РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНО ТЕЛО ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

СРБ-ЦЕРТ

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
www.cert.rs

С А Д Р Ж А Ј:

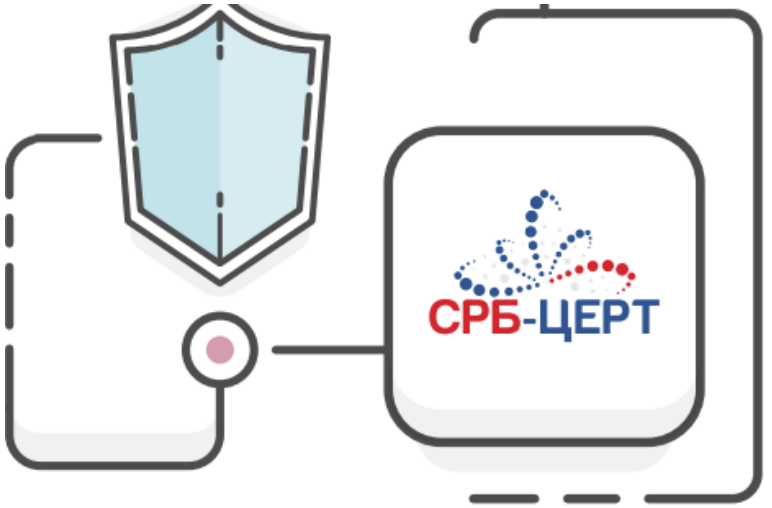
1.1. Законски оквир за формирање Националног ЦЕРТ-а

- Закон о информационој безбедности усвојен - 2016. године

- У складу са Законом о информационој безбедности:

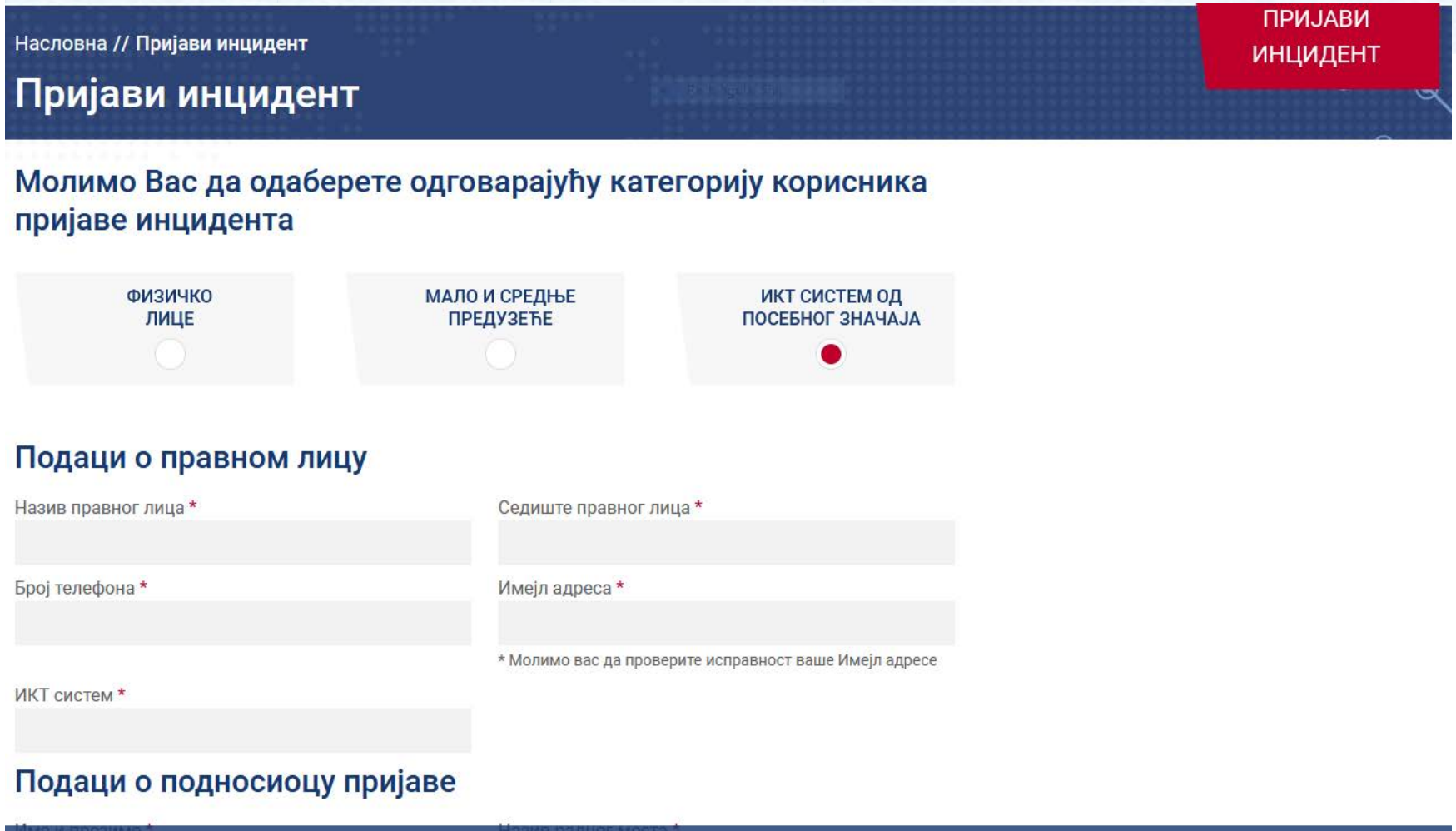
  - Национални ЦЕРТ - Национални центар за превенцију безбедносних ризика у ИКТ системима Републике Србије - почео са радом 2017. године

  - Делује у оквиру РАТЕЛ-а, (Регулаторног тела за електронске комуникације и поштанске услуге)



1.2. Надлежности Националног ЦЕРТ-а

2. Пријава инцидената Националном ЦЕРТ-у



info@cert.rs

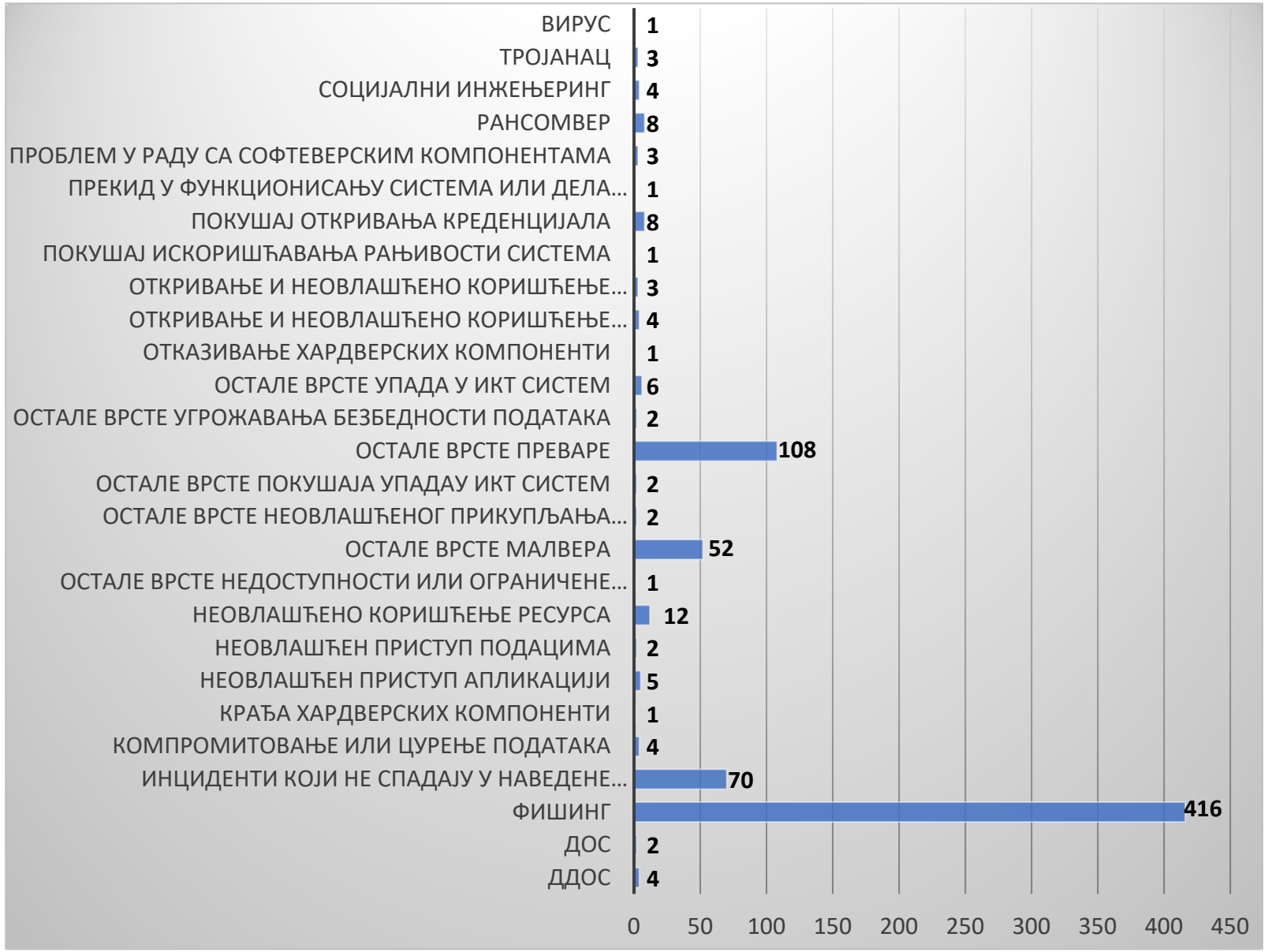
062/20-20-30

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

РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНО ТЕЛО ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

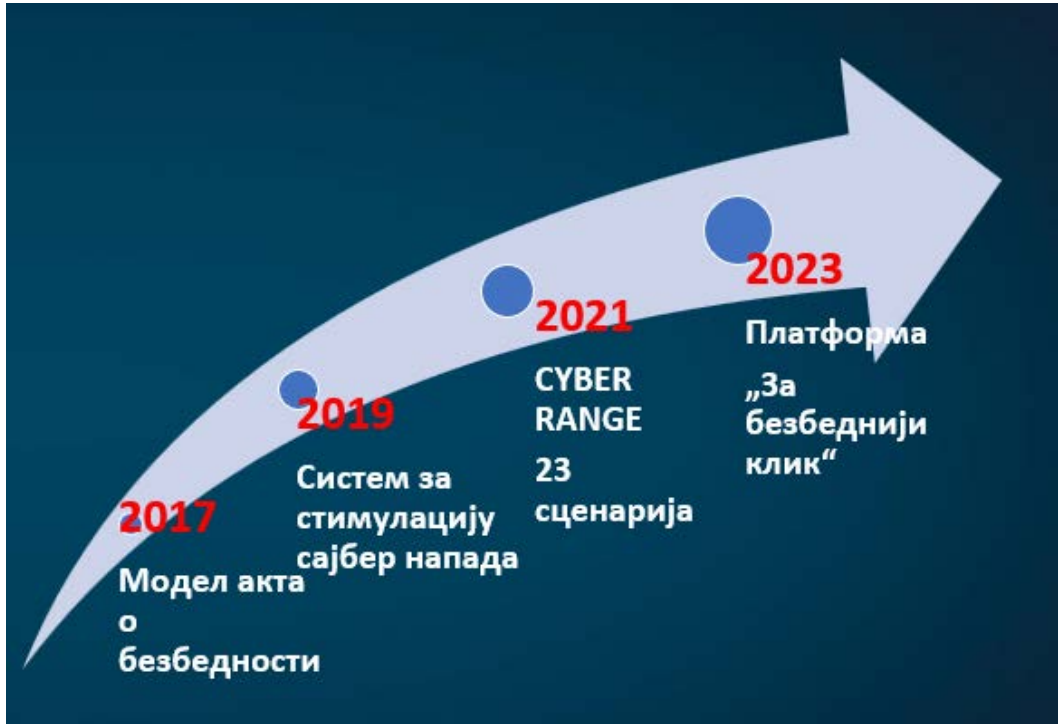
3.2. Пријављени инциденти Н ЦЕРТ-у
по врстама инцидената (2023. г)

СРБ-ЦЕРТ



4. Едукација и подизање свести из области информационе безбедности

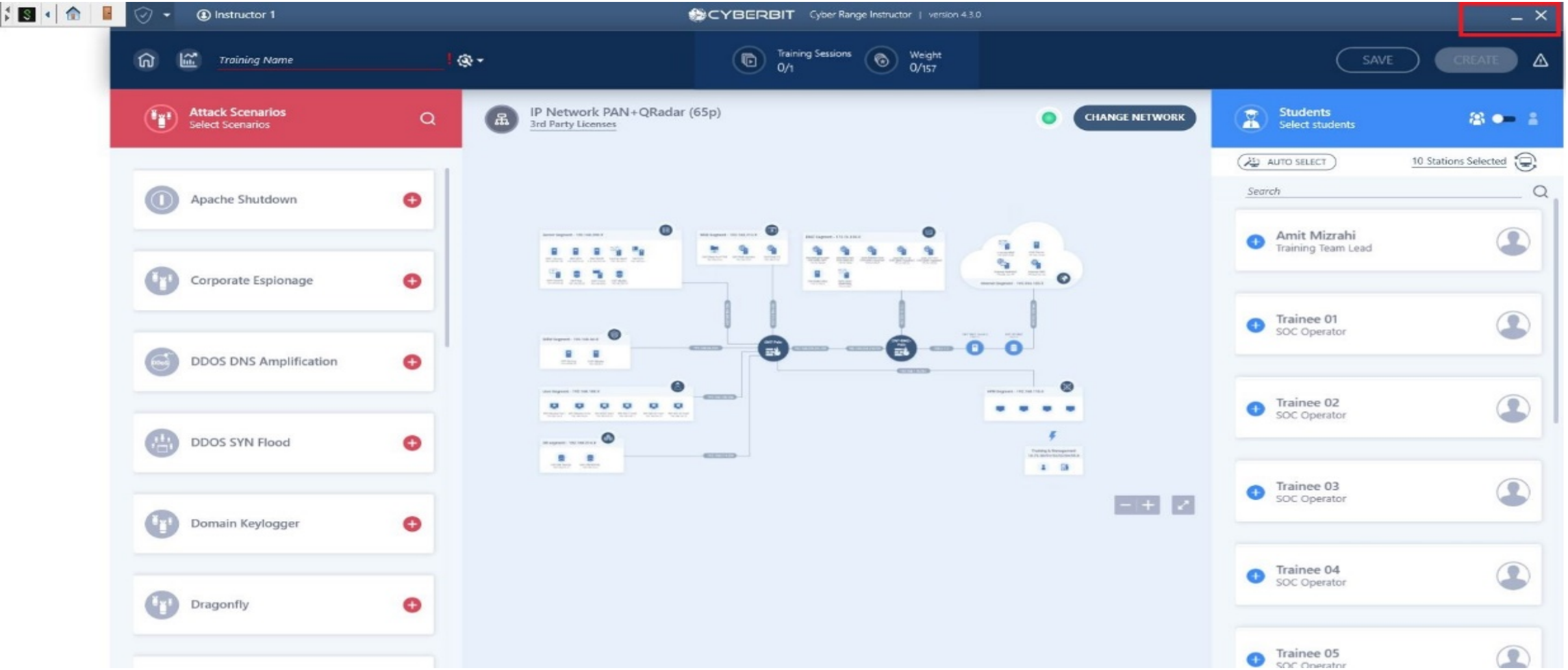
- Разумевање технологије
- Имплементација мера заштите
- Унапређење вештина и подизање нивоа знања
- Детекција и реакција на критичне безбедносне активности



РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНО ТЕЛО ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

СРБ-ЦЕРТ

4.1. Cyberbit обуке – за техничка лица



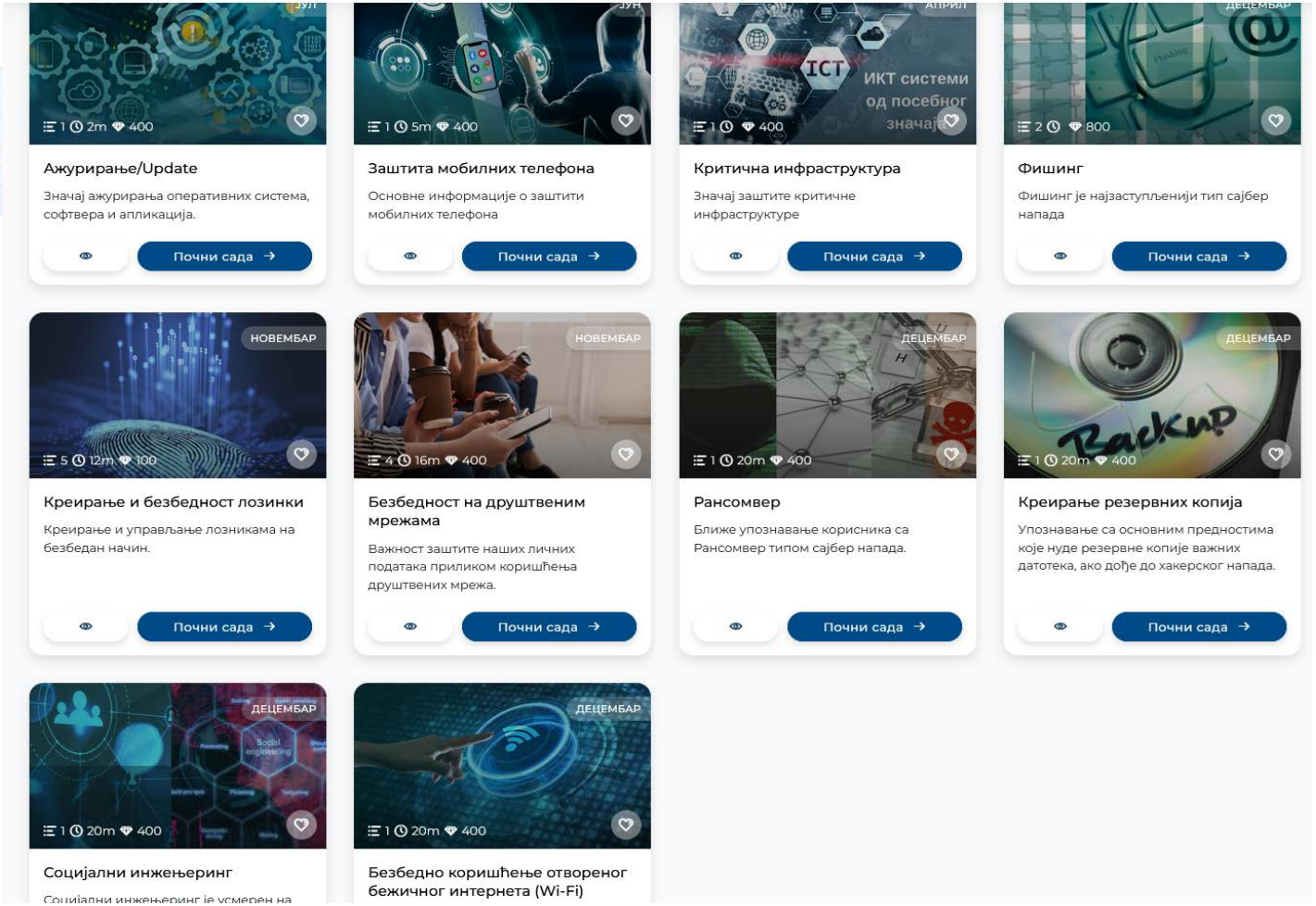
РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНО ТЕЛО ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

НАЦИОНАЛНИ ЦЕРТ РС

СРБ-ЦЕРТ

4.2 Платформа за безбеднији клик

https://learn.cert.rs/



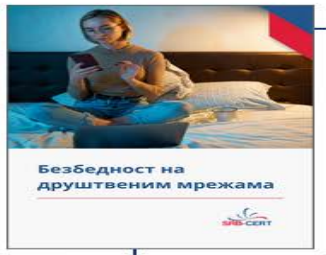
4.3. Публикације Националног ЦЕРТ-а

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

- 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

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

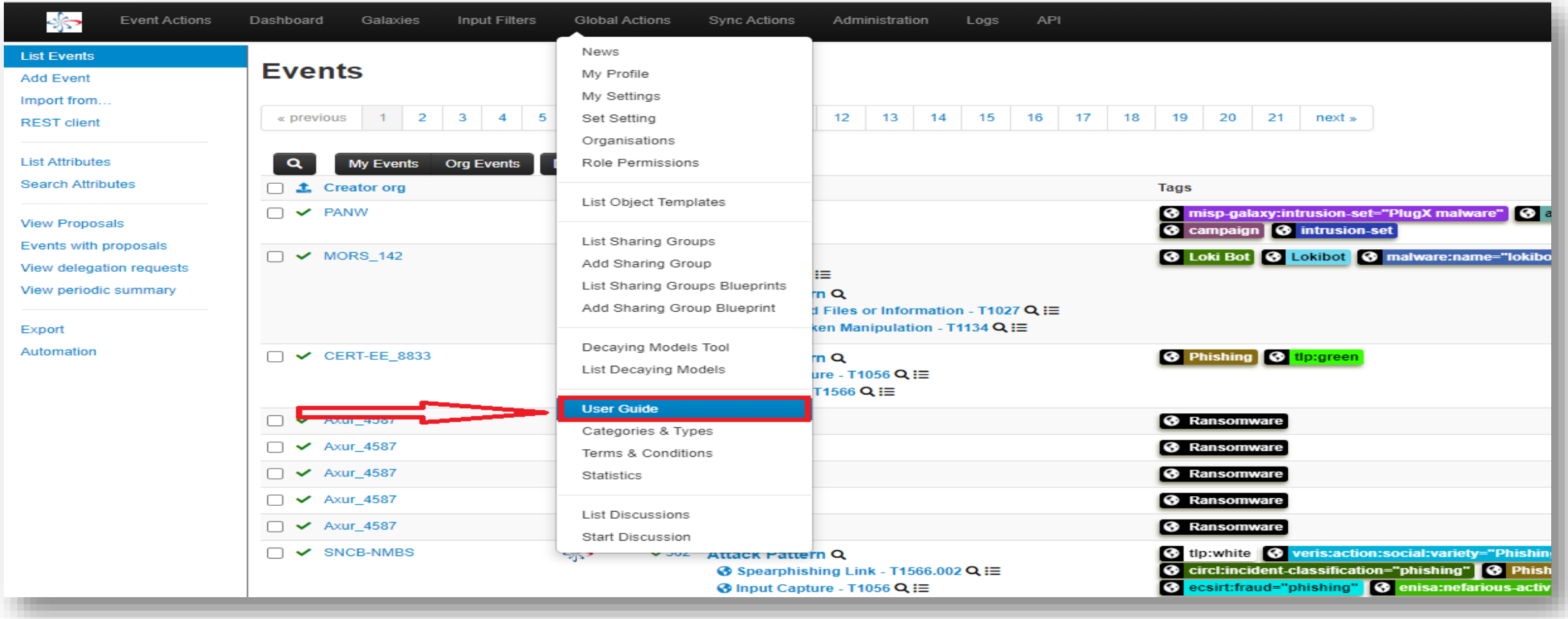
Корисници MISP платформе су релевантне институције у области ИБ, које за коришћење платформе именују представнике. Информације се деле са циљем да се дефинишу мера заштите и начин реаговања.

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

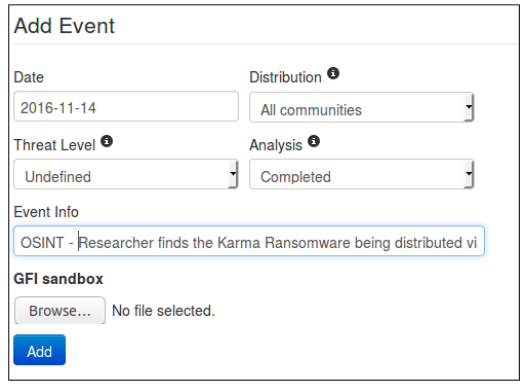
1. ЦЕРТ органа власти
2. ЦЕРТ-ови самосталних оператора ИКТ система
3. Посебни ЦЕРТ-ови
4. Оператори ИКТ система од посебног значаја

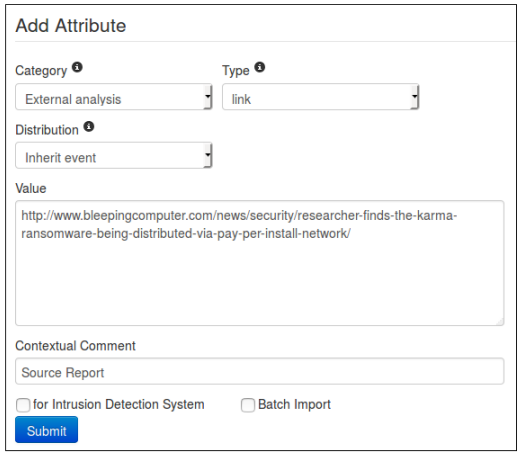
Оператори ИКТ система од посебног значаја могу постати корисници MISP платформе уколико су уписани у Евиденцију оператора ИКТ система од посебног значаја.

5.3. МИСП догађаји – картица „Events“



5.4. Додавање новог догађаја – „New MISP Event“





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.

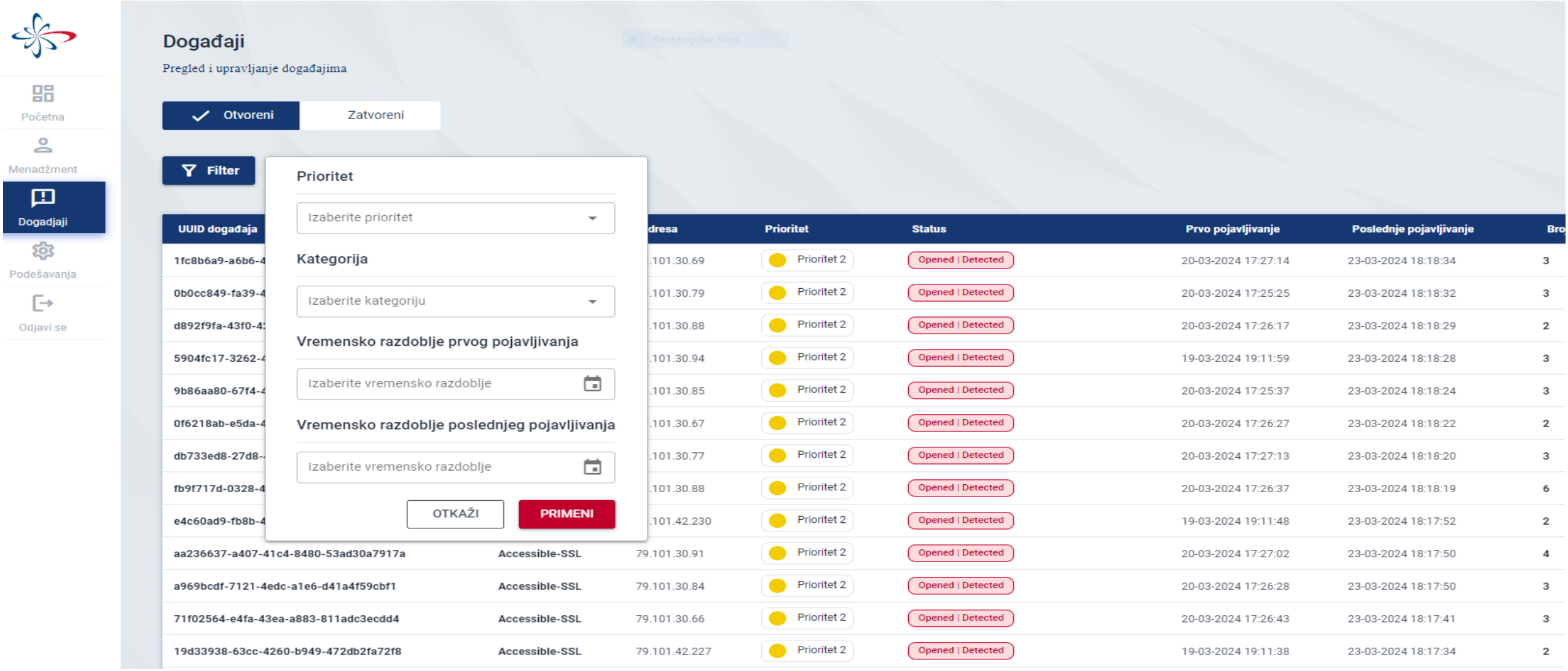
Техничке карактеристике

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



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%

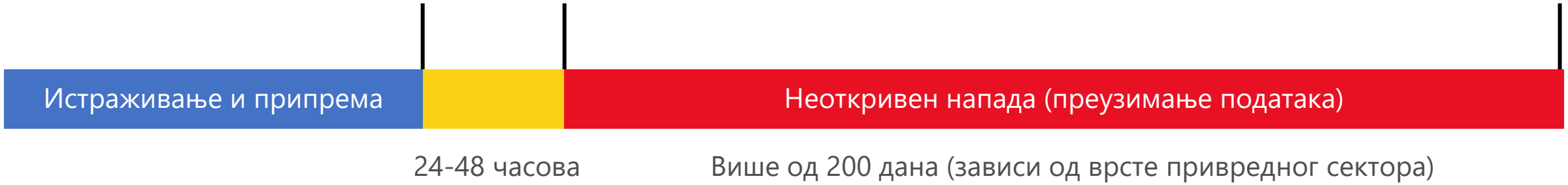
менаџера признало да су подаци били угрожени интерном грешком

РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНО ТЕЛО ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

НАЦИОНАЛНИ ЦЕРТ РС

СРБ-ЦЕРТ

7.2. Просечно време напада



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

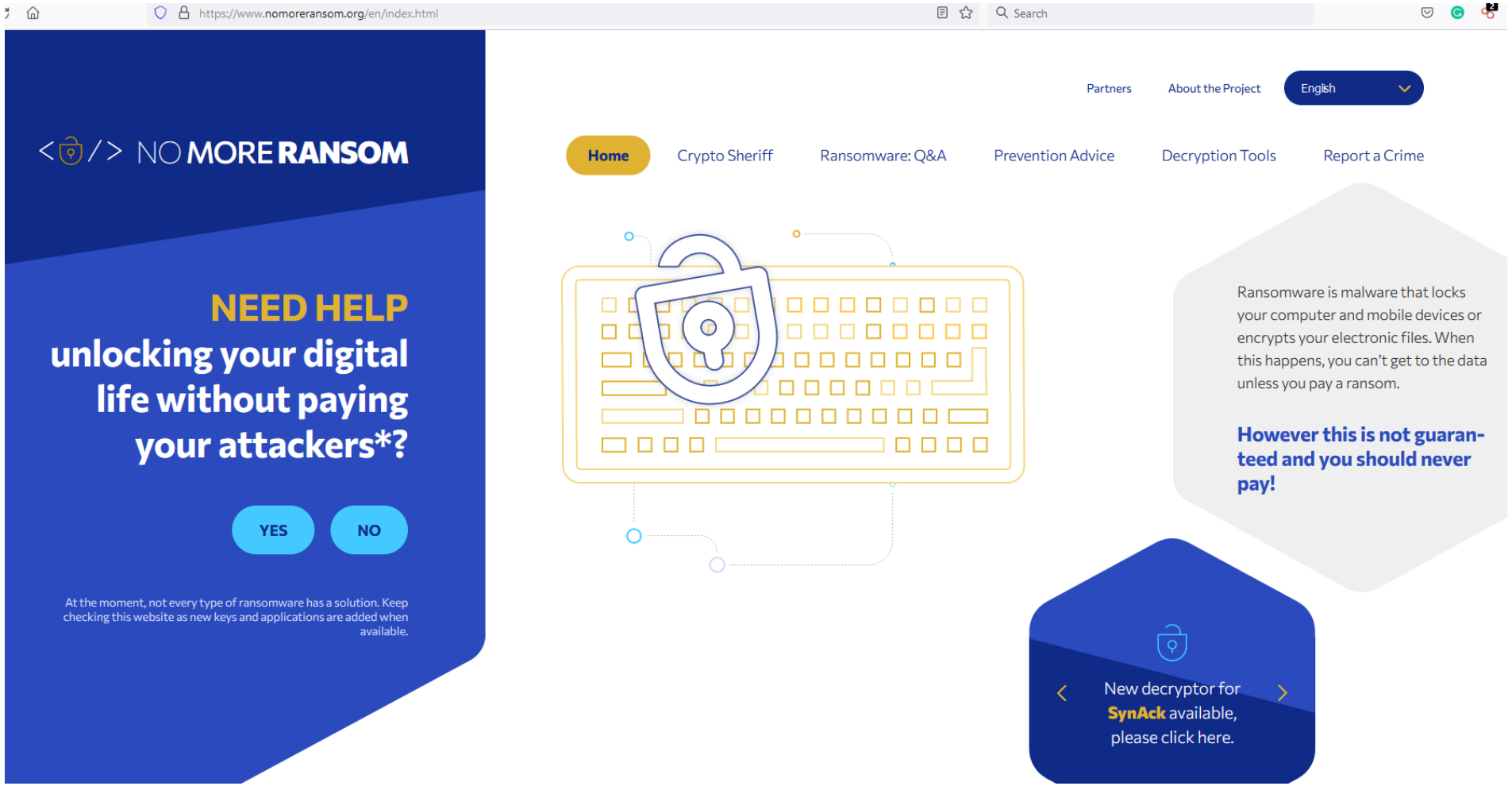
- Рансомвер (ransomware) је врста малвера (злонамерног софтвера) који закључава (шифрује) приступ подацима или мрежама и системима.
- Начин рада:
  - Шифровање фајлова: Рансомвер шифрује фајлове на уређају, онемогућавајући приступ
  - Захтев за откуп: Нападачи траже новчани откуп у облику криптовалуте 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

7.4.1. Како поступити ако се деси напад?

https://www.nomoreransom.org

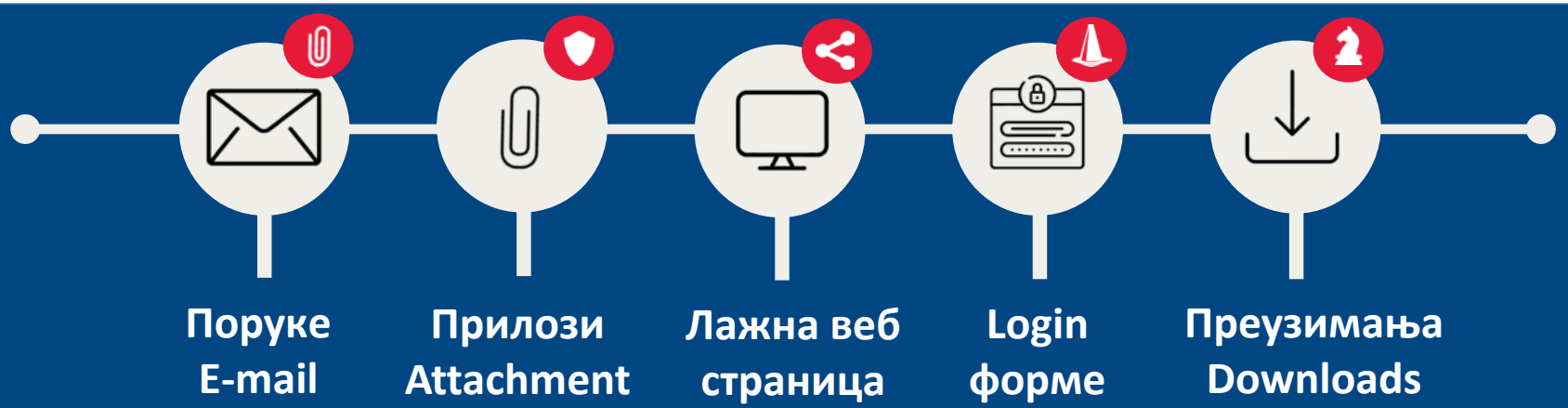


7.5. Фишинг – дефиниција и циљеви (1)

- **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

РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНО ТЕЛО ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

НАЦИОНАЛНИ ЦЕРТ РС

СРБ-ЦЕРТ

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:

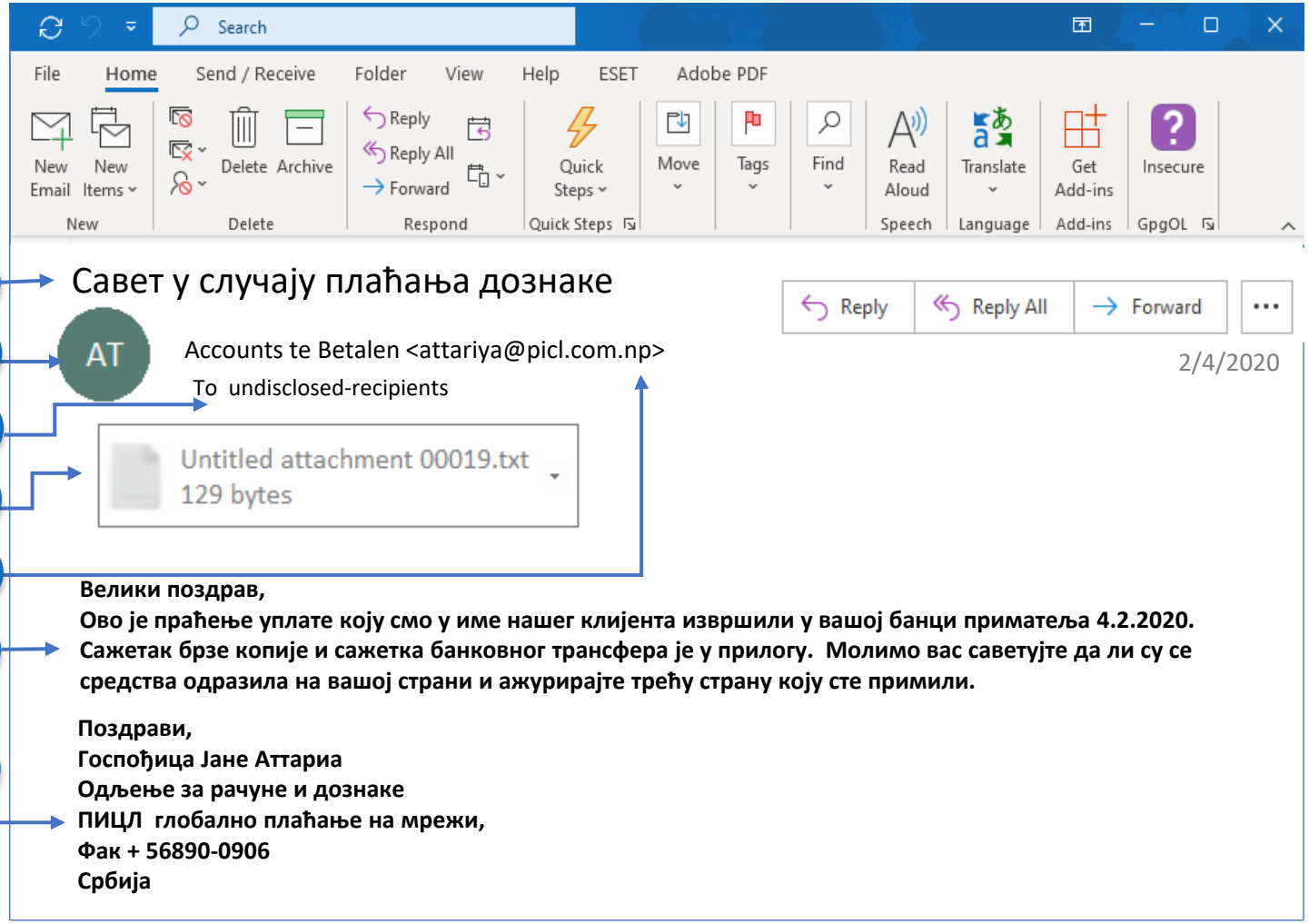
Име пошиљаоца није повезано са имејл адресом

3 TO:

Нису познате адресе на које се шаљу е-поруке

4 ПРИЛОГ

Садржи прилог или линк чије се отварање захтева



5 ДОМЕН:

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

Увек обратити пажњу да ли је домен познат

6 ТЕКСТ

Уочити:

- **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:
  - откријy (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? ...

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
www.cert.rs