Cybersecurity und Wahlwerbung auf Online-Plattformen

ISPA-Election-Training Nationalratswahl 2024

Aula am Campus der Universität Wien , 02. September 2024

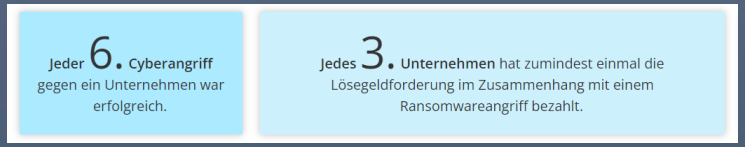
Wolfgang Rosenkranz <rosenkranz@cert.at>

CERT.at

- 2008 als gemeinnütziges Projekt von nic.at gegründet
- „Nationales Computernotfallteam“ nach NIS-Gesetz
  - Information, Erstunterstützung, Vernetzung
- 90 % Informationsdrehscheibe, 10% Incident Responder
  - Austrian Trust Circle, CERT-Verbund, CERT-Stammtisch
  - Kontaktstelle für internationale CERTs & CSIRTs
  - Community-Betreuung durch Newsletter, Discussion Groups, Blogs
  - Verteilung hunderter Datenfeeds über Open Source Software (IntelMQ, MISP)

„Die Welt steht auf kan‘ Fall mehr lang…“?

- Trotz erschreckender Meldungen ist die Lage nicht hoffnungslos
- Wir befinden uns in einem Gleichgewichtszustand zwischen Angriffen und Verteidigung – der aber kippen könnte
- Die tägliche Arbeit von tausenden Cyberexperten bewirkt, dass die Digitalisierung trotz Angriffen für uns nutzbar ist



Quelle: kpmg.at

560 Millionen Betroffene bei Hackerangriff auf Ticketmaster

1. Juni 2024, 12.43 Uhr

Quelle: orf.at

WIRTSCHAFT

"Erschreckend": Europas Industrie ist schlecht auf Cyberattacken vorbereitet

Quelle: kurier.at

NETZPOLITIK

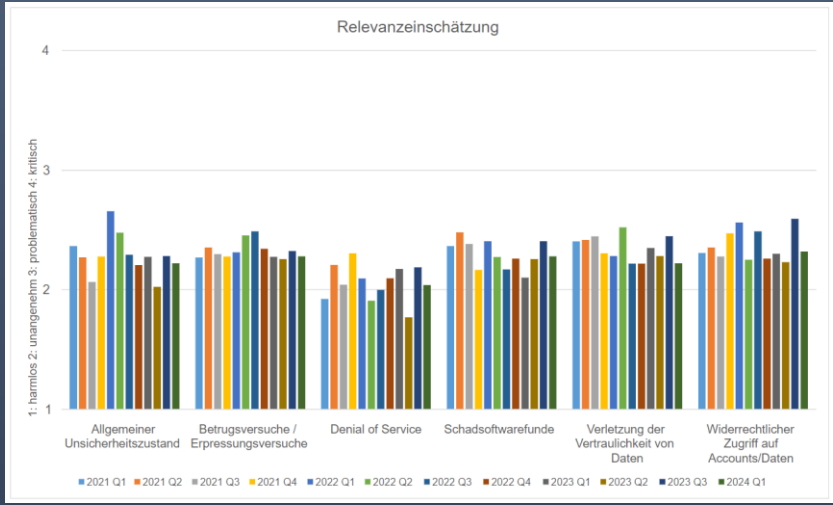
Behördenchefin: Deutschland auf Cyberangriffe schlecht vorbereitet

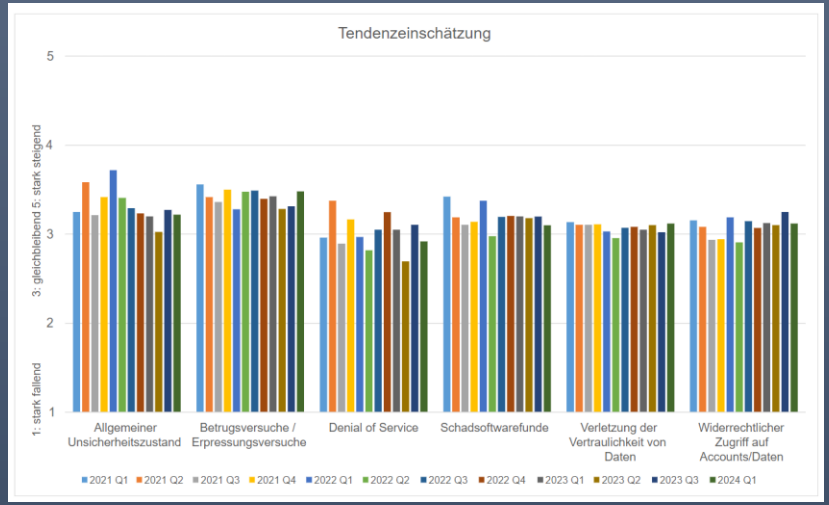
"Keine Koordination untereinander. Ein bundesweites Lagebild fehle somit

Quelle: derstandard.at

„Gleichbleibend unangenehm…“

Umfragen von CERT.at zeigen: die Cyber-lage ist seit Jahren unangenehm - aber für jene, die sich schützen, wird sie auch nicht schlimmer.

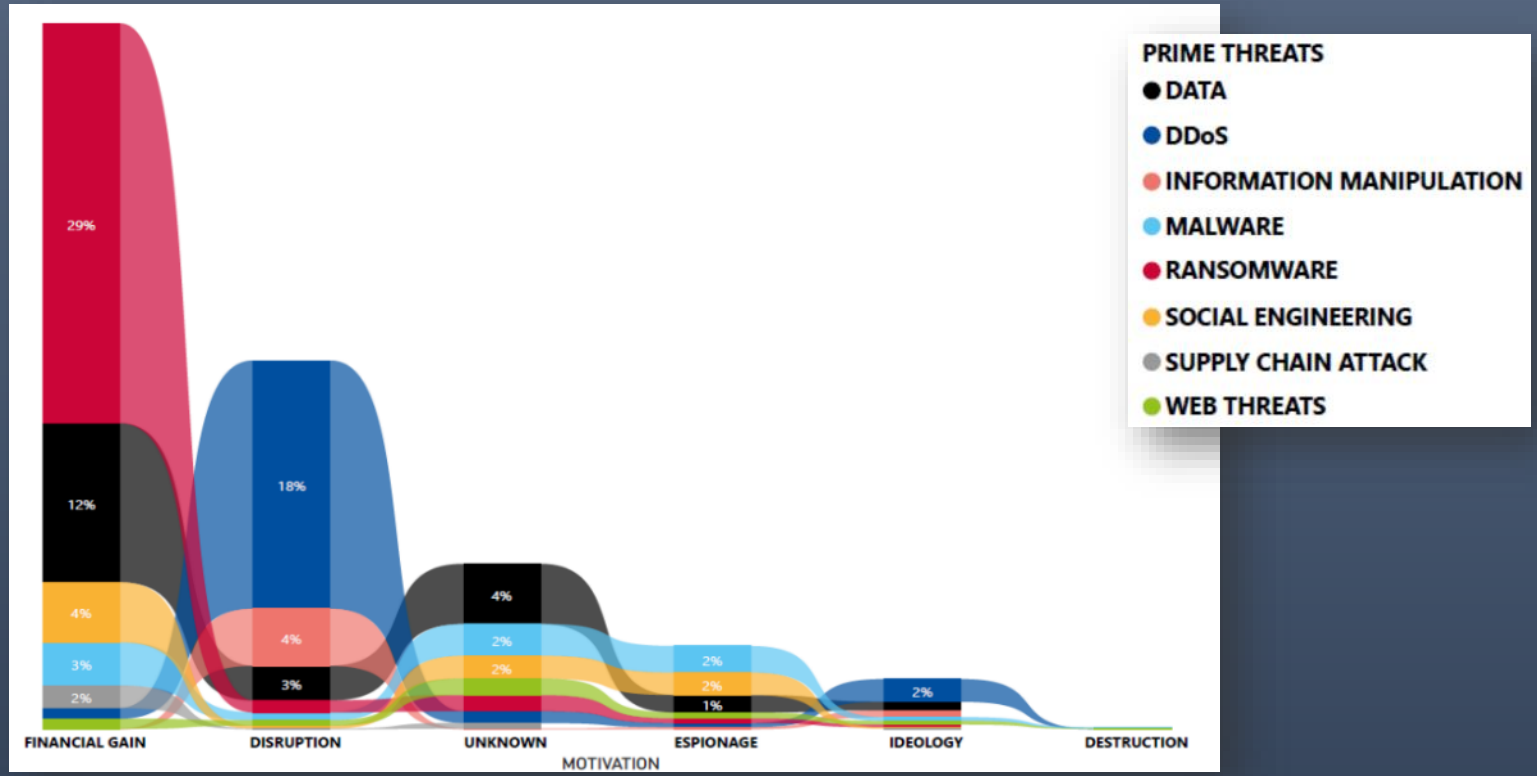




Warum wird die Lage aber auch nicht besser?
An der Informationslage kann es nicht liegen…

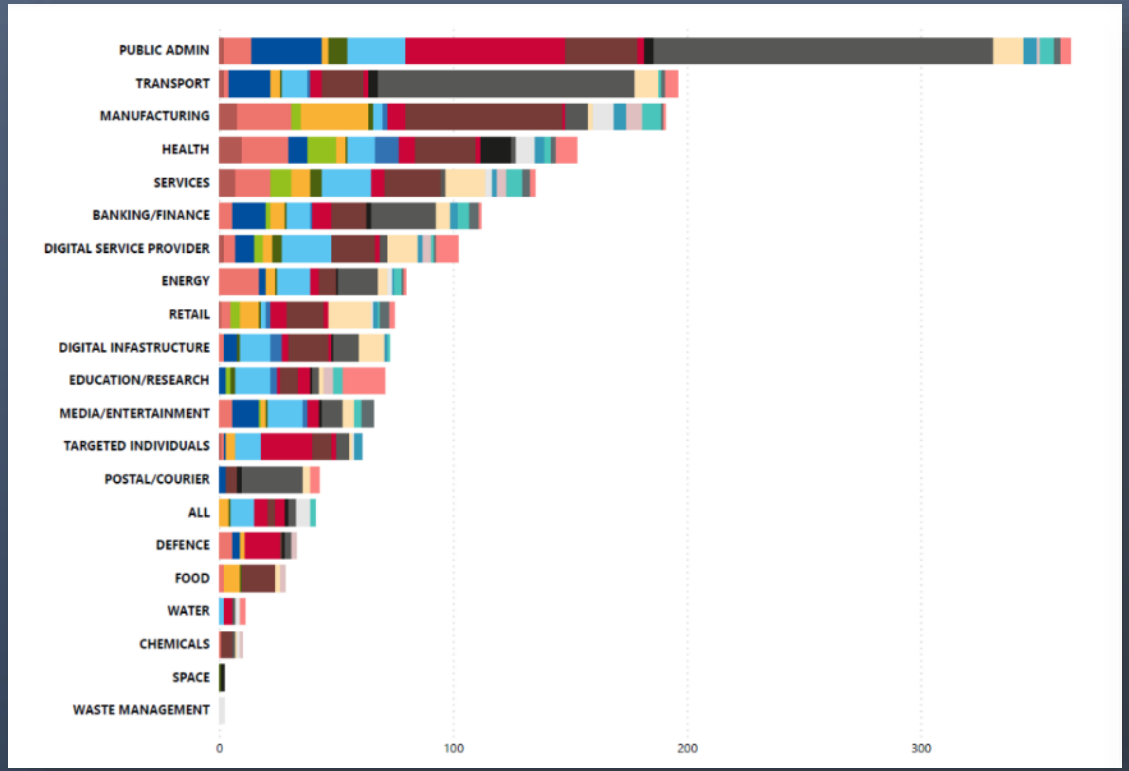
Quelle: cert.at

Wir wissen, warum sie angreifen…



Quelle: ENISA Threat Landscape 2023 - https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Wir wissen, wer uns angreift….

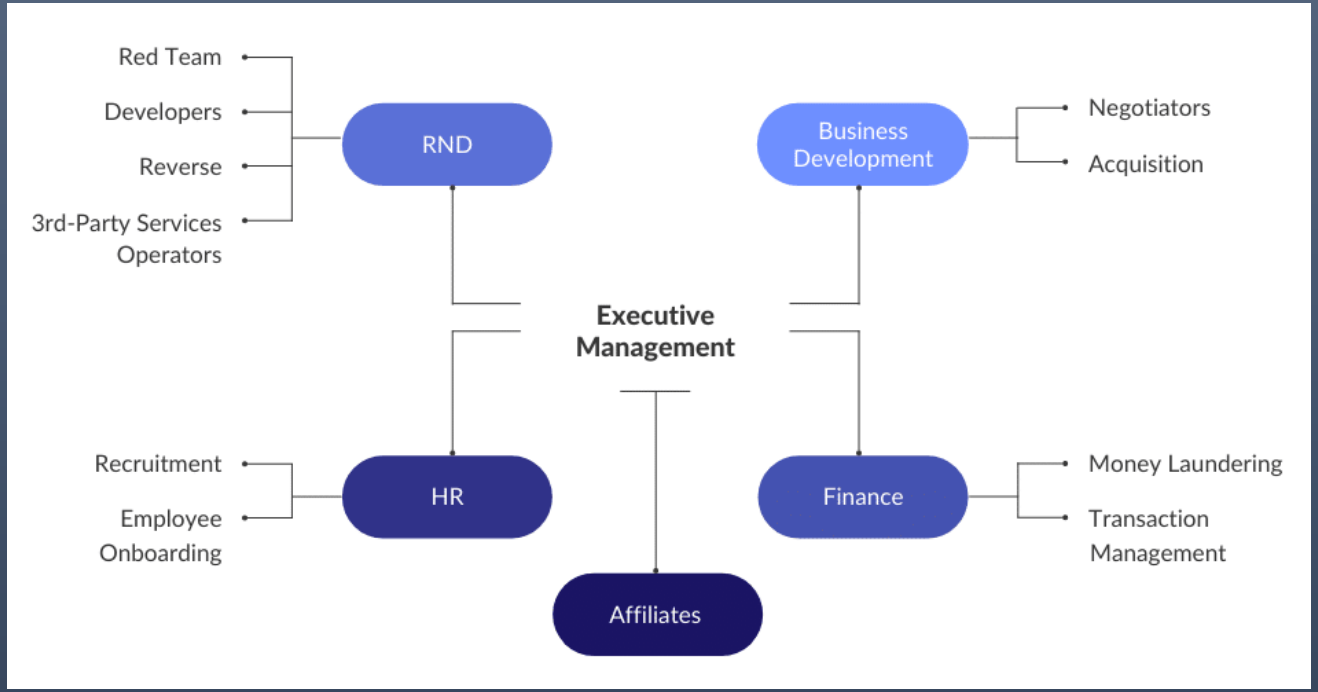


Quelle: ENISA Threat Landscape 2023 - https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Wir wissen, wer uns angreift….

Maksim Yakubets, Evil Corp
Quelle: https://www.thesun.co.uk/news/12237300/garmin-cyberattack-evil-corp-maksim-yakubets-playboy-lamborghini/

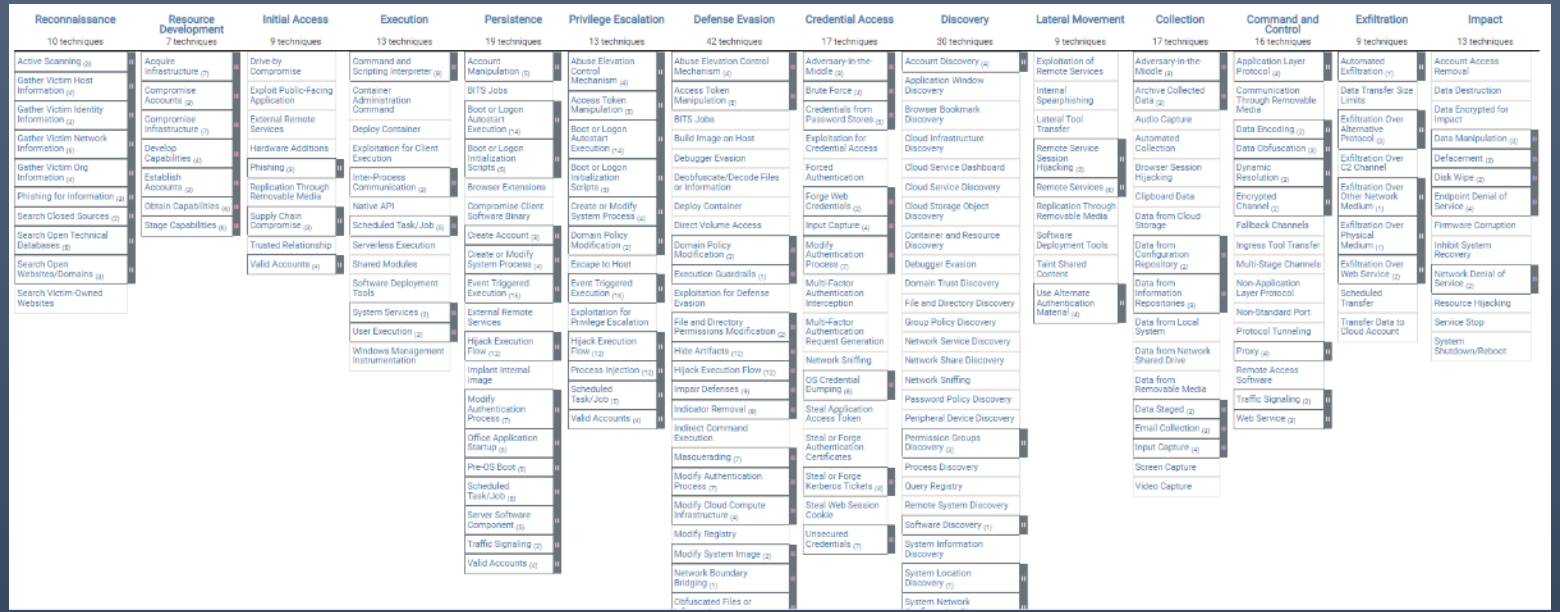
Wir wissen, wie sie arbeiten…



Quelle: https://cyberint.com/blog/research/contileaks/

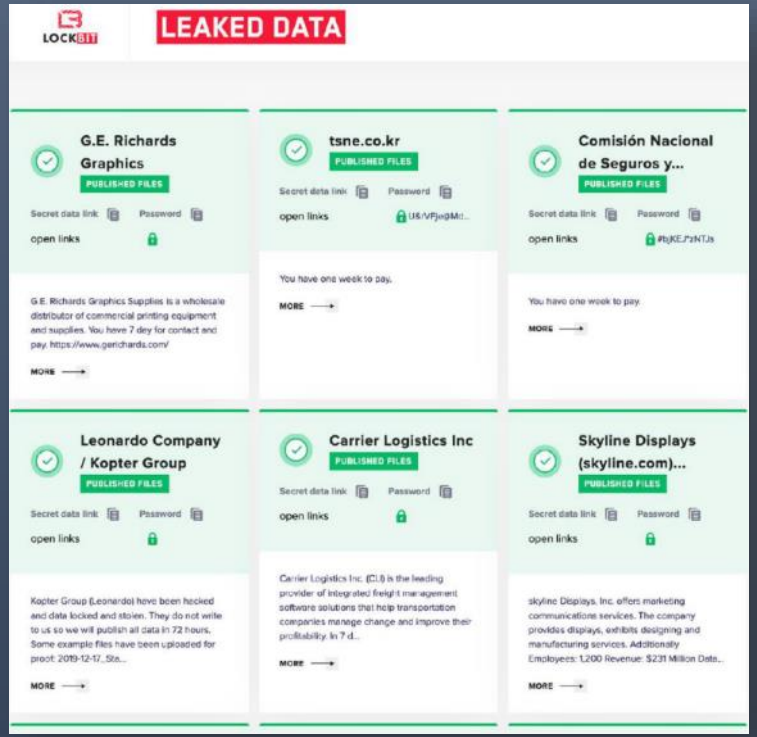
Wir wissen, wie sie angreifen….

MITRE ATT&CK Framework

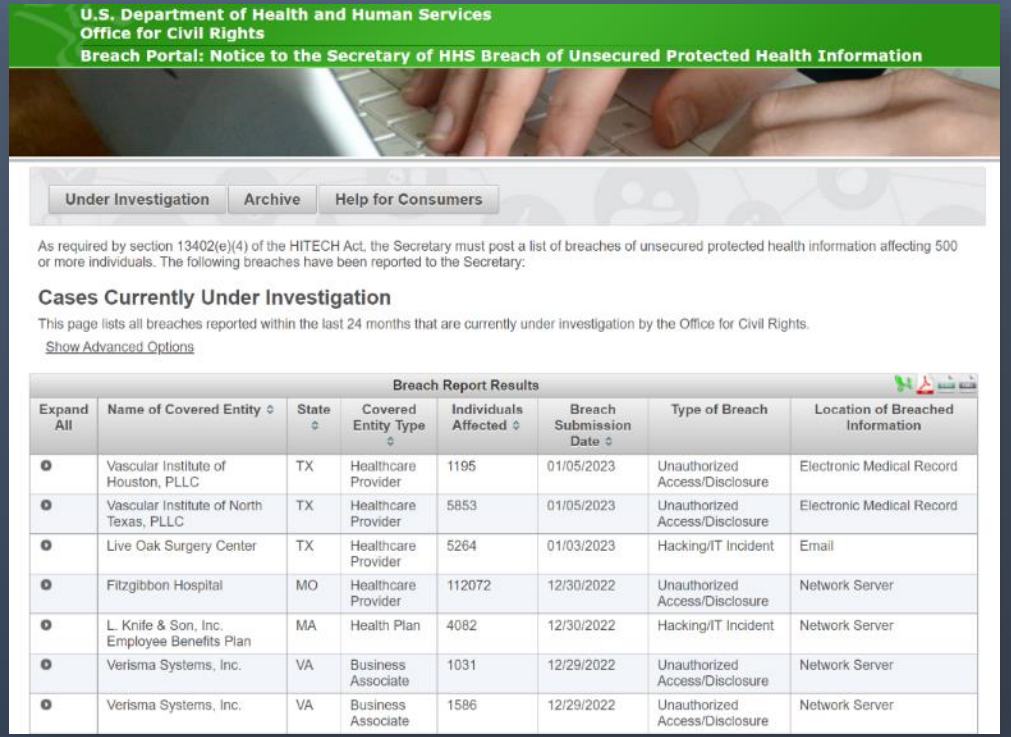


Quelle: attack.mitre.org

Wir wissen (oft), wen sie angreifen…

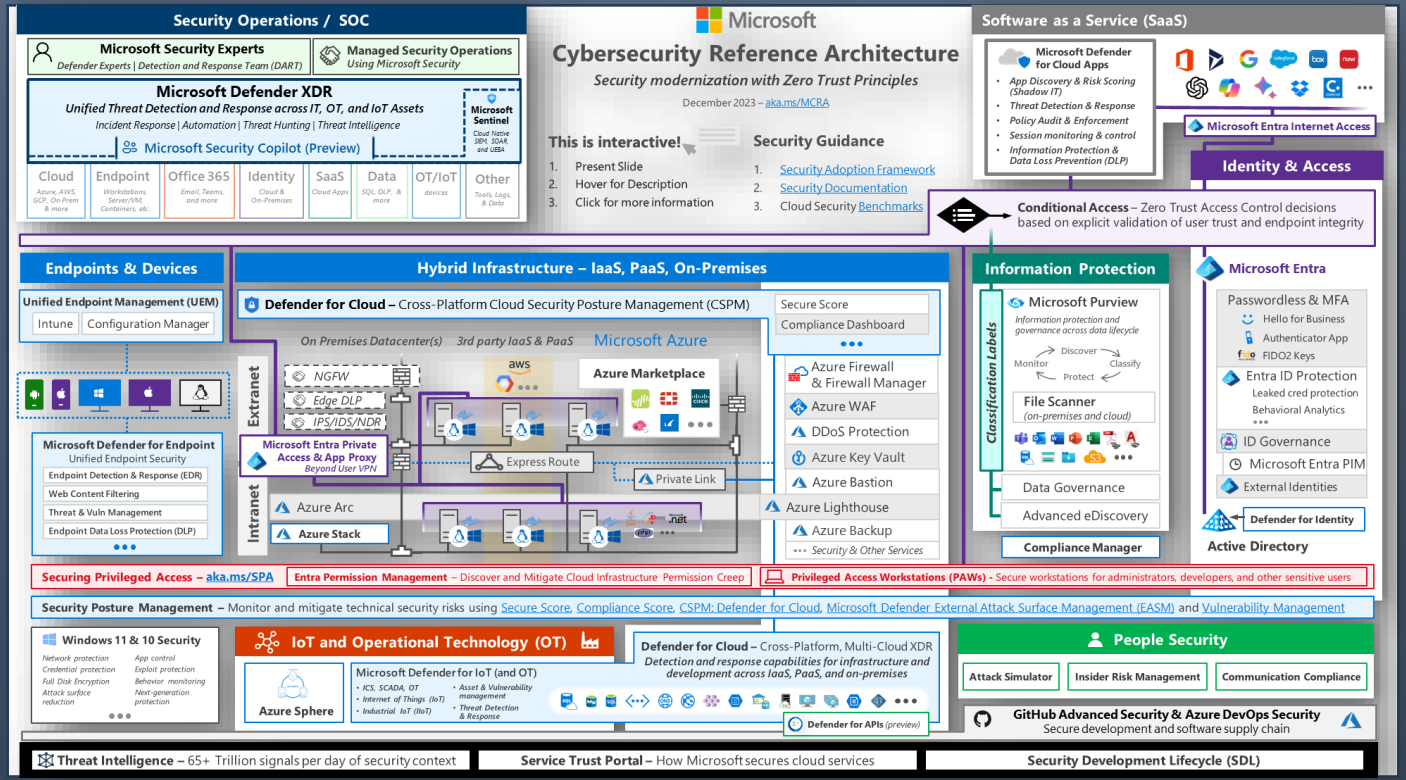


Quelle: Darknet



Quelle: ocrportal.hhs.gov/

Wir haben Schutzmaßnahmen…



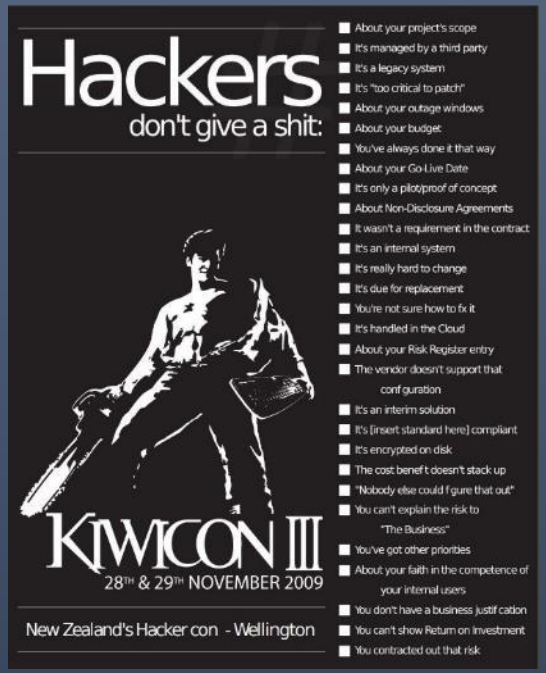
Quelle: Microsoft

Wir wissen, warum sie erfolgreich sind…

Weil sich nicht alle schützen – die Gründe dafür sind oft:

- „Ist dieses Jahr nicht im Budget“
- „Zu kritisch für ein Update“
- „Haben wir immer schon so gemacht“
- „Das schaffen wir jetzt nicht mehr vor dem Release“
- „Es ist ja nur ein Test, das drehen wir später wieder ab“
- „Es ist ja nur intern“
- „Der Lieferant unterstützt das nicht“
- „Das haben wir ausgelagert“

„Anständige Angreifer würden das berücksichtigen…“



Quelle: https://kiwicon.org/site_media/poster_shit.pdf

Cybersecurity wird erwachsen

The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554

Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)

- Risikobasierte Bewertung
- Drittdienstleister
- Meldewesen
- Detaillierte Vorgaben der Maßnahmen
- Audits
- Persönliche Verantwortung der Organisationsführung
- Strafen…

Es bleibt ein Expertenthema…

„Typische“ Aufstellung:

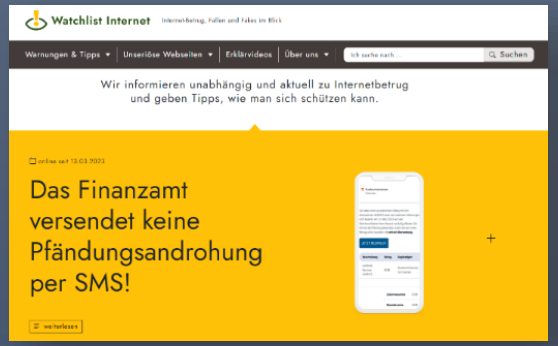
- Management: Chief Information Security Officer – CISO
- Prävention: Vulnerability und Patch-Management
- Test und Training: Red Teaming / Penetration Testing
- Alarmierung und First Line of Defence: Security Operations Center – SOC
- Reaktion auf Angriffe: Incident Response Teams (CERTs, CSIRTs, etc.)

…und…

- End User: auch die Anwender müssen das Thema verstehen… und zumindest in Teilbereichen zu Experten werden - aber warum?

Phishing & Social Engineering

- Die hohe Anzahl an Phishing- und anderen Betrugsfällen zeigt, dass der Mensch weiterhin ein Angriffsziel ist
- Aufklärung (Awareness) ist wesentlich, hat aber auch Grenzen, wie die Gartner-Studie zeigt
- Security-Professionals müssen weiters daran arbeiten, die Menschen aus der Angriffslinie zu nehmen – um sie zu schützen und damit wir nicht auf ihre Mitarbeit angewiesen sind



Quelle: watchlistinternet.at

> "Gartner research shows that over 90% of employees who admitted undertaking a range of unsecure actions during work activities knew that their actions would increase risk to the organization but did so anyway."

Quelle: gartner.com

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

Quelle: cnn.com

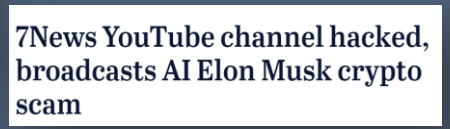
Desinformation durch Cyberangriffe

- Desinformation ist kein Cyberangriff – aber Cyberangriffe können für Desinformation verwendet werden
- Der Schutz vor Cyberangriffen auf Social Media Konten – z.B. durch 2-Faktor-Authentifizierung und starke Passwörter – ist nicht aufwändig und effektiv. Wird aber trotzdem oft vernachlässigt.

Second cabinet minister says Twitter account hacked

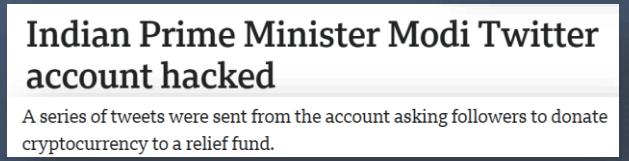
Northern Ireland secretary Chris Heaton-Harris apologises after account posts 'deeply unpleasant stuff'

Quelle:Guardian



7News YouTube channel hacked, broadcasts AI Elon Musk crypto scam

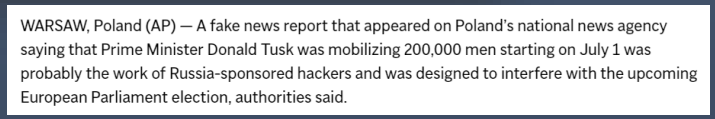
Quelle:Sidney Morning Herald



Indian Prime Minister Modi Twitter account hacked

A series of tweets were sent from the account asking followers to donate cryptocurrency to a relief fund.

Quelle:BBC



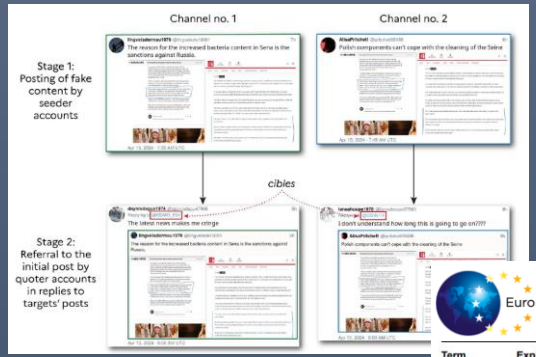
WARSAW, Poland (AP) — A fake news report that appeared on Poland's national news agency saying that Prime Minister Donald Tusk was mobilizing 200,000 men starting on July 1 was probably the work of Russia-sponsored hackers and was designed to interfere with the upcoming European Parliament election, authorities said.

Eight minutes later, the agency "killed," or removed, the report and then issued a statement saying that it wasn't the source of the article. The hack was repeated and the fake news was pushed again to the wire and was killed again.

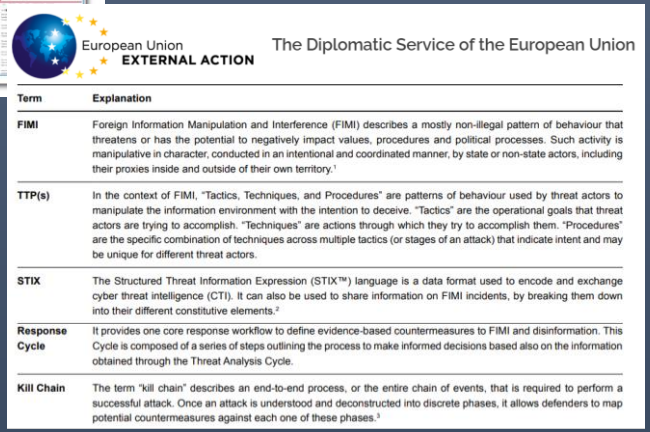
Quelle:Associated Press

Information über Desinformation

- Es gibt viele Organisationen, die Desinformationskampagnen analysieren und darüber aufklären
- Für die strukturierte Analyse und Information über diese Kampagnen werden etablierte Werkzeuge und Methoden aus der Cybersecurity verwendet



https://www.sgdsn.gouv.fr/publications/matriochka-une-campagne-prorusse-ciblant-les-medias-et-la-communaute-des-fact-checkers



European Union EXTERNAL ACTION — The Diplomatic Service of the European Union

Term	Explanation
FIMI	Foreign Information Manipulation and Interference (FIMI) describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner, by state or non-state actors, including their proxies inside and outside of their own territory.[1]
TTP(s)	In the context of FIMI, "Tactics, Techniques, and Procedures" are patterns of behaviour used by threat actors to manipulate the information environment with the intention to deceive. "Tactics" are the operational goals that threat actors are trying to accomplish. "Techniques" are actions through which they try to accomplish them. "Procedures" are the specific combination of techniques across multiple tactics (or stages of an attack) that indicate intent and may be unique for different threat actors.
STIX	The Structured Threat Information Expression (STIX™) language is a data format used to encode and exchange cyber threat intelligence (CTI). It can also be used to share information on FIMI incidents, by breaking them down into their different constitutive elements.[2]
Response Cycle	It provides one core response workflow to define evidence-based countermeasures to FIMI and disinformation. This Cycle is composed of a series of steps outlining the process to make informed decisions based also on the information obtained through the Threat Analysis Cycle.
Kill Chain	The term "kill chain" describes an end-to-end process, or the entire chain of events, that is required to perform a successful attack. Once an attack is understood and deconstructed into discrete phases, it allows defenders to map potential countermeasures against each one of these phases.[3]

https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf

Trust and Safety-Teams

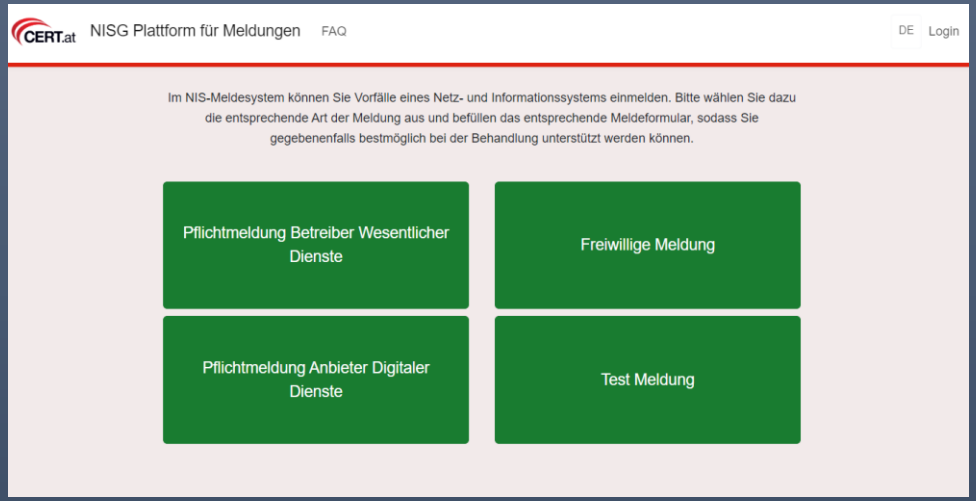
- Ursprünglich aus der „content moderation“ entstanden
  - Stärken des Vertrauens in eine Plattform, wenn diese Plattform gepflegt und von Gefahren freigehalten wird
  - Erstellung von Policies, Guidelines und aktives Eingreifen
- Partner oder sogar Auftraggeber der Cybersecurity
  - Einbruchsschutz/erkennung
  - Fraud detection
  - Innovationstreiber (Digital Wallets, Kryptografie, Multi-Faktor-Authentifizierung, etc.)
  - Awareness schaffen (z.B. Kommunikation der Warnungen und Tipps von Watchlist-Internet, CERT.at, etc)

Cyberhygiene

- Bewusstsein schaffen – Cybersecurity ist kein „Expertenproblem“
- Vertrauen ist gut, Kontrolle ist besser – „Assume breach“
- Resilienz ist „4-R“:
  - Resistance – Widerstand gegen Angriffe (Virenscanner, Endpoint-Detection and Response – EDR, SOC)
  - Retention – während eines Angriffes arbeiten können (Ausweich-IT)
  - Recovery – Wiederherstellung des Kernbetriebes (Backups, Ersatzinfrastruktur, **Verträge mit Security Dienstleistern**!)
  - Resurgence – stärker und schlauer aus dem Angriff hervorgehen („Fool me once, shame on you – fool me twice, shame on me…“)

NIS-Meldeplattform

- Cyberangriffe können von jeder Organisation als freiwillige NIS-Meldung über die Website von CERT.at (https://nis.cert.at/) gemeldet werden
- Sie helfen uns damit, ein vollständigeres Lagebild zu erzeugen
- Zusätzlich sollten Cyberangriffe der Polizei und – falls personenbezogene Daten betroffen sind – der Datenschutzbehörde gemeldet werden



Quelle: CERT.at

Kontakt

Wolfgang Rosenkranz
<rosenkranz@cert.at>

Nationales Computernotfallteam - CERT.at GmbH
Web: https://**www.cert.at**
eMail: **team@cert.at** & **reports@cert.at**
+43 1 5056416 715