ИЗВЕШТАЈ О СТАТИСТИЧКИМ ПОДАЦИМА О СВИМ ИНЦИДЕНТИМА У ИКТ СИСТЕМИМА ОД ПОСЕБНОГ ЗНАЧАЈА У 2025. ГОДИНИ

Јун, 2026. година

РАТЕЛ

СРБ-ЦЕРТ

Национални ЦЕРТ Републике Србије www.cert.rs

Садржај

Увод

Национални Национални центар за превенцију безбедносних ризика у ИКТ системима (у даљем тексту: Национални ЦЕРТ) је у периоду од почетка јануара до 28. фебруара 2026. године прикупљао статистичке податке о свим инцидентима у ИКТ системима од посебног значаја за 2025. годину, које су оператори ИКТ система од посебног значаја достављали у складу са досадашњом праксом.

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, Национални ЦЕРТ је пружио подршку операторима ИКТ система од посебног значаја.

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. Као ИКТ системи од посебног значаја препознати су:

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 28.02.2026. године, у складу са 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	336.919.194
2.	Покушај упада у ИКТ систем	7.084.352
3	Превара	232.898
4.	Инсталирање злонамерног софтвера у оквиру ИКТ система	29.835
5.	Остали инциденти	21.351
6.	Оперативни инциденти	9.417
7.	Недоступност или ограничена доступност ИКТ система	5.482
8.	Упад у ИКТ систем	510
9.	Инциденти физичко техничке безбедности	99
10.	Угрожавање безбедности података	10
	УКУПНО	**336.303.148**

Табела 2.2 – Број инцидената према групама инцидената

Најзаступљенија група инцидената је неовлашћено прикупљање података 336.919.194, у оквиру које је најдоминантнија врста инцидента скенирање портова. На другом месту је покушај упада у ИКТ систем 7.084.352 у оквиру које је најзаступљенији инцидент покушај откривања креденцијала. На трећем месту се налази превара 232.898 у оквиру које је најзаступљенији фишинг. Четврто место заузима инсталирање злонамерног софтвера у оквиру ИКТ система 29.835, најчешће тројанац. На петом месту су остали инциденти 21.351 (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	9.191
	Црв	499
	Рансомвер	48
	Тројанац	13.153
	Шпијунски софтвер	6.930
	Руткит	14
Неовлашћено прикупљање података	Скенирање портова	328.913.543
	Пресретање података између рачунара и сервера	33
	Социјални инжењеринг	2.784
	Компромитовање или цурење података	2.834
Превара	Фишинг	232.883
	Неовлашћено коришћење ресурса	15
Покушај упада у ИКТ систем	Покушај искоришћавања рањивости система	903.392
	Покушај откривања креденцијала	6.180.960

Група инцидената	Врста инцидента	Број инцидената
Упад у ИКТ систем	Откривање или неовлашћено коришћење привилегованих налога	10
	Откривање или неовлашћено коришћење непривилегованих налога	79
	Неовлашћени приступ апликацији	9
	Мрежа заражених уређаја	412
Недоступност или ограничена доступност ИКТ система	Напад са циљем онемогућавања или ометања функционисања ИКТ система	48
	Дистрибуирани напад са циљем онемогућавања или ометања функционисања ИКТ система	3.537
	Саботажа	0
	Прекид у функционисању система или дела система	1.897
Угрожавање безбедности података	Неовлашћен приступ подацима	5
	Неовлашћена измена или брисање података	5
	Криптографски напад	0
Оперативни инциденти	Отказивање хардверских компоненти	3.686
	Проблеми у раду са софтверским компонентама	5.731
Инциденти физичко-техничке безбедности	Крађа хардверских компоненти	90
	Пожар	5
	Поплава	4
Остали инциденти	Инциденти који не спадају у наведене категорије	21.351
	УКУПНО	**336.303.148**

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 29.835 инцидената, а најзаступљенији је тројанац 13.153 (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.

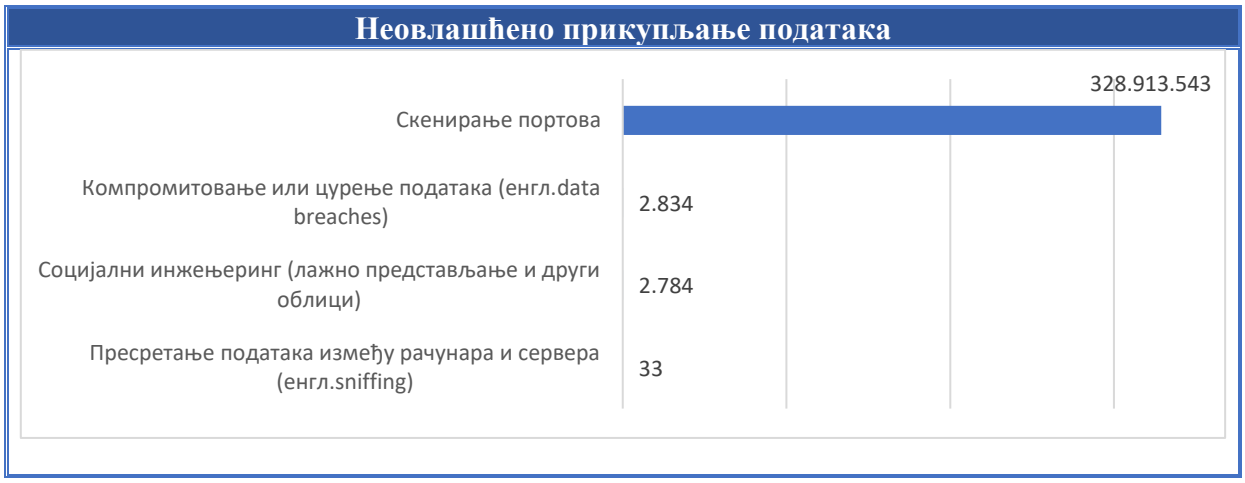
Снифинг напад, односно пресретање података подразумева коришћење апликација за надгледање, анализу и снимање мрежног саобраћаја у циљу прикупљања мрежних пакета. На овај начин нападач анализира мрежу и прибавља информације којим је може компромитовати.

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 328.913.543 скенирања портова што се као и претходне године може објаснити великим бројем аутоматизованих процеса за испитивање доступних сервиса на удаљеним рачунарима, 2.834 компромитовања или цурења

података, 2.784 социјалног инжењеринга и 33 пресретања података између рачунара и сервера, односно укупно 328.919.194 напада (Графикон 3.2.1).



Графикон 3.2.1 – Неовлашћено прикупљање података

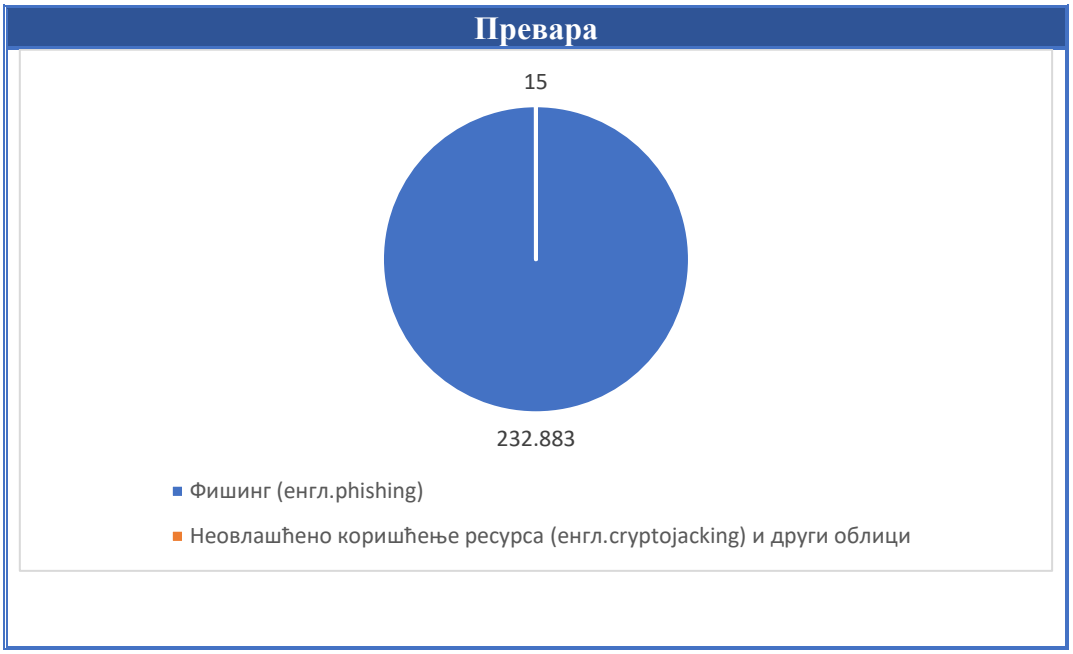
3.3. Превара

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

Фишинг је сајбер напад који се врши уз помоћ електронске поште, друштвених 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 2025. години износи 232.883, док за неовлашћено коришћење ресурса износи 15 (Графикон 3.3.1).



Графикон 3.3.1 – Превара у ИКТ системима од посебног значаја

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 2025. години нападачи су у највећој мери за упад у систем користили технике откривања креденцијала 6.180.960, док је забележен број покушаја искоришћавања рањивости система 903.392, 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.

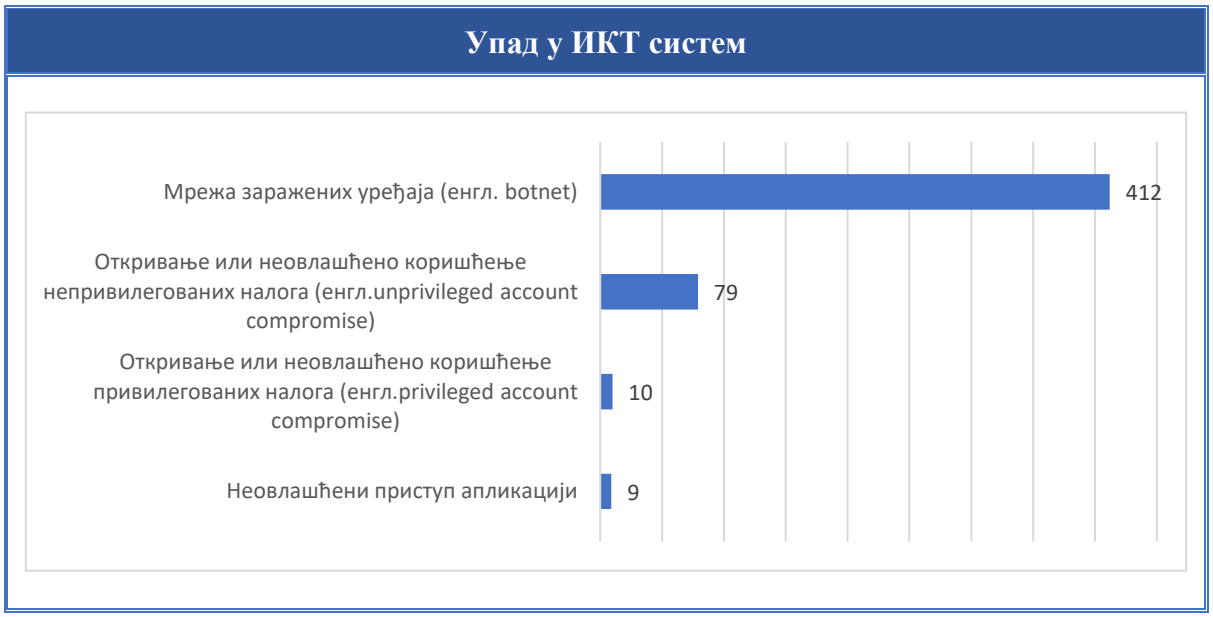
Откривање или неовлашћено коришћење непривилегованих налога (енгл. *Unprivileged Account Compromise*) омогућава нападачима да се крећу кроз ограничени део ИКТ система, са могућношћу даље компромитације ИКТ система и приступања осетљивим подацима.

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 2025. години је у оквиру групе инцидената упад у ИКТ систем био је најзаступљенији напад мрежа заражених уређаја 412, затим откривање или неовлашћено коришћење

непривилегованих налога 79, откривање или неовлашћено коришћење привилегованих налога 10 и неовлашћени приступ апликацији 9 (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.

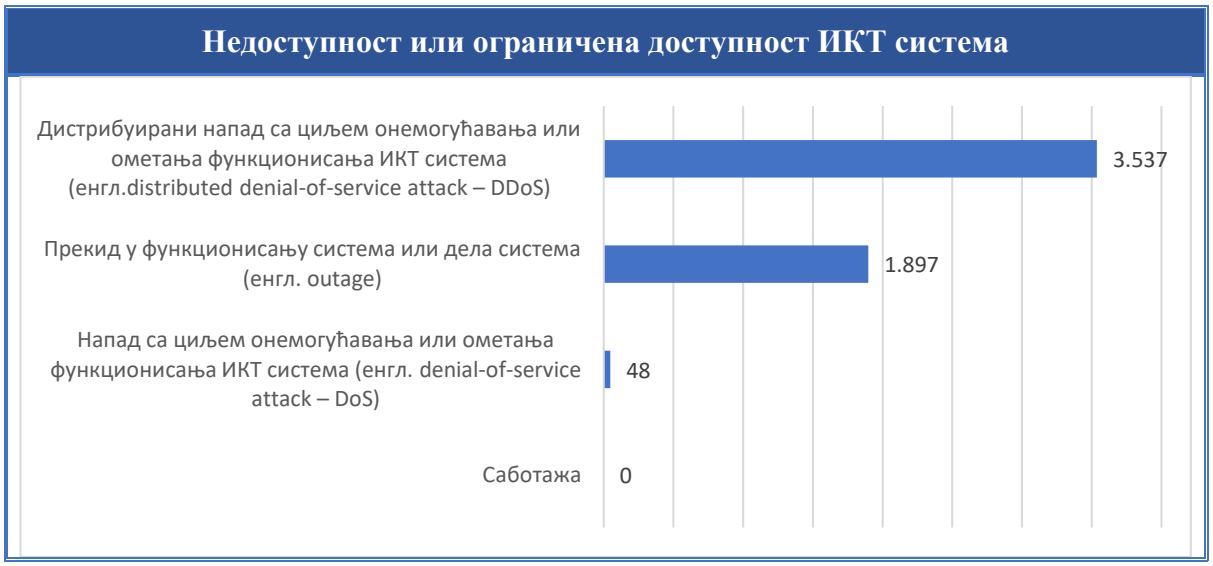
Напад са циљем онемогућавања или ометања функционисања ИКТ система (енгл. *denial-of-service attack – DoS*) је покушај нападача да онемогући приступ серверу или сервисима који су намењени крајњим корисницима.

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 3.537 *DDoS* напада, 1.897 прекида у функционисању система или дела система, 48 напада са циљем онемогућавања или ометања функционисања ИКТ система и 0 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 2025. години је забележено 5 неовлашћених приступа подацима, 5 неовлашћених измена или брисања података и 0 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 5.731, а број отказивања хардверских компоненти 3.686 (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 2025. години забележено је 90 крађа хардверских компоненти, 5 пожара и 4 поплаве (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 2025. години је било 21.351 (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	161.261
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	1
3.	ИКТ системи од посебног значаја који се користе у обављању делатности од општег интереса и другим делатностима и то:	
	енергетика	2.305.215
	саобраћај	3.105
	здравство	33.423
	банкарство и финансијска тржишта	48.338
	дигитална инфраструктура	330.484.800
	добра од општег интереса који се односе на коришћење, управљање, заштиту и унапређење добара од општег интереса	13.089
	услуге информационог друштва	1.620.103
	остале области:	
	- Електронске комуникације	1.620.071
	- Издавање службеног гласила Републике Србије	1050
	- Управљање нуклеарним објектима	281
	- Производња, промет и превоз наоружања и војне опреме	2.136.129
	- Управљање отпадом	432
	- Комуналне делатности	3.252.025
	- Производња и снабдевање хемикалијама	307
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	5.438.909

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	112.105
2.	Превара	21.068
3.	Инсталирање злонамерног софтвера у оквиру ИКТ система	10.764
4.	Остали инциденти	4.832
5.	Неовлашћено прикупљање података	4.641
6.	Оперативни инциденти	4.402
7.	Недоступност или ограничена доступност ИКТ система	3.387
8.	Упад у ИКТ систем	56
9.	Инциденти физичко техничке безбедности	4
10.	Угрожавање безбедности података	2
	УКУПНО	**161.261**

Табела 4.1.1 – Број инцидената према групама инцидената у органима власти

Током 2025. године у ИКТ системима који се користе у органима власти забележено је највише покушаја откривања креденцијала 110.238, на другом месту је фишинг 21.066, на трећем и четвртом месту налазе се вирус 5.462 и инциденти који не спадају у горе наведене категорије 4.832, док је тројанац на петом месту са 4.411 пријаве (Графикон 4.1.1).

Графикон 4.1.1 – Пет најчешћих врста инцидената у органима власти

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 2025. године пријављен је 1 покушај искоришћавања рањивости система (Графикон 4.2.1).

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

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

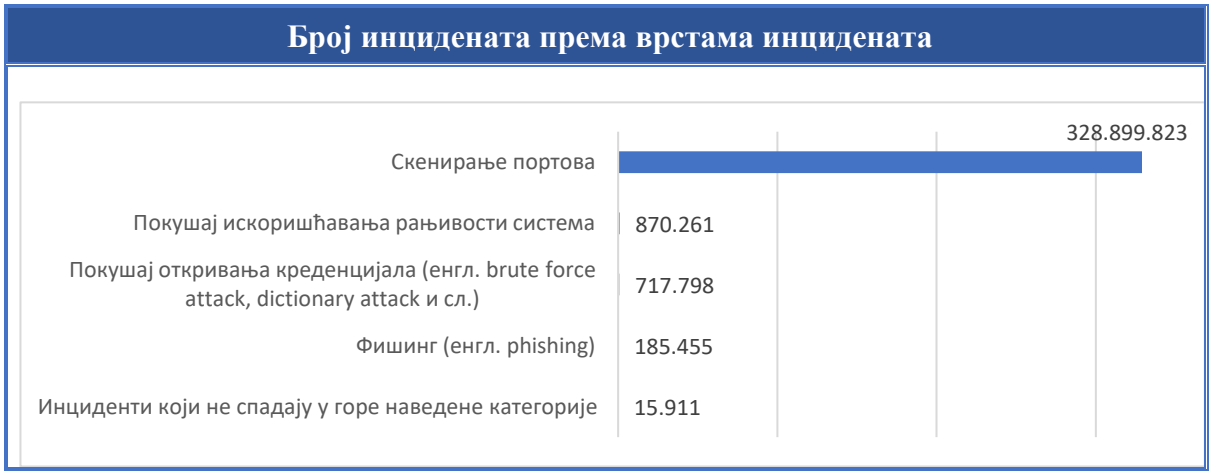
Графикон 4.2.1 – Број инцидената према врстама инцидената који се користе за обраду посебних врста података о личности

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

	Група инцидената	Број инцидената
1.	Неовлашћено прикупљање података	328.900.625
2.	Покушај упада у ИКТ систем	1.588.059
3.	Превара	185.459
4.	Остали инциденти	15.911
5.	Инсталирање злонамерног софтвера у оквиру ИКТ система	9.448
6.	Оперативни инциденти	2.087
7.	Недоступност или ограничена доступност ИКТ система	913
8.	Упад у ИКТ систем	262
9.	Инциденти физичко техничке безбедности	85
10.	Угрожавање безбедности података	6
	УКУПНО	**330.702.856**

Табела 4.3.1 – Број инцидената према групама инцидената у ИКТ системима од посебног значаја који се користе у обављању делатности од општег интереса и другим делатностима

Ова врста ИКТ система је током 2025. године била најизложенија нападима скенирања портова 328.899.823, на другом месту је покушај искоришћавања рањивости система 870.261, на трећем покушај откривања креденцијала 717.798, на четвртом фишинг 185.455 и на петом инциденти који не спадају у горе наведене категорије 15.911 (Графикон 4.3.1).



Графикон 4.3.1 –Пет најчешћих врста инцидената у ИКТ системима од посебног значаја који се користе у обављању делатности од општег интереса и другим делатностима

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	5.384.182
2.	Превара	26.267
3.	Неовлашћено прикупљање података	13.927
4.	Инсталирање злонамерног софтвера у оквиру ИКТ система	9.616
5.	Оперативни инциденти	2.925
6.	Недоступност или ограничена доступност ИКТ система	1.180
7.	Остали инциденти	608
8.	Упад у ИКТ систем	192
9.	Инциденти физичко техничке безбедности	10
10.	Угрожавање безбедности података	2
	УКУПНО	**5.438.909**

Табела 4.4.1 – Број инцидената према групама 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

Најчешћи напади на ову врсту ИКТ система током 2025. године су покушај откривања креденцијала 5.352.920, на другом месту покушај искоришћавања рањивости система 31.262, на трећем фишинг 26.258, на четвртом скенирање портова 9.604 и на петом месту тројанац 5.753 (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

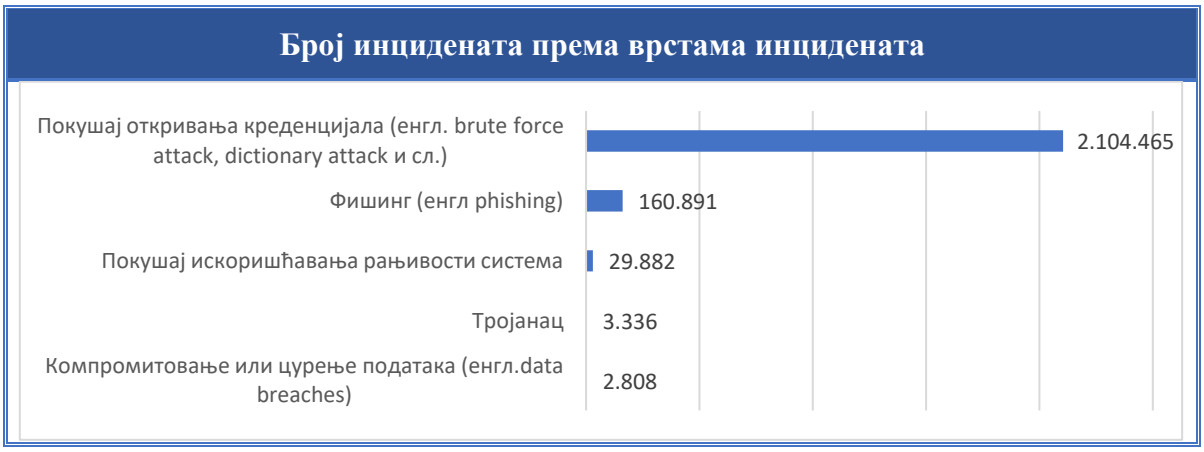
4.5. Преглед према делатности ИКТ система од посебног значаја

4.5.1. Енергетика

	Група инцидената	Број инцидената
1.	Покушај упада у ИКТ систем	2.134.347
2.	Превара	160.897
3.	Неовлашћено прикупљање података	4.869
4.	Инсталирање злонамерног софтвера у оквиру ИКТ система	3.670
5.	Оперативни инциденти	1.031
6.	Остали инциденти	315
7.	Недоступност или ограничена доступност ИКТ система	56
8.	Упад у ИКТ систем	24
9.	Инциденти физичко техничке безбедности	5
10.	Угрожавање безбедности података	1
	УКУПНО	**2.305.215**

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 2025. години био је покушај откривања креденцијала 2.104.465, на другом месту је фишинг 160.891, треће место заузима покушај искоришћавања рањивости система 29.882, док су на четвртом и петом месту тројанац 3.336 и компромитовање или цурење података 2.808 (Графикон 4.5.1.1).



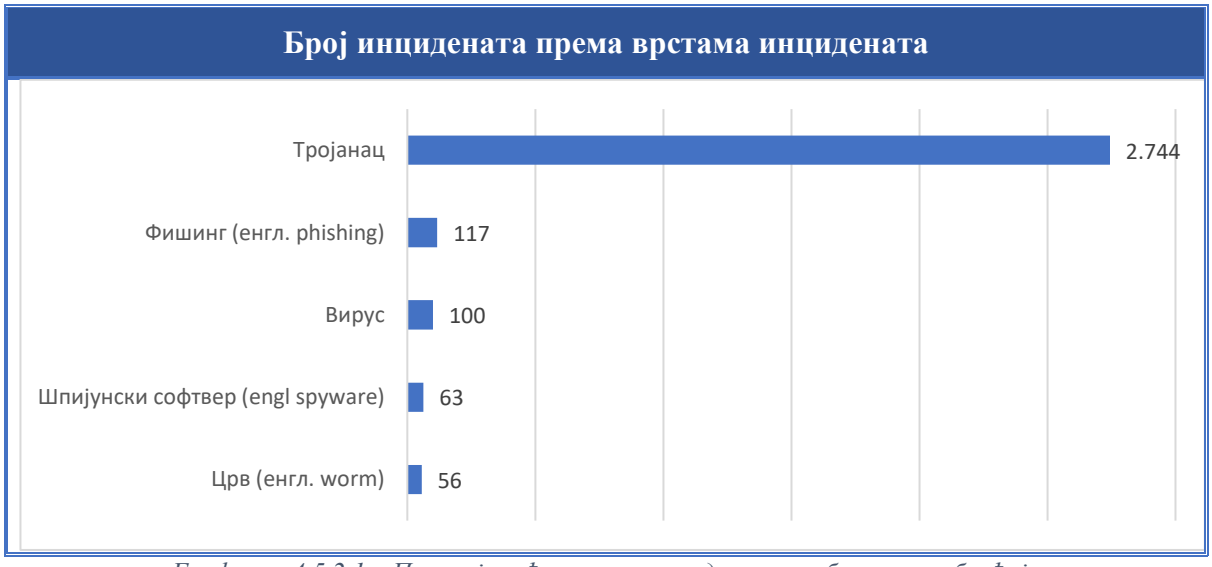
Графикон 4.5.1.1 – Пет најчешћих врста инцидената у области енергетике

4.5.2. Саобраћај

	Група инцидената	Број инцидената
1.	Инсталирање злонамерног софтвера у оквиру ИКТ система	2.963
2.	Превара	117
3.	Недоступност или ограничена доступност ИКТ система	12
4.	Оперативни инциденти	7
5.	Неовлашћено прикупљање података	2
6.	Покушај упада у ИКТ систем	1
7.	Упад у ИКТ систем	1
8.	Инциденти физичко техничке безбедности	1
9.	Угрожавање безбедности података	1
10.	Остали инциденти	0
	УКУПНО	**3.105**

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 2025. године забележен је највећи број пријава тројанца 2.744, други по заступљености је фишинг 117, треће место заузима вирус 100, четврто шпијунски софтвер 63, док је на петом месту црв 56 (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	22.479
2.	Покушај упада у ИКТ систем	8.142
3.	Оперативни инциденти	868
4.	Неовлашћено прикупљање података	861
5.	Инсталирање злонамерног софтвера у оквиру ИКТ система	686
6.	Остали инциденти	283
7.	Недоступност или ограничена доступност ИКТ система	77
8.	Упад у ИКТ систем	25
9.	Инциденти физичко техничке безбедности	2
10.	Угрожавање безбедности података	0
	УКУПНО	**33.423**

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

Током 2025. године у здравственом сектору најзаступљенији напад је фишинг 22.477, на другом месту налази се покушај откривања креденцијала 7.778, на трећем социјални инжењеринг 524, затим на четвртом месту отказивање хардверских компоненти 474 и на петом месту тројанац 430 (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.	Остали инциденти	15.852
2.	Покушај упада у ИКТ систем	15.388
3.	Инсталирање злонамерног софтвера у оквиру ИКТ система	6.476
4.	Превара	5.408
5.	Неовлашћено прикупљање података	4.122
6.	Недоступност или ограничена доступност ИКТ система	688
7.	Упад у ИКТ систем	261
8.	Оперативни инциденти	138
9.	Угрожавање безбедности података	3
10.	Инциденти физичко техничке безбедности	2
	УКУПНО	**48.388**

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 инцидената који не спадају у горе наведене категорије 15.852, на другом месту је покушај откривања креденцијала 15.383, следи фишинг 5.404, четвртом шпијунски софтвер 4.722 и на петом месту је скенирање портова 3.411 (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	328.894.875
2.	Покушај упада у ИКТ систем	1.567.127
3.	Превара	20.755
4.	Оперативни инциденти	1.886
5.	Недоступност или ограничена доступност ИКТ система	113
6.	Остали инциденти	26
7.	Инсталирање злонамерног софтвера у оквиру ИКТ система	10
8.	Инциденти физичко техничке безбедности	8
9.	Упад у ИКТ систем	0
10.	Угрожавање безбедности података	0
	УКУПНО	**330.484.800**

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 2025. године била најизложенија скенирању портова 328.894.875, на другом месту је покушај искоришћавања рањивости система 870.206, на трећем покушај откривања креденцијала 696.921, док су на четвртом и петом месту фишинг 20.775 и отказивање хардверских компоненти 1.875 (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	7.625
2.	Инсталирање злонамерног софтвера у оквиру ИКТ система	2.353
3.	Покушај упада у ИКТ систем	1.180
4.	Оперативни инциденти	864
5.	Превара	779
6.	Недоступност или ограничена доступност ИКТ система	301
7.	Упад у ИКТ систем	5
8.	Угрожавање безбедности података	0
9.	Инциденти физичко техничке безбедности	0
10.	Остали инциденти	0
	УКУПНО	**13.089**

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 2025. године забележили на првом месту скенирање портова 7.072, шпијунски софтвер 1.106 је на другом месту, док су на трећем, четвртом и петом месту тројанац 1.015, фишинг 779 и покушај откривања креденцијала 772 (Графикон 4.5.6.1).

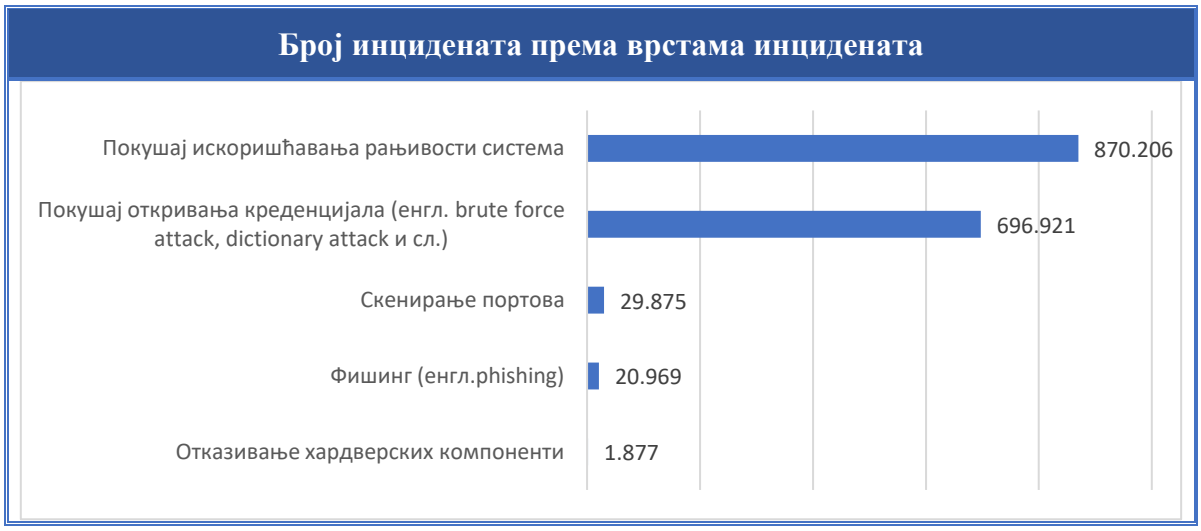
Графикон 4.5.6.1 – Пет најчешћих врста инцидената у области добра од општег интереса који се односе на коришћење, управљање, заштиту и унапређење добара

4.5.7. Услуге информационог друштва

	Група инцидената	Број инцидената
1.	Покушај упада у ИКТ систем	1.567.127
2.	Неовлашћено прикупљање података	29.890
3.	Превара	20.969
4.	Оперативни инциденти	1.889
5.	Недоступност или ограничена доступност ИКТ система	144
6.	Инсталирање злонамерног софтвера у оквиру ИКТ система	48
7.	Остали инциденти	28
8.	Инциденти физичко техничке безбедности	8
9.	Упад у ИКТ систем	0
10.	Угрожавање безбедности података	0
	УКУПНО	**1.620.103**

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 покушаја искоришћавања рањивости система 870.206, на другом месту је покушај откривања креденцијала 696.921, на трећем скенирање портова 29.875, четвртом фишинг 20.969 и петом месту отказивање хардверских компоненти 1.877 (Графикон 4.5.7.1).



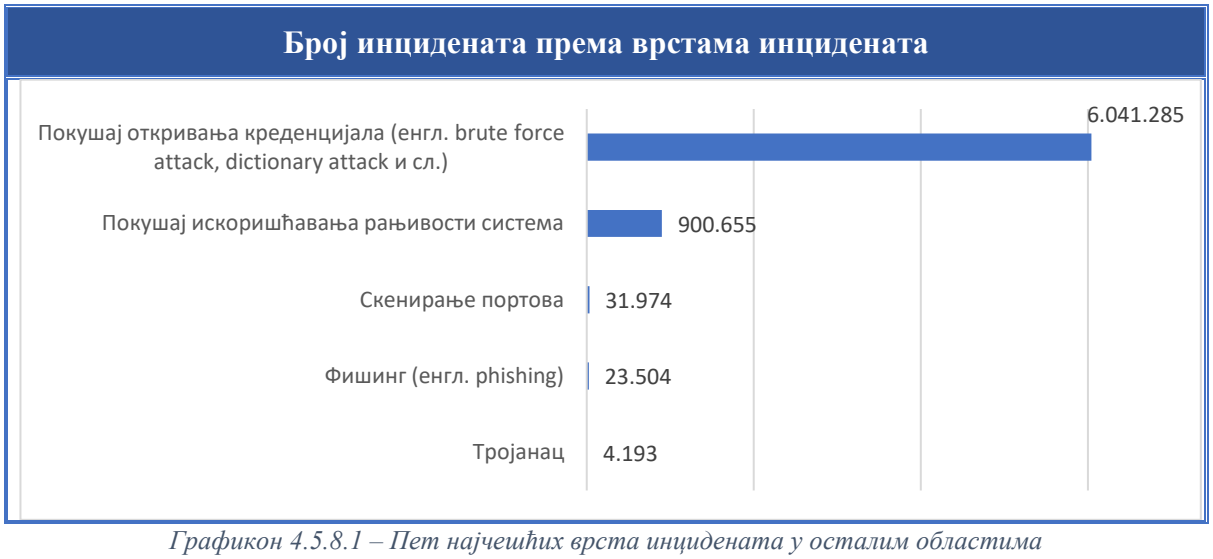
Графикон 4.5.7.1 – Пет најчешћих врста инцидената у области информационог друштва

4.5.8. Остале области

	Група инцидената	Број инцидената
1.	Покушај упада у ИКТ систем	6.941.940
2.	Неовлашћено прикупљање података	34.885
3.	Превара	23.511
4.	Инсталирање злонамерног софтвера у оквиру ИКТ система	6.130
5.	Оперативни инциденти	2.304
6.	Недоступност или ограничена доступност ИКТ система	939
7.	Остали инциденти	317
8.	Упад у ИКТ систем	141
9.	Инциденти физичко техничке безбедности	86
10.	Угрожавање безбедности података	3
	УКУПНО	**7.010.256**

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 2025. године забележиле највише покушаја откривања креденцијала 6.041.285, на другом месту је покушај искоришћавања рањивости система 900.655, на трећем скенирање портова 31.974, на четвртом фишинг 23.504 и на петом месту тројанац 4.193 (Графикон 4.5.8.1).



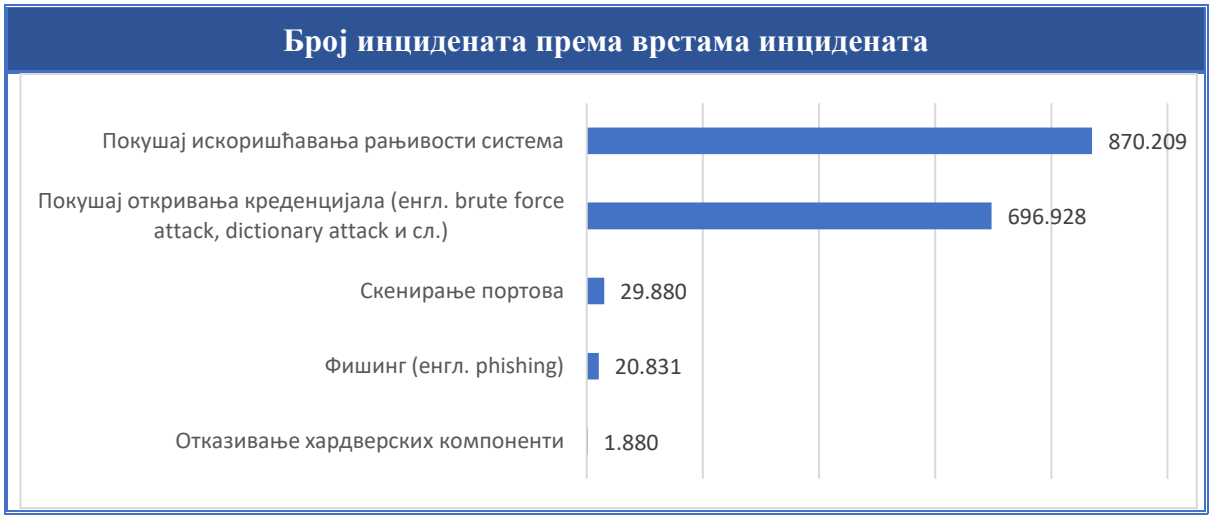
Графикон 4.5.8.1 – Пет најчешћих врста инцидената у осталим областима

4.5.8.1. Електронске комуникације

	Група инцидената	Број инцидената
1.	Покушај упада у ИКТ систем	1.567.137
2.	Неовлашћено прикупљање података	29.885
3.	Превара	20.831
4.	Оперативни инциденти	1.900
5.	Недоступност или ограничена доступност ИКТ система	122
6.	Инциденти физичко техничке безбедности	82
7.	Остали инциденти	57
8.	Инсталирање злонамерног софтвера у оквиру ИКТ система	55
9.	Угрожавање безбедности података	2
10.	Упад у ИКТ систем	0
	УКУПНО	**1.620.071**

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 2025. године детектовали највећи број покушаја искоришћавања рањивости система 870.209, друго место заузима покушај откривања креденцијала 696.928, треће скенирање портова 29.880, четврто и пето место заузимају фишинг 20.831 и отказивање хардверских компоненти 1.880 (Графикон 4.5.8.1.1).



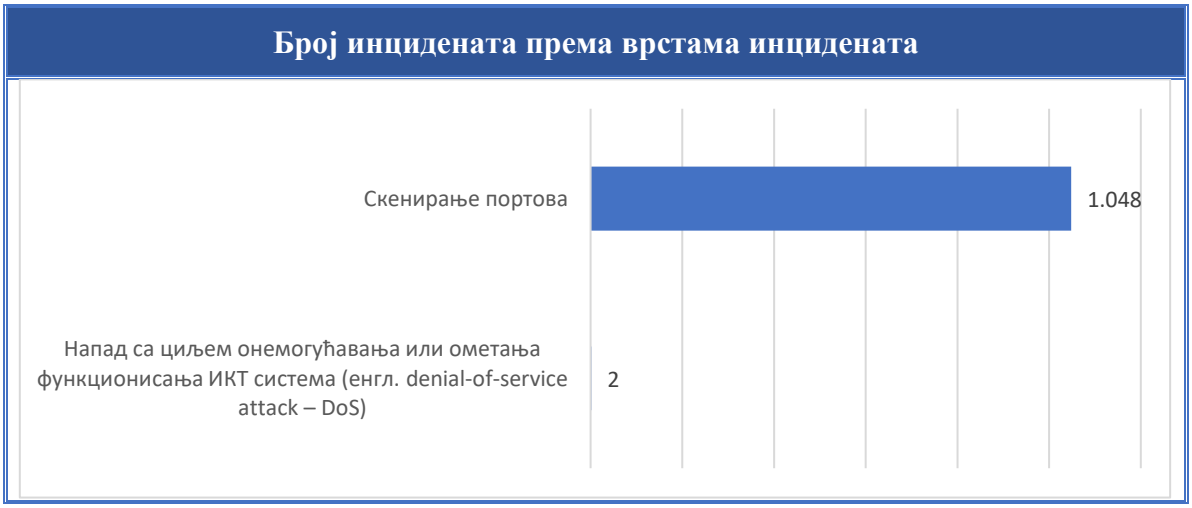
Графикон 4.5.8.1.1 – Пет најчешћих врста инцидената у области електронских комуникација

4.5.8.2. Издавање службеног гласила

	Група инцидената	Број инцидената
1.	Неовлашћено прикупљање података	1048
2.	Недоступност или ограничена доступност ИКТ система	2
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.	Оперативни инциденти	0
8.	Угрожавање безбедности података	0
9.	Инциденти физичко техничке безбедности	0
10.	Остали инциденти	0
	УКУПНО	**1050**

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 2025. године детектовали највећи број скенирања портова 1.048, док се на другом месту налази напад са циљем онемогућавања или ометања функционисања ИКТ система 2 (Графикон 4.5.8.2.1).



Графикон 4.5.8.2.1 – Најчешћа врста инцидената у области издавања службеног гласила

4.5.8.3. Управљање нуклеарним објектима

	Група инцидената	Број инцидената
1.	Превара	100
2.	Неовлашћено прикупљање података	51
3.	Недоступност или ограничена доступност ИКТ система	50
4.	Оперативни инциденти	46
5.	Инсталирање злонамерног софтвера у оквиру ИКТ система	28
6.	Покушај упада у ИКТ систем	6
7.	Упад у ИКТ систем	0
8.	Угрожавање безбедности података	0
9.	Инциденти физичко техничке безбедности	0
10.	Остали инциденти	0
	УКУПНО	**281**

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 са једнаким бројем су прекид у функционисања система или дела система и социјални инжењеринг 50, док се на трећем и четвртом месту налазе отказивање хардверских компоненти 46 и тројанац 15 (Графикон 4.5.8.3.1).

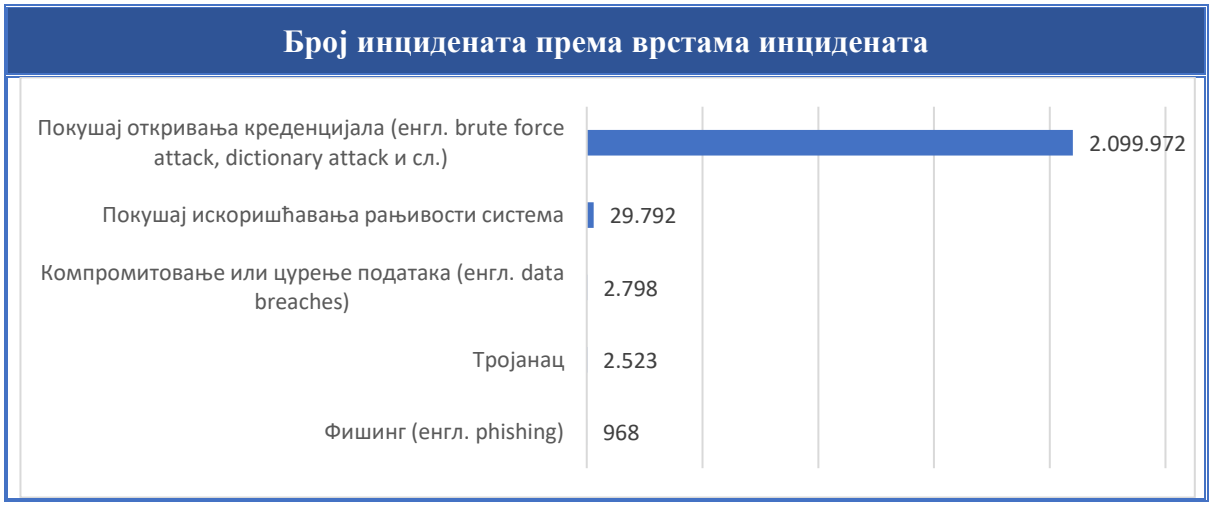
Графикон 4.5.8.3.1 – Пет најчешћих врста инцидената у области управљања нуклеарним објектима

4.5.8.4. Производња, промет и превоз наоружања и војне опреме

	Група инцидената	Број инцидената
1.	Покушај упада у ИКТ систем	2.129.764
2.	Неовлашћено прикупљање података	2.829
3.	Инсталирање злонамерног софтвера у оквиру ИКТ система	2.549
4.	Превара	974
5.	Недоступност или ограничена доступност ИКТ система	5
6.	Оперативни инциденти	5
7.	Упад у ИКТ систем	3
8.	Угрожавање безбедности података	0
9.	Инциденти физичко техничке безбедности	0
10.	Остали инциденти	0
	УКУПНО	**2.136.129**

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 наоружања и војне опреме

У области производње, промета и превоза наоружања и војне опреме најзаступљенији напад је покушај откривања креденцијала 2.099.972, на другом месту је покушај искоришћавања рањивости система 29.792, на трећем компромитовање или цурење података 2.798, док се на четвртом месту налази тројанац 2.523, а на петом месту фишинг 968 (Графикон 4.5.8.4.1).



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

4.5.8.5. Управљање отпадом

	Група инцидената	Број инцидената
1.	Остали инциденти	250
2.	Недоступност или ограничена доступност ИКТ система	58
3.	Неовлашћено прикупљање података	46
4.	Оперативни инциденти	43
5.	Превара	29
6.	Инсталирање злонамерног софтвера у оквиру ИКТ система	3
7.	Инциденти физичко техничке безбедности	3
8.	Покушај упада у ИКТ систем	0
9.	Упад у ИКТ систем	0
10.	Угрожавање безбедности података	0
	УКУПНО	**432**

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 детектовано је у највећем броју инциденти који не спадају у горе наведене категорије 250, на другом месту је прекид у функционисању система или дела система 58, на трећем је социјални инжењеринг 46, док су на четвртом и петом месту фишинг 29 и отказивање хардверских компоненти 25 (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.	Покушај упада у ИКТ систем	3.245.033
2.	Инсталирање злонамерног софтвера у оквиру ИКТ система	3.376
3.	Превара	1.401
4.	Неовлашћено прикупљање података	1.046
5.	Недоступност или ограничена доступност ИКТ система	704
6.	Оперативни инциденти	313
7.	Упад у ИКТ систем	138
8.	Остали инциденти	10
9.	Инциденти физичко техничке безбедности	3
10.	Угрожавање безбедности података	1
	УКУПНО	**3.252.025**

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 2025. године су оператори ИКТ система од посебног значаја који обављају комуналне делатности забележили највећи број покушаја откривања креденцијала 3.244.384, на другом месту је тројанац 1.519, на трећем вирус 1.404, на четвртом месту је фишинг 1.400, док је на петом месту скенирање портова 1.014 (Графикон 4.5.8.6.1).

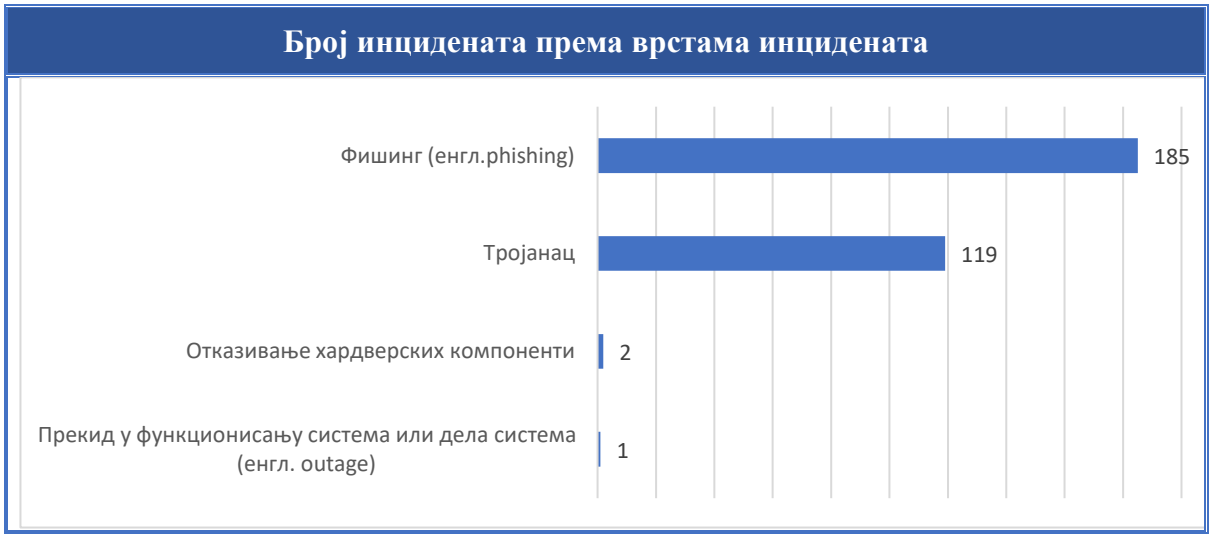
Графикон 4.5.8.6.1 – Пет најчешћих врста инцидената у области комуналних делатности

4.5.8.7. Производња и снабдевање хемикалијама

	Група инцидената	Број инцидената
1.	Превара	185
2.	Инсталирање злонамерног софтвера у оквиру ИКТ система	119
3.	Оперативни инциденти	2
4.	Недоступност или ограничена доступност ИКТ система	1
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	**307**

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 2025. године била најизложенија нападима фишинга 185 и тројанца 119, док су на трећем и четвртом месту отказивање хардверских компоненти 2 и прекид у функционисању система или дела система 1 (Графикон 4.5.8.7.1).



Графикон 4.5.8.7.1 – Најчешћа врста инцидената у области производње и снабдевања хемикалијама

5. Закључак

Годишњи извештај о статистичким подацима о свим инцидентима пружа свеобухватан преглед сајбер напада на ИКТ системе од посебног значаја. Праћење ових података пружа могућност за анализу трендова безбедносних претњи, што представља основу за развој ефикасних стратегија за заштиту од актуелних напада и јачање капацитета за сајбер отпорност.

Врста инцидената која преовлађује је скенирање портова и 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 индентификација отворених портова и активних сервиса како би се открили и искористиле потенцијалне рањивости система. Висок проценат заступљености директна је последица 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, 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 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, у области енергетике, комуналних делатности и производње, промета и превоза наоружања и војне опреме. Такође у великој мери је заступљена у области здравства, банкарства и финансијских тржишта, дигиталне инфраструктуре, информационог друштва и електронских комуникација.

Треће место заузима покушај искоришћавања рањивости система, односно 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 од посебног значаја који се користе за обраду посебних врста података о личности, у смислу закона који уређује заштиту података личности, као и у области информационог друштва и електронских комуникација. Такође, врло је заступљена у области енергетике, дигиталне инфраструктуре, производње, промета и превоза наоружања и војне опреме, као и 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.

На четвртом месту се налази фишинг. Током 2025. године спроведено је неколико великих фишинг кампања чија су мета били грађани Србије. У оквиру ових кампања злоупотребљени су називи и визуелна обележја организација, као што су ЈП Пошта Србије, Електропривреда Србије, Телеком Србија, mts, Путеви Србије, Air Serbia, Пореска управа Републике Србије и Управа за трезор, при чему су посебно били угрожени корисници банкарских услуга. Фишинг поруке су дистрибуиране 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 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, управљању нуклеарним објектима и производњом и снабдевањем хемикалијама. Веома је заступљен у ИКТ системима који се користе у обављању послова у органима власти, у енергетици, саобраћају, банкарству и финансијским тржиштима као и ИКТ системима од посебног значаја који се користи у правним лицима које оснива Република Србија, аутономна покрајина или јединица локалне самоуправе за обављање делатности од општег интереса.

С обзиром на значај групе напада - инсталирање злонамерног софтвера (малвера), треба напоменути да су током 2025. године најзаступљеније врсте малвера биле тројанац, вирус и шпијунски софтвер.

Тројанац је врста злонамерног софтвера који се представља као користан програм, како би преварио кориснике да га покрену. Након инсталације тројанац може да преузима додатне претње са интернета, инсталира друге врсте малвера на заражени рачунар, успоставља комуникацију са удаљеним нападачима и бележи све што корисник уноси преко тастатуре. Прикупљени подаци се шаљу нападачима, што може довести до крађе личних података и других корисних информација.

Ова врста малвера је најзаступљенија у ИКТ системима који се користе у обављању делатности саобраћаја. Веома је заступљен у ИКТ системима који се користе у области добра од општег интереса, која се односе на коришћење, управљање, заштиту и унапређење добара, у обављању комуналне делатности и у области производње и снабдевања хемикалијама.

Тројанац, као један од најстаријих облика злонамерног софтвера и даље показује велику издржљивост и способност прилагођавања. 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 од посебног значаја који се користе у обављању послова у органима власти, у области саобраћаја и комуналних делатности.

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 другом месту по заступљености у ИКТ системима који се користе у области добра од општег интереса који се односе на коришћење, управљање, заштиту и унапређење добара и на четвртом месту по заступљености у области саобраћаја, банкарства и финансијских тржишта.

Покушај упада у ИКТ систем је у 2025. години доминантна група инцидената, али треба напоменути да је број ових напада приближно три пута већи у односу на 2024. годину. Покушаји откривања креденцијала (укључујући *brute force* и *dictionary* нападе) забележили су значајан раст, са 2.352.887 на 6.180.960 инцидената. Истовремено, број покушаја експлоатације рањивости система порастао је са 68.801 на 903.392. Овај пораст резултат је више међусобно повезаних фактора. Пре свега, присутна је изразита аутоматизација напада, која омогућава извођење великог броја покушаја у кратком временском периоду, често кроз дистрибуиране *botnet* мреже и компромитоване инфраструктуре. Додатно, ширење дигиталних сервиса и *cloud* окружења повећава површину изложену нападима, док неуједначен ниво имплементације безбедносних контрола доприноси већој изложености система. Вештачка интелигенција и алати засновани на аутоматизацији доприносе ефикасности напада, пре свега кроз оптимизацију генерисања лозинки, адаптивно тестирање креденцијала и бржу анализу

компромитованих података. Међутим, једнако значајан утицај имају и фактори као што су недовољна примена вишефакторске аутентификације (*multifactor authentication* – MFA), као и спорије усклађивање безбедносних пракси са убрзаном дигитализацијом.

Национални ЦЕРТ је током 2025. године наставио активности на јачању информационе безбедности, обезбеђујући операторима ИКТ система од посебног значаја правовремене информације о рањивостима високог и критичног нивоа опасности, неопходне за превенцију и спречавање потенцијалних ризика и инцидената.

Узимајући у обзир важност раног упозоравања, као и потребу за систематичнијим и ефикаснијим приступом, користи се систем који је креиран за пружање за раних 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 изворних података, систем генерише упозорења и препоруке за поступање, чиме се операторима омогућава да предузму одговарајуће мере и подигну ниво безбедности.

У процесу пружања упозорења користи се и *threat intelligence* платформа, која омогућава ефикасну обраду података из неструктуираних извора, визуализацију претњи, напредну претрагу и континуирано праћење безбедносног стања у мрежном окружењу. Платформа омогућава интеграцију и корелацију различитих извора безбедносних података, чиме се унапређује рано откривање потенцијалних инцидената и повећава ситуациона свест. Њена посебна вредност огледа се у могућности неинтрузивне претраге *deep web* и *dark web* окружења, са циљем идентификације компромитованих корисничких налога, цурења података и релевантних индикатора компромитовања (IoC), као и рањивости ИКТ система од посебног значаја у Републици Србији. У оквиру платформе имплементиран је нови модул који проширује постојеће функционалности и обезбеђује унапређене механизме заштите од *phishing* напада, укључујући побољшану детекцију злонамерних домена, анализу сумњивих порука и аутоматизовано препознавање образаца социјалног инжењеринга.

Повећање отпорности ИКТ система од посебног значаја захтева проактивно деловање, које подразумева спречавање напада у најранијој фази или ублажавање њихових последица. На тај начин се уз смањење ризика од инцидената, информациона безбедност на националном нивоу подиже на виши ниво.