IZVEŠTAJ O STATISTIČKIM PODACIMA O SVIM INCIDENTIMA U IKT SISTEMIMA OD POSEBNOG ZNAČAJA

2020

REPUBLIKA SRBIJA
RATEL
REGULATORNA AGENCIJA ZA ELEKTRONSKE KOMUNIKACIJE I POŠTANSKE USLUGE

Nacionalni CERT Republike Srbije
www.cert.rs

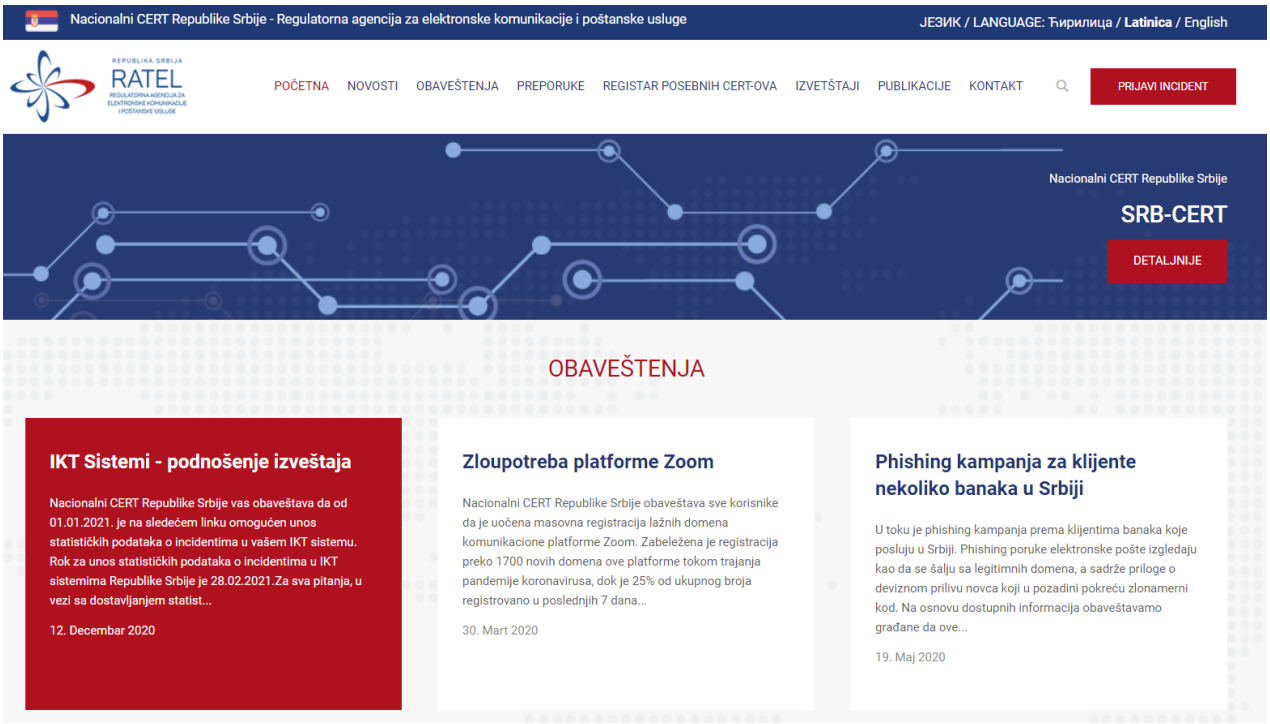
SRB-CERT

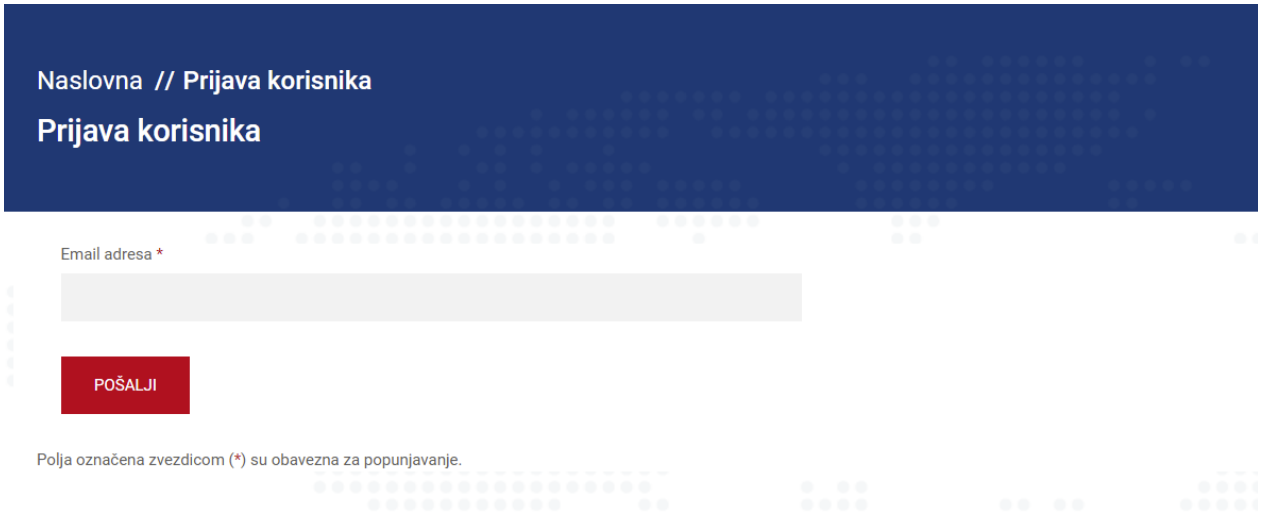
Sadržaj

UVOD

U skladu sa članom 11b. Zakona o informacionoj bezbednosti Nacionalni centar za prevenciju bezbednosnih rizika u IKT sistemima (u daljem tekstu: Nacionalni CERT) je, počev od januara 2021. godine, prikupljao statističke podatke o svim incidentima u IKT sistemima od posebnog značaja za 2020. godinu. Ovim odredbama Zakona operatori IKT sistema od posebnog značaja obavezani su da Nacionalnom CERT-u dostave tačne statističke podatke o svim incidentima u IKT sistemu za prethodnu godinu najkasnije do 28. februara tekuće godine.
Vrstu, formu i način dostavljanja ovih podataka Nacionalni CERT je utvrdio Pravilnikom o vrsti, formi i načinu dostavljanja statističkih podataka („Službeni glasnik RS“, broj 76/20) kojim je propisan i Obrazac ISP - Izveštaj o statističkim podacima o svim incidentima u IKT sistemima od posebnog značaja, a koji, pored podataka o operatoru IKT sistema od posebnog značaja, sadrži i listu incidenata prema vrstama.

Imajući u vidu cilj i svrhu prikupljanja statističkih podataka o svim incidentima Nacionalni CERT je kreirao veb aplikaciju (Slika 1), kao i uputstvo za kreiranje naloga i dostavljanje statističkih podataka koje sadrži preporuke i smernice kojim bi trebalo da se rukovode administratori sistema prilikom utvrđivanja karakteristika stvarnog negativnog uticaja svih vrsta napada na njihov IKT sistem. Na ovaj način je Nacionalni CERT pružio podršku operatorima IKT sistema u ispunjavanju ove zakonske obaveze.





Slika 1 - Veb aplikacija za dostavljanje statističkih podataka

1. OPERATORI IKT SISTEMA OD POSEBNOG ZNAČAJA

Operatori IKT sistema od posebnog značaja su pravna lica, organi vlasti ili organizacione jedinice organa vlasti koji koriste IKT sistem u okviru svoje delatnosti. Zakonom o informacionoj bezbednosti definisane su vrste IKT sistema od posebnog značaja:

1. IKT sistemi od posebnog značaja koji se koriste u obavljanju poslova u organima vlasti;
2. IKT sistemi od posebnog značaja koji se koriste za obradu posebnih vrsta podataka o ličnosti, u smislu zakona koji uređuje zaštitu podataka o ličnosti;
3. IKT sistemi koji se koriste u obavljanju delatnosti od opšteg interesa i drugim delatnostima i to u sledećim oblastima:
    1. Energetika,
    2. Saobraćaj,
    3. Zdravstvo,
    4. Bankarstvo i finansijska tržišta,
    5. Digitalna infrastruktura,
    6. Dobra od opšteg interesa koji se odnose na korišćenje, upravljanje, zaštitu i unapređenje dobara od opšteg interesa (vode, putevi, mineralne sirovine, šume, plovne reke, jezera, obale, banje, divljač, zaštićena područja),
    7. Usluge informacionog društva,
    8. Ostale oblasti;

4. IKT sistemi od posebnog značaja koji se koriste u pravnim licima i ustanovama koje osniva Republika Srbija, autonomna pokrajina ili jedinica lokalne samouprave za obavljanje delatnosti od opšteg interesa i drugim delatnostima.

Lista delatnosti u oblastima u kojima se obavljaju delatnosti od opšteg interesa definisana je Uredbom o utvrđivanju liste delatnosti od opšteg interesa i u kojima se koriste informaciono-komunikacioni sistemi od posebnog značaja (Tabela 1).

Evidenciju operatora IKT sistema od posebnog značaja vodi Ministarstvo trgovine, turizma i telekomunikacija, a Pravilnikom o podacima koje sadrži evidencija operatora informaciono-komunikacionih sistema od posebnog značaja utvrđeni su podaci koje ova Evidencija sadrži.

Slika 2 – IKT sistemi od posebnog značaja

LISTA DELATNOSTI		
Oblast	**Delatnost**	
1) ENERGETIKA	(1) proizvodnja, prenos i distribucija električne energije, u smislu zakona kojim se uređuje energetika:	- proizvodnja električne energije: - snabdevanje električnom energijom, uključujući snabdevanje na veliko; - prenos i upravljanje prenosnim sistemom električne energije;

		- distribucija električne energije i upravljanje distributivnim sistemom električne energije; - upravljanje organizovanim tržištem električne energije.
	(2) proizvodnja i prerada uglja, u smislu zakona kojim se uređuje rudarstvo:	- eksploatacija uglja.
	(3) istraživanje, proizvodnja, prerada, transport i distribucija nafte i promet nafte i naftnih derivata:	- energetske delatnosti: proizvodnja derivata nafte; transport nafte naftovodima; transport derivata nafte produktovodima; transport nafte i derivat nafte drugim oblicima transporta; trgovina naftom i derivatima nafte, u smislu zakona kojim se uređuje energetika; - eksploatacija nafte, u smislu zakona kojim se uređuje rudarstvo.
	(4) istraživanje, proizvodnja, prerada, transport i distribucija prirodnog i tečnog gasa:	- snabdevanje prirodnim gasom, u smislu zakona kojim se uređuje energetika;

		- javno snabdevanje prirodnim gasom, u smislu zakona kojim se uređuje energetika; - transport prirodnog gasa i upravljanje transportnim sistemom za prirodni gas, u smislu zakona kojim se uređuje energetika; - distribucija prirodnog gasa i upravljanje distributivnim sistemom prirodnog gasa, u smislu zakona kojim se uređuje energetika; - skladištenje i upravljanje skladištem prirodnog gasa, u smislu zakona kojim se uređuje energetika; - eksploatacija prirodnog gasa, u smislu zakona kojim se uređuje rudarstvo.
2) SAOBRAĆAJ	(1) železnički saobraćaj, u smislu zakona kojim se uređuje železnica:	- upravljanje javnom železničkom infrastrukturom; - javni prevoz u železničkom saobraćaju.
	(2) poštanski saobraćaj, u smislu zakona kojim se uređuje poštanski saobraćaj:	- poštanske usluge koje obavlja javni poštanski operator.

	(3) vodni saobraćaj, u smislu zakona kojim se uređuje plovidba i luke na unutrašnjim vodama:	- tehničko održavanje međunarodnih, međudržavnih i državnih vodnih puteva; - upravljanje lukama i pristaništima i lučka delatnost.
	(4) vazdušni saobraćaj, u smislu zakona o vazdušnom saobraćaju:	- aerodromske usluge; - kontrola letenja; - javni vazdušni prevoz.
3) ZDRAVSTVO	(1) zdravstvena zaštita, u smislu zakona kojim se uređuje zdravstvena zaštita:	- zdravstvena delatnost koju obavljaju zdravstvene ustanove i druga pravna lica koja obavljaju zdravstvenu delatnost.
4) BANKARSTVO I FINANSIJSKA TRŽIŠTA	(1) poslovi finansijskih institucija:	- poslovi finansijskih institucija, u smislu zakona kojim se uređuje Narodna banka, nad kojima nadzor, odnosno kontrolu, u skladu sa zakonom, vrši Narodna banka.
	(2) poslovi vođenja registra podataka o obavezama fizičkih i pravnih lica prema finansijskim institucijama;	
	(3) poslovi upravljanja, odnosno obavljanja delatnosti u vezi sa funkcionisanjem regulisanog tržišta, u smislu zakona kojim se uređuje tržište kapitala.	
5) DIGITALNA INFRASTRUKTURA	(1) usluge razmene internet saobraćaja (engl. „*internet exchange point*“);	
	(2) upravljanje registrom nacionalnog internet domena i sistemom za imenovanje na mreži (DNS sistemi).	

6) DOBRA OD OPŠTEG INTERESA KOJI SE ODNOSE NA KORIŠĆENJE, UPRAVLJANJE, ZAŠTITU I UNAPREŠENJE DOBARA OD OPŠTEG INTERESA	(1) vode, u smislu zakona kojim se uređuju vode:	- upravljanje vodama kao i vodnim objektima i vodnim zemljištem u javnoj svojini; - vodna delatnost.
	(2) putevi, u smislu zakona kojim se uređuju javni putevi:	- upravljanje javnim putem.
	(3) mineralne sirovine, u smislu zakona kojim se uređuje rudarstvo:	- eksploatacija mineralnih sirovina.
	(4) šume, u smislu zakona kojim se uređuju šume:	- gazdovanje šumama u državnoj svojini.
	(5) plovne reke, jezera i obale, u smislu zakona kojim se uređuje plovidba i luke na unutrašnjim vodama;	
	(6) banje, u smislu zakona kojim se uređuju banje:	- očuvanje, korišćenje, unapređenje i upravljanje banjama.
	(7) divljač, u smislu zakona kojim se uređuje divljač i lovstvo:	- delatnost korišćenja, upravljanja, zaštite i unapređivanja populacije divljači i njihovih staništa.
	(8) zaštićena područja, u smislu zakona kojim se uređuju nacionalni parkovi:	- upravljanje nacionalnim parkovima.

7) USLUGE INFORMACIONOG DRUŠTVA	(1) usluge platformi za trgovinu putem interneta, u smislu zakona kojim se uređuje elektronska trgovina;	
	(2) usluge pretraživanja interneta, u smislu zakona kojim se uređuje elektronska trgovina;	
	(3) usluge skladištenja podataka korisnika usluga (engl. „*cloud computing service*"), u smislu zakona kojim se uređuje elektronska trgovina.	
8) OSTALE OBLASTI	(1) elektronske komunikacije, u smislu zakona kojim se uređuju elektronske komunikacije:	- delatnost elektronskih komunikacija.
	(2) izdavanje službenog glasila Republike Srbije, u smislu zakona kojim se uređuje objavljivanje zakona i drugih propisa i akata:	- izdavanje službenog glasnika.
	(3) upravljanje nuklearnim objektima, u smislu sa zakona kojim se uređuje zaštita od jonizujućeg zračenja i nuklearna sigurnost:	- upravljanje nuklearnim objektima.
	(4) proizvodnja, promet i prevoz naoružanja i vojne opreme, u smislu zakona kojim se uređuje proizvodnja, promet i prevoz naoružanja i vojne opreme:	- proizvodnja naoružanja i vojne opreme; - promet naoružanja i vojne opreme; - prevoz naoružanja i vojne opreme.

Tabela 1 – Lista delatnosti

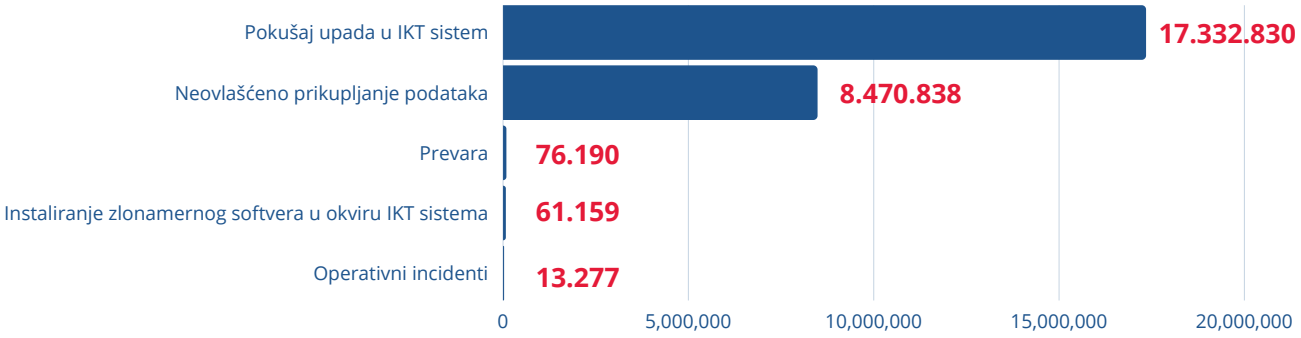
2. PREGLED PREMA GRUPI INCIDENATA

U Tabeli 2 dat je prikaz broja incidenata prema grupama incidenata, dok je u Grafikonu 1 prikazano prvih pet najbrojnijih grupa incidenata.

	GRUPA INCIDENATA	BROJ INCIDENATA
1	Pokušaj upada u IKT sistem	**17.332.830**
2	Neovlašćeno prikupljanje podataka	**8.470.838**
3	Prevara	**76.190**
4	Instaliranje zlonamernog softvera u okviru IKT sistema (malver, engl. *malware*)	**61.159**
5	Operativni incidenti	**13.277**
6	Upad u IKT sistem	**2.237**
7	Nedostupnost ili ograničena dostupnost IKT sistema	**1.914**
8	Ostali incidenti	**341**
9	Incidenti fizičko-tehničke bezbednosti	**45**
10	Ugrožavanje bezbednosti podataka	**19**
	UKUPNO	**25.958.850**

Tabela 2 – Broj incidenata prema grupama incidenata

Najzastupljenija grupa incidenata je pokušaj upada u IKT sistem (17.332.830), u okviru koje je pokušaj otkrivanja kredencijala dominantniji u odnosu na pokušaj iskorišćavanja ranjivosti sistema. Na drugom mestu je neovlašćeno prikupljanje podataka (8.470.838) u okviru koje su najzastupljeniji skeniranje portova i socijalni inženjering (Grafikon 1).



Grafikon 1 – Pet najbrojnijih grupa incidenata

3. PREGLED PREMA VRSTI INCIDENATA

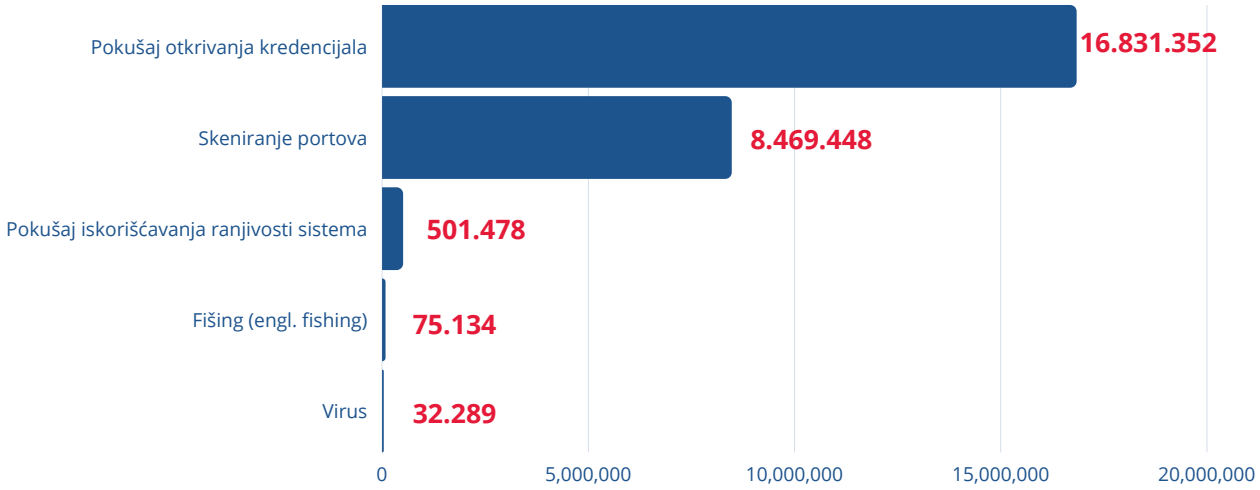
U skladu sa Uredbom o postupku obaveštavanja o incidentima u informaciono-komunikacionim sistemima od posebnog značaja i Pravilnikom o vrsti, formi i načinu dostavljanja statističkih podataka o incidentima u informaciono-komunikacionim sistemima od posebnog značaja, grupe incidenata su podeljene na vrste incidenata i podaci o broju incidenata prikazani su u Tabeli br. 3 i u Grafikonima od br. 2 do br. 12.

GRUPA INCIDENATA	VRSTA INCIDENTA	BROJ INCIDENATA
Instaliranje zlonamernog softvera u okviru IKT sistema (malver, engl. *malware*)	Virus	**32.289**
	Trojanac	**21.816**
	Špijunski softver (engl. *spyware*)	**5.591**
	Crv (engl. *worm*)	**1.284**
	Rutkit (engl. *rootkit*)	**91**
	Ransomver (engl. *ransomware*)	**88**
Neovlašćeno prikupljanje podataka	Skeniranje portova	**8.469.448**
	Socijalni inženjering (lažno predstavljanje i drugi oblici)	**1.369**
	Kompromitovanje ili curenje podataka (engl. *data breaches*)	**12**
	Presretanje podataka između računara i servera (engl. *sniffing*)	**9**

GRUPA INCIDENATA	VRSTA INCIDENTA	BROJ INCIDENATA
Prevara	Fišing (engl. *phishing*)	**75.134**
	Neovlašćeno korišćenje resursa (engl. *cryptojacking*) i drugi oblici	**1.056**
Pokušaj upada u IKT sistem	Pokušaj otkrivanja kredencijala (engl. *brute force attack, dictionary attack* i sl.)	**16.831.352**
	Pokušaj iskorišćavanja ranjivosti sistema	**501.478**
Upad u IKT sistem	Neovlašćeni pristup aplikaciji	**1.030**
	Otkrivanje ili neovlašćeno korišćenje neprivilegovanih naloga (engl. *unprivileged account compromise*)	**971**
	Mreža zaraženih uređaja (engl. *botnet*)	**228**
	Otkrivanje ili neovlašćeno korišćenje privilegovanih naloga (engl. *privileged account compromise*)	**8**
Nedostupnost ili ograničena dostupnost IKT sistema	Prekid u funkcionisanju sistema ili dela sistema (engl. *outage*)	**919**
	Distribuirani napad sa ciljem onemogućavanja ili ometanja funkcionisanja IKT sistema (engl. *distributed denial-of-service attack – DDoS*)	**10**
	Napad sa ciljem onemogućavanja ili ometanja funkcionisanja IKT sistema (engl. *denial-of-service attack – DoS*)	**37**

GRUPA INCIDENATA	VRSTA INCIDENTA	BROJ INCIDENATA
	Sabotaža	**0**
Ugrožavanje bezbednosti podataka	Kriptografski napad	**14**
	Neovlašćen pristup podacima	**3**
	Neovlašćena izmena ili brisanje podataka	**2**
Operativni incidenti	Otkazivanje hardverskih komponenti	**6.719**
	Problemi u radu sa softverskim komponentama	**6.558**
Incidenti fizičko-tehničke bezbednosti	Poplava	**27**
	Krađa hardverskih komponenti	**16**
	Požar	**2**
Ostali incidenti	Incidenti koji ne spadaju u gore navedene kategorije	**341**
	UKUPNO	**25.958.850**

Tabela 3 - Broj incidenata po vrstama



Grafikon 2 – Pet najbrojnijih vrsta incidenata

3.1. INSTALIRANJE ZLONAMERNOG SOFTVERA U OKVIRU IKT SISTEMA

Malver (engl. *malware*) je reč izvedena od dve reči – "*Malicious Software*", i predstavlja svaki softver koji je napisan u zlonamerne svrhe, odnosno koji ima cilj da nanese štetu računarskim sistemima ili mrežama. U ove programe spadaju: računarski virus, računarski crv, ransomver, računarski trojanac, špijunski softver i rutkit.

Računarski virus je deo zlonamernog kompjuterskog kôda čiji je cilj da se širi sa računara na računar tako što napada izvršne datoteke i dokumenta i može prouzrokovati namensko brisanje datoteka sa hard diska i sličnu štetu.

Računarski crv je program koji sadrži zlonamerni kôd koji se širi preko mreže, tako što se samostalno umnožava i prenosi, odnosno ne zavisi od datoteka hosta. Crvi se šire na adrese elektronske pošte sa liste kontakta žrtve ili iskorišćavaju ranjivosti mrežnih aplikacija i zbog velike brzine širenja služe za prenos ostalih tipova zlonamernog softvera.

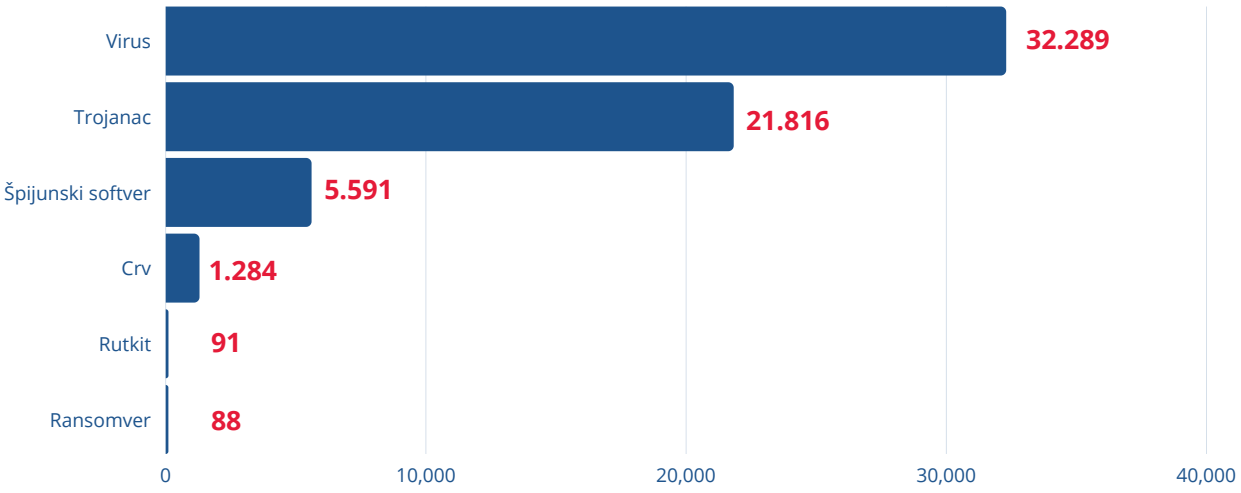
Ransomver je zlonamerni softver koji šifrira podatke na uređajima ili mrežama, a za pristup i otključavanje datoteka zahteva plaćanje otkupa. Čest je slučaj da datoteke čak i nakon plaćanja otkupa ostaju zaključane.

Računarski trojanci (trojanski konji) su pretnja koja pokušava da se predstavi korisnicima kao da su korisni programi i na taj način ih prevari da ih pokrenu. Ovi programi mogu da preuzmu druge pretnje sa interneta, ubacuju druge tipove malvera na ugrožene računare, komuniciraju sa udaljenim napadačima, kao i da beleže sve što se kuca na tastaturi i šalju napadačima.

Špijunski softver delimično presreće ili preuzima kontrolu nad računarom bez znanja ili dozvole korisnika. Sam naziv sugeriše da je reč o programima koji nadgledaju rad korisnika tako što snimaju i preuzimaju informacije sa računara poput navika pretraživanja veba, elektronske pošte, kredencijala i sl. i te podatke prenose napadaču.

Rutkit je softver koji omogućava privilegovan daljinski pristup računaru, krijući svoje prisustvo od administratora sistema. Omogućava napadaču da se sakrije u toku neovlašćenog pristupa i održava privilegovan pristup računaru zaobilaženjem uobičajenog načina autentifikacije i mehanizama autorizacije.

U okviru ove grupe incidenata prijavljeno je 32.289 instalacija virusa, dok je ransomver u IKT sistemima od posebnog značaja prijavljen 88 puta (Grafikon 3).



Grafikon 3 – Instaliranje zlonamernog softvera u okviru IKT sistema

3.2. NEOVLAŠĆENO PRIKUPLJANJE PODATAKA

Neovlašćeno prikupljanje podatka podrazumeva skeniranje portova, presretanje podataka između računara i servera, socijalni inženjering i kompromitovanje ili curenje podataka.

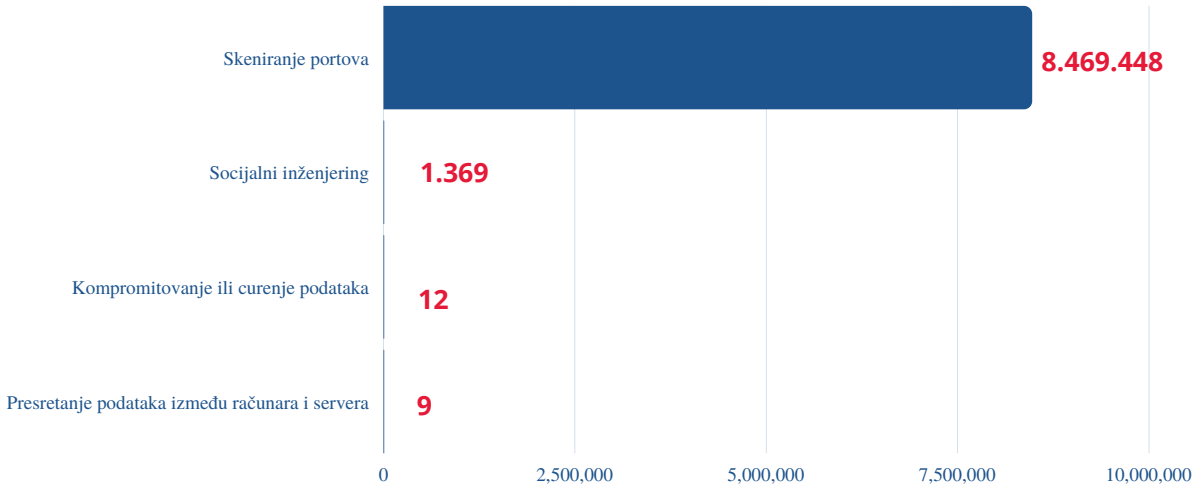
Skeniranje portova je napad koji šalje zahteve klijenata na niz adresa portova servera hosta, sa ciljem otkrivanja komunikacionih kanala koji se mogu iskoristiti, odnosno pronalaska otvorenog porta i iskorišćavanja njegove ranjivosti.

Snifing napad, odnosno presretanje podataka podrazumeva korišćenje aplikacija za nadgledanje, analizu i snimanje mrežnog saobraćaja u cilju preuzimanja mrežnih paketa. Na ovaj način napadač analizira mrežu i pribavlja informacije kojim je može kompromitovati.

Napadi **socijalnog inženjeringa** koriste ljudsku psihologiju i podložnost manipulacijama kako bi naveli žrtve na otkrivanje osetljivih podataka ili kršenje bezbednosnih mera koje će omogućiti napadaču pristup mreži.

Povreda podataka (kompromitovanje i curenje podataka) podrazumeva uspešan zlonameran pokušaj koji je doveo do izmene ili gubitka podataka.

Na grafikonu 4 prikazano je čak 8.469.448 prijava skeniranja portova što se može objasniti velikim brojem automatizovanih procesa za ispitivanje dostupnih servisa na udaljenim računarima, 1.369 prijava socijalnog inženjeringa, 12 kompromitovanja ili curenja podataka i 9 prijava presretanja podataka između računara i servera.



Grafikon 4 – Neovlašćeno prikupljanje podataka

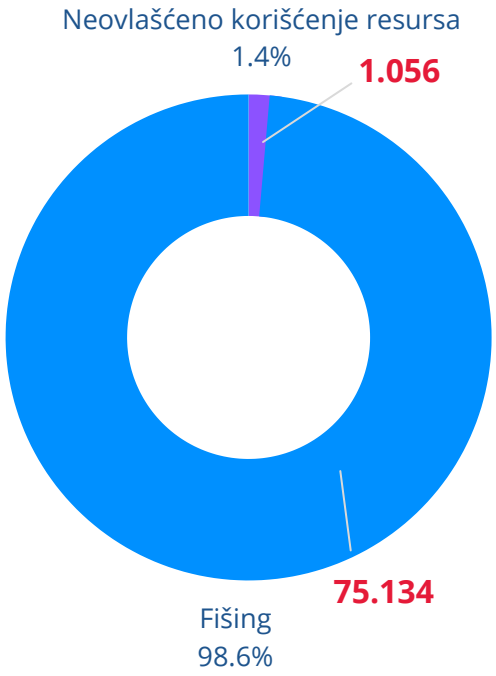
3.3. PREVARA

Pod prevarom se podrazumevaju fišing napadi, neovlašćeno korišćenje resursa i drugi oblici prevare.

Fišing je sajber napad koji se vrši uz pomoć elektronske pošte, koja sadrži zlonamerni prilog ili link koji vodi ka zaraženom sajtu ili dokumentu. Napadač koristi socijalni inženjering da bi se predstavio kao neko poznat i tako naveo žrtvu da otvori elektronsku poštu. Ovaj napad je često povezan i sa napadima poput malvera, mreže botova i sajber špijunaže.

Neovlašćeno korišćenje resursa - Kriptodžeking (poznat i kao kriptomajning) odnosno „otimanje“ ili ''rudarenje'' je novi termin koji se odnosi na programe koji koriste snagu centralne procesorske jedinice (70% do 80% neiskorišćene snage procesora) bez pristanka žrtve, da bi „rudarili“ kriptovalute za sticanje lične koristi.

Broj prijava koji se odnosi na 2020. godinu iznosi 75.134 za fišing napade, dok neovlašćeno korišćenje resursa iznosi 1.056 prijava (Grafikon 5).



Grafikon 5 – Prevara

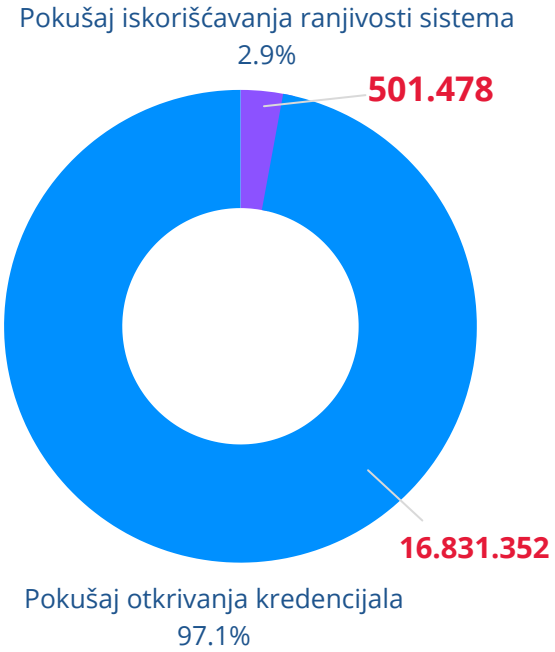
3.4. POKUŠAJ UPADA U IKT SISTEM

Prilikom pokušaja upada u IKT sistem napadači najčešće koriste tehniku *Brute Force* za otkrivanje kredencijala ili pokušavaju da iskoriste ranjivosti informacionog sistema.

Pokušaj iskorišćavanja ranjivosti sistema je napad na računarski sistem, kojim napadač koristi određenu ranjivost sistema. Ovaj napad koristi ranjivost operativnog sistema, aplikacije ili bilo kojeg drugog softverskog koda, uključujući dodatke aplikacija ili biblioteke softvera.

Brute Force napad podrazumeva pokušaj pristupa sistemu žrtve neprekidnim logovanjem različitim kombinacijama slova, brojeva i simbola sa ciljem identifikacije korisničkog imena i lozinke.

U 2020. godini napadači su u najvećoj meri za upad u sistem koristili tehnike otkrivanja kredencijala (16.831.352 pokušaja) dok su u manjoj meri za upad u IKT sistem od posebnog značaja pokušavali da iskoriste ranjivosti sistema (501.478 pokušaja, Grafikon 6).



Grafikon 6 – Pokušaj upada u IKT sistem

3.5. UPAD U IKT SISTEM

Upad u IKT sistem podrazumeva uspešno kompromitovanje sistema ili aplikacija (servisa) izvršeno sa udaljene lokacije korišćenjem nove ili poznate ranjivosti ili neovlašćenim lokalnim pristupom.

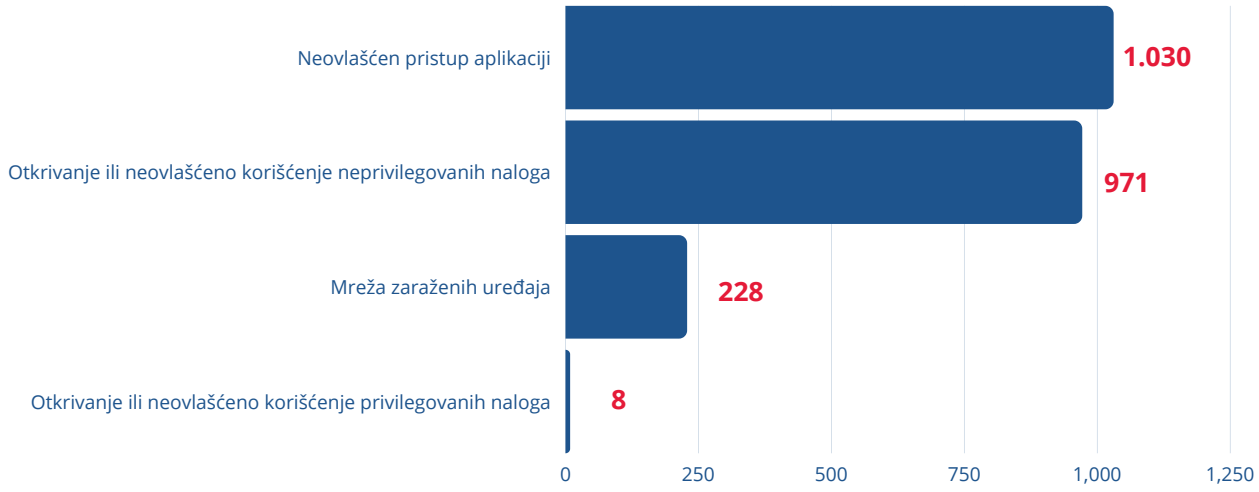
Otkrivanje ili neovlašćeno korišćenje privilegovanih naloga (engl. *Privileged Account Compromise*) omogućava napadačima da se neprimećeno kreću kroz IKT sistem i pristupe osetljivim podacima.

Otkrivanje ili neovlašćeno korišćenje neprivilegovanih naloga (engl. *Unprivileged Account Compromise*) omogućava napadačima da se neprimećeno kreću kroz ograničeni deo IKT sistema, sa mogućnošću dalje kompromitacije IKT sistema i pristupanja osetljivim podacima.

Neovlašćeni pristup aplikaciji je pristup veb lokaciji, programu, serveru, servisu ili drugom sistemu pomoću tuđeg naloga ili drugih metoda.

Mreža zaraženih uređaja je automatizovani napad koji je skenira mrežne adrese i širi zaraze na ranjivim računarima, što omogućava hakerima da preuzmu kontrolu nad zaraženim računarima i pretvore ih u botove. Na taj način se stvara mreža botova koja se koristi za napade onemogućavanja usluga (*DDoS*), kao i za izvršavanje zadataka bez znanja žrtve (slanje elektronske pošte,virusa ili krađe ličnih podataka).

U 2020. godini je najčešće zabeležen neovlašćen pristup aplikaciji (1.030 prijava), zatim otkrivanje ili neovlašćeno korišćenje neprivilegovanih naloga (971 prijava), mreža zaraženih uređaja je omogućila upad 228 puta, dok su se upadi putem otkrivanja ili neovlašćenog korišćenja privilegovanih naloga dogodili 8 puta (Grafikon 7).



Grafikon 7 – Upad u IKT sistem

3.6. NEDOSTUPNOST ILI OGRANIČENA DOSTUPNOST IKT SISTEMA

Napadima nedostupnosti ili ograničene dostupnosti IKT sistema se opterećuje mrežni saobraćaj, što dovodi do kašnjenja operacija ili pada sistema.

Dostupnost može biti ugrožena i lokalnim radnjama (uništenje, prekid u distribuciji električnom energijom i slično) ili usled više sile, spontanih grešaka ili ljudske greške bez namere ili grubog zanemarivanja.

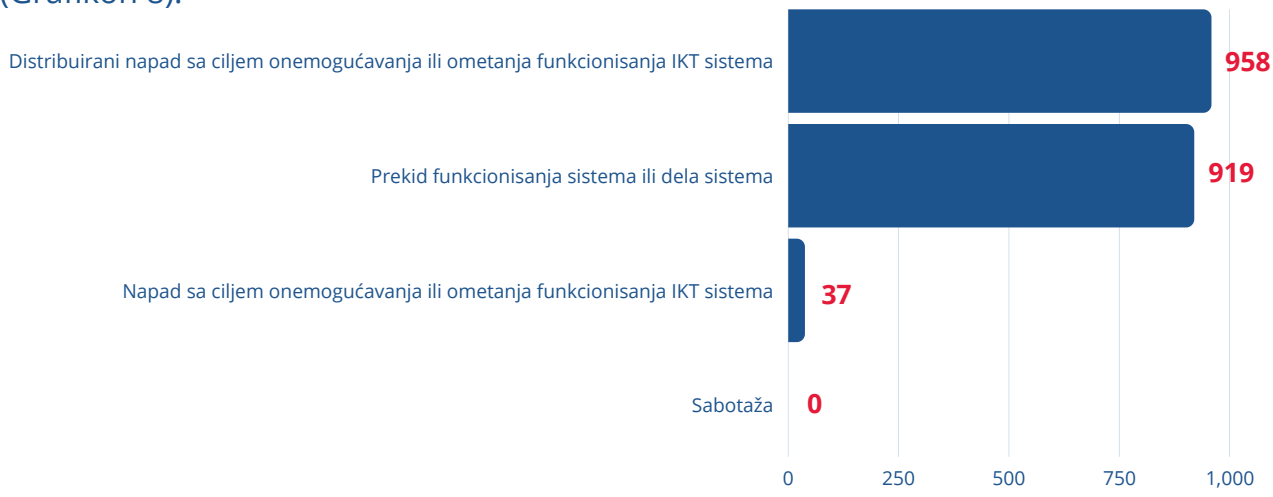
Napad sa ciljem onemogućavanja ili ometanja funkcionisanja IKT sistema (engl. *denial-of-service attack – DoS*) je pokušaj napadača da onemogući pristup serveru ili servisima koji su namenjeni krajnjim korisnicima.

Distribuirani napad sa ciljem onemogućavanja ili ometanja funkcionisanja IKT sistema (engl. *distributed denial-of-service attack – DDoS*) je višestruki napad koji ima za cilj da se poremeti normalan saobraćaj servera, usluge ili mreže preplavljujući infrastrukturu većom količinom internet saobraćaja. *DDoS* napadi postižu efikasnost koristeći više kompromitovanih računarskih sistema kao izvora saobraćaja.

Sabotaža kao napad se koristiti u svrhu sabotiranja sistema i nanošenja štete. Mogući su različiti oblici sabotaže u zavisnosti od oblasti poslovanja napadnute infrastrukture.

Prekid u funkcionisanju sistema ili dela sistema (engl. *outage*) može biti prouzrokovan i prekidom u isporuci električne energije, zbog loših vremenskih uslova ili hardverske greške koja je nastala kao posledica neispravne opreme.

IKT sistemi od posebnog značaja su detektovali 958 *DDoS* napada, 919 prekida funkcionisanja sistema ili dela zbog tehničkih problema, odnosno loših vremenskih uslova, 37 *DoS* napada, dok se sabotaža IKT sistema u 2020. godini nije dogodila (Grafikon 8).



Grafikon 8 – Nedostupnost ili ograničena dostupnost IKT sistema

3.7. UGROŽAVANJE BEZBEDNOSTI PODATAKA

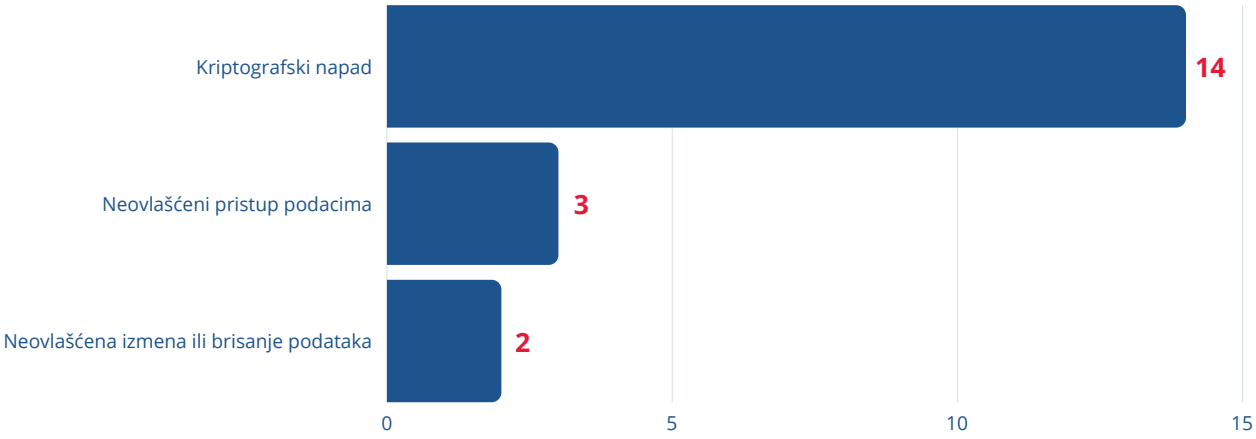
Pored zloupotrebe podataka i sistema neovlašćenim pristupom, odnosno neovlašćenom izmenom ili brisanjem podataka, narušavanje bezbednosti podataka može biti i posledica kriptografskog napada.

Neovlašćen pristup podacima je napad pomoću kog se ugrožava bezbednost podataka zloupotrebom prava pristupa podacima sistema.

Neovlašćena izmena podataka je napad pomoću kog se zloupotrebom prava pristupa podacima sistema vrši izmena, dodavanje ili brisanje podataka.

Kriptografski napad je metod zaobilaženja mera zaštite kriptografskog sistema pronalaženjem slabosti u kodu, šifri, algoritmu, kriptografskom protokolu ili šemi upravljanja ključevima.

U 2020. godini je zabeleženo 14 kriptografskih napada, tri neovlašćena pristupa podacima i dve neovlašćene izmene ili brisanje podataka (Grafikon 9).

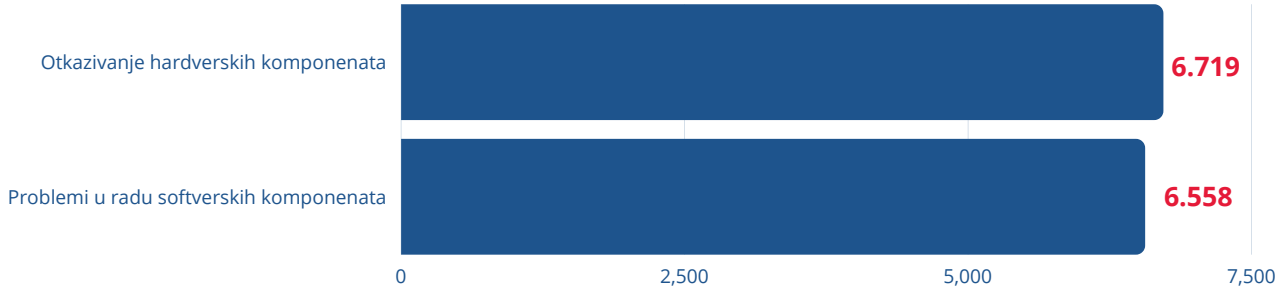


Grafikon 9 – Ugrožavanje bezbednosti podataka

3.8. OPERATIVNI INCIDENTI

Operativni incidenti su svi oni incidenti koji dovode do otkazivanja hardverskih komponenti ili problema u radu sa softverskim komponentama.

Broj otkazivanja hardverskih komponenti u 2020. godini je iznosio 6.719, a broj problema u radu sa softverskim komponentama koje su dovele do zastoja u pružanju usluga, odnosno prekida koji je na bilo koji način ugrozio poslovni proces (na primer kraći prekidi u radu) je iznosio 6.558 (Grafikon 10).

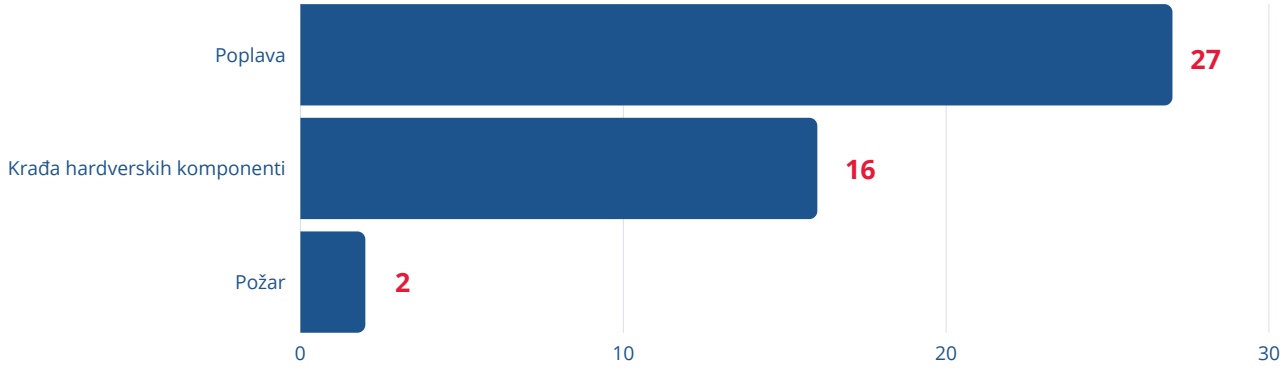


Grafikon 10 – Operativni incidenti

3.9. INCIDENTI FIZIČKO-TEHNIČKE BEZBEDNOSTI

Ovoj grupi incidenata pripadaju krađa hardverskih komponenti, požar i poplava koji su doveli do ugrožavanja fizičko-tehničke bezbednosti IKT sistema.

U 2020. godini zabeleženo je 27 poplava, 16 krađa hardverskih komponenti i 2 požara (Grafikon 11).



Grafikon 11 – Incidenti fizičko-tehničke bezbednosti

3.10. OSTALI INCIDENTI

U grupu ostalih incidenata spadaju svi incidenti koji nisu navedeni u prethodnim kategorijama.

Ostalih incidenata u 2020. godini je bilo 341 (Grafikon 12)

Grafikon 12 – Ostali incidenti

4. ZAKLJUČAK

Najčešća vrsta sajber napada je pokušaj otkrivanja kredencijala, koji podrazumeva pokušaj pristupa sistemu žrtve neprekidnim logovanjem različitim kombinacijama slova, brojeva i simbola sa ciljem identifikacije korisničkog imena i lozinke ili korišćenjem rečnika. Ovo je stara vrsta napada, ali još uvek veoma efikasna i popularna među napadačima. Pristup legitimnom nalogu može omogućiti pristup čitavom IKT sistemu. Ova vrsta napada se ne oslanja na ranjivosti IKT sistema već na slabe lozinke korisnika.

Prelaskom na režim rada od kuće povećan je broj ovih napada koji su pokušavali da iskoriste *Windows Remote Desktop Protocol (RDP)* koji administratori sistema koriste za pristup *Windows* sistemima sa udaljene lokacije. Kasnije su ovi napadi preusmereni i na pojedince koji rade od kuće i nemaju određene nivoe zaštite kao u kancelarijama, odnosno IKT sistemima što ih čini lakom metom, naročito ukoliko koriste i slabe lozinke. Odbrana od ovog napada je zahtevna i pored edukacije zaposlenih o važnosti upotrebe kompleksnih lozinki, podrazumeva i korišćenje dvo-faktorske i multi-faktorske autentifikacije, *VPN*-a, kao i enkripciju podataka na uređajima koji se koriste u poslovne svrhe.

Na drugom mestu nalazi se skeniranje portova, kojim se zapravo prikupljaju informacije i ne nanosi šteta samoj meti, ali se takvi napadi koriste za pribavljanje korisnih informacija za dalji upad. Glavni cilj ovog napada je otkrivanje koji portovi su otvoreni, koji zatvoreni, a koji filtrirani, a mogu se skenirati svi portovi, kojih ima oko 65.000 ili samo oni koji pružaju servise koji se mogu zloupotrebiti korišćenjem poznate ranjivosti. Zastupljenost je povećana i zbog automatizacije ove vrste napada, a sami IKT sistemi od posebnog značaja mogu biti deo skeniranog opsega.

Pokušaj iskorišćavanja ranjivosti sistema je na trećem mestu i predstavlja slabost čijom zloupotrebom napadači mogu ugroziti integritet, raspoloživost, autentičnost i neporecivost podataka kojima se rukuje pomoću IKT sistema.

Pokušaj iskorišćavanja ranjivosti sistema je napad kojim napadač pokušava da pristupi sistemu za koji nema odobrenje, iskorišćavanjem poznatih ili novih ranjivosti. Postoji nekoliko javno dostupnih evidencija poznatih ranjivosti kao što su *CVE*, *NVD* i *OVAL*. *CVE* identifikator obično uključuje kratak opis, a ponekad i savete, mere ublažavanja i izveštaje.

Na četvrtom mestu se nalazi fišing. Tokom 2020. godine sprovedeno je nekoliko velikih fišing kampanja čija su meta bili korisnici interneta u Srbiji. Najveće po obimu, intenzitetu, ali i učestalosti su kampanje namenjene klijentima banaka. Fišing poruke su izgledale kao da se šalju sa legitimnih domena i sadržale su priloge o deviznom prilivu novca. Fišing kampanja koja je zloupotrebila Institut za javno zdravlje „Dr Milan Jovanović Batut“ bila je usmerena na javne ustanove i privredne subjekte i sadržala je lažno obaveštenje o besplatnoj raspodeli zaštitne opreme. Ove fišing kampanje su distribuirale *Lokibot* trojanca, koji krade informacije kao što su korisnička imena, lozinke, bankovni detalji ili sadržaj novčanika kripto valuta. Informacije krade korišćenjem *keylogger*-a snima aktivnosti u pretraživaču i desktopu, a može da kreira i *backdoor* i tako omogući instaliranje dodatnih opterećenja za sistem.

Ostale kampanje su navodile korisnike da kliknu na link koji vodi na lažnu stranicu, koje je sve teže prepoznati kao nebezbedne. Napadači u sve većoj meri koriste *HTTPS* iako su tehnologije kao što su *HTTPS* i *SSL* kreirane u cilju obezbeđivanja komunikacije između klijenta i servera. Katanac na adresnoj liniji pretraživača može navesti korisnika da pomisli da je stranica bezbedna. Povećan je i broj usluga besplatnih sertifikata, a ovome doprinosi i činjenica da pretraživači uglavnom *HTTPS* stranicu obeležavaju kao bezbednu bez dodatne provere.[1] Za vreme trajanja pandemije, značajno je povećan broj lažnih internet stranica koje koriste temu virusa COVID-19, odnosno sadrže neki od pojmova pandemije u nazivu domena ("*Covid19/Coronavirus*“). Pored distribucije malvera, ove stranice se koriste za lažnu prodaju medicinske opreme, suplemenata, lekova, vakcina i prevarom korisnika, hakeri dolaze do protivpravno stečene imovinske koristi.

Napadači su koristili i novije vrste fišing napada od kojih su najzastupljeniji bili kompromitovanje poslovne e-pošte, *vishing*, *smishing*. Fišing napad, bilo da se koristi za distribuciju zaraženog priloga ili linka, zahteva reakciju potencijalne žrtve. Korišćenjem različitih mamaca, napadači su pokušavali da dođu do željene reakcije korisnika, od kojih se na globalnom nivou tokom prošle godine izdvojio „*COVID-19*“.

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

Na petom mestu je virus. Virusi mogu biti usmereni na masovno zaražavanje računarskih mreža ili na mrežu kompanije ili organizacije koja je meta. Nivo zaštite determiniše nivo angažovanja napadača pa se često dešava da su, s obzirom da većina organizacija koristi *Firewall* i druge mere zaštite od spoljnih napada, napadači prinuđeni da zatraže pomoć unutar organizacije. Metodi socijalnog inženjeringa omogućavaju napadačima lakši pristup zaposlenima i IKT sistemima u kojima rade, a prelazak na rad od kuće i stanje opšteg straha su doprineli unapređenju ovih metoda.

Računarski virus je deo zlonamernog kompjuterskog kôda čiji je cilj da se širi sa računara na računar tako što napada izvršne datoteke i dokumenta i može prouzrokovati namensko brisanje datoteka sa hard diska i sličnu štetu. Dve osnovne karakteristike virusa su sposobnost samostalnog izvršavanja, tako što će zameniti pokretanje željenog programa sopstvenim pokretanjem, i repliciranja, zamenom izvršnih datoteka kopijom datoteka zaraženih virusom.

Virus je najzastupljenija vrsta malvera, dok je trojanac na drugom mestu po ukupnoj zastupljenosti. Ovaj zlonamerni softver se korisnicima predstavlja kao korisni program i na taj način prevari korisnike da ga pokrenu. Ovaj malver može da preuzme i druge pretnje sa interneta, ubacuje druge tipove malvera na ugrožene računare, komunicira sa udaljenim napadačima, kao i da beleži sve što se kuca na tastaturi i šalje napadačima. Jedan od najpoznatijih napada Emotet je počeo kao bankarski trojanac i evoluirao do mreže zaraženih uređaja.

Treća najzastupljenija vrsta malvera je špijunski softver koji se instalira bez saglasnosti korisnika infiltriranjem kroz paket aplikacija, posetom zaraženoj internet stranici ili kroz zaraženi prilog. Ovaj malver nadgleda rad korisnika kroz snimanje ekrana, beleženjem onoga što se otkuca na tastaturi i ukradene podatke šalje autoru špijunskog softvera koji ih koristi ili prodaje dalje. Podaci do koji se dolazi na ovaj način su korisničko ime i lozinka, PIN naloga, broj kreditne kartice, teksta otkucanog na tastaturi, navika u pretraživanju interneta, korišćene adrese e-pošte.

Crv je na četvrtom mestu po zastupljenosti, a ova vrsta malvera za infiltriranje najčešće koristi ranjivosti softvera. Kao i ostale vrste malvera može se distribuirati i putem priloga e-pošte. Crv može da izmeni ili izbriše podatke, a može se koristiti i za ubacivanje dodatnog zlonamernog softvera na računar korisnika.

Najzastupljeniji malver u svetu je tokom 2020. godine bio ransomver, a mete napada su bile čak i bolnice i to u vreme vanredne i velike borbe sa pandemijom virusa *COVID-19*. Zabeleženo je i povećanje iznosa otkupnine i vremena koje je potrebno za oporavak od napada[2]. Jedan od većih ransomver napada dogodio se i u našoj zemlji, a meta napada bilo je javno komunalno preduzeće Informatika iz Novog Sada. Ransomver *Pwndlocker* je na nekoliko dana onemogućio pružanje usluga nekoliko gradskih institucija koje su u mreži gradske uprave. Ovaj ransomver je korišćen i za napade na gradske uprave i velike kompanije drugih zemalja, naročito u SAD, a napadači su određivali iznos otkupnine u zavisnosti od veličine mreže, broja zaposlenih i godišnjih prihoda. Ransomver je vrsta malvera koja je na šestom mestu po zastupljenosti u našoj zemlji.

Razlika u broju različitih vrsta malvera u odnosu na fišing napade ohrabruje, dok broj operativnih incidenata ukazuje da su stalna ulaganja u IKT neophodna, kao i da će kontinuirano ulaganje u kadrovske kapacitete i tehnologiju značajno unaprediti trenutno stanje informacione bezbednosti u Republici Srbiji.

Imajući u vidu da je 2020. godina bila godina izazova u svakom smislu, može se zaključiti da su i operatori IKT sistema od posebnog značaja uspeli da se izbore sa bezbednosnim pretnjama i napadima u sajber prostoru. Primena mera zaštite i ispunjavanje obaveze dostavljanja statističkih podataka o svim incidentima u IKT sistemima svakako čine sajber prostor Republike Srbije bezbednijim, a operatore IKT sistema stimulišu na utvrđivanje stanja i kontinuirano unapređenje informaciono-komunikacionih tehnologija i kadrovskih kapaciteta.

SRB-CERT

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