**Polletno poročilo o kibernetskih incidentih in napadih, 2023-1**

**Avgust 2023**

**O URSIV**

**Urad Vlade Republike Slovenije za informacijsko varnost** (URSIV) je pristojni nacionalni organ za informacijsko varnost, ki od 31. julija 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 (ODU)** opravlja **SIGOV-CERT** v okviru **URSIV.** Odzivni center je pristojen za priglasitev incidentov ODU, 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 digitalno preobrazbo, 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, 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 prvem polletju je zaznan padec števila priglašenih incidentov glede na stanje iz leta 2020. V primerjavi z omenjenim letom je med priglašenimi incidenti manj napadov usmerjenih zoper fizične osebe, ki pa so še vedno najpogostejša tarča napadov. Opazen porast napadov v bančnem sektorju iz zadnjega četrtletja prejšnjega leta se je zmanjšal. Najpogostejši tip napada ostaja spletno ribarjenje (phishing). Med vdori pa je najpogostejša zloraba neprivilegiranega računa.

Tudi preteklo polletje, je bilo zaznamovano s kibernetskimi aktivnostmi povezanimi s konfliktom v Ukrajini. URSIV v sodelovanju z drugimi organi in organizacijami pozorno spremlja situacijo na področju kibernetske varnosti doma, v državah članicah Evropske unije in v 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.

Zabeležen je bil kibernetski napad na Ministrstvo za zunanje in evropske zadeve (MZEZ). Po podatkih ministrstva delovanje ni bilo moteno. Zlonamerno aktivnost so odkrili sami v sodelovanju s partnerji. Izvedli so temeljito preiskavo ter sprožili ustrezne ukrepe. Napad naj bi bil posledica dejanja tretje države.

V prvem polletju 2023 so bile izvedene aktivnosti za dvig odpornosti kibernetskega sistema. Organizirana je bila tretja konferenca IBS ter prva konferenca ODU. Izvajajo se aktivnosti za implementacijo EU direktive 2022/2555 (NIS 2), katere namen je razvoj zmogljivosti za kibernetsko varnost po vsej Uniji, ublažitev groženj za omrežja in informacijske sisteme, ki se uporabljajo za opravljanje bistvenih storitev v ključnih sektorjih, ter zagotovitvi neprekinjenega izvajanja takih storitev pri spoprijemanju z incidenti.

**Konflikt v Ukrajini**

Agresija Ruske federacije tudi v prvem polletju 2023 vpliva na področje kibernetske varnosti v Republiki Sloveniji in na območju EU. Na področju priglašenih kibernetskih incidentov se rast, zaznana v drugem polletju 2022, postopoma umirja. Ostaja nad letnim povprečjem zabeleženim pred spremembo varnostne situacije. Poleg že znanih t.i. hektivističnih skupin se pojavljajo nove. Aktivno se nadaljuje skeniranje omrežij za izrabo že znanih ranljivosti in spletno ribarjenje z namenom pridobitve dostopov do ključnih informacijskih sistemov v mednarodnih organizacijah ter v sisteme izvajalcev bistvenih storitev držav članic EU. Najpogostejši način delovanja še vedno ostajajo DDoS napadi.

**Ranljivosti**

SI-CERT je v prvi polovici leta objavil več opozoril o zaznanih ranljivostih. Tako so marca opozorili na dve pomembnejši ranljivosti. Objavil je novico o uhajanju NTLM poverilnic preko Outlook ranljivosti. Microsoft je izrabo ranljivosti zaznal v omejenem številu napadov na organizacije iz vladnega, energetskega in vojaškega sektorja v Evropi, izvedbo napadov pa pripisuje napadalcem iz Rusije.

Konec meseca marca pa je objavil novico o zlorabi dobavne verige: 3CX aplikacija. Podjetje 3CX je izdalo varnostno opozorilo za aplikacijo 3CX Electron DesktopApp. Gre za zlorabo dobavne verige, natančneje pa gre v tem primeru za namestitev škodljive programske kode – trojanskega konja tipa “information stealer” – s pomočjo uradnih, digitalno podpisanih namestitvenih paketov za omenjeno aplikacijo.

Fortinet je 12. junija 2023 izdal obvestilo o ranljivosti CVE-2023-27997, ki neavtenticiranemu uporabniku omogoča oddaljeno zaganjanje poljubne kode. Ranljivost odpravlja posodobitev na zadnjo različico veje. Ranljivost naj bi se že izrabljala v posameznih napadih.

Ponovno se zapaža, 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 zaradi ne 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.

**Kibernetski napad na MZEZ**

Ministrstvo za zunanje in evropske zadeve (MZEZ) je dne 7. aprila 2023 seznanila javnost da so bili tarča kibernetskega napada. Kot so sporočili, so v prvi fazi izvajali varnostne ukrepe in ocenjevali razsežnosti ter posledice dejavnosti. Delovanje ministrstva pa ni bilo moteno. Podali so pojasnilo, da so dejavnosti odkrili sami v sodelovanju s partnerji. Vzporedno s temeljito preiskavo so sprožili ustrezne ukrepe. Ministrica za zunanje zadeve je dejala, da gre za kibernetski napad iz tretje države, ki očitno traja že dalj časa. Po njenih besedah so bila napadena zunanja ministrstva in diplomatske mreže večine članic Evropske unije.

**Spletno ribarjenje (Phishing)**

Iz podatkov SI-CERT in SIGOV-CERT je razvidno, da se je število incidentov, ki so bili obravnavani v prvem in drugem četrtletju, vidno zmanjšalo. Podatki za prvo polletje so se spustili pod raven iz leta 2020. Tovrstni napadi še vedno ostajajo najpogostejše sredstvo za zlonameren dostop do sistemov in omrežij. Pojavlja se večje število usmerjenega spletnega ribarjenja (spear phishing).

SI-CERT je opozoril na pojav Smishing napadov. Gre za ribarjenje ali phishing, kjer storilci želijo zvabiti žrtev v obisk lažnega spletnega mesta banke, pošte, spletne prodajalne ali spletne pošte. Spletno mesto zahteva vpis uporabniškega imena in gesla, iz razloga posodobitve podatkov. Na ta način pa žrtev svoje geslo pošlje goljufom. Če je takšno sporočila poslano v SMS sporočilih gre za tako imenovani smishing.

**Statistika**

V prvem polletju leta 2023 je bilo obravnavanih 1.673 incidentov. Vrh polletnih priglašenih incidentov predstavlja mesec januar. V aprilu smo zaznali občuten padec priglašenih incidentov. Gre za najnižji mesečni rezultat v beleženem obdobju.

Tabela 1: Število incidentov v 2020, 2021, 2022 in prvem polletju 2023

|  |  |  |  |
| --- | --- | --- | --- |
| 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** |
| 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** |

Graf 1: Število obravnavanih incidentov od januarja 2020 do junija 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 phishing napadov. Vse pogostejši bodo spear phishing napadi usmerjeni proti pomembnejšim tarčam. Ransomware napadi postajajo vedno bolj domiselni in sofisticirani. 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 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) 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. Število potencialnih žrtev se je po katastrofalnih poplavah avgusta pričakovano povečala. Ljudje v stiski so bolj dovzetni za različne oblike goljufij.

Ob poslabšanju varnostne situacije na območju Ukrajine 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. Pričakujemo lahko porast števila priglašenih incidentov (phishing napadov, spletnih goljufij, porazdeljenih napadov onemogočanja strežnikov, ipd.)

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

**PREDLOGI IN PRIPOROČILA**

Predlagamo ohranjanje visokega nivoja kibernetske varnosti pri IBS in ODU, upoštevanje priporočil izdanih s strani URSIV in SI-CERT ter dosledno izpolnjevanje naloženih ukrepov za odpravo nepravilnosti in podanih priporočil, ki jih izda 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/](file:///%5C%5Cad.sigov.si%5CDAT%5CUIV%5CURSIV%5CPlani_porocila%5CPolletna%20poro%C4%8Dila%20po%20ZInfV%5CPoro%C4%8Dilo2_2021%5Cwww.varninainternetu.si%5C)) 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 in ponudnikom digitalnih storitev 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.

IBS, ODU in povezane subjekte opozarjamo na hranjenje dnevniških zapisov v zakonsko določenih časovnih okvirih (najmanj 6 mesecev). Pri tem opozarjamo, da so bile z Zakonom o spremembah in dopolnitvah Zakona o informacijski varnosti (ZInfV-B) objavljenim 28. aprila 2023 v Uradnem listu RS uveljavljene spremembe in sicer je omogočeno hranjenje tudi za daljše obdobje, kadar iz analize obvladovanja tveganj in ocene sprejemljive ravni tveganj izhaja, da bi bilo tveganja ustrezno obvladovati z daljšo hrambo dnevniških zapisov. Prav tako priporočamo redno preverjanje kakovosti in ustreznosti varnostnih kopij in postopkov za obnovo.

**PRILOGA 1**

**Podatki SI-CERT**

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

|  |  |
| --- | --- |
| Mesec | Število incidentov |
| Januar | 265 |
| Februar | 217 |
| Marec | 221 |
| April | 162 |
| Maj | 192 |
| Junij | 149 |
| SKUPAJ | **1206** |

Delež incidentov po mesecih

1. **Tabela 3: Stopnje incidentov**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Oznaka | Stopnja | 1. četrtletje | 2. četrtletje | Skupaj |
| C1 | Kritičen incident |  |  |  |
| C2 | Zelo pomemben incident |  |  |  |
| C3 | Pomemben incident |  |  |  |
| C4 | Incident visoke stopnje | 5 | 5 | 10 |
| C5 | Incident srednje stopnje | 4 | 2 | 6 |
| C6 | Incident nizke stopnje | 694 | 496 | 1190 |
| SKUPAJ | **703**  | **503** | **1206** |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Skupina | Sektor | 1. četrtletje | 2. četrtletje | Skupaj |
| Ostalo | Fizična oseba | 264 | 243 | 507 |
| Ostalo | Druge pravne osebe | 180 | 139 | 319 |
| NIS | Bančništvo | 129 | 34 | 163 |
| Ostalo | Raziskovalno-izobraževalni sektor | 28 | 31 | 59 |
| Ostalo | Drugo | 26 | 20 | 46 |
| ZInfV | Organi državne uprave | 28 | 8 | 36 |
| Ostalo | Operaterji elektronskih komunikacij | 21 | 8 | 29 |
| NIS | Zdravstvo | 9 | 6 | 15 |
| NIS | Promet | 7 | 7 | 14 |
| NIS | Energija | 1 | 5 | 6 |
| NIS | Digitalna infrastruktura | 1 | 2 | 3 |
| NIS | Ponudniki spletne tržnice | 6 |  | 6 |
| NIS | Oskrba s pitno vodo in distribucija | 1 |  | 1 |
| NIS | Ponudniki računalništva v oblaku | 2 |  | 2 |
| SKUPAJ | **703** | **503** | **1206** |

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

| Kategorija | Vrsta | 1. četrtletje | 2. četrtletje | Skupaj |
| --- | --- | --- | --- | --- |
| Goljufije | Phishing sporočilo | 367 | 261 | 628 |
| Goljufije | Druge goljufije | 71 | 36 | 107 |
| Drugo | Drugo | 56 | 40 | 96 |
| Zlonamerna koda | Trojanski konj | 26 | 31 | 57 |
| Vdor | Zloraba neprivilegiranega uporabniškega računa | 22 | 24 | 46 |
| Goljufije | Spletno nakupovanje | 19 | 14 | 33 |
| Goljufije | Izsiljevanje | 20 | 13 | 33 |
| Goljufije | Kraja identitete | 17 | 12 | 29 |
| Goljufije | Phishing spletno mesto | 18 | 11 | 29 |
| Poskusi vdora | Poskusi prijav, bruteforce in napadi s slovarjem | 11 | 8 | 19 |
| Neprimerna vsebina | Neželena sporočila | 14 | 5 | 19 |
| Zlonamerna koda | Izsiljevalski virus | 12 | 4 | 16 |
| Goljufije | Goljufija z vnaprejšnjim plačilom | 4 | 7 | 11 |
| Ranljivosti | Razkritje ranljivosti | 5 | 4 | 9 |
| Zbiranje informacij | Odkrivanje potencialnih tarč in ranljivosti (skeniranje) | 5 | 4 | 9 |
| Varnost informacijskih virov | Nepooblaščeno spreminjanje podatkov | 3 | 5 | 8 |
| Razpoložljivost | Porazdeljen napad onemogočanja | 7 | 1 | 8 |
| Zlonamerna koda | Orodje za oddaljen nadzor (RAT) | 3 | 3 | 6 |
| Zlonamerna koda | Virus | 1 | 4 | 5 |
| Vdor | Napad na aplikacijo | 2 | 3 | 5 |
| Ranljivosti | Odgovorno razkrivanje | 2 | 2 | 4 |
| Varnost informacijskih virov | Odtekanje informacij | 3 | 1 | 4 |
| Goljufije | Nepooblaščeno izkoriščanje virov | 4 |  | 4 |
| Ranljivosti | Ranljivi sistemi in naprave | 1 | 2 | 3 |
| Razpoložljivost | Napad onemogočanja | 2 | 1 | 3 |
| Razpoložljivost | Izpad delovanja naprav ali omrežja | 2 | 1 | 3 |
| Poskusi vdora | Izkoriščanje znane ranljivosti | 1 | 1 | 2 |
| Goljufije | Intelektualna lastnina in avtorske pravice | 1 | 1 | 2 |
| Neprimerna vsebina | Žaljiva vsebina | 2 |  | 2 |
| Zlonamerna koda | Boti in botneti |  | 1 | 1 |
| Vdor | Zloraba privilegiranega uporabniškega računa |  | 1 | 1 |
| Razpoložljivost | Sabotaža |  | 1 | 1 |
| Zlonamerna koda | Dialler |  | 1 | 1 |
| Zlonamerna koda | Rootkit | 1 |  | 1 |
| Zbiranje informacij | Prestrezanje komunikacije | **1** |  | 1 |
| Varnost informacijskih virov | Nepooblaščen dostop do podatkov |  |  | 0 |
| Zbiranje informacij | Socialni inženiring |  |  | 0 |
| Neprimerna vsebina | Nasilna vsebina |  |  | 0 |
| Zlonamerna koda | Nadzorni strežnik |  |  | 0 |
| Test | Namenjeno testom |  |  | 0 |
| SKUPAJ | **703** | **503** | **1206** |

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

|  |  |  |  |
| --- | --- | --- | --- |
| Kategorija | 1. četrtletje | 2. četrtletje | Skupaj |
| Druge goljufije | 206.293,00 | 16.670,00 | 222.963,00 |
| Nepooblaščeno spreminjanje podatkov | 3.712,00 | 18.097,00 | 21.809,00 |
| Goljufije z vnaprejšnjim plačilom |  | 10.000,00 | 10.000,00 |
| Zloraba neprivilegiranega uporabniškega računa | 7.000,00 | 3.000,00 | 10.000,00 |
| Napad na aplikacijo | 145,00 | 6.200,00 | 6.345,00 |
| Phishing sporočilo | 1.111,00 | 3.993,00 | 5.104,00 |
| Spletno nakupovanje | 675,00 | 220,00 | 895,00 |
| SKUPAJ | **218.936,00** | **58.180,00** | **277.116,00** |

**PRILOGA 2**

**Podatki SIGOV-CERT**

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

|  |  |
| --- | --- |
| Mesec | Število incidentov |
| Januar | 94 |
| Februar | 38 |
| Marec | 75 |
| April | 43 |
| Maj | 109 |
| Junij | 108 |
| SKUPAJ | **467** |

Delež incidentov po mesecih

1. **Tabela 8: Stopnje incidentov**

|  |  |  |  |
| --- | --- | --- | --- |
| Oznaka | 1. četrtletje | 2. četrtletje | Skupaj |
| C1 |  |  |  |
| C2 |  | 1 | 1 |
| C3 |  |  |  |
| C4 |  |  |  |
| C5 | 207 | 259 | 466 |
| C6 |  |  |  |
| SKUPAJ | **207** | **260** | **467** |

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

|  |  |  |  |
| --- | --- | --- | --- |
| Izvor | 1. četrtletje | 2. četrtletje | Skupaj |
| Osrednja državna uprava | 204 | 260 | 464 |
| Lokalna samouprava | 3 | 0 | 3 |
| SKUPAJ | **207** | **260** | **467** |

1. **Tabela 10: Klasifikacija incidentov**

| Vrsta | 1. četrtletje | 2. četrtletje | Skupaj |
| --- | --- | --- | --- |
| Žaljiva/zlonamerna vsebina | 84 | 129 | 213 |
| Goljufije | 101 | 70 | 171 |
| Zbiranje informacij | 5 | 51 | 56 |
| Informacijska varnost | 8 | 3 | 11 |
| Vdori/poizkusi vdora | 5 | 4 | 9 |
| Zlonamerna koda | 3 |  | 3 |
| Drugo | 1 | 3 | 4 |
| SKUPAJ | **207** | **260** | **467** |