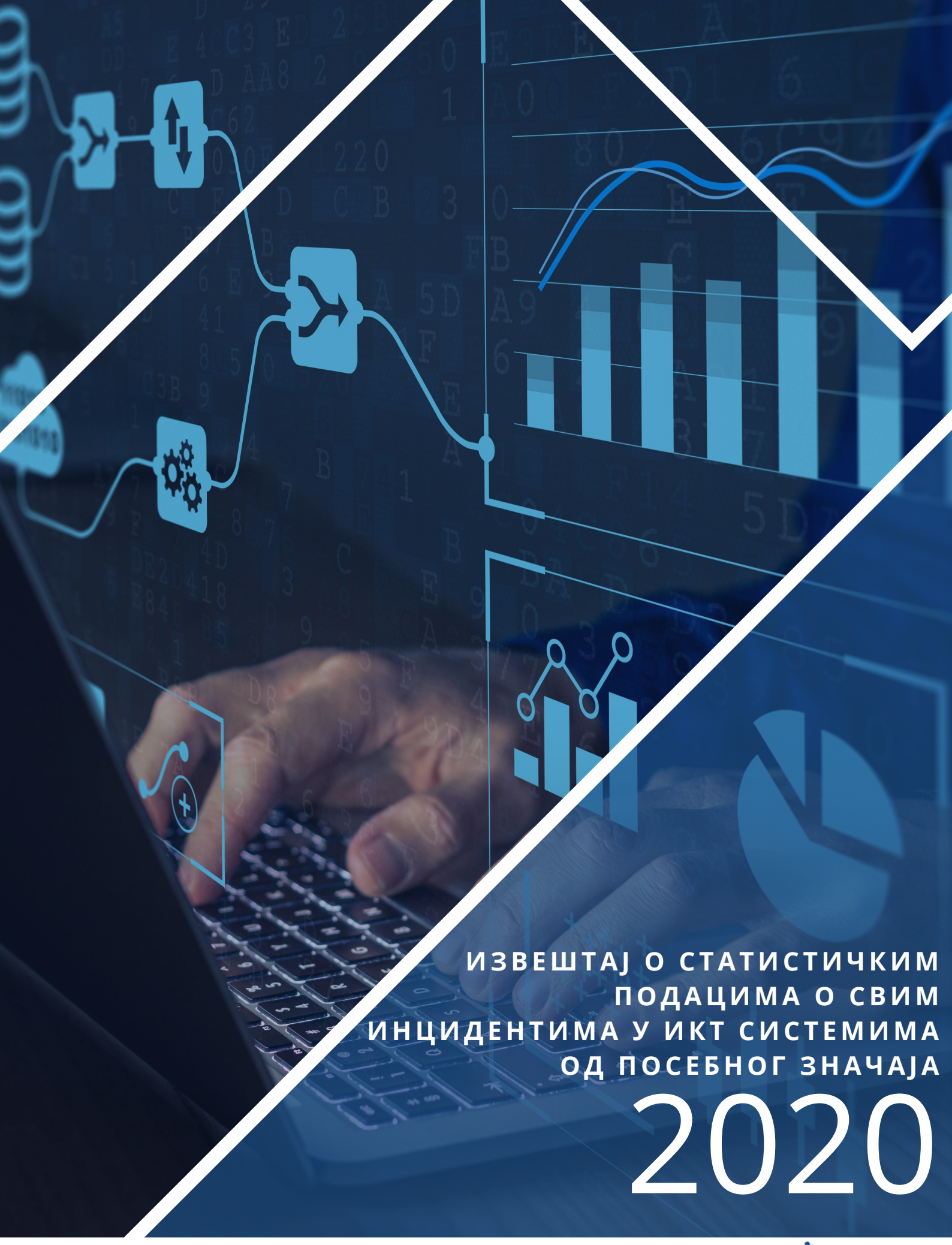


ИЗВЕШТАЈ О СТАТИСТИЧКИМ ПОДАЦИМА О СВИМ ИНЦИДЕНТИМА У ИКТ СИСТЕМИМА ОД ПОСЕБНОГ ЗНАЧАЈА

2020

РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНА АГЕНЦИЈА ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

Национални ЦЕРТ Републике Србије
www.cert.rs

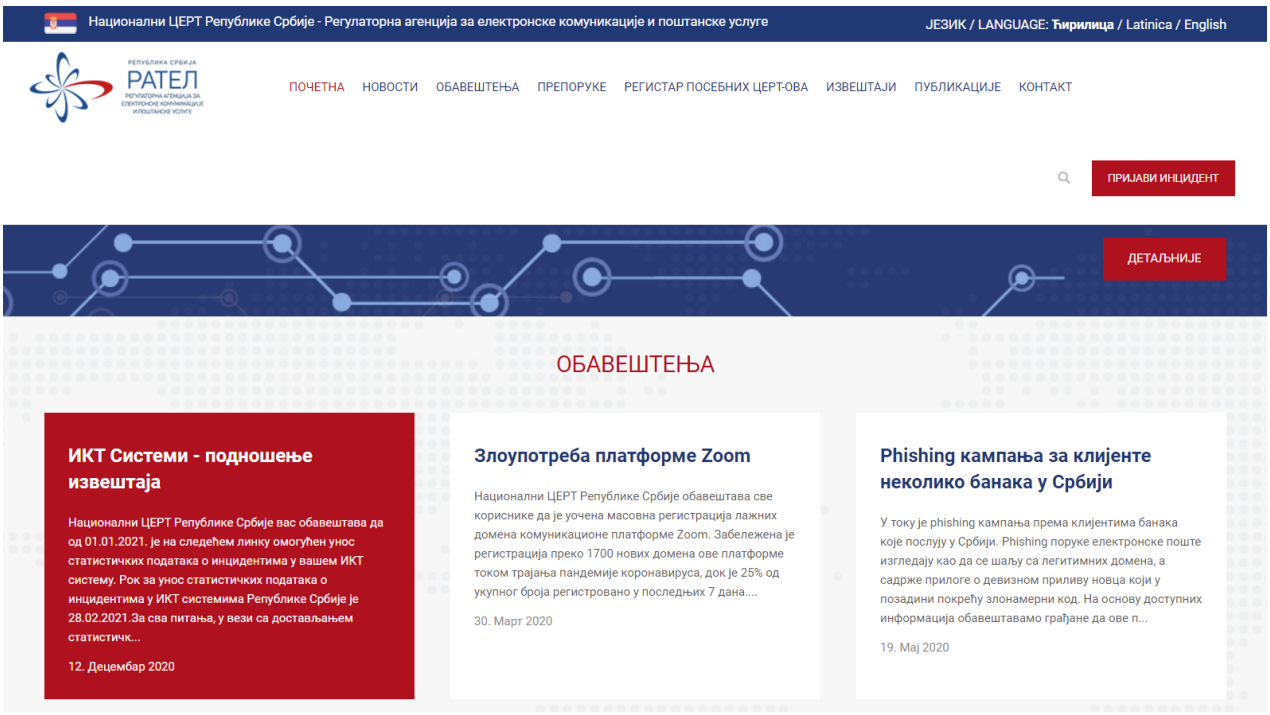
СРБ-ЦЕРТ

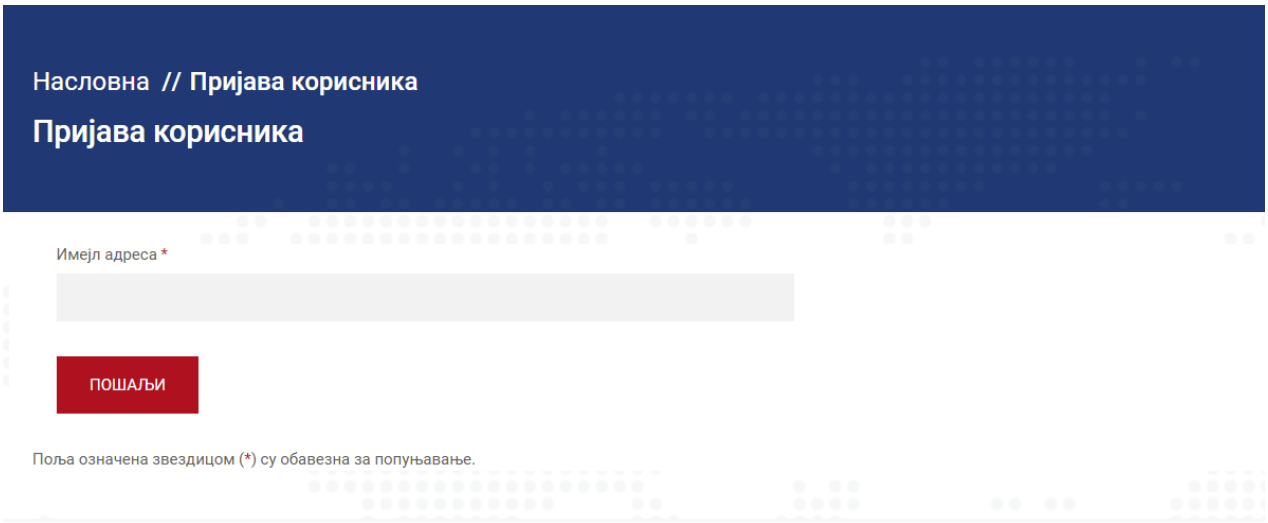
САДРЖАЈ

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 2021. године, прикупљао статистичке податке о свим инцидентима у ИКТ системима од посебног значаја за 2020. 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.

Имајући у виду циљ и сврху прикупљања статистичких података о свим инцидентима Национални ЦЕРТ је креирао веб апликацију (Слика 1), као 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 који се односи на коришћење, управљање, заштиту 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 и другим делатностима.

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 2 - 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 деривата 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 ИНФОРМАЦИО-НОГ 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

У Табели 2 дат је приказ броја инцидената према групама инцидената, док је у Графикону 1 приказано првих пет најбројнијих група инцидената.

	ГРУПА ИНЦИДЕНАТА	БРОЈ ИНЦИДЕНАТА
1	Покушај упада у ИКТ систем	**17.332.830**
2	Неовлашћено прикупљање података	**8.470.838**
3	Превара	**76.190**
4	Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. *malware*)	**61.159**
5	Оперативни инциденти	**13.277**
6	Упад у ИКТ систем	**2.237**
7	Недоступност или ограничена доступност ИКТ система	**1.914**
8	Остали инциденти	**341**
9	Инциденти физичко-техничке безбедности	**45**
10	Угрожавање безбедности података	**19**
	УКУПНО	**25.958.850**

Табела 2 – Број инцидената према групама инцидената

Најзаступљенија група инцидената је покушај упада у ИКТ систем (17.332.830), у оквиру које је покушај откривања креденцијала доминантнији у односу на покушај искоришћавања рањивости система. На другом месту је неовлашћено прикупљање података (8.470.838) у оквиру које су најзаступљенији скенирање портова и социјални инжењеринг (Графикон 1).

Графикон 1 – Пет најбројнијих група инцидената

3. ПРЕГЛЕД ПРЕМА ВРСТИ ИНЦИДЕНАТА

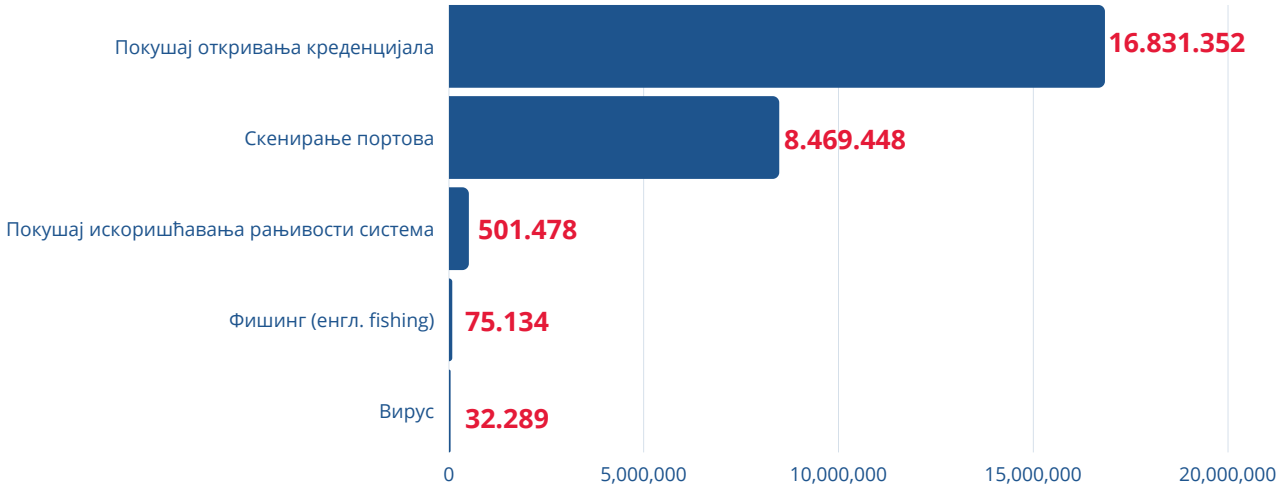
У складу са Уредбом о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја и Правилником о врсти, форми и начину достављања статистичких података о инцидентима у информационо-комуникационим системима од посебног значаја, групе инцидената су подељене на врсте инцидената и подаци о броју инцидената приказани су у Табели бр. 3 и у Графиконима од бр. 2 до бр. 12.

ГРУПА ИНЦИДЕНАТА	ВРСТА ИНЦИДЕНАТА	БРОЈ ИНЦИДЕНАТА
Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. *malware*)	Вирус	**32.289**
	Тројанац	**21.816**
	Шпијунски софтвер (енгл. *spyware*)	**5.591**
	Црв (енгл. *worm*)	**1.284**
	Руткит (енгл. *rootkit*)	**91**
	Рансомвер (енгл. *ransomware*)	**88**
Неовлашћено прикупљање података	Скенирање портова	**8.469.448**
	Социјални инжењеринг (лажно представљање и други облици)	**1.369**
	Компромитовање или цурење података (енгл. *data breaches*)	**12**
	Пресретање података између рачунара и сервера (енгл. *sniffing*)	**9**

ГРУПА ИНЦИДЕНАТА	ВРСТА ИНЦИДЕНАТА	БРОЈ ИНЦИДЕНАТА
Превара	Фишинг (енгл. *phishing*)	**75.134**
	Неовлашћено коришћење ресурса (енгл. *cryptojacking*) и други облици	**1.056**
Покушај упада у ИКТ систем	Покушај откривања креденцијала (енгл. *brute force attack*, *dictionary attack* и сл.)	**16.831.352**
	Покушај искоришћавања рањивости система	**501.478**
Упад у ИКТ систем	Неовлашћени приступ апликацији	**1.030**
	Откривање или неовлашћено коришћење непривилегованих налога (енгл. *unprivileged account compromise*)	**971**
	Мрежа заражених уређаја (енгл. *botnet*)	**228**
	Откривање или неовлашћено коришћење привилегованих налога (енгл. *privileged account compromise*)	**8**
Недоступност или ограничена доступност ИКТ система	Прекид у функционисању система или дела система (енгл. *outage*)	**919**
	Дистрибуирани напад са циљем онемогућавања или ометања функционисања ИКТ система (енгл. *distributed denial-of-service attack – DDoS*)	**10**
	Напад са циљем онемогућавања или ометања функционисања ИКТ система (енгл. *denial-of-service attack – DoS*)	**37**

ГРУПА ИНЦИДЕНАТА	ВРСТА ИНЦИДЕНАТА	БРОЈ ИНЦИДЕНАТА
	Саботажа	**0**
Угрожавање безбедности података	Криптографски напад	**14**
	Неовлашћен приступ подацима	**3**
	Неовлашћена измена или брисање података	**2**
Оперативни инциденти	Отказивање хардверских компоненти	**6.719**
	Проблеми у раду са софтверским компонентама	**6.558**
Инциденти физичко-техничке безбедности	Поплава	**27**
	Крађа хардверских компоненти	**16**
	Пожар	**2**
Остали инциденти	Инциденти који не спадају у горе наведене категорије	**341**
	УКУПНО	**25.958.850**

Табела 3 - Број инцидената по врстама



Графикон 2 – 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 хоста. 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.

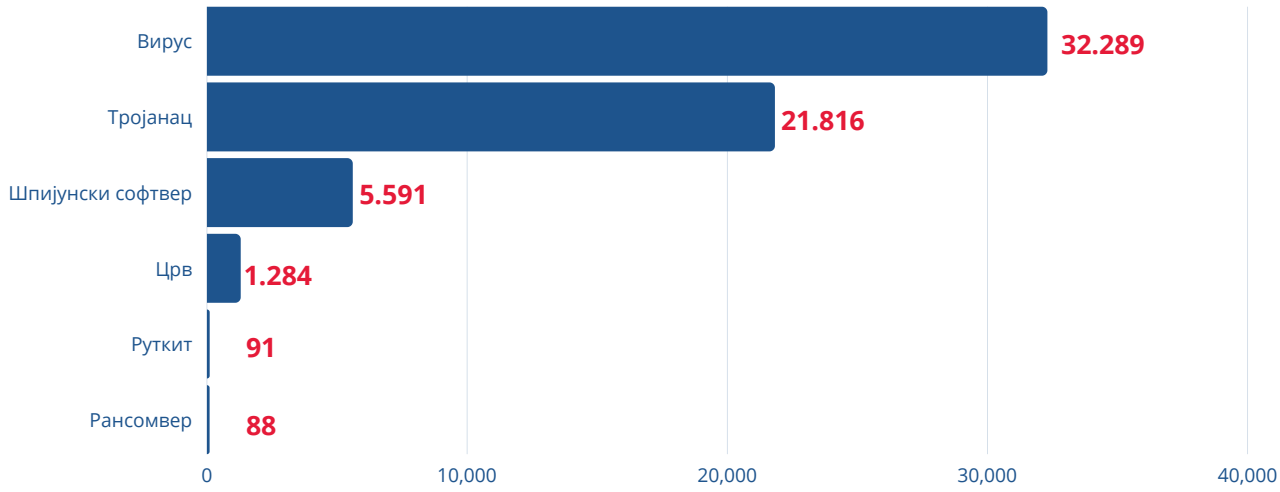
Рансомвер је злонамерни софтвер који шифрира податке на уређајима или мрежама, а за приступ и откључавање датотека захтева плаћање откупа. Чест је случај да датотеке чак и након плаћања откупа остају закључане.

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 веба, 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 се сакрије у току неовлашћеног приступа и одржава привилегован приступ рачунару заобилажењем уобичајеног начина аутентификације и механизама ауторизације.

У оквиру ове групе инцидената пријављено је 32.289 инсталација вируса, док је рансомвер у ИКТ системима од посебног значаја пријављен 88 пута (Графикон 3).



Графикон 3 – Инсталирање злонамерног софтвера у оквиру ИКТ система

3.2. НЕОВЛАШЋЕНО ПРИКУПЉАЊЕ ПОДАТАКА

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

Скенирање портова је напад који шаље захтеве клијената на низ адреса портова сервера хоста, са циљем откривања комуникационих канала који се могу искористити, односно проналаска отвореног порта и искоришћавања његове рањивости.

Снифинг напад, односно пресретање података подразумева коришћење апликација за надгледање, анализу и снимање мрежног саобраћаја у циљу преузимања 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 безбедносних мера које ће омогућити нападачу приступ мрежи.

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

На графикону 4 приказано је чак 8.469.448 пријава скенирања портова што се може објаснити великим бројем аутоматизованих процеса за испитивање доступних сервиса на удаљеним рачунарима, 1.369 пријава социјалног инжењеринга, 12 компромитовања или цурења података и 9 пријава пресретања података између рачунара и сервера.

Графикон 4 – Неовлашћено прикупљање података

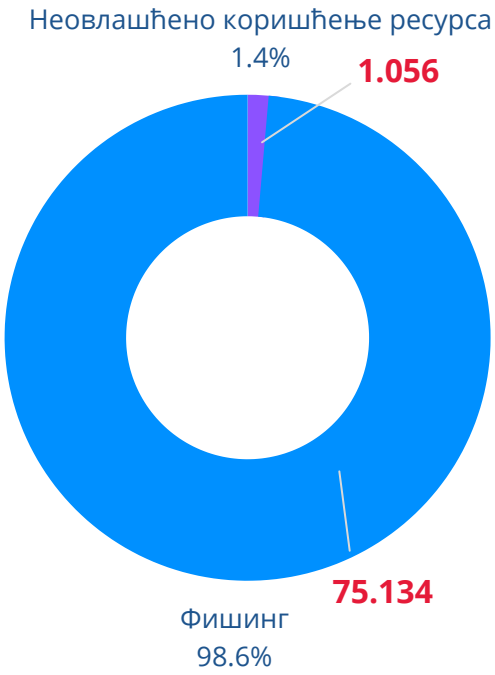
3.3. ПРЕВАРА

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

Фишинг је сајбер напад који се врши уз помоћ електронске поште, која садржи злонамерни прилог или линк који води ка зараженом сајту или документу. Нападач користи социјални инжењеринг да би се представио као неко познат и тако навео жртву да отвори електронску пошту. Овај напад је често повезан и са нападима попут малвера, мреже ботова и сајбер шпијунаже.

Неовлашћено коришћење ресурса - Криптоџекинг (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 2020. годину износи 75.134 за фишинг нападе, док неовлашћено коришћење ресурса износи 1.056 пријава (Графикон 5).



Графикон 5 – Превара

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 логовањем различитим комбинацијама слова, бројева и симбола са циљем идентификације корисничког имена и лозинке.

У 2020. години нападачи су у највећој мери за упад у систем користили технике откривања креденцијала (16.831.352 покушаја) док су у мањој мери за упад у ИКТ систем од посебног значаја покушавали да искористе рањивости система (501.478 покушаја, Графикон 6).

Графикон 6 – Покушај упада у ИКТ систем

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 непримећено крећу кроз ИКТ систем и приступе осетљивим подацима

Откривање или неовлашћено коришћење непривилегованих налога (енгл. *Unprivileged Account Compromise*) омогућава нападачима да се непримећено 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 помоћу туђег налога или других метода.

Мрежа заражених уређаја је аутоматизовани напад који скенира мрежне адресе и шири заразе на рањивим рачунарима, што омогућава хакерима да преузму контролу над зараженим рачунарима и претворе их у ботове. На тај начин се ствара мрежа ботова која се користи за нападе онемогућавања услуга (*DDoS*), као и за извршавање задатака без знања жртве (слање електронске поште, вируса или крађе личних података).

У 2020. години је најчешће забележен неовлашћен приступ апликацији (1.030 пријава), затим откривање или неовлашћено коришћење непривилегованих налога (971 пријава), мрежа заражених уређаја је омогућила упад 228 пута, док су се упади путем откривања или неовлашћеног коришћења привилегованих налога догодили 8 пута (Графикон 7).

Графикон 7 – 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, спонтаних грешака или људске грешке без намере или грубог занемаривања.

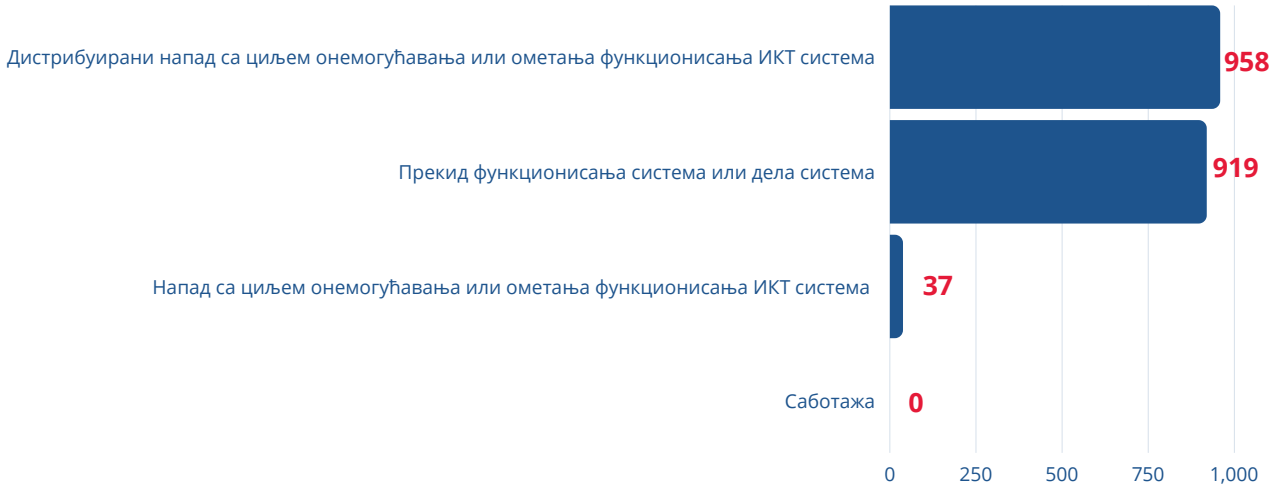
Напад са циљем онемогућавања или ометања функционисања ИКТ система (енгл. *denial-of-service attack – DoS*) је покушај нападача да онемогући приступ серверу или сервисима који су намењени крајњим корисницима.

Дистрибуирани напад са циљем онемогућавања или ометања функционисања ИКТ система (енгл. *distributed denial-of-service attack – DDoS*) је вишеструки напад који има за циљ да се поремети нормалан саобраћај сервера, услуге или мреже преплављујући инфраструктуру већом количином интернет саобраћаја. *DDoS* напади постижу ефикасност користећи више компромитованих рачунарских система као извора саобраћаја.

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 и 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 958 *DDoS* напада, 919 прекида функционисања система или дела због техничких проблема, односно лоших временских услова, 37 *DoS* напада, док се саботажа ИКТ система у 2020. години није догодила (Графикон 8).



Графикон 8 – Недоступност или ограничена доступност ИКТ система

3.7. УГРОЖАВАЊЕ БЕЗБЕДНОСТИ ПОДАТАКА

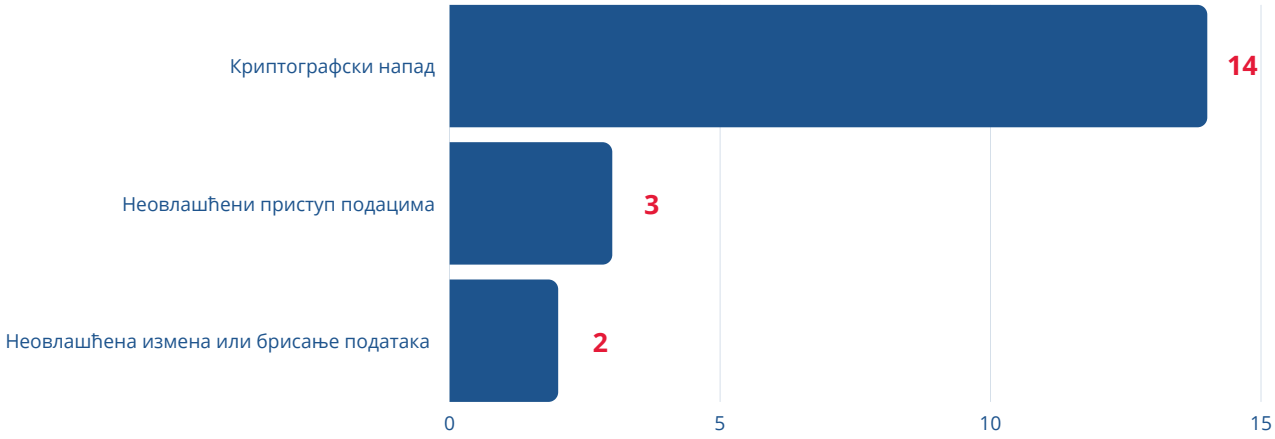
Поред злоупотребе података и система неовлашћеним приступом, односно неовлашћеном изменом или брисањем података, нарушавање безбедности података може бити и последица криптографског напада.

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 2020. години је забележено 14 криптографских напада, три неовлашћена приступа подацима и две неовлашћене измене или брисање података (Графикон 9).

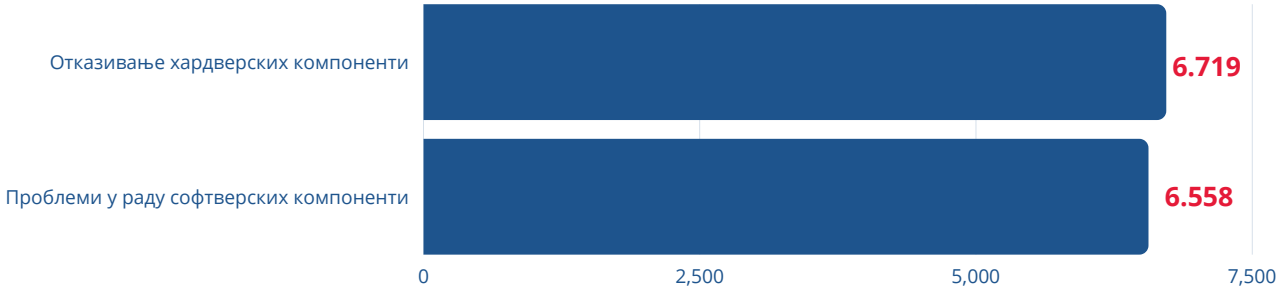


Графикон 9 – Угрожавање безбедности података

3.8. ОПЕРАТИВНИ ИНЦИДЕНТИ

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

Број отказивања хардверских компоненти у 2020. години је износио 6.719, а 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 6.558 (Графикон 10).

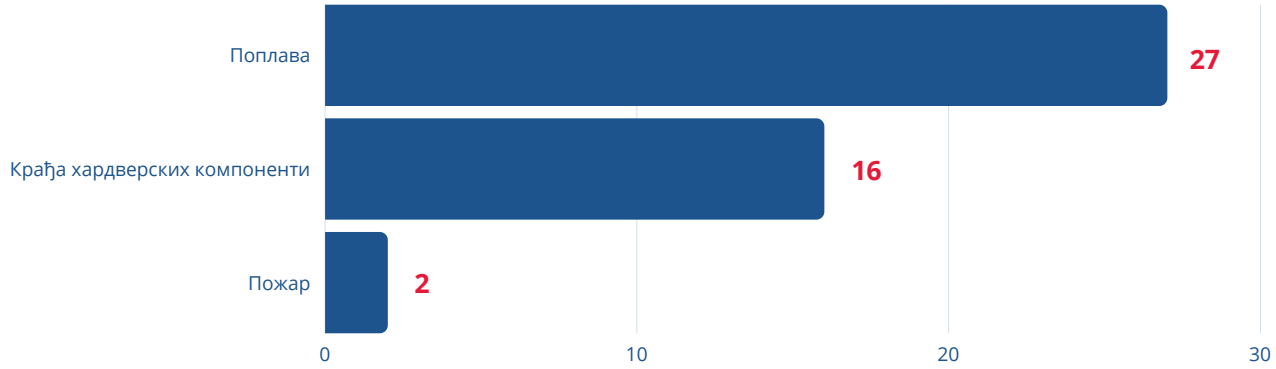


Графикон 10 – Оперативни инциденти

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 2020. години забележено је 27 поплава, 16 крађа хардверских компоненти и 2 пожара (Графикон 11).



Графикон 11 – Инциденти физичко-техничке безбедности

3.10. ОСТАЛИ ИНЦИДЕНТИ

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

Осталих инцидената у 2020. години је било 341 (Графикон 12)

Графикон 12 – Остали инциденти

4. ЗАКЉУЧАК

Најчешћа врста сајбер напада је покушај откривања креденцијала, који подразумева покушај приступа систему жртве непрекидним логовањем различитим комбинацијама слова, бројева и симбола са циљем идентификације корисничког имена и лозинке или коришћењем речника. Ово је стара врста напада, али још увек веома ефикасна и популарна међу нападачима. Приступ легитимном налогу може омогућити приступ читавом ИКТ систему. Ова врста напада се не ослања на рањивости ИКТ система већ на слабе лозинке корисника.

Преласком на режим рада од куће повећан је број ових напада који су покушавали да искористе *Windows Remote Desktop Protocol (RDP)* који администратори система користе за приступ Windows системима са удаљене локације. Касније су ови напади преусмерени и на појединце који раде од куће и немају одређене нивое заштите као у канцеларијама, односно ИКТ системима што их чини лаком метом, нарочито уколико користе и слабе лозинке. Одбрана од овог напада је захтевна и поред едукације запослених о важности употребе комплексних лозинки, подразумева и коришћење дво-факторске и мулти-факторске аутентификације, *VPN*-а, као и енкрипцију података на уређајима који се користе у пословне сврхе.

На другом месту налази се скенирање портова, којим се заправо прикупљају информације и не наноси штета самој мети, али се такви напади користе за прибављање корисних информација за даљи упад. Главни циљ овог напада је откривање који портови су отворени, који затворени, а који филтрирани, а могу се скенирати сви портови, којих има око 65.000 или само они који пружају сервисе који се могу злоупотребити коришћењем познате рањивости. Заступљеност је повећана и због аутоматизације ове врсте напада, а сами ИКТ системи од посебног значаја могу бити део скенираног опсега.

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, мере ублажавања и извештаје.

На четвртом месту се налази фишинг. Током 2020. 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. Фишинг кампања која је злоупотребила Институт за јавно здравље „Др Милан Јовановић Батут“ била је усмерена на јавне установе и привредне субјекте и садржала је лажно обавештење о бесплатној расподели заштитне опреме. Ове фишинг кампање су дистрибуирале *Lokibot* тројанца, који краде информације као што су корисничка имена, лозинке, банковни детаљи или садржај новчаника крипто валута. Информације краде коришћењем *keylogger*-а снима активности у претраживачу и десктопу, а може да креира и *backdoor* и тако омогући инсталирање додатних оптерећења за систем.

Остале кампање су наводиле кориснике да кликну на линк који води на лажну страницу, које је све теже препознати као небезбедне. Нападачи у све већој мери користе *HTTPS* иако су технологије као што су *HTTPS* и *SSL* креиране у циљу обезбеђивања комуникације између клијента и сервера. Катанац на адресној линији претраживача може навести корисника да помисли да је страница безбедна. Повећан је и број услуга бесплатних сертификата, а овоме доприноси и чињеница да претраживачи углавном *HTTPS* страницу обележавају као безбедну без додатне провере.[1] За време трајања пандемије, значајно је повећан број лажних интернет страница које користе тему вируса *COVID-19*, односно садрже неки од појмова пандемије у називу домена ("*Covid19/Coronavirus*“). Поред дистрибуције малвера, ове странице се користе за лажну продају медицинске опреме, суплемената, лекова, вакцина и преваром корисника, хакери долазе до противправно стечене имовинске користи.

Нападачи су користили и новије врсте фишинг напада од којих су најзаступљенији били компромитовање пословне е-поште, *vishing*, *smishing*. Фишинг напад, било да се користи за дистрибуцију зараженог прилога или линка, захтева реакцију потенцијалне жртве. Коришћењем различитих мамаца, нападачи су покушавали да дођу до жељене реакције корисника, од којих се на глобалном нивоу током прошле године издвојио „*COVID-19*“.

[1] https://www.enisa.europa.eu/publications/phishing

На петом месту је вирус. Вируси могу бити усмерени на масовно заражавање рачунарских мрежа или на мрежу компаније или организације која је мета. Ниво заштите детерминише ниво ангажовања нападача па се често дешава да су, с обзиром да већина организација користи *Firewall* и друге мере заштите од спољних напада, нападачи принуђени да затраже помоћ унутар организације. Методи социјалног инжењеринга омогућавају нападачима лакши приступ запосленима и ИКТ системима у којима раде, а прелазак на рад од куће и стање општег страха су допринели унапређењу ових метода.

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. Две основне карактеристике вируса су способност самосталног извршавања, тако што ће заменити покретање жељеног програма сопственим покретањем, и реплицирања, заменом извршних датотека копијом датотека заражених вирусом.

Вирус је најзаступљенија врста малвера, док је тројанац на другом месту по укупној заступљености. Овај злонамерни софтвер се корисницима представља као корисни програм и на тај начин превари кориснике да га покрену. Овај малвер може да преузме и друге претње са интернета, убацује друге типове малвера на угрожене рачунаре, комуницира са удаљеним нападачима, као и да бележи све што се куца на тастатури и шаље нападачима. Један од најпознатијих напада *Emotet* је почео као банкарски тројанац и еволуирао до мреже заражених уређаја.

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, бележењем 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, текста откуцаног на тастатури, навика у претраживању интернета, коришћене адресе е-поште.

Црв је на четвртом месту по заступљености, а ова врста малвера за инфилтрирање најчешће користи рањивости софтвера. Као и остале врсте малвера може се дистрибуирати и путем прилога е-поште. Црв може да измени или избрише податке, а може се користити и за убацивање додатног злонамерног софтвера на рачунар корисника.

Најзаступљенији малвер у свету је током 2020. године био рансомвер, а мете напада су биле чак и болнице и то у време ванредне и велике борбе са пандемијом вируса COVID-19. Забележено је и повећање износа откупнине и времена које је потребно за опоравак од напада.[2] Један од већих рансомвер напада догодио се и у нашој земљи, а мета напада било је јавно комунално предузеће Информатика из Новог Сада. Рансомвер *Pwndlocker* је на неколико дана онемогућио пружање услуга неколико градских институција које су у мрежи градске управе. Овај рансомвер је коришћен и за нападе на градске управе и велике компаније других земаља, нарочито у САД, а нападачи су одређивали износ откупнине у зависности од величине мреже, броја запослених и годишњих прихода. Рансомвер је врста малвера која је на шестом месту по заступљености у нашој земљи.

Разлика у броју различитих врста малвера у односу на фишинг нападе охрабрује, док број оперативних инцидената указује да су стална улагања у ИКТ неопходна, као и да ће континуирано улагање у кадровске капацитете и технологију значајно унапредити тренутно стање информационе безбедности у Републици Србији.

Имајући у виду да је 2020. година била година изазова у сваком смислу, може се закључити да су и оператори ИКТ система од посебног значаја успели да се изборе са безбедносним претњама и нападима у сајбер простору. Примена мера заштите и испуњавање обавезе достављања статистичких података о свим инцидентима у ИКТ системима свакако чине сајбер простор Републике Србије безбеднијим, а операторе ИКТ система стимулишу на утврђивање стања и континуирано унапређење информационо-комуникационих технологија и кадровских капацитета.

СРБ-ЦЕРТ

[2] https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf