



РЕПУБЛИКА СРБИЈА  
**РАТЕЛ**  
РЕГУЛАТОРНО ТЕЛО ЗА  
ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ  
И ПОШТАНСКЕ УСЛУГЕ



# НАЦИОНАЛНИ ЦЕРТ актуелности

05.06.2024. године

*др Горан Пауновић*

Главни саветник за безбедност ИКТ система  
Служба за ИБ и послове Националног ЦЕРТ-а,

РАТЕЛ

[goran.paunovic@ratel.rs](mailto:goran.paunovic@ratel.rs)

[www.cert.rs](http://www.cert.rs)



РЕПУБЛИКА СРБИЈА  
**РАТЕЛ**  
РЕГУЛАТОРНО ТЕЛО ЗА  
ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ  
И ПОШТАНСКЕ УСЛУГЕ

НАЦИОНАЛНИ ЦЕРТ РС



## САДРЖАЈ:

1. Национални ЦЕРТ /Законски оквир/ надлежности
2. Пријава инцидента
3. Статистика
4. Едукација
5. МИСП
6. Систем за рана упозорења
7. Актуелне сајбер претње
8. Напредна средства одбране
9. Закључак



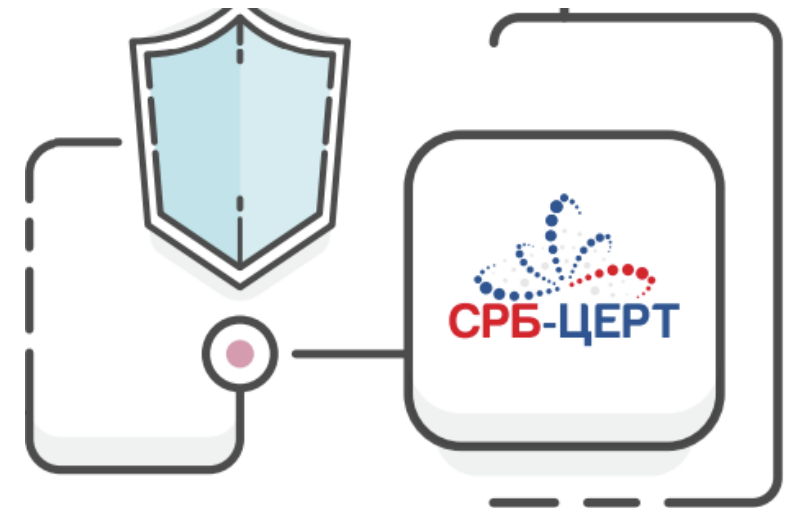
РЕПУБЛИКА СРБИЈА  
**РАТЕЛ**  
РЕГУЛАТОРНО ТЕЛО ЗА  
ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ  
И ПОШТАНСКЕ УСЛУГЕ

НАЦИОНАЛНИ ЦЕРТ РС



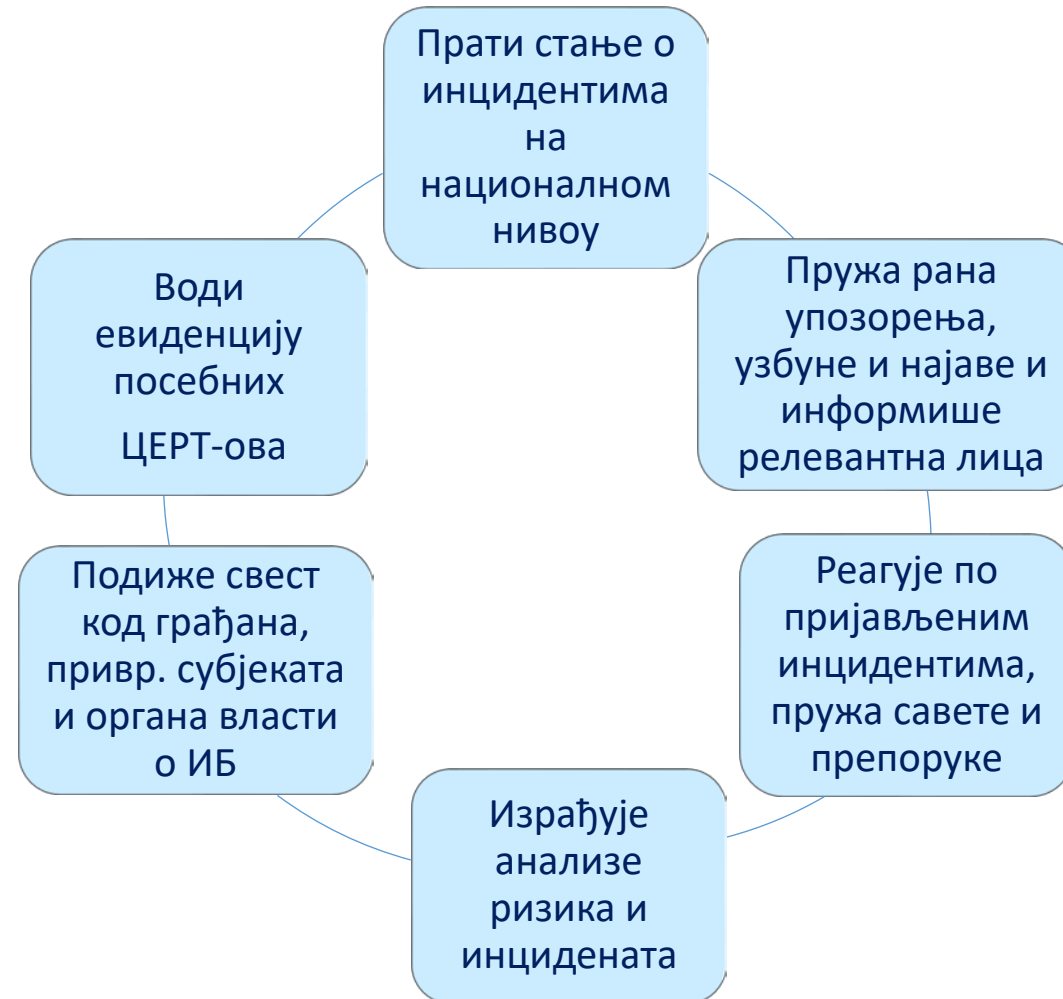
## 1.1. Законски оквир за формирање Националног ЦЕРТ-а

- Закон о информационој безбедности усвојен - 2016. године
- У складу са Законом о информационој безбедности:
  - Национални ЦЕРТ - Национални центар за превенцију безбедносних ризика у ИКТ системима Републике Србије - почео са радом 2017. године
  - Делује у оквиру РАТЕЛ-а, (Регулаторног тела за електронске комуникације и поштанске услуге)





## 1.2. Надлежности Националног ЦЕРТ-а





РЕПУБЛИКА СРБИЈА  
**РАТЕЛ**  
РЕГУЛАТОРНО ТЕЛО ЗА  
ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ  
И ПОШТАНСКЕ УСЛУГЕ

НАЦИОНАЛНИ ЦЕРТ РС



## 2. Пријава инцидента Националном ЦЕРТ-у

Насловна // Пријави инцидент

### Пријави инцидент

ПРИЈАВИ  
ИНЦИДЕНТ

Молимо Вас да одаберете одговарајућу категорију корисника пријаве инцидента

ФИЗИЧКО  
ЛИЦЕ



МАЛО И СРЕДЊЕ  
ПРЕДУЗЕЋЕ



ИКТ СИСТЕМ ОД  
ПОСЕБНОГ ЗНАЧАЈА



### Подаци о правном лицу

Назив правног лица \*

Седиште правног лица \*

Број телефона \*

Имејл адреса \*

\* Молимо вас да проверите исправност ваше Имејл адресе

ИКТ систем \*

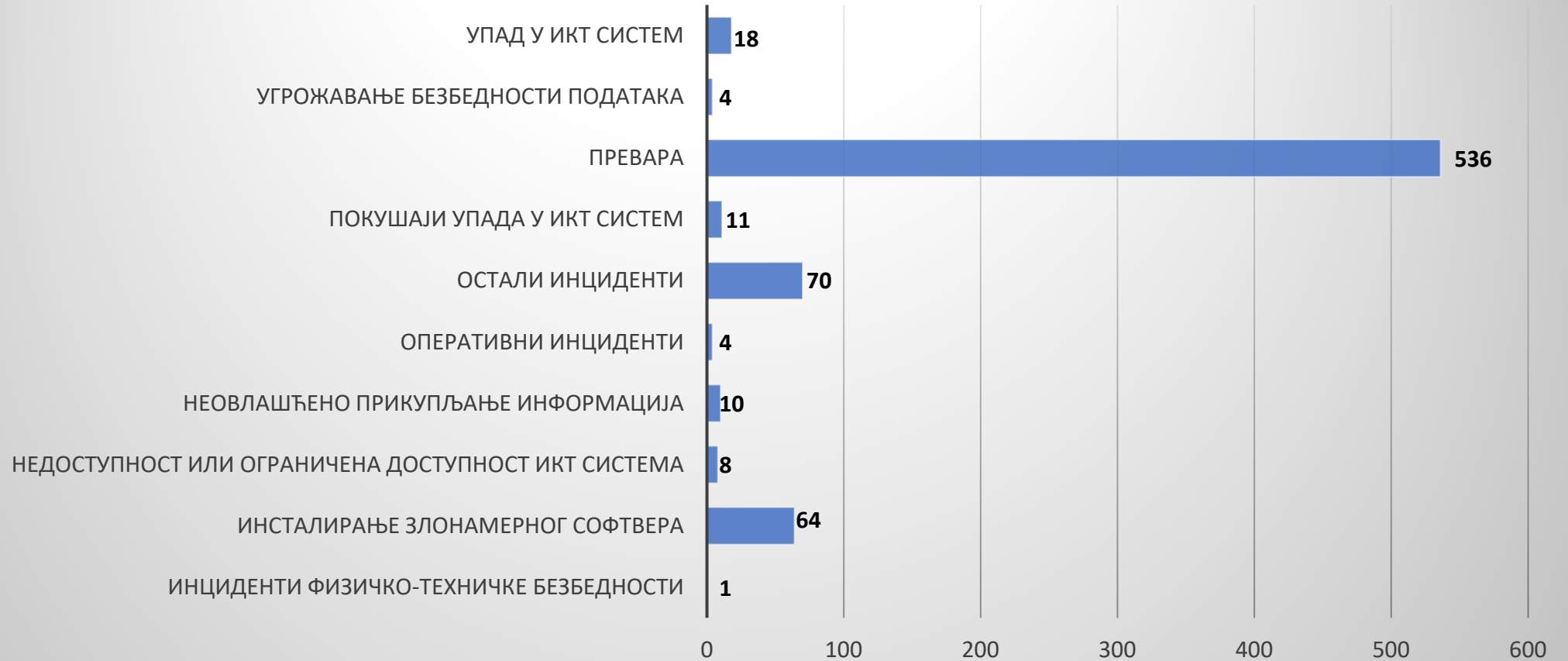
### Подаци о подносиоцу пријаве

info@cert.rs

062/20-20-30

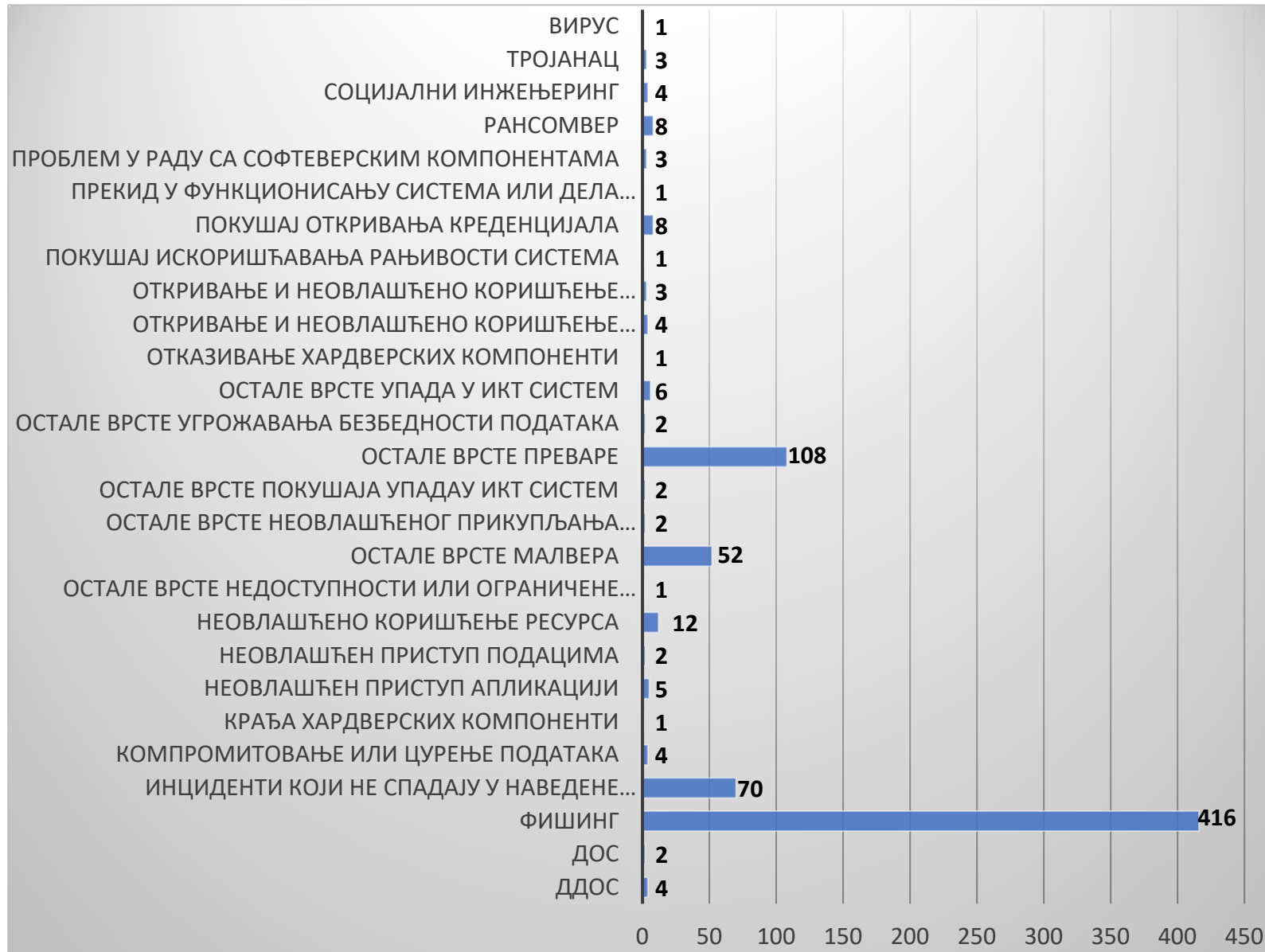


### 3.1. Пријављени инциденти Н ЦЕРТ-у по групама инцидената (2023. г)





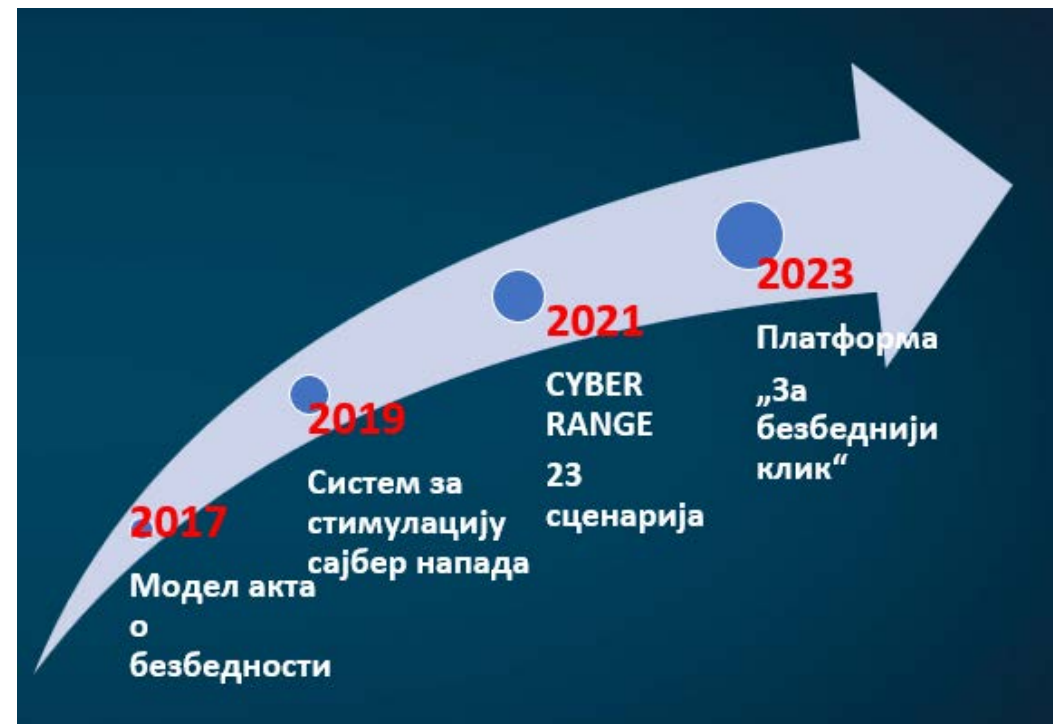
## 3.2. Пријављени инциденти Н ЦЕРТ-у по врстама инцидената (2023. г)



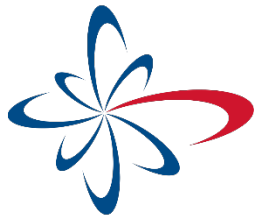


## 4. Едукација и подизање свести из области информационе безбедности

- Разумевање технологије
- Имплементација мера заштите
- Унапређење вештина и подизање нивоа знања
- Детекција и реакција на критичне безбедносне активности







РЕПУБЛИКА СРБИЈА  
**РАТЕЛ**  
РЕГУЛАТОРНО ТЕЛО ЗА  
ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ  
И ПОШТАНСКЕ УСЛУГЕ

НАЦИОНАЛНИ ЦЕРТ РС



## 4.1. Cyberbit обуке – за техничка лица

The screenshot displays the Cyberbit Cyber Range Instructor interface (version 4.3.0) for an instructor. The interface is divided into several sections:

- Header:** Shows the user as "Instructor 1" and the application name "CYBERBIT Cyber Range Instructor | version 4.3.0". A red box highlights the window control buttons (minimize, maximize, close) in the top right corner.
- Navigation Bar:** Includes a home icon, a "Training Name" field, a settings gear, "Training Sessions 0/1", "Weight 0/157", and "SAVE" and "CREATE" buttons.
- Left Panel (Attack Scenarios):** A red header "Attack Scenarios Select Scenarios" with a search icon. Below are several scenario cards with plus signs: Apache Shutdown, Corporate Espionage, DDOS DNS Amplification, DDOS SYN Flood, Domain Keylogger, and Dragonfly.
- Main Area:** Displays a network diagram titled "IP Network PAN+Qradar (65p) 3rd Party Licenses". The diagram shows a central cloud component connected to various server racks and network devices. A "CHANGE NETWORK" button is visible above the diagram.
- Right Panel (Students):** A blue header "Students Select students" with a search icon and "AUTO SELECT" button. It shows "10 Stations Selected". Below is a search bar and a list of student profiles, each with a plus sign and a profile icon:
  - Amit Mizrahi (Training Team Lead)
  - Trainee 01 (SOC Operator)
  - Trainee 02 (SOC Operator)
  - Trainee 03 (SOC Operator)
  - Trainee 04 (SOC Operator)
  - Trainee 05 (SOC Operator)



РЕПУБЛИКА СРБИЈА  
**РАТЕЛ**  
РЕГУЛАТОРНО ТЕЛО ЗА  
ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ  
И ПОШТАНСКЕ УСЛУГЕ

НАЦИОНАЛНИ ЦЕРТ РС



## 4.2 Платформа за безбеднији клик

<https://learn.cert.rs/>

The screenshot displays a grid of 10 educational cards from the CERT RS learning platform. Each card features a topic title, a brief description, and a 'Почни сада' (Start now) button. The topics include:

- Ажурирање/Update**: Значај ажурирања оперативних система, софтвера и апликација.
- Заштита мобилних телефона**: Основне информације о заштити мобилних телефона.
- Критична инфраструктура**: Значај заштите критичне инфраструктуре.
- Фишинг**: Фишинг је најзаступљенији тип сајбер напада.
- Креирање и безбедност лозинки**: Креирање и управљање лозикама на безбедан начин.
- Безбедност на друштвеним мрежама**: Важност заштите наших личних података приликом коришћења друштвених мрежа.
- Рансомвер**: Ближе упознавање корисника са Рансомвер типом сајбер напада.
- Креирање резервних копија**: Упознавање са основним предностима које нуде резервне копије важних датотека, ако дође до хакерског напада.
- Социјални инжењеринг**: Социјални инжењеринг је усмерен на
- Безбедно коришћење отвореног бежичног интернета (Wi-Fi)**



## 4.3. Публикације Националног ЦЕРТ-а

Новости

Обавештења

Препоруке

**Публикације**

Извештаји

Регистар Посебних ЦЕРТ-ова

Контакт



Насловна // Публикације

### Публикације

ПРИЈАВИ  
ИНЦИДЕНТ

Налазите се на страници Публикације. За потребе лакше претраге, изаберите жељену категорију корисника и сазнајте више о свим доступним темама изабране категорије.

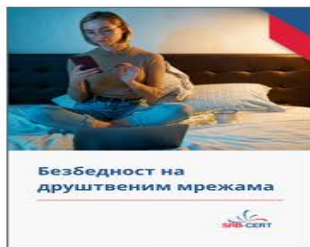
Грађани

ИКТ системи од  
посебног значаја

**Мала и средња  
предузећа**

Упутства и  
истраживања

Све публикације



Безбедност на  
друштвеним мрежама

### Безбедност на друштвеним мрежама

- Све што други људи могу сазнати о нама, као корисницима друштвених мрежа, заправо је доступно на нашим профилима, садржају који објављујемо, као и интеракцијама које имамо са другим корисницима.
- Три основна типа сајбер напада на друштвеним мрежама су:
  - Малвер,
  - Крађа личних података и
  - Вршњачко насиље.
- Како се можемо заштитити?

2. Фебруар 2023 pdf 17.48MB [Сазнајте више](#)



### Сајбер Азбука

Азбука основних сајбер препорука које вам могу помоћи да будете безбеднији док уживате, учите или радите на интернету.

25. Новембар 2022 pdf 11.60MB [Сазнајте више](#)



РЕПУБЛИКА СРБИЈА  
**РАТЕЛ**  
РЕГУЛАТОРНО ТЕЛО ЗА  
ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ  
И ПОШТАНСКЕ УСЛУГЕ

НАЦИОНАЛНИ ЦЕРТ РС



## 5. Закон – Стратегија - МИСП

- У складу са **Законом о информационој безбедности**
  - Национални ЦЕРТ прикупља и размењује информације о безбедносним ризицима и пружа рана упозорења, узбуне и најаве и информише релевантна лица о ризицима и инцидентима.
- Стратегијом развоја информационог друштва и информационе безбедности период (2021. до 2026. године) предвиђен је
  - **развој платформе за размену информација између Националног ЦЕРТ-а и ИКТ система од посебног значаја** у циљу информисања о актуелним ризицима и претњама у области информационе безбедности и промовисања примера добре праксе.



## 5.1. MISP (Malware Information Sharing Platform)

- **MISP** - Open Source Threat Sharing Platform
- Бесплатна платформа за централизовано прикупљање и дељење информација о претњама на националном нивоу.
- Циљ - преглед актуелних претњи на основу којих је могуће спровести адекватну и правовремену **превенцију, детекцију и реакцију** на претње и нападе на ИКТ системе од посебног значаја у РС.
- Алат за прикупљање информација о:
  - актуелним претњама,
  - рањивостима,
  - сајбер инцидентима,
  - препорукама и начинима заштите,
  - анализи малвера,
  - актуелним преварама и кампањама.
- Централна база података о индикаторима компромитовања
- Подаци су нормализовани, повезани и обогаћени
- Омогућава тимовима да комуницирају и сарађују



## 5.2. Групе корисника МИСП платформе

Корисници **MISP** платформе су релевантне институције у области ИБ, које за коришћење платформе именују представнике. Информације се деле са циљем да се дефинишу мера заштите и начин реаговања.

У циљу ефикасног дељења информација дефинисане су групе корисника MISP платформе:

1. ЦЕРТ органа власти
2. ЦЕРТ-ови самосталних оператора ИКТ система
3. Посебни ЦЕРТ-ови
4. Оператори ИКТ система од посебног значаја

Оператори ИКТ система од посебног значаја могу постати корисници MISP платформе уколико су уписани у Евиденцију оператора ИКТ система од посебног значаја.



## 5.3. МИСП догађаји – картица „Events“

The screenshot shows the MISP Events interface. A user menu is open, with the 'User Guide' option highlighted in blue and pointed to by a red arrow. The background shows a list of events with various tags and filters.

**Navigation:** Event Actions, Dashboard, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, Logs, API

**Left Sidebar:**

- List Events
- Add Event
- Import from... REST client
- List Attributes
- Search Attributes
- View Proposals
- Events with proposals
- View delegation requests
- View periodic summary
- Export
- Automation

**Events List:**

- My Events
- Org Events
- Creator org
- PANW
- MORS\_142
- CERT-EE\_8833
- Axur\_4587 (multiple entries)
- SNCB-NMBS

**User Menu:**

- News
- My Profile
- My Settings
- Set Setting
- Organisations
- Role Permissions
- List Object Templates
- List Sharing Groups
- Add Sharing Group
- List Sharing Groups Blueprints
- Add Sharing Group Blueprint
- Decaying Models Tool
- List Decaying Models
- User Guide**
- Categories & Types
- Terms & Conditions
- Statistics
- List Discussions
- Start Discussion

**Event Details:**

- Tags: misp-galaxy:intrusion-set="PlugX malware", campaign, intrusion-set, Loki Bot, Lokibot, malware:name="lokibot"
- Files or Information - T1027
- Manipulation - T1134
- Phishing, tlp:green
- Ransomware (multiple entries)
- tlp:white, veris:action:social:variety="Phishing", circl:incident-classification="phishing", Phish, ecsirt:fraud="phishing", enisa:nefarious-activ



## 5.4. Додавање новог догађаја – „New MISP Event“

**Add Event**

Date: 2016-11-14 Distribution: All communities

Threat Level: Undefined Analysis: Completed

Event Info: OSINT - Researcher finds the Karma Ransomware being distributed via

GFI sandbox: Browse... No file selected.

**Add**

**Add Attribute**

Category: External analysis Type: link

Distribution: Inherit event

Value: http://www.bleepingcomputer.com/news/security/researcher-finds-the-karma-ransomware-being-distributed-via-pay-per-install-network/

Contextual Comment: Source Report

for Intrusion Detection System  Batch Import

**Submit**

- View Event
- View Event History
- Edit Event
- Delete Event
- Add Attribute **1**
- Add Attachment
- Populate from OpenIOC
- Populate from ThreatConnect
- Publish Event **5**
- Publish (no email)
- Contact Reporter
- Download as...
- List Events
- Add Event

### New MISP event

Event ID	12
Uuid	5504aaa4-3c7c-4597-b0c6-1d4bc0a8da15
Org	MYORG
Owner org	MYORG
Contributors	
Email	admin@admin.test
Tags	TLP:Green x + <b>4</b>
Date	2015-03-14
Threat Level	High
Analysis	Initial
Distribution	This community only
Description	New MISP event
<b>Published</b>	<b>No</b>

— Pivots — Attributes — Discussion

x 12: New MI... **1**

+ **2** **3**

Date	Category	Type	Value	Comment	Related Events
------	----------	------	-------	---------	----------------





РЕПУБЛИКА СРБИЈА  
**РАТЕЛ**  
РЕГУЛАТОРНО ТЕЛО ЗА  
ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ  
И ПОШТАНСКЕ УСЛУГЕ

НАЦИОНАЛНИ ЦЕРТ РС



## 6. Систем за рана упозорења

У циљу подизања нивоа ИБ у РС, Национални ЦЕРТ уводи систем за рана упозорења о претњама и ризицима у области ИБ.

Систем омогућава упозорења свим Операторима ИКТ система везано за претње и ризике прикупљене из различитих извора (Threat Intelligence).

Циљ је да се конституентима омогући правовремено преузимање одговарајућих мера заштите уз одговарајуће механизме комуникације.

### Техничке карактеристике

Систем за рана упозорења омогућава:

- прикупљање,
- обраду и
- прослеђивање

информација о претњама и ризицима у области информационе безбедности у виду раних упозорења.



## 6.1. Систем за рана упозорења – картица догађаји



### Događaji

Pregled i upravljanje događajima

✓ Otvoreni

Zatvoreni

Filter

Prioritet

Izaberite prioritet

Kategorija

Izaberite kategoriju

Vremensko razdoblje prvog pojavljivanja

Izaberite vremensko razdoblje

Vremensko razdoblje poslednjeg pojavljivanja

Izaberite vremensko razdoblje

OTKAŽI

PRIMENI

UUID događaja	Adresa	Prioritet	Status	Prvo pojavljivanje	Poslednje pojavljivanje	Broj
1fc8b6a9-a6b6-4...	79.101.30.69	Prioritet 2	Opened   Detected	20-03-2024 17:27:14	23-03-2024 18:18:34	3
0b0cc849-fa39-4...	79.101.30.79	Prioritet 2	Opened   Detected	20-03-2024 17:25:25	23-03-2024 18:18:32	3
d892f9fa-43f0-4...	79.101.30.88	Prioritet 2	Opened   Detected	20-03-2024 17:26:17	23-03-2024 18:18:29	2
5904fc17-3262-4...	79.101.30.94	Prioritet 2	Opened   Detected	19-03-2024 19:11:59	23-03-2024 18:18:28	3
9b86aa80-67f4-4...	79.101.30.85	Prioritet 2	Opened   Detected	20-03-2024 17:25:37	23-03-2024 18:18:24	3
0f6218ab-e5da-4...	79.101.30.67	Prioritet 2	Opened   Detected	20-03-2024 17:26:27	23-03-2024 18:18:22	2
db733ed8-27d8-4...	79.101.30.77	Prioritet 2	Opened   Detected	20-03-2024 17:27:13	23-03-2024 18:18:20	3
fb9f717d-0328-4...	79.101.30.88	Prioritet 2	Opened   Detected	20-03-2024 17:26:37	23-03-2024 18:18:19	6
e4c60ad9-fb8b-4...	79.101.42.230	Prioritet 2	Opened   Detected	19-03-2024 19:11:48	23-03-2024 18:17:52	2
aa236637-a407-41c4-8480-53ad30a7917a	79.101.30.91	Prioritet 2	Opened   Detected	20-03-2024 17:27:02	23-03-2024 18:17:50	4
a9699bcdf-7121-4edc-a1e6-d41a4f59cbf1	79.101.30.84	Prioritet 2	Opened   Detected	20-03-2024 17:26:28	23-03-2024 18:17:50	3
71f02564-e4fa-43ea-a883-811adc3ecdd4	79.101.30.66	Prioritet 2	Opened   Detected	20-03-2024 17:26:43	23-03-2024 18:17:41	3
19d33938-63cc-4260-b949-472db2fa72f8	79.101.42.227	Prioritet 2	Opened   Detected	19-03-2024 19:11:38	23-03-2024 18:17:34	2



Početna



Menadžment



Događaji



Podešavanja



Odjavi se



## 7.1. Сајбер претње - материјални ризик за пословање

**\$4.0M**

просечна штета  
од крађе  
података по  
једном инциденту

**81%**

последица  
**слабе или  
украдене  
шифре.**

**>300K**

малициозних  
програма се  
креира и  
дистрибуира  
сваког дана

**87%**

менаџера  
признало да су  
подаци били  
угрожени  
интерном грешком



РЕПУБЛИКА СРБИЈА  
**РАТЕЛ**  
РЕГУЛАТОРНО ТЕЛО ЗА  
ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ  
И ПОШТАНСКЕ УСЛУГЕ

НАЦИОНАЛНИ ЦЕРТ РС



## 7.2. Просечно време напада

Компромитован први хост

Domain Admin компромитован

Напад детектован

Истраживање и припрема

Неоткривен напада (преузимање података)

24-48 часова

Више од 200 дана (зависи од врсте привредног сектора)

### Софистицираност напада

Користи се свака врста слабости  
Мета може бити било који уређај или сервис



### АД и админ налози

Активни директоријум контролише приступ пословним средствима  
Најчешћи напади су на активни директоријум и налоге ИТ администратора



### Недетектовани напади

Многи алати не детектују нападе  
Ваша организација је можда тренутно под нападом



### Реакција и опоравак

Одговор на напад захтева напредна знања и алате  
Потпуни опоравак има високу цену





## 7.3. Типичан сценарио сајбер напада

Обухвата злонамерни софтвер и начин активирања и коришћења, и има следеће фазе:

- Израда и тестирање злонамерног софтвера (малвера)
- Унос малвера у информациони систем (фишинг или други метод)
- Активирање малвера (одмах или са одлагањем)
- Поступак после активирања малвера:
  - **Захтев за откуп (рансомвер)**
  - **Крађа података и/или идентитета**
  - **Давање команди рачунару (нпр. као део ДДоС напада), итд.**



## 7.4. Рансомвер

- ❑ Рансомвер (ransomware) је врста малвера (злонамерног софтвера) који закључава (шифрује) приступ подацима или мрежама и системима.
- ❑ Начин рада:
  - Шифровање фајлова: Рансомвер шифрује фајлове на уређају, онемогућавајући приступ
  - Захтев за откуп: Нападаци траже новчани откуп у облику криптовалуте за декрипцију фајлова
  - Чест је случај да датотеке чак и након плаћања откупа остају закључане.
- *Поставља се питање: Да ли платити откуп? Како поступити?*
- ❑ Ризици:
  - Губитак важних података
  - Финансијски губици
  - Компромитовање приватности
  - Трајни губитак репутације / (за фирме и тржишта) ...



## 7.4.1. Поруке рансомвер нападача

### Your personal files are encrypted by CTB-Locker.



### Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.



**WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.**

View

92 18 34

Next >>

© 2016 AO Kaspersky Lab. All Rights Reserved.

MAKTUB LOCKER

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, decryption key is stored on a secret Internet server until you pay and obtain the private key, generated for this computer.

Open <http://qjuyyhqqzfeluxe7.onion.li> or <http://qjuyyhqqzfeluxe7.torstornr> or <http://qjuyyhqqzfeluxe7.tor2web> in your browser. They are public gates to the Internet.

If you have problems with gates, use direct

- 1) Download TOR Browser from [www.torproject.org](http://www.torproject.org)
- 2) In the Tor Browser open the <http://qjuyyhqqzfeluxe7.onion.li> (Note that this server is available via Tor Browser only).

Write in the following public key in the input field:

```

c3d17e-3c8730-c22226-d196d0-c88677-789684-592770-5c7
88342-882320-790526-232805-c82007-869202-398005-379604-848897-952790-802777-828077-868890-876489
895986-182888-770577-895530-860037-c87688-898446-307845-358896-803303-c89278-473228-888850-c80050
8VQ8G-LE88X-CT857-8530C-02868G-22984-07E9D-8778M-59861-0874N-0468N-DBACS-DZJD0-6ETD0
887ED-0V7FA-87969V-86877K-08457F-37077E-07072D-905305-45227D-286877-724971-800989-8956E6-83433
8782F-0308D-82F6E-37290V-87072N-80580Z-02843-7903D-82888V-210855-128024-0V1A0

```

Copy Public Key to Clipboard

© 2016 AO Kaspersky Lab. All Rights Reserved.

### Your personal files are encrypted!

Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key**.

The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.

**Once this has been done, nobody will ever be able to restore files...**

In order to decrypt the files open your personal page on site <https://34r6hq26q2h4jkzj.tor2web.fi> and follow the instruction.

Use your Bitcoin address to enter the site:  
[1K7Q5TrFxFqCEmzocfxn8Lfrxvdb39Uvm](https://34r6hq26q2h4jkzj.tor2web.fi)

Click to copy Bitcoin address to clipboard

If <https://34r6hq26q2h4jkzj.tor2web.org> is not opening, please follow the steps: You must install this browser [www.torproject.org/projects/torbrowser.html.en](http://www.torproject.org/projects/torbrowser.html.en) After installation, run the browser and enter address [34r6hq26q2h4jkzj.onion](https://34r6hq26q2h4jkzj.onion) Follow the instruction on the web-site. We remind you that the sooner you do, the more chances are left to recover the files.

**Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.**

Show encrypted files    Check Payment    Enter Decrypt Key

Click to Free Decryption on site

© 2016 AO Kaspersky Lab. All Rights Reserved.



## 7.4.1. Како поступити ако се деси напад?

<https://www.nomoreransom.org>

<img alt="lock icon" data-bbox="118 385 145 410"/> / > **NO MORE RANSOM**

Partners About the Project English

Home Crypto Sheriff Ransomware: Q&A Prevention Advice Decryption Tools Report a Crime

**NEED HELP**  
unlocking your digital  
life without paying  
your attackers\*?

YES NO

At the moment, not every type of ransomware has a solution. Keep checking this website as new keys and applications are added when available.

Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom.

**However this is not guaranteed and you should never pay!**

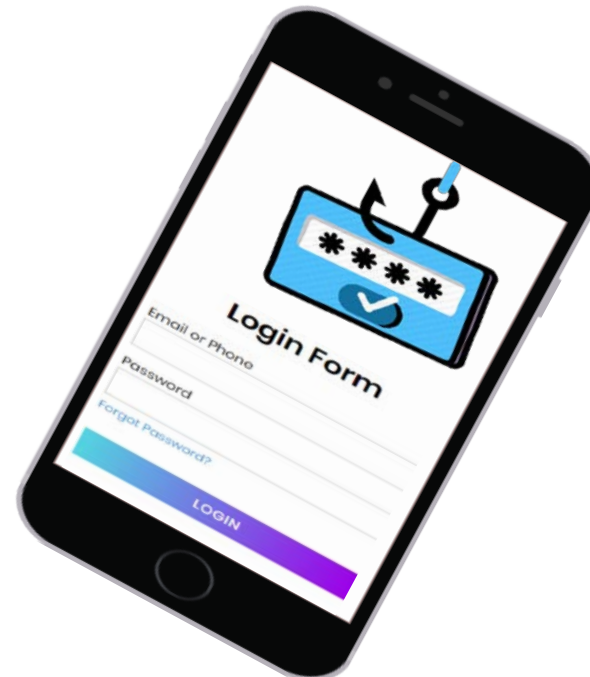
<img alt="lock icon" data-bbox="665 810 685 840"/> New decryptor for **SynAck** available, please click here. >





## 7.5. Фишинг – дефиниција и циљеви (1)

- ❑ Фишинг („phishing - пецање“) је врста социјалног инжењеринга где нападачи користе обмањујуће имејлове и СМС поруке („smishing“) и/или глас („vishing“) да би преварили жртве да открију осетљиве информације или инсталирају малвер.
- ❑ Циљеви фишинга:
  - Крађа идентитета,
  - приступ банковним налозима,
  - инсталација малвера, итд.



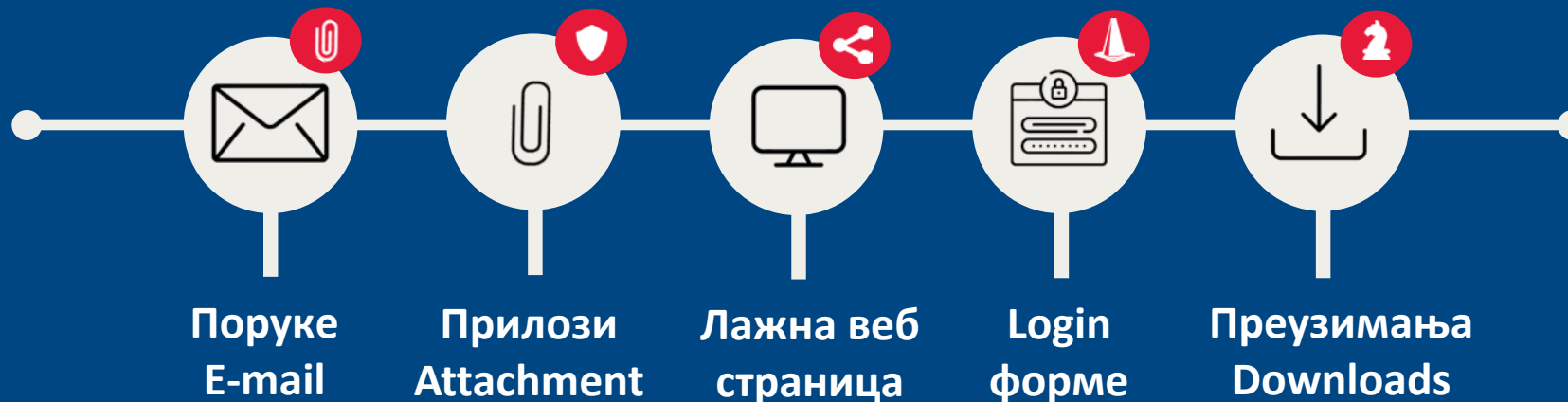
## 7.5. Фишинг – методе и карактеристике (2)

### ☐ Методе инфекције:

- *Имејлови: Лажни имејлови који захтевају "хитну акцију"*
- *СМС поруке („smishing“): Кратке поруке које воде ка малициозним сајтовима*
- *Глас или гласовне поруке („vishing“)*

### ☐ Карактеристике фишинга:

- *Обмањујући садржај: Имитирање познатих компанија / организација / особа*
- *Замке: Линкови или прилози (Attachment) које нуде кориснику (да преузме - download)*
- *Усмеравају корисника на: фалсификовани веб-сајт*





## 7.5. Фишинг - превенција и заштита (3)

- *Обука запослених о препознавању фишинг покушаја*
- *Употреба анти-фишинг филтера у имејл системима*

### **Статистика и трендови:**

- *Статистике показују стални пораст обима фишинг напада*
- *Фишинг кампање стоје иза највећих инфекција малвером*
- **Фишинг је главни извор малвера, укључујући рансомвер**



## 7.5. Препознавање фишинга (4)

### 1 НАСЛОВ Е-ПОРУКЕ:

Обратити пажњу да ли наслов има везе са нашим послом или интересовањима и да ли је одговор на нешто што нисмо тражили

### 2 FROM:

Име пошиљаоца није повезано са имејл адресом

### 3 TO:

Нису познате адресе на које се шаљу е-поруке

### 4 ПРИЛОГ

Садржи прилог или линк чије се отварање захтева

1 → **Савет у случају плаћања дознаке**

2 → **AT** Accounts te Betalen <attariya@picl.com.np>  
To undisclosed-recipients 2/4/2020

3 →

4 → **Untitled attachment 00019.txt**  
129 bytes

5 → **Велики поздрав,**  
Ово је праћење уплате коју смо у име нашег клијента извршили у вашој банци приматеља 4.2.2020. Сажетак брзе копије и сажетка банковног трансфера је у прилогу. Молимо вас саветујте да ли су се средства одразила на вашој страни и ажурирајте трећу страну коју сте примили.

6 →

7 → **Поздрави,**  
Госпођица Јане Аттарија  
Одљење за рачуне и дознаке  
ПИЦЛ глобално плаћање на мрежи,  
Фак + 56890-0906  
Србија

### 5 ДОМЕН:

Назив домена је **.np** а пошиљалац се представља да је из Србије

Увек обратити пажњу да ли је домен познат

### 6 ТЕКСТ

Учити:

- Граматичке грешке
- Лош превод појмова
- Захтев за брзу реакцију
- Захтев за унос личних података

### 7 ПОТПИС:

Име фирме у потпису се делимично поклапа са доменом из е-адресе



## 8.1. SIEM платформе

### ❑ SIEM (Security information and event management)

је софтверско решење које омогућава организацијама да:

- открију (**detect**),
- анализирају (**analyze**) и
- реагују (**respond**)

на безбедносне претње пре него што оне нанесу штету пословним операцијама.

### ❑ SIEM је техничка подршка за рад Оперативног центра за информациону безбедност **SOC (Security Operations Center)**.





## 9.1. Најважније поруке

### Основне поруке:

- Сајбер претње треба схватити озбиљно
- На време предузети систематске мере за спречавање успешних напада и њихових последица
- **Процес развоја ИБ треба реализовати паралелно са процесом изградње Информационог система**
- Пратити догађања на пољу ИБ и прилагођавати им се, размишљајући о управљању безбедносним ризицима као важном делу редовног пословања
- **Пажљиво бирати ИКТ партнере** - оне који разумеју специфичности вашег пословања



## 9.2. За крај

У којој мери поштујемо безбедносна правила и добру праксу?

Питања за Операторе ИКТ система?

- Да ли користите легалне системске и апликативне софтвере и редовно их печујете?
- Да ли имате квалитетно антивирусно или друго безбедносно решење примењено у целом систему?
- Да ли сте спречили да више корисника користи један налог?
- Да ли спроводите мере измене и заштите лозинки?
- Да ли сте сигурни да бивши запослени више немају приступ систему?
- Да ли администраторска права различитог нивоа имају само они којима су стварно неопходна?
- Да ли користите двофакторску аутентификацију (проверу права приступа - 2FA) за приступ критичним ресурсима?
- Да ли спроводите редовне обуке ради подизања свести о информационој безбедности (security awareness)?
- Да ли имате прописане и спроведене бар најосновније безбедносне процедуре? (одбрана од напада, бекап, ...)



### 9.3. Везано за бекап података - „посебан акценат“:

- **Да ли редовно, довољно често и детаљно вршите бекап података?**
- Да ли су вам подаци класификовани?
- Да ли је процес бар делимично аутоматизован?
- Да ли правите више копија?
- Да ли копије повремено проверавате?
- Да ли је бар једна копија ван активних сервера?
- Да ли је бар једна трајна копија на удаљеној безбедној локацији? ...





РЕПУБЛИКА СРБИЈА  
**РАТЕЛ**  
РЕГУЛАТОРНО ТЕЛО ЗА  
ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ  
И ПОШТАНСКЕ УСЛУГЕ

НАЦИОНАЛНИ ЦЕРТ РС



**ХВАЛА НА ПАЖЊИ !**

*др Горан Пауновић*

Главни саветник за безбедност ИКТ система  
Служба за ИБ и послове Националног ЦЕРТ-а,

РАТЕЛ

[goran.paunovic@ratel.rs](mailto:goran.paunovic@ratel.rs)

[www.cert.rs](http://www.cert.rs)