

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

Jeder **6.** Cyberangriff gegen ein Unternehmen war erfolgreich.

Jedes **3.** Unternehmen hat zumindest einmal die Lösegeldforderung im Zusammenhang mit einem Ransomwareangriff bezahlt.

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

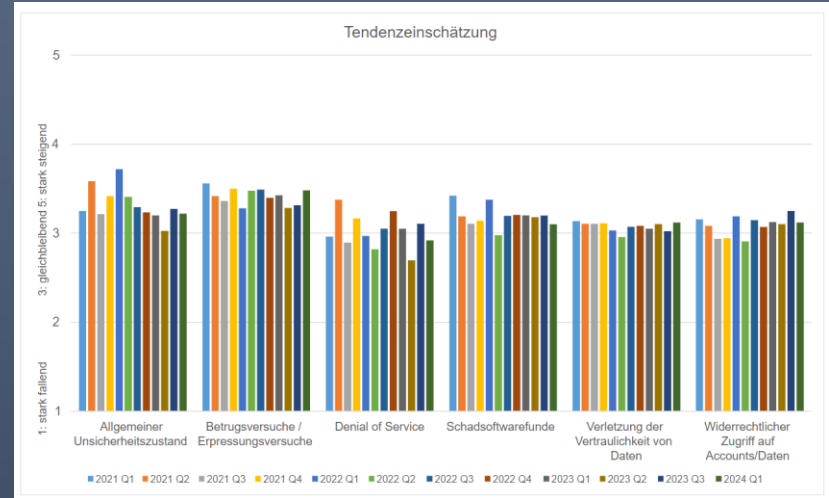
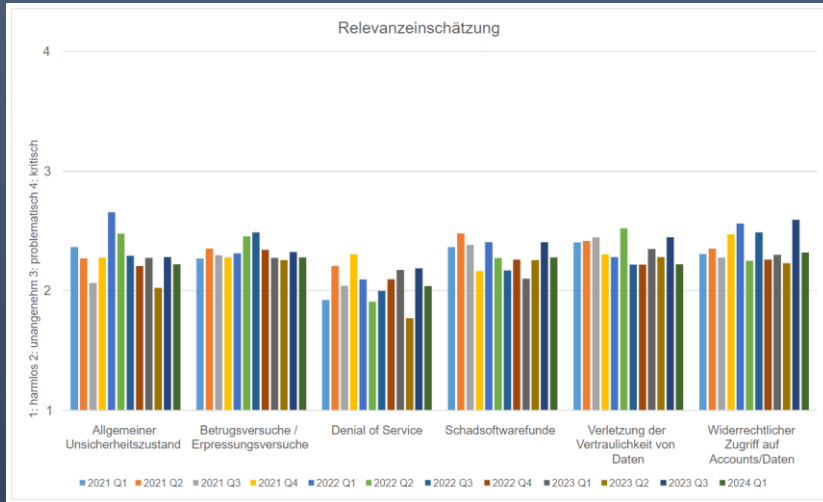
Behördenchefin: Deutschland auf Cyberangriffe schlecht vorbereitet

"Keine Koordination untereinander. Ein bundesweites Lagebild fehle somit

Quelle: derstandard.at

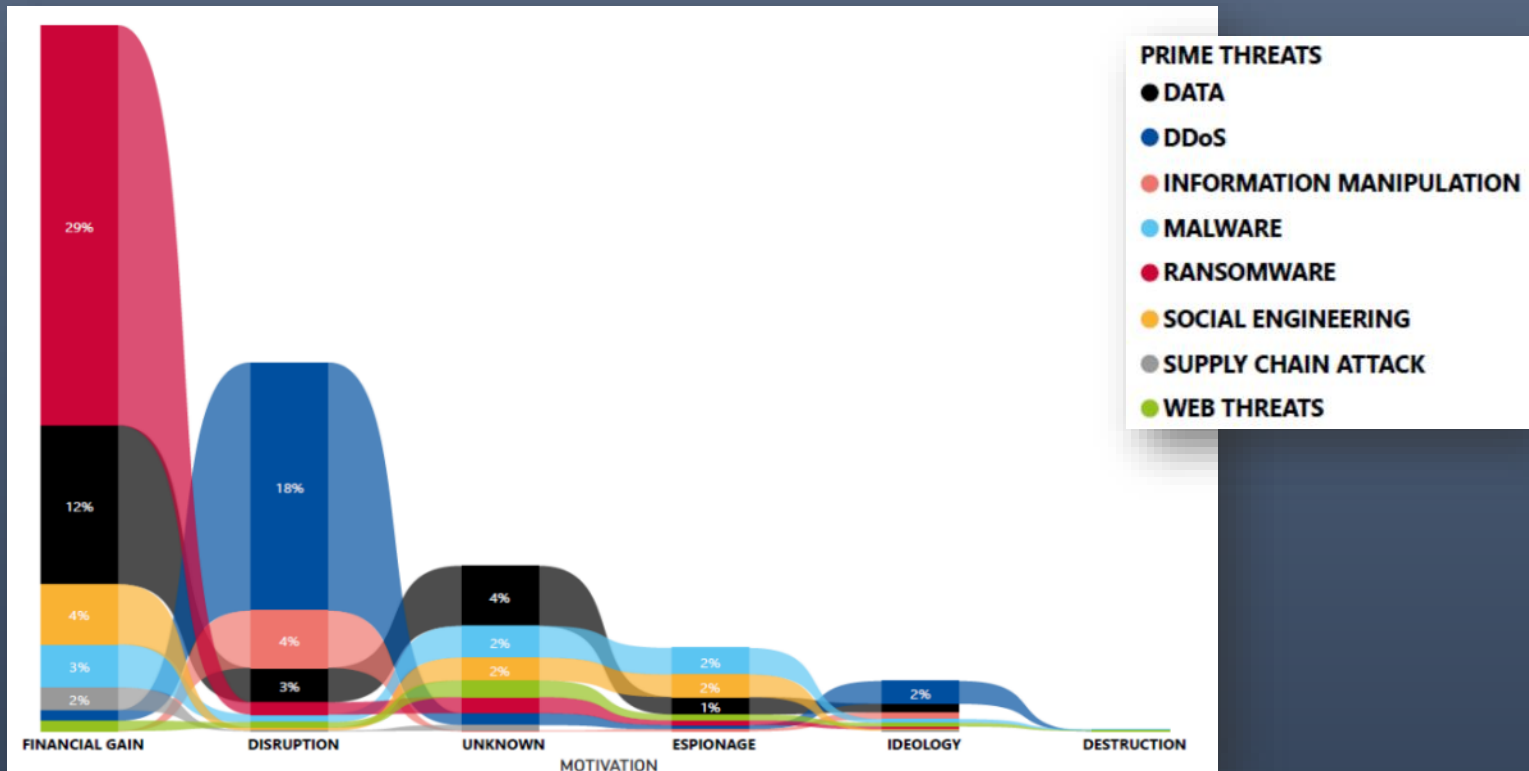
„Gleichbleibend unangenehm...“

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



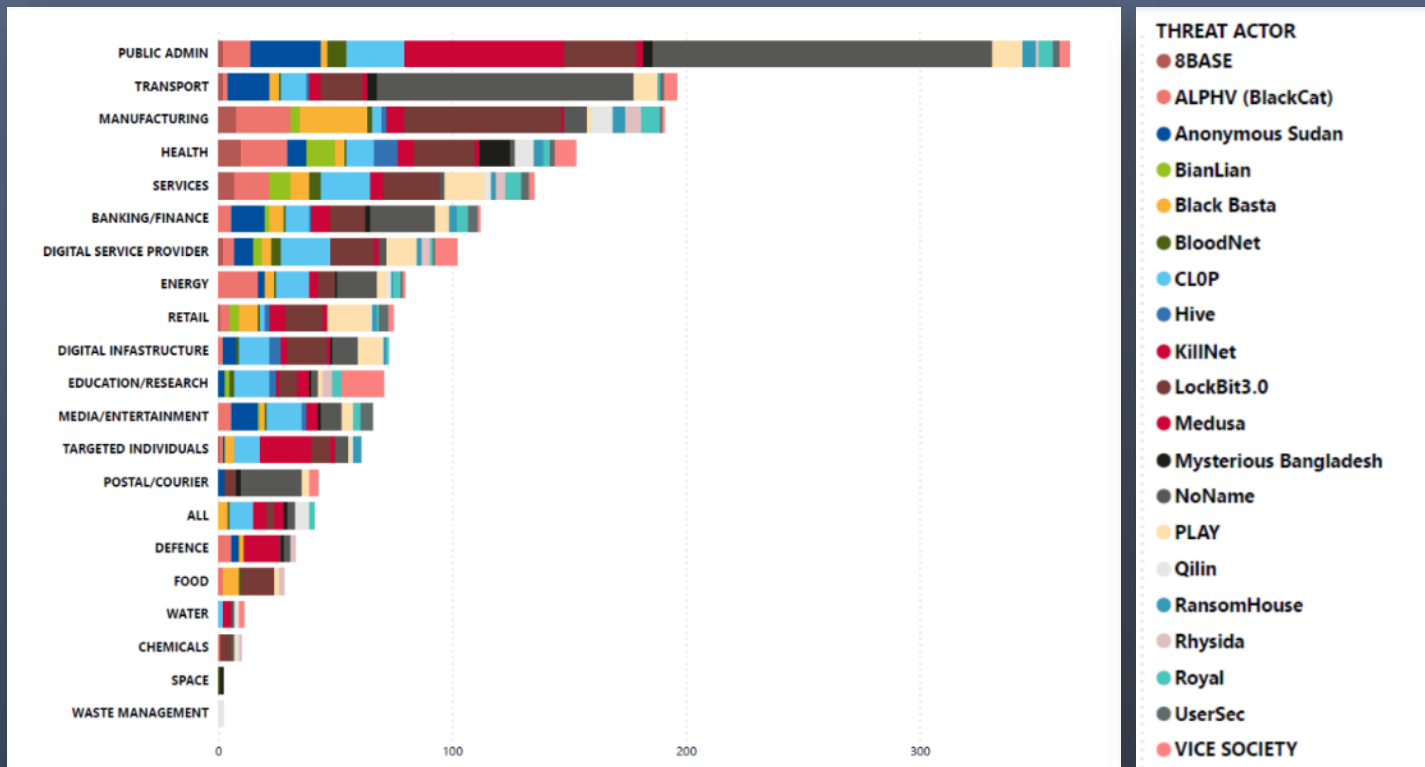
Warum wird die Lage aber auch nicht besser?
An der Informationslage kann es nicht liegen...

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>

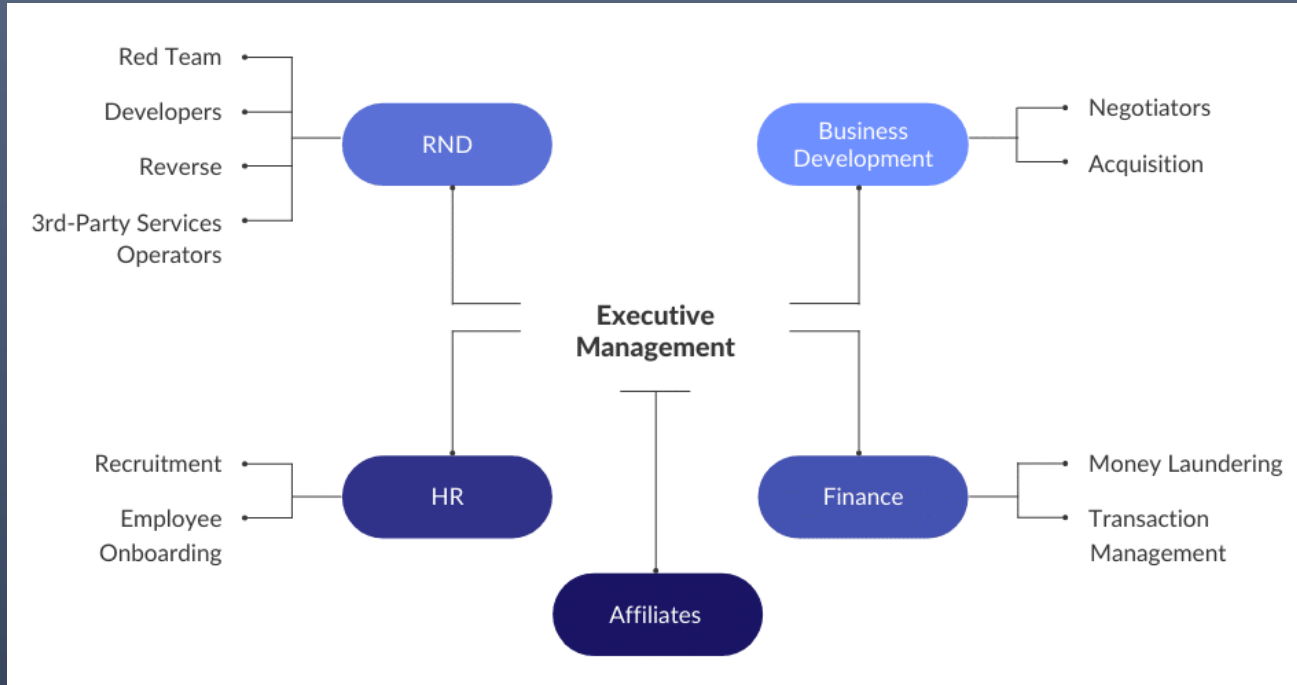
Wir wissen, wer uns angreift....



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/>

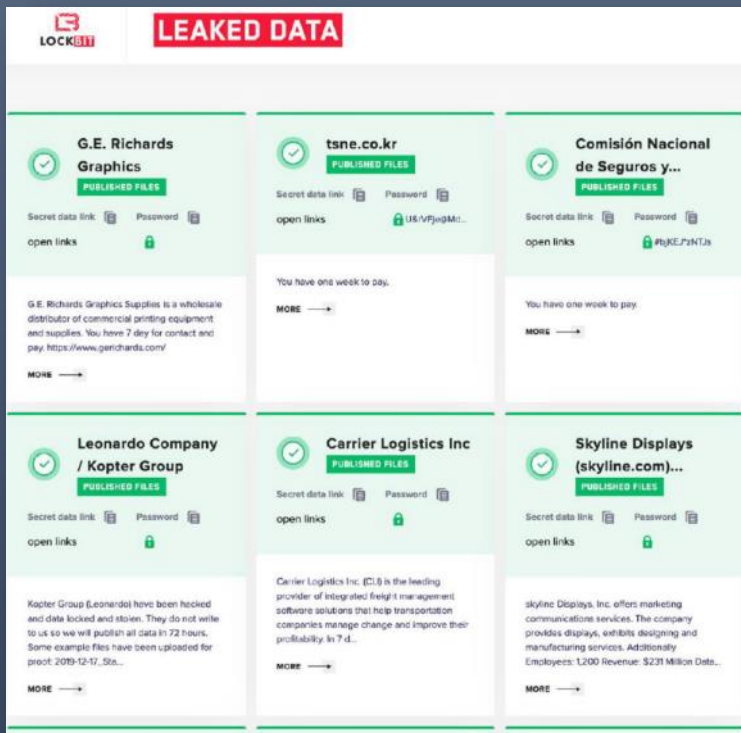
Wir wissen, wie sie angreifen....

MITRE ATT&CK Framework

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (7)	Drive-by Compromise	Command and Scripting Interpreter (4)	Account Manipulation (7)	Abuse Elevation Control Mechanism (2)	Abuse Elevation Control Mechanism (2)	Adversary in-the-Middle (2)	Account Discovery (2)	Exploitation of Remote Services	Adversary in-the-Middle (2)	Application Layer Protocol (2)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (2)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (2)	Access Token Manipulation (2)	Brute Force (2)	Application Window Discovery	Internal Spearphishing	Active Collected Data (2)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (2)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Assistant Execution (1-4)	Boot or Logon Assistant Execution (2)	Boot or Logon Assistant Execution (2)	Credentials from Password Stores (2)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (2)	Data Encrypted for Impact
Gather Victim Network Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (2)	Boot or Logon Initialization Scripts (2)	Built Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (2)	Exfiltration Over OS Channel	Data Manipulation (2)
Gather Victim Org Information (2)	Establish Accounts (2)	Phishing (2)	Inter-Process Communication (2)	Browser Extensions	Debugger Evasion	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Service(s) (2)	Browser Session Hijacking	Dynamic Resolution (2)	Exfiltration Over Other Network Medium (2)	Defacement (2)
Phishing for Information (2)	Obtain Capabilities (4)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Deobfuscate/Decode Files or Information	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (4)	Supply Chain Compromise (2)	Scheduled Task/Job (2)	Create or Modify System Process (2)	Deploy Container	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Endpoint Denial of Service (2)
Search Open Technical Databases (2)	Trusted Relationship	Valid Accounts (2)	Shared Modules	Domain Policy Modification (2)	Create or Modify System Process (2)	Domain Policy Modification (2)	Modify Authentication Process (2)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Exfiltration Over Physical Medium (1)	Firmware Corruption
Search Open Websites/Domains (2)	Valid Accounts (2)		Software Deployment Tools	Event Triggered Execution (2)	Event Triggered Execution (2)	Event Triggered Execution (2)	Multi-Factor Authentication Request Generation	Debugger Evasion	Use Alternate Authentication Material (2)	Data from Information Repositories (2)	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Inhibit System Recovery
Search Victim-Owned Websites			System Services (2)	External Remote Services	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Multi-Stage Channels	Network Denial of Service (2)	Resource Hijacking
			User Execution (2)	Hijack Execution Flow (1-2)	Hijack Execution Flow (1-2)	Hijack Execution Flow (1-2)	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Application Layer Protocol	Scheduled Transfer to Cloud Account	Service Stop
			Windows Management Instrumentation	Implant Internal Image	Process Injection (1-2)	Process Injection (1-2)	Network Sniffing	File and Directory Discovery		Data from Removable Media	Non-Standard Port	Scheduled Transfer to Cloud Account	System Shutdown/Reboot
				Modify Authentication Process (2)	Scheduled Task/Job (2)	Scheduled Task/Job (2)	Network Sniffing	Group Policy Discovery		Data Staged (2)	Protocol Tunneling	Transfer Data to Cloud Account	
				Office Application Startup (2)	Valid Accounts (4)	Valid Accounts (4)	Network Sniffing	Network Service Discovery		Email Collection (2)	Proxy (4)		
				Pre-OS Boot (2)			Network Sniffing	Network Share Discovery		Input Capture (2)	Remote Access Software		
				Scheduled Task/Job (2)			Network Sniffing	Network Sniffing		Screen Capture	Traffic Signaling (2)		
				Server Software Component (2)			OS Credential Dumping (4)	Network Sniffing		Video Capture	Web Service (2)		
				Traffic Signaling (2)			Indicator Removal (2)	Password Policy Discovery					
				Valid Accounts (4)			Inhibit Command Execution	Peripheral Device Discovery					
							Masquerading (2)	Permission Groups Discovery (2)					
							Modify Authentication Process (2)	Process Discovery					
							Steal or Forge Web browser Cookies (4)	Query Registry					
							Modify Cloud Compute Infrastructure (2)	Remote System Discovery					
							Modify Registry	Software Discovery (2)					
							Modify System Image (2)	System Information Discovery					
							Network Boundary Bridging (2)	System Location Discovery (2)					
							Deobfuscated Files or Information	System Network					

Quelle: attack.mitre.org

Wir wissen (oft), wen sie angreifen...



LOCKBIT **LEAKED DATA**

G.E. Richards Graphics PUBLISHED FILES
Secret data link Password
open links

tsne.co.kr PUBLISHED FILES
Secret data link Password
open links

Comisión Nacional de Seguros y... PUBLISHED FILES
Secret data link Password
open links

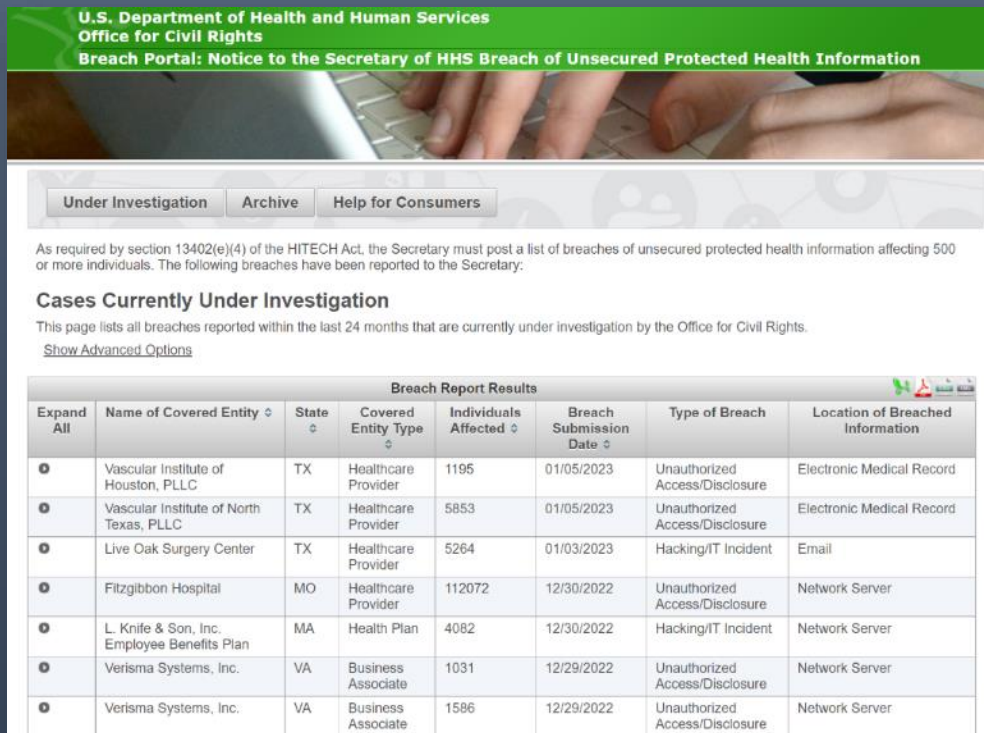
Leonardo Company / Kopter Group PUBLISHED FILES
Secret data link Password
open links

Carrier Logistics Inc PUBLISHED FILES
Secret data link Password
open links

Skyline Displays (skyline.com)... PUBLISHED FILES
Secret data link Password
open links

Quelle: Darknet

02.09.2024



**U.S. Department of Health and Human Services
Office for Civil Rights
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information**

Under Investigation Archive Help for Consumers

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. The following breaches have been reported to the Secretary.

Cases Currently Under Investigation

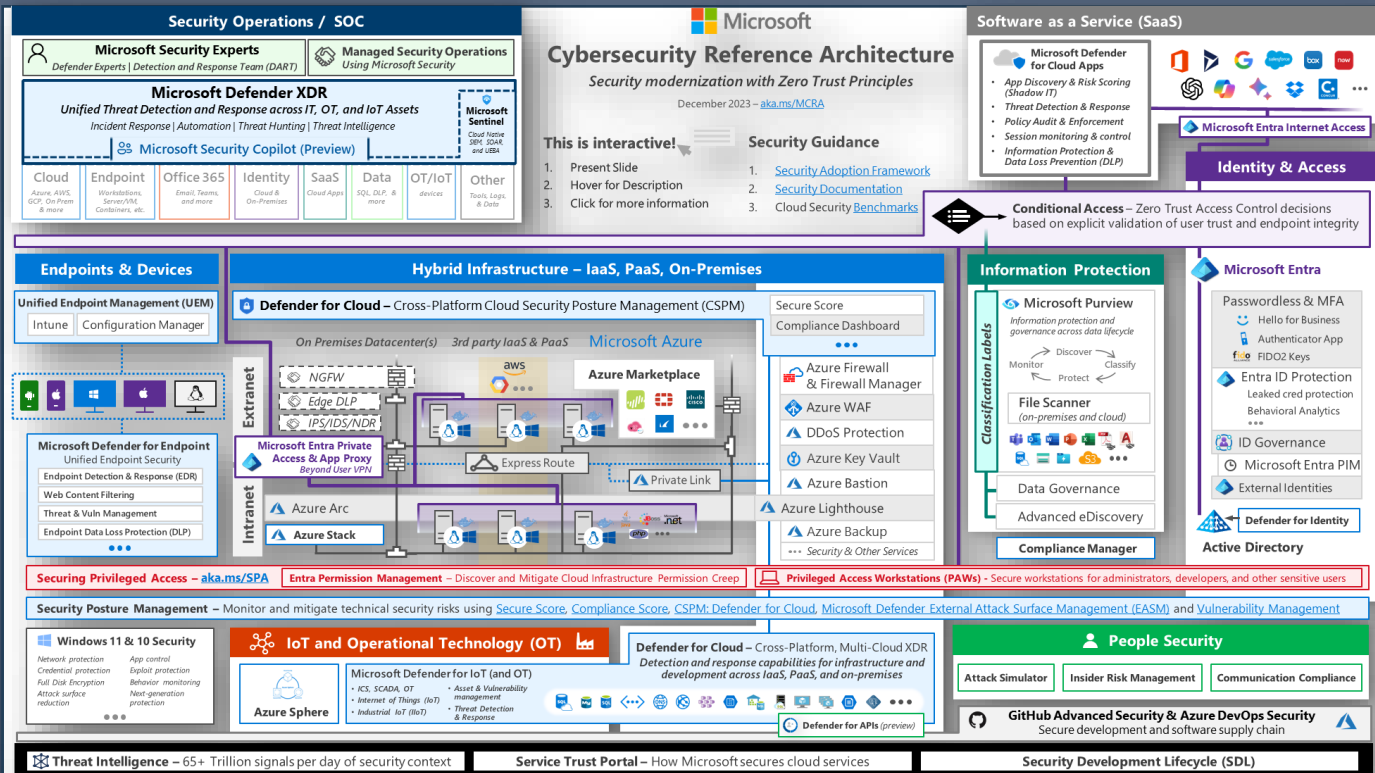
This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

[Show Advanced Options](#)

Breach Report Results							
Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
+	Vascular Institute of Houston, PLLC	TX	Healthcare Provider	1195	01/05/2023	Unauthorized Access/Disclosure	Electronic Medical Record
+	Vascular Institute of North Texas, PLLC	TX	Healthcare Provider	5853	01/05/2023	Unauthorized Access/Disclosure	Electronic Medical Record
+	Live Oak Surgery Center	TX	Healthcare Provider	5264	01/03/2023	Hacking/IT Incident	Email
+	Fitzgibbon Hospital	MO	Healthcare Provider	112072	12/30/2022	Unauthorized Access/Disclosure	Network Server
+	L. Knife & Son, Inc. Employee Benefits Plan	MA	Health Plan	4082	12/30/2022	Hacking/IT Incident	Network Server
+	Verisma Systems, Inc.	VA	Business Associate	1031	12/29/2022	Unauthorized Access/Disclosure	Network Server
+	Verisma Systems, Inc.	VA	Business Associate	1586	12/29/2022	Unauthorized Access/Disclosure	Network Server

Quelle: ocrportal.hhs.gov/

Wir haben Schutzmaßnahmen...



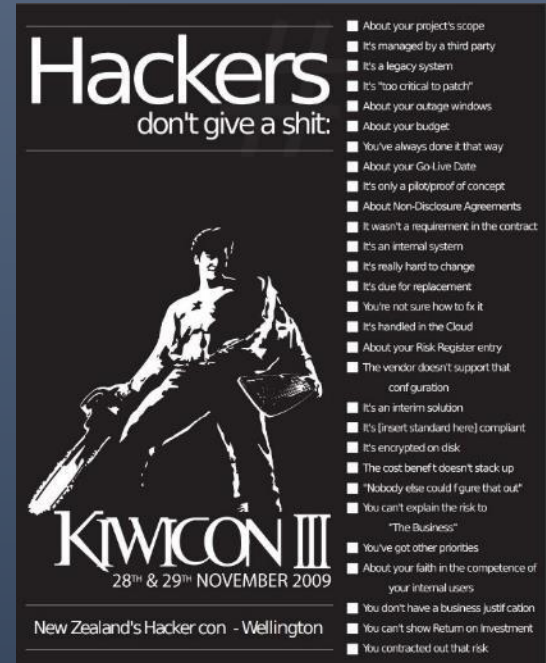
Quelle: Microsoft

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

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

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

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

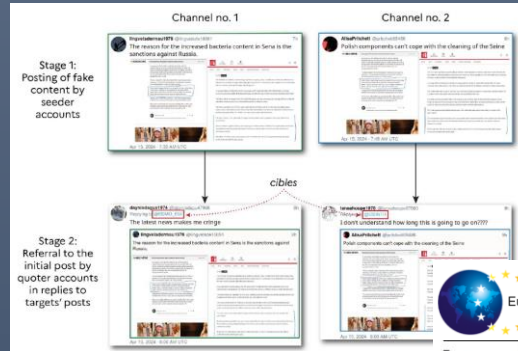
WARSAW, Poland (AP) — A fake news report that appeared on Poland's national news agency saying that Prime Minister Donald Tusk was mobilizing 200,000 men starting on July 1 was probably the work of Russia-sponsored hackers and was designed to interfere with the upcoming European Parliament election,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

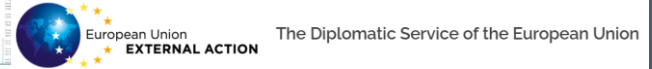
Quelle:Associated Press

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.gov.fr/publications/matrioch-ka-une-campagne-prorusse-ciblante-les-medias-et-la-communaute-des-fact-checkers>



Term	Explanation
FIMI	Foreign Information Manipulation and Interference (FIMI) describes a mostly non-legal 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

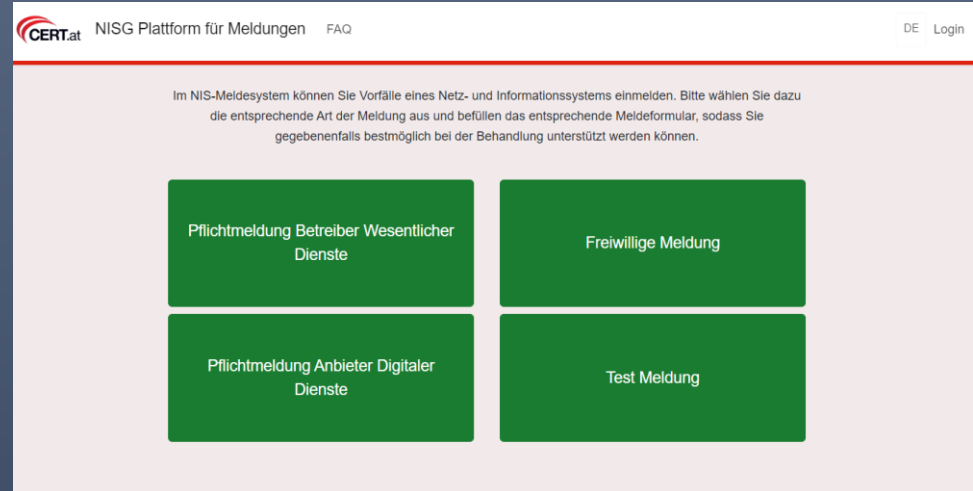
- Ursprünglich aus der „content moderation“ entstanden
 - Stärken des Vertrauens in eine Plattform, wenn diese Plattform gepflegt und von Gefahren freigehalten wird
 - Erstellung von Policies, Guidelines und aktives Eingreifen
- Partner oder sogar Auftraggeber der Cybersecurity
 - Einbruchsschutz/erkennung
 - 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 (Virens Scanner, 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