REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO
UPRAVA REPUBLIKE SLOVENIJE
ZA INFORMACIJSKO VARNOST

URSIV

Polletno poročilo o kibernetskih incidentih in napadih 2020/1

Avgust 2020

O URSIV

Uprava Republike Slovenije za informacijsko varnost (URSIV) je pristojni nacionalni organ za informacijsko varnost, ki deluje kot organ v sestavi **Ministrstva za javno upravo**. 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

UPRAVA REPUBLIKE SLOVENIJE ZA INFORMACIJSKO VARNOST
Tržaška cesta 21, 1000 Ljubljana

Telefon: (01) 478 47 78
E-naslov: gp.uiv@gov.si
Spletna stran: www.uiv.gov.si

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** (ang. 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

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 informacijsko družbo in 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) 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. 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.

Od 12. marca do 14. maja 2020 je bila na območju Republike Slovenije razglašena epidemija nalezljive bolezni SARS-CoV-2 (COVID-19). Obdobje je bilo tako zaznamovano z nalezljivo boleznijo, ki jo povzroča virus SARS-CoV-2. Kot za tujino je tudi za Slovenijo moč trditi, da je pandemija COVID-19 vplivala na kibernetsko varnost.

Izkoriščanje pandemije COVID-19

IBS so v času epidemije delovali normalno. Zaznano je bilo izkoriščanje tipičnih kibernetskih dogodkov, kot so zlonamerne kode, »phishing« in podobno, v povezavi s situacijo COVID-19, vendar niso predstavljali resnih groženj. Posebna pozornost je bila posvečena sektorju zdravstva, kjer ni bilo zaznati pomembnih incidentov, ki bi vplivali na delovanje zdravstvenih ustanov in institucij ali drugih deležnikov, ki nudijo podporo zdravstvenemu sistemu.

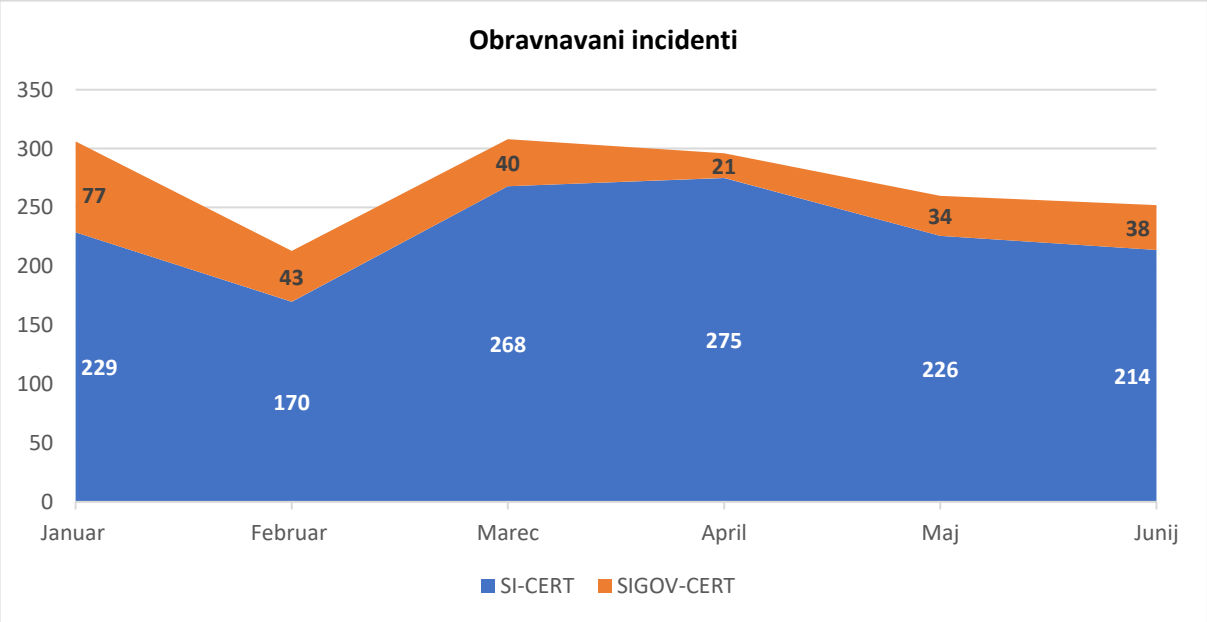
Incidenti, povezani z delom na daljavo

Operaterji elektronskih komunikacij so beležili rast prometa in števila dogodkov, ob tem pa ni bilo zabeleženih kršitev varnosti ali celovitosti. Rast je bila posledica dela in učenja na daljavo ter povečanega prometa na svetovnem spletu. Prišlo je tudi do porazdeljenega napada onemogočanja (DDoS napad) na strežnik, ki nudi podporo izobraževalnim ustanovam na področju e-učenja. Napad je bil hitro zaustavljen, delovanje strežnika pa povrnjeno v normalno delovanje.

Statistika

V prvem polletju leta 2020 sta CERT-a obravnavala 1635 incidentov:

Mesec	SI-CERT	SIGOV-CERT	Skupaj
Januar	229	77	306
Februar	170	43	213
Marec	268	40	308
April	275	21	296
Maj	226	34	260
Junij	214	38	252
SKUPAJ	**1382**	**253**	**1635**



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 CERT-a. V pripravi je nacionalni načrt odzivanja na incidente, ki bo poenotil klasifikacijo.

OCENA

Na podlagi dogajanj v prvi polovici leta 2020 ocenjujemo, da je med COVID-19 prišlo do rahlega porasta »phishing« sporočil, DDoS napadov, neželenih sporočil (spam sporočil), odkrivanja potencialnih tarč in ranljivosti (port scanninga), lažnih spletnih strani in trgovin, elektronskih sporočil kompromitiranja, distribucije zlonamernih kod. Menimo, da so se sredstva, ki smo jih v preteklosti investirali v preventivne dejavnosti ozaveščanja o varnosti na spletu (Safe.si, Varni na internetu), pokazala pozitivne rezultate pri blažitvi vplivov krize 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 povpraševanje posameznikov in podjetij na internetu po informacijah in izdelkih (predvsem zdravstvenih). Storilci letega bodo še naprej inovativni pri uvajanju različnih zlonamernih programov in škodljive programske opreme na temo pandemije COVID-19, predvsem kot posledica povečanega števila delavcev, ki delajo od doma oz. imajo oddaljeni dostop do sistemov njihovih delodajalcev. Pričakovati je razširitev dejavnosti tudi na druge vrste spletnih napadov.

PREDLOGI

Potrebno je ohranjati visok nivo kibernetske varnosti IBS in organov državne uprave.

Nadaljevati je potrebno z intenzivnim ozaveščanjem javnosti, saj opažamo, da je javnost obveščena o tem, na koga se lahko obrne ob kibernetskem incidentu, nekoliko manj pa je poučena glede prepoznavanja in odzivanja na poskuse kibernetskih prevar oziroma zlorab ter pomembnosti prijave kibernetskih incidentov SI-CERT.

Vsem uporabnikom predlagamo, da:

- preverijo implementirane varnostne mehanizme in nastavitve aplikacij, programov in informacijskih sistemov;
- preverijo varnostne nastavitve/ukrepe povezane z zmogljivostmi za delo od doma;
- 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 predlagamo, 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 okrevanje po katastrofi (ang. Disaster Recovery Procedures, DRP) in postopke odzivanja na incidente;
- pregledajo podatke iz sistema za upravljanje varnostnih dogodkov in tveganj (ang. Security Information and Event Manager, SIEM) in drugih orodij ter opravijo analizo stanja (tip in obseg dogodkov).

Dodatno pozornost je potrebno nameniti kibernetski varnosti v zdravstvenem sistemu in podpornim deležnikom na področju zdravstva, saj lahko v podobnih situacijah, kot je bila COVID-19, hitro postanejo resne tarče.

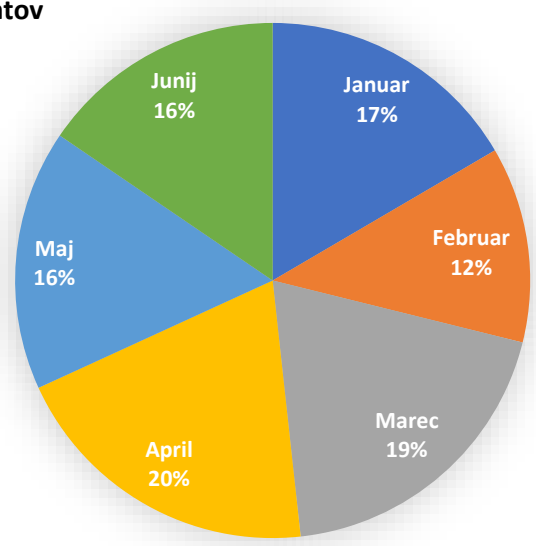
PRILOGA 1

Podatki SI-CERT

1. Število novih incidentov

Mesec	Število incidentov	Delež incidentov po mesecih
Januar	229	17%
Februar	170	12%
Marec	268	19%
April	275	20%
Maj	226	16%
Junij	214	16%
SKUPAJ	**1382**	**100%**

Delež incidentov po mesecih



2. 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	3	4
C4	Incident visoke stopnje	7	14	21
C5	Incident srednje stopnje	42	56	98
C6	Incident nizke stopnje	617	642	1259
SKUPAJ		**667**	**715**	**1382**

3. Razdelitev po izvoru

Izvor	1. četrtletje	2. četrtletje	Skupaj
Prijava incidenta	629	659	1288
Zahtevek pristojnega organa ali sodišča	1	4	5
Drugo	29	43	72
SKUPAJ	**659**	**706**	**1365**

4. Razdelitev po sektorjih

Skupina	Sektor	1. četrtletje	2. četrtletje	Skupaj
NIS	Energija	2	1	3
NIS	Digitalna infrastruktura	0	6	6
NIS	Zdravstvo	1	6	7
NIS	Promet	1	3	4
NIS	Bančništvo	18	20	38
NIS	Ponudnik računalništva v oblaku	1	1	2
ZInfV	Organi državne uprave	3	15	18
Ostalo	Operaterji el. komunikacij	6	5	11
Ostalo	Raziskovalno-izobraževalni sektor	17	23	40
Ostalo	Druge pravne osebe	144	160	304
Ostalo	Fizična oseba	445	425	870
Ostalo	Drugo	30	50	80
SKUPAJ		**668**	**715**	**1383**

5. Vrste in oznake novih incidentov

Kategorija	Vrsta	1. četrtletje	2. četrtletje	Skupaj
Neprimerna vsebina	Neželena sporočila	16	13	29
Neprimerna vsebina	Žaljiva vsebina	3	5	8
Neprimerna vsebina	Nasilna vsebina	0	1	1
Zlonamerna koda	Virus	5	9	14
Zlonamerna koda	Trojanski konj	26	23	49
Zlonamerna koda	Vohunska programska oprema	1	0	1
Zlonamerna koda	Boti in botneti	4	4	8
Zlonamerna koda	Nadzorni strežnik	5	2	7
Zlonamerna koda	Izsiljevalski virus	16	17	33
Zlonamerna koda	Orodje za oddaljen nadzor (RAT)	5	3	8
Zbiranje informacij	Odkrivanje potencialnih tarč in ranljivosti (skeniranje)	4	14	18
Zbiranje informacij	Prestrezanje komunikacije	0	1	1
Zbiranje informacij	Socialni inženiring	1	0	1
Poskusi vdora	Izkoriščanje znane ranljivosti	1	2	3
Poskusi vdora	Poskusi prijav, bruteforce in napadi s slovarjem	5	3	8

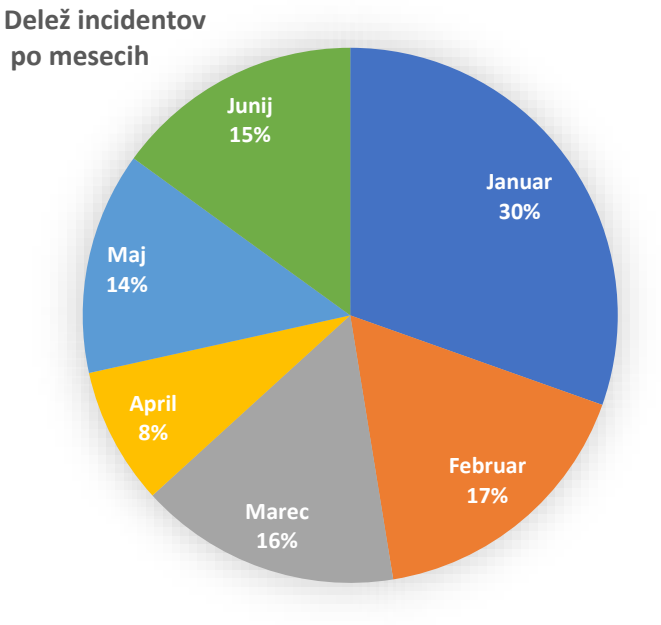
Kategorija	Vrsta	1. četrtletje	2. četrtletje	Skupaj
Vdor	Zloraba priviligiranega uporabniškega računa	1	1	2
Vdor	Zloraba nepriviligiranega uporabniškega računa	23	22	45
Vdor	Napad na aplikacijo	0	3	3
Razpoložljivost	Napad onemogočanja	1	2	3
Razpoložljivost	Porazdeljen napad onemogočanja	5	11	16
Varnost informacijskih virov	Nepooblaščen dostop do podatkov	4	5	9
Varnost informacijskih virov	Nepooblaščeno spreminjanje podatkov	1	5	6
Varnost informacijskih virov	Odtekanje informacij	2	1	3
Goljufije	Nepooblaščeno izkoriščanje virov	2	1	3
Goljufije	Intelektualna lastnina in avtorske pravice	0	5	5
Goljufije	Kraja identitete	16	16	32
Goljufije	Phishing sporočilo	120	141	261
Goljufije	Phishing spletno mesto	55	42	97
Goljufije	Spletno nakupovanje	20	22	42
Goljufije	Goljufija z vnaprejšnjim plačilom	35	44	79
Goljufije	Izsiljevanje	48	44	92
Goljufije	Druge goljufije	158	180	338
Ranljivosti	Odgovorno razkrivanje	5	2	7
Ranljivosti	Razkritje ranljivosti	1	0	1
Ranljivosti	Ranljivi sistemi in naprave	4	6	10
Drugo	Drugo	71	63	134
SKUPAJ		**664**	**713**	**1377**

PRILOGA 2

Podatki SIGOV-CERT

1. Število novih incidentov

Mesec	Število incidentov	Delež incidentov po mesecih
Januar	77	30%
Februar	43	17%
Marec	40	16%
April	21	8%
Maj	34	14%
Junij	38	15%
SKUPAJ	**253**	**100%**



2. Stopnje incidentov

Oznaka	1. četrtletje	2. četrtletje	Skupaj
C1	0	0	0
C2	0	0	0
C3	0	0	0
C4	0	6	6
C5	160	87	247
SKUPAJ	**160**	**93**	**253**

3. Razdelitev po izvoru

Izvor	1. četrtletje	2. četrtletje	Skupaj
Osrednja državna uprava	143	90	233
Lokalna uprava	17	3	20
SKUPAJ	**160**	**93**	**253**

4. Klasifikacija incidentov

Vrsta	1. četrtletje	2. četrtletje	Skupaj
Žaljiva vsebina / Vsiljena pošta (Spam)	61	31	92
Kraja / Napad z ribarjenjem (Phishing)	37	42	79
Pridobivanje informacij / Socialni inženiring	49	6	55
Zlonamerna koda / Virus	3	5	8
Zlonamerna koda	1	3	4
Zlonamerna koda / Vohunska programska oprema	1	0	1
Kršitev skladnosti / Ostale kršitve skladnosti	1	0	1
Poskusi vdora / Poskusi prijav	2	1	3
Vdori	0	1	1
Informacijska varnost	0	1	1
Ostalo	5	3	8
SKUPAJ	**160**	**93**	**253**