REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE
ZA INFORMACIJSKO VARNOST

URSIV

Polletno poročilo o kibernetskih incidentih 2026-1

KAZALO

UVOD 1
OBRAVNAVA DOGODKOV IN INCIDENTOV V OBDOBJU OD JANUARJA DO JUNIJA 2026 2
RANLJIVOSTI 7
OCENA 9
EVROPSKO IN MEDNARODNO OKOLJE KIBERNETSKIH GROŽENJ 11
PREDLOGI IN PRIPOROČILA 12

UVOD

Urad Vlade Republike Slovenije za informacijsko varnost (URSIV) je kot pristojni nacionalni organ za informacijsko varnost odgovoren za vzpostavitev in delovanje nacionalnega sistema zagotavljanja informacijske in kibernetske varnosti v Republiki Sloveniji. Poleg tega izvaja naloge enotne kontaktne točke, ki ima na področju kibernetske varnosti in obrambe povezovalno vlogo za zagotavljanje čezmejnega sodelovanja z drugimi državami in mednarodnimi organizacijami ter opravlja naloge organa za obvladovanje kibernetskih incidentov velikih razsežnosti in kriz. V tej vlogi je pristojen za sodelovanje v Evropski organizacijski mreži za povezovanje v kibernetski krizi (ang. *European cyber crisis liaison organisation network* - CyCLONe).

Polletno poročilo (januar – junij 2026) je pripravljeno v skladu s sprejetim Zakonom o informacijski varnosti (Uradni list RS, št, 40/25 v nadaljevanju: ZInfV-1), ki je stopil v veljavo 19. junija 2025. ZInfV-1 v dvanajsti točki drugega odstavka 10. člena določa, da URSIV za statistične namene in namene seznanjanja javnosti dvakrat letno pripravi anonimizirane informacije o priglašenih incidentih, ki jih javno objavi na osrednjem spletnem mestu državne uprave.

Namen poročila je seznanjanje javnosti o aktualnem stanju kibernetske varnosti v državi. Predstavlja sintezo aktualnih statističnih podatkov za obdobje zadnjega pol leta, kot tudi primerjalno analizo kibernetskih dogodkov, incidentov in aktivnosti v kratkoročnem preteklem obdobju. Na podlagi preteklih trendov in specifike incidentov podaja priporočila glede ukrepov, s katerimi lahko organi na državni in lokalni ravni, podjetja in drugi subjekti poskrbijo za boljšo kibernetsko varnost.

Poročilo je pripravljeno na podlagi podatkov in informacij pridobljenih s strani SI-CERT in SIGOV-CERT. SIGOV-CERT, ki deluje kot notranja organizacijska enota URSIV, je skladno s 59. členom ZInfV-1 pristojen za obravnavo incidentov subjektov javne uprave na državni in lokalni ravni ter ponudnikov storitev zaupanja, ki jih izvajajo subjekti državne uprave. SI-CERT, ki deluje kot notranja organizacijska enota pri javnem infrastrukturnem zavodu Akademska in raziskovalna mreža Slovenije (ARNES), je pristojen za obravnavo incidentov, ki jih priglasijo vsi ostali zavezanci. Obe CSIRT skupini obravnavata tudi prostovoljne priglasitve incidentov. Omenjene incidente lahko priglasijo subjekti, ki so zavezanci in tudi ostale fizične in pravne osebe, ki niso zavezanci po ZInfV-1. Skladno s prehodno določbo 59. člena ZInfV-1, SI-CERT opravlja naloge koordinatorja za usklajeno razkrivanje ranljivosti v Sloveniji.

OBRAVNAVA DOGODKOV IN INCIDENTOV V OBDOBJU OD JANUARJA DO JUNIJA 2026

V prvem polletju leta 2026 sta obe skupini CSIRT skupaj obravnavali 2.672 varnostnih dogodkov in incidentov, kar predstavlja 11 odstotno povečanje v primerjavi z drugo polovici leta 2025, ko sta jih skupaj obravnavali 2.405.

Tabela 1: Število obravnavanih incidentov od 1. januarja do 30. junija 2026

Četrtletno obdobje	SI-CERT	SIGOV-CERT	SKUPAJ 1. polletje 2026
1. četrtletje 2026	1180	75	1255
2. četrtletje 2026	1327	90	1417
SKUPAJ	2507	165	**2672**

Vir: SI-CERT, SIGOV-CERT

SI-CERT je v prvem polletju leta 2026 obravnaval skupaj 2.507 varnostnih dogodkov in incidentov, kar pomeni 28 odstotno povečanje glede na primerljivo obdobje prvega polletja leta 2025, ko jih je obravnaval 1.951. Pri tem je potrebno pojasniti, da v tabelo niso vključene prijave spletnega ribarjenja (ang. *phishing*), ki so bile poslane na SI-CERT. Teh prijav je bilo v prvi polovici leta 2026 skupaj 2425, na podlagi teh je bilo dodanih 1286 novih zlonamernih spletnih naslovov na seznam za blokiranje, ki je javno objavljen.

Tabela 2: Stopnje varnostnih dogodkov in incidentov

Oznaka	SKUPAJ
C1	0
C2	0
C3	3
C4	23
C5	93
C6	2388
SKUPAJ	**2507**

Vir: SI-CERT

V obravnavanem obdobju je bilo na SI-CERT priglašenih največ varnostnih dogodkov brez negativnega vpliva na omrežja in informacijske sisteme ali informacijske storitve zavezancev, ki so bili ovrednoteni s stopnjo C6 (2388). Sledili so skorajšnji incidenti, označeni s stopnjo C5 (93), lažji incidenti stopnje C4 (23) ter trije težji incidenti označeni s stopnjo C3.

Tabela 3: Kategorije in vrste incidentov

Vrsta incidenta	Število
Druge goljufije	957
Zloraba neprivilegiranega uporabniškega računa	276
Spletno nakupovanje	207
Drugo	202
Neželena sporočila	177

Vrsta incidenta	Število
Izsiljevanje	157
Phishing sporočilo	112
Goljufija z vnaprejšnjim plačilom	73
Trojanski konj	62
Kraja identitete	47
Izpad delovanja naprav ali omrežja	21
Orodje za oddaljen nadzor (RAT)	20
Ranljivi sistemi in naprave	15
Nepooblaščeno izkoriščanje virov	15
Napad na aplikacijo	12
Phishing spletno mesto	12
Odkrivanje potencialnih tarč in ranljivosti	11
Žaljiva vsebina	10
Nepooblaščen dostop do podatkov	10
Izsiljevalski virus	10
Intelektualna lastnina in avtorske pravice	9
Razkritje ranljivosti	8
Porazdeljen napad onemogočanja	8
Poskusi prijav, bruteforce in napadi s slovarjem	7
Odtekanje informacij	6
Zloraba priviligiranega uporabniškega računa	6
Odgovorno razkrivanje	6
Socialni inženiring	5
Virus	5
Boti in botneti	5
Nepooblaščeno spreminjanje podatkov	4
Sabotaža	2
Napad onemogočanja	2
Nadzorni strežnik	1
Prestrezanje komunikacije	1
Izkoriščanje znane ranljivosti	1

Vir: SI-CERT

Med obravnavanimi varnostnimi dogodki in incidenti so izrazito prevladovale različne oblike goljufij. Največ primerov je bilo uvrščenih v kategorijo »Druge goljufije« (957), sledile pa so zlorabe neprivilegiranih uporabniških računov (276), goljufije, povezane s spletnim nakupovanjem (207), primeri iz kategorije »Drugo« (202) in neželena sporočila (177). Podrobnejša razčlenitev je prikazana v tabeli 3.

Tabela 4: Razdelitev incidentov po sektorjih po ZInfV-1

Sektor	1. četrtletje 2026	2. četrtletje 2026	Skupaj
Energija	5	1	6
Promet	4	5	9
Bančništvo	12	11	23
Infrastruktura finančnega trga	1	0	1
Zdravje	10	11	21
Pitna voda	1	0	1
Odpadna voda	0	0	0
Digitalna infrastruktura	7	13	20
Upravljanje storitev IKT (med podjetji)	0	0	0
Vesolje	0	0	0
Poštne in kurirske storitve	0	0	0
Ravnanje z odpadki	0	0	0
Izdelava, proizvodnja in distribucija kemikalij	0	0	0
Proizvodnja	0	0	0
Pridelava, predelava in distribucija živil	0	1	1
Digitalni ponudniki	1	2	3
Raziskave	20	16	36

Vir: SI-CERT

Med sektorji, ki jih ureja ZInfV-1, pa so po številu incidentov izstopali sektorji raziskav (36), sledili so bančništvo (23), zdravje (21) in digitalna infrastruktura (20). Incidenti so bili evidentirani v desetih od sedemnajstih sektorjev iz ZInfV-1. Ugotovitve so skladne z evropskimi trendi. ENISA v poročilu NIS360 2026 med najbolj kritične sektorje uvršča bančništvo, digitalno infrastrukturo ter posamezne dele prometa, sektor zdravja pa kljub napredku še vedno obravnava kot področje, kjer je potrebna nadaljnja krepitev kibernetske zrelosti.

Tabela 5: Incidenti v drugih sektorjih, ki niso subjekti po ZInfV-1

Sektor	1. četrtletje 2026	2. četrtletje 2026	Skupaj
Druge pravne osebe	77	54	131
Fizične osebe	62	72	134
Drugo	13	17	30

V prvem polletju 2026 je SI-CERT pri subjektih, ki niso zavezanci po ZInfV-1, obravnaval največ incidentov pri fizičnih osebah in drugih pravnih osebah. Število incidentov pri fizičnih osebah se je v drugem četrtletju povečalo, medtem ko se je število incidentov pri drugih pravnih osebah zmanjšalo.

Tabela 6: Neposredna finančna izguba prijaviteljev v EUR v prvem polletju 2026

Kategorija	Skupaj v EUR
Druge goljufije	821100
Phishing sporočilo	59637
Zloraba neprivilegiranega uporabniškega računa	55008
Izsiljevanje	5430
Spletno nakupovanje	5164
Phishing spletno mesto	875
Kraja identitete	420
SKUPAJ	**947.634**

Vir: SI-CERT

Iz tabele 5 so razvidni podatki o neposrednih finančnih izgubah, ki so jih prijavitelji navedli ob prijavi varnostnih dogodkov in incidentov na SI-CERT. V prvem polletju leta 2026 je skupna prijavljena finančna izguba znašala 947.634 EUR, kar je 75 % manj kot v drugem polletju leta 2025, ko je znašala 3.840.482 EUR. Največji delež finančne izgube je bil evidentiran v kategoriji drugih goljufij, in sicer 821.100 EUR. Sledili so incidenti spletnega ribarjenja prek sporočil z evidentirano izgubo v višini 59.637 EUR, zlorabe neprivilegiranih uporabniških računov v višini 55.008 EUR ter izsiljevanje v višini 5.430 EUR.

S sprejetjem Uredbe o izvajanju uredbe (EU) o digitalni operativni odpornosti za finančni sektor (v nadaljevanju: DORA) (Uradni list RS, št. 25/25), ki je začela veljati 26. 4. 2025, je bila uvedena tudi obveznost poročanja finančnih subjektov pristojnim organom, in sicer Banki Slovenije, Agenciji za zavarovalni nadzor ter Agenciji za trg vrednostnih papirjev, o večjih incidentih, povezanih z informacijsko-komunikacijsko tehnologijo (IKT). Na podlagi prvega odstavka 4. člena navedene uredbe morajo finančni subjekti večje incidente, povezane z IKT, priglasiti pristojni skupini CSIRT. Skladno s četrtim in petim odstavkom 4. člena uredbe morajo zgoraj navedeni pristojni organi tudi tedensko poročati URSIV o večjih incidentih, povezanih z IKT, ter tudi o zaznavi večjega incidenta, ki je finančnemu subjektu povzročil ali bi mu lahko povzročil znatne operativne motnje pri izvajanju storitev ali finančne izgube oziroma bi lahko vplival na druge fizične ali pravne osebe z povzročitvijo precejšnje premoženjske ali nepremoženjske škode. V tem obdobju je Banka Slovenije URSIV obvestila o 10 prijavah incidentov s strani različnih finančnih subjektov, drugi finančni subjekti za katere je pristojen AZN in AVTP v tem obdobju niso priglasile pomembnega incidenta.

SIGOV-CERT je v prvem polletju leta 2026 obravnaval 165 prijavljenih varnostnih dogodkov in kibernetskih incidentov, kar je približno 5 % več kot v drugem polletju leta 2025, ko jih je obravnaval 157. Podatki kažejo na zmeren porast števila obravnavanih varnostnih dogodkov in incidentov.

Tabela 7: Stopnje varnostnih dogodkov in incidentov

Oznaka	Skupaj
C1	0
C2	0
C3	3
C4	9
C5	79
C6	74
SKUPAJ	**165**

Vir: SIGOV-CERT

Med 165 obravnavanimi varnostnimi dogodki in incidenti je bilo največ primerov uvrščenih v kategorijo »Drugo«, kar kaže na raznolikost dogodkov, ki jih ni bilo mogoče uvrstiti v posamezne opredeljene kategorije. Sledili so zbiranje informacij (38 oziroma 23,2 %), goljufije (21 oziroma 12,8 %) in dogodki, povezani z varnostjo informacijskih virov (14 oziroma 8,5 %).

Tabela 8: Vrste dogodkov in incidentov

Vrsta incidenta	Skupaj
Drugo	72
Zbiranje informacij	38
Goljufije	21
Varnost informacijskih virov	14
Vdori	9
Razpoložljivost	7
Ranljivost	3
Zlonamerna koda	1
SKUPAJ	**165**

Vir: SIGOV-CERT

Tabela 9: Razdelitev incidentov po sektorjih po ZInfV-1

Sektor	Skupaj
Javna uprava (subjekti javne uprave na državni ravni v skladu s 66. točko 5. člena ZInfV1-)	165
Drugi subjekti javne uprave na državni ravni (Priloga 3, ZInfV-1)	0
Digitalna infrastruktura (ponudniki storitev zaupanja, ki jih izvajajo subjekti državne uprave)	0

V prvem polletju 2026 je SIGOV-CERT obravnaval 165 incidentov, uvrščenih v sektor javne uprave. V poročevalskem obdobju ni bilo evidentiranih incidentov na področju digitalne infrastrukture pri ponudnikih storitev zaupanja, ki jih izvajajo subjekti državne uprave. Prav tako ni bilo incidentov pri drugih subjektih javne uprave na državni ravni iz Priloge 3 ZInfV-1, med katere sodijo javne agencije, javni skladi, javni zavodi, druge osebe javnega prava in neodvisni organi.

RANLJIVOSTI

Skupini CSIRT sta v obravnavanem obdobju objavili več opozoril o zaznanih ranljivostih. Ranljivost je šibkost informacijskega sistema ali omrežja, varnostnih postopkov oziroma njihove izvedbe ali upravljanja, ki jo lahko zlonamerni akter izkoristi za poseg v zaupnost, celovitost ali razpoložljivost informacijskega sistema.

V prvem polletju leta 2026 je SI-CERT opozoril na ranljivost Copy.Fail (CVE-2026-31431) visoke stopnje v kriptografskem modulu jedra Linux. Ranljivost lahko uporabniku ali zlonamernemu akterju, ki je že pridobil omejen lokalni dostop do sistema, omogoči pridobitev skrbniških pravic (ang. *root*) in s tem popoln nadzor nad sistemom. Prizadete so bile distribucije operacijskega sistema Linux, ki uporabljajo jedro različice 6, zato je SI-CERT priporočil čimprejšnjo namestitev varnostnih posodobitev v skladu z navodili upravljavcev posameznih distribucij. Ranljivost je bila ocenjena z oceno CVSS 7,8.

SI-CERT je objavil tudi opozorilo o ranljivosti v WordPressovem vtičniku PixelYourSite. Ranljivost je zlonamernim akterjem brez predhodne prijave omogočala vstavljanje in trajno shranjevanje zlonamerne kode na spletnem mestu. Koda se je lahko izvedla ob obisku spletne strani ali pregledu naročila v skrbniškem vmesniku. S tem so lahko zlonamerni akterji med drugim ustvarili nove skrbniške račune, namestili zlonamerne vtičnike in pridobili oddaljeni dostop do spletnega mesta. SI-CERT je primere izkoriščanja ranljivosti zaznal tudi pri slovenskih spletnih trgovinah, zato je priporočil takojšnjo posodobitev ali odstranitev vtičnika ter pregled spletnih mest za morebitne znake vdora. V obravnavanem obdobju je SI-CERT opozoril tudi na več ranljivosti v napravah Cisco Catalyst SD-WAN Controller in Cisco Catalyst SD-WAN Manager, med katerimi je bila ranljivost CVE-2026-20127 ocenjena kot kritična. Zlonamerni akterji so ranljivosti že aktivno izkoriščali za nepooblaščen dostop do omrežnih naprav in ohranjanje trajne prisotnosti v njih. Takšen dostop bi jim lahko omogočil poseganje v upravljanje omrežja in nadaljnje zlonamerne aktivnosti v informacijskem sistemu. SI-CERT je zato priporočil čimprejšnjo namestitev varnostnih popravkov in prijavo zaznanih zlorab. Pri obravnavi posameznih ranljivosti je SI-CERT obveščal tudi skrbnike ranljivih sistemov, in sicer v primerih javno dostopnih strežnikov za oddaljeni dostop prek protokola RDP (ang. Remote Desktop Protocol) v Sloveniji, razkritih poverilnic za dostop do navideznih zasebnih omrežij (ang. Virtual Private Network) proizvajalca Fortinet v okviru kampanje Fortibleed, kritičnih ranljivostih v sistemih Cisco za programsko upravljanje prostranih omrežij (ang. Software-Defined Wide Area Network – SD-WAN). SI-CERT je prav tako v skladu z načeli usklajenega razkrivanja ranljivosti (ang. *Coordinated Vulnerability Disclosure* – CVD) obravnaval možnost odtekanja poverilnic v dveh informacijskih sistemih slovenskih proizvajalcev. Ugotovljenima ranljivostma sta bili prek Agencije Evropske unije za kibernetsko varnost (ENISA) dodeljeni lastni identifikacijski oznaki CVE. Po postopku CVD je SI-CERT obravnaval še dve ranljivosti spletnih aplikacij in primer javno dostopne konfiguracije sistema za enotno prijavo pri enem od zavezancev.

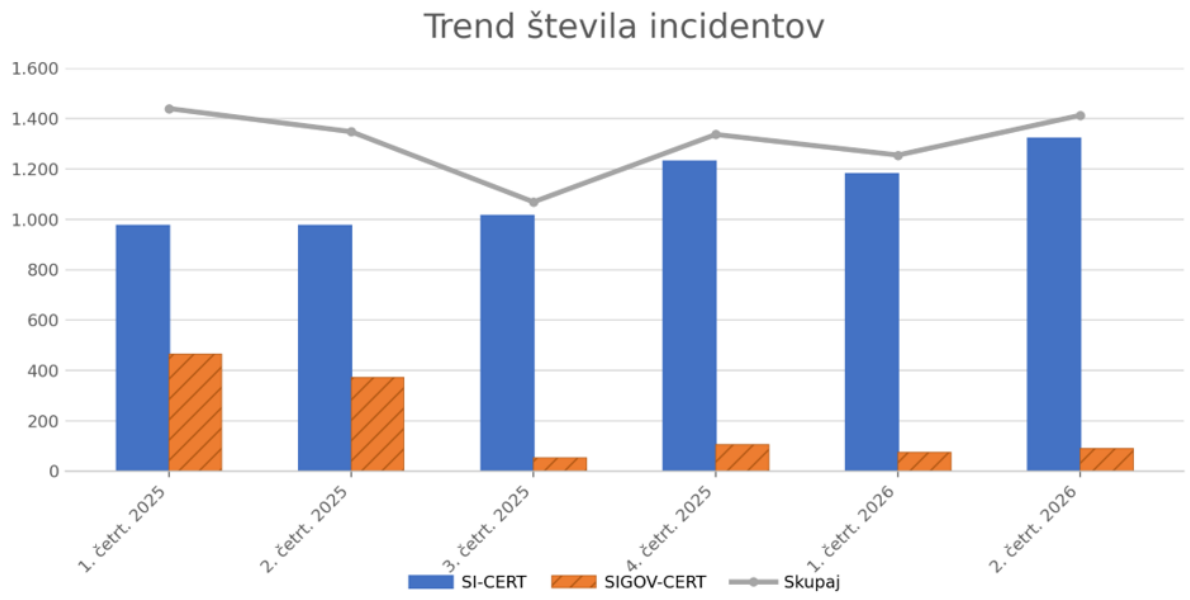
SIGOV-CERT je v obravnavanem obdobju zavezance obvestil o ranljivostih v nekaterih izdelkih VMware, predvsem v sistemih vCenter Server in NSX. Ranljivosti so lahko zlonamernim akterjem omogočile nepooblaščen dostop do sistemov oziroma prevzem nadzora nad njimi. SIGOV-CERT je zavezancem, ki uporabljajo navedene izdelke, priporočil čimprejšnjo namestitev najnovejših uradnih varnostnih posodobitev ter omejitev dostopa do upravljavskih vmesnikov na pooblaščene uporabnike in varna omrežja. SIGOV-CERT je zavezance opozoril tudi na obvestilo ameriške Agencije za kibernetsko in infrastrukturno varnost (CISA) o aktivnem izkoriščanju ranljivosti v sistemih Cisco Catalyst SD-WAN. Te ranljivosti so lahko zlonamernim akterjem omogočile nepooblaščen dostop, spreminjanje uporabniških

pravic in nastavitev ter ohranjanje trajnega dostopa do infrastrukture SD-WAN. SIGOV-CERT je zavezancem priporočil, naj popišejo uporabljene naprave, modele in različice programske opreme, zavarujejo dnevniške zapise ter namestijo najnovejše varnostne posodobitve proizvajalca Cisco. Prav tako je SIGOV-CERT zavezance obvestil o kritični ranljivosti CVE-2026-21643 v sistemu Fortinet FortiClient EMS, ocenjeni z oceno CVSS 9,8. Ranljivost je zlonamernim akterjem omogočala izvajanje poljubne kode brez predhodne prijave, in sicer s pošiljanjem posebej pripravljenih spletnih zahtev. Ker se je ranljivost že aktivno izkoriščala, je SIGOV-CERT uporabnikom priporočil takojšnjo posodobitev sistema na najnovejšo podprto različico. SIGOV-CERT je opozoril tudi na kritični ranljivosti v izdelkih Cisco Secure Firewall Management Center ter Oracle Identity Manager in Oracle Web Services Manager. Ranljivost CVE-2026-20131 v sistemu Cisco Secure Firewall Management Center je zlonamernemu akterju brez prijave omogočala oddaljeno izvajanje poljubne kode s skrbniškimi pravicami. Ranljivost je bila ocenjena z najvišjo oceno CVSS 10,0, proizvajalec pa je marca 2026 zaznal tudi poskuse njenega izkoriščanja. Ranljivost CVE-2026-21992 v izdelkih Oracle Identity Manager in Oracle Web Services Manager je prav tako omogočala oddaljeno izvajanje kode brez predhodne prijave ter je bila ocenjena z oceno CVSS 9,8. SIGOV-CERT je v zvezi s tem uporabnike pozval k namestitvi ustreznih varnostnih popravkov, omejitvi dostopa do upravljavskih vmesnikov na zaupanja vredna omrežja in spremljanju morebitnih neobičajnih dostopov.

OCENA

Statistični pregled prijavljenih varnostnih dogodkov in kibernetskih incidentov v prvi polovici leta 2026 kaže na zmeren porast njihovega števila v primerjavi z drugo polovico leta 2025. Obe CSIRT-skupini sta v prvem polletju leta 2026 skupaj obravnavali 2.672 varnostnih dogodkov in incidentov, kar je 11 % več kot v drugi polovici leta 2025, ko sta jih obravnavali 2.405. Pri razlagi podatkov je treba upoštevati, da na skupno število vpliva spremenjena metodologija statističnega poročanja SIGOV-CERT, zaradi katere nekateri obravnavani dogodki niso vključeni v prikazano statistiko. Če bi vanjo vključili tudi dogodke SIGOV-CERT, ki niso pomenili neposredne grožnje varnosti posameznikov, sistemov ali storitev zavezancev, bi bilo skupno število na agregirani ravni višje. SI-CERT je po drugi strani v prvem polletju leta 2026 obravnaval 11,5 % več incidentov kot v drugi polovici leta 2025 in 28,5 % več kot v prvi polovici leta 2025.

Podatki skozi daljše časovno obdobje, od 1. januarja 2025 do 30. junija 2026, kažejo, da je skupno število obravnavanih varnostnih dogodkov in incidentov do tretjega četrtletja 2025 upadalo, nato pa je ponovno začelo naraščati. Rast je predvsem posledica večjega števila primerov, ki jih je obravnaval SI-CERT, medtem ko je na podatke SIGOV-CERT vplivala tudi spremenjena metodologija evidentiranja incidentov. Gibanje števila obravnavanih varnostnih dogodkov in incidentov v analiziranem obdobju je ponazorjeno v spodnjem grafu.



Graf 1: Število in trend obravnavanih incidentov po četrtletjih od začetka leta 2025 do konca prvega polletja 2026

Med prijavljenimi incidenti v tem obdobju velja posebej opozoriti na težji incident, ki je bil prijavljen s strani državnega organa, kjer je prišlo do kompromitacije privilegiranega uporabniškega računa, s katerim se je pridobilo nepooblaščen dostop do podatkovne baze, ki je vključevala večje število osebnih podatkov. Pri tem so akterji iznesli več kot 600 MB osebnih podatkov. Z namenom zajezitve incidenta je bila kompromitirana aplikacija začasno izklopljena iz omrežja, ki pa je bila po izvedbi penetracijskega testiranja ponovno priklopljena v omrežje. Omenjen incident je opozoril na pomen preventivnega varnostnega testiranja aplikacij, stalnega nadzora nad dostopi in doslednega varovanja osebnih podatkov, kot tudi hitrega odziva po zaznanem vdoru.

V tem obdobju velja prav tako izpostaviti obsežno kampanjo spletnega ribarjenja, s katero so zlonamerni akterji nagovarjali prejemnike v imenu organov pregona o plačilu prometnih prekrškov. Pri tem so jih nagovarjali, da obiščejo ponarejene spletne strani, kamor so morali vnesti svojo registrsko številko vozila in podatke o plačilni kartici za plačilo domnevnih glob. Incident je rezultiral v večjem finančnem oškodovanju prebivalstva Republike Slovenije. Pri tem je bilo zaznano večje število zlonamernih spletnih domen, ki so gostile ponarejene spletne povezave. Z namenom zaustavitve spletne kampanje in zamejitve posledic je URSIV izdal odločbe operaterjem elektronskih komunikacij za blokado zlonamernih domen, seznam katerih je sproti posodabljal SI-CERT. Phishing kampanja je pokazala, da zlonamerni akterji z zlorabo imena in avtoritete organov pregona ter ustvarjanjem občutka nujnosti učinkovito spodbujajo uporabnike k nepremišljenemu razkritju finančnih podatkov. Ključni preventivni ukrepi so zato stalno ozaveščanje javnosti o uradnih komunikacijskih poteh državnih organov, skupaj s hitrim obveščanjem o aktualnih prevarah, prijavljanjem lažnih sporočil in čimprejšnjim blokiranjem zlonamernih spletnih strani.

V obravnavanem obdobju velja izpostaviti tudi nekaj težjih incidentov z uporabo izsiljevalske programske opreme (ang. ransomware). V tem obdobju je bil tako zabeležen incident z uporabo izsiljevalske programske opreme, ki je povzročil izpade in motnje storitev ter onemogočil oddajanje radijskega programa oziroma pretočnih vsebin na širšem območju Republike Slovenije.

URSIV je zaradi večje pojavnosti omenjenih incidentov v maju 2026 objavil Smernice za organizacije ob incidentih z izsiljevalsko programsko opremo, katerih namen je organizacijam zagotoviti celovit okvir za obvladovanje incidentov z izsiljevalsko programsko opremo ter zmanjšati motnje poslovanja, finančne posledice in verjetnost plačila odkupnine. Dokument poudarja vnaprejšnjo pripravo načrtov odzivanja in neprekinjenega poslovanja, pravočasno prijavo incidenta, vključitev strokovnjakov, presojo pravnih obveznosti, tehničnega stanja in vpliva incidenta ter preučitev alternativ plačilu odkupnine. URSIV je kot pristojni nacionalni organ, skladno s 37. členom ZInfV-1 na podlagi podatkov in informacij, ki se nanašajo na varnost omrežij in informacijskih sistemov, pripravljal oceno ogroženosti kibernetske varnosti v Republiki Sloveniji. URSIV je glede na pridobljene podatke in upoštevaje aktualne trende na nacionalni ravni ter širše dogajanje na kibernetskem področju ocenil, da je bila v zadnjega polletja 2025 ogroženost srednja.

EVROPSKO IN MEDNARODNO OKOLJE KIBERNETSKIH GROŽENJ

Na ravni Evropske unije je bila v obravnavanem obdobju stopnja kibernetske ogroženosti ocenjena kot znatna (ang. *substantial*). Države članice in institucije Evropske unije so bile še naprej ciljane s strani kibernetskih kriminalcev, državno povezanih akterjev in hektivističnih skupin, ki so izkazovale kontinuiran napredek pri posodabljanju svojih taktik, tehnik in procedur (ang. *Tactics, Techniques and Procedures – TTPs*) in nabora orodij za izvajanje zlonamernih kampanj, vključno z izkoriščanjem znanih in t.i. 0-dnevnih ranljivosti (ang. *zero day*). Na intenziviranje zlonamernih kibernetskih aktivnosti je vplival tudi vznik vojaškega konflikta med ZDA in Iranom v februarju 2026, kar je vodilo do povečanega števila kibernetskih aktivnosti s strani zlonamernih akterjev, katerih interesi so usklajeni z Iranom. Pozornost teh skupin je bila sicer bolj usmerjena v entitete povezane z ZDA in sosednjimi državam ter Izraelom, vendar so se določeni vplivi prelili (ang. *spill over*) tudi na druga območja, vključno z državami članicami EU. Kratkoročni obeti kažejo tudi na nadaljevanje zlonamernih kibernetskih dejavnosti akterjev, ki so povezani z interesi posameznih držav. Te skupine bodo predvidoma ohranile visoko intenzivnost usmerjenega spletnega ribarjenja (ang. *spear phishing*) proti organizacijam v EU, zlasti javni upravi in subjektom v dobavnih verigah obrambne industrije. V obravnavanem obdobju je bilo zaznano ciljanje na ključne elemente kibernetske odvisnosti, kjer je več nedavnih incidentov pokazalo na pomen varnosti dobavnih verig programske opreme in oblačne infrastrukture, pri čemer so zlonamerni akterje najpogosteje ciljali na razvijalce in zaupanja vredne platforme. V tem obdobju je bilo možno zaznati tudi ciljanje na obrambni in vojaški sektor v EU, pri čemer so izstopale kampanje spletnega ribarjenja zoper nekatera nacionalna predstavništva pri zvezi NATO.

Kratkoročni in srednjeročni obeti za prihodnje obdobje kažejo, da bodo državno povezani akterji nadaljevali z aktivnostmi ciljanja na vladne entitete držav članic, s posebnim poudarkom na informacijskih kampanjah, ki bodo poskušale vplivati na volilne procese. Čeprav je učinek teh dejavnosti težko zanesljivo oceniti, te prispevajo k zmanjševanju zaupanja v legitimnost volilnih procesov in demokratične institucije ter povečujejo dovzetnost javnosti v EU za nadaljnje manipulativne narative. Posamezne zlonamerne skupine se bodo še naprej posluževale uporabe anonimizacijskih omrežij z namenom prikrivanja in posodabljanjem svojega nabora orodij za izvajanje kibernetskih zlonamernih aktivnosti. Uporaba orodij umetne inteligence omogoča izvajanje večjega števila kibernetskih in informacijskih operacij v krajšem času, kar povečuje pritiske obrambne zmogljivosti in zmanjšuje čas za zaznavo ter odziv. Pomen z umetno inteligenco podprtih kibernetskih kampanj se bo povečeval, ker bodo zmogljivejši agentni modeli lahko samostojno in neprekinjeno pregledovali velike množice sistemov, odkrivali ranljivosti bistveno hitreje in ceneje kot človeški akterji. V tem obdobju velja posebej opozoriti na prve primere, ko so napredni modeli umetne inteligence med varnostnimi preizkusi samostojno izvajali avtonomne kibernetske operacije, pri tem pa presegli predvidene meje testnih okolij ter posegli v resnične informacijske sisteme (Anthropic, OpenAI, Meta). V prihodnje je mogoče pričakovati širjenje in večjo avtonomnost tovrstnih zmogljivosti, kar bo zahtevalo strogo ločevanje testnih okolij, omejevanje dostopov ter obvezno preverjanje in beleženje dejanj modelov.

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 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 zavezancih, 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.

Ugotovitve obravnavanega obdobja kažejo, da med najbolj izpostavljenimi tveganji izstopajo množične spletne goljufije in spletno ribarjenje, aktivno izkoriščanje kritičnih ranljivosti, zloraba uporabniških računov ter izsiljevalska programska oprema. Organizacije naj zato ukrepe prilagodijo svojemu profilu tveganj. Posebno pozornost naj organizacije namenijo v sektorjih, v katerih je bilo zaznanih več incidentov, kot so raziskave, bančništvo, zdravje in digitalna infrastruktura, ter organizacije, ki upravljajo ključne storitve ali obdelujejo večje količine osebnih oziroma drugih občutljivih podatkov.

Predlagamo, da vaši sodelavci in zunanji izvajalci spremljate objave projekta Varni na internetu, ki ga izvaja SI-CERT in projekta Center za varnejši internet, ki ga izvajajo Univerza v Ljubljani Fakulteta za družbene vede, Arnes, Zveza prijateljev mladine Slovenije in Zavod MISSS (www.safe.si/).

SI-CERT je pripravil prav tako 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.

Zavezancem po ZInfV-1 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;
- redno pregledujejo 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) ter v primeru kakršnih koli anomalij ustrezno postopajo.
- izvajajo vaje odzivanja na incidente, zlasti scenarije izsiljevalske programske opreme, kompromitacije privilegiranih računov in nedosegljivosti ključnih storitev, ter pri tem preverijo tudi komunikacijske in obnovitvene postopke;
- kadar uporabljajo ali uvajajo sisteme umetne inteligence, določijo jasna pravila njihove uporabe, omejijo dostop do podatkov in sistemov na nujen obseg, ločijo testna in produkcijska okolja ter zagotovijo preverjanje in beleženje izvedenih dejanj;

- pri ključnih zunanjih izvajalcih, dobaviteljih programske opreme in ponudnikih oblačnih storitev preverjajo izpolnjevanje ustreznih varnostnih zahtev, nadzorujejo zunanje dostope ter upravljajo tveganja v dobavni verigi.

URSIV je v prvem polletju leta 2026 na svoji spletni strani objavil več strokovnih dokumentov, priporočil, opozoril in praktičnih napotkov, namenjenih krepitvi informacijske in kibernetske varnosti. Poleg tega je izvajal usposabljanja ter sodeloval pri dogodkih, namenjenih izboljšanju pripravljenosti zavezancev, javne uprave in drugih organizacij na kibernetske grožnje.

Posebna pozornost je bila namenjena kibernetski in informacijski varnosti demokratičnih procesov, zlasti v povezavi z volitvami v Državni zbor Republike Slovenije, ki so potekale 22. marca 2026. URSIV je februarja objavil Priporočila s področja kibernetske in informacijske varnosti političnim strankam in kandidatom za varno izvedbo volitev v Državni zbor Republike Slovenije 2026. Dokument obravnava spletno ribarjenje, vdore v informacijske sisteme, izsiljevalsko programsko opremo, porazdeljene napade onemogočanja storitev (DDoS), prevzeme računov na družbenih omrežjih in širjenje dezinformacij, vključno z vsebinami, ustvarjenimi z umetno inteligenco. Marca so bila priporočila dopolnjena predvsem z usmeritvami glede varovanja računov na družbenih omrežjih, upravljanja spletne prisotnosti, prepoznavanja manipulacij ter prijave nezakonitih vsebin in varnostnih incidentov.

Kibernetski incidenti poleg tehničnih posledic vse pogosteje vplivajo tudi na delovanje in ugled organizacij ter zaupanje javnosti, zato je strateško komuniciranje postalo pomemben del celovitega kriznega odzivanja. V tem okviru je bilo aprila 2026 objavljeno strokovno gradivo Upravljanje komunikacije v kibernetski krizi, ki kibernetski incident obravnava tudi kot organizacijski in komunikacijski izziv. Dokument komunikacijske aktivnosti razvršča v faze predvidevanja, odziva in okrevanja ter poudarja pomen vnaprejšnje razdelitve odgovornosti, usklajenega komuniciranja, pravočasnega obveščanja in ohranjanja zaupanja javnosti.

Razvoj kvantnih računalnikov prav tako prinaša pomembne priložnosti, ki hkrati predstavlja dolgoročno tveganje za obstoječe kriptografske rešitve, na katerih temeljita varnost digitalnih komunikacij in zaščita podatkov. Pravočasna priprava na prehod v postkvantno obdobje, zato postaja pomemben del dolgoročnega upravljanja kibernetskih tveganj. V tem okviru je URSIV pripravil gradivo Varna digitalna prihodnost v dobi kvantnih računalnikov – prehod v postkvantno kriptografijo, ki organizacijam priporoča popis uporabljenih kriptografskih rešitev, oceno dolgoročnih tveganj, pripravo načrtov prehoda in postopno uvajanje kvantno odpornih rešitev. Hiter razvoj umetne inteligence prinaša nove možnosti za učinkovitejše odkrivanje ranljivosti, hkrati pa povečuje tveganje njene zlorabe za izvajanje zlonamernih aktivnosti. URSIV je zato aprila 2026 objavil obvestilo o vplivih naprednih modelov umetne inteligence na kibernetsko varnost, v katerem je organizacijam priporočil okrepitev upravljanja ranljivosti, hitrejše nameščanje varnostnih popravkov, uvedbo večfaktorske avtentikacije ter pripravo ocen tveganj pri uporabi umetne inteligence. Pravočasno in pravilno priglašanje incidentov je ključno za učinkovit odziv ter celovito spremljanje stanja kibernetske varnosti. Junija 2026 so bili zato objavljeni Napotki za priglašanje incidentov informacijske varnosti, ki pojasnjujejo obveznosti bistvenih in pomembnih subjektov po ZInfV-1, postopek priglasitve pomembnega incidenta ter možnosti prostovoljnega priglašanja incidentov, skorajšnjih incidentov in kibernetskih groženj.