ИЗВЕШТАЈ О СТАТИСТИЧКИМ ПОДАЦИМА О СВИМ ИНЦИДЕНТИМА У ИКТ СИСТЕМИМА ОД ПОСЕБНОГ ЗНАЧАЈА У 2021. ГОДИНИ

Јун, 2022. година

СРБ-ЦЕРТ

РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНА АГЕНЦИЈА ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

Национални ЦЕРТ Републике Србије www.cert.rs

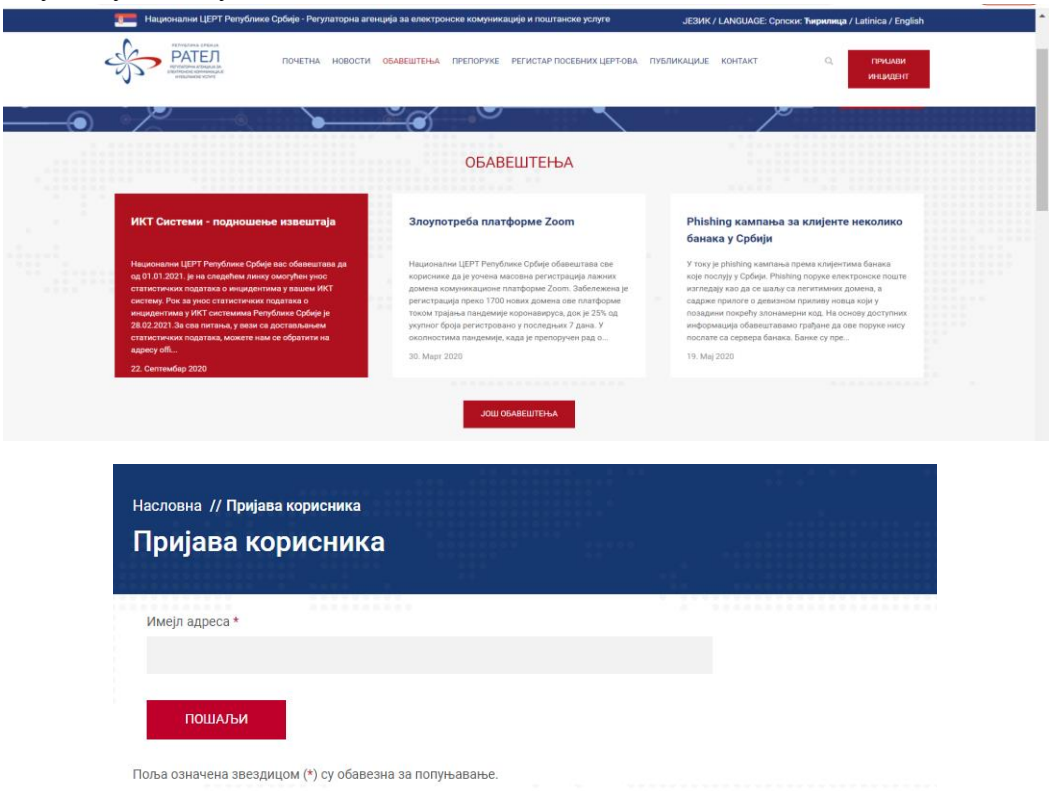
Садржај

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 2022. године, прикупљао статистичке податке о свим инцидентима у ИКТ системима од посебног значаја за 2021. годину. Овим одредбама Закона оператори ИКТ система од посебног значаја обавезани су да Националном ЦЕРТ-у доставе тачне статистичке податке о свим инцидентима у ИКТ систему за претходну годину најкасније до 28. фебруара текуће године.

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

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



Слика 1 - Веб апликација за достављање статистичких података

1. Оператори ИКТ система од посебног значаја

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

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

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

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

Слика 1.1 - ИКТ системи од посебног значаја

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

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

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

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

Табела 1 – Листа делатности

2. Преглед према групи инцидената

Оператори ИКТ система од посебног значаја су своје тачне и ажурне статистичке податке о свим инцидентима у ИКТ системима доставили у периоду од 01.01. до 28.02.2022. године, у складу са Законом о информационој безбедности и Правилником о врсти, форми и начину достављања статистичких података.

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

	Група инцидената	Број инцидената
1.	Неовлашћено прикупљање података	7.925.493
2.	Покушај упада у ИКТ систем	5.273.078
3.	Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. *malware*)	27.319
4.	Остали инциденти	17.813
5.	Превара	17.555
6.	Оперативни инциденти	9.679
7.	Недоступност или ограничена доступност ИКТ система	6.459
8.	Упад у ИКТ систем	1.487
9.	Инциденти физичко-техничке безбедности	112
10.	Угрожавање безбедности података	12
	УКУПНО	**13.279.007**

Табела 2.1 – Број инцидената према групама инцидената

Најзаступљенија група инцидената је неовлашћено прикупљање података (7.925.493), у оквиру које је најдоминантнија врста инцидента скенирање портова. На другом месту је покушај упада у ИКТ систем (5.273.078) у оквиру које је најзаступљенији инцидент покушај откривања креденцијала. На трећем месту се налази инсталирање злонамерног софтвера у оквиру ИКТ система (27.319). Четврто место заузимају остали инциденти (17.813) које чине сви они инциденти који не спадају у дефинисане категорије. Пето место заузима превара (17.555) и то у највећем броју фишинг (Графикон 2.1).

Графикон 2.1 – Пет најбројнијих група инцидената

3. Преглед према врсти инцидената

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

Група инцидената	Врста инцидента	Број инцидената
Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл.malware)	Тројанац	16.052
	Вирус	9.346
	Шпијунски софтвер (енгл. *spyware*)	1.252
	Црв (енгл. *worm*)	419
	Рансомвер (енгл. *ransomware*)	173
	Руткит (енгл. *rootkit*)	77
Неовлашћено прикупљање података	Скенирање портова	7.924.368
	Социјални инжењеринг (лажно представљање и други облици)	1.057
	Компромитовање или цурење података (енгл. *data breaches*)	67
	Пресретање података између рачунара и сервера (енгл. *sniffing*)	1
Превара	Фишинг (енгл *phishing*)	16.836
	Неовлашћено коришћење ресурса (енгл. *cryptojacking*) и други облици	719
Покушај упада у ИКТ систем	Покушај откривања креденцијала (енгл. *brute force attack, dictionary attack* и сл.)	4.984.475
	Покушај искоришћавања рањивости система	288.603
Упад у ИКТ систем	Неовлашћени приступ апликацији	744
	Откривање или неовлашћено коришћење непривилегованих налога (енгл. *unprivileged account compromise*)	723
	Мрежа заражених уређаја (енгл. *botnet*)	14
	Откривање или неовлашћено коришћење привилегованих налога (енгл. *privileged account compromise*)	6
Недоступност или ограничена доступност ИКТ система	Дистрибуирани напад са циљем онемогућавања или ометања функционисања ИКТ система (енгл. *distributed denial-of-service attack – DDoS*)	3.036

Група инцидената	Врста инцидента	Број инцидената
	Напад са циљем онемогућавања или ометања функционисања ИКТ система (енгл. *denial-of-service attack – DoS*)	2.563
	Прекид у функционисању система или дела система (енгл. *outage*)	860
	Саботажа	0
Угрожавање безбедности података	Криптографски напад	6
	Неовлашћена измена или брисање података	4
	Неовлашћен приступ подацима	2
Оперативни инциденти	Проблеми у раду са софтверским компонентама	6.274
	Отказивање хардверских компоненти	3.405
Инциденти физичко-техничке безбедности	Крађа хардверских компоненти	85
	Пожар	16
	Поплава	11
Остали инциденти	Инциденти који не спадају у горе наведене категорије	17.813
	УКУПНО	**13.279.007**

Табела 3.1 - Број инцидената по врстама

Графикон 3.1 – Пет најбројнијих врста инцидената

3.1. Инсталирање злонамерног софтвера у оквиру ИКТ система

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

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

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

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

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

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

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

У оквиру ове групе инцидената пријављено је 27.319 инсталирања злонамерног софтвера, од чега је тројанац у ИКТ системима од посебног значаја пријављен 16.052 пута (Графикон 3.1.1).

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 приказано је чак 7.924.368 пријава скенирања портова што се може објаснити великим бројем аутоматизованих процеса за испитивање доступних сервиса на удаљеним рачунарима, 1,057 пријава социјалног инжењеринга, 67 компромитовања или цурења података и 1 пријава пресретања података између рачунара и сервера, односно укупно 7.925.488 (Графикон 3.2.1)..

Графикон 3.2.1 – Неовлашћено прикупљање података

3.3. Превара

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

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

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

Број пријава који се односи на 2021. годину износи 16,836 за фишинг нападе, док неовлашћено коришћење ресурса износи 719 пријава (Графикон 3.3.1).

Графикон 3.3.1 – Превара систем

3.4. Покушај упада у ИКТ систем

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

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

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

У 2021. години нападачи су у највећој мери за упад у систем користили технике откривања креденцијала (4.984.475 покушаја) док су у мањој мери за упад у ИКТ систем од посебног значаја покушавали да искористе рањивости система (288.603 покушаја, Графикон 3.4.1).

Графикон 3.4.1 – Покушај упада у ИКТ

3.5. Упад у ИКТ систем

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

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

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

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

Мрежа заражених уређаја је аутоматизовани напад код ког нападач скенира мрежне адресе, користи рањивост на уређајима и преузима контролу над њима. На тај начин се ствара мрежа заражених уређаја која се може користи за нападе који ометају функционисање ИКТ система (*DDoS*).

У 2021. години је најчешће забележен неовлашћен приступ апликацији (744 пријава), затим откривање или неовлашћено коришћење непривилегованих налога (723 пријава),

мрежа заражених уређаја је омогућила упад 14 пута, док су се упади путем откривања или неовлашћеног коришћења привилегованих налога догодили 6 пута (Графикон 3.5.1).

Графикон 3.5.1 – Упад у ИКТ систем

3.6. Недоступност или ограничена доступност ИКТ система

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

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

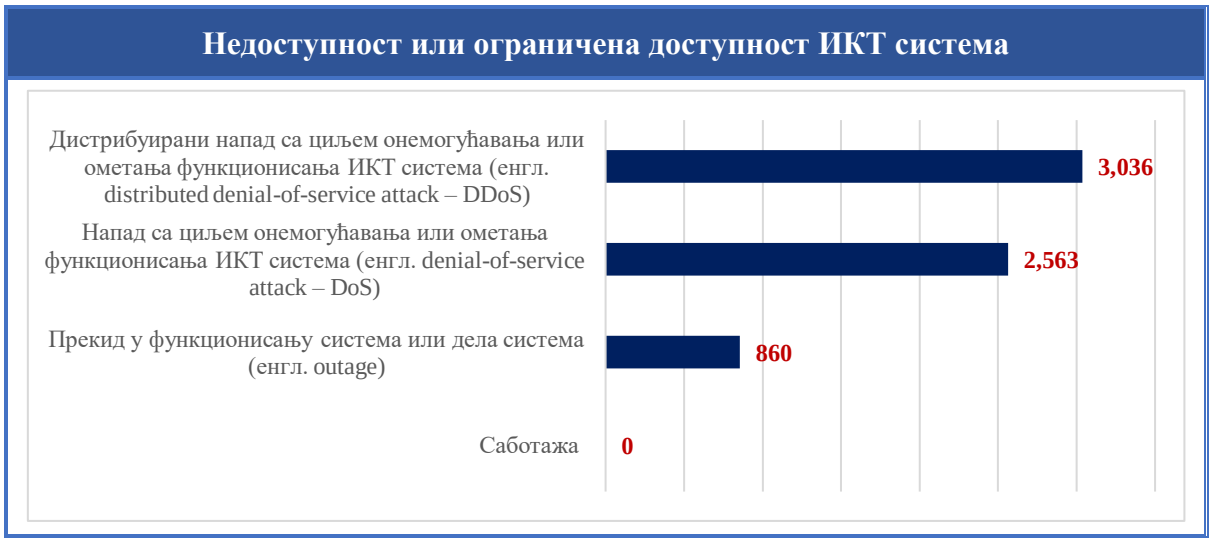
Напад са циљем онемогућавања или ометања функционисања ИКТ система (енгл. *denial-of-service attack – DoS*) је покушај нападача да онемогући приступ серверу или сервисима који су намењени крајњим корисницима.

Дистрибуирани напад са циљем онемогућавања или ометања функционисања ИКТ система (енгл. *distributed denial-of-service attack – DDoS*) има исти циљ као и DoS напад. DDoS напади постижу већу ефикасност користећи истовремено више компромитованих рачунарских система као изворе напада.

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

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

ИКТ системи од посебног значаја су детектовали 3.036 *DDoS* напада, 2.563 *DoS* напада, 860 прекида функционисања система или дела због техничких проблема, односно лоших временских услова, док саботажа ИКТ система у 2021. години није забележена (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 2021. години је забележено 6 криптографских напада, 4 неовлашћене измене или брисање података и 2 неовлашћена приступа подацима и (Графикон 3.7.1).

Графикон 3.7.1 – Угрожавање безбедности података

3.8. Оперативни инциденти

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

Број проблема у раду са софтверским компонентама које су довеле до застоја у пружању услуга, односно прекида који је на било који начин угрозио пословни процес (на пример краћи прекиди у раду) је износио 6.274, а број отказивања хардверских компоненти у 2021. години је износио 3.405 (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 2021. години забележено је 85 крађа хардверских компоненти, 16 пожара и 11 поплава (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 2021. години је било 17.813 (Графикон 3.10.1). Ове инциденте чине сви они инциденти који не спадају у наведене категорије.

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 неки ИКТ системи од посебног значаја, због врсте делатности коју обављају сврстани у више категорија.

	Врста ИКТ система од посебног значаја	Број инцидената
1.	ИКТ системи од посебног значаја који се користе у обављању послова у органима власти	21.384
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	164.169
	саобраћај	5.537
	здравство	125.938
	банкарство и финансијска тржишта	314.915
	дигитална инфраструктура	6.921.644
	добра од општег интереса који се односе на коришћење, управљање, заштиту и унапређење добара од општег интереса	2.002.296
	услуге информационог друштва	6.921.676
	остале области:	
	- Електронске комуникације	6.921.843
	- Издавање службеног гласила Републике Србије	/
	- Управљање нуклеарним објектима	83
	- Производња, промет и превоз наоружања и војне опреме	2.144.283
	- Управљање отпадом	511
	- Комуналне делатности	25.849
	- Производња и снабдевање хемикалијама	1.699.541
4.	ИКТ системи од посебног значаја који се користе у правним лицима и установама које оснива Република Србија, аутономна покрајина или јединица локалне самоуправе за обављање делатности од општег интереса	2.168.187

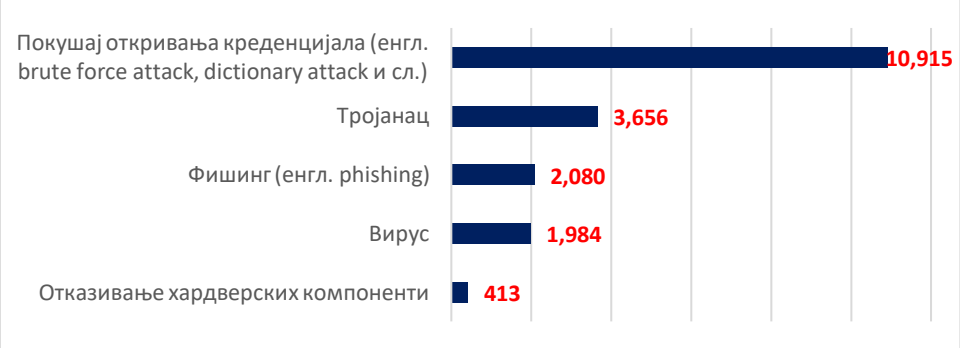
Табела 4.1 – Број пријављених инцидената према врсти ИКТ система

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	11.291
2.	Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. *malware*)	5.822
3.	Превара	2.083
4.	Оперативни инциденти	816
5.	Неовлашћено прикупљање података	562
6.	Остали инциденти	293
7.	Недоступност или ограничена доступност ИКТ система	262
8.	Угрожавање безбедности података	220
9.	Упад у ИКТ систем	26
10.	Инциденти физичко-техничке безбедности	9
	УКУПНО	**21.384**

Табела 4.1.1 – Број инцидената према групама инцидената у органима власти

Током 2021.године у ИКТ системима који се користе у органима власти забележено је највише покушаја откривања креденцијала (10.915), на другом месту је тројанац (3.656), на трећем и четвртом месту налазе се фишинг (2.080) и вирус (1.984), док је отказивање хардверских компоненти (4113) на петом месту (Графикон 4.1.1).



Графикон 4.1.1 – Број инцидената према групама 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 пријављени су недоступност или ограничена доступност ИКТ система и остали инциденти.

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

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

4.3.1. Енергетика

	Група инцидената	Број инцидената
1.	Покушај упада у ИКТ систем	2.134.108
2.	Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. *malware*)	14.700
3.	Неовлашћено прикупљање података	9.005
4.	Оперативни инциденти	3.776

5.	Превара	2.463
6.	Недоступност или ограничена доступност ИКТ система	87
7.	Упад у ИКТ систем	12
8.	Остали инциденти	10
9.	Угрожавање безбедности података	7
10.	Инциденти физичко-техничке безбедности	1
	УКУПНО	**2.164.169**

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

Најзаступљенији напад у области енергетике у 2021. години је био покушај откривања креденцијала (2.128.445), на другом месту је тројанац (10.045), треће место заузима скенирање портова (8.935), док су на четвртом и петом месту покушај искоришћавања рањивости система (5.663) и вирус (4.373) (Графикон 4.3.1.1).

Графикон 4.3.1.1 – Пет најчешћих врста инцидената у области енергетике

4.3.2. Саобраћај

	Група инцидената	Број инцидената
1.	Неовлашћено прикупљање података	3.516
2.	Покушај упада у ИКТ систем	1.643
3.	Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. *malware*)	310
4.	Превара	46
5.	Оперативни инциденти	11
6.	Недоступност или ограничена доступност ИКТ система	10
7.	Инциденти физичко-техничке безбедности	1

8.	Упад у ИКТ систем	0
9.	Угрожавање безбедности података	0
10.	Остали инциденти	0
	УКУПНО	**5.537**

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

У области саобраћаја је током 2021.године забележен је највећи број скенирања портова (3.515), други по заступљености је покушај откривања креденцијала (1.643), треће место заузима тројанац (164), четврто вирус (130), док је на петом месту фишинг (46) (Графикон 4.3.2.1).

Графикон 4.3.2.1 – Пет најчешћих врста инцидената у области саобраћаја

4.3.3. Здравство

	Група инцидената	Број инцидената
1.	Неовлашћено прикупљање података	66.971
2.	Покушај упада у ИКТ систем	52.644
3.	Превара	4.291
4.	Оперативни инциденти	1.047
5.	Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. *malware*)	533
6.	Остали инциденти	290
7.	Недоступност или ограничена доступност ИКТ система	154
8.	Инциденти физичко-техничке безбедности	5
9.	Упад у ИКТ систем	3
10.	Угрожавање безбедности података	0
	УКУПНО	**125.938**

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

Током 2021.године здравствени сектор је био најизложенији нападима скенирања портова (66.874), на другом месту је покушај откривања креденцијала (51.644), на трећем фишинг (4.290), четвртом (1.000) и петом месту је отказивање хардверских компоненти (628) (Графикон 4.3.3.1).

Графикон 4.3.3.1 – Пет најчешћих врста инцидената у области здравства

4.3.4. Банкарство и финансијска тржишта

	Група инцидената	Број инцидената
1.	Покушај упада у ИКТ систем	280.013
2.	Остали инциденти	16.978
3.	Неовлашћено прикупљање података	8.533
4.	Превара	5.865
5.	Оперативни инциденти	1.656
6.	Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. *malware*)	1.173
7.	Недоступност или ограничена доступност ИКТ система	682
8.	Упад у ИКТ систем	9
9.	Инциденти физичко-техничке безбедности	4
10.	Угрожавање безбедности података	2
	УКУПНО	**314.915**

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

ИКТ системи од посебног значаја из области банкарства и финансијских тржишта пријављују највећи број покушаја искоришћавања рањивости система (222.586), други је покушај откривања креденцијала (57.427), трећи инциденти који не спадају у горе наведене категорије (16.978), четврти скенирање портова (8.500) и пети фишинг (5.865) (Графикон 4.3.4.1).

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

4.3.5. Дигитална инфраструктура

	Група инцидената	Број инцидената
1.	Неовлашћено прикупљање података	6.814.720
2.	Покушај упада у ИКТ систем	101.945
3.	Оперативни инциденти	1.547
4.	Упад у ИКТ систем	1.422
5.	Превара	756
6.	Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. *malware*)	671
7.	Недоступност или ограничена доступност ИКТ система	530
8.	Остали инциденти	39
9.	Инциденти физичко-техничке безбедности	14
10.	Угрожавање безбедности података	0
	УКУПНО	**6.921.644**

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

Дигитална инфраструктура је током 2021.године била најизложенија скенирању портова (6.814.720), на другом месту је покушај искоришћавања рањивости система (52.809), трећем покушај откривања креденцијала (49.136), док су на четвртом и петом месту отказивање хардверских компоненти (1.516) и неовлашћени приступ апликацији (716) (Графикон 4.3.5.1).

Графикон 4.3.5.1 – Пет најчешћих врста инцидената у области дигиталне инфраструктуре

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

	Група инцидената	Број инцидената
1.	Покушај упада у ИКТ систем	1.000.070
2.	Неовлашћено прикупљање података	1.000.029
3.	Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. *malware*)	1.657
4.	Превара	346
5.	Оперативни инциденти	160
6.	Недоступност или ограничена доступност ИКТ система	20
7.	Остали инциденти	12
8.	Упад у ИКТ систем	2
9.	Угрожавање безбедности података	0
10.	Инциденти физичко-техничке безбедности	0
	УКУПНО	**2.002.296**

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

ИКТ системи који се користе у области добра од општег интереса који се односе на коришћење, управљање, заштиту и унапређење добара су током 2021. године забележили једнак број покушаја откривања креденцијала (1.000.000) и скенирања портова (1.000.000), док су на трећем, четвртом и петом месту тројанац (1.192), фишинг (346) и шпијунски софтвер (334) (Графикон 4.3.6.1).

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

4.3.7. Услуге информационог друштва

	Група инцидената	Број инцидената
1.	Неовлашћено прикупљање података	6.814.720
2.	Покушај упада у ИКТ систем	101.945
3.	Оперативни инциденти	1.549
4.	Упад у ИКТ систем	1.422
5.	Превара	756
6.	Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. *malware*)	671
7.	Недоступност или ограничена доступност ИКТ система	560
8.	Остали инциденти	39
9.	Инциденти физичко-техничке безбедности	14
10.	Угрожавање безбедности података	0
	УКУПНО	**6.924.676**

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

Област информационог друштва бележи највише скенирања портова (6.814.720), на другом месту је покушај искоришћавања рањивости система (52.809), трећем (49.136), четвртом отказивање хардверских компоненти (1.517) и петом месту неовлашћени приступ апликацији (716) (Графикон 4.3.7.1).

Графикон 4.3.7.1 – Пет најчешћих врста инцидената у области информационог друштва

4.3.8. Остале области

	Група инцидената	Број инцидената
1.	Неовлашћено прикупљање података	7.925.488
2.	Покушај упада у ИКТ систем	5.273.078
3.	Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. *malware*)	27.318
4.	Остали инциденти	17.811
5.	Превара	17.554
6.	Оперативни инциденти	9.677
7.	Недоступност или ограничена доступност ИКТ система	6.456
8.	Упад у ИКТ систем	1.487
9.	Инциденти физичко-техничке безбедности	112
10.	Угрожавање безбедности података	12
	УКУПНО	**6.924.676**

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

И остале области у којима се обављају делатности од општег интереса и друге делатности су током 2021. године забележиле највише скенирања портова (7.924.368), на другом месту је покушај откривања креденцијала (4.984.475), трећем покушај искоришћавања рањивости (288.603), четвртом инциденти који не спадају у наведене категорије (17.811) и петом фишинг (16.835) (Графикон 4.3.8.1).

Графикон 4.3.8.1 – Пет најчешћих врста инцидената у осталим областима

4.3.8.1. Електронске комуникације

	Група инцидената	Број инцидената
1.	Неовлашћено прикупљање података	6.814.720
2.	Покушај упада у ИКТ систем	101.985
3.	Оперативни инциденти	1.551
4.	Упад у ИКТ систем	1.422
5.	Превара	757
6.	Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. *malware*)	675
7.	Недоступност или ограничена доступност ИКТ система	569
8.	Инциденти физичко-техничке безбедности	86
9.	Остали инциденти	78
10.	Угрожавање безбедности података	0
	УКУПНО	**6.921.843**

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

ИКТ системи које користе оператори из области електронских комуникација су током 2021. године детектовали највећи број скенирања портова, друго место заузима покушај искоришћавања рањивости система (52.846), треће покушај откривања креденцијала (49.139), четврто и пето место заузима отказивање хардверских компоненти (1.517) и неовлашћени приступ апликацији (716) (Графикон 4.3.8.1.1).

Графикон 4.3.8.1.1 – Пет најчешћих врста инцидената у области електронских комуникација

4.3.8.2. Издавање службеног гласила

ИКТ системи од посебног значаја који се користе у области издавања службеног гласила нису претрпели сајбер инциденте у 2021. години.

4.3.8.3. Управљање нуклеарним објектима

	Група инцидената	Број инцидената
1.	Превара	50
2.	Остали инциденти	10
3.	Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. *malware*)	8
4.	Оперативни инциденти	6
5.	Покушај упада у ИКТ систем	5
6.	Недоступност или ограничена доступност ИКТ система	4
7.	Неовлашћено прикупљање података	0
8.	Упад у ИКТ систем	0
9.	Угрожавање безбедности података	0
10.	Инциденти физичко-техничке безбедности	0
	УКУПНО	**83**

Табела 4.3.8.3.1 – 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 (50), на другом месту су инциденти који не спадају у горе наведене категорије (10), трећем

отказивање хардверских компоненти (6), док тројанац (5) и покушај откривања креденцијала (5) имају једнак број (Графикон 4.3.8.3.1).

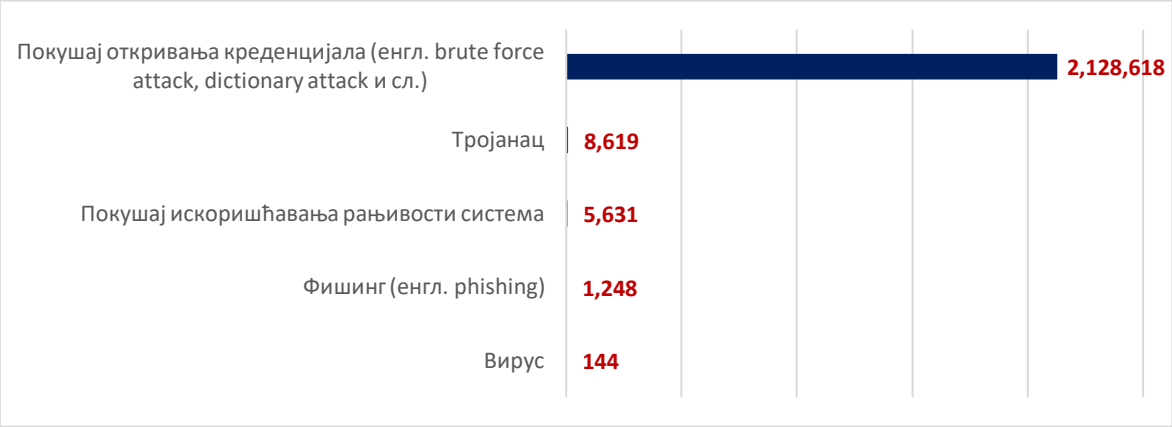
Графикон 4.3.8.3.1 – Пет најчешћих врста инцидената у области управљања нуклеарним објектима

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

	Група инцидената	Број инцидената
1.	Покушај упада у ИКТ систем	2.134.249
2.	Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. *malware*)	8.763
3.	Превара	1.248
4.	Недоступност или ограничена доступност ИКТ система	14
5.	Оперативни инциденти	8
6.	Остали инциденти	1
7.	Упад у ИКТ систем	0
8.	Угрожавање безбедности података	0
9.	Неовлашћено прикупљање података	0
10.	Инциденти физичко-техничке безбедности	0
	УКУПНО	**2.144.283**

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

У области производње, промета и превоза нуклеарног наоружања и војне опреме најзаступљенији напад је покушај откривања креденцијала (2.128.618), други је тројанац (8.619), трећи покушај искоришћавања рањивости система (5.631). четврти фишинг (1.248) и пети вирус (144) (Графикон 4.3.8.4.1).



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

4.3.8.5. Управљање отпадом

	Група инцидената	Број инцидената
1.	Остали инциденти	278
2.	Неовлашћено прикупљање података	104
3.	Оперативни инциденти	65
4.	Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. *malware*)	27
5.	Превара	18
6.	Покушај упада у ИКТ систем	13
7.	Упад у ИКТ систем	5
8.	Недоступност или ограничена доступност ИКТ система	1
9.	Угрожавање безбедности података	0
10.	Инциденти физичко-техничке безбедности	0
	УКУПНО	**511**

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

У области управљања отпадом најзаступљенији су инциденти који не спадају у горе наведене категорије (278), другом скенирање портова (83), трећем отказивање хардверских компоненти (33), четврти проблеми у раду са софтверским компонентама (32) и пети социјални инжењеринг (21) (Графикон 4.3.8.5.1).

Графикон 4.3.8.5.1 – Пет најчешћих врста инцидената у области управљања отпадом

4.3.8.6. Комуналне делатности

	Група инцидената	Број инцидената
1.	Покушај упада у ИКТ систем	8.551
2.	Неовлашћено прикупљање података	5.621
3.	Недоступност или ограничена доступност ИКТ система	5.154
4.	Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. *malware*)	3.358
5.	Оперативни инциденти	2.209
6.	Превара	803
7.	Остали инциденти	139
8.	Упад у ИКТ систем	8
9.	Инциденти физичко-техничке безбедности	6
10.	Угрожавање безбедности података	0
	УКУПНО	**25.849**

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

Током 2021. године су оператори ИКТ система од посебног значаја који обављају комуналне делатности забележили највећи број покушаја искоришћавања рањивости система (6.050), на другом месту је скенирање портова (5.500), трећем покушај откривања креденцијала (2.501), док су *DoS* и *DDoS* напади изједначени (2.500) (Графикон 4.3.8.6.1).

Графикон 4.3.8.6.1 – Пет најчешћих врста инцидената у области управљања отпадом

4.3.8.7. Производња и снабдевање хемикалијама

	Група инцидената	Број инцидената
1.	Покушај упада у ИКТ систем	1.682.133
2.	Неовлашћено прикупљање података	16.452
3.	Превара	929
4.	Недоступност или ограничена доступност ИКТ система	14
5.	Оперативни инциденти	12
6.	Остали инциденти	1
7.	Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. *malware*)	0
8.	Упад у ИКТ систем	0
9.	Угрожавање безбедности података	0
10.	Инциденти физичко-техничке безбедности	0
	УКУПНО	**1.699.541**

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

Област производње и снабдевања хемикалијама је током 2021. године била најизложенија нападима покушаја откривања креденцијала (1.682.133), скенирања портова (15.982), фишинг (929), социјални инжењеринг (470) и прекид у функционисању система или дела система (14) (Графикон 4.3.8.7.1).

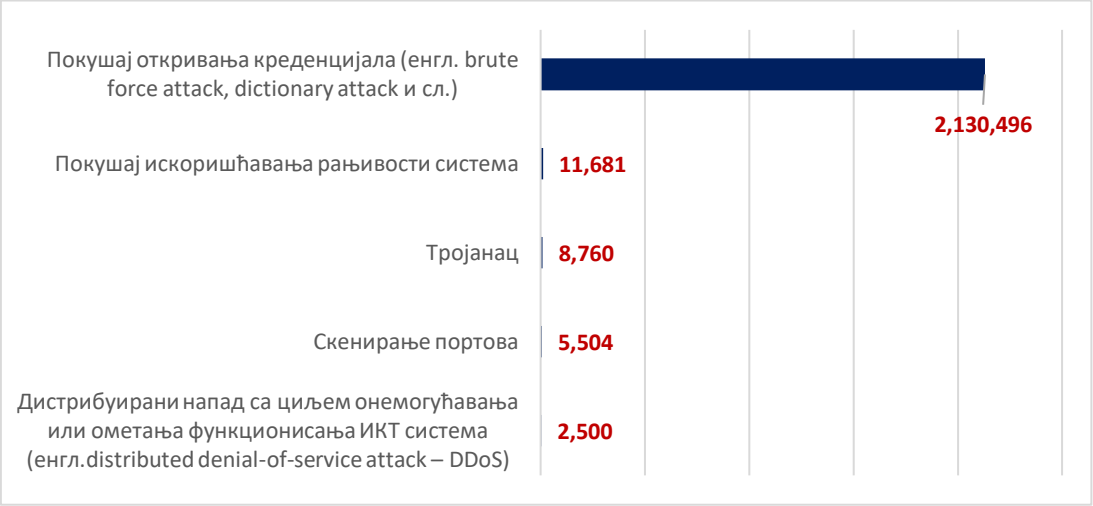
Графикон 4.3.8.7.1 – Пет најчешћих врста инцидената у области производње и снабдевања хемикалијама

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

	Група инцидената	Број инцидената
1.	Покушај упада у ИКТ систем	2.142.177
2.	Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. *malware*)	10.736
3.	Неовлашћено прикупљање података	6.613
4.	Недоступност или ограничена доступност ИКТ система	5.147
5.	Оперативни инциденти	2.051
6.	Превара	1.325
7.	Остали инциденти	131
8.	Инциденти физичко-техничке безбедности	5
9.	Упад у ИКТ систем	2
10.	Угрожавање безбедности података	0
	УКУПНО	**2.168.187**

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

Ова врста ИКТ система је током 2021. године била најизложенија нападима покушаја откривања креденцијала (2.130.496), на другом месту је покушај искоришћавања рањивости система (11.681), трећем тројанац (8.760), четвртом скенирање портова (5.504) и петом месту *DDoS* (2.500) (Графикон 4.4.1).



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

5. Закључак

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

Током 2021.године настављен је тренд напада из 2020.године. Период пандемије вирусом COVID-19 обележио је рад од куће који подразумева приступ ИКТ систему послодавца из окружења које није једнако безбедно као окружење послодавца. Мера заштите постизања безбедности рада на даљину и употребе мобилних уређаја је и током 2021.године била у фокусу. Неопходност рада на даљину и обављање послова на мрежи послодавца, када су се запослени налазили ван просторија послодавца било је изузетно важно јер се на тај начин обезбеђивао континуитет пословања. Овакав рад најчешће је остварен VPN приступом информационом систему, који подразумева и дефинисање правила и услова за повезивање на мрежу са удаљене локације. Сајбер нападачи су нападе усмеравали управо користећи ово сазнање, околности у којима се рад обављао од куће, те стога не изненађује континуитет заступљености покушаја откривања креденцијала.

Најзаступљенија врста инцидената је скенирање портова која припада групи напада неовлашћено прикупљање података. Ова група и врста напада су биле веома заступљене и у 2020.години и заузимале су друго место. 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 обављању делатности у области саобраћаја, здравства, дигиталне инфраструктуре, услуга информационог друштва, као и области електронских комуникација и осталим областима у којима се обављају делатности од општег интереса.

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 комбинацијама 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 који се користе у обављању делатности у области енергетике и добара од општег интереса. Такође, овом нападу су најизложенији били и ИКТ системи који се користе у обављању послова у органима власти.

Покушај искоришћавања рањивости система је на трећем месту и представља слабост чијом злоупотребом нападачи могу угрозити интегритет, расположивост, аутентичност и непорецивост података којима се рукује помоћу ИКТ система. Покушај искоришћавања рањивости система је напад којим нападач покушава да приступи систему за који нема одобрење, искоришћавањем познатих или нових рањивости. Постоји неколико јавно доступних евиденција познатих рањивости као што су *CVE, NVD* и *OVAL*. *CVE* идентификатор обично укључује кратак опис, а понекад и савете, упутства и извештаје. Доминација овог напада указује да ИКТ системи од посебног значаја недовољно пажње посвећују ефикасним управљањем закрпама, односно редовном ажурирању.

Ова врста напада је најзаступљенија у ИКТ системима који се користе у обављању послова у области комуналних делатности и банкарства и финансијских тржишта, док је покушај откривања креденцијала на другом месту по заступљености у области банкарства и финансијских тржишта. Такође, покушај откривања креденцијала је најдоминантнији и у ИКТ системима који се користе у правним лицима које оснива Република Србија, аутономна покрајина или јединица локалне самоуправе за обављање делатности од општег интереса, у ИКТ системима у области производње, промета и превоза наоружања и војне опреме, као и у области производње и снабдевања хемикалијама.

Инциденти који не спадају у наведене категорије налазе се на четвртом месту. Ово је најзаступљенија врста напада у ИКТ системима који се користе за обављање послова у области управљања отпадом и на трећем месту у области банкарства и финансијских тржишта. Имајући у виду динамичан развој метода напада и самих врста сајбер напада, ради идентификције нових група и врста напада, у следећем периоду извештавања о

статистичким подацима о инцидентима, ИКТ системи од посебног значаја ће имати могућност да унесу опис детектованог инцидента. На тај начин ће се утврдити нови трендови и претње које су заступљене у Републици Србији.

На петом месту се налази фишинг. Током 2021.године спроведено је неколико великих фишинг кампања чија су мета били корисници интернета у Србији. Највеће по обиму, интензитету, али и учесталости су кампање намењене клијентима банака. Фишинг поруке су изгледале као да се шаљу са легитимних домена и садржале су прилоге о девизном приливу новца. Ове фишинг кампање су најчешће дистрибуирале Lokibot тројанца, који краде информације као што су корисничка имена, лозинке, банковни детаљи или садржај новчаника крипто валута. Овај тројанац поред праћења активности корисника, а може да креира и *backdoor* и тако омогући спровођење следећих фаза напада или поновно заражавање система. Треба споменути и фишинг кампању која је злоупотребила тему COVID-19 и издавање дигиталних зелених сертификата. Фишинг порука садржала је линк за преузимање електронског документа о вакцинацији, и од корисника се тражило да кликом на линк преузме наводни дигитални зелени сертификат.

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

Фишинг кампања усмерена на кориснике платформи за е-трговину има исту методологију. Наводни купац комуникацију почиње питањем оглашивачу да ли је производ и даље доступан и да ли купопродају могу да обаве електронским путем. Тада им у своје име или у име „администратора платформе за е-трговину“ доставља линк са објашњењем да је наводни купац већ уплатио средства преко апликације и од оглашивача тражи кликне на линк који води на страницу на којој се захтева да унесе у одређена поља податке са банковне картице (број картице и CVV број) како би му се наводно извршила уплата. Национални ЦЕРТ је поводом ових фишинг напада објавио неколико обавештења, саопштења за јавност и имао неколико гостовања у медијима 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 управљања нуклеарним објектима, на трећем месту у органима власти и области здравства, добара од општег интереса и производње и снабдевања хемикалијама, док је на четвртом месту у области производње, промета и превоза наоружања и војне опреме. У ИКТ системима који се користе за обављање

делатности у области саобраћаја, банкарства и финансијских тржишта заузима пето место.

Имајући у виду значај групе напада инсталирање злонамерног софтвера и да као група напада заузима треће место по заступљености, треба напоменути да су током 2021. године најзаступљеније врсте малвера биле тројанац, вирус и шпијунски софтвер.

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

Ова врста малвера је најзаступљенија у ИКТ системима који се користе у обављању послова у органима власти, док се на другом месту налази вирус.

Иако је тројанац један од најстаријих облика злонамерног софтвера показао се као веома издржљив и прилагодљив. Успешно избегава откривање, уграђује се и преплиће у рутинске рачунарске операције и генерално је еволуирао тако да избегава детектовање, а опстанак и напредак обезбеђује тако што постаје део комплекснијих сајбер напада[1].

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

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

Статистички подаци указују да су аутоматизовани напади доминантни у ИКТ системима од посебног значаја, што представља и глобални тренд да су савремени сајбер напади постали јако аутоматизовани.

С друге стране, многи произвођачи софтвера за сајбер безбедност аутоматизацију виде као начин да постану ефикаснији и као средство за уштеду радне снаге или броја запослених. Поред тога, аутоматизацију такође треба посматрати као алат који може и треба да се користи за боље предвиђање понашања и брже извршавање заштите. Ако се

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

примени на одговарајући начин и са правим алатима, аутоматизација може значајно помоћи у спречавању сајбер напада.[2]

Криминална активност у сајбер простору је након изузетног пораста у другој половини 2020. године, током 2021.године постепено јењавала, у смислу да није било глобалних вести или великих кампања, док је тема COVID-19 након масовне злоупотребе почела да бледи. У исто време, нови напади настављају да се појављују на тржишту сајбер претњи, а како малвер постаје софистицираније, тиме је пад укупног броја напада компензован већим последицама успешног напада. Најопаснији од свих у овом смислу су банкарски малвер и шпијунски софтвер.[3]

На глобалном нивоу, посебно је запажен пораст мобилних банкарских тројанаца у односу на 2020.годину. У истраживању које је спровела компанија Kaspersky број ових тројанаца у 2021.години је удвостручен у односу на 2020.годину[4].

Имајући у виду заступљеност ове врсте малвера на националном нивоу, Национални ЦЕРТ је током марта и априла 2022.године спровео техничку обуку на Cyberbit платформи запосленима у локалним самоуправама, која за циљ има увежбавање одбране од тројанаца. Ова јединствена обука подразумева рад у хипер-реалистичној симулацији сајбер напада и омогућава учесницима вежбе ефикасно унапређење вештина и способности одбране од сајбер напада који су све софистицираније и тежи за детектовање. На овај начин је достављање статистичких података о свим инцидентима у ИКТ системима, поред јединственог и свеобухватног сагледавања стања сајбер претњи, допринело и планирању адекватног одговора на исте кроз унапређење знања ИТ стручњака ИКТ система од посебног значаја. Дакле, ова законска обавеза оператора ИКТ система од посебног значаја има важан, посредан и непосредан, утицај на безбедност сајбер простора Републике Србије.

[2] https://www.paloaltonetworks.com/cyberpedia/4-ways-cybersecurity-automation-should-be-used
[3] https://securelist.com/mobile-malware-evolution-2021/105876/
[4] https://securelist.com/mobile-malware-evolution-2021/105876/