REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE
ZA INFORMACIJSKO VARNOST

URSIV

Polletno poročilo o kibernetskih incidentih in napadih, 2022-1

September 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 **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.

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

Prvo polletje leta 2022, je bilo zaznamovano s kibernetskimi aktivnostmi povezanimi s konfliktom v Ukrajini. Glede na pretekla primerljiva obdobja je prva polovica leta 2022 na področju števila priglašenih incidentov postavila nov mejnik. 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 prva konferenca IBS ter izvedene kibernetske vaje (Locked Shields 2022, Cyber Europe 2022 in KIVA 2022).

Konflikt v Ukrajini

Napad Ruske federacije na Ukrajino 24. februarja 2022 se je odrazil tudi na področju kibernetskih incidentov. Splošno obvestilo o kibernetskih napadih, povezanih z vojno v Ukrajini, najdete na spletni strani SI-CERT (glej: https://www.cert.si/si-cert-2022-01/). Zapisali so, da vsi Evropski odzivni centri za kibernetsko varnost (CSIRT, *Computer Security Incident Response Team*), že od konca januarja 2022 spremljamo napade na omrežja in sisteme v Ukrajini.

Na podlagi poročil in informacij je ukrajinsko-ruski konflikt povzročil znatno povečanje uspešnih in učinkovitih kibernetskih napadov na države članice Evropske unije ter institucije, telesa in agencije Evropske unije. Zaznan je porast kibernetskega aktivizma (npr. aktivnosti skupine Killnet) in skeniranje omrežij za izrabo že znanih ranljivosti (npr. log4j). Prav tako so bili zabeleženi DDoS napadi in okrepljena Emotet kampanja. Tudi v Slovenije sta odzivan centra zaznala posvečano število priglašenih incidentov pred in po začetku konflikta.

MSDT Ranljivost (Microsoft Support Diagnostic Tool)

V začetku junija je bila odkrita kritična ranljivost z oznako CVE-2022-30190, ki v določenih primerih napadalcem omogoča izvedbo poljubne kode. Microsoft je 14. 6. 2022 izdal uradne popravke ranljivosti. Tipičen napad poteka na način, da napadalec žrtvi po elektronski pošti pošlje MS Office datoteko. Ta po odprtju preko ms-msdt sheme na sistem prenese dodatno kodo in jo izvede s pravicami prijavljenega uporabnika, kar ima lahko za posledico zlorabo celotnega sistema. V nekaterih primerih je za zagon škodljive kode v Office programih potrebno onemogočiti t. i. “Zaščiten pogled“, ki je privzeto omogočen za datoteke iz zunanjih virov, vendar pa ta način ne ščiti pred vsemi vektorji napada (npr. predogled RTF datoteke v Raziskovalcu) (glej https://www.cert.si/si-cert-2022-02/).

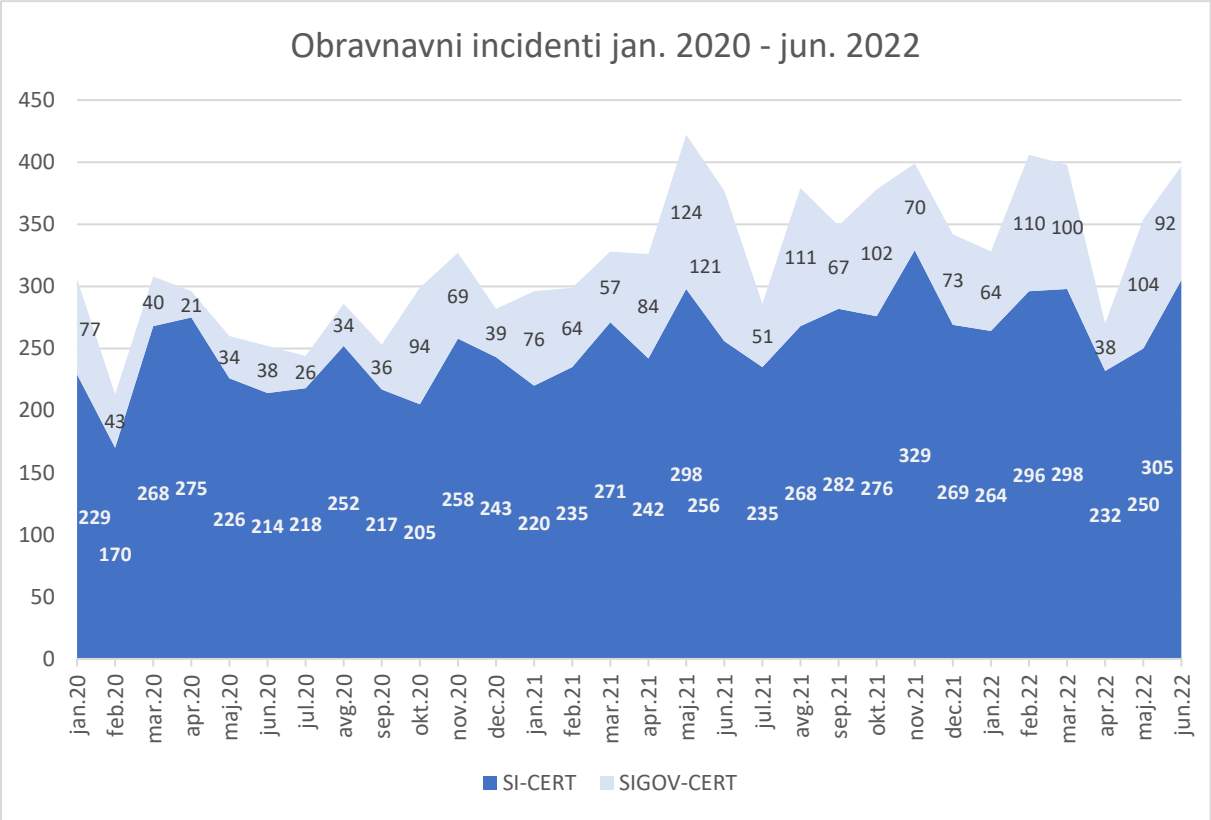
Phishing napadi ne pojenjajo

Iz podatkov, ki jih je posredoval SI-CERT, zaključujemo, da phishing napadi ne pojenjajo, saj še vedno predstavljajo večji delež med obravnavanimi incidenti. Gre za tehniko družbenega inženiringa, kjer se ustvari videz avtentičnosti sporočila in se naslovnika prelisiči v razkritje prijavnih podatkov ali številke kreditne kartice. Povečano število phishing sporočil, ki naj bi bilo posledica dogajanja v povezavi s konfliktom v Ukrajini, je zaznal tudi SIGOV-CERT.

Statistika

V prvem polletju leta 2022 je bilo obravnavanih **2153** incidentov.

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**



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. 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 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, kažejo 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 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 v letošnjem letu. 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 jih kje izdal URSIV 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 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.

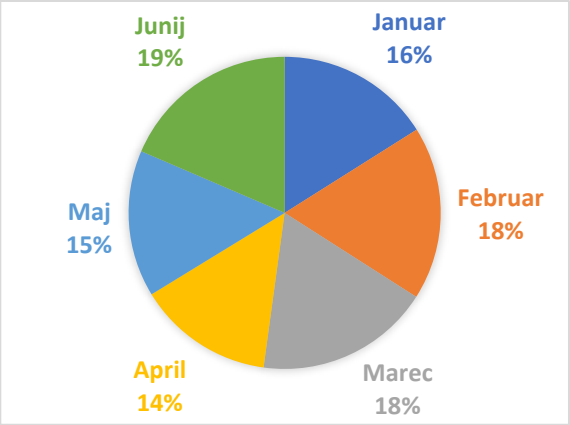
IBS in organe državne uprave opozarjamo na hranjenje dnevniških zapisov v zakonsko določenih časovnih okvirih (najmanj 6 mesecev). Prav tako priporočamo redno preverjanje kakovosti in ustreznosti varnostnih kopij in postopkov za obnovo. Posebno pozornost je potrebno še vedno nameniti zdravstvenem sistemu 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
Januar	264
Februar	296
Marec	298
April	232
Maj	250
Junij	305
SKUPAJ	**1645**



Delež incidentov po mesecih

Stopnje incidentov

Oznaka	Stopnja	1. četrtletje	2. četrtletje	Skupaj
C1	Kritičen incident	0	0	0
C2	Zelo pomemben incident	0	0	0
C3	Pomemben incident	1	0	1
C4	Incident visoke stopnje	2	3	5
C5	Incident srednje stopnje	52	41	93
C6	Incident nizke stopnje	802	743	1545
SKUPAJ		**857**	**787**	**1644**

*Opomba: * Incident C3 v 1. četrtletju je vadbeni incident v sklopu vaje Cyber Europe 2022.*

2. Razdelitev po sektorjih

Skupina	Sektor	1. četrtletje	2. četrtletje	Skupaj
NIS	Energija	3	1	4
NIS	Digitalna infrastruktura	1		1
NIS	Zdravstvo	3	2	5
NIS	Promet	4	2	6
NIS	Bančništvo	22	32	54
NIS	Preskrba s hrano		1	1
ZInfV	Organi državne uprave	14	11	25
Ostalo	Operaterji elektronskih komunikacij	10	4	14
Ostalo	Raziskovalno-izobraževalni sektor	27	32	59
Ostalo	Druge pravne osebe	157	169	326
Ostalo	Fizična oseba	579	474	1053
Ostalo	Drugo	37	59	96
SKUPAJ		**857**	**787**	**1644**

3. Vrste in oznake novih incidentov

Kategorija	Vrsta	1. četrtletje	2. četrtletje	Skupaj
Neprimerna vsebina	Neželena sporočila	25	31	56
Neprimerna vsebina	Žaljiva vsebina	3	1	4
Neprimerna vsebina	Nasilna vsebina			
Zlonamerna koda	Črv			
Zlonamerna koda	Virus	2	3	5
Zlonamerna koda	Trojanski konj	81	76	157
Zlonamerna koda	Rootkit			
Zlonamerna koda	Boti in botneti	5	1	6
Zlonamerna koda	Nadzorni strežnik			
Zlonamerna koda	Izsiljevalski virus	10	12	22
Zlonamerna koda	Orodje za oddaljen nadzor (RAT)	11	4	15
Zbiranje informacij	Odkrivanje potencialnih tarč in ranljivosti (skeniranje)	9	12	21
Zbiranje informacij	Prestrezanje komunikacije			
Zbiranje informacij	Socialni inženiring		2	2
Poskusi vdora	Izkoriščanje znane ranljivosti		2	2
Poskusi vdora	Poskusi prijav, bruteforce in napadi s slovarjem	3	4	7
Vdor	Zloraba privilegiranega uporabniškega računa			
Vdor	Zloraba neprivilegiranega uporabniškega računa	30	30	60
Vdor	Napad na aplikacijo	2	1	3
Razpoložljivost	Napad onemogočanja	1	2	3
Razpoložljivost	Porazdeljen napad onemogočanja	5	4	9
Razpoložljivost	Izpad delovanja naprav ali omrežja			
Varnost informacijskih virov	Nepooblaščen dostop do podatkov	2	1	3
Varnost informacijskih virov	Nepooblaščeno spreminjanje podatkov	1	5	6
Varnost informacijskih virov	Odtekanje informacij	1		1
Goljufije	Nepooblaščeno izkoriščanje virov	2		2
Goljufije	Intelektualna lastnina in avtorske pravice	5	3	8
Goljufije	Kraja identitete	15	8	23
Goljufije	Phishing sporočilo	216	206	422
Goljufije	Phishing spletno mesto	36	44	80
Goljufije	Spletno nakupovanje	20	14	34
Goljufije	Goljufija z vnaprejšnjim plačilom	36	34	70
Goljufije	Izsiljevanje	26	24	50

Kategorija	Vrsta	1. četrtletje	2. četrtletje	Skupaj
Goljufije	Druge goljufije	207	145	352
Ranljivosti	Odgovorno razkrivanje		2	2
Ranljivosti	Razkritje ranljivosti	10	14	24
Ranljivosti	Ranljivi sistemi in naprave	5	4	9
Drugo	Drugo	88	98	186
Test	Namenjeno testom			
SKUPAJ		**857**	**787**	**1644**

4. Neposredna finančna izguba prijavitelja v EUR

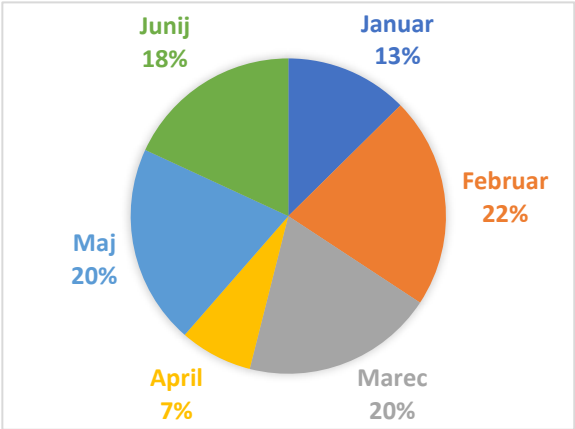
Kategorija	1. četrtletje	2. četrtletje	Skupaj
Druge goljufije	361.226,93	80.841,00	442.067,93
Goljufije z vnaprejšnjim plačilom	120.000,00	231.000,00	351.000,00
Phishing sporočilo	15.000,00		15.000,00
Spletno nakupovanje	5.725,00	170,00	5.895,00
Nepooblaščeno spreminjanje podatkov		2.596,00	2.596,00
Nepooblaščeno izkoriščanje virov	900,00		900,00
Zloraba neprivilegiranega uporabniškega računa	250,00		250,00
Izsiljevanje		100,00	100,00
SKUPAJ	**503.101,93**	**314.707,00**	**817.808,93**

PRILOGA 2

Podatki SIGOV-CERT

1. Število novih incidentov

Mesec	Število incidentov
Januar	64
Februar	110
Marec	100
April	38
Maj	104
Junij	92
SKUPAJ	**508**



Delež incidentov po mesecih

2. Stopnje incidentov

Oznaka	1. četrtletje	2. četrtletje	Skupaj
C1			
C2			
C3			
C4		1	1
C5	271	231	502
C6	3	2	5
SKUPAJ	**274**	**234**	**508**

3. Razdelitev po izvoru

Izvor	1. četrtletje	2. četrtletje	Skupaj
Osrednja državna uprava	273	230	503
Lokalna uprava	1	4	5
SKUPAJ	**274**	**234**	**508**

4. Klasifikacija incidentov

Vrsta	1. četrtletje	2. četrtletje	Skupaj
Goljufije	145	41	186
Informacijska varnost	2	12	14
Žaljiva/zlonamerna vsebina	57	97	154
Zbiranje informacij	22	7	29
Zlonamerna koda	46	67	113
Vdori/poizkusi vdora		1	1
Ranljivost		3	3
Drugo	2	6	8
SKUPAJ	**274**	**234**	**508**