REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE
ZA INFORMACIJSKO VARNOST

URSIV

Polletno poročilo o kibernetskih incidentih in napadih

2021-2

Februar 2022

O URSIV

Urad Vlade Republike Slovenije za informacijsko varnost (URSIV) je pristojni nacionalni organ za informacijsko varnost, ki od 31. 7. 2021 deluje kot samostojna vladna služba. Izvaja naloge enotne kontaktne točke za zagotavljanje čezmejnega sodelovanja z ustreznimi organi drugih držav članic EU in z evropsko mrežo skupin za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij (CSIRT) ter druge naloge mednarodnega sodelovanja.

Kontakt

URAD VLADE REPUBLIKE SLOVENIJE ZA INFORMACIJSKO VARNOST
Ulica gledališča BTC 2, 1000 Ljubljana

Telefon: (01) 478 47 78
E-naslov: gp.uiv@gov.si
Spletna stran: www.uiv.gov.si
Twitter: @URSIV_Slovenia

O CSIRT

CSIRT je skupina, ki se odziva na incidente na področju informacijske varnosti, sprejema prijave o kršitvah varnosti, izvaja analize in pomaga priglasiteljem pri obvladovanju incidentov.

Naloge **nacionalnega odzivnega centra za kibernetsko varnost** opravlja **SI-CERT** *(angl. Slovenian Computer Emergency Response Team)* v okviru javnega zavoda **Akademska in raziskovalna mreža Slovenije (Arnes)**. Odzivni center je pristojen tudi za priglasitev incidentov izvajalcev bistvenih storitev (v nadaljevanju: IBS) iz sektorjev energija, digitalna infrastruktura, oskrba s pitno vodo in njena distribucija, zdravstvo, promet, bančništvo, infrastruktura finančnega trga, preskrba s hrano in varstvo okolja ter ponudnikov digitalnih storitev.

Kontakt

SI-CERT
ARNES, p.p. 7, SI-1001 Ljubljana

Telefon: (01) 479 88 22
Faks: (01) 479 88 23
E-naslovi:
Prijava incidenta: cert@cert.si
Splošni naslov: info@cert.si
Za medije: press@cert.si
Spletna stran: www.cert.si
Twitter: @sicert

Naloge **odzivnega centra za incidente v informacijskih sistemih organov državne uprave** opravlja **SIGOV-CERT** v okviru **Ministrstva za javno upravo.** Odzivni center je pristojen tudi za priglasitev incidentov organov državne uprave, ki upravljajo informacijske sisteme in dele omrežja oziroma izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti.

Kontakt

SIGOV-CERT[1]
Ministrstvo za javno upravo
Direktorat za informatiko
Sektor za informacijsko varnost
Tržaška cesta 21, 1000 Ljubljana

Telefon: (01) 478 86 51
Faks: (01) 478 86 49
E-naslov: cert@gov.si

PRAVNA PODLAGA

V skladu s šestim odstavkom 25. člena Zakona o informacijski varnosti (Uradni list RS, št. 30/18 in 95/21) URSIV in odzivna centra SI-CERT ter SIGOV-CERT, na podlagi podatkov s seznama incidentov in kibernetskih napadov za statistične namene in namene seznanjanja javnosti, dvakrat letno pripravijo anonimizirane informacije, ki jih tudi javno objavijo na svojih spletnih straneh.

SPLOŠNA OCENA

V drugem polletju nismo zabeležili kibernetskih incidentov z bistvenim vplivom na zaupnost, celovitost in razpoložljivost omrežij, informacijskih sistemov oziroma informacijskih storitev. SIGOV-CERT ni zaznal oz. poročal o incidentih s pomembnim vplivom na neprekinjeno izvajanje storitev organov državne uprave**,** SI-CERT pa pri IBS ni zaznal incidentov s pomembnim vplivom na neprekinjeno izvajanje bistvenih storitev, ki jih zagotavljajo.

Decembra 2021 je bilo zaradi zaznane kritične ranljivosti razglašeno stanje povečane ogroženosti varnosti omrežij in informacijskih sistemov zavezancev po Zakonu o informacijski varnosti. Vse večje število razkritih ranljivosti predstavlja za odzivna centra večjo obremenitev in nujno potrebo po organizacijski in kadrovski krepitvi.

[1] Od 1. 1. 2022 dalje SIGOV-CERT deluje kot sektor znotraj URSIV.

Kritična ranljivosti Microsoft Exchange (ProxyShell)

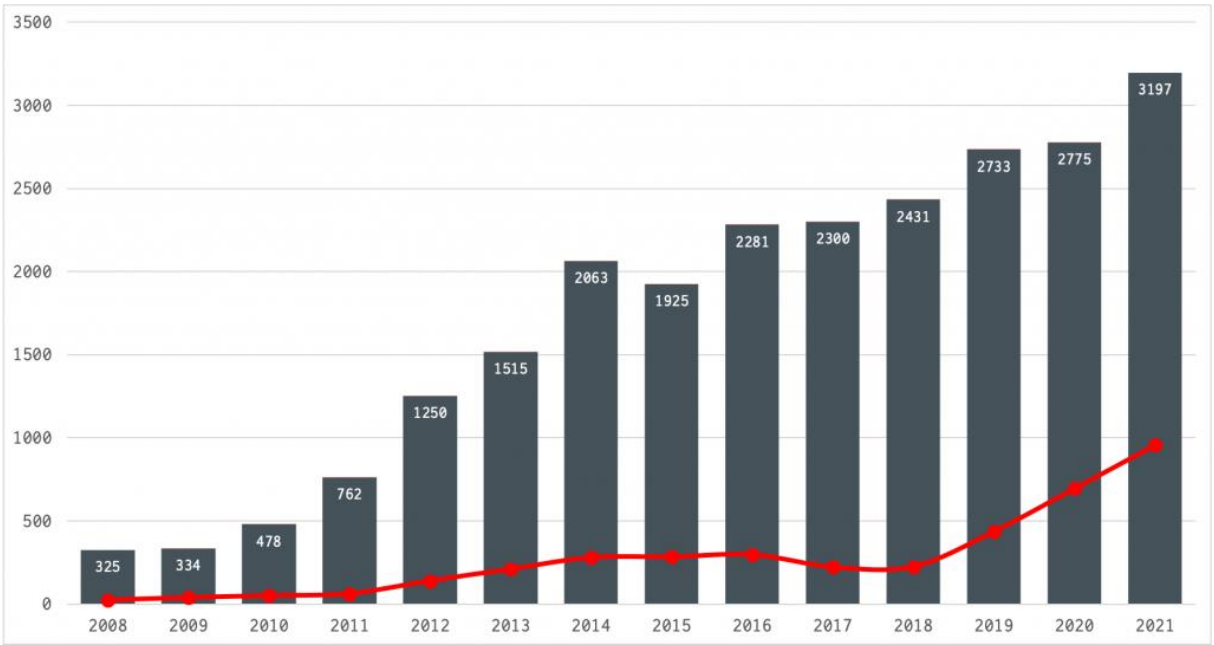
Avgusta 2021 smo bili seznanjeni s kritično ranljivostjo Microsoft Exchange (ProxyShell), ki omogoča oddaljeno izvajanje ukazov na ranljivem strežniku prek odprtih vrat 443. Ranljive so naslednje različice produkta:

- Microsoft Exchange Server 2019 Cumulative Update 9
- Microsoft Exchange Server 2019 Cumulative Update 8
- Microsoft Exchange Server 2016 Cumulative Update 20
- Microsoft Exchange Server 2016 Cumulative Update 19
- Microsoft Exchange Server 2013 Cumulative Update 23

Podobno, kot pri ProxyLogon ranljivosti (marec 2021), je predpogoj za izkoriščanje ranljivosti dostop do vrat 443 Exchange strežnika. Interni strežniki zato niso bili izpostavljeni aktivnemu skeniranju, vendar je SI-CERT vseeno svetoval čimprejšnjo nadgradnjo.

Vztrajna rast phishing napadov

SI-CERT ocenjuje, da phishing napadi ne pojenjajo, saj predstavljajo vedno večji delež med obravnavanimi incidenti, kar je razvidno iz spodnjega grafa. Gre za načeloma zelo enostavno tehniko družbenega inženiringa, kjer se ustvari videz avtentičnosti sporočila in se naslovnika prelisiči v razkritje prijavnih podatkov ali številke kreditne kartice. Opazili so trend phishing napadov v imenu dostavnih služb (Pošta Slovenije, DHL). Storilci so izkoristili porast spletnega nakupovanja v času epidemije.



Število obravnavanih incidentov na SI-CERT po letih (z deležem phishing incidentov in projekcijo za 2021)

Nadaljuje se rast števila incidentov v državni upravi

SIGOV-CERT je v tretjem četrtletju 2021 zaznal upad števila priglašenih incidentov glede na prejšnje četrtletje. Menijo, da je bil vzrok v vpeljavi dodatnih varnostnih mehanizmov in povečano razumevanje informacijske varnosti pri uporabnikih. V četrtem četrtletju pa so zaznali prirast števila incidentov glede na prejšnje četrtletje. Poglavitni vzrok je v povečanem številu elektronskih sporočil – goljufij (phishing), katere varnostni mehanizmi in uporabniki pripoznajo kot zlonamerne. Še vedno se srečujejo tudi s poskusi goljufij s pomočjo elektronske pošte, ki vsebuje povezave na spletna mesta z zlonamerno vsebino ter žaljive vsebine preko SPAM pošte.

Kritična ranljivost Java knjižnice Apache Log4j

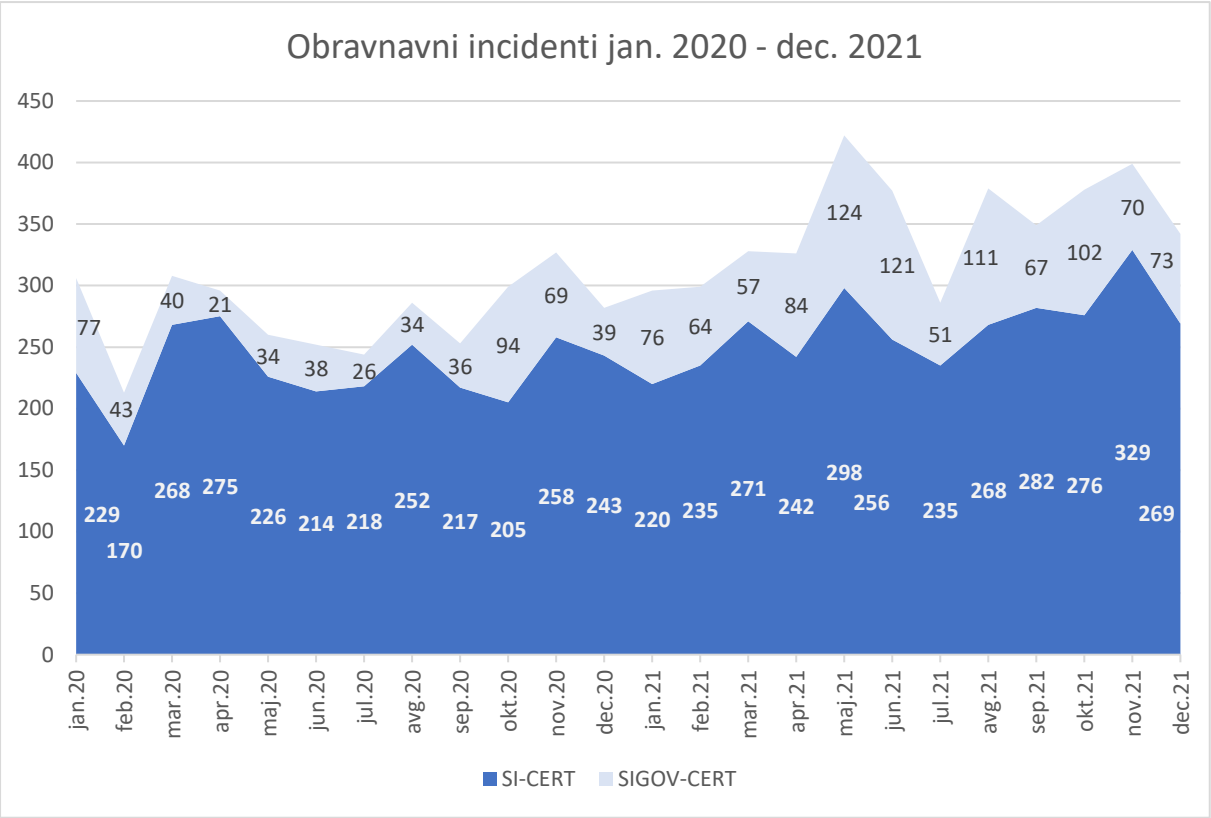
Ob koncu leta je v programski knjižnici Java logging library Log4j bila odkrita kritična ranljivost z oznako CVE-2021-44228, ki napadalcem omogoča izvajanje poljubne kode na sistemu *(angl. RCE – Remote Code Execution)* ali krajo občutljivih informacij. Do zlorabe ranljivosti pride ob zapisu posebnega niza znakov, ki vsebuje JNDI zahtevek, v dnevniško datoteko. Med analizo ranljivosti sta bili v predmetni knjižnici odkriti še ranljivosti CVE-2021-45046, ki omogoča izvedbo kode na daljavo (RCE), ter CVE-2021-45105, ki omogoča izvedbo napada z zavrnitvijo storitve (DoS, Denial-of-service). SI-CERT je objavil podatke o ranljivosti in navodila na spletu, ter obvestil zavezance po Zakonu o informacijski varnosti. Na podlagi zaznanih podatkov je URSIV sprejel odločitev, da se zaradi razsežnosti razkritih kritičnih ranljivosti in množične uporabe informacijskih produktov Java knjižnica Apache Log4j razglasi povečana stopnja ogroženosti varnosti omrežij in informacijskih sistemov. Ocenjeno je bilo, da ranljivost lahko vpliva na izvajanje bistvenih storitev ter delovanje informacijskih storitev, ki so potrebni za nemoteno delovanje države ali zagotavljanje nacionalne varnosti v Republiki Sloveniji. Zavezancem po Zakonu o informacijski varnosti so bile izdane odločbe z obveznimi ukrepi. Povečana stopnja ogroženosti varnosti omrežij in informacijskih sistemov je bila razglašena 14. 12. 2021 ob 15:00 uri.

Statistika

V drugem polletju leta 2021 sta odzivna centra obravnavala 2133 incidentov. V novembru je Si-CERT beležil rekordno število priglasitev.

Mesec	SI-CERT	SIGOV-CERT	Skupaj
Januar 2020	229	77	306
Februar 2020	170	43	213
Marec 2020	268	40	308
April 2020	275	21	296
Maj 2020	226	34	260
Junij 2020	214	38	252
SKUPAJ 1. polletje 2020	**1382**	**253**	**1635**
Julij 2020	218	26	244
Avgust 2020	252	34	286
September 2020	217	36	253
Oktober 2020	205	94	299
November 2020	258	69	327
December 2020	243	39	282
SKUPAJ 2. polletje 2020	**1393**	**298**	**1691**
SKUPAJ 2020	**2775**	**551**	**3326**
Januar 2021	220	76	296
Februar 2021	235	64	299
Marec 2021	271	57	328
April 2021	242	84	326
Maj 2021	298	124	422
Junij 2021	256	121	377
SKUPAJ 1. polletje 2021	**1522**	**526**	**2048**
Julij 2021	235	51	286
Avgust 2021	268	111	379
September 2021	282	67	349
Oktober 2021	276	102	378
November 2021	329	70	399
December 2021	269	73	342
SKUPAJ 2. polletje 2021	**1659**	**474**	**2133**
SKUPAJ 2021	**3181**	**1000**	**4181**

Ostali anonimizirani statistični podatki, ki sta jih posredovala SI-CERT in SIGOV-CERT, se nahajajo v prilogi 1 oziroma prilogi 2. Upoštevana je klasifikacija stopnje incidentov, ki jo pri svojem delu uporabljata odzivna centra.



OCENA

Na podlagi podatkov iz druge polovice leta 2021 ocenjujemo, da se bo nadaljevala izpostavljenost uporabnikov na phishing sporočila. Vse večji pomen dobivajo napadi na t.i. dobavno verigo. Pri slednjih je potrebna hitra odzivnost vseh deležnikov, da se prepreči morebitno oškodovanje. Ocenjujemo, da so se sredstva, ki smo jih v preteklosti investirali v preventivne dejavnosti ozaveščanja o varnosti na spletu (Varni na internetu, Safe.si) ter program e-izobraževanju javnih uslužbencev, pokazala pozitivne rezultate pri zaznavanju in blažitvi vplivov incidentov na področju kibernetske varnosti.

Na podlagi mednarodnih poročil ocenjujemo, da lahko v prihodnje pride do dodatnega porasta kibernetskega kriminala, saj izvajalci kriminalnih dejanj zlorabljajo povečano aktivnost posameznikov in pospešeno preoblikovanje poslovnih procesov podjetij. Storilci le-tega bodo še naprej inovativni pri uvajanju različnih zlonamernih programov in škodljive programske opreme Pričakovati je razširitev dejavnosti tudi na druge vrste spletnih napadov in prevar (npr. socialni inženiring, direktorska prevara, vrivanjem v poslovno komunikacijo, ljubezenske prevare). Vse bolj pa so zaradi hitrega zaslužka na udaru tudi posamezniki, ki želijo investirati v kripto valute.

Ob poslabšanju zdravstvene situacije lahko pričakujmo okrepljene aktivnosti na področju dela na domu, učenja na daljavo in spletnega nakupovanja. Zato lahko pričakujemo porast števila priglašenih incidentov (phishing napadov, spletnih goljufij, porazdeljenih napadov onemogočanja na strežnik, ipd.)

Področje odzivanja na ranljivosti bo pomemben dejavnik tudi v letošnjem letu. Zato moramo nadaljevati s sistematičnim pristopom in koordinirano obravnavo razkritih ranljivosti.

PREDLOGI IN PRIPOROČILA

Predlagamo ohranjaje visokega nivoja kibernetske varnosti IBS in organov državne uprave ter dosledno izpolnjevanje naloženih ukrepov za odpravo nepravilnosti in podanih priporočil, ki jih je oz. jih bo izdala Inšpekcija za informacijsko varnost, ki deluje v okviru URSIV.

Predlagamo, da spremljate oziroma vaše sodelavce opozorite na objave projekta Varni na internetu, ki ga izvaja SI-CERT (www.varninainternetu.si/) in projekta Center za varnejši internet, ki ga izvajajo Univerza v Ljubljani Fakulteta za družbene vede, Zavod Arnes, Zveza prijateljev mladine Slovenije in Zavod MISSS (www.safe.si/). SI-CERT je pripravil novo video serijo KLIK in brezplačni tečaj Varni v pisarni.

Vsem uporabnikom priporočamo, da:

- preverijo implementirane varnostne mehanizme in nastavitve aplikacij, programov in informacijskih sistemov;
- preverijo varnostne nastavitve/ukrepe povezane z zmogljivostmi za delo od doma;
- redno posodabljajo programsko opremo;
- izvedejo druge potrebne ukrepe za zagotovitev varnosti omrežij in podatkov ter podajo morebitne predloge za izboljšave.

IBS, organom državne uprave ter ostalim podjetjem in ustanovam priporočamo, da:

- posvetijo dodatno pozornost neobičajnim ali povečanim kibernetskim aktivnostim znotraj svojih sistemov, ki bi lahko pomenile kibernetsko tveganje za njihovo delovanje;
- preverijo ukrepe za neprekinjeno delovanje oziroma zagotavljanje storitev;
- pregledajo postopke za okrevanje po katastrofi *(angl. Disaster Recovery Procedures, DRP)* in postopke odzivanja na incidente;
- pregledajo podatke iz sistema za upravljanje varnostnih dogodkov in tveganj *(angl. Security Information and Event Manager, SIEM)* in drugih orodij ter opravijo analizo stanja (tip in obseg dogodkov).

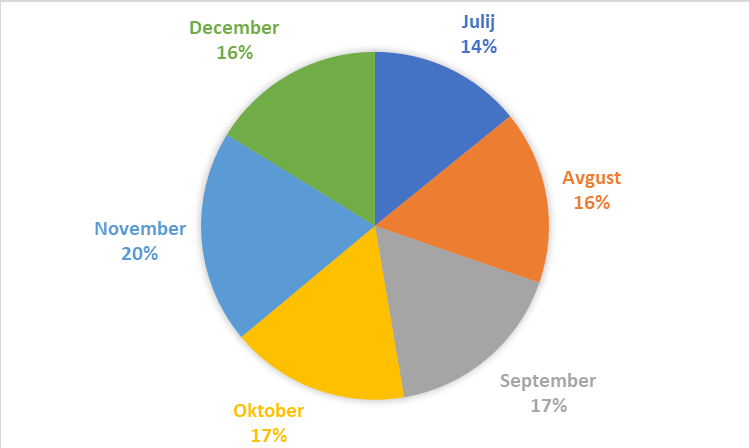
IBS in organe državne uprave opozarjamo na hranjenje dnevniških zapisov v zakonsko določenih časovnih okvirih. Posebno pozornost je potrebno še vedno nameniti zdravstvenem sistemu in podpornim deležnikom na področju zdravstva, saj lahko v podobnih situacijah, kot je COVID-19, hitro postanejo resne tarče, kar so žal že izkusile nekatere evropske države.

PRILOGA 1

Podatki SI-CERT

1. Število novih incidentov

Mesec	Število incidentov
Julij	235
Avgust	268
September	282
Oktober	276
November	329
December	269
SKUPAJ	**1659**



Delež incidentov po mesecih

2. Stopnje incidentov

Oznaka	Stopnja	3. četrtletje	4. četrtletje	Skupaj
C1	Kritičen incident	0	0	0
C2	Zelo pomemben incident	0	0	0
C3	Pomemben incident	1	5	6
C4	Incident visoke stopnje	21	6	27
C5	Incident srednje stopnje	52	70	122
C6	Incident nizke stopnje	711	793	1504
SKUPAJ		**785**	**874**	**1659**

3. Razdelitev po sektorjih

Skupina	Sektor	3. četrtletje	4. četrtletje	Skupaj
NIS	Energija	2	3	5
NIS	Ponudnik računalništva v oblaku		1	1
NIS	Zdravstvo		3	3
NIS	Promet	4	3	7
NIS	Bančništvo	14	11	25
ZInfV	Organi državne uprave	10	10	20
Ostalo	Operaterji elektronskih komunikacij	6	8	14
Ostalo	Raziskovalno-izobraževalni sektor	21	21	42
Ostalo	Druge pravne osebe	143	179	322
Ostalo	Fizična oseba	557	593	1150
Ostalo	Drugo	28	42	70
SKUPAJ		**785**	**874**	**1659**

4. Vrste in oznake novih incidentov

Kategorija	Vrsta	3. četrtletje	4. četrtletje	Skupaj
Neprimerna vsebina	Neželena sporočila	41	26	76
Neprimerna vsebina	Žaljiva vsebina	2	3	5
Neprimerna vsebina	Nasilna vsebina			
Zlonamerna koda	Črv	1	1	2
Zlonamerna koda	Virus	10	5	15
Zlonamerna koda	Trojanski konj	33	51	84
Zlonamerna koda	Rootkit			
Zlonamerna koda	Boti in botneti	1	3	4
Zlonamerna koda	Nadzorni strežnik			
Zlonamerna koda	Izsiljevalski virus	13	24	37
Zlonamerna koda	Orodje za oddaljen nadzor (RAT)	9	6	15
Zbiranje informacij	Odkrivanje potencialnih tarč in ranljivosti (skeniranje)	17	6	23
Zbiranje informacij	Prestrezanje komunikacije	1		1
Zbiranje informacij	Socialni inženiring			
Poskusi vdora	Izkoriščanje znane ranljivosti	1		1
Poskusi vdora	Poskusi prijav, bruteforce in napadi s slovarjem	16	2	18
Vdor	Zloraba privilegiranega uporabniškega računa			
Vdor	Zloraba neprivilegiranega uporabniškega računa	29	19	48
Vdor	Napad na aplikacijo	2	1	3
Razpoložljivost	Napad onemogočanja	2	1	3
Razpoložljivost	Porazdeljen napad onemogočanja	4	4	8
Razpoložljivost	Izpad delovanja naprav ali omrežja	2	2	4
Varnost informacijskih virov	Nepooblaščen dostop do podatkov	2	3	5
Varnost informacijskih virov	Nepooblaščeno spreminjanje podatkov	3	9	12
Varnost informacijskih virov	Odtekanje informacij	2	2	4
Goljufije	Nepooblaščeno izkoriščanje virov	1	1	2
Goljufije	Intelektualna lastnina in avtorske pravice	3	3	6
Goljufije	Kraja identitete	12	18	30
Goljufije	Phishing sporočilo	247	262	509
Goljufije	Phishing spletno mesto	25	40	65
Goljufije	Spletno nakupovanje	7	16	23
Goljufije	Goljufija z vnaprejšnjim plačilom	54	50	104
Goljufije	Izsiljevanje	36	29	65

Kategorija	Vrsta	3. četrtletje	4. četrtletje	Skupaj
Goljufije	Druge goljufije	141	163	304
Ranljivosti	Odgovorno razkrivanje	2	7	9
Ranljivosti	Razkritje ranljivosti	10	1	11
Ranljivosti	Ranljivi sistemi in naprave	4	9	13
Drugo	Drugo	52	107	159
Test	Namenjeno testom			
SKUPAJ		**785**	**874**	**1659**

5. Neposredna finančna izguba prijavitelja v EUR

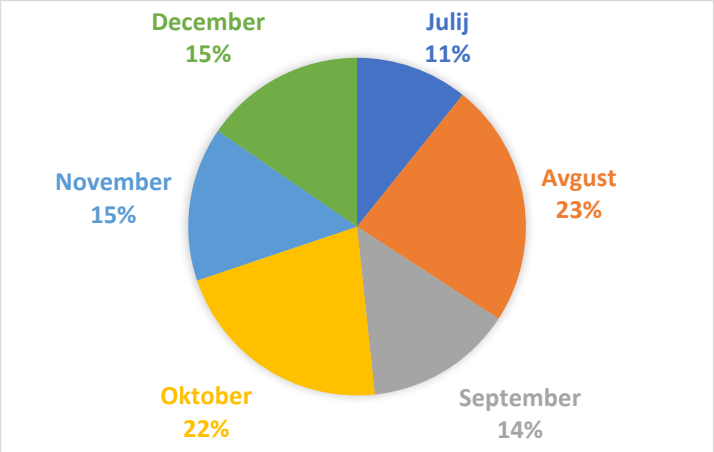
Kategorija	3. četrtletje	4. četrtletje	Skupaj
Druge goljufije	204.025,00	195.125,00	399.150,00
Goljufije z vnaprejšnjim plačilom	21.950,00	121.615,00	143.565,00
Kraja identitete	120.150,00		120.150,00
Zloraba neprivilegiranega uporabniškega računa	100,00	87.128,00	87.228,00
Nepooblaščeno spreminjanje podatkov	4.492,00	34.875,00	39.367,00
Phishing sporočilo	20.000,00	734,76	20.734,76
Odtekanje informacij		16.000,00	16.000,00
Izsiljevalski virus	480,00	1.860,00	2.340,00
Spletno nakupovanje	40,00	1.080,00	1.120,00
Izsiljevanje	300,00	250,00	550,00
Drugo	145,00	60,00	205,00
Napad na aplikacijo		100,00	100,00
SKUPAJ	**371.682,00**	**458.827,76**	**830.509,76**

PRILOGA 2

Podatki SIGOV-CERT

1. Število novih incidentov

Mesec	Število incidentov
Julij	51
Avgust	111
September	67
Oktober	102
November	70
December	73
SKUPAJ	**474**



Delež incidentov po mesecih

2. Stopnje incidentov

Oznaka	3. četrtletje	4. četrtletje	Skupaj
C1			
C2			
C3			
C4		1	
C5	229	244	473
SKUPAJ	**229**	**245**	**474**

3. Razdelitev po izvoru

Izvor	3. četrtletje	4. četrtletje	Skupaj
Osrednja državna uprava	227	244	471
Lokalna uprava	2	1	3
SKUPAJ	**229**	**245**	**474**

4. Klasifikacija incidentov

Vrsta	3. četrtletje	4. četrtletje	Skupaj
Goljufije	106	111	217
Informacijska varnost		1	1
Žaljiva/zlonamerna vsebina	47	71	118
Zbiranje informacij	38	23	61
Zlonamerna koda	11	19	30
Vdori/poizkusi vdora		2	2
Razpoložljivost	1		1
Ranljivost	1		1

Vrsta	3. četrtletje	4. četrtletje	Skupaj
Drugo	25	18	43
SKUPAJ	**229**	**245**	**474**