REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE
ZA INFORMACIJSKO VARNOST

URSIV

Številka: 386-23/2025-1544-2
Datum: 24. 4. 2025

Polletno poročilo o kibernetskih incidentih in napadih, 2024-2

April 2025

UVOD

Urad Vlade Republike Slovenije za informacijsko varnost (URSIV) je kot pristojni nacionalni organ za informacijsko varnost med drugim odgovoren za vzpostavitev in delovanje nacionalnega sistema zagotavljanja informacijske in kibernetske varnosti v Republiki Sloveniji. Poleg tega 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).

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 dvakrat letno pripravi poročilo o varnostnih dogodkih[1] in incidentih[2] kibernetske varnosti v Republiki Sloveniji. Namen poročila je seznanjanje javnosti o aktualnem stanju kibernetske varnosti v državi. Posledično predstavlja sintezo aktualnih statističnih podatkov za obdobje zadnjega pol leta, kot tudi primerjalno analizo kibernetskih dogodkov, incidentov in aktivnosti v kratkoročnem preteklem obdobju. Hkrati pa glede na podlagi preteklih trendov in specifike kibernetskih incidentov poda priporočila glede ukrepov, s katerimi lahko organi na državni in lokalni ravni podjetja in drugi subjekti poskrbijo za boljšo kibernetsko varnost njih samih.

Poročilo je pripravljeno na podlagi podatkov in informacij pridobljenih s strani SI-CERT *(angl. Slovenian Computer Emergency Response Team)*, ki je pristojni nacionalni odzivni center za kibernetsko varnost za zavezance kot izvajalce 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 ponudniki digitalnih storitev. Poleg tega poročilo vsebuje tudi podatke SIGOV-CERT, ki je pristojni odzivni center za incidente v informacijskih sistemih organov državne uprave (ODU) in povezanih subjektov. SIGOV-CERT je notranja organizacijska enota URSIV. Oba odzivna centra se v skladu z zakonom odzivata tudi na prostovoljno priglašene dogodke in incidente.

OBRAVNAVA DOGODKOV IN INCIDENTOV V OBDOBJU OD JULIJA DO DECEMBRA 2024

V drugem polletju leta 2024 sta oba odzivna centra skupaj obravnavala 2419 varnostnih dogodkov in incidentov, kar pomeni minimalni vpad v primerjavi s prvim polletjem 2024, ko je bilo zabeleženih 2589 varnostnih dogodkov in incidentov. Med priglašenimi dogodki in incidenti je bilo največ priglasitev izvedenih na podlagi prostovoljne priglasitve s strani fizičnih oseb in subjektov, ki niso zavezanci po Zakonu o informacijski varnosti. Poleg tega so bili najbolj izpostavljeni raziskovalno-izobraževalni sektor, organi državne uprave in operaterji elektronskih komunikacij. Vrh polletnih prijav dogodkov in incidentov je bil dosežen v oktobru, sicer pa se trend naraščanja incidentov zaznava že od septembra, ko je Republika Slovenija kot nestalna članica Varnostnega sveta Organizacije združenih narodov (OZN) prevzela enomesečno predsedovanje. Bolj podrobni statistični podatki so razvidni v tabeli 1 spodaj.

[1] Varnostni dogodek je vsaka zaznana kibernetska aktivnost, ki nima vpliva na omrežja in informacijske sisteme oziroma informacijske storitve zavezancev, ima pa lahko zaznan ali možen vpliv na posamezne fizične osebe ali posamezna podjetja v državi, ki niso zavezanci.

[2] Kibernetski incident je vsak dogodek, ki ima dejanski negativni učinek na varnost omrežij in informacijskih sistemov.

Tabela 1: Število obravnavanih incidentov od 1. julija do 30. decembra 2024

Mesec	SI-CERT	SIGOV-CERT	SKUPAJ 2. polletje 2024
julij 2024	281	23	304
avgust 2024	241	70	311
september 2024	261	165	426
oktober 2024	294	203	497
november 2024	224	194	418
december 2024	268	195	463
SKUPAJ	1569	850	**2419**

Vir: SI-CERT, SIGOV-CERT

SI-CERT je v drugem polletju obravnaval skupaj 1569 varnostnih dogodkov in incidentov, kar predstavlja minimalen vpad v primerjavi s 1. polletjem 2024, ko jih je bilo obravnavanih 1576. Pri tem je pomembno pojasniti, da v tabelo niso vključeni enostavni incidenti spletnega ribarjenja (ang. phishing), ki so bili sicer prijavljeni in le evidentirani na SI-CERT. Posledično niso bili všteti v skupno število incidentov. Skupno število teh incidentov v letu 2024 je sicer znašalo 1429.

Tabela 2: Stopnje varnostnih dogodkov in incidentov

Oznaka	3. četrtletje 2024	4. četrtletje 2024	SKUPAJ
C1	0	0	0
C2	0	0	0
C3	0	3	3
C4	8	3	11
C5	40	31	71
C6	735	749	1484
SKUPAJ	783	786	**1569**

Vir: SI-CERT

V tem obdobju je SI-CERT obravnaval tri pomembne incidente stopnje C3, 11 primerov incidentov stopnje C4, 71 primerov incidentov C5 in 1484 primerov varnostnih dogodkov stopnje C6.

Tabela 3: Kategorije in vrste incidentov

Kategorija	Skupaj
Druge goljufije	500
Drugo	200
Izsiljevanje	167
Zloraba nepriviligiranega računa	130
Spletno nakupovanje	103
Neželena sporočila	78
Goljufija z vnaprejšnjim plačilom	57
Trojanski konj	45
Phishing sporočilo	42
Nepooblaščeno izkoriščanje virov	30
Kraja identitete	26
Porazdeljen napad onemogočanja	21

Odkrivanje potencialnih tarč in ranljivosti	16
Intelektualna lastnina in avtorske pravice	13
Razkritje ranljivosti	13
Napad na aplikacijo	13
Žaljiva vsebina	11
Ranljivi sistemi in naprave	11
Phishing spletno mesto	11
Zloraba priviligiranega uporabniškega računa	10
Orodje za oddaljen nadzor (RAT)	10
Nepooblaščen dostop do podatkov	8
Nepooblaščeno spreminjanje podatkov	8
Izsiljevalski virus	8
Poskusi prijav, bruteforce in napadi s slovarjem	7
Boti in botneti	6
Odgovorno razkrivanje	5
Virus	4
Napad onemogočanja	4
Izpad delovanja naprav ali omrežja	4
Odtekanje informacij	2
Rootkit	1
Novinarska vprašanja	1
Nasilna vsebina	1

Vir: SI-CERT

Med oblikami varnostnih dogodkov in kibernetskih incidentov so prevladovale različne oblike spletnih goljufij, katerih žrtve so predvsem fizične in druge pravne osebe, ki dogodke in incidente prijavljajo na podlagi prostovoljne prijave in niso zavezanci po ZInfV, kar je razvidno iz tabele 3. Statistično gledano velja v tem obdobju poleg omenjenih incidentov izpostaviti tudi izsiljevanje, zlorabo neprivilegiranih računov in incidente povezane s spletnim nakupovanjem.

Tabela 4: Razdelitev incidentov po sektorjih

Skupina	Sektor	3. četrtletje 2024	4. četrtletje 2024	Skupaj
NIS	Energija	3	6	9
NIS	Digitalna infrastruktura	2	0	2
NIS	Zdravstvo	1	3	4
NIS	Promet	1	1	2
NIS	Bančništvo	6	2	8
Nis	Infrastruktura finančnih trgov	0	0	0
NIS	Ponudnik spletne tržnice	0	0	0
NIS	Ponudnik računalništva v oblaku	1	1	2
NIS	Varstvo okolja	0	0	0
NIS	Preskrba s hrano	0	0	0
NIS	Oskrba s pitno vodo	0	0	0
ZInfV	Državne ustanove	11	13	24

Ostalo	Operaterji elektronskih komunikacij	6	7	13
Ostalo	Raziskovalno-izobraževalni sektor	31	22	53
Ostalo	Druge pravne osebe	51	70	121
Ostalo	Fizična oseba	38	43	81
Ostalo	Drugo	13	17	30

Vir: SI-CERT

Iz podatkov o razdelitvi incidentov po sektorjih je razvidno, da so bili med najbolj prizadetimi poleg fizičnih oseb in subjektov, ki niso zavezanci po Zakonu o informacijski varnosti, raziskovalno-izobraževalni sektor, državne ustanove in operaterji elektronskih komunikacij.

Tabela 5: Neposredna finančna izguba prijaviteljev v EUR

Kategorija	3. četrtletje 2024	4. četrtletje 2024	Skupaj
Druge goljufije	733.597,00	335.873,00	1.069.470,00
Drugo	33,00	0,00	33,00
Goljufije z vnaprejšnjim plačilom	40.800,00	2.400,00	43.200,00
Izsiljevalski virus	0,00	0,00	0,00
Izsiljevanje	1.070,00	20.000,00	21.070,00
Kraja identitete	0,00	0,00	0,00
Napad na aplikacijo	351.000,00		351.000,00
Nepooblaščeno izkoriščanje virov	48.775,00	21.000,00	69.775,00
Nepooblaščeno spreminjanje podatkov	32.575,00	0,00	32.575,00
Odtekanje informacij	0,00	0,00	0,00
Phishing spletno mesto	750,00		750,00
Phishing sporočilo	0,00	210.600,00	210.600,00
Spletno nakupovanje	588,00	5.772,00	6.360,00
Trojanski konj	0,00	0,00	0,00
Zloraba neprivilegiranega uporabniškega računa	10.470,00	6.064,00	16.534,00
Zloraba privilegiranega uporabniškega računa	0,00	0,00	0,00
Orodje za oddaljen nadzor (RAT)	0,00	0,00	0,00
SKUPAJ	1.219.658,00	601.709,00	**1.821.367,00**

Vir: SI-CERT

Iz tabele 4 so razvidne neposredne finančne izgube prijaviteljev različnih varnostnih dogodkov in incidentov, ki jih je zabeležil SI-CERT. V primerjavi s prvim polletnim obdobjem se ugotavlja povečanje skupne priglašene finančne izgube prijaviteljev, ki je v drugi polovici leta 2024 znašala 1.821,367,00 EUR[3]. Največja zabeležena finančna izguba na področju goljufij je v tem obdobju znašala 1.069.470,00 EUR, kar nakazuje na več kot enkratno povečanje glede na prejšnje polletno obdobje[4]. Ob tem ostale

[3] V polletnem poročilu za 1. polovico 2024 je bila skupna višina finančne izgube po vseh kategorijah 692.537,00 EUR.

[4] V prvem polletnem obdobju 2024 je največja zabeležena finančna izguba na področju goljufij znašala 525.983,00 EUR.

finančne izgube prav tako niso zanemarljive in predstavljajo breme predvsem za manjša in srednje velika podjetja ter primerljive organizacije.

SIGOV-CERT je v drugem polletju zaznal zmanjšanje priglašenih varnostnih dogodkov in kibernetskih incidentov glede na preteklo obdobje. Skupno je bilo obravnavanih 850 varnostnih dogodkov in incidentov. V primerjavi s prejšnjim polletnim obdobjem se je število zmanjšalo iz 1013 na 850 varnostnih incidentov in dogodkov. V 2. polletju 2024 ni bilo priglašenih težjih incidentov označenih s stopnjo C3 ali višje, v primerjavi s prejšnjim obdobjem, ko je bilo obravnavanih osem tovrstnih incidentov. V omenjenem obdobju se je obravnavalo štiri incidente označene s stopnjo C4 in 846 incidentov stopnje C5, kar je razvidno v spodnji tabeli 6.

Tabela 6: Stopnje varnostnih dogodkov in incidentov

Oznaka	3. četrtletje 2024	4. četrtletje 2024	SKUPAJ
C1	0	0	0
C2	0	0	0
C3	0	0	0
C4	2	2	4
C5	256	590	846
C6	0	0	0
SKUPAJ	258	592	**850**

Vir: SIGOV-CERT

Pri analizi vrst dogodkov in incidentov je bilo ugotovljeno, da je bila najpogostejša oblika prijavljenega incidenta uporaba žaljive vsebine oziroma vsiljene pošte (SPAM), s 619 primeri. Sledila so sporočila elektronskega ribarjenja (175), različne oblike goljufij (45) in uporaba zlonamerne kode (7), kar je podrobneje prikazano v spodnji tabeli.

Tabela 7: Vrste dogodkov in incidentov

Vrsta incidenta	3. četrtletje	4. četrtletje	Skupaj
Nezaželena sporočila (SPAM)	148	471	619
Zlonamerna koda	3	4	7
Vdori/poizkusi vdora	1	0	1
Razpoložljivost	0	1	1
Goljufije	13	32	45
Phishing sporočilo	93	82	175
Ranljivost	0	2	2
Drugo	0	0	0
SKUPAJ	258	592	**850**

Vir: SIGOV-CERT

Ranljivosti

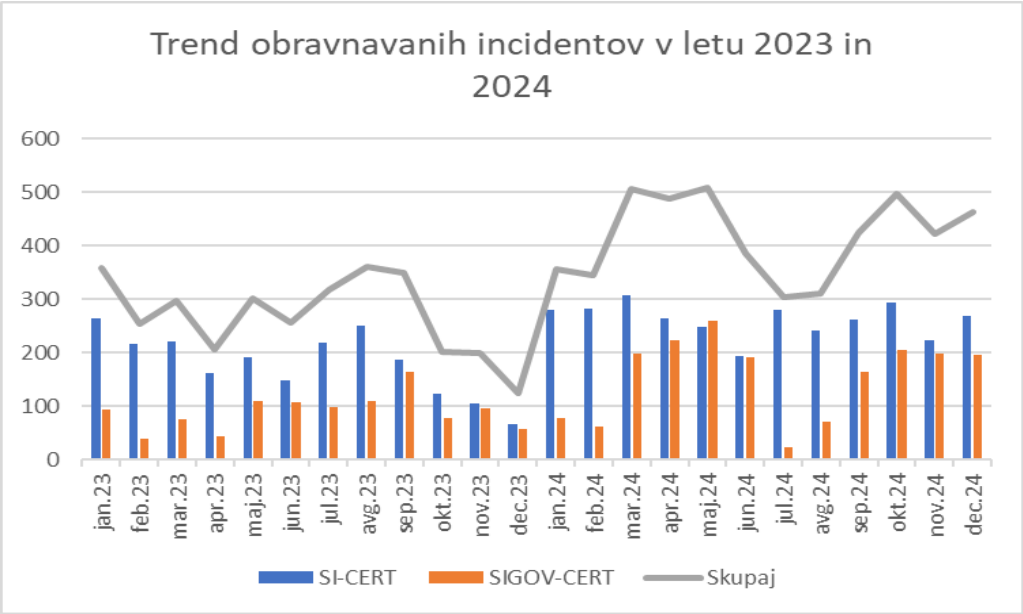
Skupini CSIRT sta v drugi polovici leta objavili več opozoril o zaznanih ranljivostih. Ranljivost je obstoj šibkosti arhitekture informacijskega sistema ali omrežja, v varnostnih protokolih ali procesih, ali kot posledica napak v implementaciji ali upravljanju in je lahko izrabljena s strani zlonamernih akterjev.

V zadnjem polletju je SI-CERT opozoril na verigo ranljivosti v sistemu OpenPrinting CUPS, ki napadalcu omogoča, da pod določenimi pogoji izvede poljubno programsko kodo na ranljivem sistemu s pravicami uporabnika 'IP'. Gre za štiri ranljivosti sistema OpenPrinting CUPS v operacijskem sistemu GNU/Linux, ki napadalcu omogočajo, da na sistemu namesti nov tiskalnik in naloži posebej prirejeno datoteko, ki se zažene, ko uporabnik uporabi nov tiskalnik za tiskanje. V zvezi s temi ranljivostmi so bili podani priporočeni ukrepi, vključno s takojšnjo posodobitvijo ranljivih različic programske opreme GeoServer na najnovejše razpoložljive verzije.

SIGOV-CERT je v drugem polletju leta 2024 objavil več opozoril o kritičnih ranljivostih, vključno s CVE-2024-36401 in CVE-2024-36404, ki sta povezani z izkoriščanjem ranljivosti v Java kodi. Omenjeni ranljivosti sta bili odkrite na strežniku, kjer bi napadalci lahko ustvarili datoteko z zlonamerno kodo. Glede na široko uporabo omenjene programske opreme v javnih storitvah je bilo priporočeno, da se preveri tudi vsa programska oprema Geoserver starejših različic od 2.25.2. V obravnavanem obdobju je bilo objavljeno tudi opozorilo o kritični ranljivosti CVE-2024-53677 v povezavi z Apache Struts, ki ima visoko oceno CVSS. Ta ranljivost napadalcem omogoča manipulacijo parametrov za nalaganje datotek, kar lahko vodi v nalaganje zlonamerne datoteke in izvajanje oddaljene izvršitve kode. Uporabnikom je bilo priporočeno, da nadgradijo na najnovejšo različico (6.4.0), ki odpravlja to težavo.

OCENA

Statistični pregled števila priglašenih varnostnih incidentov in dogodkov v letu 2023 in 2024 kaže na povečanje števila incidentov v letu 2024, obenem pa se še naprej izkazuje večja raznolikost obravnavanih incidentov.



Graf 1: Število obravnavnih incidentov v letih 2023 in 2024

V obravnavanem obdobju so med varnostnimi dogodki in kibernetskimi incidenti prevladovale različne oblike goljufij, uporaba zlonamerne programske opreme z izsiljevanjem, zloraba neprivilegiranih računov in incidenti povezani s spletnim nakupovanjem. Zbrani podatki kažejo, da napadi postajajo vse bolj sofisticirani in kompleksni. Goljufi uporabljajo napredne tehnike socialnega inženiringa, da pridobijo zaupne informacije od žrtev. Zlonamerna elektronska sporočila in spletno ribarjenje so postali bolj ciljno usmerjeni in personalizirani, kar je povečalo njihovo učinkovitost. Pri tem pomaga vse hitreje razvijajoča tehnologija umetne inteligence in tehnologija za izdelavo kompleksnih ponaredkov (ang. Deepfake), ki omogočajo ustvarjanje zelo realističnih ponarejenih video vsebin.

Vse večjo nevarnost predstavljajo kibernetske aktivnosti, ki izkoriščajo ranljivosti v dobavni verigi in služijo kot vstopni vektor, na primer za postavitev vohunske programske opreme ali kot vektor napada v primeru eskalacije že tako napetih odnosov med velikimi geopolitičnimi akterji. Gre za zelo pogosto obliko kibernetskega kriminala, za katero ocenjujemo, da bo tudi v prihodnje ostala ena izmed poglavitnih groženj za posameznike, podjetja državne organe in njihove poslovne ter delovne procese. Nenazadnje ima vse omenjeno tudi negativne učinke na varnost države.

Izkušnje iz druge polovice leta 2024 so pokazale, da se geopolitične napetosti in oboroženi konflikti po svetu še naprej odražajo v kibernetskem prostoru Republike Slovenije. Tako so imele določene odločitve ali stališča Republike Slovenije, na primer vezane na podporo Ukrajini, vpliv na kibernetsko varnost Republike Slovenije. V zadnjem polletju 2024 velja v tem kontekstu izpostaviti napoved posamezne zlonamerne skupine o izvedbi napadov na slovenske vladne spletne strani, ki je bila posledica dosedanje podpore Republike Slovenije Ukrajini. Skladno s tem in upoštevaje neprestano spreminjajoče kibernetsko varnostno okolje, ki ga zaznamuje porast kibernetskih groženj in incidentov,

se zato zahteva večja budnost in odzivnost. V tem obdobju je posebej odmeval kibernetski incident z uporabo izsiljevalske programske opreme (ransomware) v raziskovalno-izobraževalnem sektorju, ki je bil obravnavan kot težji incident.

Stopnja kibernetske ogroženosti na ravni EU ostaja na srednji ravni, zaradi realnih možnosti kibernetskih incidentov na pomembne in bistvene subjekte ter organe državne uprave. Države članice so ciljane s strani kibernetskih kriminalcev, državno povezanih akterjev in hektivistov, ki izkazujejo zmožnosti izboljševanja in posodabljanja svojih taktik, tehnik in procedur (TTPs) in nabora orodij za izvajanje zlonamernih kampanj. Zadnji srednjeročni in dolgoročni obeti nakazujejo, da bodo državno povezani akterji še naprej ciljali države članice in vladne institucije preko uporabe kampanj kibernetskega vohunjenja. Izkoriščanje orodij umetne inteligence s strani državno povezanih akterjev postaja nova normalnost, predvsem v kontekstu informacijskih operacij, ki bodo skušale vplivati na volilne procese držav članic.

URSIV je v sodelovanju z drugimi organi in mednarodnimi organizacijami pozorno spremljal situacijo na področju informacijske in kibernetske varnosti Republike Slovenije, v državah članicah Evropske unije ter širše. Med drugim je poleg rednih koordinacijskih in drugih aktivnosti na nacionalni ravni URSIV podpiral napore ozaveščanja ter krepitve informacijske in kibernetske varnosti v Republiki Sloveniji.

PREDLOGI IN PRIPOROČILA

Ob boku vse večjim geopolitičnim napetostim in porastu konfliktov po svetu, se soočamo tudi s splošnim povečanjem tako števila kot tudi raznolikosti kibernetskih dogodkov in incidentov. Njim so tako vse bolj izpostavljeni vsi uporabniki kibernetskega prostora. Pričakovati je, da se bo trend v tem, ali celo povečanem obsegu nadaljeval tudi v prihodnje. Posledično 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/) in projekta Center za varnejši internet, ki ga izvajajo Univerza v Ljubljani Fakulteta za družbene vede, Javni zavod Arnes, Zveza prijateljev mladine Slovenije in Zavod MISSS (www.safe.si/). SI-CERT je pripravil video serijo KLIK in brezplačni tečaj Varni v pisarni.

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 več faktorske 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.