

Polletno poročilo o kibernetičkih incidentih in napadih

Avgust 2021

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

Šmartinska cesta 152, 1000 Ljubljana

Telefon: (01) 478 47 78

E-naslov: gp.uiv@gov.si

Spletna stran: www.uiv.gov.si

Twitter: [@URSIV_Slovenia](https://twitter.com/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 prigrasiteljem pri obvladovanju incidentov.

Naloge nacionalnega odzivnega centra za kibernetičko 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 prigrasitev 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](https://twitter.com/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](#)

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 kibernetičnih 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 kibernetičnih 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. Razglašeno je bilo stanje povečane ogroženosti varnosti omrežij in informacijskih sistemov zavezancev po Zakonu o informacijski varnosti. Velja tudi opozoriti na nedelovanje Pravno-informacijskega sistema Republike Slovenije, maj 2021, ki je povzročil nezmožnost uporabe storitve širšemu krogu uporabnikov.

Kritične ranljivosti Microsoft Exchange strežnikov

Podjetje Microsoft je 3. marca 2021 zjutraj (po srednjeevropskem času) objavilo, da v njihovem izdelku Microsoft Exchange Server, enemu od najbolj razširjenih strežnikov za elektronsko pošto, vodenje koledarjev in stikov ter sodelovanje, obstaja več kritičnih ranljivosti. SI-CERT je 3. marca 2021 objavil varnostno obvestilo SI-CERT 2021-016 v katerem je opisal ranljivosti Microsoft Exchange strežnikov ter podal preventivne ukrepe, ki se nanašajo na namestitev popravkov, pregled indikatorjev zlorabe in ukrepe pri zaznani zlorabi. O ranljivosti so bili takoj obveščeni vsi IBS. Temu je sledil pregled slovenskega internet prostora z namenom identifikacije ranljivih strežnikov, sporočila o ranljivosti in ustreznih ukrepih. Na podlagi preliminarne analize SI-CERT, ki je kazala na razširjenost potencialno ranljivih strežnikov v Republiki Sloveniji, je URSIV sklepal, da obstaja povečana ogroženost varnosti omrežij in informacijskih sistemov pri IBS različnih sektorjev in organih državne uprave, ki upravljajo z informacijskimi sistemi in deli omrežja oziroma izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti in ki uporabljajo Exchange strežnike. URSIV je prav tako ocenil, da so lahko ogroženi tudi upravljalci kritične infrastrukture. URSIV je 7. marca 2021 ocenil, da je nastopilo stanje povečane ogroženosti varnosti omrežij in informacijskih sistemov zavezancev po Zakonu o informacijski varnosti, ki so bili s sklepom Vlade Republike Slovenije na podlagi navedenega zakona določeni kot IBS oziroma organi državne uprave ter 8. marca 2021 izdal odločbe desetim IBS, s katerimi jim je naložil ustrezne ukrepe v povezavi s prej omenjenimi kritičnimi ranljivostmi. Ker je bila odprava kritičnih ranljivosti Microsoft Exchange serverjev v Sloveniji ponekod sorazmerno počasna, še posebej v manjših podjetjih, sta URSIV in SI-CERT 15. marca 2021 objavila skupno sporočilo za javnost, s katerim sta pozvala vse lastnike in upravljalce Microsoft Exchange Server strežnikov v Sloveniji, da poskrbijo za varnost svojih organizacij, zaposlenih, poslovnih partnerjev in drugih tako, da čim prej nadgradijo svoje Microsoft Exchange strežnike z uradno izdanimi popravki.

Ranljivost Pulse VPN

Na podlagi mednarodnega sodelovanja je SI-CERT pridobil podatke o kritični ranljivosti Pulse VPN za slovenske uporabnike. O ranljivosti so obvestili znane subjekte ter SIGOV-CERT. Omenjena ranljivost se že dalj časa aktivno izkorišča v napadih.

Aplikacija za akreditacijo in organiziranje dogodkov

Uporabniki nekaterih storitev e-uprave so v maju dobili nenavadno SMS-sporočilo. Izkazalo se je, da ne gre za vdor v računalniški sistem javne uprave, temveč za testiranje množičnega pošiljanja SMS-vsebin. Ugotovljeno je bilo, da razvijalci in naročnik niso izvedli predpisanih postopkov varnostne presoje sistema.

Rast števila incidentov v državni upravi

SIGOV-CERT zaznava nadaljnjo rast števila incidentov. Trend zaznan v tretjem kvartalu leta 2020 se nadaljuje. Izstopajoč je drugi kvartal leta 2021 predvsem maj in junij. V prvem polletju je bilo obravnavanih že 526 incidentov. V prejšnjem letu je bilo le-teh 551. Vzrok prirasta je večje število poskusov goljufij - phishinga ter poskusov okužbe z zlonamerno kodo preko elektronske pošte. Prevladujoč vektor napada je bil elektronska pošta, preko ribarjenja. Tovrstna elektronska sporočila so v začetku kvartala vsebovala po večini pripombe z znano zlonamerno kodo, predvsem Emotet. Kasneje pa je postal prevladujoč način elektronska pošta, ki je vsebovala povezave na zlorabljene domene oziroma IP naslove, ki so vsebovali zlonamerno kodo.

Pravno-informacijski sistem Republike Slovenije

V povezavi z incidentom, ki je povzročil izpad delovanja Pravno-informacijski sistem Republike Slovenije (pisrs.si), za katerega je stvarno pristojna Služba vlade za zakonodajo (SVZ) upravljanje pa poteka preko MJU, je bilo ugotovljeno da je vdor onesposobil le delovanje storitve pisrs.si in da do vdora na druge strežnike ni prišlo. V analizi je bilo ugotovljeno, da storitev uporablja Redhat Enterprise 5.9, ki nima več podpore in Apache Solr 4.0 iz leta 2012. Za slednjega je bila ugotovljena ranljivost iz leta 2019.

Statistika

V prvem polletju leta 2020 sta odzivna centra obravnavala 2048 incidentov. V mesecu maju sta odzivna centra beležila rekordno število priglasičev.

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

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. V fazi implementacije je Nacionalni načrt odzivanja na kibernetiske incidente, ki med drugim določa klasifikacijo incidentov.

OCENA

Na podlagi podatkov iz prve 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 kibernetike varnosti.

Na podlagi mednarodnih poročil ocenjujemo, da lahko v prihodnje pride do dodatnega porasta kibernetike kriminala, saj izvajalci kriminalnih dejanj zlorabljajo povečano aktivnost posameznikov in pospešeno preoblikovanje poslovnih procesov podjetij. Storitvi 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, vrivanje v poslovno komunikacijo, ljubezenske prevare). Vse bolj pa so zaradi hitrega zasluzka na udaru tudi posamezniki, ki želijo investirati v kripto valute.

V drugi polovici leta oziroma ob pričetku šolskega in študijskega leta ter v povezavi z vplivom epidemije COVID-19 je moč pričakovati rast uporabe fiksnih in mobilnih omrežij. Ob morebitnem poslabšanju zdravstvene situacije lahko pričakujemo okrepljene aktivnosti na področju dela na domu, učenja na daljavo in spletnega nakupovanja. Zato lahko pričakujemo porast števila priglasihen incidentov (phishing napadov, spletnih goljufij, porazdeljenih napadov onemogočanja na strežnik, ipd.)

PREDLOGI IN PRIPOROČILA

Predlagamo ohranjanje visokega nivoja kibernetike 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.

Ozaveščanje o spletnih groznjah naj postane stalnica. Gre za najcenejši način boja proti prevaram na spletu. 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/)."

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 posodablajo 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 kibernetiskim aktivnostim znotraj svojih sistemov, ki bi lahko pomenile kibernetisko 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. Dodatno pozornost je potrebno nameniti kibernetiski varnosti v državni upravi predvsem v času predsedovanja Republike Slovenije Svetu Evropske unije v drugi polovici leta 2021. Posebno pozornost je potrebno še vedno nameniti zdravstvenemu 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 220

Februar 235

Marec 271

April 242

Maj 298

Junij 256

SKUPAJ 1522

2. Stopnje incidentov

Oznaka Stopnja 1. četrletje 2. četrletje Skupaj

C1 Kritičen incident 0 0 0

C2 Zelo pomemben incident 0 0 0

C3 Pomemben incident 2 3 5

C4 Incident visoke stopnje 20 11 31

C5 Incident srednje stopnje 59 63 122

C6 Incident nizke stopnje 645 719 1364

SKUPAJ 726 796 1522

3. Razdelitev po sektorjih

Skupina Sektor 1. četrletje 2. četrletje Skupaj

NIS Energija 2 3 5

NIS Digitalna infrastruktura 3 2 5

NIS Zdravstvo 1 4 5

NIS Promet 0 1 1

NIS Bančništvo 41 21 62

ZInfV Organi državne uprave 15 7 22

Ostalo Operaterji elektronskih komunikacij 14 2 16

Ostalo Raziskovalno-izobraževalni sektor 39 37 76

Ostalo Druge pravne osebe 132 167 299

Ostalo Fizična oseba 442 507 949

Ostalo Drugo 37 45 82

SKUPAJ 726 796 1522

4. Vrste in oznake novih incidentov

Kategorija Vrsta 1. četrletje 2. četrletje Skupaj

Neprimerna vsebina Neželena sporočila 23 30 53

Neprimerna vsebina Žaljiva vsebina 6 2 8

Neprimerna vsebina Nasilna vsebina

Zlonamerna koda Virus 7 7 14

Zlonamerna koda Trojanski konj 40 47 87

Zlonamerna koda Vohunska programska oprema (angl. Spyware) 1 0 1

Zlonamerna koda Rootkit

Zlonamerna koda Boti in botneti 4 1 5

Zlonamerna koda Nadzorni strežnik

Zlonamerna koda Izsiljevalski virus 11 16 27

Zlonamerna koda Orodje za oddaljen nadzor (RAT) 7 7 14

Zbiranje informacij Odkrivanje potencialnih tarč in ranljivosti (skeniranje) 13 5 18

Zbiranje informacij Prestrežanje komunikacije

Zbiranje informacij Socialni inženiring

Poskusi vdora Izkoriščanje znane ranljivosti

Poskusi vdora Poskusi prijav, bruteforce in napadi s slovarjem 9 5 14

Vdor Zloraba privilegiranega uporabniškega računa 4 2 6

Vdor Zloraba neprilegiranega uporabniškega računa 25 32 57

Vdor Napad na aplikacijo 2 0 2

Razpoložljivost Napad onemogočanja 1 2 3

Razpoložljivost Porazdeljen napad onemogočanja 8 12 20

Razpoložljivost Izpad delovanja naprav ali omrežja

Varnost informacijskih virov Nepooblaščen dostop do podatkov 3 4 7

Varnost informacijskih virov Nepooblaščno spreminjanje podatkov 1 9 10

Varnost informacijskih virov Odtekanje informacij 1 1 2

Goljufije Nepooblaščno izkoriščanje virov 2 1 3

Goljufije Intelektualna lastnina in avtorske pravice 1 3 4

Goljufije Kraja identitete 17 21 38

Goljufije Phishing sporočilo 76 181 257

Goljufije Phishing spletno mesto 67 53 120

Goljufije Spletno nakupovanje 35 28 63

Goljufije Goljufija z vnaprejšnjim plačilom 44 34 78

Goljufije Izsiljevanje 46 27 73
Goljufije Druge goljufije 167 184 351
Ranljivosti Odgovorno razkrivanje 0 3 3
Ranljivosti Razkritje ranljivosti 2 1 3
Ranljivosti Ranljivi sistemi in naprave 11 9 20
Drugo Drugo 92 68 160
Test Namenjeno testom 0 1 1
SKUPAJ 726 796 1522

5. Neposredna finančna izguba prijavitelja v EUR

Kategorija 1. četrletje 2. četrletje Skupaj

Druge goljufije 275801,00 150086,00 425887,00
Nepooblaščno spreminjanje podatkov 0 123113,00 123113,00
Odtekanje informacij 0 22045,00 22045,00
Spletno nakupovanje 12758,50 4258,49 17016,99
Zloraba nepriviligiranega uporabniškega računa 7595,00 653,00 8248,00
Trojanski konj 40,00 3500,00 3540,00
Izsiljevalski virus 900,00 490,00 1390,00
Phishing sporočilo 0 945,00 945,00
Drugo 0 290,00 290,00
Izsiljevanje 100,00 0 100,00
Zloraba privilegiranega uporabniškega računa 0 50,00 50,00
Kraja identitete 40,00 0 40,00
SKUPAJ 297234,50 305430,49 602664,99

PRILOGA 2

Podatki SIGOV-CERT

1. Število novih incidentov

Mesec Število incidentov

Januar 76

Februar 64

Marec 57

April 84

Maj 124

Junij 121

SKUPAJ 526

2. Stopnje incidentov

Oznaka 1. četrletje 2. četrletje Skupaj

C1

C2

C3 0 1 1

C4

C5 197 328 525

SKUPAJ 197 329 526

3. Razdelitev po izvoru

Izvor 1. četrletje 2. četrletje Skupaj

Osrednja državna uprava 193 329 522

Lokalna uprava 4 0 4

SKUPAJ 197 329 526

4. Klasifikacija incidentov

Vrsta 1. četrletje 2. četrletje Skupaj

Goljufije 91 145 236

Informacijska varnost 0 2 2

Žaljiva/zlonamerna vsebina 39 71 110

Zbiranje informacij 17 78 95

Zlonamerna koda 34 21 55

Vdori/poizkusi vdora 2 2 4

Ranljivost 3 2 5

Drugo 11 8 19

SKUPAJ 197 329 526