ИЗВЕШТАЈ О СТАТИСТИЧКИМ ПОДАЦИМА О СВИМ ИНЦИДЕНТИМА У ИКТ СИСТЕМИМА ОД ПОСЕБНОГ ЗНАЧАЈА У 2024. ГОДИНИ

Јун, 2025. година

РАТЕЛ

СРБ-ЦЕРТ

Национални ЦЕРТ Републике Србије www.cert.rs

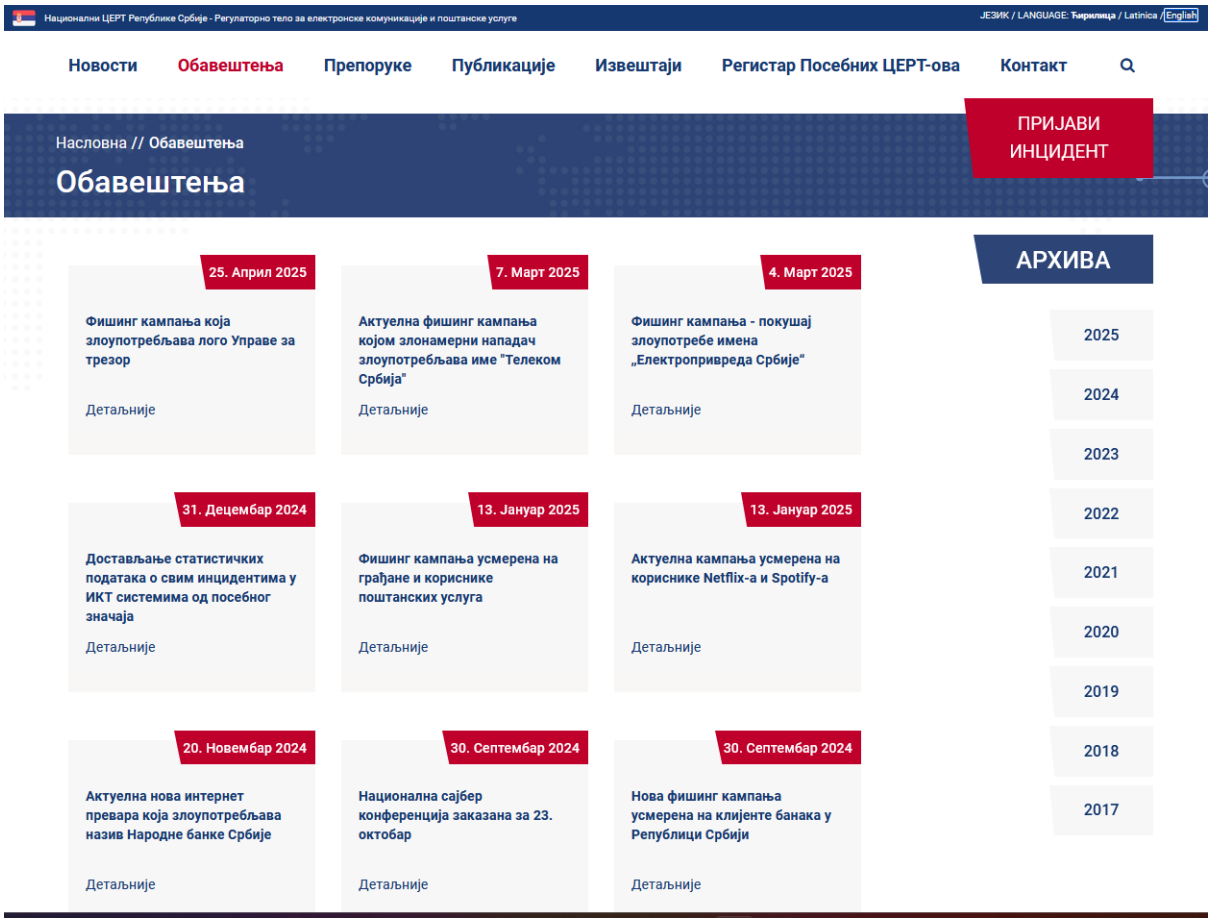
Садржај

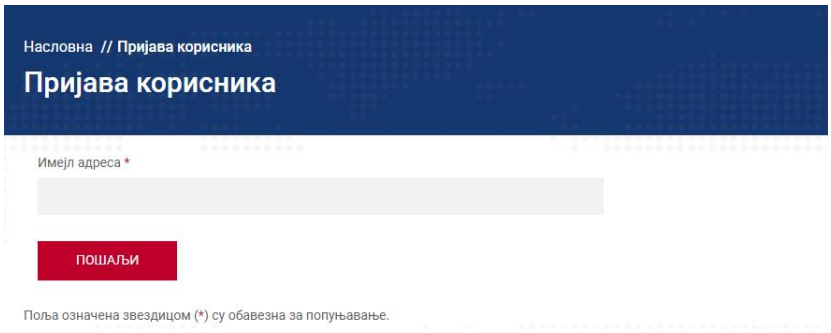
Увод

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 2025. године, прикупљао статистичке податке о свим инцидентима у ИКТ системима од посебног значаја за 2024. 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 информисања 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 28.02.2025. године, у складу са Законом о информационој безбедности и Правилником о врсти, форми и начину достављања статистичких података.

У табели 2.2 дат је приказ броја инцидената према групама инцидената, док је на графикону 2.1 приказано првих пет најзаступљенијих група инцидената.

	Група инцидената	Број инцидената
1.	Неовлашћено прикупљање података	108.606.782
2.	Покушај упада у ИКТ систем	2.421.688
3	Превара	66.250
4.	Инсталирање злонамерног софтвера у оквиру ИКТ система	30.445
5.	Недоступност или ограничена доступност ИКТ система	24.072
6.	Остали инциденти	14.732
7.	Оперативни инциденти	10.885
8.	Упад у ИКТ систем	1.590
9.	Инциденти физичко техничке безбедности	115
10.	Угрожавање безбедности података	47
	УКУПНО	**111.176.606**

Табела 2.2 – Број инцидената према групама инцидената

Најзаступљенија група инцидената је неовлашћено прикупљање података 108.606.782, у оквиру које је најдоминантнија врста инцидента скенирање портова. На другом месту је покушај упада у ИКТ систем 2.421.688 у оквиру које је најзаступљенији инцидент покушај откривања креденцијала. На трећем месту се налази превара 66.250 у оквиру које је најзаступљенији фишинг. Четврто место заузима инсталирање злонамерног софтвера у оквиру ИКТ система 30.445, најчешће тројанац. На петом месту су недоступност или ограничена доступност ИКТ система 24.072 и то у највећем броју напад са циљем онемогућавања или ометања функционисања ИКТ система (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 на Графиконима у наставку.

Група инцидената	Врста инцидента	Број инцидената
Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. *malware*)	Вирус	9.780
	Црв	670
	Рансомвер	168
	Тројанац	17.533
	Шпијунски софтвер	2.262
	Руткит	32
Неовлашћено прикупљање података	Скенирање портова	108.602.318
	Пресретање података између рачунара и сервера	18
	Социјални инжењеринг	2.586
	Компромитовање или цурење података	1.860
Превара	Фишинг	65.560
	Неовлашћено коришћење ресурса	690
Покушај упада у ИКТ систем	Покушај искоришћавања рањивости система	68.801
	Покушај откривања креденцијала	2.352.887

Група инцидената	Врста инцидента	Број инцидената
Упад у ИКТ систем	Откривање или неовлашћено коришћење привилегованих налога	60
	Откривање или неовлашћено коришћење непривилегованих налога	594
	Неовлашћени приступ апликацији	792
	Мрежа заражених уређаја	144
Недоступност или ограничена доступност ИКТ система	Напад са циљем онемогућавања или ометања функционисања ИКТ система	19.063
	Дистрибуирани напад са циљем онемогућавања или ометања функционисања ИКТ система	1.897
	Саботажа	1
	Прекид у функционисању система или дела система	3.111
Угрожавање безбедности података	Неовлашћен приступ подацима	37
	Неовлашћена измена или брисање података	6
	Криптографски напад	4
Оперативни инциденти	Отказивање хардверских компоненти	4.406
	Проблеми у раду са софтверским компонентама	6.479
Инциденти физичко-техничке безбедности	Крађа хардверских компоненти	101
	Пожар	4
	Поплава	10
Остали инциденти	Инциденти који не спадају у наведене категорије	14.732
	УКУПНО	**111.176.606**

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.

Тројанци 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 детектовано је 30.445 инцидената, а најзаступљенији је тројанац 17.533 (Графикон 3.1.1). Тројанац је најзаступљенија врста малвера од 2021. године.

Графикон 3.1.1 – Инсталирање злонамерног софтвера у оквиру ИКТ система

3.2. Неовлашћено прикупљање података

Неовлашћено прикупљање података 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 108.602.318 скенирања портова што се као и претходне године може објаснити великим бројем аутоматизованих процеса за испитивање доступних сервиса на удаљеним рачунарима, 2.586 социјалног инжењеринга, 1.860

компромитовања или цурења података и 18 пресретања података између рачунара и сервера, односно укупно 108.606.782 напада (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 поверљиве 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 инцидената који се односи на фишинг нападе у 2024. години износи 65.560, док за неовлашћено коришћење ресурса износи 690 (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 2024. години нападачи су у највећој мери за упад у систем користили технике откривања креденцијала 2.352.887, док је забележен мањи број покушаја искоришћавања рањивости система 68.801, као што се може видети на Графикону 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.

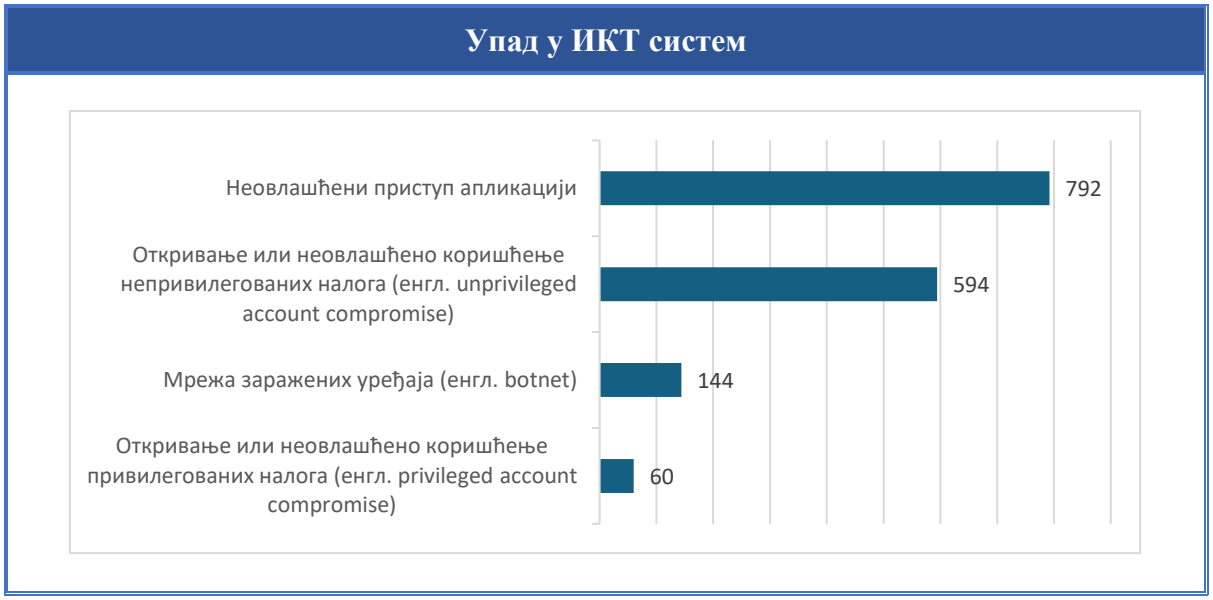
Откривање или неовлашћено коришћење привилегованих налога (енгл. *Privileged Account Compromise*) омогућава нападачима да се крећу кроз ИКТ систем и приступе осетљивим подацима.

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 2024. години је у оквиру групе инцидената упад у ИКТ систем био најзаступљенији неовлашћени приступ апликацији 792, затим откривање или неовлашћено коришћење непривилегованих налога 594, мрежа заражених уређаја 144 и откривање или неовлашћено коришћење привилегованих налога 60 (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.

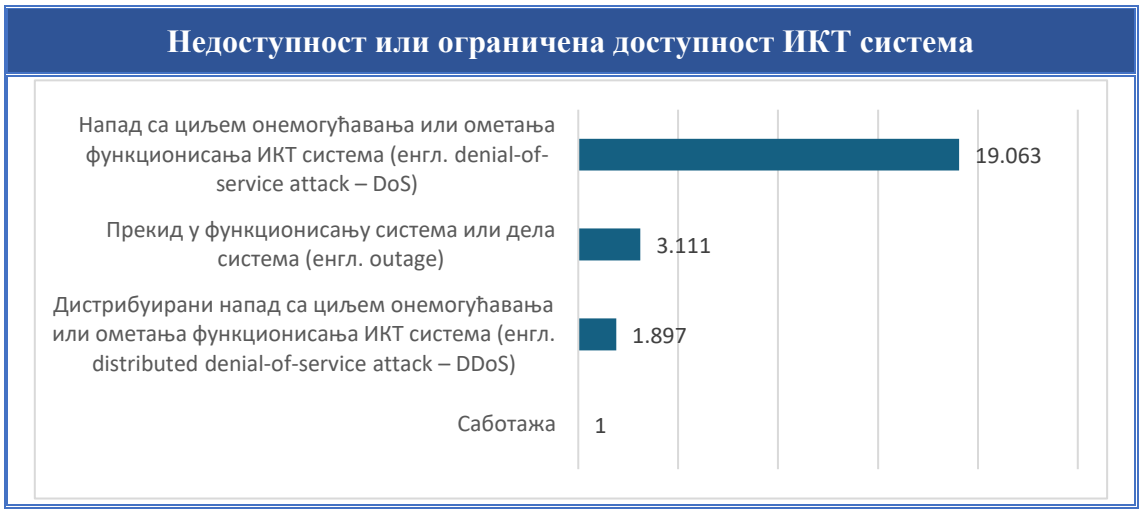
Напад са циљем онемогућавања или ометања функционисања ИКТ система (енгл. *denial-of-service attack – DoS*) је покушај нападача да онемогући приступ серверу или сервисима који су намењени крајњим корисницима.

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.

У ИКТ системима од посебног значаја је детектовано 19.063 *DDoS* напада, 3.111 прекида у функционисању система или дела система, 1.897 дистрибуираних напада са циљем онемогућавања или ометања функционисања ИКТ система и једна саботажа (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 2024. години је забележено 37 неовлашћених приступа подацима, 6 неовлашћених измена или брисања података и 4 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 који су довели до застоја у пружању услуга, односно прекида који је на било који начин угрозио пословни процес (на пример краћи прекиди у раду) је износио 6.479, а број отказивања хардверских компоненти 4.406 (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 2024. години забележено је 101 крађа хардверских компоненти, 10 поплава и 4 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 2024. години је било 14.732 (Графикон 3.10.1).

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 чињенице да обављају више 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	119.665
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	2
3.	ИКТ системи од посебног значаја који се користе у обављању делатности од општег интереса и другим делатностима и то:	
	енергетика	2.006.825
	саобраћај	3.894
	здравство	35.224
	банкарство и финансијска тржишта	27.022
	дигитална инфраструктура	8.545.368
	добра од општег интереса који се односе на коришћење, управљање, заштиту и унапређење добара од општег интереса	100.016.027
	услуге информационог друштва	8.533.170
	остале области:	
	- Електронске комуникације	2.589
	- Издавање службеног гласила Републике Србије	14.786
	- Управљање нуклеарним објектима	162
	- Производња, промет и превоз наоружања и војне опреме	1.997.718
	- Управљање отпадом	2.348
	- Комуналне делатности	17.335
	- Производња и снабдевање хемикалијама	266.166
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	55.351

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	60.802
2.	Недоступност или ограничена доступност ИКТ система	18.554
3.	Остали инциденти	11.572
4.	Превара	10.222
5.	Инсталирање злонамерног софтвера у оквиру ИКТ система	10.182
6.	Неовлашћено прикупљање података	7.206
7.	Оперативни инциденти	1.085
8.	Упад у ИКТ систем	38
9.	Угрожавање безбедности података	4
10.	Инциденти физичко техничке безбедности	0
		119.665

Табела 4.1.1 – Број инцидената према групама инцидената у органима власти

Током 2024. године у ИКТ системима који се користе у органима власти забележено је највише покушаја откривања креденцијала 60.207, на другом месту је *DoS* напад 16.958, на трећем и четвртом месту налазе се инциденти који не спадају у горе наведене категорије 11.572 и фишинг 10.219, док је скенирање портова на петом месту са 6.751 пријаве (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 током 2024. године пријављен је 1 тројанац и 1 пријава пресретања података између рачунара и сервера (Графикон 4.2.1).

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

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

Графикон 4.2.1 – Број инцидената према врстама инцидената

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

	Група инцидената	Број инцидената
1.	Неовлашћено прикупљање података	108.596.126
2.	Покушај упада у ИКТ систем	2.348.425
3.	Превара	26.345
4.	Инсталирање злонамерног софтвера у оквиру ИКТ система	14.536
5.	Оперативни инциденти	6.413
6.	Недоступност или ограничена доступност ИКТ система	5.180
7.	Остали инциденти	2.979
8.	Упад у ИКТ систем	1.429
9.	Инциденти физичко техничке безбедности	111
10.	Угрожавање безбедности података	38
	УКУПНО	**111.001.582**

Табела 4.3.1 – Број инцидената према групама инцидената у ИКТ системима од посебног значаја који се користе за обраду посебних врста података о личности

Ова врста ИКТ система је током 2024. године била најизложенија нападима скенирања портова 108.593.271, на другом месту је покушај откривања креденцијала 2.283.582, на трећем покушај искоришћавања рањивости система 64.843, на четвртом фишинг 25.664 и на петом тројанац 8.910. (Графикон 4.3.1).

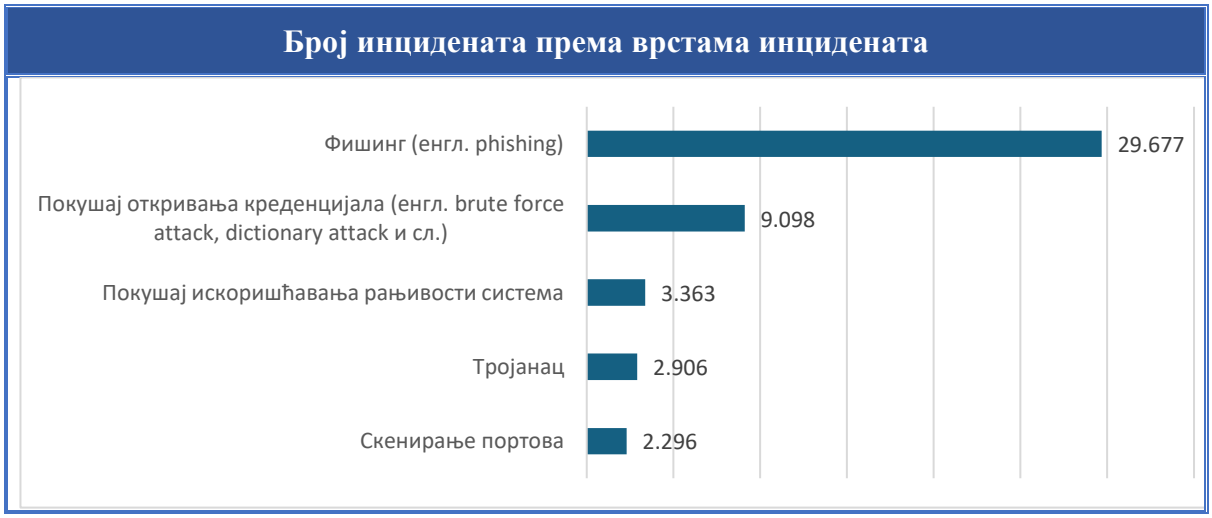
Графикон 4.3.1 – Број инцидената према врстама инцидената

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.	Превара	29.683
2.	Покушај упада у ИКТ систем	12.461
3.	Инсталирање злонамерног софтвера у оквиру ИКТ система	5.724
4.	Неовлашћено прикупљање података	3.449
5.	Оперативни инциденти	3.385
6.	Недоступност или ограничена доступност ИКТ система	336
7.	Остали инциденти	181
8.	Упад у ИКТ систем	123
9.	Угрожавање безбедности података	5
10.	Инциденти физичко техничке безбедности	4
	УКУПНО	**55.351**

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

Најчешћи напади на ову врсту ИКТ система током 2024. године су фишинг 29.667, на другом месту покушај откривања креденцијала 9.098, на трећем покушај искоришћавања рањивости система 3.363, на четвртом тројанац 2.906 и на петом месту скенирање портова са 2.296 (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

4.5. Преглед према делатности ИКТ система од посебног значаја

4.5.1. Енергетика

	Група инцидената	Број инцидената
1.	Покушај упада у ИКТ систем	1.988.077
2.	Инсталирање злонамерног софтвера у оквиру ИКТ система	6.982
3.	Превара	4.364
4.	Оперативни инциденти	3.129
5.	Неовлашћено прикупљање података	2.421
6.	Недоступност или ограничена доступност ИКТ система	1.824
7.	Упад у ИКТ систем	22
8.	Угрожавање безбедности података	5
9.	Инциденти физичко техничке безбедности	1
10.	Остали инциденти	0
	УКУПНО	**2.006.825**

Табела 4.5.1.1 – 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 2024. години је био покушај откривања креденцијала 1.976.295, на другом месту је покушај искоришћавања рањивости система 11.782, треће место заузима тројанац 6.595, док су на четвртом и петом месту фишинг 4.364 и проблеми у раду са софтверским компонентама 2.970 (Графикон 4.5.1.1).

Графикон 4.5.1.1 – Пет најчешћих врста инцидената у области енергетике

4.5.2. Саобраћај

	Група инцидената	Број инцидената
1.	Инсталирање злонамерног софтвера у оквиру ИКТ система	2.652
2.	Недоступност или ограничена доступност ИКТ система	1.219
3.	Оперативни инциденти	10
4.	Покушај упада у ИКТ систем	7
5.	Превара	4
6.	Неовлашћено прикупљање података	1
7.	Остали инциденти	1
8.	Упад у ИКТ систем	0
9.	Инциденти физичко техничке безбедности	0
10.	Угрожавање безбедности података	0
	УКУПНО	**3.894**

Табела 4.5.2.1 – Број инцидената према групама инцидената у ИКТ системима од посебног значаја који се користе у обављању делатности у области саобраћаја

У области саобраћаја током 2024. године забележен је највећи број пријава тројанца 1.959, други по заступљености је прекид у функционисању система или дела система 1.218, треће место заузима шпијунски софтвер 572, четврто вирус 82, док је на петом црв 39 (Графикон 4.5.2.1).

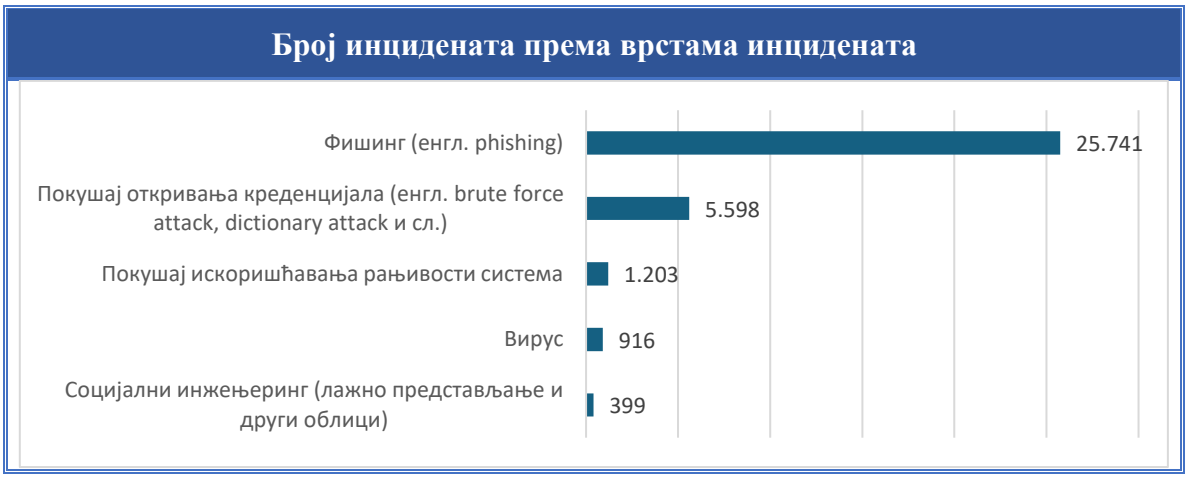
Графикон 4.5.2.1 – Пет најчешћих врста инцидената у области саобраћаја

4.5.3. Здравство

	Група инцидената	Број инцидената
1.	Превара	25.747
2.	Покушај упада у ИКТ систем	6.801
3.	Инсталирање злонамерног софтвера у оквиру ИКТ система	1.122
4.	Оперативни инциденти	707
5.	Неовлашћено прикупљање података	475
6.	Остали инциденти	180
7.	Недоступност или ограничена доступност ИКТ система	167
8.	Упад у ИКТ систем	20
9.	Угрожавање безбедности података	3
10.	Инциденти физичко техничке безбедности	2
	УКУПНО	**35.224**

Табела 4.5.3.1 – Број инцидената према групама инцидената у ИКТ системима од посебног значаја који се користе у обављању делатности здравства

Током 2024. године је у здравственом сектору најзаступљенији фишинг напад 25.741, на другом месту налази се покушај откривања креденцијала 5.598, на трећем покушаји искоришћавања рањивости система 1.203, затим на четвртом месту вирус 916 и на петом месту социјални инжењеринг 399 (Графикон 4.5.3.1).



Графикон 4.5.3.1 – Пет најчешћих врста инцидената у области здравства

4.5.4. Банкарство и финансијска тржишта

	Група инцидената	Број инцидената
1.	Превара	10.689
2.	Инсталирање злонамерног софтвера у оквиру ИКТ система	5.670
3.	Неовлашћено прикупљање података	3.754
4.	Остали инциденти	2.906
5.	Покушај упада у ИКТ систем	2.548
6.	Недоступност или ограничена доступност ИКТ система	948
7.	Упад у ИКТ систем	332
8.	Оперативни инциденти	141
9.	Угрожавање безбедности података	22
10.	Инциденти физичко техничке безбедности	12
	УКУПНО	**27.022**

Табела 4.5.4.1 – Број инцидената према групама инцидената у ИКТ системима од посебног значаја који се користе у обављању делатности у области банкарства и финансијских тржишта

У ИКТ системима од посебног значаја из области банкарства и финансијских тржишта је детектован највећи број фишинг напада 0.576, на другом месту је вирус 3.445, следи скенирање портова 3.178, четвртом инциденти који не спадају у горе наведене категорије броје 2.906 и на петом месту је покушај откривања креденцијала 2.530 (Графикон 4.5.4.1).

Графикон 4.5.4.1 – Пет најчешћих врста инцидената у области банкарства и финансијских тржишта

4.5.5. Дигитална инфраструктура

	Група инцидената	Број инцидената
1.	Неовлашћено прикупљање података	8.437.345
2.	Покушај упада у ИКТ систем	102.472
3.	Оперативни инциденти	2.023
4.	Упад у ИКТ систем	1.073
5.	Недоступност или ограничена доступност ИКТ система	968
6.	Превара	900
7.	Инсталирање злонамерног софтвера у оквиру ИКТ система	553
8.	Инциденти физичко техничке безбедности	34
9.	Остали инциденти	0
10.	Угрожавање безбедности података	0
	УКУПНО	**8.545.368**

Табела 4.5.5.1 – 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 2024. године била најизложенија скенирању портова 8.437.145, на другом месту је покушај искоришћавања рањивости система 52.224, на трећем покушај откривања креденцијала 50.248, док су на четвртом и петом месту отказивање хардверских компоненти 2.011 и неовлашћено коришћење ресурса (енгл. *cryptojacking*) и други облици 567 (Графикон 4.5.5.1).

Графикон 4.5.5.1 – Пет најчешћих врста инцидената у области дигиталне инфраструктуре

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

	Група инцидената	Број инцидената
1.	Неовлашћено прикупљање података	100.002.579
2.	Превара	10.485
3.	Оперативни инциденти	1.302
4.	Покушај упада у ИКТ систем	906
5.	Инсталирање злонамерног софтвера у оквиру ИКТ система	506
6.	Недоступност или ограничена доступност ИКТ система	157
7.	Упад у ИКТ систем	50
8.	Остали инциденти	31
9.	Угрожавање безбедности података	10
10.	Инциденти физичко техничке безбедности	1
	УКУПНО	**100.016.027**

Табела 4.5.6.1 – 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 2024. године забележили на првом месту скенирање портова 100.002.061, фишинг 10.485 је на другом месту, док су на трећем, четвртом и петом месту проблеми у раду са софтверским компонентама 1.138, покушај откривања креденцијала 570 и социјални инжењеринг 514 (Графикон 4.5.6.1).

Графикон 4.5.6.1 – Пет најчешћих врста инцидената у области добра од општег интереса који се односе на коришћење, управљање, заштиту и унапређење добара

4.5.7. Услуге информационог друштва

	Група инцидената	Број инцидената
1.	Неовлашћено прикупљање података	8.426.800
2.	Покушај упада у ИКТ систем	101.742
3.	Оперативни инциденти	2.107
4.	Упад у ИКТ систем	1.073
5.	Превара	615
6.	Инсталирање злонамерног софтвера у оквиру ИКТ система	554
7.	Недоступност или ограничена доступност ИКТ система	243
8.	Инциденти физичко техничке безбедности	34
9.	Остали инциденти	2
10.	Угрожавање безбедности података	0
	УКУПНО	**8.533.170**

Табела 4.5.7.1 – 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 8.426.780, на другом месту је покушај искоришћавања рањивости система 51.859, на трећем покушај откривања креденцијала 49.883, четвртом отказивање хардверских компоненти 2.017 и петом месту неовлашћено коришћење ресурса (енгл. *cryptojacking*) и други облици којих је било 567 (Графикон 4.5.7.1).

Графикон 4.5.7.1 – Пет најчешћих врста инцидената у области информационог друштва

4.5.8. Остале области

	Група инцидената	Број инцидената
1.	Неовлашћено прикупљање података	8.581.618
2.	Покушај упада у ИКТ систем	2.349.592
3.	Инсталирање злонамерног софтвера у оквиру ИКТ система	9.911
4.	Превара	6.570
5.	Оперативни инциденти	4.702
6.	Недоступност или ограничена доступност ИКТ система	1.996
7.	Упад у ИКТ систем	1.140
8.	Остали инциденти	160
9.	Инциденти физичко техничке безбедности	100
10.	Угрожавање безбедности података	4
	УКУПНО	**10.955.793**

Табела 4.5.8.1 – 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 2024. године забележиле највише скенирања портова 8.579.503, на другом месту је покушај откривања креденцијала 2.283.308, на трећем покушај искоришћавања рањивости система 66.284, на четвртом тројанац 7.484 и на петом месту фишинг 6.002 (Графикон 4.5.8.1).

Графикон 4.5.8.1 – Пет најчешћих врста инцидената у осталим областима

4.5.8.1. Електронске комуникације

	Група инцидената	Број инцидената
1.	Оперативни инциденти	2.021
2.	Недоступност или ограничена доступност ИКТ система	185
3.	Инсталирање злонамерног софтвера у оквиру ИКТ система	124
4.	Превара	121
5.	Инциденти физичко техничке безбедности	98
6.	Остали инциденти	25
7.	Покушај упада у ИКТ систем	10
8.	Неовлашћено прикупљање података	3
9.	Упад у ИКТ систем	2
10.	Угрожавање безбедности података	0
	УКУПНО	**2.589**

Табела 4.5.8.1.1 – 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 2024. године детектовали највећи број отказивања хардверских компоненти 2.005, друго место заузима дистрибуирани напади са циљем онемогућавања или ометања функционисања ИКТ система (енгл. *DDoS*) 177, треће фишинг 121, четврто и пето место заузимају вирус 103 и крађа хардверских компоненти 96 (Графикон 4.5.8.1.1).

Графикон 4.5.8.1.1 – Пет најчешћих врста инцидената у области електронских комуникација

4.5.8.2. Издавање службеног гласила

	Група инцидената	Број инцидената
1.	Неовлашћено прикупљање података	14.760
2.	Оперативни инциденти	26
3.	Покушај упада у ИКТ систем	0
4.	Инсталирање злонамерног софтвера у оквиру ИКТ система	0
5.	Превара	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	**14.786**

Табела 4.5.8.2.1 – 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 2024. године детектовали највећи број скенирања портова 14.760, док се на другом месту налази проблеми у раду са софтверским компонентама којих је било 26 (Графикон 4.5.8.2.1).

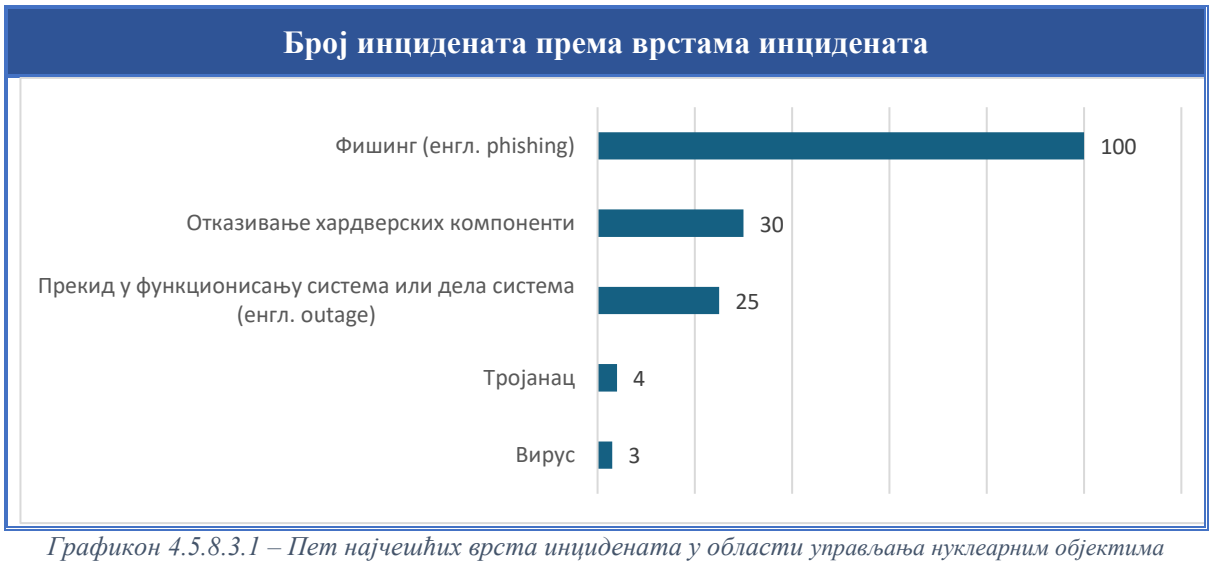
Графикон 4.5.8.2.1 – Пет најчешћих врста инцидената у области издавања службеног гласила

4.5.8.3. Управљање нуклеарним објектима

	Група инцидената	Број инцидената
1.	Превара	100
2.	Оперативни инциденти	30
3.	Недоступност или ограничена доступност ИКТ система	25
4.	Инсталирање злонамерног софтвера у оквиру ИКТ система	7
5.	Покушај упада у ИКТ систем	0
6.	Неовлашћено прикупљање података	0
7.	Упад у ИКТ систем	0
8.	Угрожавање безбедности података	0
9.	Инциденти физичко техничке безбедности	0
10.	Остали инциденти	0
	УКУПНО	**162**

Табела 4.5.8.3.1 – Број инцидената према групама инцидената у ИКТ системима од посебног значаја који се користе у обављању делатности у области управљања нуклеарним објектима

У области управљања нуклеарним објектима најзаступљенији напад је фишинг 100, на другом месту отказивање хардверских компоненти 30, на трећем прекид у функционисања система или дела система 25, док се на четвртом и петом месту налазе тројанац 4 и вирус 3 (Графикон 4.5.8.3.1).



Графикон 4.5.8.3.1 – Пет најчешћих врста инцидената у области управљања нуклеарним објектима

4.5.8.4. Производња, промет и превоз нуклеарног наоружања и војне опреме

	Група инцидената	Број инцидената
1.	Покушај упада у ИКТ систем	1.988.833
2.	Инсталирање злонамерног софтвера у оквиру ИКТ система	4.217
3.	Неовлашћено прикупљање података	2.065
4.	Недоступност или ограничена доступност ИКТ система	1.538
5.	Превара	1.046
6.	Упад у ИКТ систем	14
7.	Угрожавање безбедности података	4
8.	Оперативни инциденти	1
9.	Инциденти физичко техничке безбедности	0
10.	Остали инциденти	0
	УКУПНО	**1.997.718**

Табела 4.5.8.4.1 – 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 1.977.050, на другом месту је покушај искоришћавања рањивости система 11.783, на трећем тројанац 4.192, док се на четвртом месту налази компромитовање или цурење података 1.851, а на петом месту је напад са циљем онемогућавања или ометања функционисања ИКТ система (енгл. *DoS*) 1.531 (Графикон 4.5.8.4.1).

Графикон 4.5.8.4.1 – Пет најчешћих врста инцидената у области производње, промета и превоза нуклеарног наоружања и војне опреме

4.5.8.5. Управљање отпадом

	Група инцидената	Број инцидената
1.	Покушај упада у ИКТ систем	2.000
2.	Остали инциденти	125
3.	Недоступност или ограничена доступност ИКТ система	110
4.	Оперативни инциденти	54
5.	Превара	32
6.	Неовлашћено прикупљање података	20
7.	Инсталирање злонамерног софтвера у оквиру ИКТ система	6
8.	Упад у ИКТ систем	1
9.	Угрожавање безбедности података	0
10.	Инциденти физичко техничке безбедности	0
	УКУПНО	**2.348**

Табела 4.5.8.5.1 – 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 детектован је једнак број напада покушај искоришћавања рањивости система и покушај откривања креденцијала 1.000, на другом месту су инциденти који не спадају у горе наведене категорије 125, док су на трећем и четвртом месту прекид у функционисању система или дела система 110 и фишинг 32 (Графикон 4.5.8.5.1).

Графикон 4.5.8.5.1 – Пет најчешћих врста инцидената у области управљања отпадом

4.5.8.6. Комуналне делатности

	Група инцидената	Број инцидената
1.	Инсталирање злонамерног софтвера у оквиру ИКТ система	4.993
2.	Покушај упада у ИКТ систем	4.936
3.	Превара	4.458
4.	Оперативни инциденти	2.565
5.	Неовлашћено прикупљање података	238
6.	Недоступност или ограничена доступност ИКТ система	77
7.	Упад у ИКТ систем	51
8.	Остали инциденти	15
9.	Инциденти физичко техничке безбедности	2
10.	Угрожавање безбедности података	0
	УКУПНО	**17.335**

Табела 4.5.8.6.1 – Број инцидената према групама инцидената у ИКТ системима од посебног значаја који се користе у обављању делатности у области комуналних делатности

Током 2024. године су оператори ИКТ система од посебног значаја који обављају комуналне делатности забележили највећи број фишинг напада 4.458, на другом месту је тројанац 2.727, на трећем покушај искоришћавања рањивости система 2.642, на четвртом месту је покушај откривања креденцијала 2.294, док је на петом месту вирус 1.591 (Графикон 4.5.8.6.1).

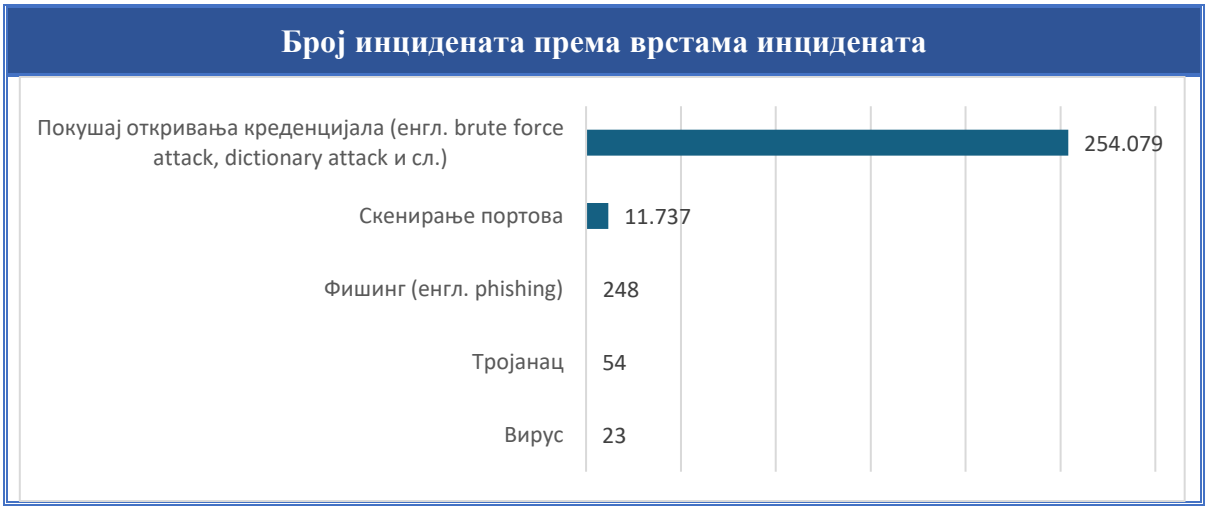
Графикон 4.5.8.6.1 – Пет најчешћих врста инцидената у области управљања отпадом

4.5.8.7. Производња и снабдевање хемикалијама

	Група инцидената	Број инцидената
1.	Покушај упада у ИКТ систем	254.079
2.	Неовлашћено прикупљање података	11.756
3.	Превара	248
4.	Инсталирање злонамерног софтвера у оквиру ИКТ система	77
5.	Оперативни инциденти	4
6.	Недоступност или ограничена доступност ИКТ система	2
7.	Упад у ИКТ систем	0
8.	Угрожавање безбедности података	0
9.	Инциденти физичко техничке безбедности	0
10.	Остали инциденти	0
	УКУПНО	**266.166**

Табела 4.5.8.7.1 – 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 2024. године била најизложенија нападима покушаја откривања креденцијала 254.079, скенирања портова 11.737, док је на трећем месту фишинг 248, а на четвртом и петом месту су тројанац 54 и вирус са 23 (Графикон 4.5.8.7.1).



Графикон 4.5.8.7.1 – Пет најчешћих врста инцидената у области производње и снабдевања хемикалијама

5. Закључак

Годишњи извештај о статистичким подацима свих инцидента пружа свеобухватан преглед сајбер напада на ИКТ системе од посебног значаја. Континуирано праћење ових података омогућава анализу трендова безбедносних претњи, што представља темељ за развој ефикасних стратегија за заштиту од актуелних напада и систематско јачање капацитета за сајбер отпорност.

Најзаступљенија врста инцидената је скенирање портова која припада групи напада неовлашћено прикупљање података. Ова група и врста напада су најзаступљеније од 2020. године од када се креира преглед статистичких података на годишњем нивоу. 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 дигиталној инфраструктури, услугама информационог друштва, за издавање службеног гласила, као и у ИКТ системима који се баве добрима од општег интереса који се односе на коришћење, управљање и заштиту и унапређење добара.

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, као и производњи и снабдевању хемикалијама.

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 *EUVD (European Union Vulnerability Database)*. *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, Национални ЦЕРТ операторима ИКТ система од посебног значаја пружа рана упозорења о откривеним рањивостима и начинима за ублажавање ризика насталог услед откривене рањивости.

Ова врста напада је најзаступљенија у ИКТ системима који управљају отпадом, а врло је заступљена и у енергетици, дигиталној инфраструктури, услугама информационог друштва, као и нуклеарним објектима, наоружању и војној опреми.

На четвртом месту се налази фишинг. Током 2024. године спроведено је неколико великих фишинг кампања чија су мета били грађани Србије, посебно корисници банкарских и поштанских услуга. Фишинг поруке су дистрибуиране наводно у име банака које послују на територији Републике Србије путем електронске поште, платформи за инстант комуникацију, SMS-ом, као и преко друштвених мрежа, и за циљ су имале прикупљање података грађана о банковним картицама. Национални ЦЕРТ је поводом ових фишинг напада објавио је 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 здравства, банкарства и финансија, управљању нуклеарним објектима и комуналним делатностима. Веома је заступљен у ИКТ системима који се користе у обављању послова у органима власти, у енергетици, у ИКТ системима који се баве добрима од општег интереса који се односе на коришћење, управљање, заштиту и унапређење добара од општег интереса, електронским комуникацијама, управљања отпадом и производњом и снабдевањем хемикалијама.

Имајући у виду значај групе напада - инсталирање злонамерног софтвера (малвера), треба напоменути да су током 2024. 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 те податке шаљу нападачима.

Ова врста малвера је најзаступљенија у ИКТ системима који се користе за обраду посебних података о личности, у смислу закона који уређује заштиту података о личности и у обављању делатности саобраћаја. Веома је заступљен у ИКТ системима који се користе у енергетици, у производњи, промету и превозу нуклеарног наоружања и војне опреме, комуналне делатности и производњом и снабдевањем хемикалијама.

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.

На другом месту по заступљености злонамерног софтвера је вирус. Вируси могу бити усмерени на масовно заражавање рачунарских мрежа, 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 нападачи користе методе социјалног инжењеринга које омогућавају лакши приступ запосленима и ИКТ системима у којима они раде. Вирус је нарочито заступљен у ИКТ системима који се користе у области саобраћаја, здравства, банкарства и финансијских тржишта, електронских комуникација, управљању нуклеарним објектима, комуналним делатностима и производњи и снабдевању хемикалијама.

Трећа најзаступљенија врста малвера је шпијунски софтвер који може да 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. Шпијунски софтвер је на трећем месту по заступљености код ИКТ система који се користе у области саобраћаја.

Покушај упада у ИКТ систем је у 2024. години доминантна група инцидената, али треба напоменути да је број ових напада мањи у односу на 2023. годину. Покушај откривања креденцијала (енгл. *brute force attack, dictionary attack* и сл.) је мањи за 34%, док је покушај искоришћавања рањивости система мањи за 64%. Смањење ових врста напада указује да се примењује вишеслојна заштита која обухвата техничке мере, свест корисника и проактивни мониторинг укључујући и редовно откривање и отклањање рањивости.

Током 2024. године, Национални ЦЕРТ је наставио са интензивним активностима усмереним на унапређење информационе безбедности, пружајући операторима ИКТ система од посебног значаја релевантне и благовремене информације о рањивостима високог и критичног нивоа опасности. Ове информације су од суштинског значаја за правовремено реаговање и спречавање потенцијалних безбедносних ризика, односно инцидената.

Имајући у виду значај досадашњих резултата у области раног упозоравања, као и потребу за систематичнијим и ефикаснијим приступом, креиран је систем за рана упозорења. Овај систем представља проактиван механизам осмишљен да омогући благовремено откривање и реаговање на потенцијалне пропусте, рањивости и сајбер нападе, пре него што они доведу до озбиљних последица по функционисање ИКТ система. Систем функционише кроз прикупљање, анализу и корелацију података у реалном времену, омогућавајући континуирано праћење стања у ИКТ окружењу. На основу добијених увида, систем генерише упозорења и конкретне препоруке за поступање, чиме се операторима омогућава да предузму превентивне мере и унапреде своје безбедносне капацитете.

Проактивно деловање, које подразумева спречавање напада у најранијој фази или ублажавање њихових последица, значајно доприноси повећању отпорности ИКТ система од посебног значаја. Оваквим приступом се не само смањује ризик од

инцидената, већ се и подиже укупни ниво информационе безбедности на националном нивоу.