#/viris[*]

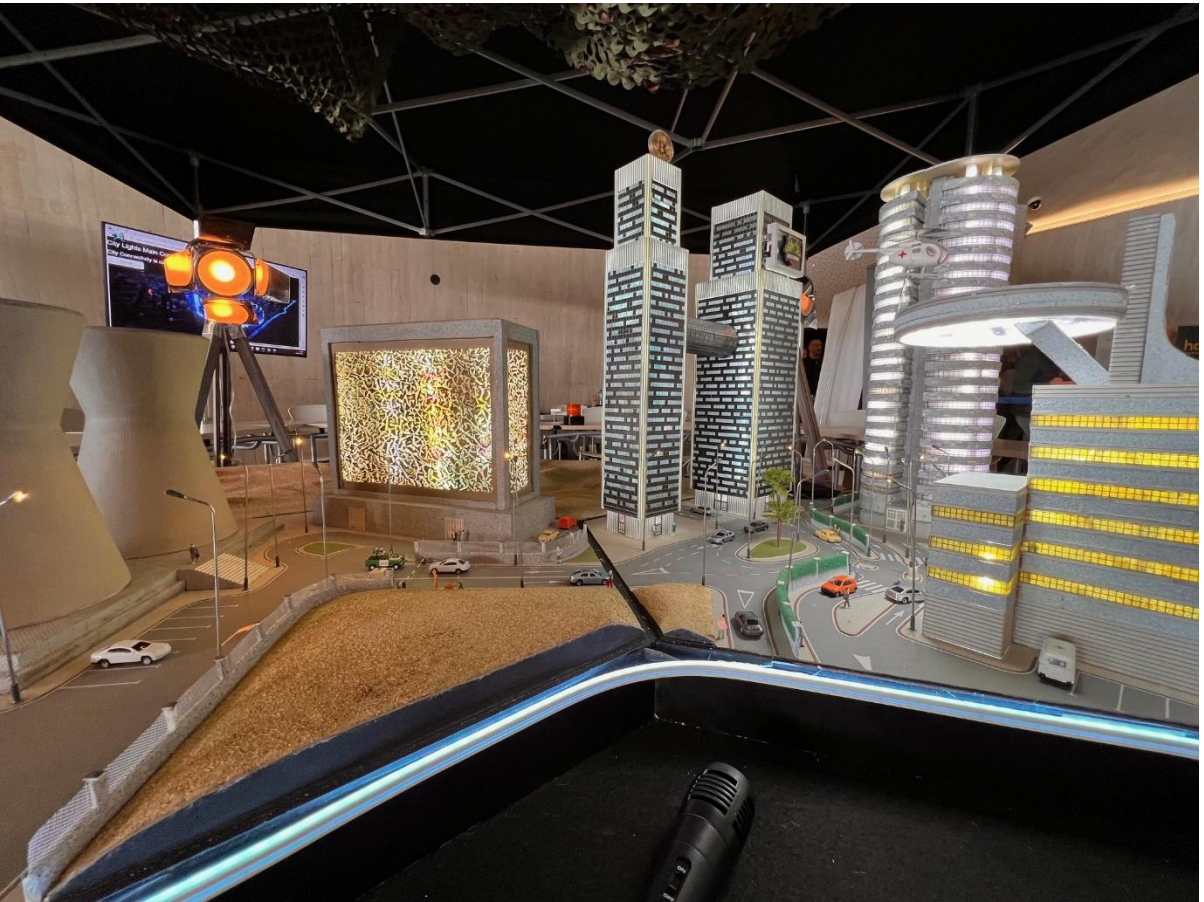
Kibernetske grožnje – poslovna tveganja, ki jih ne moremo več ignorirati

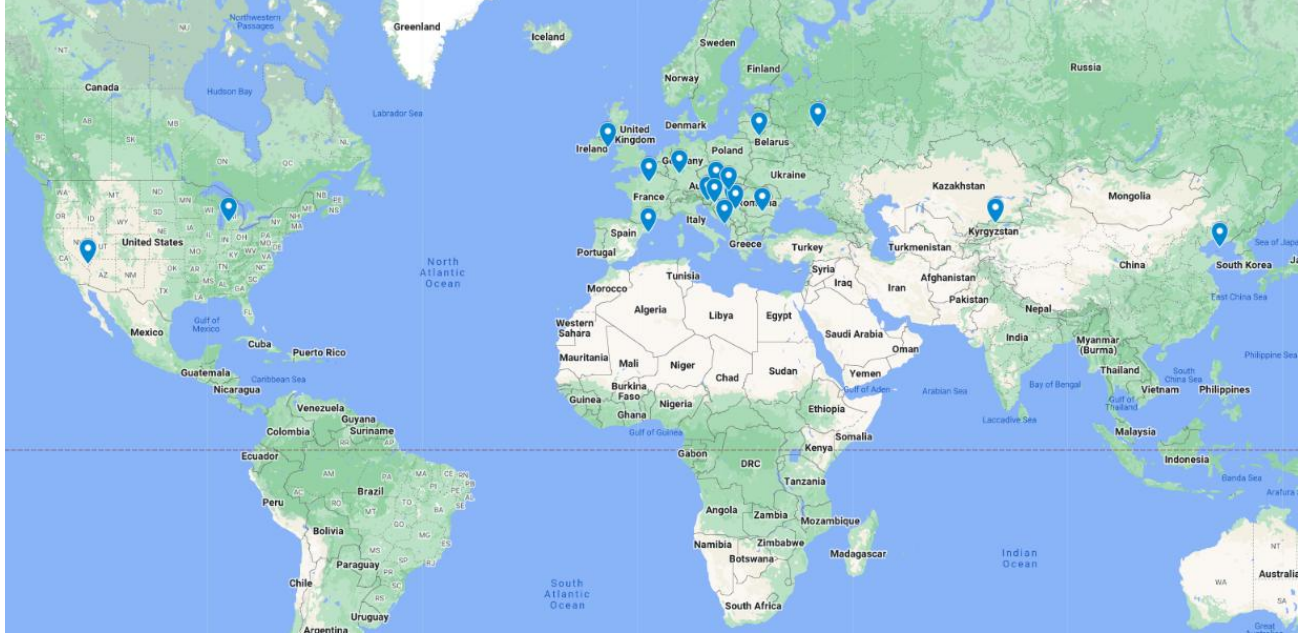
MILAN GABOR

Sekcija za Kibernetsko Varnost

Milan Gabor/

- Etični heker






Oops !

Russian hackers stole Microsoft corporate emails in month-long breach

By **Lawrence Abrams**

January 19, 2024 07:02 PM 5

Microsoft warned Friday night that some of its corporate email accounts were breached and data stolen by a Russian state-sponsored hacking group known as Midnight Blizzard.

The company detected the attack on January 12th, with Microsoft's investigation ultimately determining that the attack was conducted by Russian threat actors known more commonly as Nobelium or APT29.

Ko gorijo oblaki

Threat Management, Identity, Email security

Microsoft key stolen by Chinese hackers provided access far beyond Outlook

Derek B. Johnson July 21, 2023

The private encryption key used by Chinese hackers to break into the email accounts of high-level U.S. government officials disclosed last week also gave them access to a vast array of other Microsoft products, according to new research from cloud security firm Wiz.

On July 11, the Redmond-based tech giant disclosed that a threat actor linked to the Chinese government had — through an acquired Microsoft private encryption key — forged authentication tokens that gave them access to Exchange Online Outlook email accounts for more than 25 organizations, including government agencies.

In a blog post published Friday, Shir Tamari, head of research at Wiz, said further investigation has revealed the compromised key would have given the hacking group, which Microsoft calls Storm-0558, access to far more than Outlook, spanning many other Microsoft services that uses the same authentication process.

"Our researchers concluded that the compromised MSA key could have allowed the threat actor to forge access tokens for multiple types of Azure Active Directory applications, including every application that supports personal account

rive, customers' applications that

Our investigation found that a consumer signing system crash in April of 2021 resulted in a snapshot of the crashed process ("crash dump"). The crash dumps, which redact sensitive information, should not include the signing key. In this case, a race condition allowed the key to be present in the crash dump (this issue has been corrected). The key material's presence in the crash dump was not detected by our systems (this issue has been corrected).

We found that this crash dump, believed at the time not to contain key material, was subsequently moved from the isolated production network into our debugging environment on the internet connected corporate network. This is consistent with our standard debugging processes. Our credential scanning methods did not detect its presence (this issue has been corrected).

After April 2021, when the key was leaked to the corporate environment in the crash dump, the Storm-0558 actor was able to successfully

CrowdStrike Chaos Highlights Key Cyber Vulnerabilities with Software Updates

Posted on July 30, 2024

Earlier this month, a software update from the cybersecurity firm CrowdStrike caused Microsoft Windows operating systems to crash—resulting in potentially the largest IT outage in history.

Disruptions were widespread. Around the world, businesses and services were unable to operate as computers crashed, and some critical infrastructure sectors (like transportation, healthcare, and finance) were disrupted. For example, commercial flights were grounded, critical hospital care was interrupted, and financial institutions were unable to service clients.

Here at GAO, we have long highlighted concerns for Congress about IT vulnerabilities, a lack of security awareness, poor cyber hygiene, and a need for more cyber preventative measures to combat disruptions like the CrowdStrike outage. In our prior work, we have identified risks to the nation's critical infrastructure sectors and in the supply chain of software supporting IT systems.

Related Posts

Blog Post

The Next Big Cyber Threat Could Come from

Lokalno okolje?

SLOVENIJA

Direktor: 'vojni napad' lekarne stal več kot dva milijona evrov

Ljubljana, 08. 08. 2019 08.31 |

PREDVIDEN ČAS BRANJA: **3 min**

AVTOR /M.V., M.S. / STA

KOMENTARJI 152

Lekarna Ljubljana je po treh dneh nedelovanja znova vzpostavila centralni informacijski sistem, vanj pa je že vključenih več lekarn. V drugih enotah trenutno še vedno izdajajo zdravila na papirnat recept, nakup zdravila pa ni mogoč. Po besedah direktorja Marjana Sedeja je nastalo za več kot dva milijona evrov škode.

Hekerski napad na HSE razkriva vrsto golih cesarjev

Zaradi vdora ohromljeni Holding Slovenske elektrarne vzbuja dvome o varnosti kritične infrastrukture.

Kibernetski napad na spletno stran predsednice republike. Hekerji napovedujejo še več napadov.

SI-CERT: Ne gre za vdor v sistem

Hekerji so napadli uradno spletišče predsednice republike, ki je zdaj spet dosegljivo. SI-CERT je potrdil, da ni šlo za vdor v sistem, temveč zgolj za upočasnitev delovanja in da so podatki varni.

Eno večjih slovenskih podjetij tarča kibernetskega napada

NOVICE · Forbes Slovenija · 14. maja, 2024 11.16 > 14. maja, 2024 11.36

»Če hočete izvedeti, kako bo videti digitalna apokalipsa, pojdite v Maribor«

Univerza je v stiku z ustreznimi organi in IT-strokovnjaki in se trudi vzpostaviti sistem. Odpravljanje škode bi lahko trajalo več tednov.

SLOVENIJA

V Telekomu Slovenije zaznali kibernetski incident

Ljubljana , 26. 02. 2025 15.36 | Posodobljeno pred 28 dnevi

PREDVIDEN ČAS BRANJA: **1 min**

AVTOR
STA

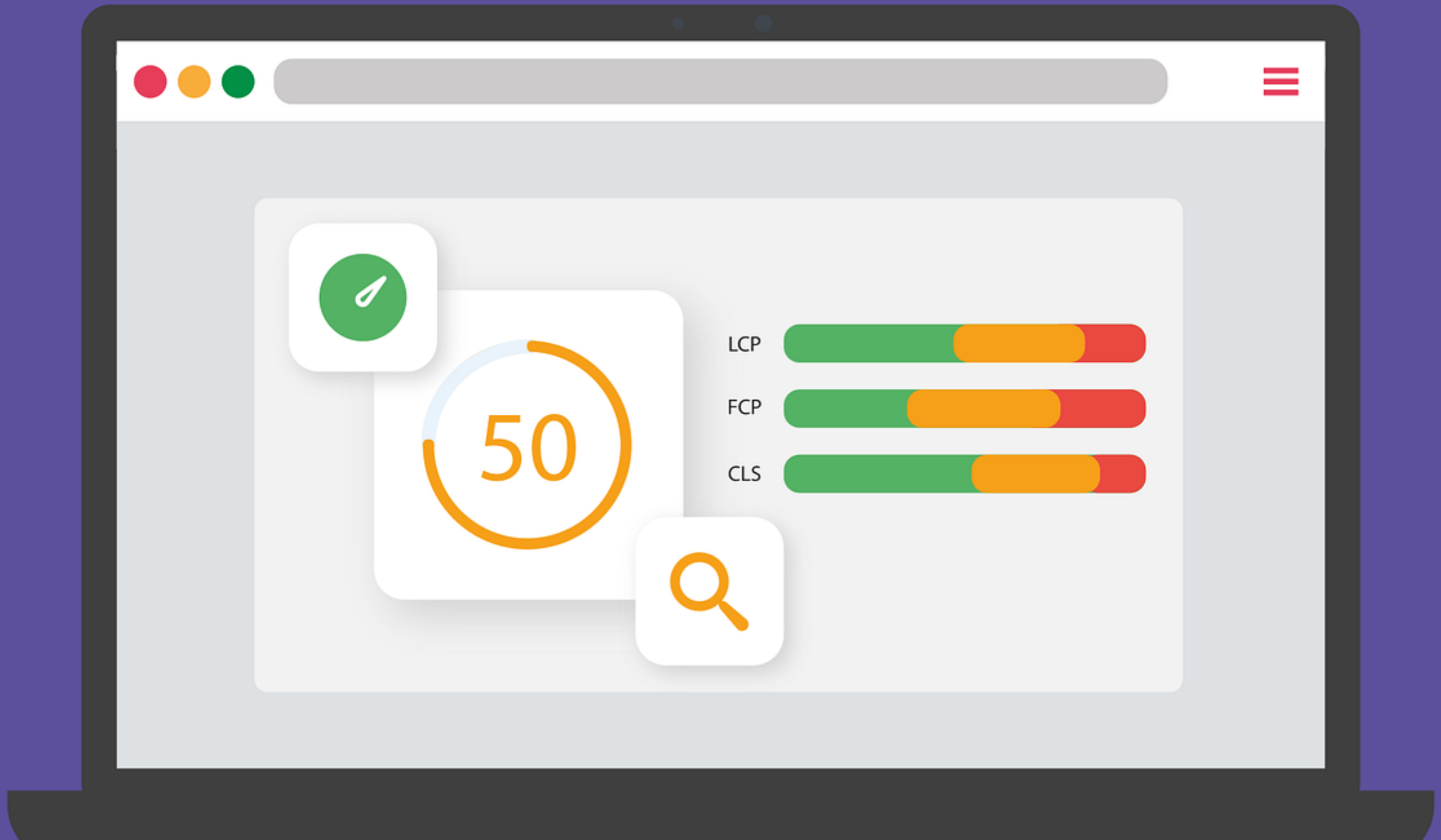
KOMENTARJI
14

V družbi Telekom Slovenije so zaznali kibernetski incident, v katerem so bili razkriti nekateri interni poslovni podatki. Zaradi interesa preiskave v tem trenutku ne morejo razkriti podrobnosti. So pa poudarili, da ni prišlo do vdora v zbirke podatkov o njihovih naročnikih ali o komunikacijah slednjih.

Okužena javna uprava: sporen nakup nevarnih kitajskih USB ključkov

Etični heker: "Pri USB ključkih obramba pred kibernetskimi napadi odpove."

"Mnogi uporabniki se ne zavedajo, da brisanje datotek z USB ključka ne pomeni trajnega izbrisa. Že 'prazna' naprava, ki je vsebovala občutljive dokumente, še vedno predstavlja


50
LCP
FCP
CLS

TOP 10 EMERGING CYBER-SECURITY THREATS FOR 2030

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

https://www.enisa.europa.eu/publications/foresight-2030-threats

TOP 15 CYBERSECURITY THREATS

SPRINTZEAL

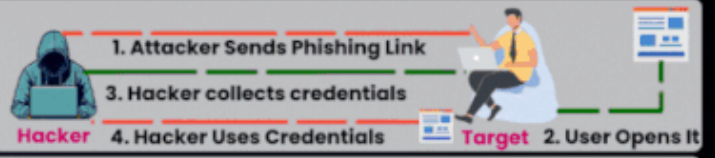
1. Ransomware Attacks
2. Internet of Things (IOT) Vulnerabilities
3. Social Engineering and Phishing Attacks
4. Supply Chain Attacks
5. AI-Powered Cyber Threats
6. Advanced Persistent Threats (APTs)
7. Zero-Day Exploits
8. Cloud Security Risks
9. Mobile Malware and Vulnerabilities
10. Insider Threats
11. Artificial Intelligence (AI) Misuse
12. Data Breaches and Privacy Violations
13. Advanced Phishing Techniques
14. Nation-State Cyber Attacks
15. Cryptocurrency-Related Threats

Top 8 Cyber Attacks - 2024

Cyber Security News

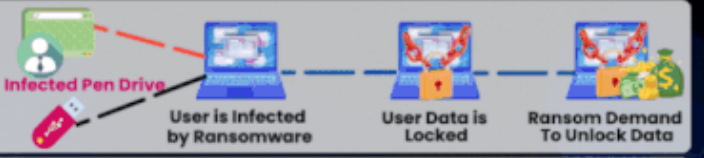
1 Phishing Attack

The use of deceptive emails, texts, or websites to gain sensitive information.



2 Ransomware

Malware that can encrypt data and make you pay to get them back.



3 Denial-of-Service (DoS)

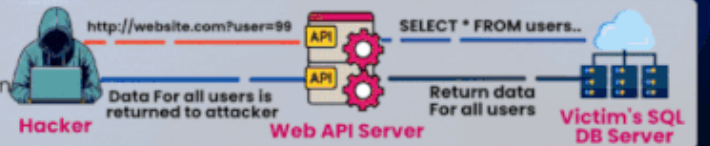
Loading excessive load on a machine or network so that it stops working normally.

4 Man-in-the-Middle (MitM)

Engaging in covert interception and manipulation of communication between two parties without noticing it.

5 SQL Injection

To get the Access to the database, Vulnerabilities in Database queries can be exploited



6 Cross-Site Scripting (XSS)

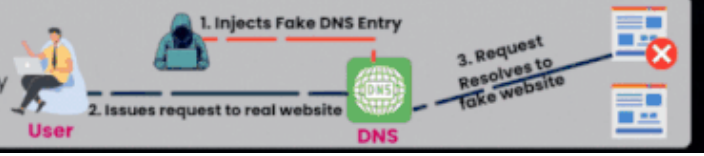
Putting malicious code into websites that other people visit.

7 Zero-Day Exploits

Attacks take advantage of unknown vulnerabilities before programmers can fix them.

8 DNS Spoofing

Sending DNS queries to malicious sites so that they can be accessed without permission.



TOP 2025 CYBER THREAT PREDICTIONS
BY CYEN

1

Technology Abuse
AI or quantum decryption-enabled sensitive data breaches.

2

Supply Chain Attacks
Massive hacks enabled by a single company breach.

3

Ransomware
Growing number of easy but lucrative hacks (SMEs target).

4

Denial of Services
As a political instrument in growing geo-political crises

5

Non-compliance
With new EU, US regulations, new cyber risk grows: fines, claims, legal liability.

Prepare for the worst and hope for the best!

CYEN

Cybersecurity Predictions for 2025

1. Crypto-Stealers in Open Source Software
2. Risks from Unmaintained Open-Source Projects
3. Quantum Computing & Encryption Vulnerabilities
4. AI-Powered Malware
5. Insider Threats
6. Sophisticated Social Engineering Attacks

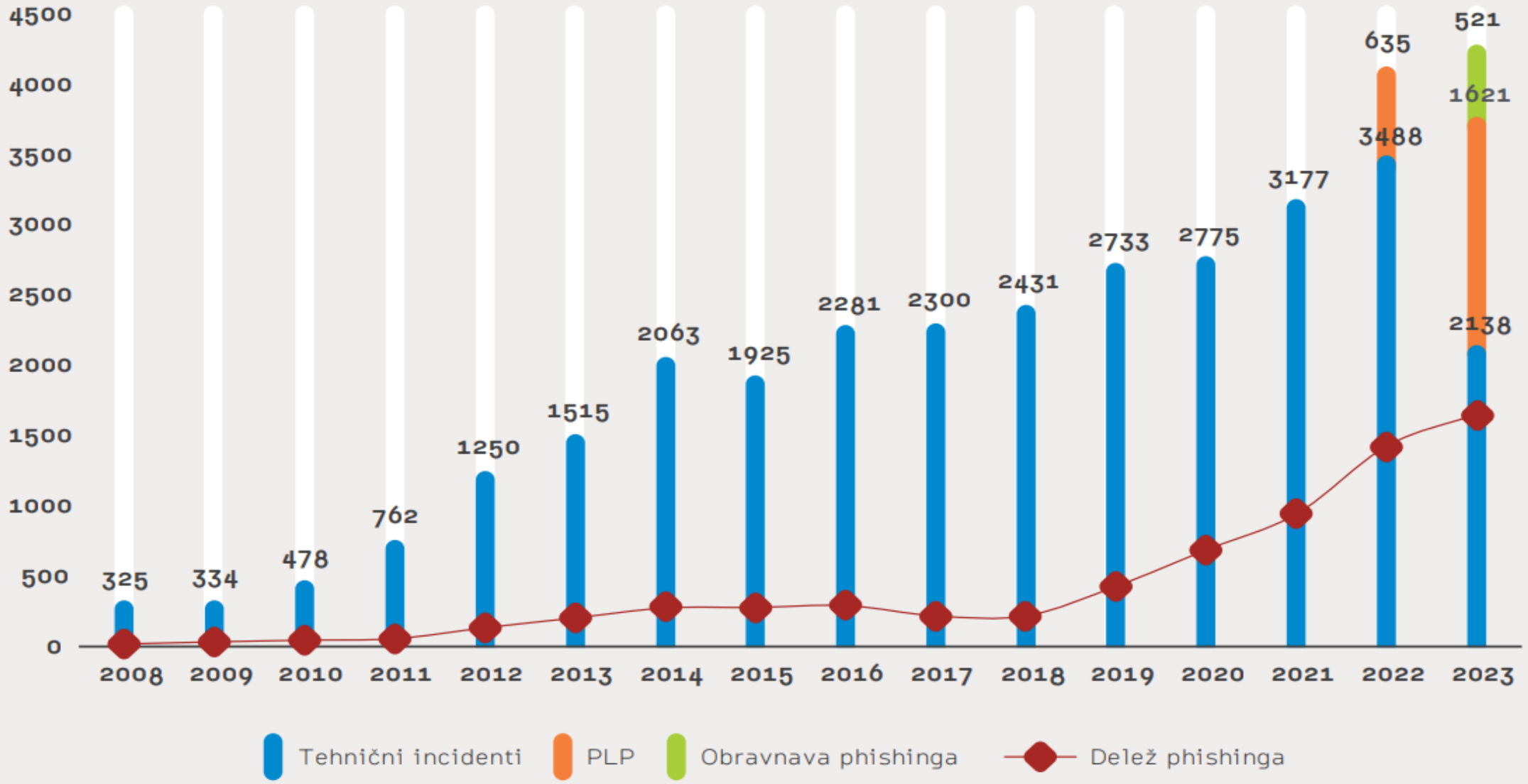
Neverjetne statistike: tudi v Sloveniji več milijonov škode

Razsežnosti kibernetskega kriminala so iz leta v leto večje, in če mislite, da vaše podjetje ne more postati tarča, se motite.

Slovenija prav nič ne zaostaja

Tudi v Sloveniji kibernetske grožnje naraščajo in postajajo vse bolj prefinjene. Podjetja in posamezniki se spopadajo z večjo nevarnostjo t. i. smishing napadov (SMS-sporočila, namenjena kraji finančnih podatkov), direktorskih prevar in kripto investicijskih goljufij, je razvidno iz zadnjega poročila nacionalnega odzivnega centra za kibernetsko varnost SI-CERT. Poročilo poudarja potrebo po povečanju ozaveščenosti in preventivnih ukrepov, saj so napadi z vsakoletnim porastom škode postali resna grožnja za gospodarstvo in prebivalstvo. Podatki, ki jih navaja poročilo, so osupljivi: slovenska policija zazna kar 27,5 milijona evrov škode v različnih goljufijah, največji porast je v kategoriji investicijskih prevar, kjer so zaznali kar 13 milijonov evrov škode.**

INCIDENTI SKOZI LETA



https://www.cert.si/wp-content/uploads/2024/05/Porocilo-o-kibernetski-varnosti_2023_SI-CERT_web.pdf

PRIJAVITELJI PO SEKTORJIH

924 (12%)
fizična oseba

606 (12%)
druge pravne osebe

269 (12%)
bančništvo

116 (5%)
raziskovanje in izobraževanje

60 (3%)
državni organi

40 (2%)
operater elektronskih komunikacij

22 (1%)
zdravstvo

20 (1%)
energija

20 (1%)
promet

6 (0%)
digitalni trg

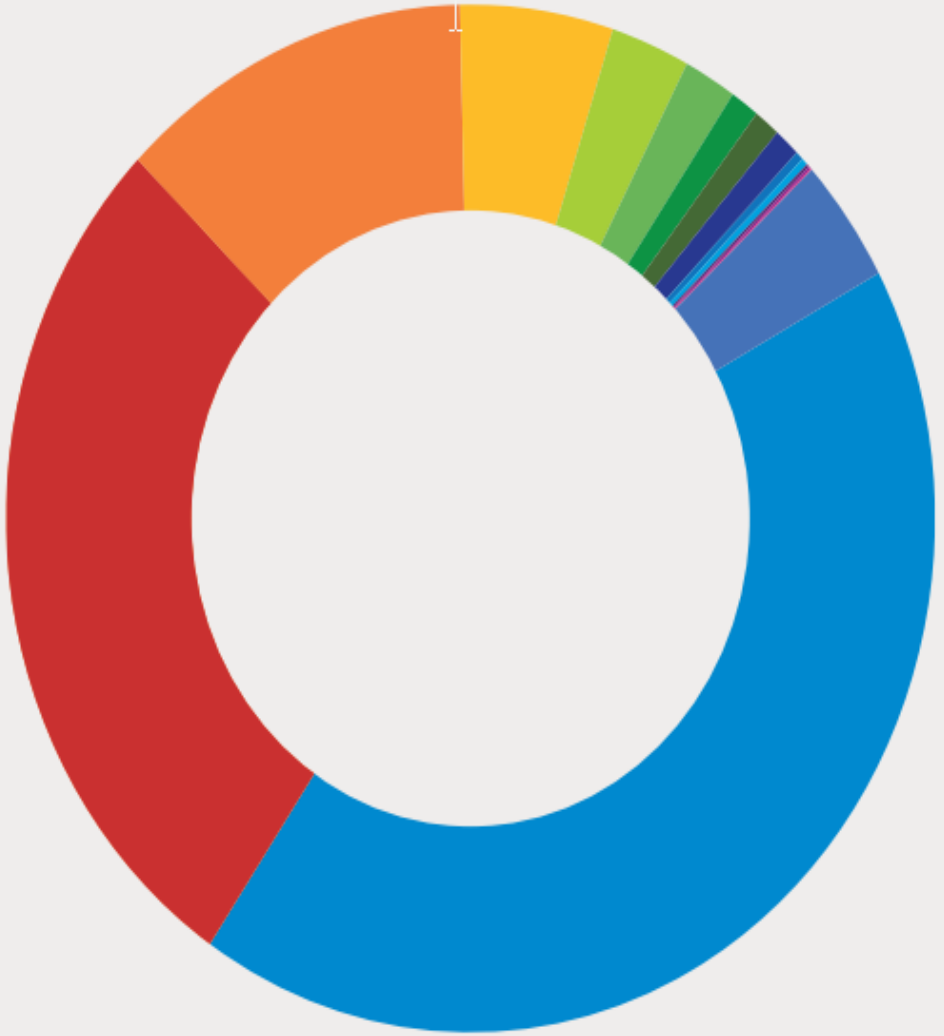
5 (0%)
digitalna infrastruktura

2 (0%)
pitna voda

2 (0%)
oblačno računalništvo

1 (0%)
finančni trgi

86 (4%)
drugo



https://www.cert.si/wp-content/uploads/2024/05/Porocilo-o-kibernetski-varnosti_2023_SI-CERT_web.pdf

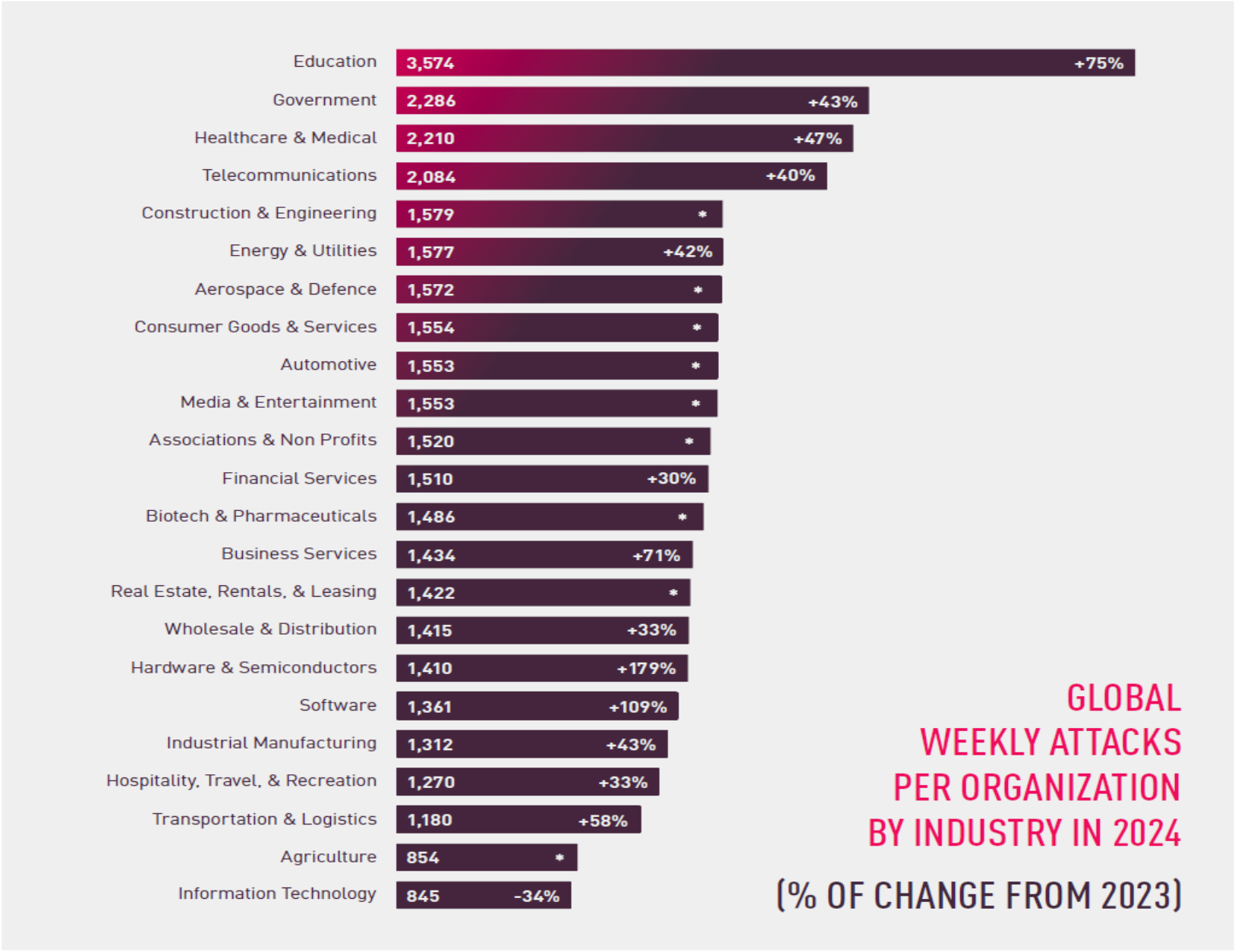


Figure 3 - Global average of weekly attacks per organization by industry in 2024 [% of change from 2023].
[*] Newly introduced sectors which were not part of the previous report.

ATTACKS PER ORGANIZATION

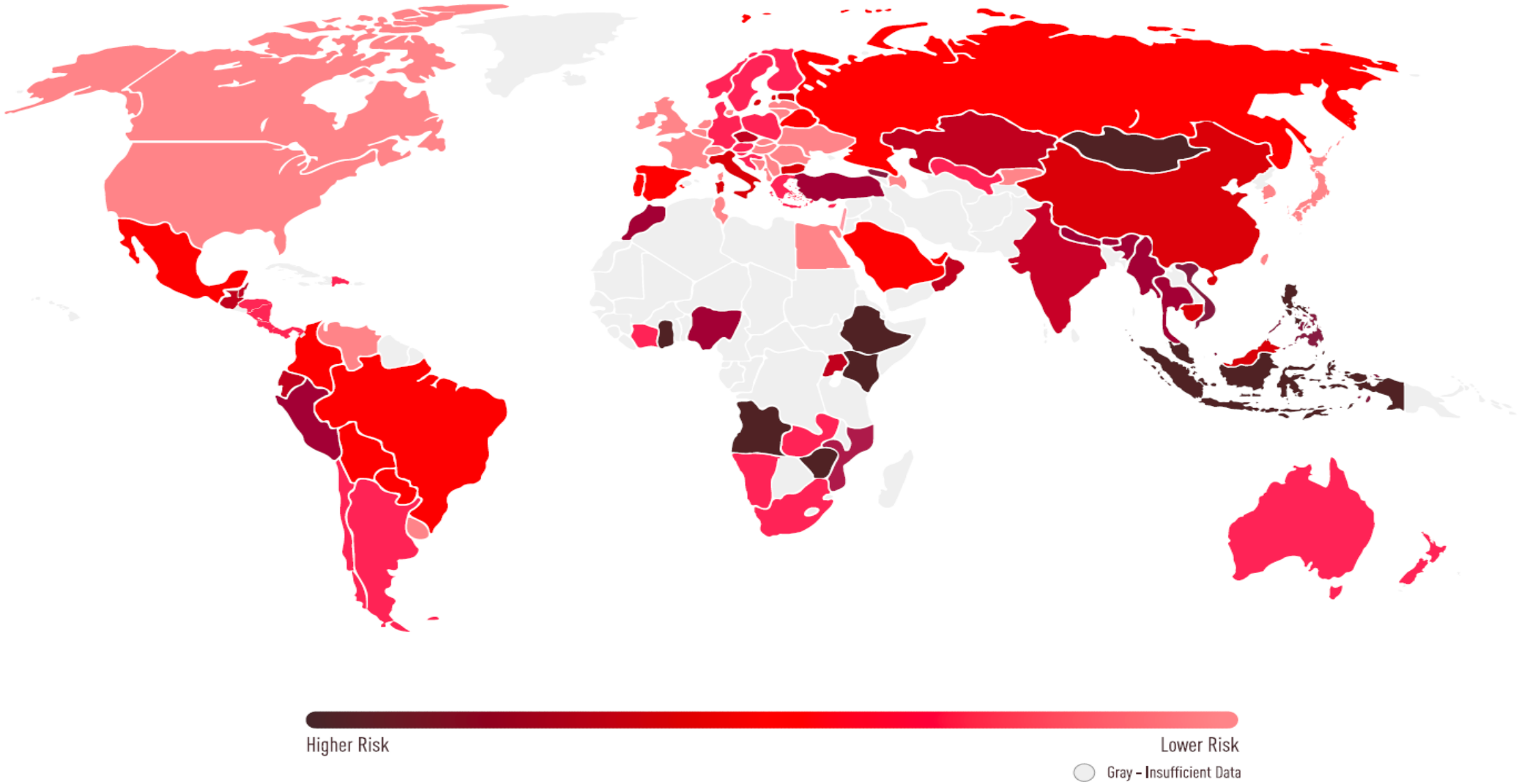
The overall global attacks against organizations significantly increased in the past year, with the average number of weekly attacks per organization reaching 1,673. This is 44% higher than in 2023. Figure 3 illustrates the average number of weekly attacks per organization by industry. In 2024, there was a significant increase in the number of attacks per week across most sectors. The education sector experiences the highest volume, with a 75% year-over-year (YoY) increase, surpassing an average of 3,574 weekly attacks. Education institutions were specifically targeted for personal information collection. This persistent rise in attack rates impacts universities, schools, and educational departments and services.

The healthcare sector also witnessed a 47% increase in average weekly attacks. Cyber criminals are increasingly abandoning their previous self-imposed prohibitions against targeting healthcare services. The health sector is particularly vulnerable to prolonged service disruptions (as noted in the earlier Ransomware section) and the highly sensitive nature of patient data they hold.

The technological supply chain sector, including software, hardware, and semiconductor companies, also experienced a significant surge in cyberattacks. Notably, the hardware and semiconductor industries saw the sharpest rise, with a staggering 179% increase in average weekly attacks, with the total number now exceeding 1,400. This spike can be attributed to the growing global demand for hardware and the heightened focus on AI technologies. As critical components of modern infrastructure and innovation, these industries have become prime targets for cyber criminals seeking to exploit supply chain vulnerabilities for financial gain, espionage, or disruption.

THE OVERALL GLOBAL ATTACKS AGAINST ORGANIZATIONS SIGNIFICANTLY INCREASED IN THE PAST YEAR, WITH THE AVERAGE NUMBER OF WEEKLY ATTACKS PER ORGANIZATION REACHING 1,673. THIS IS 44% HIGHER THAN IN 2023

https://www.cert.si/wp-content/uploads/2024/05/Porocilo-o-kibernetski-varnosti_2023_SI-CERT_web.pdf



The state of Cyber Security 2025 by Check Point

Figure 2 - The map displays the cyber threat risk index globally, demonstrating the main risk areas around the world.


"THERE ARE TWO KINDS OF BIG COMPANIES, THOSE WHO'VE BEEN HACKED, AND THOSE WHO DON'T KNOW THEY'VE BEEN HACKED."
-JAMES COMEY, FORMER FBI DIRECTOR
197 days
Average time to identify a breach
69 days
Average time after detection to full recovery
$4.45Million
Average cost of a data breach in 2023 (2% YoY increase)
$1.76Million
Average savings for organizations that use security AI and automation extensively compared to the ones that don't
Source: IBM (2023), Ponemon Institute (2023
COURE
NEVER LET A COMPUTER KNOW YOU'RE IN A HURRY


RUSSIAN MARKET
Username
Password
Captcha
G41F3
Create an account


Password:
****

CVE-2024-27198 Vulnerability Timeline | March 4th

14:00 UTC

Jetbrains releases Teamcities 2023.11.4 update

14:59 UTC

Jetbrains publicly discloses CVE-2024-27198

19:23 UTC

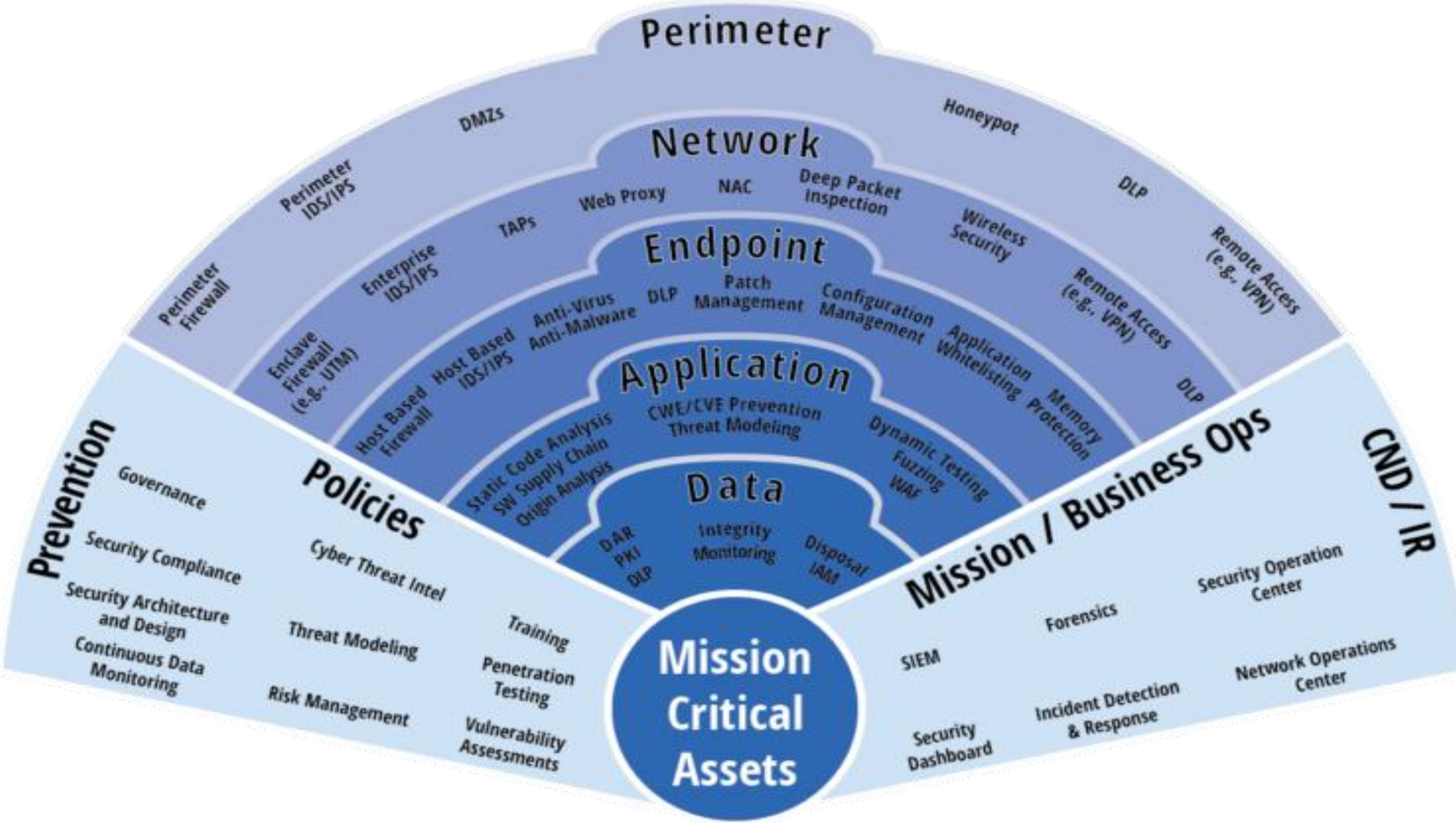
Rapid7 shares a blog, including proof-of-concept exploitation

19:45 UTC

Cloudflare observes attempted exploitation

Dva tipa organizacij

- Regulirane
  - Zakonodaja
  - Druge zahteve regulatorjev
  - Redno/a preverjanje
  - Zavedanje
  - Dvig nivoja varnosti
  - Vložki/investicije
- Neregulirane
  - Delajo po navdihu
  - Izvajajo aktivnosti po incidentih
  - Varnost ni nujno prioriteta

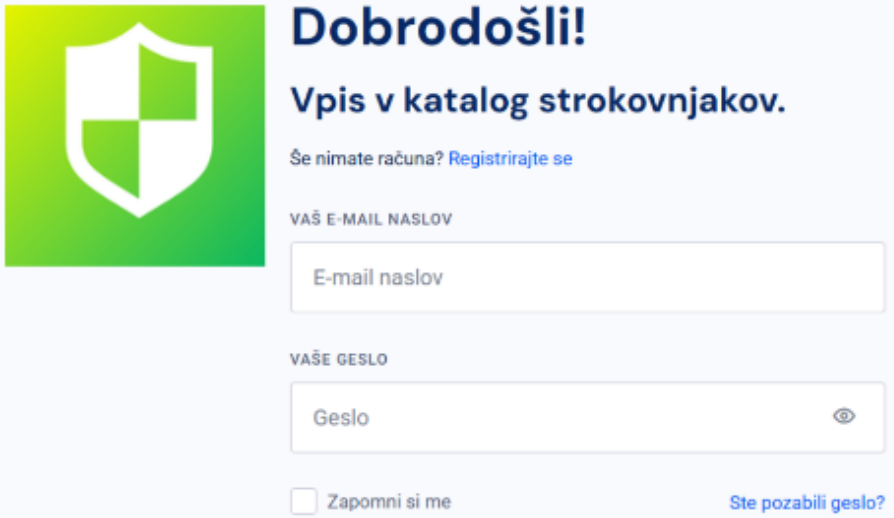

Perimeter
DMZs
Honeypot
Perimeter IDS/IPS
Network
Web Proxy
NAC
Deep Packet Inspection
DLP
TAPs
Wireless Security
Remote Access (e.g., VPN)
Perimeter Firewall
Enterprise IDS/IPS
Endpoint
Patch Management
Configuration Management
Remote Access (e.g., VPN)
Anti-Virus Anti-Malware
DLP
Enclave Firewall (e.g., UTM)
Application Whitelisting
Memory Protection
Host Based IDS/IPS
Application
DLP
Host Based Firewall
CWE/CVE Prevention Threat Modeling
Static Code Analysis SW Supply Chain Origin Analysis
Dynamic Testing Fuzzing WAF
Data
DAR PKI DLP
Integrity Monitoring
Disposal IAM
Prevention
Policies
Mission / Business Ops
CND / IR
Governance
Security Compliance
Security Architecture and Design
Continuous Data Monitoring
Cyber Threat Intel
Threat Modeling
Risk Management
Training
Penetration Testing
Vulnerability Assessments
Mission Critical Assets
Forensics
Security Operation Center
SIEM
Network Operations Center
Incident Detection & Response
Security Dashboard

Dobre prakse

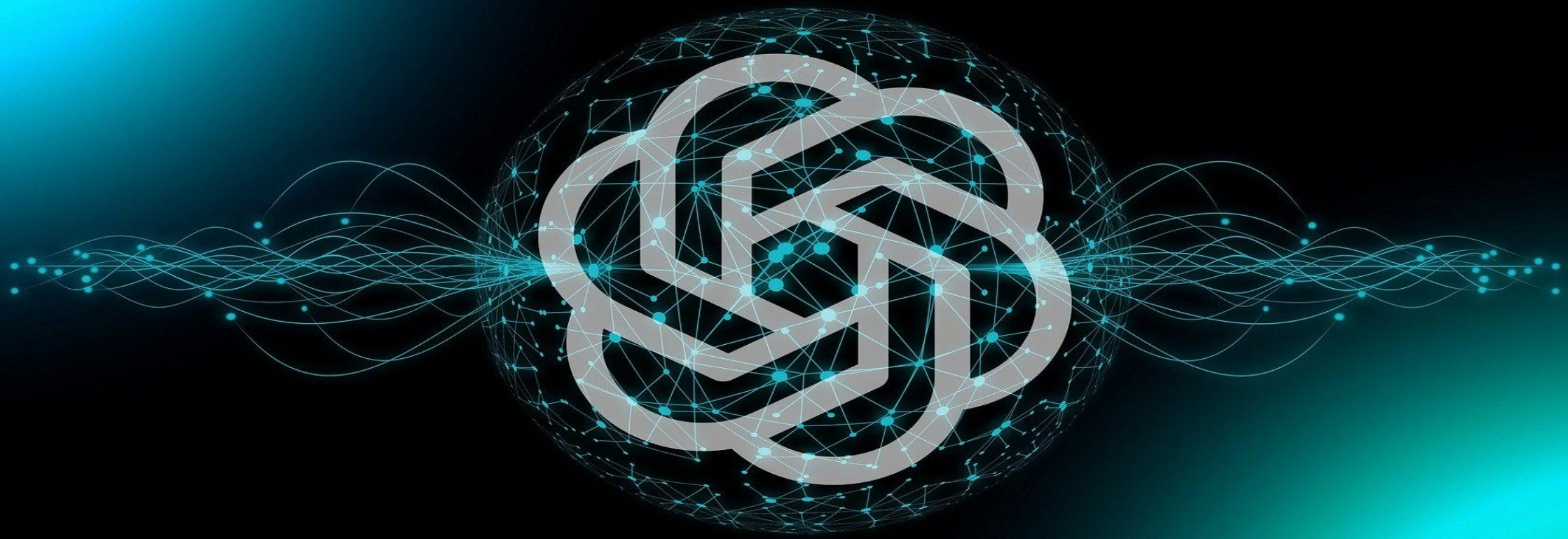
Prenova Kataloga strokovnjakov na področju kibernetske varnosti

20. FEB. 2025

Začeli smo z aktivnostmi, povezanimi s **prenovo Kataloga strokovnjakov DIH Slovenije**, pri čemer bo v prvem delu posodobljen seznam strokovnjakov na področju **kibernetske varnosti**. Ta posodobitev bo podjetjem olajšala dostop do preverjenih zunanjih izvajalcev za varnostne preglede in penetracijske teste. **Vpis na druga področja trenutno ni mogoč.**




FUTURE
I'M
READY



#/viris[# *]

Generative AI is the new strategic battleground

Weaponization of AI

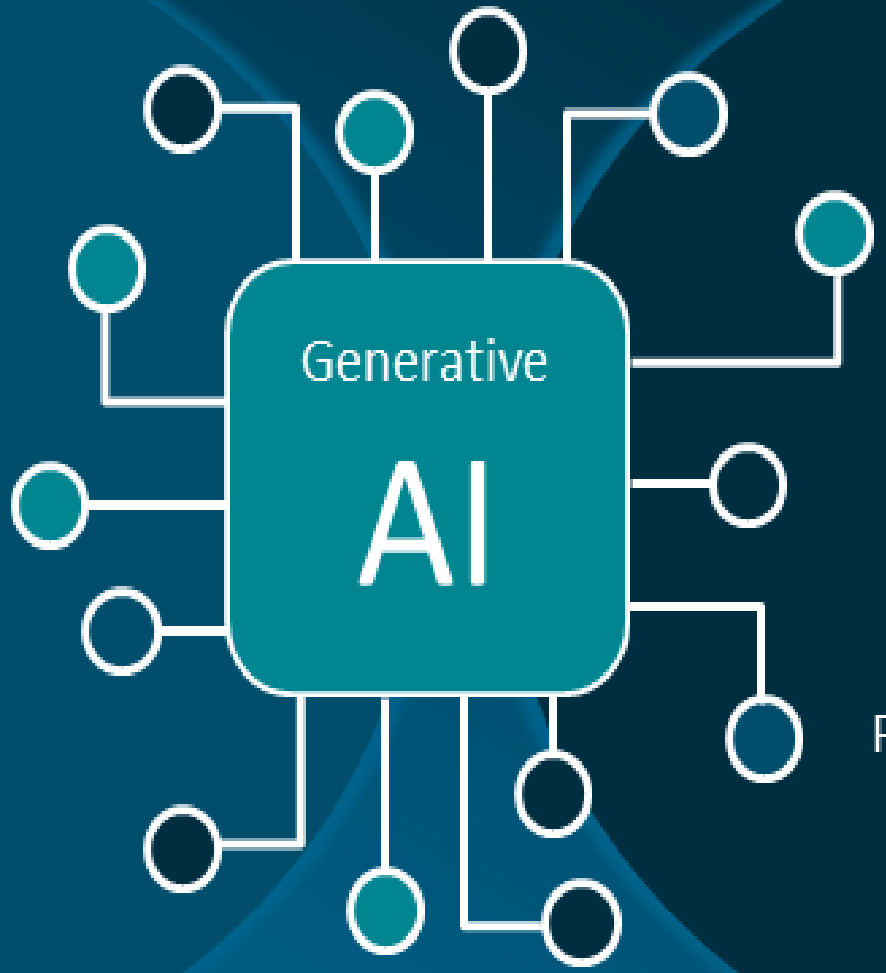
More threat actors to launch attacks

More convincing phishing campaigns

New deep fake social engineering schemes

Malware mutation

Exploit software vulnerabilities



AI to augment cybersecurity

Boost cybersecurity SOC analysts

Breach risk predictions

Enhance cybersecurity posture

Asset inventory management

Prioritize vulnerability remediations

Accelerate resolution time

Prihodnost

- NIS-2 in ZInfV-1 bosta pripomogla k dvigu informacijske varnosti, vendar …
- Regulativa ni vedno dobra/slaba
- Vidimo, da se svet spreminja in zato se je potrebno prilagoditi!
- Fokus na AI!

- **Preventiva** boljša kot **kurativa!**


DISASTER
RECOVERY
CONTROL
IMT
SLA
INCIDENT
MANAGEMENT
DIAGNOSIS
RESPONSE
EVENT
SECURITY
PROTOCOL
OPERATIONS
POLICY
PLANNING
ANALYSIS
DETECTION

#/viris[*]

@MilanGabor