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

URSIV

Polletno poročilo o kibernetskih incidentih in napadih 2020/2

Februar 2021

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** *(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

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 drugem 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. Zabeležen je bil incident stopnje C2, za katerega pa smo dolžni opozoriti, da gre za incident prožen v testnem okolju v okviru vaje Cyber Coalition 2020.

Izkoriščanje pandemije COVID-19

Od 19. oktobra do 31. decembra 2020 je bila na območju Republike Slovenije ponovno razglašena epidemija nalezljive bolezni COVID-19. IBS so v drugem polletju delovali normalno. Zaznano je bilo izkoriščanje tipičnih kibernetskih dogodkov, kot so zlonamerne kode, »phishing« in podobno, verjetno tudi 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 in spletnim nakupovanjem

Prva polovica leta je bila v znamenju rasti uporabe fiksnih in mobilnih omrežij. Tretje četrtletje je bilo zaznamovano s postopnim sproščanjem omejitvenih ukrepov zaradi izboljšanja epidemiološke situacije. S ponovno razglasitvijo epidemije COVID-19 beležimo rast incidentov, ki so posledica dela in učenja na daljavo ter povečanega prometa na svetovnem spletu. Tako smo bili priča ponovitvi porazdeljenega napada onemogočanja (DDoS napad) na strežnik, ki nudi podporo izobraževalnim ustanovam na področju e-učenja. Napad je bil uspešno zaustavljen. Preusmeritev potrošnikov na spletne nakupe zaradi zaprtja neživilskih trgovin in restavracij pa je rezultiralo v porastu uporabe spletnega nakupovanja, kar s pridom izkoriščajo spletni goljufi ter akterji phishing napadov. Pri slednjih je bila zaznana zloraba znanih dostavnih podjetij.

Porast števila incidentov v državni upravi

Tudi SIGOV-CERT je zaznal povečano število incidentov v primerjavi s tretjim kvartalom 2020. Prevladujoč vektor napada je bila elektronska pošta, preko ribarjenja. Opažajo vedno bolj napredne oziroma ciljno usmerjene napade, sama struktura in vsebina v elektronskih sporočilih je pogosto prilagojena žrtvi napada. Tovrstna elektronska sporočila so v začetku četrtega četrtletja vsebovala po večini priponke z znano zlonamerno kodo, kasneje pa je postal prevladujoč način preko povezav na domene oziroma IP naslove z zlonamerno kodo. Še vedno opažajo prisotnost priponk in povezav, ki vsebujejo Emotet zlonamerno kodo.

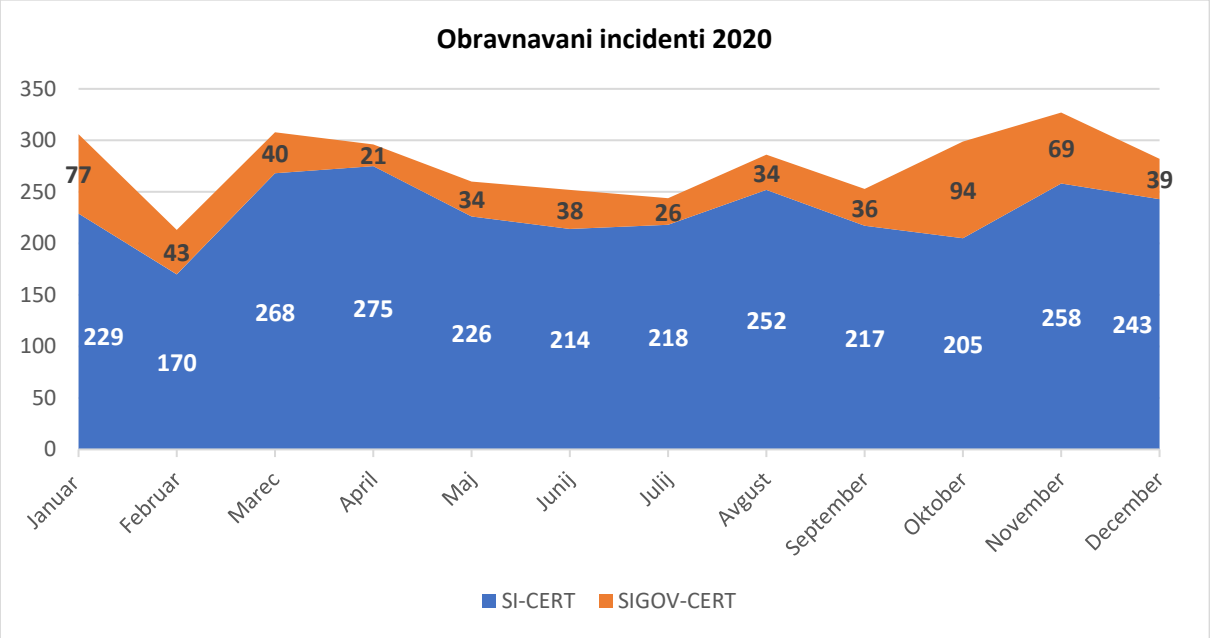
»SolarWinds«

Konec leta 2020 je na mednarodnem področju zaznamovalo decembrsko razkritje vdora v ameriško podjetje SolarWinds oziroma njihov produkt Orion platformo za nadzor in upravljanje z informacijsko komunikacijskimi sredstvi, ki jo med drugim uporabljajo večja podjetja in državne ustanove. Do vdora naj bi prišlo že marca 2020 s strani državno podprtega akterja. Ob razkritju ranljivosti sta SI-CERT in SIGOV-CERT opravila ustrezno analizo, izvedla preventivne ukrepe ter seznanila zavezance. SI-CERT je ugotovil zelo majhno razširjenost platforme v Sloveniji, pri posameznih namestitvah pa so ocenjevali možnost, da ta vsebuje zlonamerno komponento. Do sedaj v nobenem primeru niso mogli potrditi, zato menijo, da vdor v SolarWinds nima konkretnih posledic za omrežja v Sloveniji.

Statistika

V drugem polletju leta 2020 sta odzivna centra obravnavala 1691 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 1. polletje	**1382**	**253**	**1635**
Julij	218	26	244
Avgust	252	34	286
September	217	36	253
Oktober	205	94	299
November	258	69	327
December	243	39	282
SKUPAJ 2. polletje	**1393**	**298**	**1691**
SKUPAJ 2020	**2775**	**551**	**3326**



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 končnega medresorskega usklajevanja je nacionalni načrt odzivanja na kibernetske incidente, ki bo poenotil klasifikacijo incidentov.

OCENA

Na podlagi podatkov iz druge polovice leta 2020 ocenjujemo, da se bo nadaljevala izpostavljenost uporabnikov na phishing sporočila. Za slednje lahko rečemo, da so bili »hit leta 2020«. 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 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 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 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.

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 *(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);
- da spremljajo novoodkrite podrobnosti v zvezi s »SolarWinds vdorom« še posebej glede vektorjev napada, ki niso povezani s produktom SolarWinds Orion.

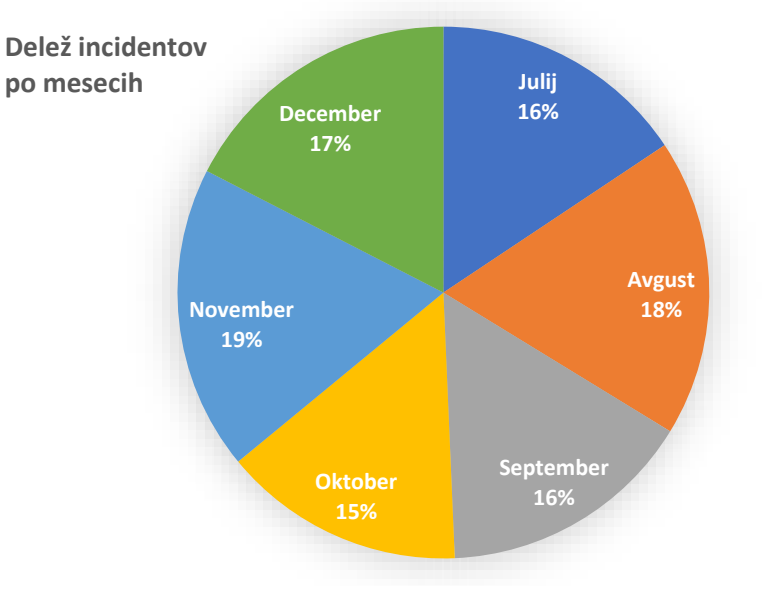
Dodatno pozornost je potrebno nameniti kibernetski varnosti v državni upravi predvsem v luči priprav na predsedovanje Republike Slovenije Svetu Evropske unije v drugi polovici leta 2021. Posebno pozornost je potrebno še vedno nameniti zdravstvenem sistemu in podpornim deležnikom na področju zdravstva, saj lahko v podobnih situacijah, kot je COVID-19, hitro postanejo resne tarče.

PRILOGA 1

Podatki SI-CERT

1. Število novih incidentov

Mesec	Število incidentov	Delež incidentov po mesecih
Julij	218	16%
Avgust	252	18%
September	217	16%
Oktober	205	15%
November	258	19%
December	243	17%
SKUPAJ	**1393**	**100%**



2. Stopnje incidentov

Oznaka	Stopnja	3. četrtletje	4. četrtletje*	Skupaj
C1	Kritičen incident	0	0	0
C2	Zelo pomemben incident	0	1	1
C3	Pomemben incident	5	1	6
C4	Incident visoke stopnje	11	16	27
C5	Incident srednje stopnje	66	69	135
C6	Incident nizke stopnje	605	619	1224
SKUPAJ		**687**	**706**	**1393**

*Opomba: * Incidenta C2 in C3 v 4. četrtletju sta vadbena incidenta v sklopu vaje Cyber Coalition 2020.*

3. Razdelitev po izvoru

Izvor	3. četrtletje	4. četrtletje	Skupaj
Prijava incidenta	632	670	1302
Zahtevek pristojnega organa ali sodišča	1		1
Drugo	45	34	79
SKUPAJ	**678**	**704**	**1382**

4. Razdelitev po sektorjih

Skupina	Sektor	3. četrtletje	4. četrtletje	Skupaj
NIS	Energija	1	0	1
NIS	Digitalna infrastruktura	2	0	2
NIS	Zdravstvo	7	7	14
NIS	Promet	4	5	9
NIS	Bančništvo	30	22	52
NIS	Ponudnik spletne tržnice	3	0	3
NIS	Ponudnik računalništva v oblaku	0	0	0
NIS	Varstvo okolja	1	0	1
ZInfV	Organi državne uprave	14	19	33
Ostalo	Operaterji elektronskih komunikacij	14	18	32
Ostalo	Raziskovalno-izobraževalni sektor	20	28	48
Ostalo	Druge pravne osebe	137	150	287
Ostalo	Fizična oseba	413	429	842
Ostalo	Drugo	35	26	61
SKUPAJ		**681**	**704**	**1385**

5. Vrste in oznake novih incidentov

Kategorija	Vrsta	3. četrtletje	4. četrtletje	Skupaj
Neprimerna vsebina	Neželena sporočila	11	32	43
Neprimerna vsebina	Žaljiva vsebina	7	7	14
Neprimerna vsebina	Nasilna vsebina	2	0	2
Zlonamerna koda	Virus	15	17	32
Zlonamerna koda	Trojanski konj	64	28	92
Zlonamerna koda	Vohunska programska oprema	0	0	0
Zlonamerna koda	Rootkit	0	1	1
Zlonamerna koda	Boti in botneti	4	4	8
Zlonamerna koda	Nadzorni strežnik	0	0	0
Zlonamerna koda	Izsiljevalski virus	16	20	36
Zlonamerna koda	Orodje za oddaljen nadzor (RAT)	3	3	6
Zbiranje informacij	Odkrivanje potencialnih tarč in ranljivosti (skeniranje)	3	7	10
Zbiranje informacij	Prestrezanje komunikacije	0	0	0
Zbiranje informacij	Socialni inženiring	1	0	1
Poskusi vdora	Izkoriščanje znane ranljivosti	1	0	1

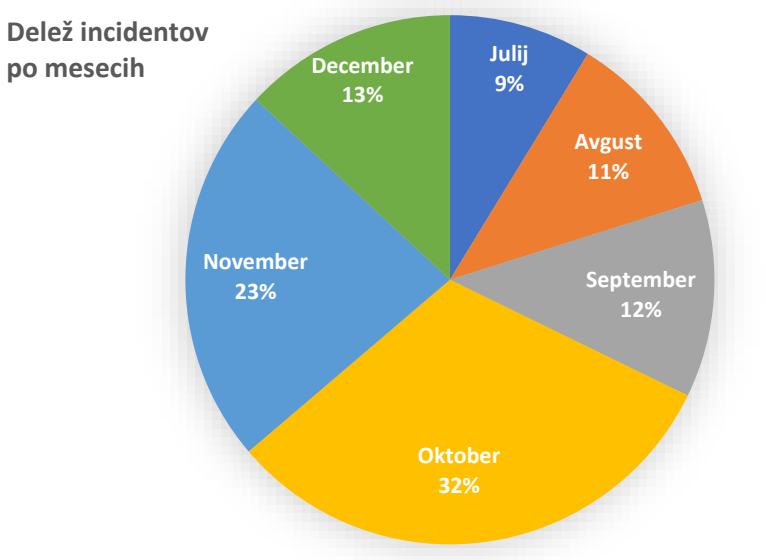
Kategorija	Vrsta	3. četrtletje	4. četrtletje	Skupaj
Poskusi vdora	Poskusi prijav, bruteforce in napadi s slovarjem	4	4	8
Vdor	Zloraba privilegiranega uporabniškega računa	3	2	5
Vdor	Zloraba neprivilegiranega uporabniškega računa	21	16	37
Vdor	Napad na aplikacijo		1	1
Razpoložljivost	Napad onemogočanja	1	3	4
Razpoložljivost	Porazdeljen napad onemogočanja	8	7	15
Razpoložljivost	Izpad delovanja naprav ali omrežja		2	2
Varnost informacijskih virov	Nepooblaščen dostop do podatkov	4	0	4
Varnost informacijskih virov	Nepooblaščeno spreminjanje podatkov	0	2	2
Varnost informacijskih virov	Odtekanje informacij	2	0	2
Goljufije	Nepooblaščeno izkoriščanje virov		1	1
Goljufije	Intelektualna lastnina in avtorske pravice	1	4	5
Goljufije	Kraja identitete	18	17	35
Goljufije	Phishing sporočilo	139	89	228
Goljufije	Phishing spletno mesto	41	64	105
Goljufije	Spletno nakupovanje	19	36	55
Goljufije	Goljufija z vnaprejšnjim plačilom	40	48	88
Goljufije	Izsiljevanje	19	33	52
Goljufije	Druge goljufije	173	157	330
Ranljivosti	Odgovorno razkrivanje	3	4	7
Ranljivosti	Razkritje ranljivosti	0	1	1
Ranljivosti	Ranljivi sistemi in naprave	2	8	10
Drugo	Drugo	62	83	145
Test	Namenjeno testom	0	1	1
SKUPAJ		**687**	**702**	**1389**

PRILOGA 2

Podatki SIGOV-CERT

1. Število novih incidentov

Mesec	Število incidentov	Delež incidentov po mesecih
Julij	26	9%
Avgust	34	11%
September	36	12%
Oktober	94	32%
November	69	23%
December	39	13%
SKUPAJ	**298**	**100%**



2. Stopnje incidentov

Oznaka	3. četrtletje	4. četrtletje	Skupaj
C1	0	0	0
C2	0	0	0
C3	0	0	0
C4	7	18	25
C5	89	184	273
SKUPAJ	**96**	**202**	**298**

3. Razdelitev po izvoru

Izvor	3. četrtletje	4. četrtletje	Skupaj
Osrednja državna uprava	85	197	282
Lokalna uprava	11	5	16
SKUPAJ	**96**	**202**	**298**

4. Klasifikacija incidentov

Vrsta	3. četrtletje	4. četrtletje	Skupaj
Žaljiva vsebina / Vsiljena pošta (Spam)	25	53	78
Kraja / Napad z ribarjenjem (Phishing)	44	77	121
Pridobivanje informacij	1	0	1
Pridobivanje informacij / Socialni inženiring	1	40	41
Zlonamerna koda	1	0	1
Zlonamerna koda / Virus	15	18	33
Zlonamerna koda /izsiljevalski virus	2	0	2
Vdori	1	0	1
Informacijska varnost	1	2	3
Ostalo	5	12	17
SKUPAJ	**96**	**202**	**298**