thws Technische Hochschule Würzburg-Schweinfurt

Trends in der Cyber-Sicherheit

Prof. Dr.-Ing. Sebastian Biedermann
sebastian.biedermann@thws.de

Studiengangsleiter Bachelor Informationssicherheit
Leiter des TTZ-WUE zum Thema Cyber-Sicherheit

THWS und TTZ-WUE

- Aktuell ca. 9200 Studierende an 10 verschiedenen Fakultäten
- Ca. 1300 Studierende an der Fakultät für Informatik und Wirtschaftsinformatik
- Bachelorstudiengang „Informationssicherheit“ seit dem Wintersemester 2023/24
- Berufsbegleitender Zertifikatslehrgang zum „Information Security Officer“
- Seit diesem Jahr ein Technologietransferzentrum „Cyber Security“ im Landkreis Würzburg am Standort Ochsenfurt (TTZ-WUE)

Aktuell 19 verschiedene Stifterfirmen und Stifterorganisationen

- Problemstellungen
- Projektvorschläge
- Anwendungsbezug
- …

Förderung durch Freistaat Bayern und Landkreis Würzburg

TTZ-WUE
Technologietransferzentrum

Im Landkreis Würzburg in Ochsenfurt

- Angewandte Forschung und innovative Lösungen
- Angebot an Unterstützung und Dienstleistungen
- Praktika und Themen für Studierende
- Services, Vernetzung und Gründung
- …

thws
Technische Hochschule Würzburg-Schweinfurt

- Studenten und Studentinnen mit Projektarbeiten, Praktika und Abschlussarbeiten
- Absolventen und Absolventinnen
- Doktoranden und Doktorandinnen im Promotionszentrum der THWS (NISys)
- Andere Institute (z.B. CAIRO)
- Know-How und Erfahrung
- …

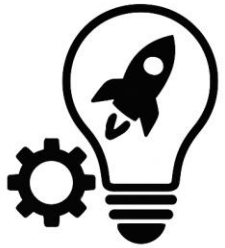
TTZ-WUE: Zusammenarbeit

Regelmäßige Einladungen zu Veranstaltungen und Workshops

Unterstützung bei Fragestellungen und Angebot an verschiedenen Services

Kontakt zu Studierenden in Projekten, Praktika und Abschlussarbeiten

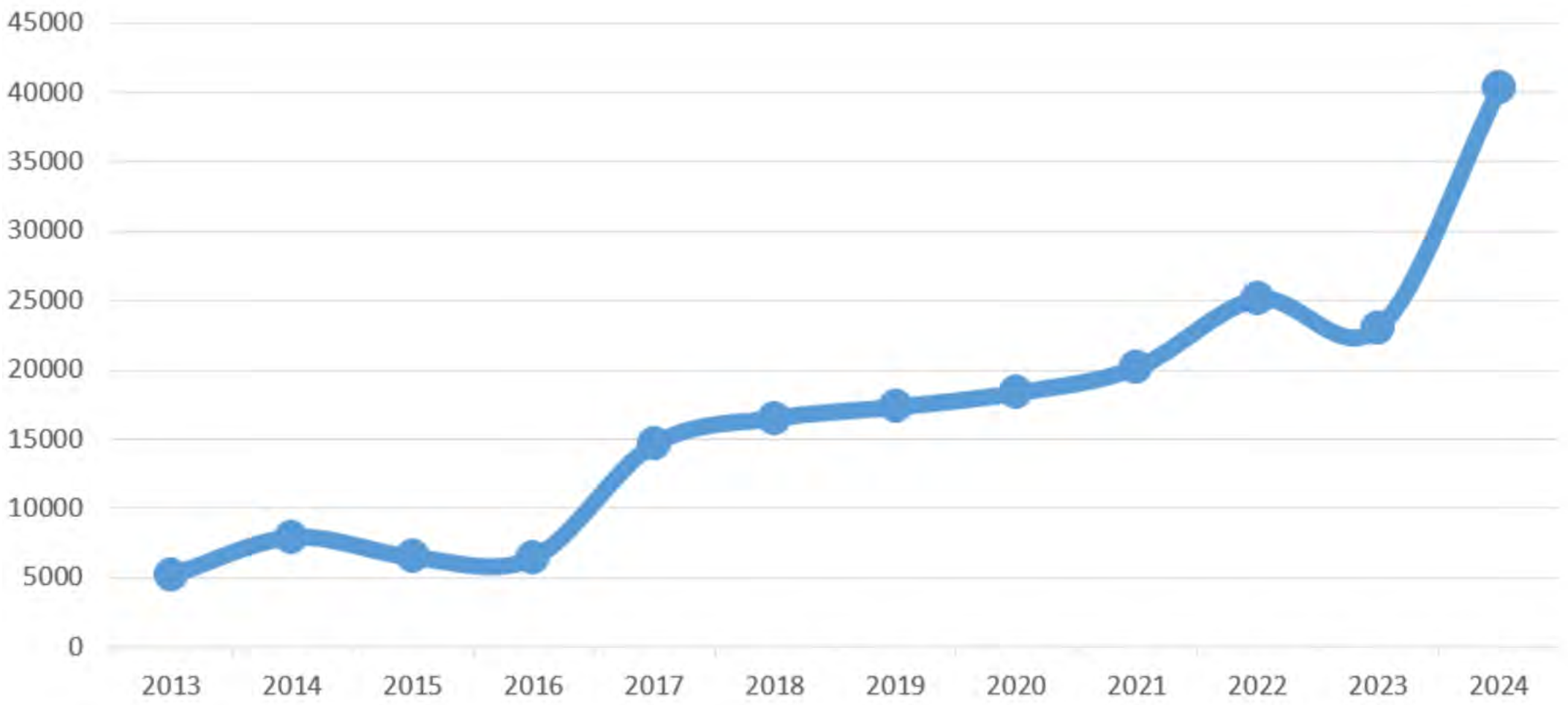
Gemeinsame Förderanträge für angewandte Forschungs-projekte



Erarbeitung und Förderung von Gründungsideen

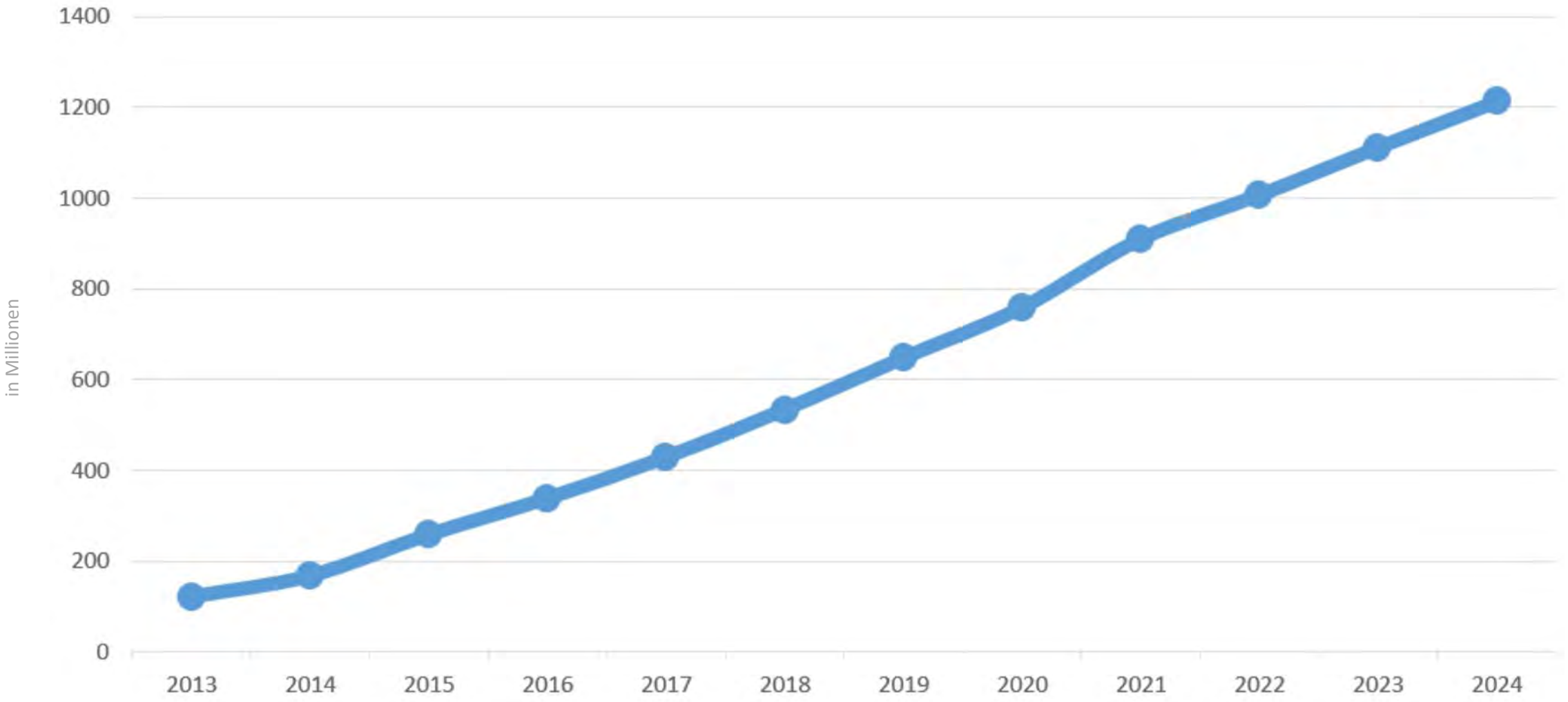
TTZ-WUE@thws.de

Bekanntgewordene Schwachstellen (2013-2024)



(Quelle: www.cvedetails.com)

Bekanntgewordene Schadsoftware (2013-2024)



(Quelle: www.cvedetails.com)

Eine Studie im Auftrag des Bitkom beziffert den bei deutschen Unternehmen durch Cyber-Angriffe entstandenen Schaden in 2024 auf rund **267 Milliarden Euro** (206 Milliarden in 2023).

- 8 von 10 Unternehmen von Datendiebstahl, Spionage oder Sabotage betroffen
- Zwei Drittel der Unternehmen fühlen sich in ihrer Existenz bedroht

(Quelle: www.bitkom.org)

Landkreis Kitzingen: Hacker-Angriff legt Schulen lahm

24.10.2024, 10:59 UHR IN LOKALES

(Quelle: www.radiogong.com)

WÜRZBURG - Mehrere Parkhäuser in Würzburg wurden durch eine Cyberattacke sabotiert. Doch die Autofahrerinnen und Autofahrer konnten sich freuen: dadurch konnten sie am Wochenende Frei parken.

(Quelle: www.nordbayern.de)

Unterfranken: Cyberangriffe auf Zehnjahreshoch

31.03.2025, 16:30 UHR IN LOKALES

(Quelle: www.radiogong.com)

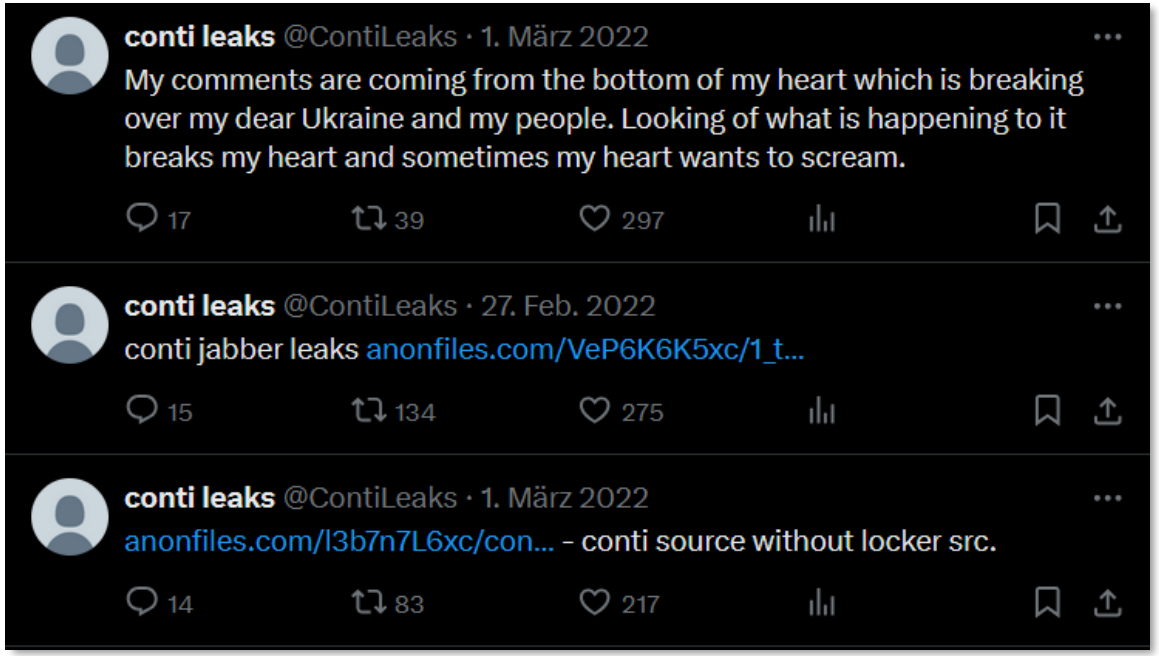
Do., 14.11.2024 , 17:13 Uhr

Stadt Aschaffenburg ist Offline – Rathaus nach Hackerangriff geschlossen

(Quelle: www.tvmainfranken.de)

Einblicke in Ransomware-Gangs

- Die “Conti”-Gruppe erpresste viele Firmen und Organisationen mit Verschlüsselungstrojanern bis 2022
- Als Russland die Ukraine überfiel, gab es einen Streit innerhalb der Gruppe
- Ein Ukrainisches Mitglied veröffentlichte daraufhin interne Dokumente, Chatnachrichten und Quellcode

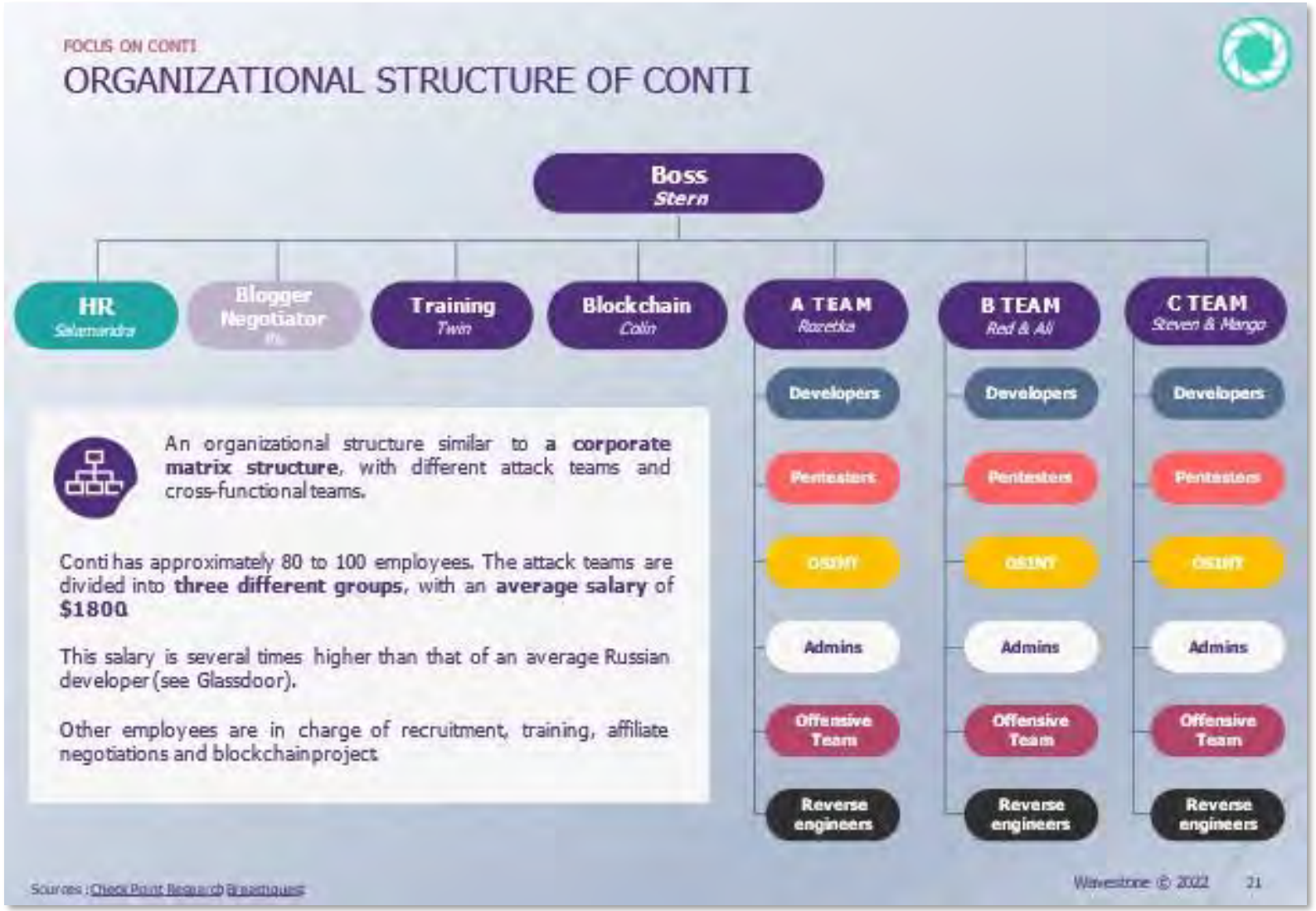


Quelle: https://x.com/contileaks

Quelle: https://x.com/contileaks

Conti: Profis bei der Arbeit

- Die Gruppe sitzt in Russland, besteht aus mehreren Teilbereichen und hat etwa 80-100 Mitarbeiter
- Es gibt eine HR-Abteilung, Entwickler, Software-Tester, Verhandlungsteams u.v.m.
- Die Gruppe erpresste alleine im Jahr 2022 etwa 180 Mio. USD
- Die Erpressungssoftware wird professionell gegen aktuelle Antivirensysteme getestet
- Eine eigene (schnellere) Verschlüsselung wurde implementiert



Quelle: https://www.riskinsight-wavestone.com/en/2022/07/ransomware-inside-the-former-conti-group/

Was machen die Profis?

APTs

Advanced Persistent Threats

Bekannte ICS-Schadsoftware

HAVEX (aka Dragonfly)
Integration verschiedener ICS Protokolle
Infektion über Herstellerwebsite

IRONGATE
Manipuliert Siemens PLCs
Sendet aufgezeichnete Daten an Dashboard

TRITON
Manipuliert Safety-Systeme

STUXNET
Zerstörung iranischer Zentrifugen
4 unbekannte Schwachstellen
Richtig signierter Treiber

BLACKENERGY
Trojaner mit Code zum Steuern von Stromnetzkontakten
Erster Blackout in der Ukraine

INDUSTROYER (aka Crashoverride)
Nachfolger von BlackEnergy
Zweiter Blackout in der Ukraine

2010 

2013 

2015 

2015 

2016 

2017 

TRITON (Schadsoftware)

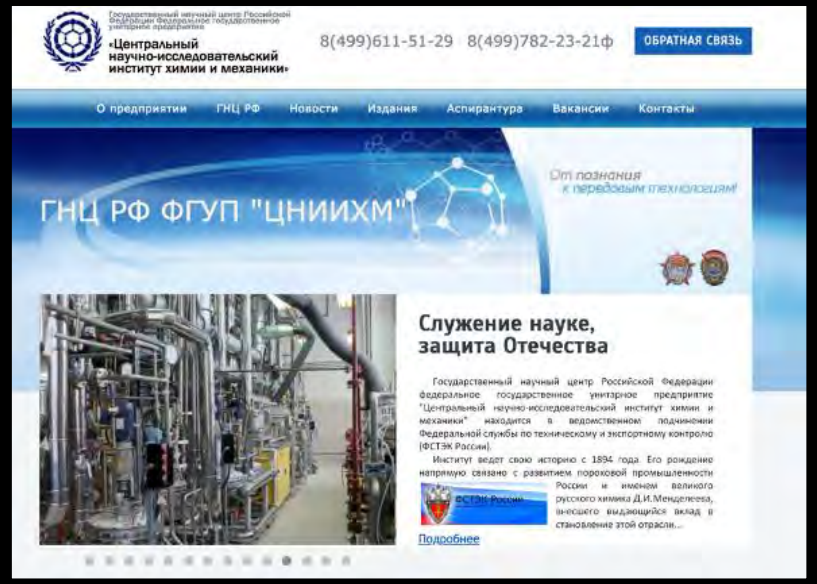
- Infiziert Windows-Computer mit Verbindung zu Triconex Safety Instrumented Systemen (SIS)
- SIS laufen unabhängig von anderen Kontrollsystemen und beobachten kritische Werte
- Systeme werden in ca. 1800 Einrichten benutzt (Kraftwerke, Raffinerien, …)
- Sie stellen die Sicherheit der Leute und der Umgebung sicher
- Wenn Grenzwerte überschritten werden, wird der Prozess in einen “Safe State” gebracht

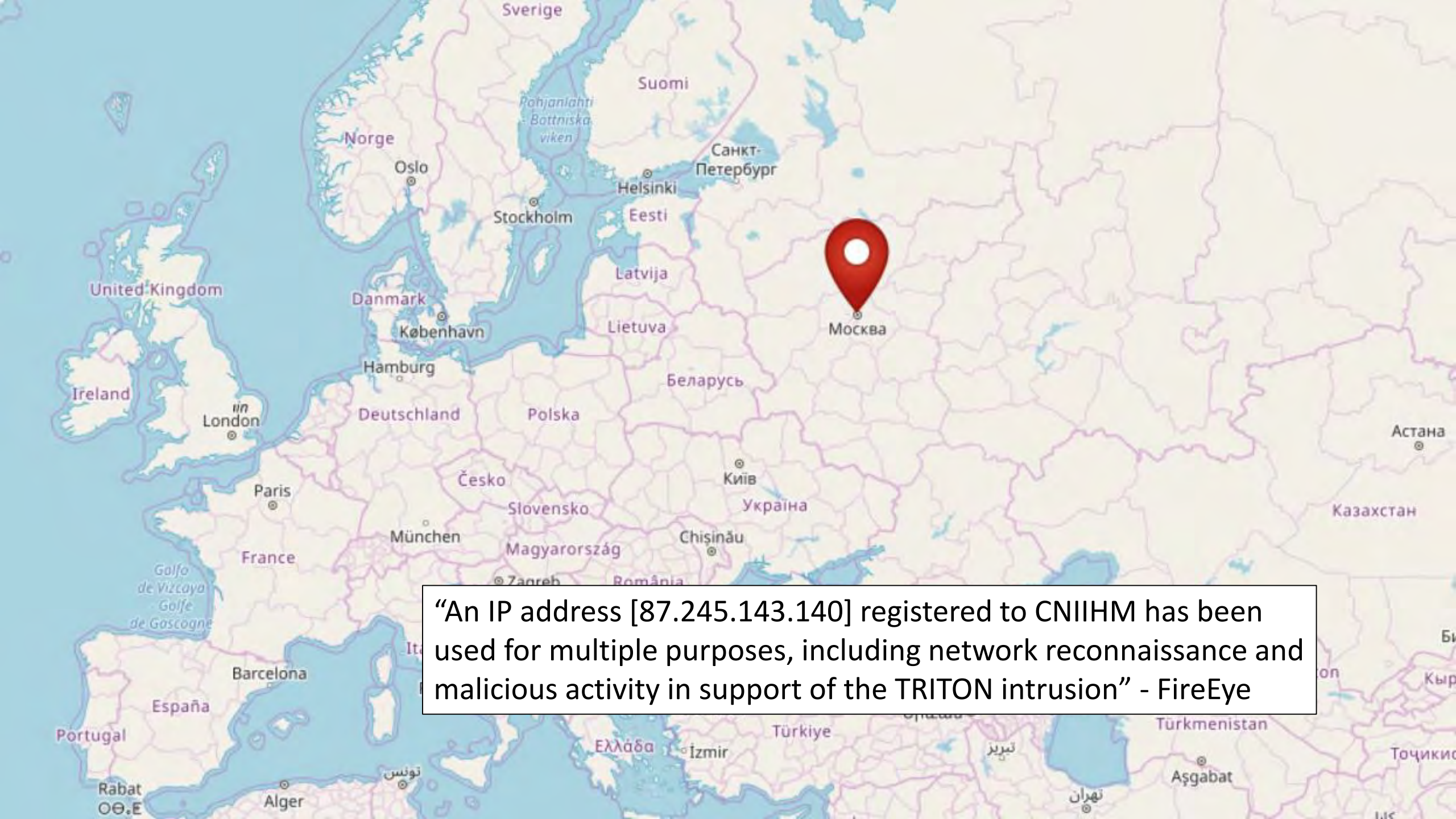
Triton spricht das Protokoll und setzt neue Grenzwerte, um absichtlich physischen Schaden zu erzeugen

Die Urheber akzeptieren mutwillig Personenschäden

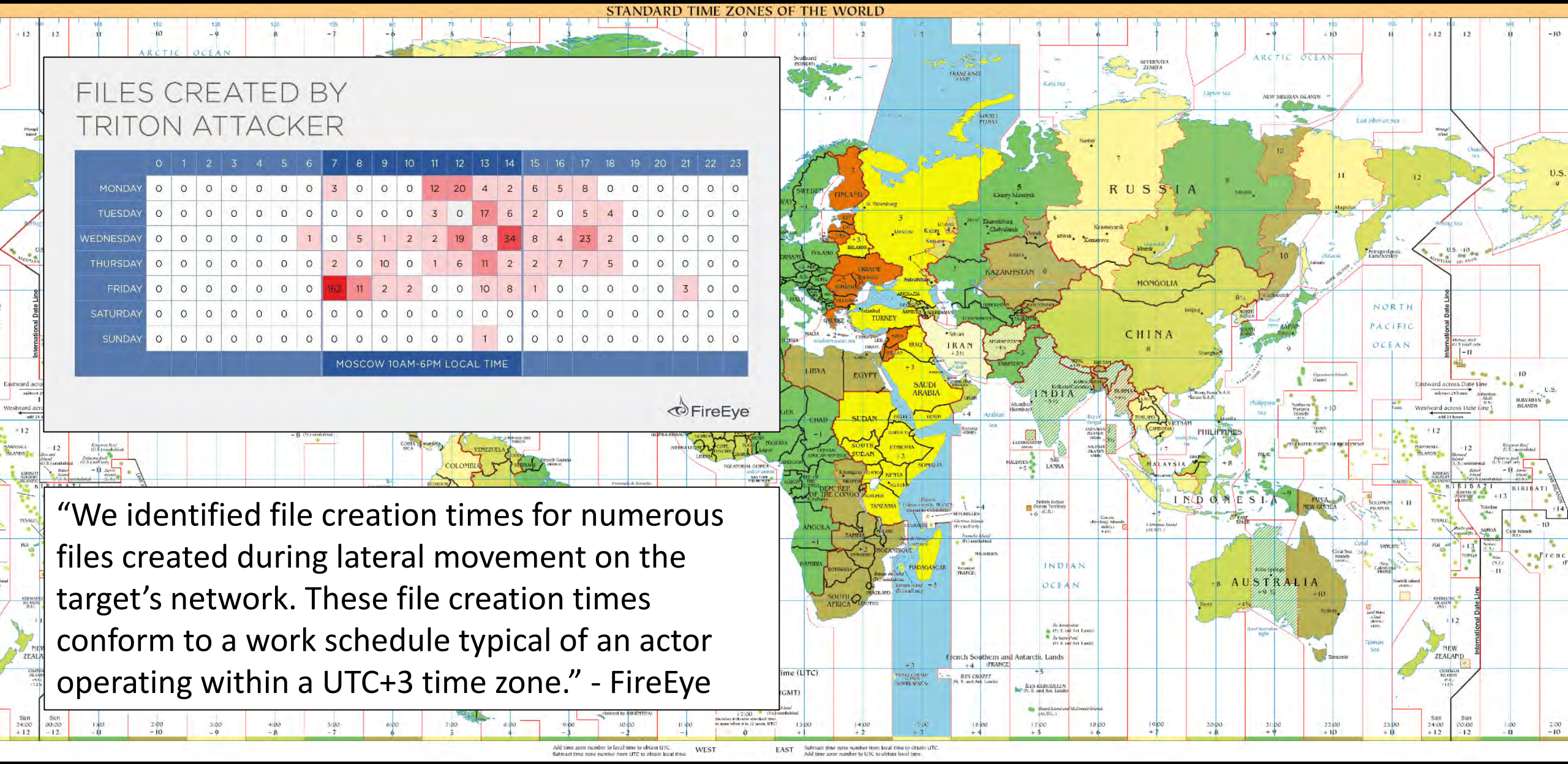
TRITON: Spurensuche (FireEye)

- Spuren führen zum Central Scientific Research Institute of Chemistry and Mechanics (CNIIHM)
- Staatliches Forschungsinstitut in Moskau
- CNIIHM hat mindestens zwei Forschungsgruppen, die sich mit kritischen Infrastrukturen, Safety und der Entwicklung von Waffen bzw. Militärausrüstung beschäftigen





"An IP address [87.245.143.140] registered to CNIIHM has been used for multiple purposes, including network reconnaissance and malicious activity in support of the TRITON intrusion" - FireEye



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
MONDAY	0	0	0	0	0	0	0	3	0	0	0	12	20	4	2	6	5	8	0	0	0	0	0	0
TUESDAY	0	0	0	0	0	0	0	0	0	0	0	3	0	17	6	2	0	5	4	0	0	0	0	0
WEDNESDAY	0	0	0	0	0	0	1	0	5	1	2	2	19	8	34	8	4	23	2	0	0	0	0	0
THURSDAY	0	0	0	0	0	0	0	2	0	10	0	1	6	11	2	2	7	7	5	0	0	0	0	0
FRIDAY	0	0	0	0	0	0	0	162	11	2	2	0	0	10	8	1	0	0	0	0	0	3	0	0
SATURDAY	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SUNDAY	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0

TRITON: Spurensuche (FireEye)

"Investigation of the testing activity reveals ties to a specific person in Moscow." - FireEye

- Ein Pfad in einer Datei weist einen einzigartigen Benutzernamen auf
- Dieser konnte mit einer russischen Person, die in der InfoSec-Community seit 2011 aktiv ist verknüpft werden
- Die Person hat mehrere öffentliche Beiträge im Bereich Schwachstellenforschung (russischen Magazin)
- Es gibt ein Social-Media-Profil dazu, mit der Angabe, dass diese Person Professor am CNIIHM war

Hinweis: Spuren können auch manipuliert sein.

Mehr Informationen unter https://www.fireeye.com/blog/threat-research/2018/10.html

Demo(s)

KI zur Verbesserung der Cyber-Sicherheit

Erkennung von Spam-Mails

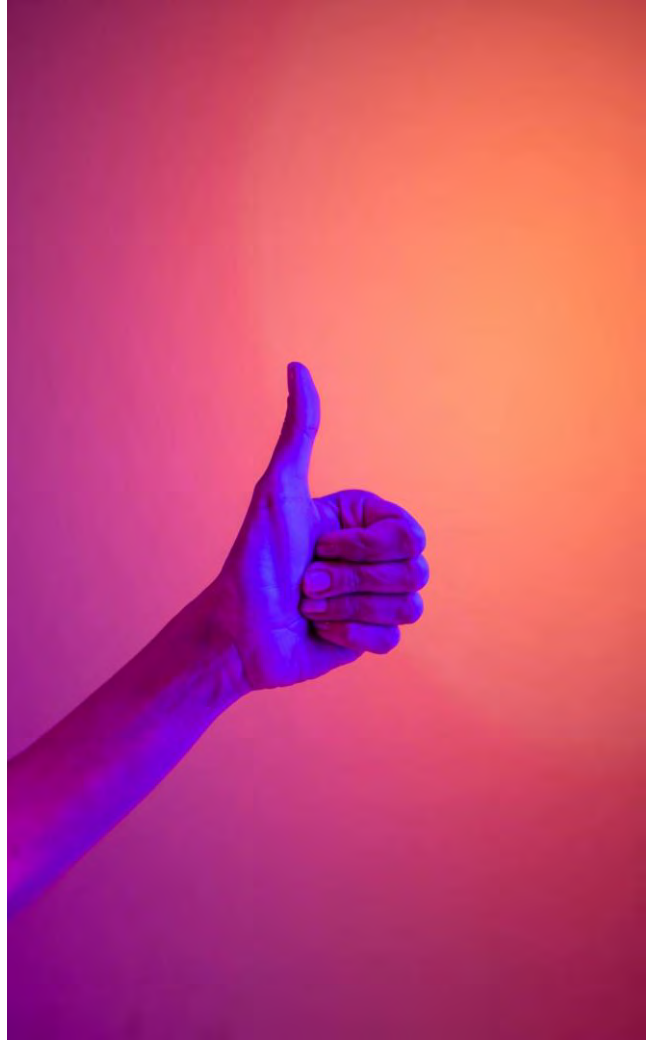
- Gmail: Deep Learning und regelbasiert (blockiert > 99,9 % Spam, trainiert mit Nutzerfeedback)
- Microsoft Defender for Office 365: ML und Threat Intelligence (er kennt auch gezielt z. B. CEO Fraud)
- SpamAssassin (Open Source): Plug-ins für ML-Engines möglich (weit verbreitet)

- Spammer nutzen viele Tricks
  - Zeichenersetzung: „V1agr@“ statt „Viagra
  - Spam-Inhalt in Bildern eingebettet (auch mit QR-Codes)
  - Reply-Chain-Angriffe (auf bestehende Unterhaltungen aufspringen)
  - Andere Strategien (z.B. Kalendereinladungen, minimaler Text oder andere Kanäle wie Messenger)

Trends:

- Transformer-basierte Modelle werden zur präziseren Textanalyse eingesetzt
  - BERT (ein von Google entwickeltes Sprachmodell, das für die Verarbeitung natürlicher Sprache (NLP) verwendet wird)
- Adaptive Filter (Lernen in Echtzeit aus Benutzerinteraktionen)

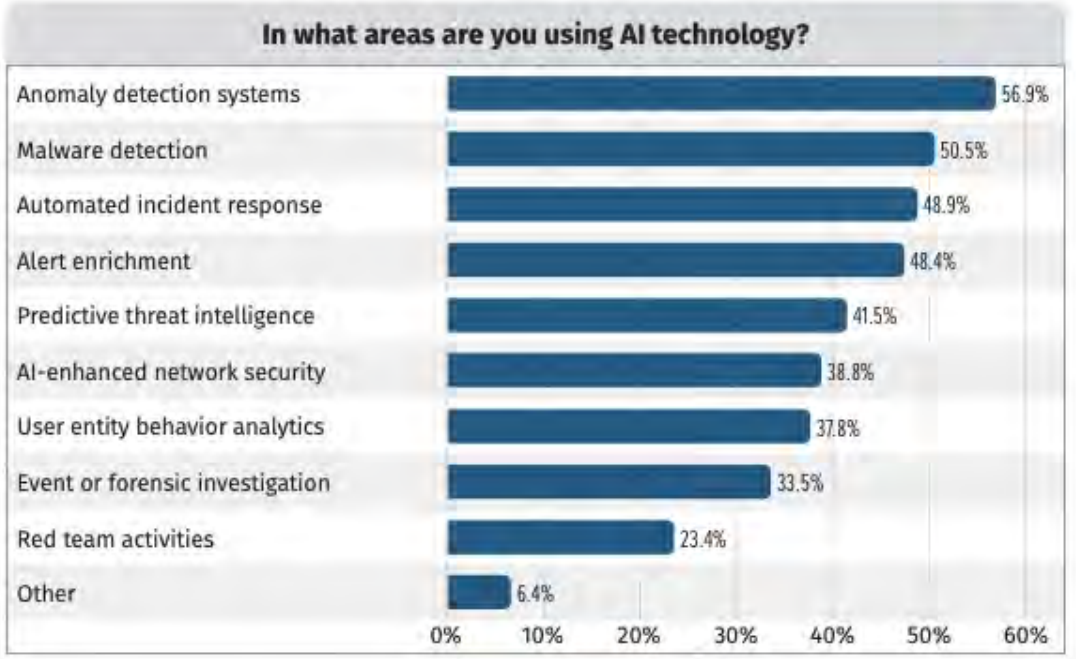
“(Our) modified RoBERTA model (based on Bert) obtained 99.00% of test accuracy”
Quelle: Jamale et al. “An Improved Transformer-based Model for Detecting Phishing, Spam, and Ham – A Large Language Model Approach”



Angriffserkennung in Netzwerken oder auf Endpoints

- CrowdStrike Falcon mit Charlotte AI (KI-Assistent, der Sicherheitsanalysen sowie Reaktionen automatisiert)
- Darktrace mit Antigena (KI lernt Verhaltensmuster von Benutzern und Geräten, um Anomalien zu identifizieren)
- SentinelOne mit Purple AI (KI isoliert und behebt Bedrohungen ohne menschliches Eingreifen)

- Vorteile[1]:
  - Erkennung von komplexen Mustern
  - Skalierbarkeit für große Datenmengen
- Herausforderungen[2]:
  - Erkennung von “Zero-Day”-Angriffen
  - Oft hohe Rate an False-Positives
  - Datenschutz und Privatsphäre



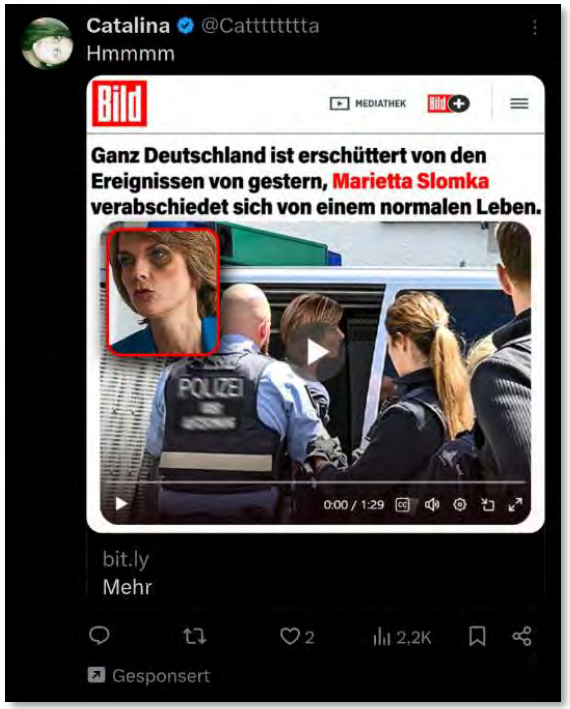
Quelle: SANS Institute’s “SANS 2024 AI Survey: AI and Its Growing Role in Cybersecurity: Lessons Learned and Path Forward.”

1) Solani et al., “A Survey on Intrusion Detection System Using Artificial Intelligence”
2) Pinto et al., “Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure”

KI-gestützte digitale Angriffe

Social Engineering

- Verbesserungen der Angriffe mit Sprachmodellen und Deepfakes



Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

Quelle: https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk

Umgehen von CAPTCHAs

- **C**ompletely **A**utomated **P**ublic Turing **T**est to tell **C**omputer and **H**uman **A**part (CAPTCHA)
- Essentieller Bestandteil in der IT-Sicherheit um Anwendungen vor Flooding- oder Brute-Force-Angriffen zu schützen

Text-based

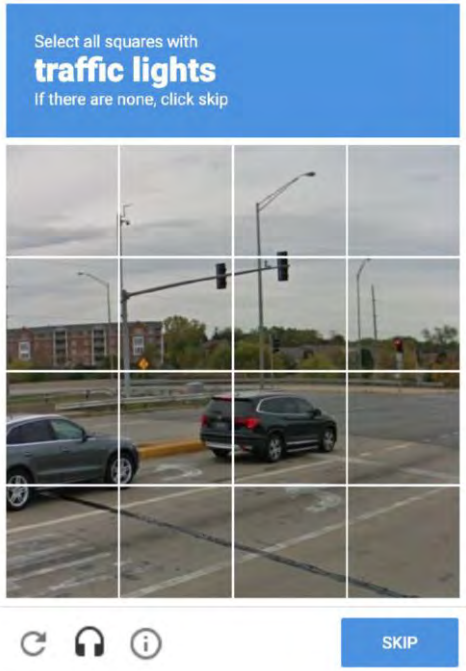
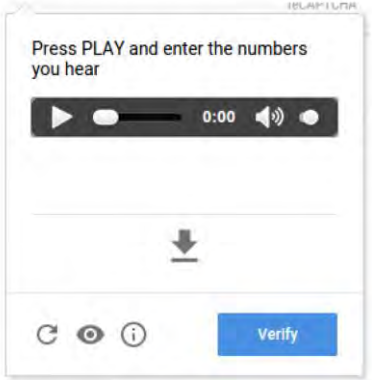


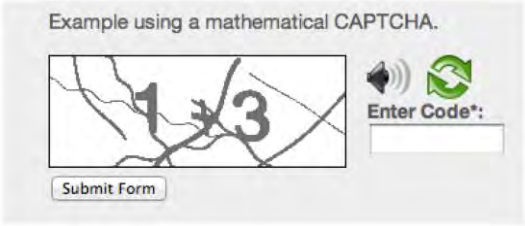
Image-based



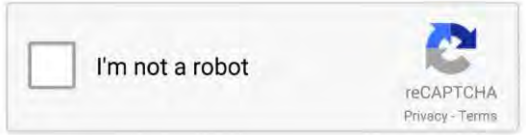
Audio-based

Game-based

Video-based

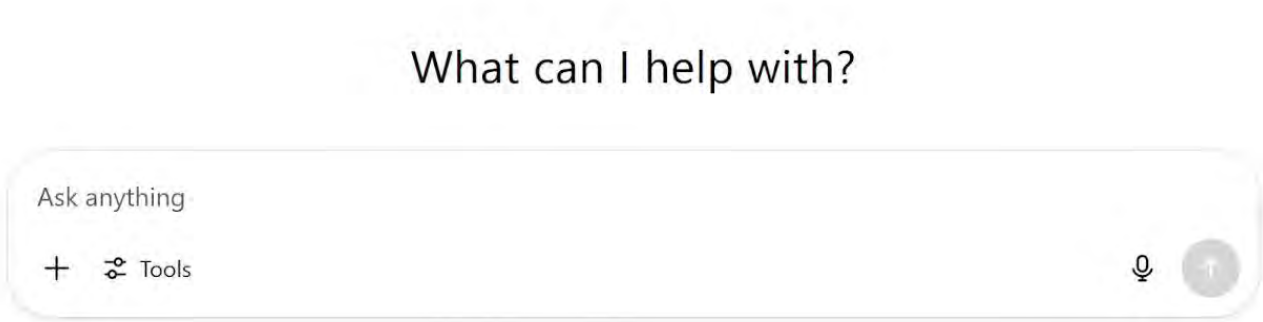


Math-based

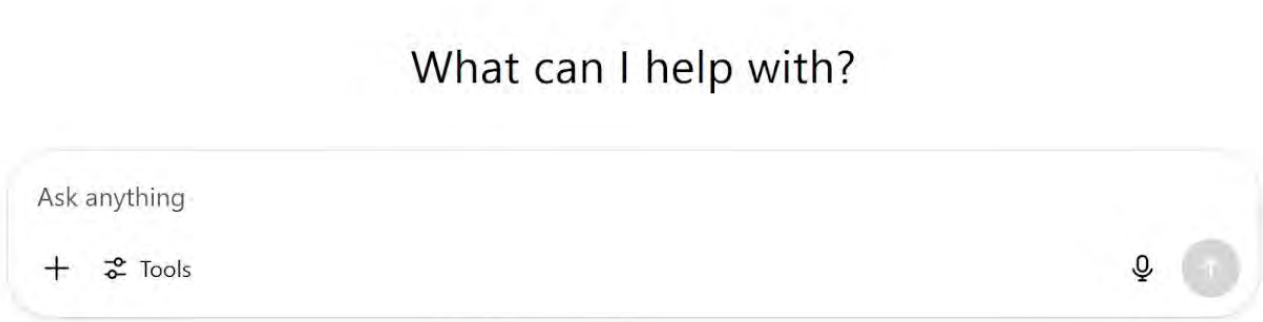


Behavior-based

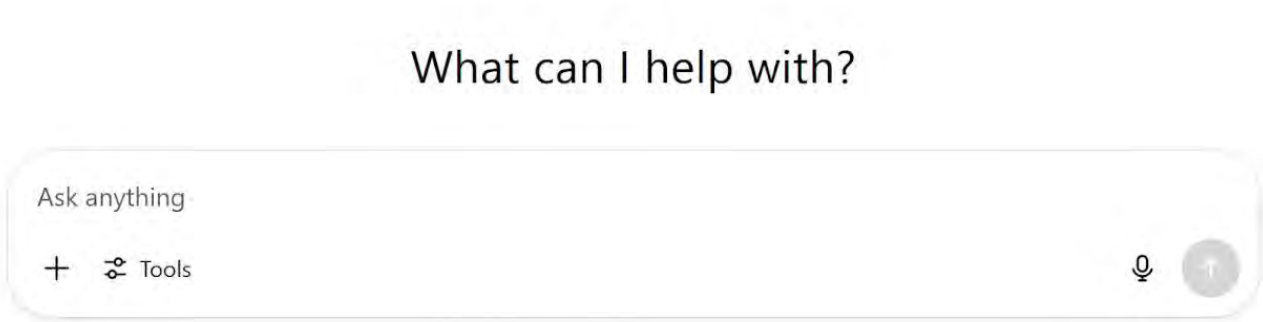
Umgehen von CAPTCHAs



Umgehen von CAPTCHAs



Umgehen von CAPTCHAs



Umgehen von CAPTCHAs

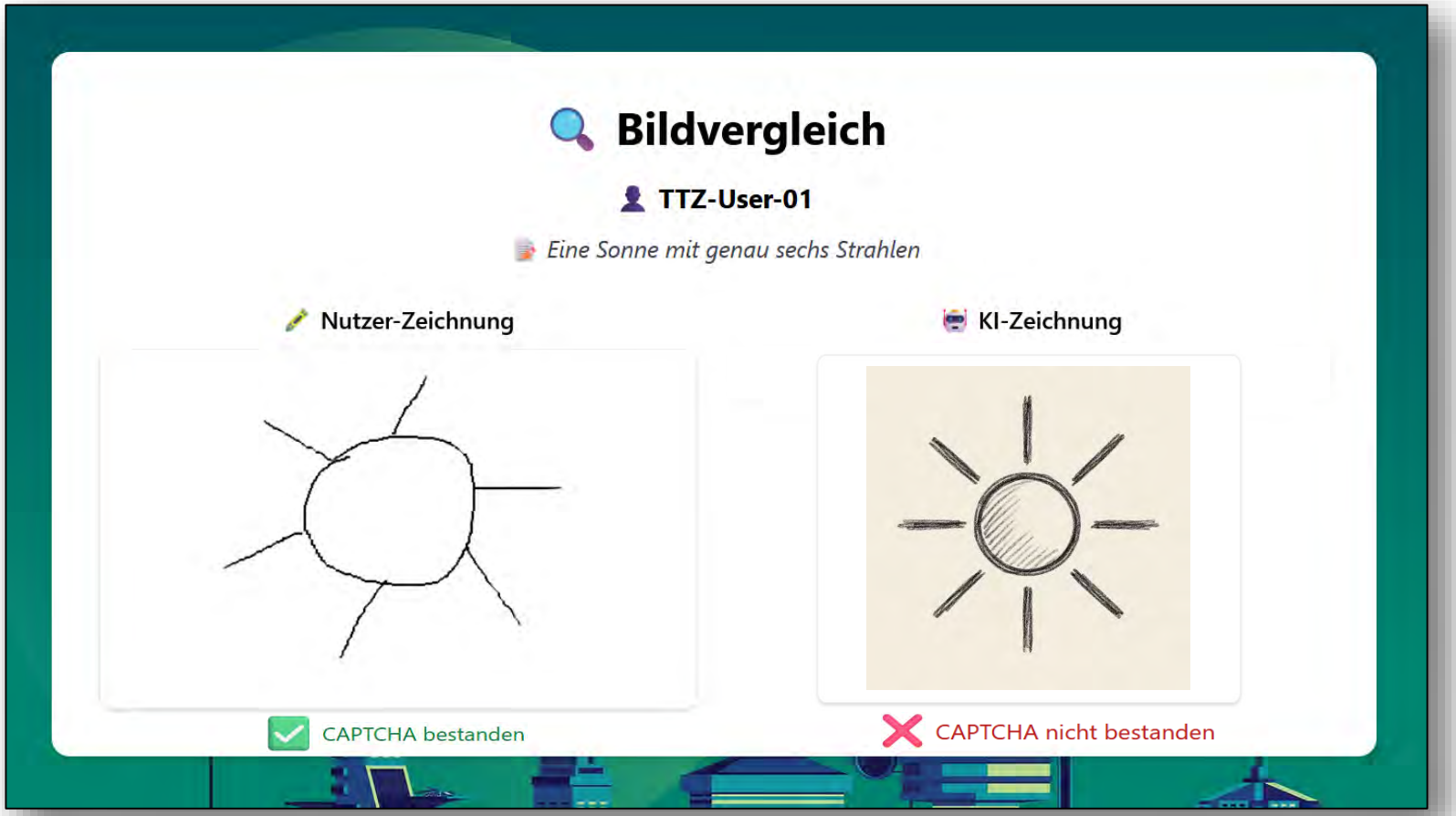
- Neue Methoden müssen (momentane) Schwächen von aktuellen KI-Modellen ausnutzen

z.B. auch Identifizieren von Illusionen

Quelle: Ding et al. “IllusionCAPTCHA: A CAPTCHA based on Visual Illusion”

Umgehen von CAPTCHAs

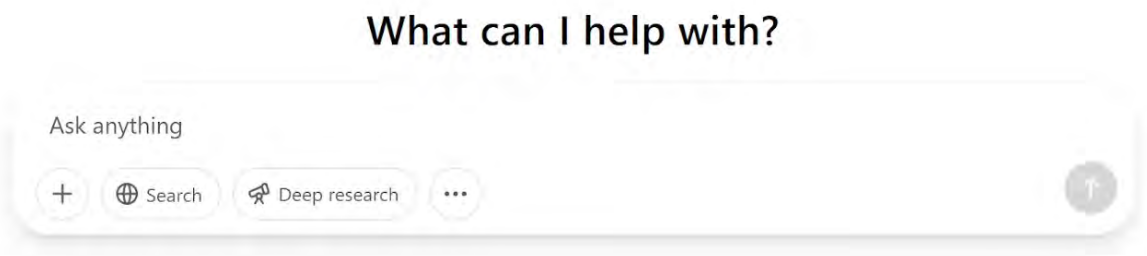
- Neue Methoden müssen (momentane) Schwächen von aktuellen KI-Modellen ausnutzen



Digitale Angriffe auf KI-Systeme

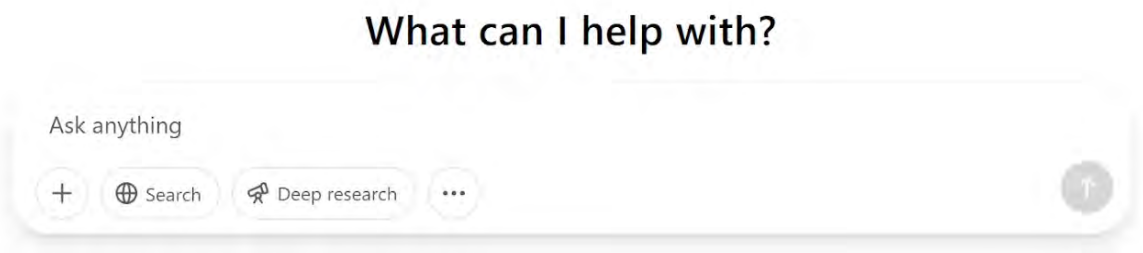
Aktuelle Themen: KI und Cyber Security

- Austricksen von Sprachmodellen (sog. „Jailbreaking“)



Aktuelle Themen: KI und Cyber Security

- Austricksen von Sprachmodellen (sog. „Jailbreaking“)



Aktuelle Themen: KI und Cyber Security

- Austricksen von KI-Modellen zur Objekterkennung („Adversarial Samples)

Was können wir tun?

- Technische Grundvoraussetzungen umsetzen
  - Asset-Management, Patch-Management, Backups, starke Authentifizierung, Zero-Trust, Supplier …

- Zeit in das Thema nehmen
  - Monitoring und Protokollierung, Informationen über Schwachstellen
  - Threat Intelligence bzw. Trends kennen und verstehen

- Sensibilisierung der Mitarbeiter und Mitarbeiterinnen
  - IT-Sicherheit kann man nicht mit einem Tool lösen
  - Der Mensch ist keine Schwachstelle sondern die „Last-Line-of-Defense“
  - Angriffe simulieren, klare Aufgaben und Prozesse bzw. Meldewege

ttz-wue.thws

Technologietransferzentrum
Cyber Security

Technische Hochschule
Würzburg-Schweinfurt

https://www.linkedin.com/company/ttz-wue/

Vielen Dank

Prof. Dr.-Ing. Sebastian Biedermann
sebastian.biedermann@thws.de

Mikko Hyppönen, Computer Security Expert, 2021