REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE
ZA INFORMACIJSKO VARNOST

URSIV

Polletno poročilo o kibernetskih incidentih in napadih, 2022-2

Februar 2023

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 **URSIV.** 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. Centralizirani organi državne uprave priglašajo incidente varnostno operativnemu centru Ministrstva za javno upravo, ki je pristojen za sprejem in obravnavo.

Kontakt

SIGOV-CERT

URAD VLADE REPUBLIKE SLOVENIJE ZA INFORMACIJSKO VARNOST

Ulica gledališča BTC 2, 1000 Ljubljana

Telefon: (01) 478 47 78

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, v nadaljevanju ZInfV) 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 smo zabeležili kibernetski incident z bistvenim vplivom na zaupnost, celovitost in razpoložljivost omrežij, informacijskih sistemov oziroma informacijskih storitev. Informacijski sistem Uprave Republike Slovenije za zaščito in reševanje (URSZR) je bil žrtev kibernetskega napada, ki je bil posledica slabega vzdrževanja in načrtovanja. Opravljen je bil inšpekcijski nadzor Inšpekcije za informacijsko varnost, ki deluje v okviru URSIV.

Tudi drugo polletje leta 2022, je bilo zaznamovano s kibernetskimi aktivnostmi povezanimi s konfliktom v Ukrajini. Glede na pretekla primerljiva obdobja je druga polovica leta 2022 na področju števila priglašenih incidentov postavila nov rekord. URSIV v sodelovanju z drugimi organi in organizacijami, pozorno spremlja situacijo na področju kibernetske varnosti doma, v državah članicah Evropske unije ter Ukrajini. V skladu z nalogo iz ZInfV URSIV izvaja redne koordinacijske aktivnosti. V skladu z Nacionalnim načrtom odzivanja na kibernetske incidente (NOKI) deluje Koordinacijska skupina za kibernetsko varnost, ki se sestaja vsaj enkrat na dva tedna.

V omenjenem obdobju so bile izvedene aktivnosti za dvig odpornosti kibernetskega sistema. Organizirana je bila druga konferenca IBS ter izvedene kibernetske vaje »Cyber Coalition 2022« in »Parallel and Coordinated Exercise EU Integrated Resolve 2022 – PACE EU IR 22«.

Konflikt v Ukrajini

Agresija Ruske federacije na Ukrajino se je odrazila tudi v drugi polovici leta. Na področju priglašenih kibernetskih incidentov zaznavamo rast, ki je verjetno posledica spremenjene varnostne situacije. Soočeni smo s pojavom t.i. hektavističnih skupin, ki s svojim aktivnostmi v kibernetskem prostoru predstavljajo podporo obema stranema v konfliktu. Poleg aktivnosti kibernetskega aktivizma (npr. aktivnosti skupine Killnet) se nadaljuje skeniranje omrežij za izrabo že znanih ranljivosti. V Evropski uniji in članicah NATA so zabeleženi DDoS napadi. Oba slovenska odzivna centra zaznavata posvečano število priglašenih incidentov v času konflikta.

Ranljivosti

SI-CERT je v drugi polovici leta objavil več opozoril o zaznanih ranljivostih. Tako so julija opozoril na več ranljivosti v produktih podjetja Siemens, vodilnem proizvajalcu na področju sistemske avtomatizacije v proizvodnji. Septembra je bilo objavljeno opozorilo o dveh ranljivostih Microsoft Exchange strežnika, ki omogočata napadalcem izvedbo napada z zagonom poljubne kode, pri čemer je pogoj za uspešno izvedbo napada predhodna pridobitev pravic avtenticiranega uporabnika. Novembra pa so javnost opozorili na ranljivost OpenSSL knjižnica različic 3.0.0 do 3.0.6. Ob koncu leta je bila zaznana ranljivost FortiOS SSL-VPN ter ranljivost Citrix ADC in Citrix Gateway.

Vedno znova zapažamo, da napadalci izkoriščajo stare ranljivosti programske opreme – tiste za katere že obstajajo popravki. Navedeno je mogoče zato, ker vzdrževalci informacijskih sistemov oz. programske opreme ne poskrbijo za pravočasno nameščanje popravkov. Vzroki so lahko v preobremenjenosti vzdrževalcev, neustreznem obvladovanju informacijskih sistemov in tudi malomarnosti oz. neodgovornem ravnanju.

Kibernetski napad na URSZR

Informacijski sistem URSZR je bil v jutranjih urah 17. 8. žrtev kibernetskega napada z izsiljevalskim virusom. Vstopna točka za napad je bil zasebni računalnik zaposlenega, ki se je v omrežje URSZR povezal preko VPN dostopa Napadu na sistem URSZR, enemu izmed treh stebrov nacionalne varnosti, je botrovalo slabo načrtovanje in vzdrževanje informacijsko komunikacijskega sistema. Delovanje informacijskega sistema zaščite in reševanja je bilo močno okrnjen in prizadeto. MORS je k odpravi težav pristopil na način ponovne vzpostavitve sistemov v drugem okolju (v okviru IS MORS).

Nedelovanje DRO

Dopoldne 9. 12. je na državnem računalniškem omrežju (DRO) prihajalo do težav pri delovanju, zato nekatere spletne storitve niso bile dosegljive. Težave na sistemu, ki so jih reševali z najvišjo prioriteto, so bile odpravljen v nekaj urah. Pristojni organi so pri pregledu ugotovili, da je bilo nedelovanje spletne strani GOV.SI posledica okoliščin v povezavi s tehničnimi težavami in DDoS aktivnostmi. Sprejeti so bili omejevalni ukrepi in odpravljene tehnične težave.

Phishing napadi ne pojenjajo

Iz podatkov SI-CERT in SIGOV-CERT je razvidno, da se je število incidentov, ki so bili obravnavani v tretjem in četrtem četrtletju, povečalo. Rekordna sta bila september in oktober. Upad je bil zaznan le

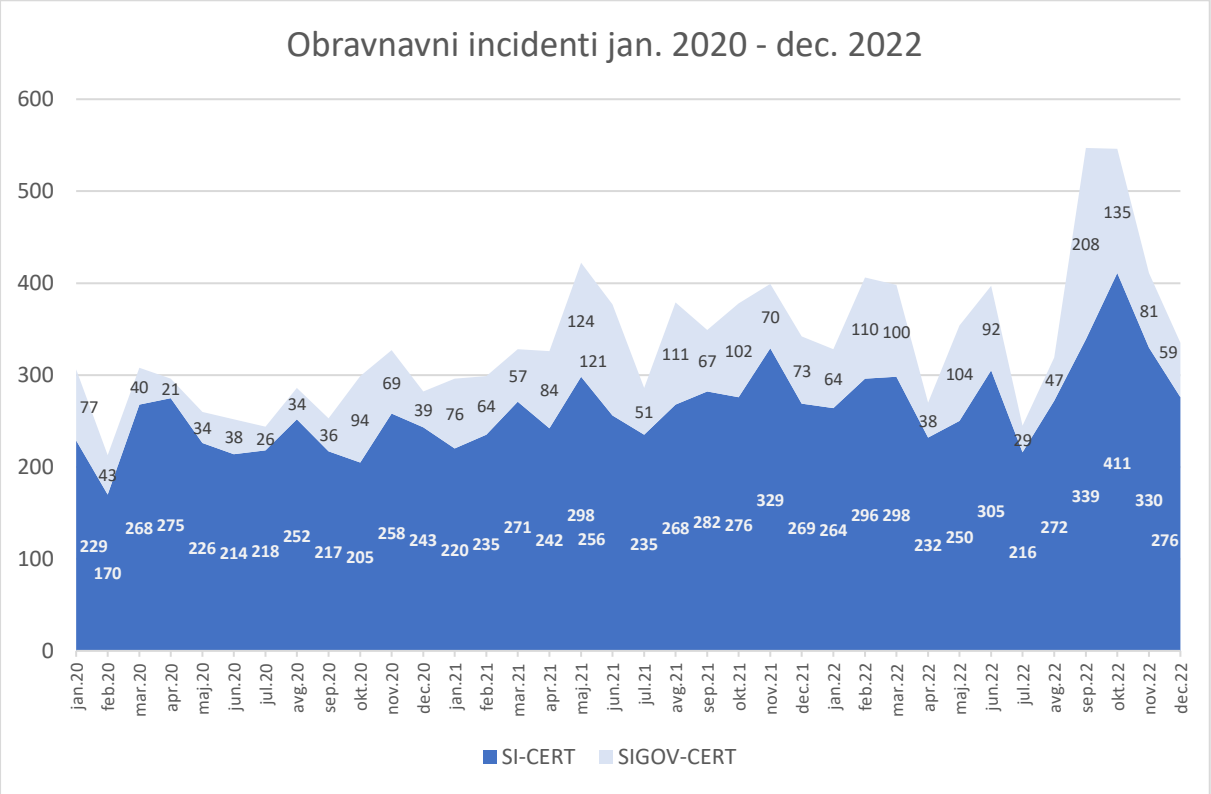
v poletnih mesecih. Povečalo se je števila incidentov povezanih s phishing sporočili in spletnimi mesti. Zaznali so rast števila poskusov, v katerih se storilci izdajajo za organe pregona, finančne ustanove, ponudnike informacijskih storitev ali distribucijska podjetja.

Statistika

V drugem polletju leta 2022 je bilo obravnavanih 2.403 incidentov. Vrh priglašenih incidentov predstavljata mesec september in oktober.

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**
Januar 2022	264	64	328
Februar 2022	296	110	406
Marec 2022	298	100	398
April 2022	232	38	270

Maj 2022	250	104	354
Junij 2022	305	92	397
SKUPAJ 1. polletje 2022	**1645**	**508**	**2153**
Julij 2022	216	29	245
Avgust 2022	272	47	319
September 2022	339	208	547
Oktober 2022	411	135	546
November 2022	330	81	411
December 2022	276	59	335
SKUPAJ 2. polletje 2022	**1844**	**559**	**2403**
SKUPAJ 2022	**3498**	**1067**	**4565**



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 predstavljenih podatkov ocenjujemo, da se bo nadaljevala izpostavljenost uporabnikov na phishing sporočila, ki postajajo vedno bolj sofisticirana. Zaradi konflikta v Ukrajini so že tako pomembni napadi na t.i. dobavno verigo dobili novo dimenzijo. Pri slednjih je potrebna hitra odzivnost vseh deležnikov, da se prepreči oz. omili morebitno oškodovanje. Zavezanci lahko pričakujejo povečano število skeniranj za izrabo potencialnih ranljivosti v sistemih.

Ocenjujemo, da 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, kažejo pozitivne rezultate pri zaznavanju in blažitvi vplivov incidentov na področju kibernetske varnosti. Prav tako se kažejo pozitivni učinki preventivnih aktivnosti v zvezi s procesom gostovanja informacijskih rešitev na Državnem računalniškem oblaku, ki vključuje varnostno preverjanje novih rešitev.

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 varnostne situacije na območju Ukrajine lahko pričakujmo okrepljene aktivnosti t.i. aktivističnih skupin kot tudi skupin podprtimi s strani držav udeleženih v konfliktu. Pričakujemo lahko porast števila priglašenih incidentov (phishing napadov, spletnih goljufij, porazdeljenih napadov onemogočanja na strežnik, ipd.)

Področje odzivanja na ranljivosti bo pomemben dejavnik tudi letu 2023. Zato moramo nadaljevati s sistematičnim pristopom in koordinirano obravnavo razkritih ranljivosti.

PREDLOGI IN PRIPOROČILA

Predlagamo ohranjanje visokega nivoja kibernetske varnosti IBS in organov državne uprave, upoštevanje priporočil, ki sta jih izdala URSIV in SI-CERT 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 in tudi zunanje izvajalce 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 video serijo KLIK in brezplačni tečaj Varni v pisarni.

Vsem odgovornim za upravljanje informacijskih sistemov in omrežij 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 zagotavljanju neprekinjenega poslovanja 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) in v primeru kakršnih koli anomalij ustrezno postopajo.

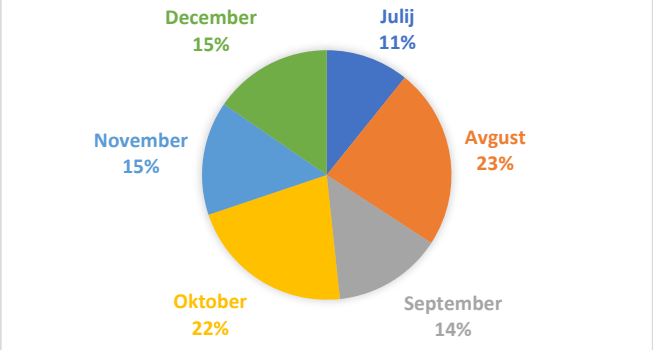
IBS in organe državne uprave opozarjamo na hranjenje dnevniških zapisov v zakonsko določenih časovnih okvirih (najmanj 6 mesecev). Prav tako priporočamo redno preverjanje kakovosti in ustreznosti varnostnih kopij in postopkov za obnovo.

PRILOGA 1

Podatki SI-CERT

1. Število novih incidentov

Mesec	Število incidentov
Julij	216
Avgust	272
September	339
Oktober	411
November	330
December	276
SKUPAJ	**1844**



Delež incidentov po mesecih

2. Stopnje incidentov

Oznaka	Stopnja	3. četrtletje	4. četrtletje	Skupaj
C1	Kritičen incident			
C2	Zelo pomemben incident			
C3	Pomemben incident	2	2	4
C4	Incident visoke stopnje	3	2	5
C5	Incident srednje stopnje	39	40	79
C6	Incident nizke stopnje	783	973	1756
SKUPAJ		**827**	**1017**	**1825**

3. Razdelitev po sektorjih

Skupina	Sektor	3. četrtletje	4. četrtletje	Skupaj
Ostalo	Fizična oseba	331	256	587
Ostalo	Druge pravne osebe	179	290	469
NIS	Bančništvo	126	220	346
Ostalo	Operaterji elektronskih komunikacij	81	83	164
Ostalo	Drugo	70	89	159
ZInfV	Organi državne uprave	8	38	46
Ostalo	Raziskovalno-izobraževalni sektor	17	25	42
NIS	Energija	7	2	9
NIS	Ponudniki spletne tržnice	3	6	9
NIS	Zdravstvo	4	3	7
NIS	Promet		3	3
NIS	Oskrba s pitno vodo in distribucija	1		1
NIS	Digitalna infrastruktura		1	1
NIS	Ponudniki računalništva v oblaku		1	1
SKUPAJ		**827**	**1017**	**1844**

4. Vrste in oznake novih incidentov

Kategorija	Vrsta	3. četrtletje	4. četrtletje	Skupaj
Goljufije	Phishing sporočilo	303	493	796
Goljufije	Druge goljufije	148	118	266
Goljufije	Phishing spletno mesto	44	88	132
Drugo	Drugo	53	67	120
Zlonamerna koda	Trojanski konj	54	66	120
Goljufije	Izsiljevanje	36	30	66
Vdor	Zloraba neprivilegiranega uporabniškega računa	25	26	51
Goljufije	Goljufija z vnaprejšnjim plačilom	36	8	44
Goljufije	Spletno nakupovanje	22	13	35
Neprimerna vsebina	Neželena sporočila	19	11	30
Ranljivosti	Razkritje ranljivosti	13	14	27
Goljufije	Kraja identitete	13	10	23
Zlonamerna koda	Izsiljevalski virus	12	11	23
Zbiranje informacij	Odkrivanje potencialnih tarč in ranljivosti (skeniranje)	3	18	21
Zlonamerna koda	Orodje za oddaljen nadzor (RAT)	13	5	18
Poskusi vdora	Poskusi prijav, bruteforce in napadi s slovarjem	4	7	11
Varnost informacijskih virov	Nepooblaščeno spreminjanje podatkov	4	5	9
Razpoložljivost	Porazdeljen napad onemogočanja	5	3	8
Neprimerna vsebina	Žaljiva vsebina	2	3	5
Ranljivosti	Ranljivi sistemi in naprave	1	4	5
Varnost informacijskih virov	Nepooblaščen dostop do podatkov	3	2	5
Goljufije	Nepooblaščeno izkoriščanje virov	3	1	4
Varnost informacijskih virov	Odtekanje informacij	1	3	4
Vdor	Napad na aplikacijo	2	1	3
Goljufije	Intelektualna lastnina in avtorske pravice	2	1	3
Zlonamerna koda	Virus		3	3
Zlonamerna koda	Boti in botneti	2		2
Razpoložljivost	Napad onemogočanja	2		2
Ranljivosti	Odgovorno razkrivanje	1	1	2
Zbiranje informacij	Socialni inženiring	1		1
Neprimerna vsebina	Nasilna vsebina		1	1
Zlonamerna koda	Nadzorni strežnik		1	1
Poskusi vdora	Izkoriščanje znane ranljivosti		1	1
Razpoložljivost	Izpad delovanja naprav ali omrežja		1	1
Test	Namenjeno testom		1	1
SKUPAJ		**827**	**1017**	**1844**

5. Neposredna finančna izguba prijavitelja v EUR

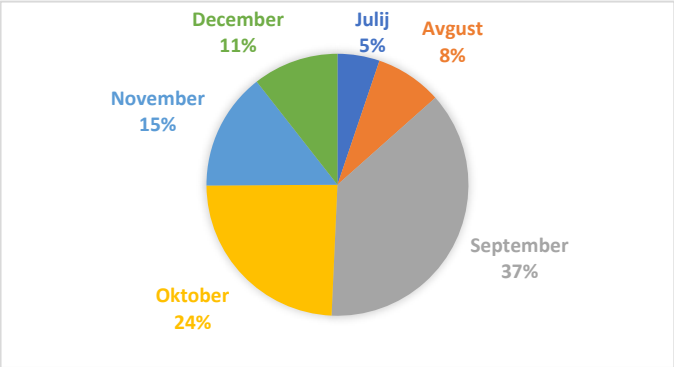
Kategorija	3. četrtletje	4. četrtletje	Skupaj
Goljufije z vnaprejšnjim plačilom	10.910,00	500.000,00	510.910,00
Druge goljufije	123.626,00	165.014,00	288.640,00
Zloraba neprivilegiranega uporabniškega računa	10,00	55.200,00	55.210,00
Phishing sporočilo	6.500,00	8.002,00	14.502,00
Izsiljevanje	1.540,00	100,00	1.640,00
Spletno nakupovanje	80,00	180,00	260,00
Trojanski konj	250,00		250,00
Phishing spletno mesto		150,00	150,00
Nepooblaščeno spreminjanje podatkov		86,00	86,00
SKUPAJ	**142.916,00**	**728.732,00**	**871.648,00**

PRILOGA 2

Podatki SIGOV-CERT

1. Število novih incidentov

Mesec	Število incidentov
Julij	29
Avgust	47
September	208
Oktober	135
November	81
December	59
SKUPAJ	**559**



Delež incidentov po mesecih

2. Stopnje incidentov

Oznaka	3. četrtletje	4. četrtletje	Skupaj
C1			
C2			
C3	1		1
C4			
C5	278	275	553
C6	5		5
SKUPAJ	**284**	**275**	**559**

3. Razdelitev po izvoru

Izvor	3. četrtletje	4. četrtletje	Skupaj
Osrednja državna uprava	283	271	554
Lokalna samouprava	1	4	5
SKUPAJ	**284**	**275**	**559**

4. Klasifikacija incidentov

Vrsta	3. četrtletje	4. četrtletje	Skupaj
Goljufije	177	77	254
Žaljiva/zlonamerna vsebina	84	94	178
Zbiranje informacij	4	78	82
Zlonamerna koda	13	5	18
Vdori/poizkusi vdora		9	9
Informacijska varnost	1		1
Drugo	5	12	17
SKUPAJ	**284**	**275**	**559**