ИЗВЕШТАЈ О СТАТИСТИЧКИМ ПОДАЦИМА О СВИМ ИНЦИДЕНТИМА У ИКТ СИСТЕМИМА ОД ПОСЕБНОГ ЗНАЧАЈА У 2022. ГОДИНИ

Јун, 2023. година

РАТЕЛ

СРБ-ЦЕРТ

Национални ЦЕРТ Републике Србије www.cert.rs

Садржај

Увод 3

1. Оператори ИКТ система од посебног значаја 4

2. Преглед према групи инцидената 9

3. Преглед према врсти инцидената 11

4. Преглед према врсти ИКТ система од посебног значаја 22

4.1. ИКТ системи од посебног значаја који се користе у обављању послова у органима власти 23

4.2. ИКТ системи од посебног значаја који се користе за обраду посебних врста података о личности, у смислу закона који уређује заштиту података о личности 24

4.3. ИКТ системи од посебног значаја који се користе у обављању делатности од општег интереса и другим делатностима 25

4.3.1. Енергетика 25

4.3.2. Саобраћај 26

4.3.3. Здравство 27

4.3.4. Банкарство и финансијска тржишта 28

4.3.5. Дигитална инфраструктура 29

4.3.6. Добра од општег интереса који се односе на коришћење, управљање, заштиту и унапређење добара 30

4.3.7. Услуге информационог друштва 31

4.3.8. Остале области 32

4.3.8.1. Електронске комуникације 33

4.3.8.2. Издавање службеног гласила 34

4.3.8.3. Управљање нуклеарним објектима 35

4.3.8.4. Производња, промет и превоз нуклеарног наоружања и војне опреме 35

4.3.8.5. Управљање отпадом 36

4.3.8.6. Комуналне делатности 37

4.3.8.7. Производња и снабдевање хемикалијама 38

4.4. ИКТ системи од посебног значаја који се користе у правним лицима које оснива Република Србија, аутономна покрајина или јединица локалне самоуправе за обављање делатности од општег интереса 39

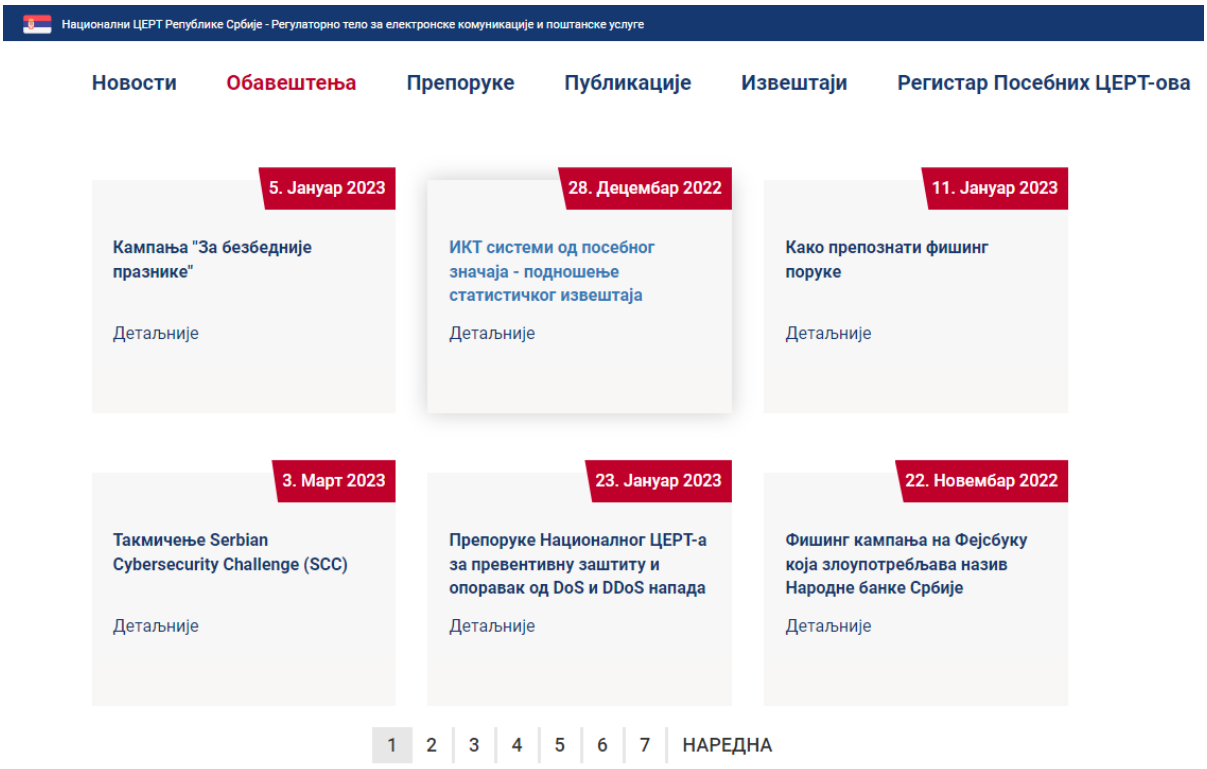
5. Закључак 40

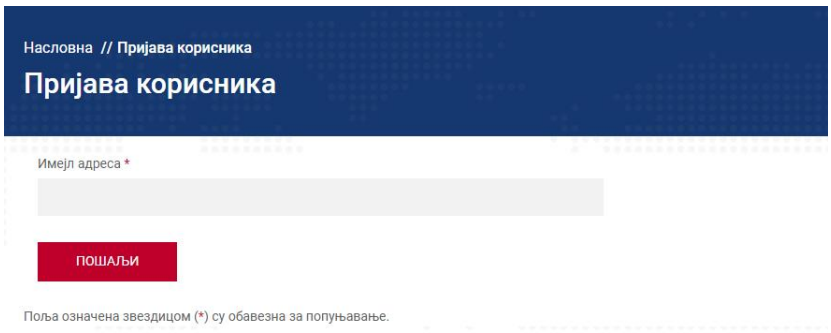
Увод

У складу са чланом 11б. Закона о информационој безбедности Национални центар за превенцију безбедносних ризика у ИКТ системима (у даљем тексту: Национални ЦЕРТ) је, почев од јануара 2023. године, прикупљао статистичке податке о свим инцидентима у ИКТ системима од посебног значаја за 2022. годину. Овим одредбама Закона оператори ИКТ система од посебног значаја обавезани су да Националном ЦЕРТ-у доставе тачне статистичке податке о свим инцидентима у ИКТ систему за претходну годину најкасније до 28. фебруара текуће године.

Врсту, форму и начин достављања ових података Национални ЦЕРТ је утврдио Правилником о врсти, форми и начину достављања статистичких података („Службени гласник РС“, број 76/20) којим је прописан и Образац ИСП - Извештај о статистичким подацима о свим инцидентима у ИКТ системима од посебног значаја, а који, поред података о оператору ИКТ система од посебног значаја, садржи и листу инцидената према врстама.

Подаци су достављени кроз веб апликацију (Слика 1) коју је Национални ЦЕРТ успоставио. Операторима ИКТ система од посебног значаја је достављено и упутство за креирање налога и достављање статистичких података које садржи препоруке и смернице којим би требало да се руководе администратори система приликом утврђивања карактеристика стварног негативног утицаја свих врста напада на њихов ИКТ систем. На овај начин је Национални ЦЕРТ пружио подршку операторима ИКТ система у испуњавању ове законске обавезе.





Слика 1 - Веб апликација за достављање статистичких података

1. Оператори ИКТ система од посебног значаја

Оператори ИКТ система од посебног значаја су правна лица, органи власти или организационе јединице органа власти који користе ИКТ систем у оквиру своје делатности. Законом о информационој безбедности дефинисане су врсте ИКТ система од посебног значаја:

1) ИКТ системи од посебног значаја који се користе у обављању послова у органима власти
2) ИКТ системи од посебног значаја који се користе за обраду посебних врста података о личности, у смислу закона који уређује заштиту података о личности

3) ИКТ системи који се користе у обављању делатности од општег интереса и другим делатностима и то у следећим областима:
   1. Енергетика
   2. Саобраћај
   3. Здравство
   4. Банкарство и финансијска тржишта
   5. Дигитална инфраструктура
   6. Добра од општег интереса коришћење, управљање, заштита и унапређење добара од општег интереса (воде, путеви, минералне сировине, шуме, пловне реке, језера, обале, бање, дивљач, заштићена подручја)
   7. Услуге информационог друштва
   8. Остале области
4) ИКТ системи од посебног значаја који се користе у правним лицима и установама које оснива Република Србија, аутономна покрајина или јединица локалне самоуправе за обављање делатности од општег интереса

Листа делатности у областима у којима се обављају делатности од општег интереса дефинисана је Уредбом о утврђивању листе делатности од општег интереса и у којима се користе информационо-комуникациони системи од посебног значаја (Табела 1).

Евиденцију оператора ИКТ система од посебног значаја води Министарство трговине, туризма и телекомуникација, а Правилником о подацима које садржи евиденција оператора информационо-комуникационих система од посебног значаја утврђени су подаци које ова Евиденција садржи.

Слика 1.1 - ИКТ системи од посебног значаја

ЛИСТА ДЕЛАТНОСТИ		
Област	**Делатност**	
1) ЕНЕРГЕТИКА	(1) производња, пренос и дистрибуција електричне енергије, у смислу закона којим се уређује енергетика:	- производња електричне енергије: - снабдевање електричном енергијом, укључујући снабдевање на велико; - пренос и управљање преносним системом електричне енергије; - дистрибуција електричне енергије и управљање дистрибутивним системом електричне енергије; - управљање организованим тржиштем електричне енергије.
	(2) производња и прерада угља, у смислу закона којим се уређује рударство:	- експлоатација угља.
	(3) истраживање, производња, прерада, транспорт и дистрибуција нафте и промет нафте и нафтних деривата:	- енергетске делатности: производња деривата нафте; транспорт нафте нафтоводима; транспорт деривата нафте продуктоводима; транспорт нафте и дериват нафте другим облицима транспорта; трговина нафтом и дериватима нафте, у смислу закона којим се уређује енергетика; - експлоатација нафте, у смислу закона којим се уређује рударство.

	(4) истраживање, производња, прерада, транспорт и дистрибуција природног и течног гаса:	- снабдевање природним гасом, у смислу закона којим се уређује енергетика; - јавно снабдевање природним гасом, у смислу закона којим се уређује енергетика; - транспорт природног гаса и управљање транспортним системом за природни гас, у смислу закона којим се уређује енергетика; - дистрибуција природног гаса и управљање дистрибутивним системом природног гаса, у смислу закона којим се уређује енергетика; - складиштење и управљање складиштем природног гаса, у смислу закона којим се уређује енергетика; - експлоатација природног гаса, у смислу закона којим се уређује рударство.
2) САОБРАЋАЈ	(1) железнички саобраћај, у смислу закона којим се уређује железница:	- управљање јавном железничком инфраструктуром; - јавни превоз у железничком саобраћају.
	(2) поштански саобраћај, у смислу закона којим се уређује поштански саобраћај:	- поштанске услуге које обавља јавни поштански оператор.
	(3) водни саобраћај, у смислу закона којим се уређује пловидба и луке на унутрашњим водама:	- техничко одржавање међународних, међудржавних и државних водних путева; - управљање лукама и пристаништима и лучка делатност.
	(4) ваздушни саобраћај, у смислу закона о ваздушном саобраћају:	- аеродромске услуге; - контрола летења; - јавни авио-превоз.

3) ЗДРАВСТВО	(1) здравствена заштита, у смислу закона којим се уређује здравствена заштита:	- здравствена делатност коју обављају здравствене установе и друга правна лица која обављају здравствену делатност.
4) БАНКАРСТВО И ФИНАНСИЈСКА ТРЖИШТА	(1) послови финансијских институција:	- послови финансијских институција, у смислу закона којим се уређује Народна банка, над којима надзор, односно контролу, у складу са законом, врши Народна банка.
	(2) послови вођења регистра података о обавезама физичких и правних лица према финансијским институцијама;	
	(3) послови управљања, односно обављања делатности у вези са функционисањем регулисаног тржишта, у смислу закона којим се уређује тржиште капитала.	
5) ДИГИТАЛНА ИНФРАСТРУКТУРА	(1) услуге размене интернет саобраћаја (енгл. „internet exchange point”);	
	(2) управљање регистром националног интернет домена и системом за именовање на мрежи (ДНС системи).	
6) ДОБРА ОД ОПШТЕГ ИНТЕРЕСА КОЈИ СЕ ОДНОСЕ НА КОРИШЋЕЊЕ, УПРАВЉАЊЕ, ЗАШТИТУ И УНАПРЕШЕЊЕ ДОБАРА ОД ОПШТЕГ ИНТЕРЕСА	(1) воде, у смислу закона којим се уређују воде:	- управљање водама као и водним објектима и водним земљиштем у јавној својини; - водна делатност.
	(2) путеви, у смислу закона којим се уређују јавни путеви:	- управљање јавним путем.
	(3) минералне сировине, у смислу закона којим се уређује рударство:	- експлоатација минералних сировина.
	(4) шуме, у смислу закона којим се уређују шуме:	- газдовање шумама у државној својини.
	(5) пловне реке, језера и обале, у смислу закона којим се уређује пловидба и луке на унутрашњим водама	
	(6) бање, у смислу закона којим се уређују бање:	- очување, коришћење, унапређење и управљање бањама.
	(7) дивљач, у смислу закона којим се уређује дивљач и ловство:	- делатност коришћења, управљања, заштите и унапређивања популације дивљачи и њихових станишта.

	(8) заштићена подручја, у смислу закона којим се уређују национални паркови:	- управљање националним парковима
7) УСЛУГЕ ИНФОРМАЦИОНОГ ДРУШТВА	(1) услуге платформи за трговину путем интернета, у смислу закона којим се уређује електронска трговина;	
	(2) услуге претраживања интернета, у смислу закона којим се уређује електронска трговина	
	(3) услуге складиштења података корисника услуга (енгл. „cloud computing service"), у смислу закона којим се уређује електронска трговина.	
8) ОСТАЛЕ ОБЛАСТИ	(1) електронске комуникације, у смислу закона којим се уређују електронске комуникације:	- делатност електронских комуникација
	(2) издавање службеног гласила Републике Србије, у смислу закона којим се уређује објављивање закона и других прописа и аката:	- издавање службеног гласника.
	(3) управљање нуклеарним објектима, у смислу са закона којим се уређује заштита од јонизујућег зрачења и нуклеарна сигурност:	- управљање нуклеарним објектима.
	(4) производња, промет и превоз наоружања и војне опреме, у смислу закона којим се уређује производња, промет и превоз наоружања и војне опреме:	- производња наоружања и војне опреме; - промет наоружања и војне опреме; - превоз наоружања и војне опреме.

Табела 1 – Листа делатности

2. Преглед према групи инцидената

Оператори ИКТ система од посебног значаја су своје тачне и ажурне статистичке податке о свим инцидентима у ИКТ системима доставили у периоду од 01.01. до 28.02.2023. године, у складу са Законом о информационој безбедности и Правилником о врсти, форми и начину достављања статистичких података.

У табели 2.1 дат је приказ броја инцидената према групама инцидената, док је у графикону 2.1 приказано првих пет најзаступљенијих група инцидената.

	Група инцидената	Број инцидената
1.	Неовлашћено прикупљање података	7.696.766
2.	Покушај упада у ИКТ систем	2.979.577
3	Превара	58.417
4.	Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. *malware*)	54.780
5.	Оперативни инциденти	13.322
6.	Недоступност или ограничена доступност ИКТ система	2.405
7.	Упад у ИКТ систем	2.029
8.	Остали инциденти	1.346
9.	Инциденти физичко техничке безбедности	178
10.	Угрожавање безбедности података	18
	УКУПНО	**10.808.838**

Табела 2.2 – Број инцидената према групама инцидената

Најзаступљенија група инцидената је неовлашћено прикупљање података (7.696.766), у оквиру које је најдоминантнија врста инцидента скенирање портова. На другом месту је покушај упада у ИКТ систем (2.979.577) у оквиру које је најзаступљенији инцидент откривање или неовлашћено коришћење неприивилегованих налога. На трећем месту се налази превара (58.417) чији највећи број чини фишинг. Четврто место заузима инсталирање злонамерног софтвера у оквиру ИКТ система (54.780) најчешће тројанац. На петом месту су оперативни инциденти (13.322) и то у највећем броју проблеми у раду са софтверским компонентама (Графикон 2.1).

Графикон 2.1 – Пет најбројнијих група инцидената

3. Преглед према врсти инцидената

У складу са Уредбом о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја и Правилником о врсти, форми и начину достављања статистичких података о инцидентима у информационо-комуникационим системима од посебног значаја, групе инцидената су подељене на врсте инцидената и подаци о броју инцидената приказани су у Табели бр. 3.1 и у Графиконима у наставку.

Група инцидената	Врста инцидента	Број инцидената
Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл.malware)	Тројанац	32.145
	Вирус	15.564
	Шпијунски софтвер (енгл. spyware)	3.653
	Црв (енгл. worm)	1.781
	Руткит (енгл. rootkit)	1.569
	Рансомвер (енгл. ransomware)	68
Неовлашћено прикупљање података	Скенирање портова	7.691.232
	Социјални инжењеринг (лажно представљање и други облици)	4.859
	Пресретање података између рачунара и сервера (енгл. sniffing)	605
	Компромитовање или цурење података (енгл. *data breaches*)	70
Превара	Фишинг (енгл. *phishing*)	57.623
	Neovlašćeno korišćenje resursa (engl. *cryptojacking*) i drugi oblici	794
Покушај упада у ИКТ систем	Покушај откривања креденцијала (енгл. *brute force attack, dictionary attack* и сл.)	2.513.290
	Покушај искоришћавања рањивости система	466.287
Упад у ИКТ систем	Откривање или неовлашћено коришћење непривилегованих налога (енгл. *unprivileged account compromise*)	1.152
	Неовлашћени приступ апликацији	812
	Мрежа заражених уређаја (енгл. *botnet*)	56
	Откривање или неовлашћено коришћење привилегованих налога (енгл. *privileged account compromise*)	9

Група инцидената	Врста инцидента	Број инцидената
Недоступност или ограничена доступност ИКТ система	Прекид у функционисању система или дела система (енгл. *outage*)	1.052
	Дистрибуирани напад са циљем онемогућавања или ометања функционисања ИКТ система (енгл. *distributed denial-of-service attack – DDoS*)	702
	Напад са циљем онемогућавања или ометања функционисања ИКТ система (енгл. *denial-of-service attack – DoS*)	646
	Саботажа	5
Угрожавање безбедности података	Неовлашћен приступ подацима	8
	Неовлашћена измена или брисање података	7
	Криптографски напад	3
Оперативни инциденти	Проблеми у раду са софтверским компонентама	9.009
	Отказивање хардверских компоненти	4.313
Инциденти физичко-техничке безбедности	Крађа хардверских компоненти	149
	Поплава	20
	Пожар	9
Остали инциденти	Инциденти који не спадају у горе наведене категорије	1.346
	УКУПНО	**10.808.838**

Табела 3.1 - Број инцидената по врстама

Графикон 3.1 – Пет најбројнијих врста инцидената

3.1. Инсталирање злонамерног софтвера у оквиру ИКТ система

Малвер (енгл. *malware*) је реч изведена од две речи – "*Malicious Software*", и представља сваки софтвер који је написан у злонамерне сврхе, односно који има циљ да нанесе штету рачунарским системима или мрежама. У ове програме спадају: рачунарски вирус, рачунарски црв, рансомвер, рачунарски тројанац, шпијунски софтвер и руткит.

Рачунарски вирус је део злонамерног компјутерског кôда чији је циљ да се шири са рачунара на рачунар тако што напада извршне датотеке и документа и може проузроковати наменско брисање датотека са хард диска и сличну штету.

Рачунарски црв је програм који садржи злонамерни кôд који се шири преко мреже, тако што се самостално умножава и преноси, односно не зависи од датотека зараженог уређаја. Црви се шире на адресе електронске поште са листе контакта жртве или искоришћавају рањивости мрежних апликација и због велике брзине ширења служе за пренос осталих типова злонамерног софтвера.

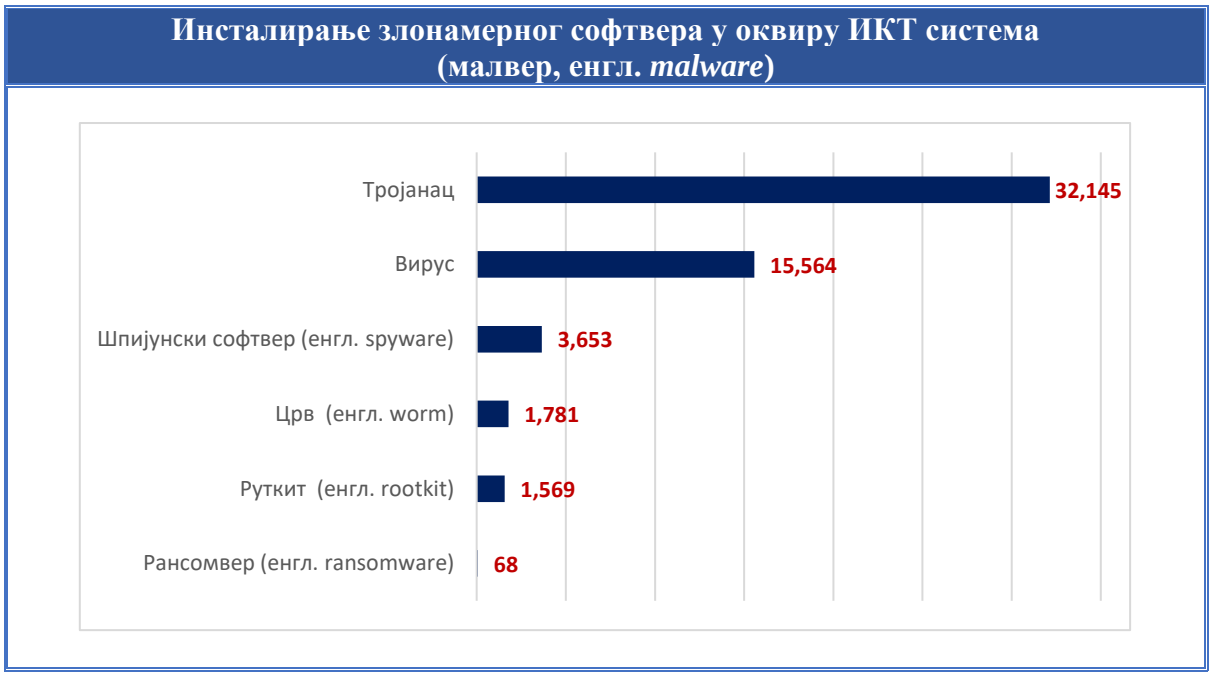
Рансомвер је злонамерни софтвер који шифрира податке на уређајима или мрежама, а за приступ и откључавање датотека се захтева плаћање откупа. Чест је случај да датотеке чак и након плаћања откупа остају закључане.

Рачунарски тројанци (тројански коњи) су претња која покушава да се представи корисницима као да су корисни програми и на тај начин их превари да их покрену. Ови програми могу да преузму друге претње са интернета, убацују друге типове малвера на угрожене рачунаре, комуницирају са удаљеним нападачима, као и да бележе све што се куца на тастатури и шаљу нападачима.

Шпијунски софтвер делимично пресреће или преузима контролу над рачунаром без знања или дозволе корисника. Сам назив сугерише да је реч о програмима који надгледају рад корисника тако што снимају и преузимају информације са рачунара попут навика претраживања интернет страница, електронске поште, креденцијала и сл. и те податке преносе нападачу.

Руткит је софтвер који омогућава привилегован даљински приступ рачунару, кријӯћи своје присуство од администратора система. Омогућава нападачу да прикрије трагове неовлашћеног приступа и одржава привилегован приступ рачунару заобилажењем уобичајеног начина аутентификације и механизама ауторизације.

У оквиру ове групе инцидената пријављено је 54.780 инсталирања злонамерног софтвера, од чега је тројанац у ИКТ системима од посебног значаја пријављен 32.145 пута (Графикон 3.1.1). Ова врста малвера је и у претходној години најчеће детектована.



Графикон 3.1.1 – Инсталирање злонамерног софтвера у оквиру ИКТ система

3.2. Неовлашћено прикупљање података

Неовлашћено прикупљање податка подразумева скенирање портова, пресретање података између рачунара и сервера, социјални инжењеринг и компромитовање или цурење података.

Скенирање портова је напад код којег се шаљу ИП пакети на изабране портове, са циљем откривања отворених комуникационих канала и активних сервиса чије се рањивости могу искористити.

Снифинг напад, односно пресретање података подразумева коришћење апликација за надгледање, анализу и снимање мрежног саобраћаја у циљу прикупљања мрежних пакета. На овај начин нападач анализира мрежу и прибавља информације којим је може компромитовати.

Напади **социјалног инжењеринга** користе људску психологију и подложност манипулацијама како би навели жртве на откривање осетљивих података или кршење мера заштите које ће омогућити нападачу приступ ИКТ систему.

Повреда података (компромитовање и цурење података) подразумева успешан злонамеран покушај који је довео до измене или губитка података.

На графикону 3.2.1 је приказано 7.691.232 пријава скенирања портова што се као и претходне године може објаснити великим бројем аутоматизованих процеса за испитивање доступних сервиса на удаљеним рачунарима, 4.859 пријава социјалног инжењеринга, 605 пресретања података између рачунара и сервера и 70 пријава компромитовања или цурења података, односно укупно 7.696.766 пријава (Графикон 3.2.1).

Графикон 3.2.1 – Неовлашћено прикупљање података

3.3. Превара

Под преваром се подразумевају фишинг напади, неовлашћено коришћење ресурса и други облици преваре.

Фишинг је сајбер напад који се врши уз помоћ електронске поште, друшвених мрежа, телефонског позива или СМС-а, којим се захтева да се посети линк или отвори документ. Нападач користи социјални инжењеринг да би се представио као неко познат и тако навео жртву да остави поверељиве податке или преузме злонамерни софтвер. Зато не чуди да је овај напад често повезан и са нападима попут малвера, мреже ботова и сајбер шпијунаже.

Неовлашћено коришћење ресурса - Криптоцекинг (познат и као криптомајнинг) односно „отимање“ или "рударење" је нови термин који се односи на програме који користе снагу централне процесорске јединице (70% до 80% неискоришћене снаге процесора) без пристанка жртве, да би „рударили“ криптовалуте за стицање личне користи.

Број пријава који се односи на фишинг нападе у 2022. години се увећао више од три пута у односу на претходну и износи 57.623, док за неовлашћено коришћење ресурса износи 794 пријава (Графикон 3.3.1).

Графикон 3.3.1 – Превара систем

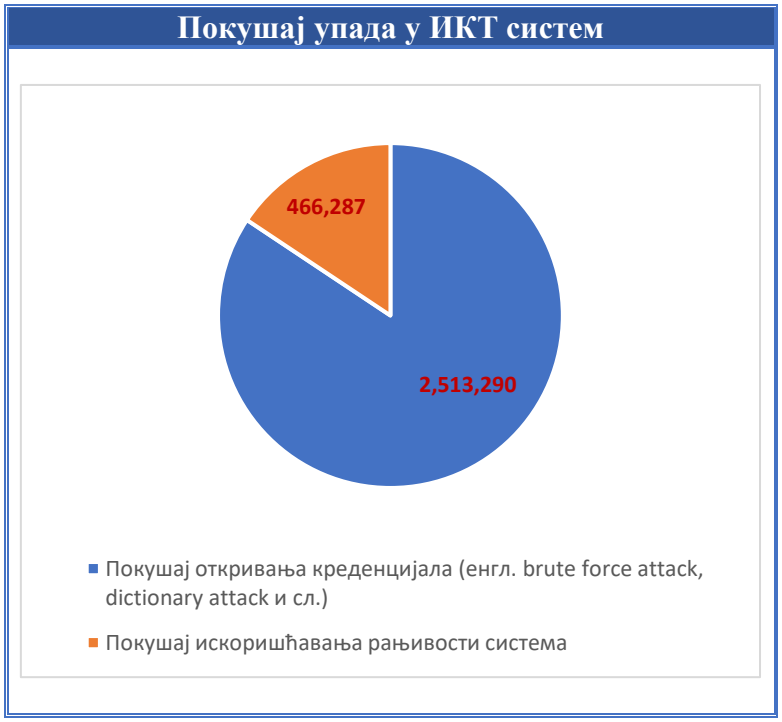
3.4. Покушај упада у ИКТ систем

Приликом покушаја упада у ИКТ систем нападачи најчешће користе технику *Brute Force* за откривање креденцијала или покушавају да искористе рањивости информационог система.

Покушај искоришћавања рањивости система је напад на рачунарски систем, којим нападач користи одређену рањивост система. Овај напад користи рањивост оперативног система, апликације или било којег другог софтверског кода, укључујући додатке апликација или библиотеке софтвера.

Brute Force напад подразумева покушај приступа систему жртве непрекидним уносом различитих комбинација слова, бројева и симбола са циљем идентификације корисничког имена и лозинке.

У 2022. години нападачи су у највећој мери за упад у систем користили технике откривања креденцијала (2.513.290 покушаја) док су у односу на прошлу годину у већој мери покушавали да искористе рањивости система (466.287 покушаја, Графикон 3.4.1).



Графикон 3.4.1 – Покушај упада у ИКТ

3.5. Упад у ИКТ систем

Упад у ИКТ систем подразумева успешно компромитовање система или апликација (сервиса) извршено са удаљене локације коришћењем нове или познате рањивости или неовлашћеним локалним приступом.

Откривање или неовлашћено коришћење привилегованих налога (енгл. *Privileged Account Compromise*) омогућава нападачима да се крећу кроз ИКТ систем и приступе осетљивим подацима.

Откривање или неовлашћено коришћење непривилегованих налога (енгл. *Unprivileged Account Compromise*) омогућава нападачима да се крећу кроз ограничени део ИКТ система, са могућношћу даље компромитације ИКТ система и приступања осетљивим подацима.

Неовлашћени приступ апликацији је приступ веб локацији, програму, серверу, сервису или другом систему коришћењем туђег налога или других метода.

Мрежа заражених уређаја је аутоматизовани напад код ког нападач скенира мрежне адресе, користи рањивост на уређајима и преузима контролу над њима. На тај начин се

ствара мрежа заражених уређаја која се може користи за нападе који ометају функционисање ИКТ система (*DDoS*).

У 2022. години је најчешће забележено откривање или неовлашћено коришћење непривилегованих налога (1.152 пријаве), затим неовлашћени приступ апликацији (812 пријава), мрежа заражених уређаја је омогућила упад 56 пута, док су се упади путем откривања или неовлашћеног коришћења привилегованих налога догодили 9 пута (Графикон 3.5.1).

Графикон 3.5.1 – Упад у ИКТ систем

3.6. Недоступност или ограничена доступност ИКТ система

Нападима недоступности или ограничене доступности ИКТ система се оптерећује мрежни саобраћај, што доводи до кашњења операција или пада система.

Доступност може бити угрожена и локалним радњама (уништење, прекид у дистрибуцији електричном енергијом и слично) или услед више силе, ненамерних или намерних људских грешака.

Напад са циљем онемогућавања или ометања функционисања ИКТ система (енгл. *denial-of-service attack – DoS*) је покушај нападача да онемогући приступ серверу или сервисима који су намењени крајњим корисницима.

Дистрибуирани напад са циљем онемогућавања или ометања функционисања ИКТ система (енгл. *distributed denial-of-service attack – DDoS*) има исти циљ као и DoS

напад. DDoS напади постижу већу ефикасност користећи истовремено више компромитованих рачунарских система као изворе напада.

Саботажа као напад се користити у сврху саботирања система и наношења штете. Могући су различити облици саботаже у зависности од области пословања нападнуте инфраструктуре.

Прекид у функционисању система или дела система *(енгл. outage)* може бити проузрокован прекидом у испоруци електричне енергије, због лоших временских услова или хардверске грешке која је настала као последица неисправне опреме.

ИКТ системи од посебног значаја су детектовали 1.052 прекида у функционисања система или дела система због техничких проблема, односно лоших временских услова, око четири пута мање *DDoS* напада у односу на прошлу годину, односно 702 напада, 646 *DoS* напада, док је саботажа ИКТ система у 2022. години забележена 5 пута (Графикон 3.6.1).

Графикон 3.6.1 – Недоступност или ограничена доступност ИКТ система

3.7. Угрожавање безбедности података

Поред злоупотребе података и система неовлашћеним приступом, односно неовлашћеном изменом или брисањем података, нарушавање безбедности података може бити и последица криптографског напада.

Неовлашћен приступ подацима је напад помоћу ког се угрожава безбедност података злоупотребом права приступа подацима система.

Неовлашћена измена података је напад помоћу ког се злоупотребом права приступа подацима система врши измена, додавање или брисање података.

Криптографски напад је метод заобилажења мера заштите криптографског система проналажењем слабости у коду, шифри, алгоритму, криптографском протоколу или шеми управљања кључевима.

У 2022. години је забележено 8 неовлашћених приступа подацима, 7 неовлашћених измена или брисања података и 3 криптографска напада (Графикон 3.7.1).

Графикон 3.7.1 – Угрожавање безбедности података

3.8. Оперативни инциденти

Оперативни инциденти су сви они инциденти који доводе до отказивања хардверских компоненти или проблема у раду са софтверским компонентама.

Број проблема у раду са софтверским компонентама које су довеле до застоја у пружању услуга, односно прекида који је на било који начин угрозио пословни процес (на пример краћи прекиди у раду) је износио 9.009, а број отказивања хардверских компоненти у 2022. години је износио 4.313 (Графикон 3.8.1).

Графикон 3.8.1 – Оперативни инциденти

3.9. Инциденти физичко-техничке безбедности

Овој групи инцидената припадају крађа хардверских компоненти, пожар и поплава који су довели до угрожавања физичко-техничке безбедности ИКТ система.

У 2022. години забележено је 149 крађа хардверских компоненти, 20 поплава и 9 пожара (Графикон 3.9.1).

Графикон 3.9.1 – Инциденти физичко-техничке безбедности

3.10. Остали инциденти

У групу осталих инцидената спадају сви инциденти који нису наведени у претходним категоријама.

Осталих инцидената у 2022. години је било 1.346 (Графикон 3.10.1). Ове инциденте чине сви они инциденти који не спадају у наведене категорије, а то су на пример: детекција потецијално небезбедних апликација, неодобрене платне транскације и лажни профили на друштвеним мрежама.

Графикон 3.10.1 – Остали инциденти

4. Преглед према врсти ИКТ система од посебног значаја

Број пријављених инцидената према врсти ИКТ система од посебног значаја је дат у Табели 4.1. Треба узети у обзир да су неки ИКТ системи од посебног значаја, због врсте делатности коју обављају сврстани у више категорија.

	Врста ИКТ система од посебног значаја	Број инцидената
1.	ИКТ системи од посебног значаја који се користе у обављању послова у органима власти	92.976
2.	ИКТ системи од посебног значаја који се користе за обраду посебних врста података о личности, у смислу закона који уређује заштиту података о личности	0
3.	ИКТ системи од посебног значаја који се користе у обављању делатности од општег интереса и другим делатностима и то:	
	енергетика	2.034.969
	саобраћај	6.482
	здравство	31.166
	банкарство и финансијска тржишта	922.968
	дигитална инфраструктура	7.366.982
	добра од општег интереса који се односе на коришћење, управљање, заштиту и унапређење добара од општег интереса	30.409
	услуге информационог друштва	7.365.461
	остале области:	
	- Електронске комуникације	7.365.495
	- Издавање службеног гласила Републике Србије	164
	- Управљање нуклеарним објектима	122
	- Производња, промет и превоз наоружања и војне опреме	2.010.075
	- Управљање отпадом	203
	- Комуналне делатности	31.874
	- Производња и снабдевање хемикалијама	321.451
4.	ИКТ системи од посебног значаја који се користе у правним лицима и установама које оснива Република Србија, аутономна покрајина или јединица локалне самоуправе за обављање делатности од општег интереса	2.037.942

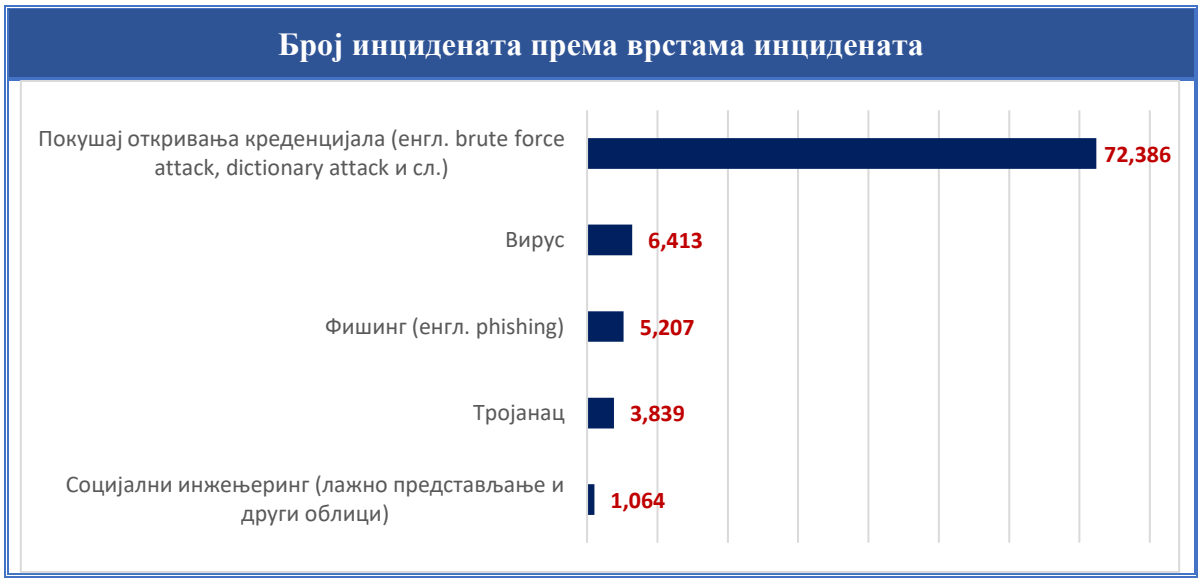
Табела 4.1 – Број пријављених инцидената према врсти ИКТ система

4.1. ИКТ системи од посебног значаја који се користе у обављању послова у органима власти

	Група инцидената	Број инцидената
1.	Покушај упада у ИКТ систем	72.572
2.	Инсталирање злонамерног софтвера у оквиру ИКТ система	11.656
3.	Превара	5.208
4.	Неовлашћено прикупљање података	1.212
5.	Оперативни инциденти	1.089
6.	Остали инциденти	874
7.	Недоступност или ограничена доступност ИКТ система	345
8.	Упад у ИКТ систем	10
9.	Угрожавање безбедности података	5
10.	Инциденти физичко техничке безбедности	5
	УКУПНО	**92.976**

Табела 4.1.1 – Број инцидената према групама инцидената у органима власти

Током 2022. године у ИКТ системима који се користе у органима власти забележено је највише покушаја откривања креденцијала, чак шест пута више него претходне године (72.386), на другом месту је вирус (6.413), на трећем и четвртом месту налазе се фишинг (5.207) и тројанац (3.839), док је социјални инжењеринг (лажно представљање и други облици) (1.064) на петом месту (Графикон 4.1.1).



Графикон 4.1.1 – Број инцидената према врстама инцидената

4.2. ИКТ системи од посебног значаја који се користе за обраду посебних врста података о личности, у смислу закона који уређује заштиту података о личности

У ИКТ системима који се користе за обраду посебних врста података о личности нису забележени инциденти.

	Група инцидената	Број инцидената
1.	Недоступност или ограничена доступност ИКТ система	0
2.	Остали инциденти	0
3.	Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. *malware*)	0
4.	Неовлашћено прикупљање података	0
5.	Превара	0
6.	Покушај упада у ИКТ систем	0
7.	Упад у ИКТ систем	0
8.	Угрожавање безбедности података	0
9.	Оперативни инциденти	0
10.	Инциденти физичко-техничке безбедности	0
	УКУПНО	**0**

Табела 4.2.1 – Број инцидената према групама инцидената у ИКТ системима од посебног значаја који се користе за обраду посебних врста података о личности

4.3. ИКТ системи од посебног значаја који се користе у обављању делатности од општег интереса и другим делатностима

4.3.1. Енергетика

	Група инцидената	Број инцидената
1.	Покушај упада у ИКТ систем	1.996.169
2.	Инсталирање злонамерног софтвера у оквиру ИКТ система	19.607
3.	Оперативни инциденти	6.695
4.	Неовлашћено прикупљање података	6.661
5.	Превара	5.603
6.	Недоступност или ограничена доступност ИКТ система	185
7.	Остали инциденти	33
8.	Упад у ИКТ систем	12
9.	Угрожавање безбедности података	4
10.	Инциденти физичко техничке безбедности	0
	УКУПНО	**2.034.969**

Табела 4.3.1.1 – Број инцидената према групама инцидената у ИКТ системима од посебног значаја који се користе у обављању делатности у области енергетике

Најзаступљенији напад у области енергетике у 2022. години је био покушај откривања креденцијала (1.991.277), на другом месту је тројанац (13.104), треће место заузима скенирање портова (6.604), док су на четвртом и петом месту вирус (6.429) и проблеми у раду са софтверским компонентама (6.129) (Графикон 4.3.1.1).

Графикон 4.3.1.1 – Пет најчешћих врста инцидената у области енергетике

4.3.2. Саобраћај

	Група инцидената	Број инцидената
1.	Превара	4.410
2.	Инсталирање злонамерног софтвера у оквиру ИКТ система	1.642
3.	Неовлашћено прикупљање података	251
4.	Оперативни инциденти	164
5.	Недоступност или ограничена доступност ИКТ система	12
6.	Покушај упада у ИКТ систем	1
7.	Упад у ИКТ систем	1
8.	Инциденти физичко техничке безбедности	1
9.	Угрожавање безбедности података	0
10.	Остали инциденти	0
	УКУПНО	**6.482**

Табела 4.3.2.1 – Број инцидената према групама инцидената у ИКТ системима од посебног значаја који се користе у обављању делатности у области саобраћаја

У области саобраћаја током 2022. године у највећем броју забележен је фишинг (4.410), други по заступљености је вирус (899), треће место заузима тројанац (727), четврто социјални инжењеринг (лажно представљање и други облици) (251), док је на петом отказивање хардверских компоненти (130) (Графикон 4.3.2.1).

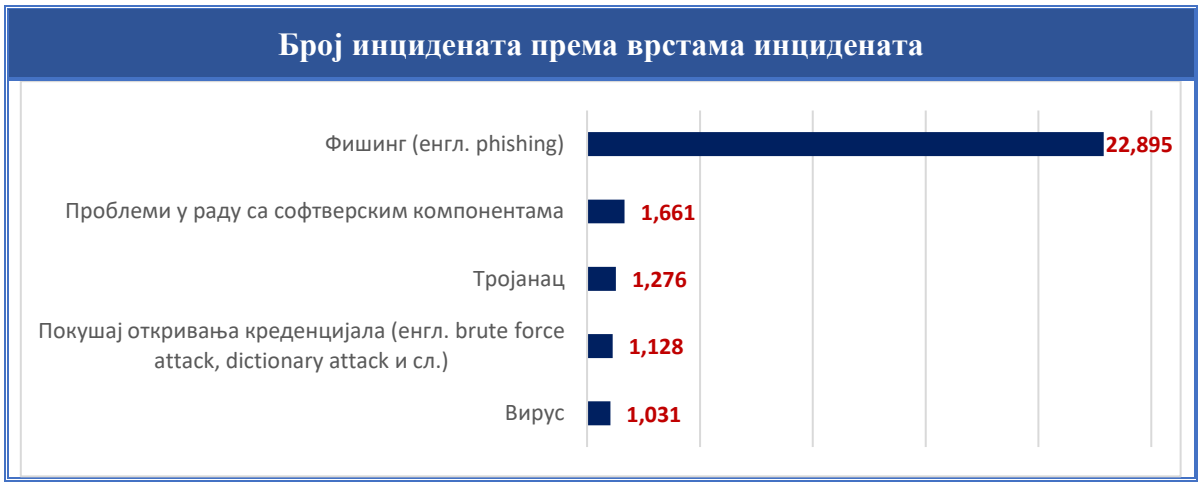
Графикон 4.3.2.1 – Пет најчешћих врста инцидената у области саобраћаја

4.3.3. Здравство

	Група инцидената	Број инцидената
1.	Превара	22.897
2.	Инсталирање злонамерног софтвера у оквиру ИКТ система	2.963
3.	Оперативни инциденти	2.355
4.	Покушај упада у ИКТ систем	1.933
5.	Неовлашћено прикупљање података	468
6.	Упад у ИКТ систем	385
7.	Недоступност или ограничена доступност ИКТ система	152
8.	Инциденти физичко техничке безбедности	9
9.	Угрожавање безбедности података	2
10.	Остали инциденти	2
	УКУПНО	**31.166**

Табела 4.3.3.1 – Број инцидената према групама инцидената у ИКТ системима од посебног значаја који се користе у обављању делатности здравства

Током 2022. године здравствени сектор је био најизложенији фишинг нападима (22.895), на другом месту су проблеми у раду са софтверским компонентама (1.661), на трећем тројанац (1.276), четвртом покушај откривања креденцијала (1.128) и петом месту је вирус (1.031) (Графикон 4.3.3.1).



Графикон 4.3.3.1 – Пет најчешћих врста инцидената у области здравства

4.3.4. Банкарство и финансијска тржишта

	Група инцидената	Број инцидената
1.	Покушај упада у ИКТ систем	487.992
2.	Неовлашћено прикупљање података	415.364
3.	Превара	16.684
4.	Оперативни инциденти	1.791
5.	Недоступност или ограничена доступност ИКТ система	711
6.	Остали инциденти	232
7.	Инсталирање злонамерног софтвера у оквиру ИКТ система	187
8.	Инциденти физичко техничке безбедности	18
9.	Упад у ИКТ систем	7
10.	Угрожавање безбедности података	0
	УКУПНО	**922.986**

Табела 4.3.4.1 – Број инцидената према групама инцидената у ИКТ системима од посебног значаја који се користе у обављању делатности у области банкарства и финансијских тржишта

ИКТ системи од посебног значаја из области банкарства и финансијских тржишта пријављују највећи број скенирања портова (415.220), други је покушај искоришћавања рањивости система (400.004), трећи покушај откривања креденцијала (87.988), четврти фишинг (16.652) и пети отказивање хардверских компоненти (1.529) (Графикон 4.3.4.1).

Графикон 4.3.4.1 – Пет најчешћих врста инцидената у области банкарства и финансијских тржишта

4.3.5. Дигитална инфраструктура

	Група инцидената	Број инцидената
1.	Неовлашћено прикупљање података	7.255.014
2.	Покушај упада у ИКТ систем	106.272
3.	Упад у ИКТ систем	1.554
4.	Оперативни инциденти	1.524
5.	Недоступност или ограничена доступност ИКТ система	1.099
6.	Превара	812
7.	Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. *malware*)	607
8.	Остали инциденти	62
9.	Инциденти физичко техничке безбедности	38
10.	Остали инциденти	62
	УКУПНО	**7.366.982**

Табела 4.3.5.1 – Број инцидената према групама инцидената у ИКТ системима од посебног значаја који се користе у обављању делатности у области дигиталне инфраструктуре

Дигитална инфраструктура је током 2022. године била најизложенија скенирању портова (7.255.01), на другом месту је покушај искоришћавања рањивости система (54.687), трећем покушај откривања креденцијала (51.585), док су на четвртом и петом месту отказивање хардверских компоненти (1.507) и неовлашћени приступ апликацији (798) (Графикон 4.3.5.1).

Графикон 4.3.5.1 – Пет најчешћих врста инцидената у области дигиталне инфраструктуре

4.3.6. Добра од општег интереса који се односе на коришћење, управљање, заштиту и унапређење добара

	Група инцидената	Број инцидената
1.	Инсталирање злонамерног софтвера у оквиру ИКТ система	18.056
2.	Покушај упада у ИКТ систем	6.425
3.	Неовлашћено прикупљање података	3.572
4.	Превара	2.233
5.	Оперативни инциденти	99
6.	Недоступност или ограничена доступност ИКТ система	15
7.	Угрожавање безбедности података	6
8.	Упад у ИКТ систем	3
9.	Инциденти физичко техничке безбедности	0
10.	Остали инциденти	0
	УКУПНО	**30.409**

Табела 4.3.6.1 – Број инцидената према групама инцидената у ИКТ системима од посебног значаја који се користе у обављању делатности у области добара од општег интереса

ИКТ системи који се користе у области добра од општег интереса који се односе на коришћење, управљање, заштиту и унапређење добара су током 2022. године забележили на првом месту тројанац (12.840), покушај искоришћавања рањивости система (5.654) се налази на другом, док су на трећем, четвртом и петом месту шпијунски софтвер (3.173), социјални инжењеринг (2.957) и фишинг (2.233) (Графикон 4.3.6.1).

Графикон 4.3.6.1 – Пет најчешћих врста инцидената у области добра од општег интереса који се односе на коришћење, управљање, заштиту и унапређење добара

4.3.7. Услуге информационог друштва

	Група инцидената	Број инцидената
1.	Неовлашћено прикупљање података	7.254.949
2.	Покушај упада у ИКТ систем	105.542
3.	Упад у ИКТ систем	1.554
4.	Оперативни инциденти	1.527
5.	Превара	811
6.	Инсталирање злонамерног софтвера у оквиру ИКТ система	607
7.	Недоступност или ограничена доступност ИКТ система	371
8.	Остали инциденти	62
9.	Инциденти физичко техничке безбедности	38
10.	Угрожавање безбедности података	0
	УКУПНО	**7.365.461**

Табела 4.3.7.1 – Број инцидената према групама инцидената у ИКТ системима од посебног значаја који се користе у обављању делатности у области услуга информационог друштва

Област информационог друштва бележи највише скенирања портова (7.254.947), на другом месту је покушај искоришћавања рањивости система (54.322), на трећем покушај откривања креденцијала (51.220), четвртом отказивање хардверских компоненти (1.510) и петом месту неовлашћени приступ апликацији (798) (Графикон 4.3.7.1).

Графикон 4.3.7.1 – Пет најчешћих врста инцидената у области информационог друштва

4.3.8. Остале области

	Група инцидената	Број инцидената
1.	Неовлашћено прикупљање података	7.272.210
2.	Покушај упада у ИКТ систем	2.415.990
3.	Инсталирање злонамерног софтвера у оквиру ИКТ система	28.180
4.	Превара	7.652
5.	Оперативни инциденти	2.735
6.	Упад у ИКТ систем	1.619
7.	Недоступност или ограничена доступност ИКТ система	574
8.	Остали инциденти	207
9.	Инциденти физичко техничке безбедности	145
10.	Угрожавање безбедности података	7
	УКУПНО	**9.729.319**

Табела 4.3.8.1 – Број инцидената према групама инцидената у ИКТ системима од посебног значаја који се користе у обављању делатности осталих области

И остале области у којима се обављају делатности од општег интереса и друге делатности су током 2021. године забележиле највише скенирања портова (7.268.338), на другом месту је покушај откривања креденцијала (2.351.092), трећем покушај искоришћавања рањивости система (65.898), четвртом тројанац (23.017) и петом фишинг (6.893) (Графикон 4.3.8.1).

Графикон 4.3.8.1 – Пет најчешћих врста инцидената у осталим областима

4.3.8.1. Електронске комуникације

	Група инцидената	Број инцидената
1.	Неовлашћено прикупљање података	7.254.648
2.	Покушај упада у ИКТ систем	105.604
3.	Упад у ИКТ систем	1.557
4.	Оперативни инциденти	1.539
5.	Превара	826
6.	Инсталирање злонамерног софтвера у оквиру ИКТ система	620
7.	Недоступност или ограничена доступност ИКТ система	370
8.	Остали инциденти	194
9.	Инциденти физичко техничке безбедности	137
10.	Угрожавање безбедности података	0
	УКУПНО	**7.365.495**

Табела 4.3.8.1.1 – Број инцидената према групама инцидената у ИКТ системима од посебног значаја који се користе у обављању делатности у области електронских комуникација

ИКТ системи које користе оператори из области електронских комуникација су током 2022. године детектовали највећи број скенирања портова (7.254.647), друго место заузима покушај искоришћавања рањивости система (54.381), треће покушај откривања креденцијала (51.223), четврто и пето место заузима отказивање хардверских компоненти (1.511) и неовлашћени приступ апликацији (798) (Графикон 4.3.8.1.1).

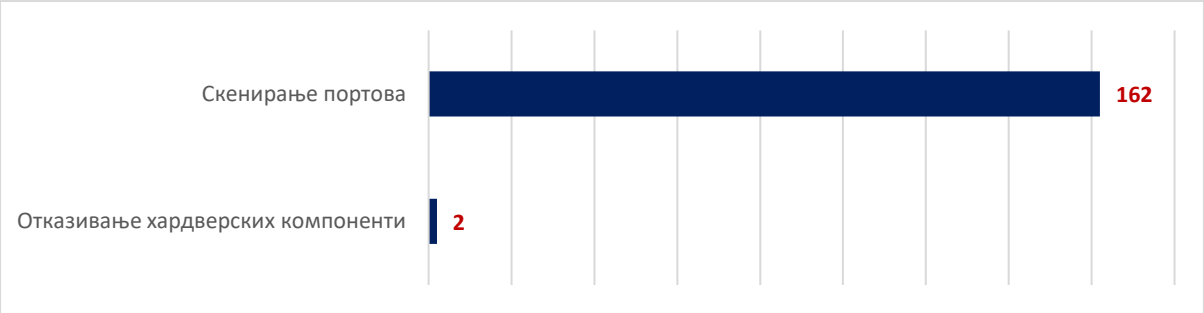
Графикон 4.3.8.1.1 – Пет најчешћих врста инцидената у области електронских комуникација

4.3.8.2. Издавање службеног гласила

	Група инцидената	Број инцидената
1.	Неовлашћено прикупљање података	162
2.	Оперативни инциденти	2
3.	Инсталирање злонамерног софтвера у оквиру ИКТ система	0
4.	Превара	0
5.	Покушај упада у ИКТ систем	0
6.	Упад у ИКТ систем	0
7.	Недоступност или ограничена доступност ИКТ система	0
8.	Угрожавање безбедности података	0
9.	Инциденти физичко техничке безбедности	0
10.	Остали инциденти	0
	УКУПНО	**164**

Табела 4.3.8.2.1 – Број инцидената према групама инцидената у ИКТ системима од посебног значаја који се користе у обављању делатности у области издавања службеног гласника

ИКТ системи које користе оператори из области издавања службеног гласила су током 2022. године детектовали скенирање портова 162 пута и отказивање хардверских компоненти 2 пута (Графикон 4.3.8.1.1).



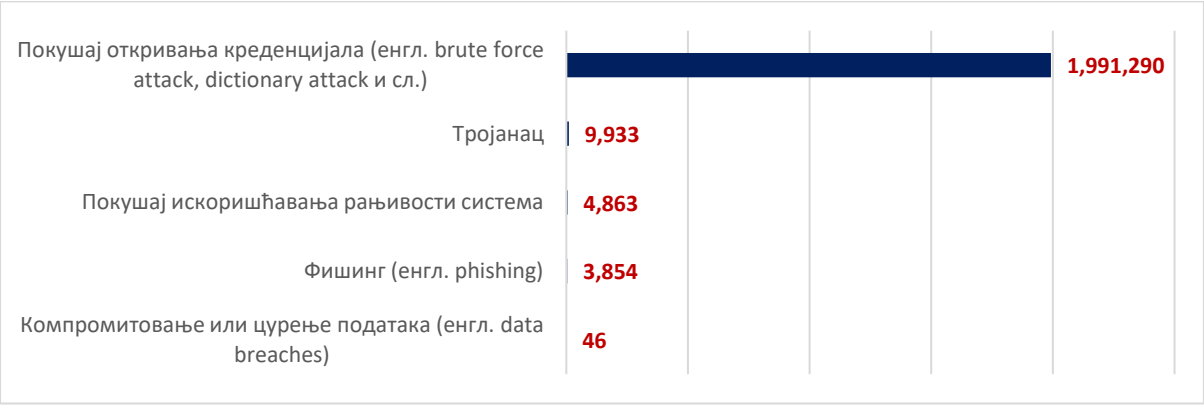
Графикон 4.3.8.2.1 – Пет најчешћих врста инцидената у области издавања службеног гласила

4.3.8.3. Управљање нуклеарним објектима
4.3.8.4. Производња, промет и превоз нуклеарног наоружања и војне опреме

	Група инцидената	Број инцидената
1.	Покушај упада у ИКТ систем	1.996.153
2.	Инсталирање злонамерног софтвера у оквиру ИКТ система	9.965
3.	Превара	3.854
4.	Неовлашћено прикупљање података	51
5.	Оперативни инциденти	31
6.	Недоступност или ограничена доступност ИКТ система	12
7.	Упад у ИКТ систем	5
8.	Остали инциденти	3
9.	Инциденти физичко техничке безбедности	1
10.	Угрожавање безбедности података	0
	УКУПНО	**2.010.075**

Табела 4.3.8.4.1 – Број инцидената према групама инцидената у ИКТ системима од посебног значаја који се користе у обављању делатности у области производње, промета и превоза нуклеарног наоружања и војне опреме

У области производње, промета и превоза нуклеарног наоружања и војне опреме најзаступљенији напад је покушај откривања креденцијала (1.991.290), други је тројанац (9.933), трећи покушај искоришћавања рањивости система (4.863), четврти фишинг (3.854) и пети вирус (46) (Графикон 4.3.8.4.1).



Графикон 4.3.8.4.1 – Пет најчешћих врста инцидената у области производње, промета и превоза нуклеарног наоружања и војне опреме

4.3.8.5. Управљање отпадом

	Група инцидената	Број инцидената
1.	Неовлашћено прикупљање података	77
2.	Оперативни инциденти	36
3.	Превара	34
4.	Покушај упада у ИКТ систем	25
5.	Инсталирање злонамерног софтвера у оквиру ИКТ система	20
6.	Недоступност или ограничена доступност ИКТ система	7
7.	Упад у ИКТ систем	2
8.	Угрожавање безбедности података	1
9.	Инциденти физичко техничке безбедности	1
10.	Остали инциденти	0
	УКУПНО	**203**

Табела 4.3.8.5.1 – Број инцидената према групама инцидената у ИКТ системима од посебног значаја који се користе у обављању делатности у области управљања отпадом

У области управљања отпадом најзаступљенији је био социјални инжењеринг (63), фишинг (34), на трећем и четвртом месту је једнак број пријава за покушај искоришћавања рањивости система (25) и отказивање хардверских компоненти (25), док је пето место проблеми у раду са софтверским компонентама (11) (Графикон 4.3.8.5.1).

Графикон 4.3.8.5.1 – Пет најчешћих врста инцидената у области управљања отпадом

4.3.8.6. Комуналне делатности

	Група инцидената	Број инцидената
1.	Инсталирање злонамерног софтвера у оквиру ИКТ система	17.568
2.	Покушај упада у ИКТ систем	6.683
3.	Неовлашћено прикупљање података	3.805
4.	Превара	2.434
5.	Оперативни инциденти	1.126
6.	Недоступност или ограничена доступност ИКТ система	181
7.	Упад у ИКТ систем	55
8.	Остали инциденти	10
9.	Угрожавање безбедности података	6
10.	Инциденти физичко техничке безбедности	6
	УКУПНО	**31.874**

Табела 4.3.8.6.1 – Број инцидената према групама инцидената у ИКТ системима од посебног значаја који се користе у обављању делатности у области комуналних делатности

Током 2022. године су оператори ИКТ система од посебног значаја који обављају комуналне делатности забележили највећи број инсталирања тројанаца (12.481), на другом месту је покушај искоришћавања рањивости система (5.654), трећем социјални инжењеринг (2.977), четвртом шпијунски софтвер (2.856) и петом фишинг (2.434) (Графикон 4.3.8.6.1).

Графикон 4.3.8.6.1 – Пет најчешћих врста инцидената у области управљања отпадом

4.3.8.7. Производња и снабдевање хемикалијама

	Група инцидената	Број инцидената
1.	Покушај упада у ИКТ систем	307.550
2.	Неовлашћено прикупљање података	13.480
3.	Превара	407
4.	Оперативни инциденти	11
5.	Недоступност или ограничена доступност ИКТ система	2
6.	Инциденти физичко техничке безбедности	1
7.	Инсталирање злонамерног софтвера у оквиру ИКТ система	0
8.	Упад у ИКТ систем	0
9.	Угрожавање безбедности података	0
10.	Остали инциденти	0
	УКУПНО	**321.451**

Табела 4.3.8.7.1 – Број инцидената према групама инцидената у ИКТ системима од посебног значаја који се користе у обављању делатности у области производње и снабдевања хемикалијама

Област производње и снабдевања хемикалијама је током 2022. године била најизложенија нападима покушај откривања креденцијала (307.550), скенирање портова (13.288), фишинг (407), социјални инжењеринг (192) и проблеми у раду са софтверским компонентама (9) (Графикон 4.3.8.7.1).

Графикон 4.3.8.7.1 – Пет најчешћих врста инцидената у области производње и снабдевања хемикалијама

4.4. ИКТ системи од посебног значаја који се користе у правним лицима које оснива Република Србија, аутономна покрајина или јединица локалне самоуправе за обављање делатности од општег интереса

	Група инцидената	Број инцидената
1.	Покушај упада у ИКТ систем	2.002.494
2.	Инсталирање злонамерног софтвера у оквиру ИКТ система	24.861
3.	Превара	5.537
4.	Неовлашћено прикупљање података	3.792
5.	Оперативни инциденти	1.040
6.	Недоступност или ограничена доступност ИКТ система	182
7.	Остали инциденти	16
8.	Упад у ИКТ систем	9
9.	Угрожавање безбедности података	6
10.	Инциденти физичко техничке безбедности	5
	УКУПНО	**2.037.942**

Табела 4.4.1 – Број инцидената према групама инцидената у ИКТ системима од посебног значаја који се користе у обављању делатности у областима од општег интереса и другим делатностима

Ова врста ИКТ система је током 2022. године била најизложенија нападима покушаја откривања креденцијала (1.991.977), на другом месту је тројанац (20.252), трећем покушај искоришћавања рањивости система (10.517), четвртом фишинг (5.537) и петом месту социјални инжењеринг (2.915) (Графикон 4.4.1).

Графикон 4.4.1 – Пет најчешћих врста инцидената у ИКТ системима од посебног значаја који се користе у правним лицима које оснива Република Србија, аутономна покрајина или јединица локалне самоуправе за обављање делатности од општег интереса

5. Закључак

Годишњи извештај о статистичким подацима о свим инцидентима представља свеобухватан преглед сајбер претњи у ИКТ системима од посебног значаја. Праћење ових података омогућава сагледавање трендова напада, што представља основ за креирање адекватних стратегија за одбрану од актуелних напада.

Најзаступљенија врста инцидената је скенирање портова која припада групи напада неовлашћено прикупљање података. Ова група и врста напада су биле веома заступљене и у 2021. години. Скенирање портова је напад који служи за прикупљање информација и не наноси директну штету самој мети, већ се користи за прибављање корисних информација за следеће фазе напада. Главни циљ овог напада је откривање који портови су отворени и који се сервиси користе како би се искористиле потенцијалне рањивости. Заступљеност је повећана и због аутоматизације ове врсте напада, а сами ИКТ системи од посебног значаја могу бити део скенираног опсега.

Ова врста напада је најзаступљенија у ИКТ системима који се користе у банкарству и финансијском тржишту, дигиталној инфраструктури и услугама информационог друштва.

На другом месту налази се покушај откривања креденцијала који спада у групу напада покушај упада у ИКТ систем. Ова врста напада подразумева покушај приступа систему жртве непрекидним испробавањем различитих комбинација слова, бројева и симбола са циљем идентификације корисничког имена и лозинке или коришћењем речника. Реч је о добро познатој врсти напада, која је још увек веома ефикасна и популарна међу нападачима јер приступ легитимном налогу може омогућити приступ читавом ИКТ систему. Ови напади се не ослањају на рањивости ИКТ система већ на слабе лозинке корисника.

Ова врста напада је најзаступљенија у ИКТ системима од посебног значаја који се користе у обављању послова у органима власти, у области енергетике, производње, промета и превоза нуклеарног наоружања и војне опреме, производњи и снабдевању хемикалијама, као и у ИКТ системима од посебног значаја који се користе у правним лицима које оснива Република Србија, аутономне покрајине или јединице локалне самоуправе за обављање делатности од општег интереса.

Покушај искоришћавања рањивости система је на трећем месту и представља слабост чијом злоупотребом нападачи могу угрозити интегритет, расположивост, аутентичност и непорецивост података којима се рукује помоћу ИКТ система. Покушај искоришћавања рањивости система је напад којим нападач покушава да приступи систему за који нема одобрење, искоришћавањем познатих или нових рањивости. Постоји неколико јавно доступних евиденција познатих рањивости као што су *CVE, NVD* и *OVAL*. *CVE* идентификатор обично укључује кратак опис, а понекад и савете, упутства и извештаје. Број ових напада указује на потребу за ефикаснијим управљањем закрпама, односно редовном ажурирању. У ту сврху Национални ЦЕРТ редовно објављује информације о рањивостима и закрпама које се тичу најзаступљенијих

софтвера и уређаја у нашој земљи (https://www.cert.rs/preporuke.html). Поред тога, најављена је примена нове методологије од које се очекује да унапреди процену критичности рањивости (*Common Vulnerability Scoring System* верзија 4.0), као и развијен систем за процену вероватноће искоришћавања рањивости од стране нападача у краткорочном периоду (*Exploit Prediction Scoring System*). Ове активности подржане су од стране FIRST *(Forum of Incident Response and Security Teams*) удружења, чији је пуноправни члан и Национални ЦЕРТ Републике Србије.

Ова врста напада је веома заступљена у области банкарства и финансија, дигиталној инфраструктури и у ИКТ системима који управљају добрима од општег интереса који се односе на коришћење, управљање, заштиту и унапређење добара.

На четвртом месту се налази фишинг. Током 2022. године спроведено је неколико великих фишинг кампања чија су мета били корисници интернета у Србији. Посебно се истичу кампање које су биле усмерене на кориснике поштанских услуга и платформи за е-трговину. Е-пошта је најчешће садржала обавештење да је пристигао пакет за корисника, али да није могао бити испоручен јер није уплаћен одређени износ за царинске трошкове. У поруци е-поште се даље од корисника захтевало да кликне на линк на којем пише "Да бисте потврдили испоруку вашег пакета Кликните овде", након чега је корисник наводно добијао е-пошту или СМС поруку којом се потврђује испорука пошиљке. Кликом на понуђени линк корисник се преусмерава на лажну страницу за интернет плаћање Поште Србије, у којој се захтевао унос података: број платне картице, име и презиме, рок трајања, као и *CVV2/CVC2* број картице. Сви подаци које су корисници уносили на лажну форму омогућили су нападачима приступ њиховом банковном рачуну и непосредну финансијску добит за нападача.

Фишинг кампања усмерена на кориснике платформи за е-трговину има исту методологију. Наводни купац комуникацију почиње питањем оглашивачу да ли је производ и даље доступан и да ли купопродаја може да се обави електронским путем. Тада нападач у своје име или у име „администратора платформе за е-трговину“ доставља жртви тј. Оглашивачу, линк са објашњењем да је наводни купац већ уплатио средства преко апликације и од оглашивача тражи да кликне на линк који води на страницу на којој се захтева да унесе у одређена поља податке са банковне картице (број картице и CVV број) како би му се наводно извршила уплата. Национални ЦЕРТ је поводом ових фишинг напада објавио више обавештења и саопштења за јавност како би грађанима указао на заступљеност ове преваре.

Фишинг је на првом месту по заступљености у ИКТ системима који се користе за обављање послова у области саобраћаја, здравству, управљању нуклеарним објектима, на другом месту у ИКТ системима који се баве управљањем отпадом, на трећем месту у ИКТ системима који се баве производњом и снабдевањем хемикалијама, на четвртом месту у области ИКТ система од посебног значаја који се користе у правним лицима које оснива Република Србија, аутономна покрајина или јединица локалне самоуправе, У ИКТ системима производње, промета и превоза наоружања и војне опреме, док у ИКТ системима који се користе за обављање делатности у области комуналних услуга и ИКТ система који се баве добрима од општег интереса који се односе на коришћење, управљање заштиту и и унапређење добара фишинг заузима пето место.

Имајући у виду значај групе напада инсталирање злонамерног софтвера (малвера), треба напоменути да су током 2022. године најзаступљеније врсте малвера биле тројанац, вирус и шпијунски софтвер.

Тројанац је врста злонамерног софтвера која покушава да се представи корисницима као корисни програм и на тај начин их превари да га покрену. Ови програми могу да преузму друге претње са интернета, убацују друге типове малвера на угрожене рачунаре, комуницирају са удаљеним нападачима, као и да бележе све што се куца на тастатури и шаљу нападачима.

Ова врста малвера је најзаступљенија у ИКТ системима који се користе у обављању комуналних делатности и ИКТ системима који се баве добрима од општег интереса који се односе на коришћење, управљање заштиту и и унапређење добара. На другом месту по заступљености тројанац се јавља код ИКТ система у области енергетике, у области ИКТ система од посебног значаја који се користе у правним лицима које оснива Република Србија, аутономна покрајина или јединица локалне самоуправе, ИКТ системима који се баве пословима производње, промета и превоза наоружања и војне опреме. Иако је тројанац један од најстаријих облика злонамерног софтвера показао се као веома издржљив и прилагодљив. Успешно избегава откривање, уграђује се и преплиће у рутинске рачунарске операције и генерално је еволуирао тако да избегава детектовање, а опстанак и напредак обезбеђује тако што постаје део комплекснијих сајбер напада[1].

На другом месту по заступљености злонамерног софтвера је вирус. Вируси могу бити усмерени на масовно заражавање рачунарских мрежа или на мрежу компаније или организације која је мета. Ниво заштите одређује ниво ангажовања неопходног да се напад успешно спроведе. С обзиром да већина организација користи *Firewall* и друге мере заштите од спољних напада, често се дешава да се користе методе социјалног инжењеринга које омогућавају нападачима лакши приступ запосленима и ИКТ системима у којима ти запослени раде.

Вирус је по заступљености на другом месту у ИКТ системима који се користе у области саобраћаја и ИКТ системима од посебног значаја који се користе у обављању послова у органима власти, док је на четвртом месту у ИКТ систему здравства.

Трећа најзаступљенија врста малвера је шпијунски софтвер који се инсталира без сагласности корисника инфилтрирањем кроз пакет апликација, посетом зараженој интернет страници или кроз заражени прилог. Овај малвер надгледа рад корисника кроз снимање екрана, бележење онога што се откуца на тастатури а украдене податке шаље аутору шпијунског софтвера који их користи или продаје другим лицима. Подаци до којих се долази на овај начин су корисничко име и лозинка, ПИН налога, број кредитне картице, текст откуцан на тастатури, навике у претраживању интернета, коришћене адресе е-поште.

[1] https://umbrella.cisco.com/blog/how-trojan-malware-is-evolving-to-survive-and-evade-cybersecurity-in-2021

Шпијунски софтвер је на трећем месту по заступљености код ИКТ система у чијој су надлежности добра од општег интереса која се односе на коришћење, управљање заштиту и и унапређење добара а на четвртом месту код ИКТ система који се баве комуналним делатностима.

Важно је напоменути да нови напади настављају да се појављују на тржишту сајбер претњи, а како малвер постаје софистицираније, тиме је пад укупног броја напада компензован већим последицама успешно реализованих напада. Најопаснији од свих у овом смислу су банкарски малвер и шпијунски софтвер[2].

Имајући у виду представљене трендове покушаја откривања креденцијала, фишинг напада, откривања рањивости система и инсталирања малициозних софтвера, Национални ЦЕРТ Републике Србије континуирано унапређује процесе прикупљања и обраде информација о актуелним претњама у сајбер простору и пружа рана упозорења операторима ИКТ система од посебног значаја. Циљ оваквог проактивног деловања је заустављање напада у раној фази, те спречавања настанка значајног угрожавања безбедности инфраструктуре и услуга оператора ИКТ система од посебног значајног. Такође, поред пружања упозорења институцијама о претњама које се тичу само њих, Национални ЦЕРТ је у складу са Стратегијом развоја информационог друштва и информационе безбедности за период од 2021. до 2026. године развио платформу 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. У оквиру ове платформе ће се размењивати информације о индикаторима компромиса (ИП адресе са које долазе напади, променама на оперативном систему/командама које малициозни софтвери извршавају, детаљним описима фишинг напада, итд) од чега се очекује да олакша детекцију напада и унапреди процес управљања инцидентима операторима ИКТ система од посебног значаја. Након припреме неопходних упутстава операторима ИКТ система од посебног значаја биће омогућен приступ платформи и информацијама о претњама које преко 600 ЦЕРТ-ова, чланица FIRST организације размењују овим путем.

На крају, не треба заборавити да је у већини случајева људски фактор највећи ризик по информациону безбедност. Из овог разлога, Национални ЦЕРТ наставља са едукацијом како запослених на пословима који се тичу информационих технологија и безбедности у операторима ИКТ система од посебног значаја, тако и шире јавности. Национални ЦЕРТ је у континуитету током 2022. године спроводио техничку обуку на Cyberbit платформи систем администраторима који раде у локалним самоуправама, док је крајем 2022. године у рад пуштена и платформа за подизање свести и знања о информационој безбедности кроз интерактивне програме под називом "За безбеднији клик". На овој платформи се тренутно могу пронаћи интерактивни садржаји везани за тему фишинга, креирања и безбедности лозинки, безбедности на друштвеним мрежама, рансомвер напада, креирања резервних копија података, социјалног инжењеринга, и безбедности коришћења отвореног бежичног интернета (Wi-Fi).

[2] https://securelist.com/mobile-malware-evolution-2021/105876/


СРБ-ЦЕРТ