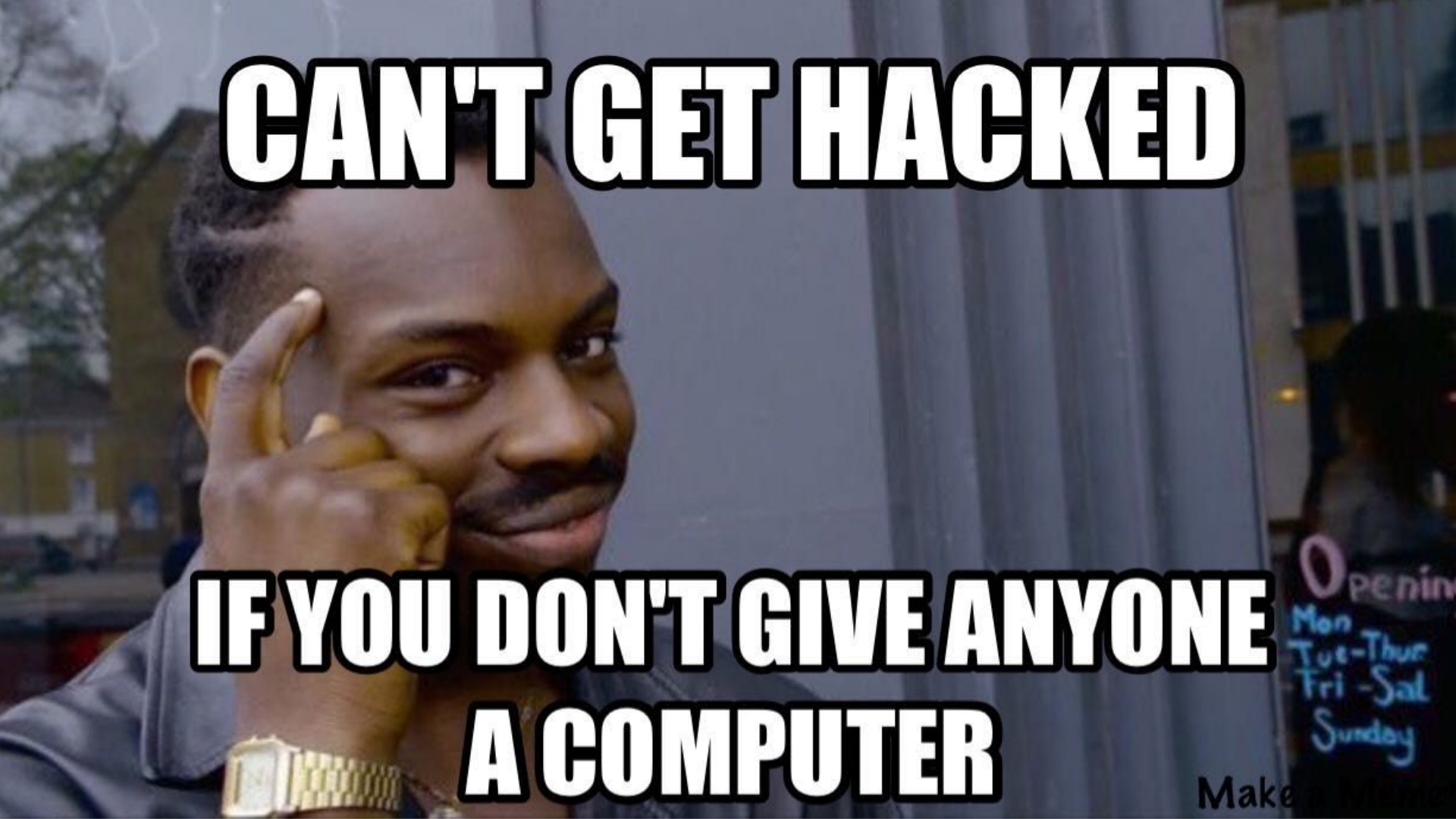
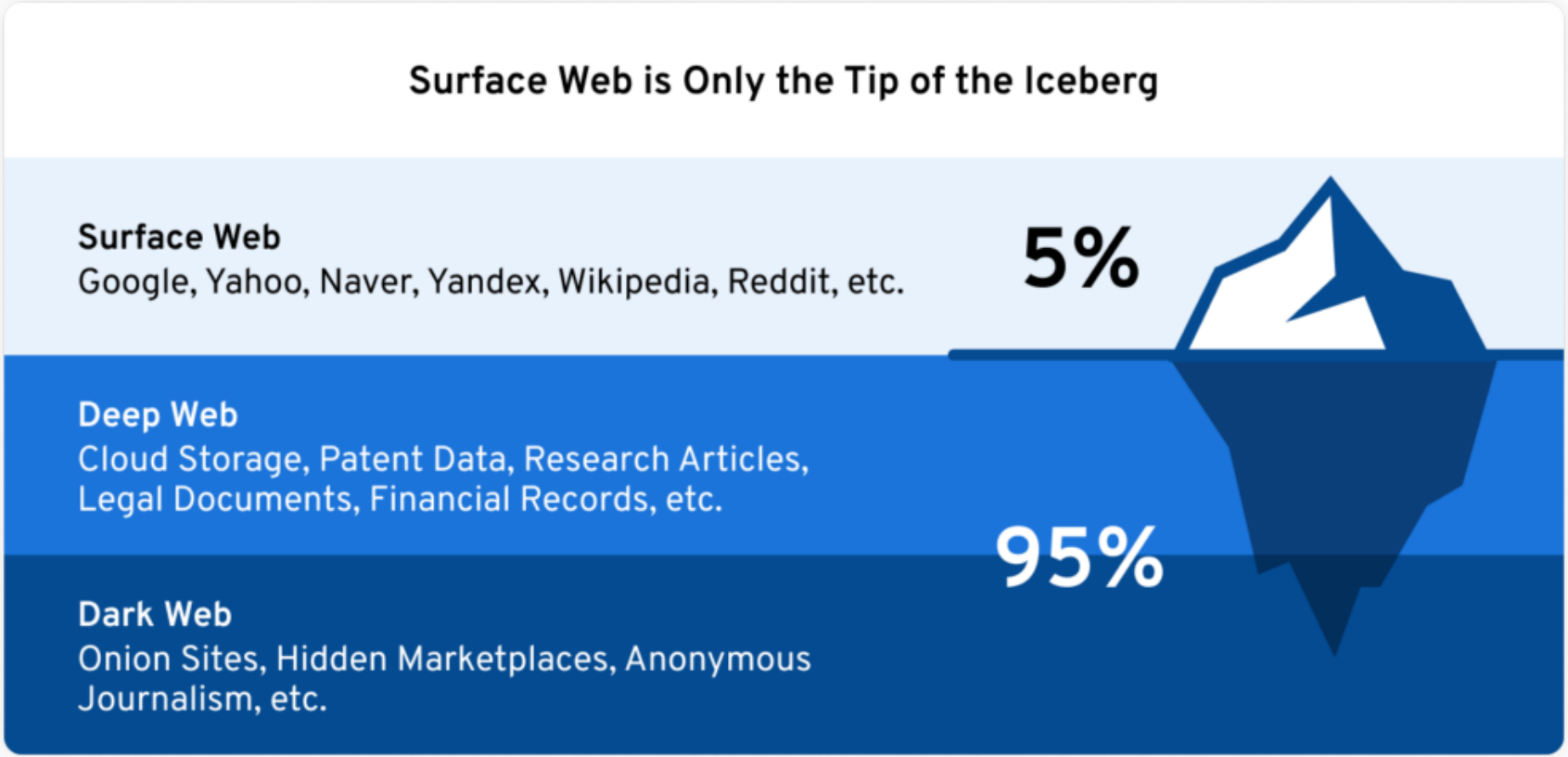

SBA
Research

KI und Digitalisierung von der Security- und Privacy-Seite beleuchten

MINT Kongress, 25. Feb 2025

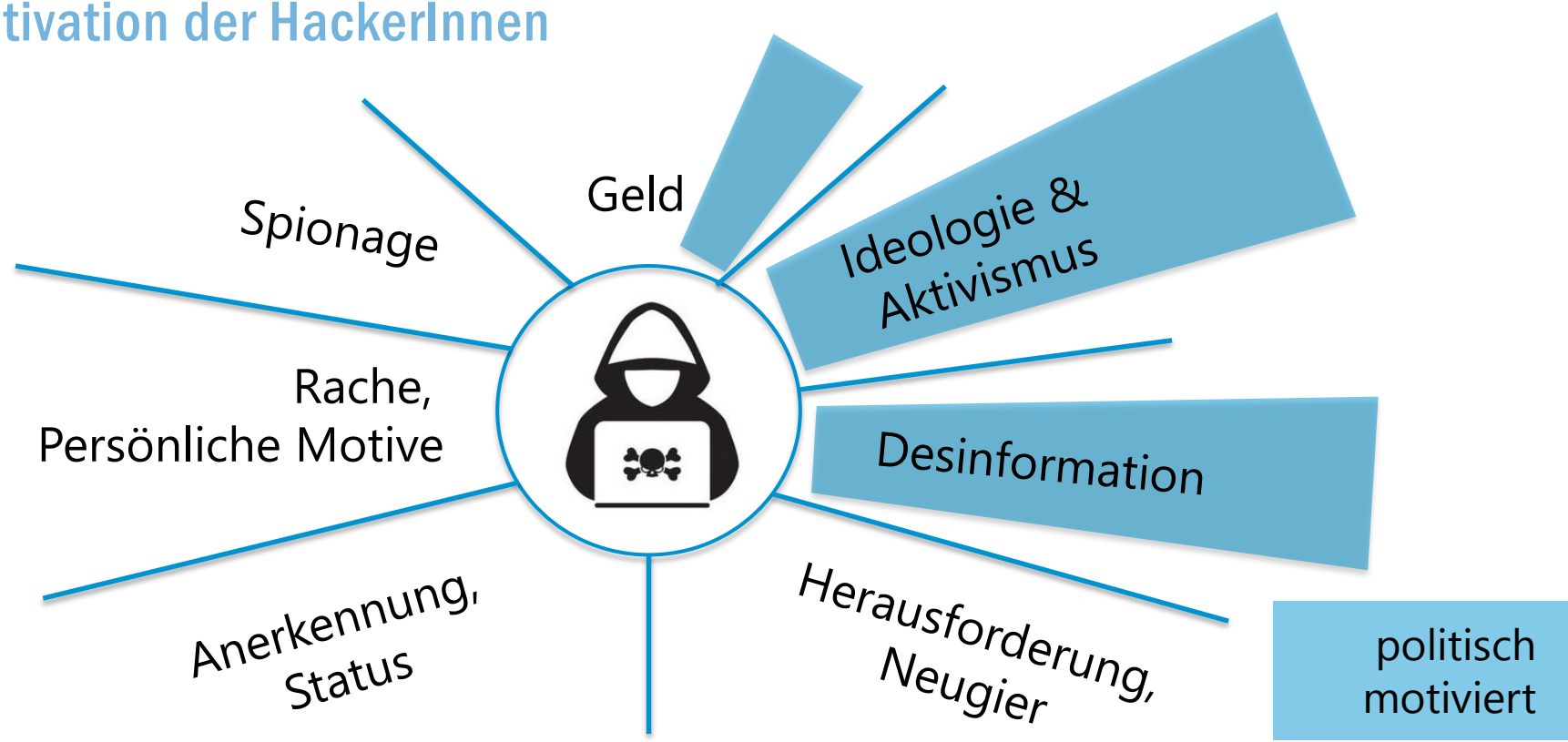
Bundesministerium Arbeit und Wirtschaft
Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
FFG
wirtschaftsagentur wien | Für die Stadt Wien
netidee FÖRDERUNGEN
Europäische Kommission
FWF Österreichischer Wissenschaftsfonds


CAN'T GET HACKED
IF YOU DON'T GIVE ANYONE A COMPUTER
Mon
Tue-Thur
Fri -Sat
Sunday



https://www.keepersecurity.com/blog/es/2023/06/28/deep-web-vs-dark-web-whats-the-difference/

Warum?
Motivation der HackerInnen

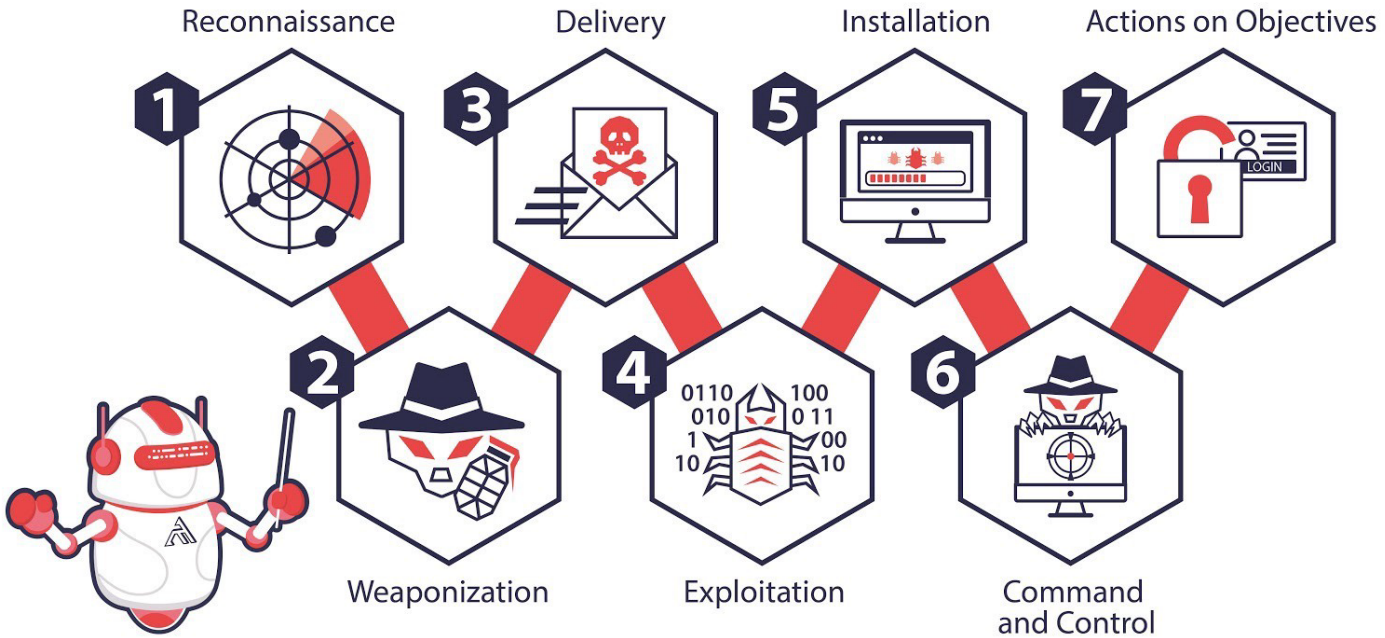


Warum ich?

Bei mir gibt es doch nichts zu holen

Cyber Kill Chain

Wie gehen Hacker vor?



https://www.klogixsecurity.com/hs-fs/hubfs/Untitled%20design-Dec-02-2020-09-35-04-49-PM.png?width=1600&name=Untitled%20design-Dec-02-2020-09-35-04-49-PM.png

BUSINESS MODEL

Hacker müssen **nicht mehr** über besondere **Programmierkenntnisse** verfügen oder ihre eigene Schadsoftware entwickeln.
Sie **können** die „**Kunden**“ **sein**. Der **Anbieter** übernimmt die gesamte Vorarbeit und **verkauft** einen **einsatzbereiten Cyberangriff.**

PaaS Fraud aaS

Ransomware aaS

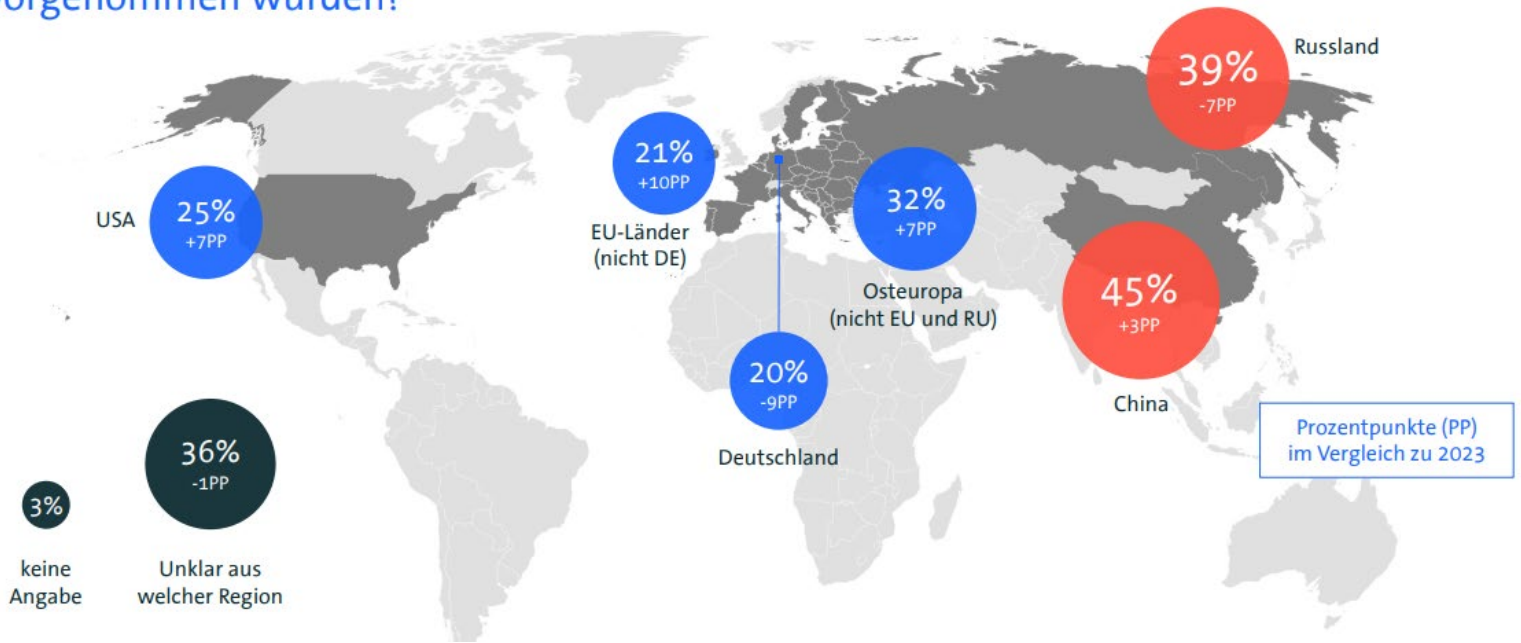
Threat Landscape

Jetzt und in Zukunft

https://www.enisa.europa.eu/news/enisa-news/hackers-for-hire-drive-the-evolution-of-the-new-enisa-threat-landscape https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030

Quelle der Angriffe

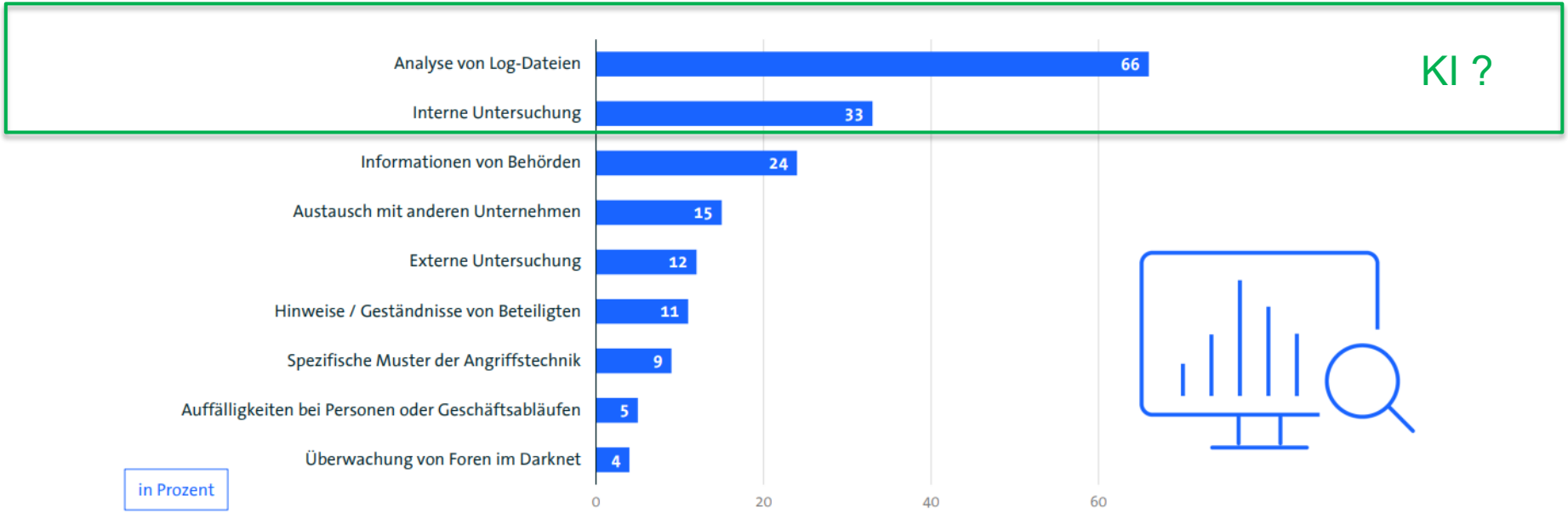
Konnten Sie feststellen, von wo aus bzw. aus welcher Region diese Handlungen vorgenommen wurden?



Bitkom Research 2024 https://www.bitkom.org/sites/main/files/2024-08/240828-bitkom-charts-wirtschaftsschutz-cybercrime.pdf

Wie Taten aufgedeckt werden

Auf welcher Grundlage haben Sie die Erkenntnisse erlangt?



Bitkom Research 2024 https://www.bitkom.org/sites/main/files/2024-08/240828-bitkom-charts-wirtschaftsschutz-cybercrime.pdf

Wie schütze ich mich?

NIST Cybersecurity Framework 2.0
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Warum KI & Security?

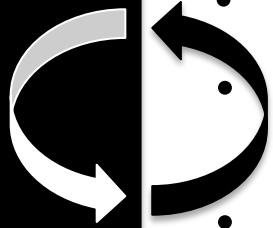
Because we can!

Because hackers use it too!

KI & Cyber Security

Angreifer

- Geschwindigkeit
- Skalierbarkeit & Effizienz
- Einstiegshürde gesenkt
- Automatisierung
- Personalisierte Angriffe



Verteidiger

- Geschwindigkeit
- Skalierbarkeit & Effizienz
- Fachkräftemangel entgegenwirken
- Neue Anwendungen durch Sprachmodelle
- Vermeidung menschlicher Fehler

Neuartige Risiken

- KI wird zum Angriffsvektor
- Programmierfehler, Supply Chain, Fehler im Training oder den Daten, gezielte Angriffe (adversarial machine learning), …
- Nachvollziehbarkeit und Transparenz (Black Box)
- Abhängigkeit und Wissensverlust
- Data Drift
- Achtloses Verhalten

Gefahren

Wie nutzen Hacker KI für Angriffe?

- Phishing Emails
- Deepfakes
- Erzeugen von Malware mit Hilfe von LLM
- KI basierte Angriffe
- Dark Market LLM, bösartige LLM

Allgemeine Gefahr

- Halluzinationen von LLMs

Chancen

AI unterstütze Verteidigung

- Verteidigung von Phishing Angriffen
- Finden und schließen von Schwachstellen
- Unterstützung beim Threat Hunting
- Anomalie Erkennung
- Erstellung von Honeypots

Studie

Präsentation

Sicherheitsforschung
AI & Security bei SBA Research

- **Model Watermarking** - Schutz vor Diebstahl geistigen Eigentums (Daten oder trainierte ML-Modelle)
- **Federated Learning** - Datenschutzschonende Berechnungsmethoden
- **Neuartige Methoden zur Datenanonymisierung**, auch komplexer Datentypen
- Synthetische Daten

Security 1X1

oder die 5 IT-Sicherheitsgebote

1. **Passwörter**
   - wählen Sie **sichere Passwörter**
   - **trennen** Sie **berufliche** und **private Passwörter**
   - Aktivieren Sie wenn möglich die **2-Faktor Authentifizierung**
2. Generelle **Achtsamkeit** und gesunde Skepsis beim Umgang mit **Mails**, **Anhängen** und **Downloads**
3. Halten Sie **Ihre Geräte** und **Software aktuell**
4. Benützen Sie einen **aktuellen Virenschutz** und **Firewall**
5. Erstellen Sie **regelmäßig Datensicherungen**

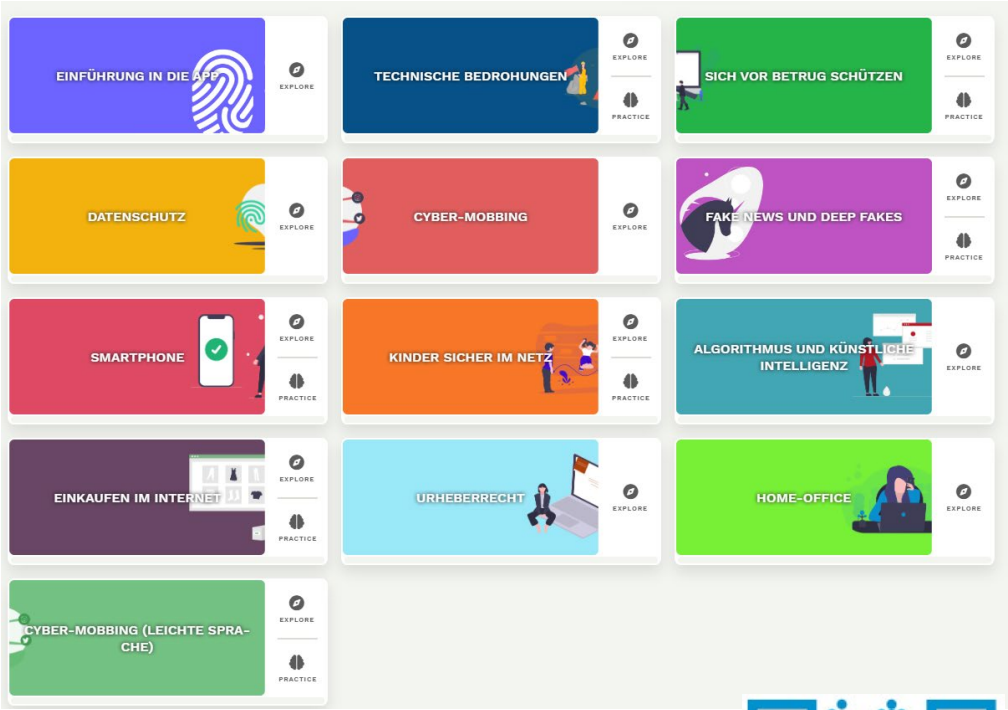
Cybersecurity in der Schule

Interesse wecken und Wissen vermitteln

Cyber Security Quiz

- Seit 2021
- Partner: Ovos, OIAT, SBA Research, CSA
- In Kooperation mit BDW, BMBWF, DIA, AK, FFG, Stadt Wien, fit4internet
- 25.000+ UserInnen

https://cybersecurityquiz.at/



GÜTESIEGEL LERN-APPS

2024 gingen **240 IT-Expertinnen** an **80 Schulen** in ganz **Österreich** und sprachen mit **170 Klassen/Gruppen** über die Faszination IT.

Zielgruppe 3. & 4. Klasse Sek I

Wieder 9. Dez 2025

https://shedigital.at/die-it/

Shecurity

Hackerinnen Training

SHECURITY

- Zielgruppe: FINTA*
- Alter: 14 – 65 Jahre
- Monatliche Security-Trainings meist hybrid, kostenfrei
- Fokus auf technische Security Themen

https://verbotengut.at/allgemein/hackerinnen-training/

SBA Research

CYBER SECURITY AUSTRIA

TU WIEN CYSEC CYBERSECURITYCENTER

Security & Schulen

Angebote der Cybersecurity Austria

- **Austrian Cybersecurity Challenge** – SchülerInnen, StudentInnen, offene Klasse
- Security Training für LehrerInnen
- Hackerinnen Training

https://verbotengut.at/

Stephanie Jakoubi

Teamleitung Strategische Partnerschaften & Kommunikation
Geschäftsleitung

Vorsitzende CSP Cyber Sicherheit Plattform
Gründerin Shecurity Hackerinnen Training

SBA Research gGmbH
Floragasse 7, 1040 Wien
stjakoubi@sba-research.org