**Polletno poročilo o kibernetskih incidentih in napadih, 2023-2**

**Februar 2024**

**O URSIV**

**Urad Vlade Republike Slovenije za informacijsko varnost** (URSIV) je pristojni nacionalni organ za informacijsko varnost v skladu z Zakonom o informacijski varnosti. Odgovoren je za vzpostavitev in delovanje nacionalnega sistema zagotavljanja informacijske in kibernetske varnosti v Republiki Sloveniji. 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, da pristojnemu nacionalnemu organu priglasi incidente zavezancev, to so izvajalci 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 (ODU)** **in povezanih subjektov** opravlja **SIGOV-CERT kot notranje organizacijska enota**  **URSIV.** ODU so organi, ki upravljajo informacijske sisteme in dele omrežja oziroma izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti. Povezani subjekti so državni organi, organi lokalnih skupnosti, javne agencije in nosilci javnih pooblastil ter drugi subjekti, ki niso organi državne uprave iz zgornje opredelitve ali izvajalci bistvenih storitev iz pristojnosti SI-CERT in se povezujejo s centralnim državnim informacijsko-komunikacijskim omrežjem oziroma sistemom.

**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, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23, 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 se je padec števila priglašenih incidentov v primerjavi z zadnjima dvema letoma nadaljeval. V tretjem četrtletju je med priglašenimi incidenti zaznano povečanje napadov usmerjenih zoper fizične osebe, ki ostajajo najpogostejša žrtev zlonamernih aktivnosti. Porast napadov, ki je bil opazen v tretjem četrtletju prejšnjega leta, se je proti koncu leta 2023 občutno zmanjšal. Po številu priglašenih kibernetskih incidentov ostaja bančništvo najbolj obremenjen sektor iz skupine subjektov, ki jih naslavlja Direktiva o ukrepih za visoko skupno raven kibernetske varnosti v EU (NIS). Najpogostejši tip napada ostaja spletno ribarjenje (ang. phishing). Med vdori pa je najpogostejša zloraba neprivilegiranega računa.

Najverjetnejši razlog za občutno zmanjšanje števila priglašenih incidentov je manjše število priglašenih poskusov spletnega ribarjenja ter drugih goljufij. To je lahko posledica večje kibernetske higiene med prebivalstvom in nepriglašanje lažnih elektronskih sporočil in poskusov goljufij, ki jih prejemniki prepoznajo, izbrišejo in ne priglasijo. Urad Vlade RS za informacijsko varnost in nacionalna skupina CSIRT sta izvedla več kampanj ozaveščanja o nevarnosti ter opozarjala splošno javnost na zlonamerne dejavnosti in uporabo goljufivih elektronskih sporočil ter spletnih mest.

Preteklo polletje je bilo, poleg kibernetskih aktivnosti povezanimi s konfliktom v Ukrajini, zaznamovano tudi z grožnjami, ki so se pojavile zaradi konflikta na Bližnjem vzhodu. URSIV je v sodelovanju z drugimi organi in mednarodnimi organizacijami pozorno spremljal situacijo na področju informacijske in kibernetske varnosti doma, v državah članicah Evropske unije ter na drugih vplivnih območjih. Skladno s tem je izvajal tudi redne koordinacijske aktivnosti na nacionalni ravni in s tem pripomogel k zagotavljanju informacijske in kibernetske varnosti v Republiki Sloveniji.

**INCIDENTI**

**Pomembna incidenta v državni upravi**

Varnostno operativni center Ministrstva za digitalno preobrazbo (VOC MDP) je obravnaval dva vdora v informacijski sistem in ju priglasil na URSIV. Vdor v sistem za obravnavanje certifikatov ADR vozil in tahografov tovornih vozil TAHOEV Ministrstva za infrastrukturo ter sistem VODE, ki ga upravlja Ministrstvo za naravne vire in prostor. Zadeva je bila prijavljena tudi na policijo. Izvedeni so bili ustrezni ukrepi za zamejitev dostopa. Oba kibernetska incidenta sta bila ocenjena s stopnjo C3.

**Kibernetski incident v podjetju HSE**

Novembra je bil zabeležen kibernetski incident v Holdingu Slovenske elektrarne d.o.o. (HSE), ki ga je podjetje prostovoljno priglasilo na SI-CERT. Incident je bil ocenjen s stopnjo C3. Po podatkih holdinga je prišlo do vdora v informacijski sistem v poslovnem delu. Po zagotovilih pristojnih proizvodnja električne energije v državi zaradi dogodka ni bila ogrožena. Opravljena je bila preiskava in analiza ter izvedeni ustrezni postopki zamejitve incidenta.

**Spletno ribarjenje (Phishing)**

Iz podatkov, zbranih s strani SI-CERT in SIGOV-CERT za tretje in četrto četrtletje, je razvidno, da se je število priglašenih incidentov zmanjšalo in je bilo najnižje odkar se vodi statistika incidentov v tej obliki. Kljub temu napadi spletnega ribarjenja še vedno ostajajo najpogostejše sredstvo za zlonameren dostop do sistemov in omrežij, ob tem pa se povečuje število usmerjenega spletnega ribarjenja (ang. spear phishing).

SI-CERT je v začetku drugega polletja zaznal večje število napadov prek telefona v obliki SMS sporočil (ang. smishing). Gre za ribarjenje ali phishing, kjer storilci želijo zvabiti žrtev v obisk lažnega spletnega mesta banke, pošte, dostavne službe, spletne prodajalne ali spletne pošte.

**Ranljivosti**

Skupini CSIRT sta v drugi polovici leta objavili več opozoril o zaznanih ranljivostih. Tako so julija opozorili na dve pomembnejši ranljivosti. Ranljivost produkta Citrix/NetScaler ADC in Gateway omogoča neavtenticiranemu uporabniku oddaljeno zaganjanje poljubne kode. Ranljivost produkta Ivanti Endpoint Manager Mobile (MobileIron) pa omogoča nepooblaščen dostop do administrativnega vmesnika API. V mesecu oktobru je bilo izdano varnostno opozorilo zaradi ranljivosti operacijskega sistema Cisco IOS XE.

Ponovno zaznavamo, da napadalci izkoriščajo znane ranljivosti programske opreme, ki že imajo popravke na voljo. Razlog lahko leži v nedoslednem vzdrževanju informacijskih sistemov oz. programske opreme ter nedoslednega nameščanja popravkov. Pojavljajo se tudi tako imenovani »pozabljeni strežniki«. Vzroki so lahko v preobremenjenosti vzdrževalcev, neustreznem obvladovanju informacijskih sistemov in tudi malomarnosti oz. neodgovornem ravnanju.

**Statistika**

V drugem polletju leta 2023 je bilo obravnavanih 1554 incidentov. Vrh polletnih priglasitev incidentov predstavlja mesec avgust. V oktobru smo zaznali občuten padec. Število priglašenih incidentov v mesecu decembru je najnižji mesečni rezultat v zabeleženem obdobju.

Tabela 1: Število incidentov v 2021, 2022 in 2023

|  |  |  |  |
| --- | --- | --- | --- |
| Mesec | SI-CERT | SIGOV-CERT | Skupaj |
| 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** |
| Januar 2023 | 265 | 94 | 359 |
| Februar 2023 | 217 | 38 | 255 |
| Marec 2023 | 221 | 75 | 296 |
| April 2023 | 162 | 43 | 205 |
| Maj 2023 | 192 | 109 | 301 |
| Junij 2023 | 149 | 108 | 257 |
| SKUPAJ 1. polletje 2023 | **1206** | **467** | **1673** |
| Julij 2023 | 219 | 99 | 318 |
| Avgust 2023 | 251 | 110 | 361 |
| September 2023 | 186 | 163 | 349 |
| Oktober 2023 | 124 | 78 | 202 |
| November 2023 | 105 | 95 | 200 |
| December 2023 | 66 | 58 | 124 |
| SKUPAJ 2. polletje 2023 | **951** | **603** | **1554** |
| SKUPAJ 2023 | **2157** | **1070** | **3227** |

Graf 1: Število obravnavanih incidentov od januarja 2021 do december 2023

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 različnim oblikam spletnega ribarjenja (ang. phishing). Vse pogostejše bo usmerjeno spletno ribarjenje (ang. spear phishing) proti pomembnejšim tarčam. Napadi z izsiljevalskimi virusi (ang. Ransomware) postajajo vedno bolj domiselni in sofisticirani. Zaradi konflikta v Ukrajini in na Bližnjem vzhodu so že tako pomembni napadi na t.i. dobavno verigo dobili novo dimenzijo. Pri slednjih je potrebna hitra odzivnost vseh deležnikov, da se prepreči oziroma omili morebitno oškodovanje. Zavezanci lahko pričakujejo povečano število skeniranj za izrabo potencialnih ranljivosti v sistemih.

Ocenjujemo, da sredstva vložena v preventivne dejavnosti ozaveščanja o varnosti na spletu (Varni na internetu, Safe.si) in program e-izobraževanja 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 bo v prihodnje kibernetski kriminal, postal ena izmed poglavitnih groženj za posameznike in poslovne procese 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). Posamezniki z izrazito željo po hitrem zaslužku ostajajo priljubljena tarča spletnih goljufov.

Zaradi poslabšanja varnostne situacije na območju Ukrajine in Bližnjega vzhoda ter v povezavi z novo vlogo Republike Slovenije v mednarodnih odnosih, ki je nastala z izvolitvijo za nestalno članico Varnostnega sveta Organizacije združenih narodov, lahko pričakujmo okrepljene aktivnosti t.i. aktivističnih skupin kot tudi skupin podprtih s strani držav udeleženih v konfliktu.

Področje odzivanja na ranljivosti bo pomemben dejavnik tudi v prvem polletju 2024. V ta namen moramo nadaljevati s sistematičnim pristopom in koordinirano obravnavo razkritih ranljivosti.

**PREDLOGI IN PRIPOROČILA**

Predlagamo izvajanje aktivnosti za ohranjanje visokega nivoja kibernetske varnosti pri IBS in ODU, upoštevanje priporočil izdanih s strani URSIV, SIGOV-CERT in SI-CERT ter dosledno izpolnjevanje naloženih ukrepov za odpravo nepravilnosti in podanih priporočil, ki jih izda Inšpekcija za informacijsko varnost.

Predlagamo, da spremljate oziroma vaše sodelavce in tudi zunanje izvajalce opozorite na objave projekta Varni na internetu, ki ga izvaja SI-CERT ([https://www.varninainternetu.si/)](https://www.varninainternetu.si/%29%20) 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/](http://www.safe.si/)). SI-CERT je pripravil video serijo [KLIK](https://www.youtube.com/playlist?list=PLUVdjpfSn3X-dwd_g6HI-cFC5eu0Xb2yF) in brezplačni tečaj [Varni v pisarni](https://www.varnivpisarni.si/).

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;
* vključijo uporabo večfaktorske avtentikacije.

IBS, ODU, ponudnikom digitalnih storitev in povezanim subjektom ter ostalim podjetjem in ustanovam priporočamo, da:

* dosledno skrbijo za ustrezen nivo varnostnega zavedanja zaposlenih in osnovne prakse kibernetske higiene ter izvajajo primerne aktivnosti za preprečitev notranjih groženj;
* 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 zagotavljanje 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.

PRILOGA 1

**Podatki SI-CERT**

1. **Tabela 2: Število novih incidentov**

|  |  |
| --- | --- |
| Mesec | Število incidentov |
| Julij | 219 |
| Avgust | 251 |
| September | 186 |
| Oktober | 124 |
| November | 105 |
| December | 66 |
| SKUPAJ | **951** |

Delež incidentov po mesecih

1. **Tabela 3: Stopnje incidentov**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Oznaka | Stopnja | 3. četrtletje | 4. četrtletje | Skupaj |
| C1 | Kritičen incident |  |  |  |
| C2 | Zelo pomemben incident |  |  |  |
| C3 | Pomemben incident |  | 1 | 1 |
| C4 | Incident visoke stopnje | 1 | 8 | 9 |
| C5 | Incident srednje stopnje | 2 | 2 | 4 |
| C6 | Incident nizke stopnje | 653 | 284 | 937 |
| SKUPAJ | **656** | **295** | **951** |

1. **Tabela 4: Razdelitev po sektorjih**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Skupina | Sektor | 3. četrtletje | 4. četrtletje | Skupaj |
| Ostalo | Fizična oseba | 301 | 89 | 390 |
| Ostalo | Druge pravne osebe | 178 | 110 | 288 |
| NIS | Bančništvo | 96 | 12 | 108 |
| Ostalo | Raziskovalno-izobraževalni sektor | 33 | 25 | 58 |
| Ostalo | Drugo | 17 | 25 | 42 |
| ZInfV | Organi državne uprave | 10 | 13 | 23 |
| Ostalo | Operaterji elektronskih komunikacij | 9 | 3 | 12 |
| NIS | Zdravstvo | 3 | 4 | 7 |
| NIS | Promet | 4 | 2 | 6 |
| NIS | Energija | 4 | 10 | 14 |
| NIS | Digitalna infrastruktura | 1 | 1 | 2 |
| NIS | Ponudniki spletne tržnice | 0 | 0 | 0 |
| NIS | Oskrba s pitno vodo in distribucija | 0 | 1 | 1 |
| NIS | Ponudniki računalništva v oblaku | 0 | 0 | 0 |
| SKUPAJ | **656** | **295** | **951** |

1. **Tabela 5: Vrste in oznake novih incidentov**

| Kategorija | Vrsta | 3. četrtletje | 4. četrtletje | Skupaj |
| --- | --- | --- | --- | --- |
| Goljufije | Phishing sporočilo | 376 | 66 | 442 |
| Goljufije | Druge goljufije | 55 | 22 | 77 |
| Drugo | Drugo | 29 | 39 | 68 |
| Zlonamerna koda | Trojanski konj | 50 | 36 | 86 |
| Vdor | Zloraba neprivilegiranega uporabniškega računa | 33 | 36 | 69 |
| Goljufije | Spletno nakupovanje | 14 | 5 | 19 |
| Goljufije | Izsiljevanje | 12 | 6 | 18 |
| Goljufije | Kraja identitete | 6 | 1 | 7 |
| Goljufije | Phishing spletno mesto | 7 | 9 | 16 |
| Poskusi vdora | Poskusi prijav, bruteforce in napadi s slovarjem | 4 | 1 | 5 |
| Neprimerna vsebina | Neželena sporočila | 5 | 4 | 9 |
| Zlonamerna koda | Izsiljevalski virus | 6 | 10 | 16 |
| Goljufije | Goljufija z vnaprejšnjim plačilom | 4 | 1 | 5 |
| Ranljivosti | Razkritje ranljivosti | 8 | 3 | 11 |
| Zbiranje informacij | Odkrivanje potencialnih tarč in ranljivosti (skeniranje) | 2 | 10 | 12 |
| Varnost informacijskih virov | Nepooblaščeno spreminjanje podatkov | 3 | 7 | 10 |
| Razpoložljivost | Porazdeljen napad onemogočanja | 9 | 4 | 13 |
| Zlonamerna koda | Orodje za oddaljen nadzor (RAT) | 12 | 4 | 16 |
| Zlonamerna koda | Virus | 1 | 2 | 3 |
| Vdor | Napad na aplikacijo | 3 | 3 | 6 |
| Ranljivosti | Odgovorno razkrivanje | 2 | 3 | 5 |
| Varnost informacijskih virov | Odtekanje informacij | 1 | 0 | 1 |
| Goljufije | Nepooblaščeno izkoriščanje virov | 1 | 3 | 4 |
| Ranljivosti | Ranljivi sistemi in naprave | 6 | 4 | 10 |
| Razpoložljivost | Napad onemogočanja | 0 | 2 | 2 |
| Razpoložljivost | Izpad delovanja naprav ali omrežja | 0 | 4 | 4 |
| Poskusi vdora | Izkoriščanje znane ranljivosti | 1 | 2 | 3 |
| Goljufije | Intelektualna lastnina in avtorske pravice | 0 | 0 | 0 |
| Neprimerna vsebina | Žaljiva vsebina | 4 | 0 | 4 |
| Zlonamerna koda | Boti in botneti | 1 | 2 | 3 |
| Zlonamerna koda | Črv | 1 | 1 | 2 |
| Vdor | Zloraba privilegiranega uporabniškega računa | 0 | 2 | 2 |
| Razpoložljivost | Sabotaža | 0 | 0 | 0 |
| Zlonamerna koda | Dialler | 0 | 0 | 0 |
| Zlonamerna koda | Rootkit | 0 | 0 | 0 |
| Zbiranje informacij | Prestrezanje komunikacije | 0 | 0 | 0 |
| Varnost informacijskih virov | Nepooblaščen dostop do podatkov | 0 | 3 | 3 |
| Zbiranje informacij | Socialni inženiring | 0 | 0 | 0 |
| Neprimerna vsebina | Nasilna vsebina | 0 | 0 | 0 |
| Zlonamerna koda | Nadzorni strežnik | 0 | 0 | 0 |
| Test | Namenjeno testom | 0 | 0 | 0 |
| SKUPAJ | **656** | **295** | **951** |

1. **Tabela 6: Neposredna finančna izguba prijavitelja v EUR**

|  |  |  |  |
| --- | --- | --- | --- |
| Kategorija | 3. četrtletje | 4. četrtletje | Skupaj |
| Druge goljufije | 59.017,00 | 127.684,00 | 186.701,00 |
| Nepooblaščeno spreminjanje podatkov |  |  | 0,00 |
| Goljufije z vnaprejšnjim plačilom | 4.769,00 | 0 | 4.769,00 |
| Zloraba neprivilegiranega uporabniškega računa | 44.000,00 | 110.766,00 | 154.766,00 |
| Napad na aplikacijo |  |  | 0,00 |
| Trojanski konj | 4.500,00 |  | 4.500,00 |
| Phishing sporočilo | 7.782,00 | 28.571,00 | 36.353,00 |
| Phishing spletno mesto | 25.000,00 |  | 25.000,00 |
| Izsiljevanje | 8.000,00 |  | 8.000,00 |
| Spletno nakupovanje | 292,00 | 2.510,00 | 2.802,00 |
| SKUPAJ | **153.360,00** | **269.531,00** | **422.891,00** |

**PRILOGA 2**

**Podatki SIGOV-CERT**

1. **Tabela 7: Število novih incidentov**

|  |  |
| --- | --- |
| Mesec | Število incidentov |
| Julij | 99 |
| Avgust | 110 |
| September | 163 |
| Oktober | 78 |
| November | 95 |
| December | 58 |
| SKUPAJ | **603** |

Delež incidentov po mesecih

1. **Tabela 8: Stopnje incidentov**

|  |  |  |  |
| --- | --- | --- | --- |
| Oznaka | 3. četrtletje | 4. četrtletje | Skupaj |
| C1 |  |  |  |
| C2 |  |  |  |
| C3 |  | 2 | 2 |
| C4 |  | 1 | 1 |
| C5 | 227 | 373 | 600 |
| C6 |  |  |  |
| SKUPAJ | 227 | 376 | 603 |

1. **Tabela 9: Razdelitev po izvoru**

|  |  |  |  |
| --- | --- | --- | --- |
| Izvor | 3. četrtletje | 4. četrtletje | Skupaj |
| Osrednja državna uprava | 220 | 372 | 591 |
| Lokalna samouprava | 7 | 4 | 11 |
| SKUPAJ | **227** | **376** | **603** |

1. **Tabela 10: Klasifikacija incidentov**

| Vrsta | 3. četrtletje | 4. četrtletje | Skupaj |
| --- | --- | --- | --- |
| Žaljiva/zlonamerna vsebina | 32 | 73 | 105 |
| Goljufije | 122 | 208 | 330 |
| Zbiranje informacij | 57 | 29 | 86 |
| Informacijska varnost | 6 | 1 | 7 |
| Vdori/poizkusi vdora | 0 | 7 | 7 |
| Zlonamerna koda | 1 | 6 | 7 |
| Drugo | 9 | 52 | 61 |
| SKUPAJ | **227** | **376** | **603** |