Cyber Security Incident Management

ISPA Academy

Linz, 25. November 2024

Wolfgang Rosenkranz <rosenkranz@cert.at>

Incident Management @ CERT.at

- Beispielszenario: Ransomware beim Dienstleister
  - Kontakt zu einer Organisation, deren Dienstleister Ransomware an seine Kunden weiterverteilt hat
  - Aus Chats war ableitbar, dass jemand für den Dienstleister mit den Angreifern verhandelt – aber wer?
  - Ein CERT-Partner aus einem anderen EU-Land meldet sich bei CERT.at – ein Verhandlungsdienstleister will den Fall übergeben, der Kreis schließt sich

- Conclusio: Vernetzung als wichtigste Form der Incident Response

CERT.at

- 2008 als gemeinnütziges Projekt von nic.at gegründet und über die IPA finanziert
- Offizielles „nationales Computernotfallteam“ nach NIS-Gesetz
- 90 % Informationsdrehscheibe, 10% Incident Responder
  - Austrian Trust Circle, CERT-Verbund, CERT-Stammtisch
  - Kontaktstelle für internationale CERTs & CSIRTs
  - Newsletter, Discussion Groups, Blogs
  - Verteilung hunderter Datenfeeds über Open Source Software (IntelMQ, MISP)
- Betrieb des Austrian Energy CERT und technischer Betrieb des GovCERT

Nationale und internationale Kooperation

- Austrian Trust Circle (ATC)
- CERT-Verbund
- Cyber Sicherheit Plattform des Bundes
- FIRST – Global Forum of Incident Response and Security Teams
- TF-CSIRT – Task Force on Computer Security Incident Response Teams
- CNW - European Union CSIRT Network
- CECSP – Central European Cyber Security Platform
- TI – Trusted Introducer Organisation
- EGC – European GovCERTs
- FI-ISAC – European Financial Institutes Information Sharing and Analysis

TARGETING AUTHORITIES

Hacker attacks: are we already in a digital war?

Nachrichten | 21.11.2024 06:00

Nobody knows who they are. But hackers have Austria specifically in their sights. (Bild: Mohamad Zaki - stock.adobe.com)

oe24 POLITIK-LIVE

PARTEIEN AFFÄREN REGIERUNG MEINUNGEN

SONDERTHEMA: GLÜCKSMOMENTE XXXLUTZ UNSERE TIERE ADMIRAL SPORTWETTEN KARRIEREDAY SK

Inland > Politik > Affären

© Getty

CYBER-KRIEG

Hacker legen halbe Republik lahm

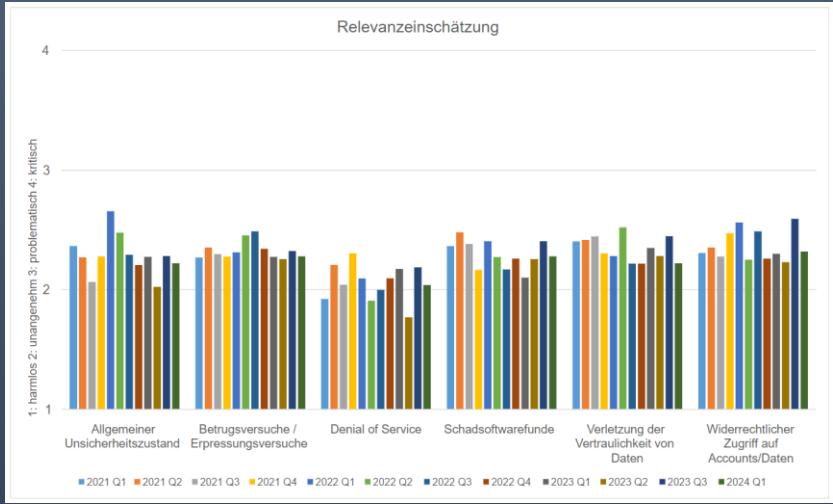
NoName057(16) – DDoSia Projekt

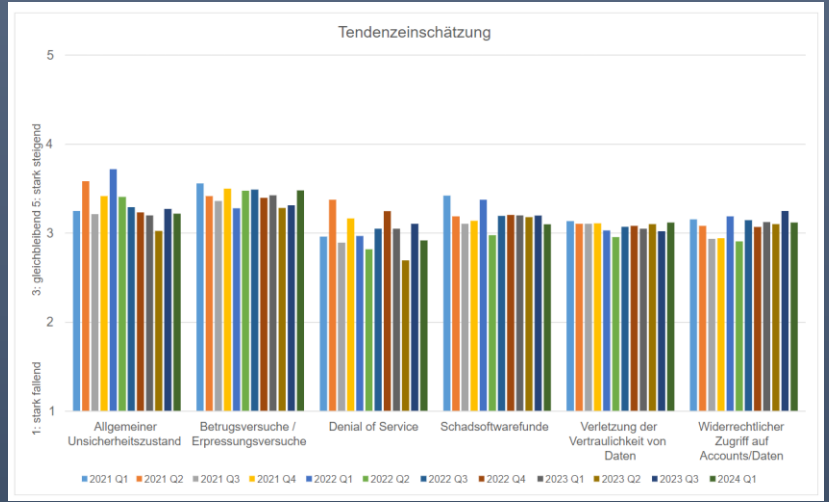
- Crowdsource Projekt
- Aktuelle Zielliste unter: https://witha.name/data/ abrufbar
- Stellen sich selbst als Rächer für Anti-Russland Aktionen dar
- Laufende Weiterentwicklungen (zB. Go statt Python, etc.)

personenverkehr.oebb.at	195.69.192.144
sempal.com	185.65.244.234
shop.wienmobil.at	193.178.171.28
ticket.datapark.ua	77.88.199.105
tucha.ua	193.151.89.67
uss.gov.ua	213.156.91.88
webapi.vor.at	94.247.144.241
www.a1.group	80.75.40.8
www.arsenalcdb.com.ua	62.244.26.170
www.brz.gv.at	194.37.73.140
www.cert.at	131.130.249.233

„Gleichbleibend unangenehm…“

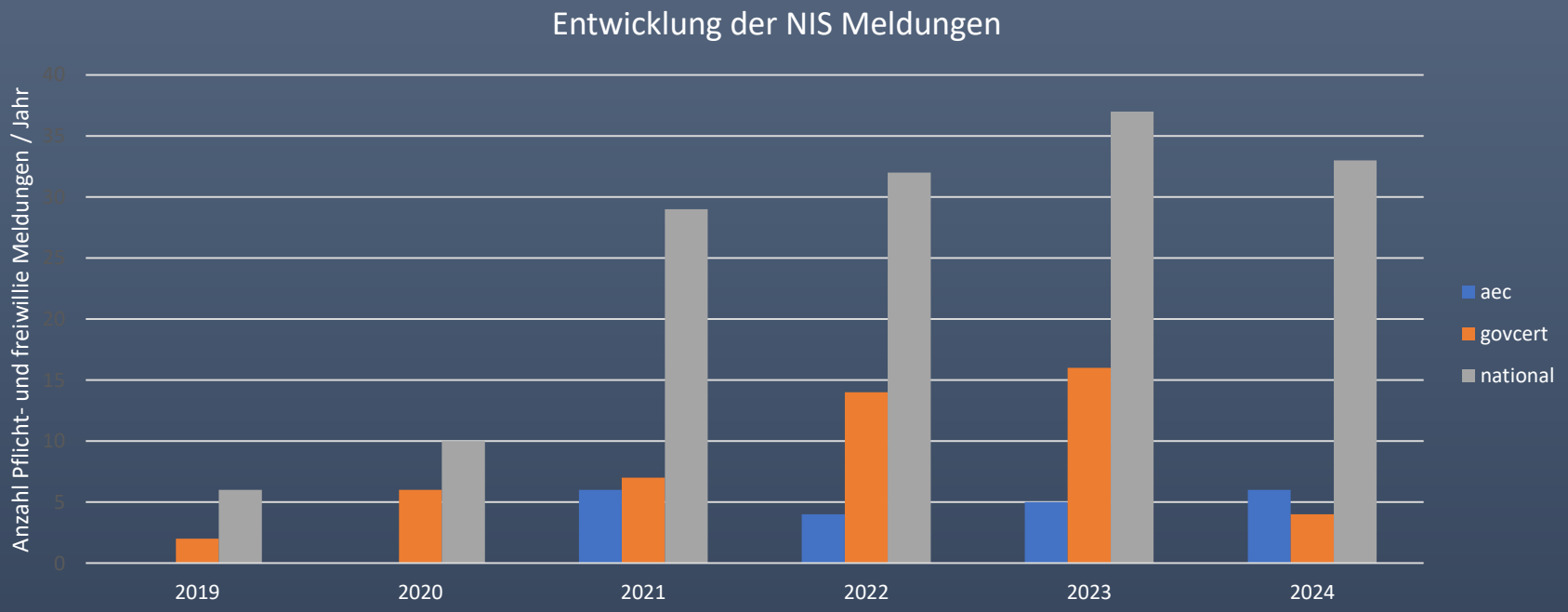
Umfragen von CERT.at zeigen: die Cyber-lage ist seit Jahren unangenehm - aber für jene, die sich schützen, wird sie auch nicht schlimmer.



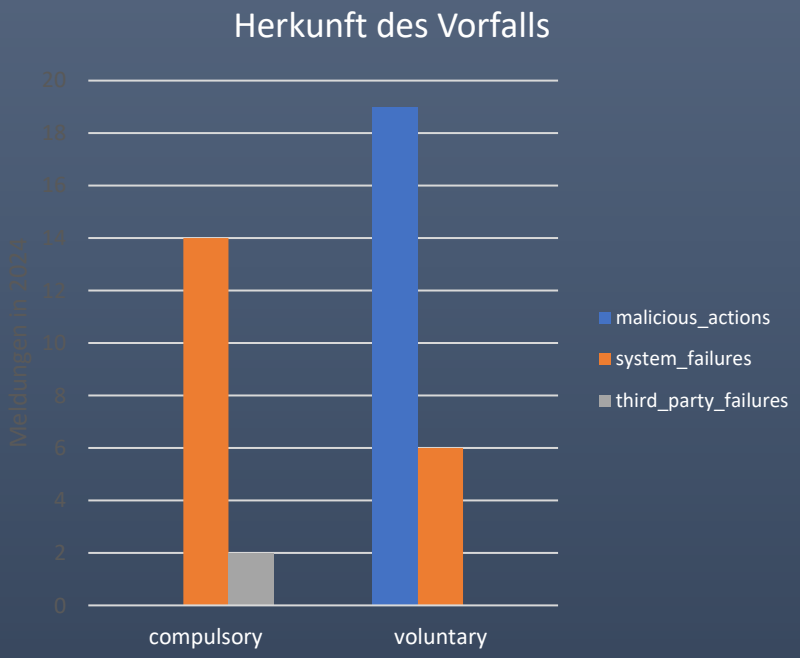


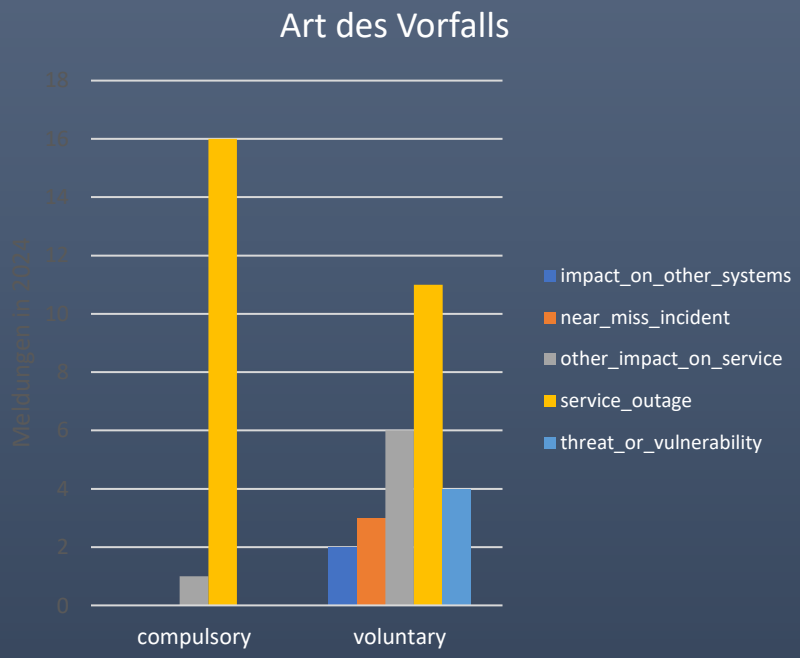
Quelle: cert.at

NIS Meldungen



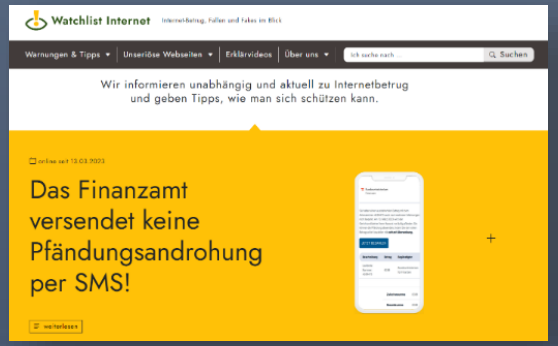
NIS Meldungen 2024 Details





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

Incident Response und Strategie

- Strategische Vorbereitung statt hektischem, spontanem Reagieren
  - Von Training über aktuelle Listen bis Ausweicharbeitsplätze
  - Reihenfolge der zu prüfenden und zu bereinigenden Systeme festlegen
  - Nachweis einer professionellen Vorgangsweisen gegenüber Behörden
- Kurzfristige Mobilisierung des Maximums an Unterstützung
  - Vorhandene Netzwerke nutzen und neue aufbauen
- Anpassung des Geschäftsmodell
  - Wenn es in der aktuellen Bedrohungslage nach einem Angriff nicht gerettet werden kann, sollte es angepasst oder verworfen werden

Incident Strategie für Unternehmen

- Risikoanalysen und Risikoentscheidungen
  - Kernelement aller aktuellen Cybersecurity-Vorgaben (NIS 2, DORA, etc.)
    - Welche Entscheidungen sind inzwischen verpflichtende Vorgaben?
  - Eingehen auf Erpressungen aus strategischer Sicht als Option?
    - Kryptowährungen selbst einkaufen oder Dienstleister damit beauftragen?
  - Ist eine Cyberversicherung sinnvoll?
    - Schadenkompensation oder aktive Unterstützung durch Security-Experten?
  - Verträgt das Image des Unternehmens eine Unterbrechung/ein Datenleck?
    - Kommunikationsstrategie festlegen und ausformulieren
  - Eigenes Personal oder professionellen Dienstleister trainieren?

Incident Strategie für Unternehmen

Entscheider haben zwei Kernaufgaben:

- Entscheidungen treffen
  - Entscheider können sich auf zwei Arten von Entscheidungen vorbereiten:
    - Ein/Ausschalten (Aktivieren/Deaktivieren, Starten/Stoppen)
    - Ressourcen zuteilen/verschieben
  - Verbunden damit: Verantwortung für die Entscheidungen übernehmen
- Kommunikation
  - Andere Organisationen informieren, dass die eigene Organisation Services nicht mehr/nicht mehr vollständig übernehmen kann
    - Auswirkungen auf andere kommunizieren

Incident Strategie für Unternehmen

Vorbereitungsmaßnahmen

- Pre-Approved Actions
  - Vorbereitete Erlaubnis für eigenständige Aktionen der Mitarbeiter:innen (Ein/Ausschalten, Löschen, informieren, etc.)
- Pre-Coordinated Actions
  - Vorbereitetes gemeinsames Handeln mit anderen Akteuren (Synchronisation, Planung)
- Contracts
  - Vertragliche Verpflichtungen (Unterstützungsleistungen in Form von Ressourcen, Zeit, etc.)

Incident Management @ CERT.at

- Beispielszenario: Unbekannter Akteur in Firmennetz
  - APT, Ransomware-Vorbereitung, Spionage?
  - Firmenleitung auf Notabschaltung vorbereiten, falls Verschlüsselung startet
    - Pre-Approved Action möglich?
  - Einbindung von Behörden – DSN vor DSB
    - Vertraulichkeit mit jeder neuen Einbindung gefährdet
  - Wesentlicher Ressourcenaufwand, insbesondere bei Personal
    - Verzögerte Entscheidung ermöglichte bessere Planung, erschöpfte aber auch das Personal
    - Planspiele, BIA, BCM, etc. hätten auf das Szenario vorbereiten können

Kontakt

CERT.at

Wolfgang Rosenkranz

eMail: rosenkranz@cert.at

Web: https://**www.cert.at**

eMail: **team@cert.at** & **reports@cert.at**

+43 1 5056416 715