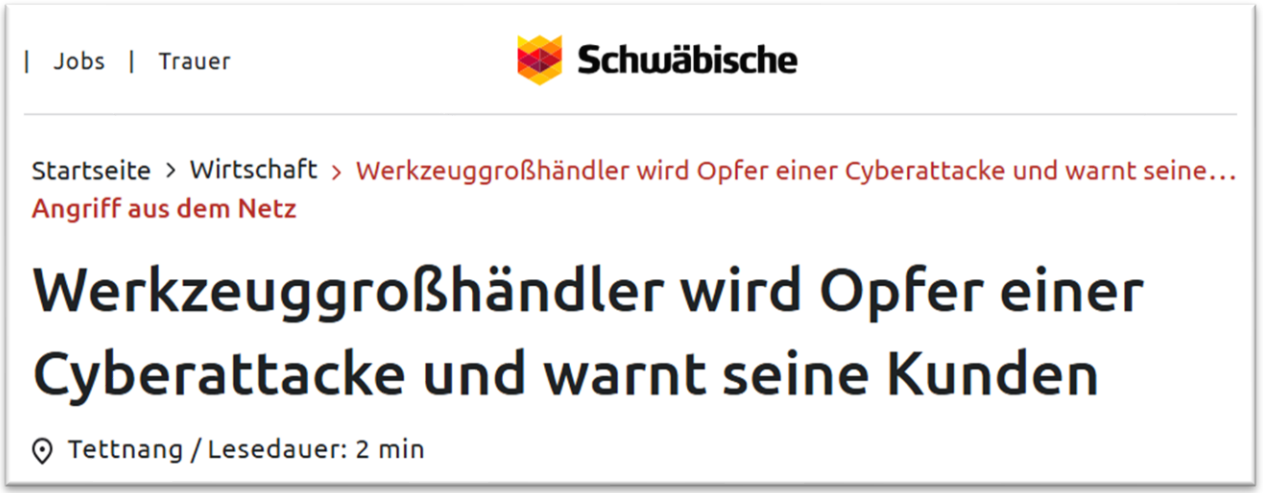
CYBERKRIMINALITÄT

«Über hundert Personen haben sich gemeldet, um mich zu warnen» – Chef der Weinfelder Finanzen wurde Opfer von Phishing-Angriff

Am Donnerstag hatte Erwin Wagner von der Weinfelder Finanzverwaltung keine ruhige Minute. Unbekannte verschickten in seinem Namen täuschend echte E-Mails mit schädlichem Anhang. Dies rief Reaktionen von Empfängern aus der ganzen Schweiz hervor.

Chain-Phishing – Infiltration über MS-Account von Erwin Wagner via gefälschter E-Mail von Thurgau Tourismus

Quelle: Thurgauer Zeitung, 21.03.2025



| Jobs | Trauer Schwäbische

Startseite > Wirtschaft > Werkzeuggroßhändler wird Opfer einer Cyberattacke und warnt seine…
Angriff aus dem Netz

Werkzeuggroßhändler wird Opfer einer Cyberattacke und warnt seine Kunden

Tettnang / Lesedauer: 2 min

Quelle: Schwäbische / Schwäbischer Verlage, 22.04.2025

Klinik-Hack

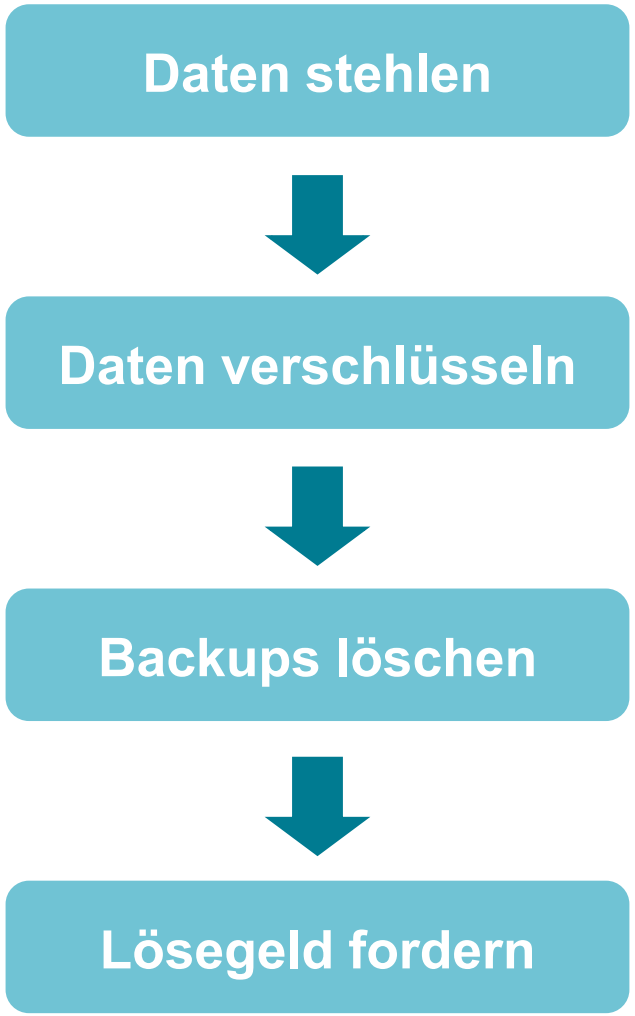
Cyberangriff auf Kliniken am Bodensee: Verdacht der Computersabotage

Die Polizei ermittelt im Zuge des Hackerangriffs auf den Medizin Campus Bodensee aktuell wegen des Verdachts der Computersabotage.

Quelle: Ärzte Zeitung Springer Medizin, 14.01.2022

Was ist ein typisches Cyber-Schadenbild und dessen Auswirkungen?

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



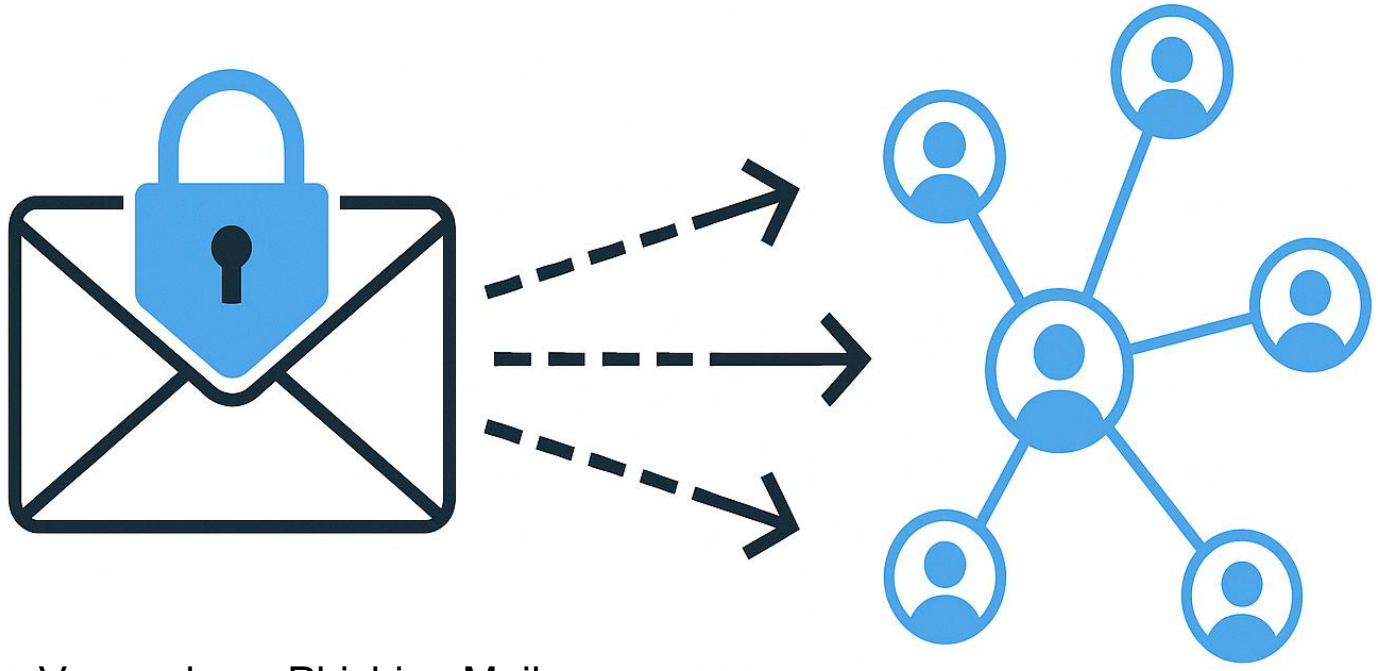
Hacker zerstören Daten von bis zu 200 Coiffeursalons

Ransom-Fall wie er sich oft abspielt:

- **Grosser Kunde – grosse Auswirkung**
- **Kleiner Kunde – kleinere Auswirkung**

Welche Auswirkungen hat eine Cyber-Attacke?

Übernahme von E-Mail Konten
& Verwendung von Adressen



- Versand von Phishing Mails
- Gefährdung Dritter
- Image Schaden gegenüber Kunden und Lieferanten

Welche Auswirkungen hat eine Cyber-Attacke?

Abfluss von Daten

- Private Informationen werden öffentlich
- Geschäftsdaten im Darknet gehandelt
- Informationen Dritter werden öffentlich
- Image Schaden gegenüber Kunden und Lieferanten

Welche Auswirkungen hat eine Cyber-Attacke?

Verschlüsselung von Daten und Systemen

- Datenverlust oder Verfälschung
- Systemausfall
- Ausfall operatives Geschäft
- Folgeschäden

Welche Auswirkungen hat eine Cyber-Attacke?

Betriebsunterbruch und Zeitverlust

Finanzieller Schaden

Arbeitsaufwand zur Behebung

Vielschichtig und betriebliches Thema

Datenverlust

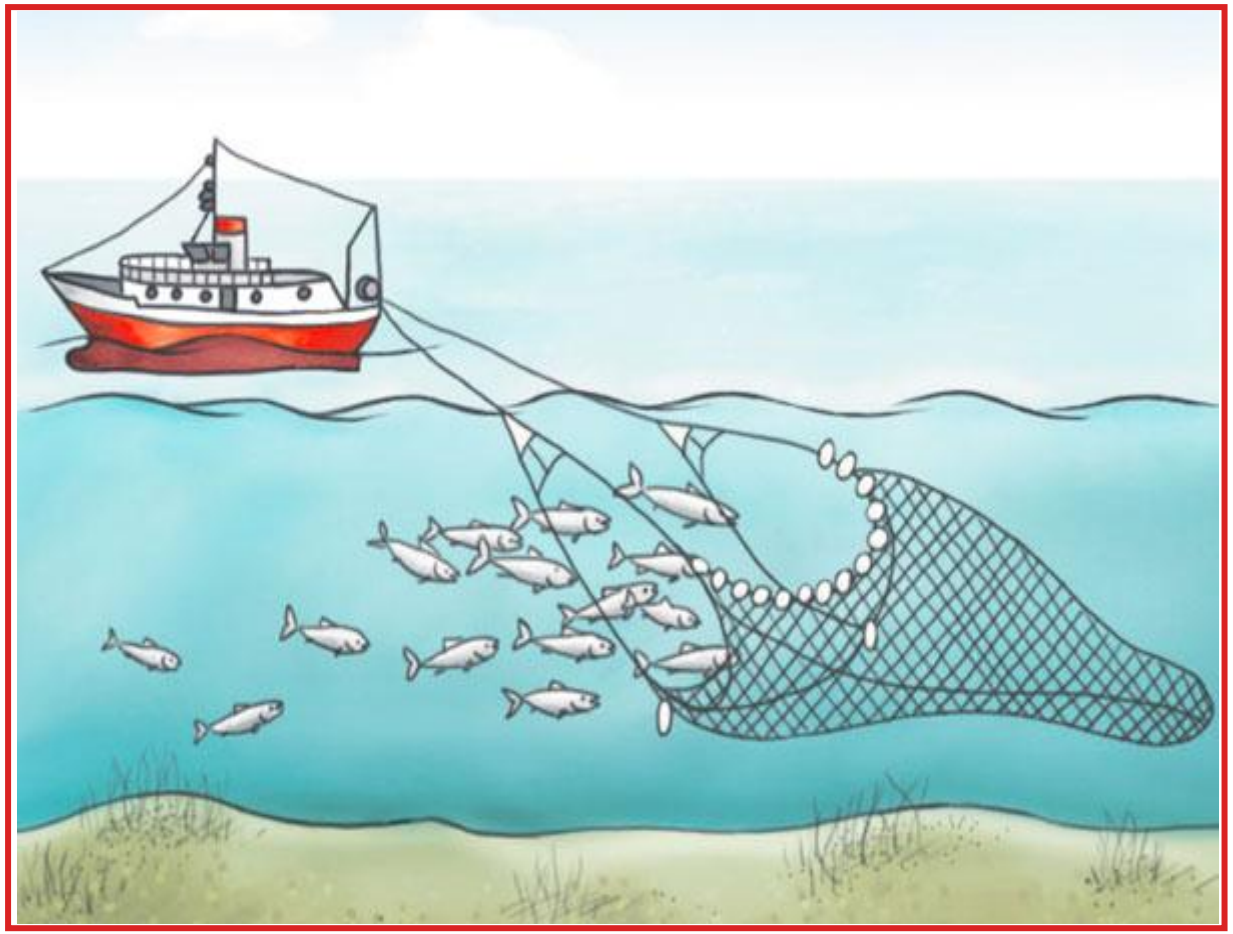
Stillstand der Geschäftsentwicklung

Emotionale Belastung und Stress

Vertrauens-/ Reputationsverlust

Unsichere Geschäftspartner

ALLE werden angegriffen!



"Amateure hacken Systeme, Profis hacken Menschen"

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

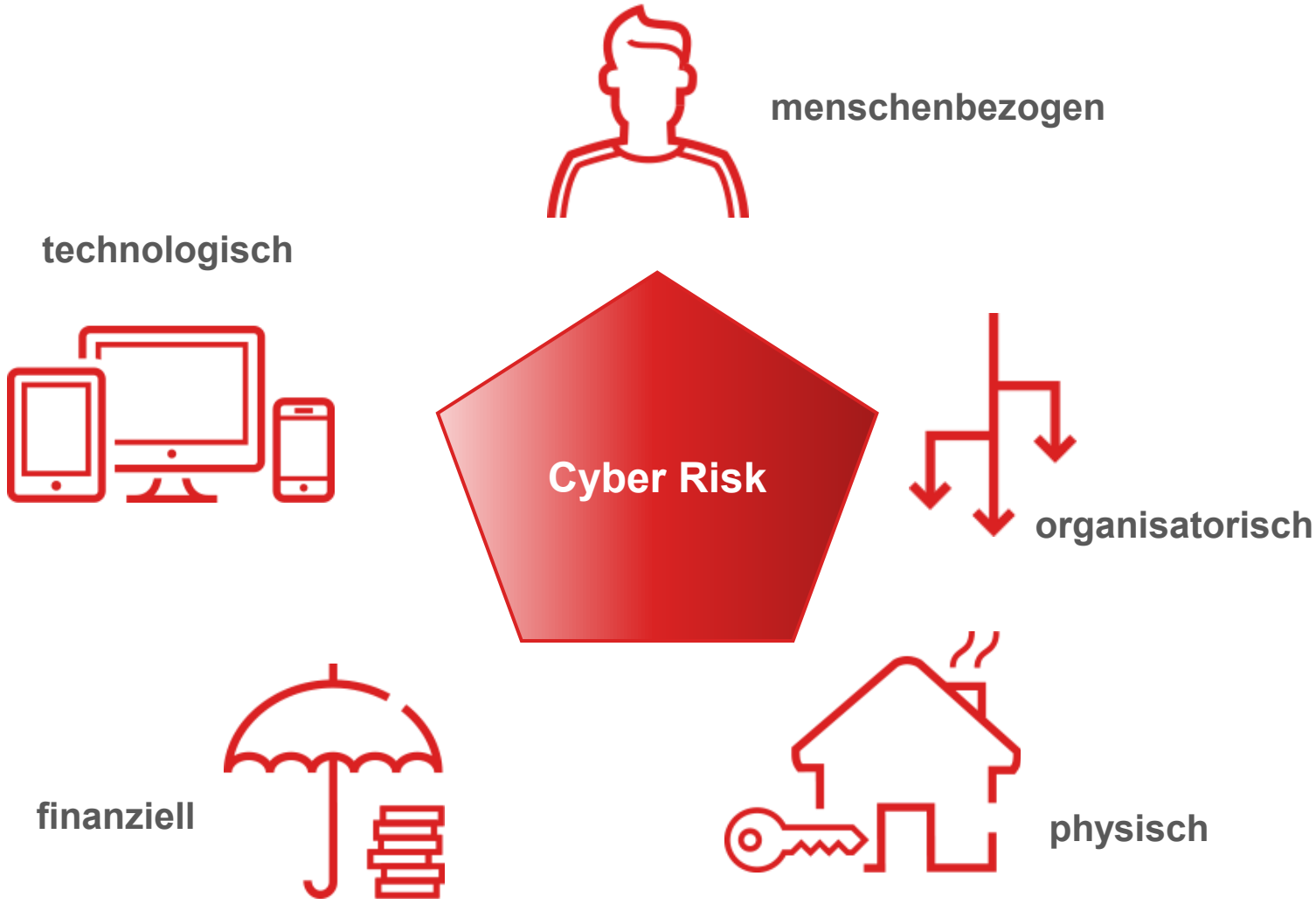
***80 % der Angriffe** zielen auf den Menschen*

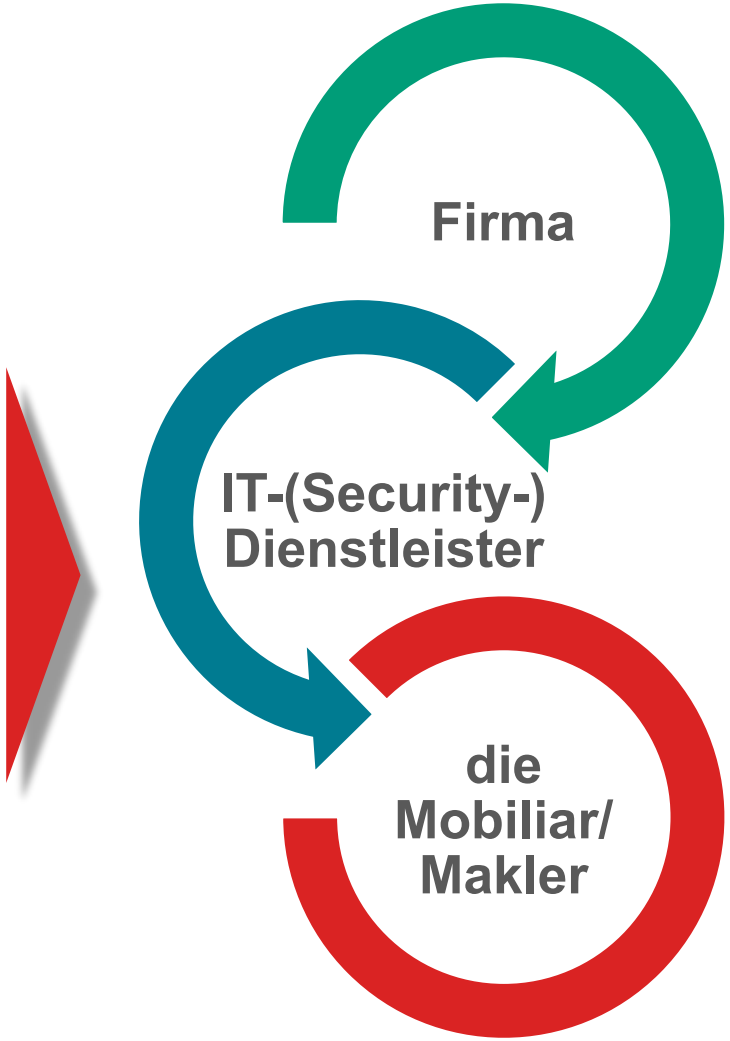
Quelle: Enisa Top Threats 2025

***Ausgefeilteres und skalierfähiges Social Engineering** – GenAI als Treiber*

Wie steht es um Ihr Unternehmen und wie können Sie sich schützen?

Handlungsbedarf entlang von 5 Dimensionen und mit kompetenten, vertrauenswürdigen Partnern

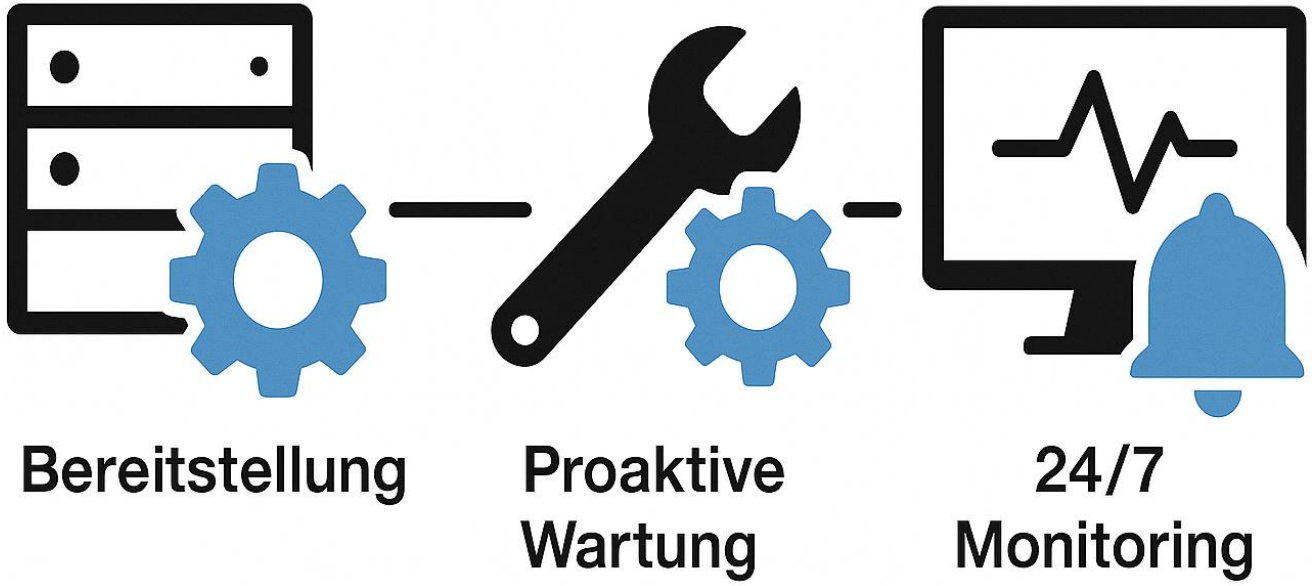




Was ist die Rolle des Managed IT-(Security-)Dienstleisters?

Wir als Ihr Managed IT Security Dienstleister

Ein moderner Managed Service Provider (MSP) agiert als strategischer Partner, der nicht nur den Betrieb sicherstellt, sondern das Unternehmen proaktiv schützt und weiterentwickelt.



Operativer Betrieb & Technische Exzellenz

- **Bereitstellung & Management:**
  Konzeption, Aufbau und Verwaltung einer sicheren und performanten IT-Systemlandschaft.

- **Proaktive Wartung & Instandhaltung:**
  Sicherstellung der Systemstabilität und -verfügbarkeit durch kontinuierliche Pflege und Updates.

- **24/7-Monitoring & Incident Response:**
  Lückenlose Überwachung der Infrastruktur und sofortige Reaktion auf Störungen und Sicherheitsvorfälle.

Proaktive Sicherheit & Strategie

- **Threat Intelligence & Abwehr:**
  Analyse aktueller Bedrohungen und Implementierung präventiver Schutzmaßnahmen.
- **Sicherheitsüberprüfungen:**
  Regelmäßige Durchführung von Schwachstellenanalysen, Audits und Penetrationstests zur Identifizierung von Risiken.
- **Kontinuierliche Optimierung:**
  Weiterentwicklung der Sicherheitsarchitektur zur Anpassung an neue Bedrohungen und geschäftliche Anforderungen.
- **Strategische Roadmap:**
  Entwicklung einer langfristigen IT-Sicherheitsstrategie, die die Geschäftsziele unterstützt und absichert.

Partnerschaftliche Beratung & Unterstützung

- **Security-Awareness-Programme:**
  Schulung und Sensibilisierung der Mitarbeiter zur Minimierung menschlicher Risikofaktoren.
- **Business Continuity & Notfallplanung:**
  Beratung und Unterstützung bei der Erstellung von Notfallkonzepten zur Sicherung des Geschäftsbetriebs.
- **Governance & Compliance:**
  Unterstützung bei der Einhaltung gesetzlicher Vorgaben und branchenspezifischer Standards.
- **Regelmäßiges Reporting & Transparenz:**
  Bereitstellung verständlicher Berichte über Systemstatus, durchgeführte Maßnahmen und Sicherheitslage.

Was ist die Rolle des Versicherers?

Finanzielle Absicherung des Restrisikos – Mehrwert einer Cyberversicherung

Aufzeigen von **Schadenfällen** und möglichen **Angriffsvektoren**

https://cst.apps.mobiliar.ch

Zugang zu **dedizierten Vertragspartnern**

Kontaktieren Sie die Mobiliar Generalagentur Kreuzlingen

Inkludierte Präventions-massnahmen

mobiliar.ch/cyber-training

Versicherungsspezifische Deckungen

– Betriebsunterbruch und Kosten für Daten-/Systemwiederherstellung

Stärkung der **Cyber Widerstandsfähigkeit**

Vor einer… ← Cyber-attacke → *Nach einer…*

Verständnis Bedrohungslage und Verwundbarkeit

- **Bewusstsein** – www.mobiliar.ch/cyber
- **Betroffenheit** anhand **Schadenbeispiele**
- **Überprüfung Cyber-Sicherheit**

Vorbereitung und Vermeidung des Cyber-Angriffs

- **Erstellung Bereitschaft:** Kontaktlisten und Abschluss **Cyber-Versicherung**
- Umsetzung **IT-Grundschutzhygiene**
- **Stärkung der menschlichen Firewall**

Erkennung und Reaktion

- **Erkennung** IT-Betriebsstörung vs. Cyber-Attacke
- **Dokumentation** und **Alarmierung** IT-Dienstleister und **Versicherer**
- Übergang in **Notbetrieb** und Unterstützung **Partnernetzwerk Versicherer**

Wiederherstellung, Rückkehr in Normalbetrieb

- **Wiederherstellung** IT-System/Daten durch IT-Dienstleister
- **Finanzielle Entschädigung** durch Versicherer und **Aufarbeitung Arbeitsrückstände**
- **Lessons Learned**

Praktische Tipps zur Umsetzung

Sicherstellung der Zukunftsfähigkeit im Cyber Risk

Gelebte

Cyber-Sicherheitskultur

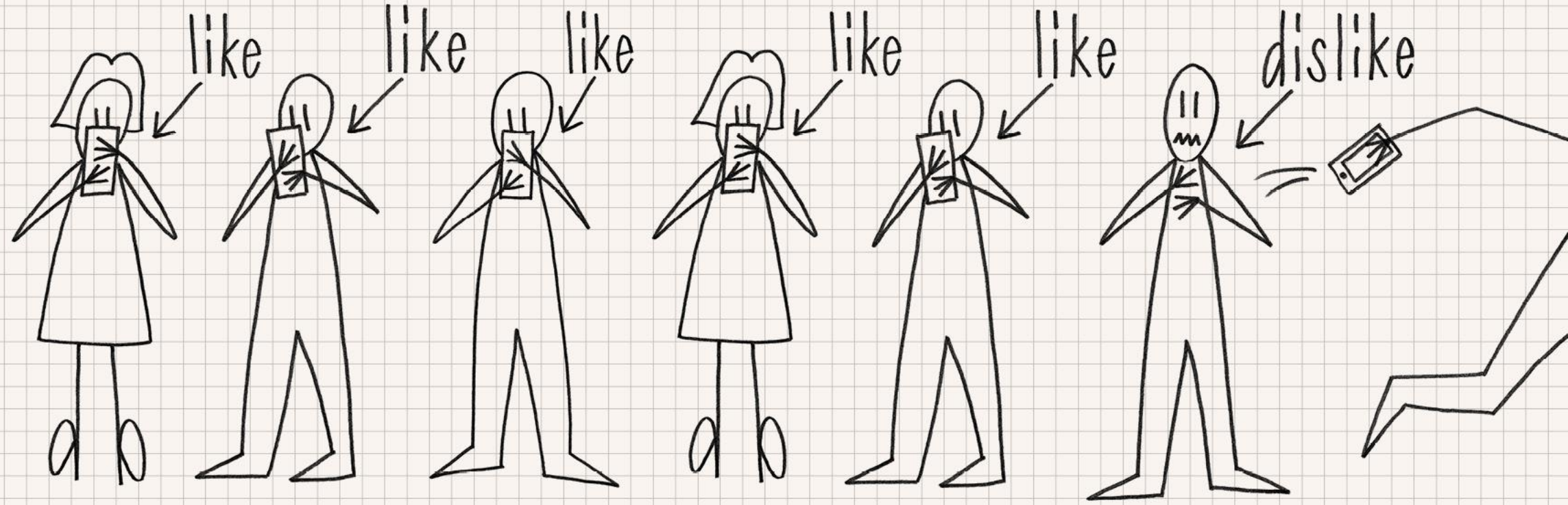
und Investition in den

Cyber-Schutz

- Korrekt **konfigurierte, geschützte und gepflegte IT**
- **Desaster Recovery Plan**
- **Awareness** gesamtes Team
- **Cyberversicherung**

Diskussion und Fragen

Schadenskizze



Vielen Dank für Ihre Aufmerksamkeit

Anhang

Erwartungen der Versicherungsgesellschaften an KundInnen

Zu adressieren mit IT-Dienstleister

Netzwerkschutz: Segmentierung, Firewall, VPN

Anti-Viren-Schutz auf allen Geräten inkl. Server

Unveränderbares, offline **Backup**

- **Regelmässige Durchführung von Updates**

⇨ Keine Mindestanforderung

KONTAKTE

Für Fragen rund um die Restrisiko-Versicherung

Ihre Mobiliar Generalagentur Kreuzlingen

Telefon 071 677 00 30 oder

E-Mail kreuzlingen@mobiliar.ch

Für IT-technische Security-Fragen

Ihre Weihrich Informatik

Telefon 071 677 13 30 oder

E-Mail info@weihrich.ch