REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE
ZA INFORMACIJSKO VARNOST

URSIV

Številka: 386-23/2025-1544-7

Datum: 17. 3. 2026

Polletno poročilo o kibernetskih incidentih, 2025-2

Marec 2026

KAZALO

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, 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 (julij – december 2025) 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 tudi 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 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 JULIJA DO DECEMBRA 2025

V drugem polletju leta 2025 sta oba odzivna centra skupaj obravnavala 2405 varnostnih dogodkov in incidentov, kar predstavlja manjši vpad (okoli pet odstotni) glede na prvo polovico leta 2025, ko je bilo zabeleženih 2546 dogodkov in incidentov. Omenjen statistični padec števila incidentov je posledica predvsem spremenjene metodologije SIGOV-CERT, kjer incidenti, ki niso predstavljali neposredne grožnje za varnost posameznikov, sistemov in storitev zavezancev niso bili vključeni v statistični pregled. Vrh polletnih prijav dogodkov in incidentov je bil dosežen v četrtem četrtletju 2025 (oktober, november in december), medtem ko je bilo v tretjem četrtletju 2025 zabeleženo nižje število incidentov.

Tabela 1: Število obravnavanih incidentov od 1. julija do 31. decembra

Mesec	SI-CERT	SIGOV-CERT	SKUPAJ 2. polletje 2025
julij 2025	338	17	355
avgust 2025	358	13	371
september 2025	319	23	342
oktober 2025	428	32	460
november 2025	412	25	437
december 2025	393	47	439
SKUPAJ	2248	157	**2405**

Vir: SI-CERT, SIGOV-CERT

SI-CERT je v prvem polletju obravnaval skupaj 2248 varnostnih dogodkov in incidentov, kar predstavlja porast števila incidentov v primerjavi s prvim polletjem 2025, ko jih je bilo obravnavanih 1951. Pri tem je potrebno pojasniti, da v tabelo niso vključeni incidenti spletnega ribarjenja (ang. *phishing*), ki so bili prijavljeni na SI-CERT in niso imeli zelo omejen negativen učinek. Skupno število teh incidentov je znašalo 2198.

Tabela 2: Stopnje varnostnih dogodkov in incidentov

Oznaka	3. četrtletje 2025	4. četrtletje 2025	SKUPAJ
C1	0	0	0
C2	0	0	0
C3	0	2	2
C4	7	5	12
C5	48	51	99
C6	960	1175	2135
SKUPAJ	1015	1233	**2248**

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 (2135). Sledili so skorajšnji incidenti, označeni s stopnjo C5 (99), lažji incidenti stopnje C4 (12) ter dva težja incidenta označena s stopnjo C3.

Tabela 3: Kategorije in vrste incidentov

Vrsta incidenta	Število
Druge goljufije	826
Izsiljevanje	268
Spletno nakupovanje	228
Zloraba neprivilegiranega uporabniškega računa	190
Drugo	169
Neželena sporočila	116
Trojanski konj	91
Phishing sporočilo	59
Goljufija z vnaprejšnjim plačilom	56
Kraja identitete	33
Nepooblaščeno izkoriščanje virov	27
Ranljivi sistemi in naprave	17
Izsiljevalski virus	15
Odkrivanje potencialnih tarč in ranljivosti (skeniranje)	15
Nepooblaščeno spreminjanje podatkov	14
Orodje za oddaljen nadzor (RAT)	14
Nepooblaščen dostop do podatkov	12
Virus	11
Intelektualna lastnina in avtorske pravice	11
Phishing spletno mesto	11
Napad na aplikacijo	8
Porazdeljen napad onemogočanja	7
Izpad delovanja naprav ali omrežja	7
Žaljiva vsebina	7
Razkritje ranljivosti	5
Nasilna vsebina	4
Odtekanje informacij	4
Poskusi prijav, bruteforce in napadi s slovarjem	4
Izkoriščanje znane ranljivosti	3
Zloraba priviligiranega uporabniškega računa	3
Namenjeno testom	2
Črv	2
Odgovorno razkrivanje	2
Socialni inženiring	2
Boti in botneti	1
Napad onemogočanja	1
Prestrezanje komunikacije	1

Vir: SI-CERT

Med varnostnimi dogodki in incidenti so prevladovale različne oblike spletnih goljufij. Statistični podatki za obravnavano obdobje poleg navedenih primerov izpostavljajo tudi incidente izsiljevanja, goljufij pri spletnem nakupovanju ter zlorab neprivilegiranih uporabniških računov, kot je prikazano v tabeli 3.

Tabela 4: Razdelitev incidentov po sektorjih

Sektor	3. četrtletje 2025	4. četrtletje 2025	Skupaj
Energija	3	7	10
Promet	3	1	4
Bančništvo	0	1	1
Infrastruktura finančnih trgov	1	0	1
Zdravje	8	5	13
Pitna voda	0	0	0
Odpadna voda	0	0	0
Digitalna infrastruktura	2	3	5
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
Pridelava, predelava in distribucija hrane	1	0	1
Proizvodnja	0	0	0
Digitalni ponudniki	0	0	0
Raziskave	15	19	34
Druge pravne osebe	89	124	213
Fizične osebe	56	61	117
Drugo	9	13	22

Vir: SI-CERT

Podatki o razdelitvi incidentov po sektorjih kažejo, da so bili med najbolj prizadetimi poleg fizičnih oseb in subjektov, ki niso zavezanci po ZInfV-1, tudi sektorji raziskave, zdravje ter energija.

Tabela 5: Neposredna finančna izguba prijaviteljev v EUR v drugem polletju 2025

Kategorija	Skupaj v EUR
Druge goljufije	2662467
Nepooblaščeno izkoriščanje virov	452562
Phishing sporočilo	403528
Zloraba neprivilegiranega uporabniškega računa	132284
Nepooblaščeno spreminjanje podatkov	71908
Nepooblaščen dostop do podatkov	68700
Spletno nakupovanje	23146
Trojanski konj	18310
Odtekanje informacij	3908
Izsiljevanje	3500
Drugo	119
Neželena sporočila	50
SKUPAJ	**3.840.482**

Vir: SI-CERT

Iz tabele 5 so razvidne neposredne finančne izgube prijaviteljev različnih varnostnih dogodkov in incidentov, ki jih je zabeležil SI-CERT. V primerjavi s prvim polletjem 2025, ko je neposredna finančna izguba prijaviteljev znašala 1.207.998 EUR, je bilo v drugi polovici leta 2025 ugotovljeno povečanje skupne priglašene finančne izgube, ki je znašala 3.840.482 EUR. Največja zabeležena finančna izguba je bila ugotovljena na področju drugih goljufij, in sicer v višini 2.662.367 EUR. Posebej velja izpostaviti tudi nepooblaščeno izkoriščanje virov, ki je povzročilo škodo v višini 452.562 EUR, sporočila spletnega ribarjenja v višini 403.528 EUR ter zlorabo neprivilegiranih uporabniških računov v višini 132.284 EUR. Tudi druge finančne izgube niso zanemarljive in predstavljajo pomembno breme zlasti za mala in srednje velika podjetja ter primerljive organizacije. Ob tem velja opozoriti, da prijavitelji ob prijavi incidenta na SI-CERT podatke o finančnih izgubah razkrivajo prostovoljno, zato je lahko dejansko oškodovanje žrtev bistveno večje in posledično ne odraža celotnega obsega vse nastale škode.

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. V drugi polovici leta 2025 je SI-CERT prejel štiri priglasitve o incidentih, in eno obvestilo o uspešnem spletnem ribarjenju usmerjeno proti zaposlenemu pri zavezancu po DORA. Skladno s četrtim in petim odstavkom 4. člena uredbe morajo zgoraj navedeni pristojni organi 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. Agencija za zavarovalni nadzor (AZN) je v tem obdobju poročala o enem večjem incidentu pri enem

zavezancu, Agencija za trg vrednostnih papirjev (ATVP) pa o dveh večjih incidentih pri zavezancih iz svoje pristojnosti.

SIGOV-CERT je v drugem polletju zaznal zmanjšanje priglašenih varnostnih dogodkov in kibernetskih incidentov glede na preteklo obdobje. Skupno je bilo obravnavanih 157 varnostnih dogodkov in incidentov, kar predstavlja vpad glede na prejšnje polletno obdobje (835), kar je posledica spremenjene metodologije, kot že pojasnjeno zgoraj. V prvem četrtletju je bil priglašen en incident klasificiran s stopnjo C3, 36 incidentov stopnje C4, 12 incidentov stopnje C5 in štirje incidenti stopnje C6. V drugem četrtletju je bil priglašen en incident stopnje C3, 28 incidentov stopnje C4, 21 incidentov s stopnjo C5 ter 54 incidentov stopnje C6. Podrobnejši podatki so razvidni v spodnji tabeli.

Tabela 6: Stopnje varnostnih dogodkov in incidentov

Oznaka	3. četrtletje 2025	4. četrtletje 2025	Skupaj
C1	0	0	0
C2	0	0	0
C3	1	1	2
C4	36	28	64
C5	12	21	33
C6	4	54	58
SKUPAJ	**53**	**104**	**157**

Vir: SIGOV-CERT

Zabeležene so bile različne oblike spletnih goljufij in spletnega ribarjenja, ki ostaja najpogostejša oblika priglašenega kibernetskega incidenta zadnjega polletja pri subjektih javne uprave na državni ravni, kar je razvidno iz spodnje tabele. Poleg tega velja izpostaviti tudi incidente povezane z žaljivo zlonamerno vsebino in incidente z uporabo zlonamerne kode.

Tabela 7: Vrste dogodkov in incidentov

Vrsta incidenta	3. četrtletje 2025	4. četrtletje 2025	Skupaj
Žaljiva/zlonamerna vsebina	12	17	29
Zlonamerna koda	1	8	9
Zbiranje informacij	0	3	3
Poizkusi vdora	0	0	0
Vdori	1	1	2
Razpoložljivost	0	1	1
Varnost informacijskih virov	0	0	0
Goljufije	35	20	55
Ranljivost	0	0	0
Drugo	4	54	58
SKUPAJ	**53**	**104**	**157**

Vir: SIGOV-CERT

RANLJIVOSTI

Skupini CSIRT sta v obravnavanem obdobju 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.

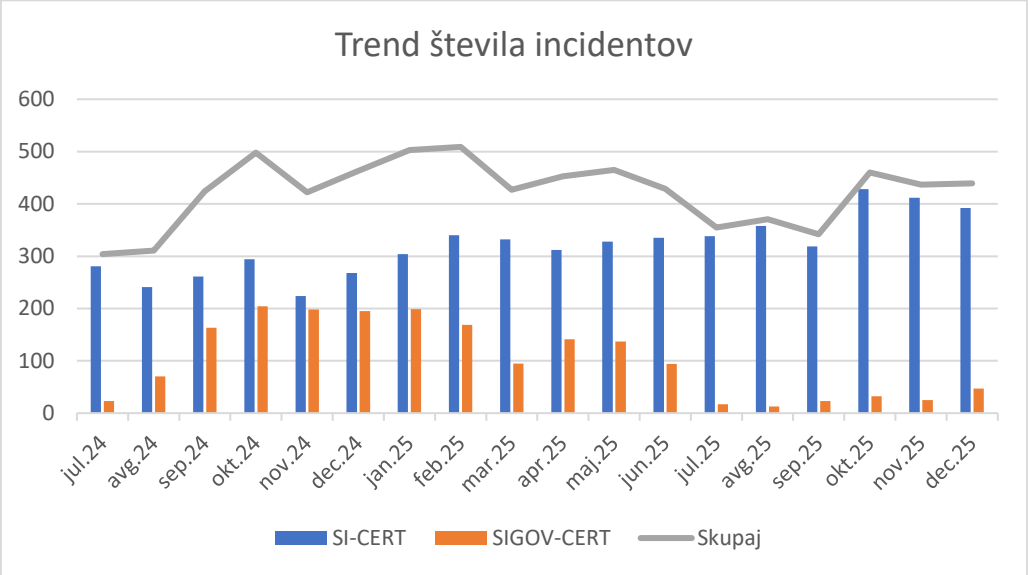
V drugem polletju 2025 je SI-CERT opozoril na obstoj kritične ranljivosti Microsoft Sharepoint. Microsoft je izdal navodila za ukrepanje zaradi SharePoint ranljivosti CVE-2025-53770, ki je omogočala izvedbo poljubne programske kode na daljavo (ang. *Remote Code Execution* - RCE). V zvezi s tem je SI-CERT izdal priporočene ukrepe, da se na omrežjih s samostojno SharePoint namestitvijo nemudoma namestijo popravki proizvajalca. SI-CERT je prav tako opozoril na obstoj več ranljivosti ASA naprav (ang. *Adaptive Security Appliances – ASA*), ki so se aktivno izkoriščale z namenom nepooblaščenega dostopa do naprav in trajne prisotnosti storilcev na napravah. V zvezi s tem se je priporočalo čimprejšnjo namestitev popravkov za omenjene ranljivosti. Ameriška agencija za kibernetsko varnost (ang. *Cybersecurity and Infrastructure Security Agency* – CISA) je naznanila, da so se ranljivosti že začele izkoriščati za pridobitev nepooblaščenega dostopa do ranljivih naprav. SI-CERT je pridobil seznam javno dostopnih ASA naprav v Sloveniji s podatkom o zadnji nadgradnji sistema, na podlagi katere je opravil obveščanje skrbnikov naprav. V zvezi s tem je izdal priporočila, da se sledi predlogom agencije CISA. SI-CERT je prav tako poročal o izpostavljenosti izvorne kode podjetja F5 Inc., kjer so zlonamerni akterji v avgustu 2025 pridobili dolgotrajen nepooblaščen dostop do nekaterih notranjih sistemov podjetja, vključno z sistemom za usmerjanje prometa do strežnikov in varnost aplikacij (BIG-IP) in platformami za upravljanje inženirskega znanja. Tekom nepooblaščenega dostopa naj bi ukradli občutljive podatke, med njimi del izvorne kode BIG-IP, in informacije o nerazkritih ranljivostih. V zvezi s tem je SI-CERT priporočil upravljavcem F5 sistemov, da nemudoma preverijo ali so nameščene najnovejše posodobitve za BIG-IP, F5OS, BIG-IQ, BIG-IP Next for Kubernetes, APM odjemalce, da zamenjajo administrativne poverilnice, omejijo dostopne skupine, vklopijo večfaktorsko avtentikacijo za upravljavske račune, omogočijo pošiljanje dogodkov v SIEM, spremljanje prijav administrativnih računov in sprememb v privilegijev, itd. V drugi polovici leta je v SI-CERT izvedel 15 posamičnih kampanj obveščanj skrbnikov sistemov z zaznanimi ranljivostmi.

SIGOV-CERT je v omenjenem obdobju obvestil zavezance o obstoju ranljivosti ničelnega dne (ang. *0-day vulnerability*) podjetja Fortinet. Gre za ranljivost Fortinet Fortiweb, ki je preko neustrezno filtriranih parametrov omogočala vbrizgavanje ukazov na nivoju operacijskega sistema (ang. *OS Command Injection*), ki je lahko avtenticiranemu zlonamernemu akterju omogočila izvajanje posebej oblikovane kode prek HTTP zahtev ali CLI ukazov. Uporabnikom rešitev Fortinet FortiWeb je bila priporočena namestitev popravkov za ranljivost kot tudi upoštevanje priporočil proizvajalcev omenjene rešitve ter izvedba posodobitev na zadnjo različico uporabljene programske opreme. Ob tem se je prav tako priporočilo, da skupaj z upravljalci Fortinet sistemov preverijo obstoj novo kreiranih neznanih uporabnikov, ki imajo povišane privilegije ali indikatorji, ki bi lahko nakazovali na izkoriščanje ranljivosti. V tem obdobju so poročali tudi o kritični ranljivosti CVE-2025-59287, ki je prizadela storitev Windows Server Update Services (WSUS) podjetja Microsoft. Slednja je zlonamernim akterjem omogočala oddaljeno izvrševanje kode brez prijave, kar bi lahko privedlo do popolne kompromitacije strežnika. SIGOV-CERT je v zvezi s tem priporočil namestitev varnostnega paketa, ki ga je Microsoft izdal kot popravek.

OCENA

Statistični pregled števila priglašenih varnostnih dogodkov in incidentov v drugi polovici leta 2025 kaže upad števila incidentov v primerjavi s prvo polovico leta 2025. Ob tem je treba pojasniti, da navedeno ni posledica zmanjšanja zlonamernih kibernetskih aktivnosti, temveč predvsem manjšega števila incidentov, ki jih je statistično poročal SIGOV-CERT zaradi uveljavitve spremenjene metodologije. Če bi v skupno statistiko vključili tudi incidente SIGOV-CERT, ki niso predstavljali neposredne grožnje za varnost posameznikov, sistemov in storitev zavezancev, bi bilo skupno število incidentov na agregirani ravni bistveno višje. Po drugi strani je SI-CERT v tem obdobju zabeležil 15-odstotno rast števila incidentov glede na prvo polovico leta 2025, v primerjavi z drugo polovico leta 2024 pa 43-odstotno povečanje.

V spodnji tabeli je prikazana primerjalna krivulja števila obravnavanih incidentov v prvi in drugi polovici leta 2025.



Graf 1: Število in trend obravnavnih incidentov v prvem in drugem polletju 2025

Med prijavljenimi incidenti v tem obdobju velja posebej opozoriti na težji incident, ki je bil priglašen konec oktobra 2025 s strani organa v sestavi enega od ministrstev, kjer je prišlo do izkoriščanja kritične varnostne ranljivosti ene izmed aplikacij. Slednje je omogočalo neavtoriziran dostop do 873.201 osebnih podatkov (ime, priimek, naslov, EMŠO in davčna številka), kar je predstavljajo največje razkritje osebnih podatkov državljanov Republike Slovenije, ki so bili s tem dodatno izpostavljeni potencialnim zlorabam. URSIV je v zvezi z incidentom zagotavljal tehnično podporo prizadetemu organu pri obvladovanju incidenta, poleg izvedbe koordinacijskih sestankov z organi kazenskega pregona in informacijskim pooblaščencem z namenom izmenjave informacij in ključnih ugotovitev za zagotovitev čimbolj učinkovite zajezitve škodljivih posledic incidenta. S tem v zvezi je URSIV izdal Priporočila za izvajanje ukrepov za preprečitev dostopa do podatkovnih zbirk, ki jih je objavil na spletni strani.

Prav tako velja izpostaviti usmerjeno phishing kampanjo zoper uporabnike storitev elektronskega bančništva, kjer je prišlo do zlorabe imena in družbe ponudnika storitev elektronskega bančništva. V tem primeru so zlonamerni akterji z lažnimi spletnimi stranmi in telefonskimi klici v slovenskem jeziku pridobivali vstopne podatke za dostop do bančnih računov in izvajali plačila, zaradi česar je nastala

večja finančna škoda. URSIV je z namenom preprečitve negativnih posledic in nastanka večje finančne škode izdal štiri odločbe operaterjem za blokado posameznih zlonamernih domen.

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.

Na ravni Evropske unije je bila v obravnavanem obdobju stopnja kibernetske ogroženosti prav tako ocenjena kot srednja (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*). Državno povezane zlonamerne skupine so še naprej izkoriščale ranljivosti v razširjeni programski opremi, kar je privedlo do obsežnih kompromitacij v vladnem in telekomunikacijskem sektorju na globalni ravni. V tem obdobju smo bili priča tudi nadaljnjim poročilom o ofenzivnih kibernetskih operacijah, usmerjenih v javno upravo in energetski sektor z izvajanjem kampanj ciljnega lažnega predstavljanja. Slednje so izkazovale visoko stopnjo tehnične prilagodljivosti, kar se je kazalo tudi v uporabi umetne inteligence (UI), ki jim je med drugim omogočala vdore v tehnološka in storitvena podjetja. Nadaljevale so se tudi kibernetsko-vohunske kampanje, usmerjene proti obrambnim in telekomunikacijskim organizacijam ter organizacijam s področij letalstva, prometa in politike.

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. 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. Na področju kibernetskega kriminala in uporabe izsiljevalske programske opreme (ang. *ransomware*), je opaziti pojav novih naprednih različic teh programov, ki postajajo dostopne vedno večjemu krogu zlonamernih akterjev. Razvoj kibernetskega kriminala kot storitev omogoča, da kompleksne operacije izvajajo tudi posamezniki, ki sami nimajo tehničnega znanja za razvoj potrebne programske opreme. Prav tako se pričakuje, da nadaljevanje hektivističnih aktivnosti v enakomernem tempu, zlasti v času nacionalnih volitev in dogodkov na ravni EU. Porazdeljeni napadi onemogočanja storitev (ang. *Distributed Denial of Service – DDoS*) bodo ostali prevladujoča taktika zlonamernih skupin.

V drugem polletnem obdobju 2025 je Evropska agencija za kibernetsko varnost (ang. *European Union Agency for Cybersecurity - ENISA*) objavila Pregled kibernetskih groženj za leto 2025 (ang. *ENISA Threat Landscape*), ki predstavlja pregled trendov in osrednjih groženj državam članicam na podlagi informacij zbranih iz odprtih virov in anonimiziranih informacij držav članic. Ključni trendi iz poročila kažejo na naraščajočo pojavnost spletnega ribarjenja. Ta se vse bolj avtomatizira z razvojem platform, ki ponujajo t. i. spletno ribarjenje kot storitev (ang. *Phishing-as-a-Service*), kar omogoča tudi manj izkušenim zlonamernim akterjem izvajanje kompleksnejših operacij. Poročilo izpostavlja tudi vse pogostejšo

zlorabo tretjih ponudnikov ter napade prek dobavnih verig. Takšni primeri vključujejo zlonamerne aktivnosti, usmerjene proti IT-ponudnikom, upravljavcem mobilnih aplikacij ter repozitorijem odprtokodne programske opreme. Mobilne naprave, zlasti naprave z operacijskim sistemom Android, ostajajo pogosta tarča zlonamernih aplikacij, kot so trojanski konji, vohunskih programov in orodij za oddaljen dostop, ki so pogosto povezana z državno podprtimi akterji.

V novembru 2025 je ENISA objavila sektorski pregled kibernetskih groženj za javno upravo (ang. *ENISA Sectoral Threat Landscape*), ki predstavlja analizo najpogostejših groženj v letu 2024. Poročilo ugotavlja, da se javne uprave držav članic EU soočajo s kibernetskimi grožnjami različnih akterjev, pri čemer je po številu incidentov najpogostejši hektivizem (ang. *hacktivism*). Ugotavlja se, da so bile hektivistične aktivnosti predvsem ideološko motivirane ter pogosto povezane z geopolitičnimi dogodki, kot je ruska agresija na Ukrajino. Posamezne zlonamerne skupine, povezane z državnimi akterji, so bile aktivne tudi v kampanjah kibernetskega vohunjenja proti javnim upravam držav članic, pri čemer so posebej ciljale na vladne institucije.

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.

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.

V drugi polovici 2025 je prišlo tudi do več primerov incidentov, pri katerih je prišlo do nepooblaščenega dostopa do podatkov oziroma njihovega razkritja. Med najpogostejšimi vzroki za te incidente se navaja neustrezno upravljanje dostopov do podatkovnih zbirk, ranljivosti v spletnih aplikacijah in informacijskih sistemih, nezadostno načrtovanje varstva podatkov že v fazi razvoja informacijskih rešitev in pomanjkljivo spremljanje in zaznavanje nepooblaščenih dostopov.

V tej luči se na podlagi dobrih praks s področja informacijske varnosti zavezancem priporoča izvajanje naslednjih ukrepov:

- dosledno izvajanje načela najmanjših privilegijev (ang. *least privilege*), kar pomeni, da imajo uporabniki dostop do zgolj tistih podatkov, ki so nujno potrebni za opravljanje njihovih nalog;
- redno izvajanje varnostnih pregledov informacijskih rešitev, testov ranljivosti in penetracijskih testov;
- pri razvoju in uvedbi novih informacijskih sistemov zagotoviti načelo varstva podatkov že v fazi načrtovanja in privzetega varstva podatkov (ang. *privacy by design and by default*);
- izvajanje izobraževanj zaposlenih o informacijski varnosti, testiranje odzivnosti zaposlenih na tehnike socialnega inženiringa in ozaveščanje o pravilnem ravnanju z osebnimi in zaupnimi podatki.

Analiza prijavljenih incidentov kaže na ponavljajoče se vzorce in vzroke varnostnih incidentov, zato v nadaljevanju predstavljamo tudi posamezne dokumente in priporočila, ki jih je URSIV pripravil z namenom podpore zavezancem pri izvajanju zahtev ZInfV-1, ki pripomorejo tudi k preventivnim aktivnostim oziroma zaščiti pred incidenti.

V decembru 2025 je bila objavljena vzorčna varnostna dokumentacija, ki je zasnovana kot pomoč predvsem malim in srednje velikim organizacijam pri izpolnjevanju zahtev ZinfV-1 in pri vzpostavljanju celovitega sistema upravljanja informacijske in kibernetske varnosti. Slednja vsebuje najpogostejše splošne in posebne varnostne politike ter ukrepe za zagotavljanje varnosti omrežnih in informacijskih sistemov. Dokumenti predstavljajo izhodiščni okvir, ki ga mora vsaka organizacija prilagoditi svoji dejanski informacijsko-komunikacijski infrastrukturi, posebnostim svojega sektorja, obsegu poslovanja, uporabi zunanjih ponudnikov storitev ter rezultatom izvedene analize obvladovanja tveganj.

URSIV je objavil tudi drugo dopolnjeno izdajo Priročnika kibernetske varnosti, ki je bila sprva objavljena marca 2025. Priročnik ponuja ključne smernice in priporočila za zaščito informacijskih sistemov pred kibernetskimi grožnjami. Namenjen je zavezancem po ZInfV-1 ter vsem organizacijam v javnem in zasebnem sektorju, ki želijo izboljšati svojo kibernetsko varnost in nasloviti varnostno kulturo. Priročnik vključuje pregled nacionalnega sistema kibernetske varnosti, pravni in mednarodni okvir, vzpostavitev

varnostnega sistema v organizacijah, odzivanje na kibernetske incidente, krizno komuniciranje ter priporočila za varno uporabo in razvoj informacijskih sistemov. Druga posodobljena izdaja priročnika je bila objavljena decembra 2025 zaradi sprejetja novega ZInfV-1.

V tem obdobju je URSIV objavil tudi posodobljeno različico pojasnil k ZInfV-1 za zavezance, ki vključuje dodatne razlage glede izvajanja zakona, predvsem na temeljnih področjih kot so opredelitve zavezancev, samo-registracija, komunikacija z organi, poročanje o incidentih in ukrepi kibernetske varnosti.

URSIV je v decembru 2025 na podlagi Uredbe o usposabljanju odgovornih oseb na področju obvladovanja tveganj informacijske in kibernetske varnosti (Uradni list RS, št. 78/25) pričel z izvajanjem usposabljanj odgovornih oseb na področju obvladovanja tveganj informacijske in kibernetske varnosti. Usposabljanja potekajo enkrat na mesec, na njih pa se odgovorne osebe seznanijo in pridobijo temeljna znanja glede zagotavljanja informacijske in kibernetske varnosti, zakonodaje, predpisov in mednarodnih standardov, upravljanje sredstev in tveganj, ocene vplivov na poslovanje in neprekinjeno poslovanje, odzivanje na incidente informacijske varnosti, varnost dobavnih verig in izvajanja dolžnega nadzorstva.