REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE
ZA INFORMACIJSKO VARNOST

URSIV

Številka: 386-23/2025-1544-6

Datum: 19. 9. 2025

Polletno poročilo o kibernetskih incidentih, 2025-1

September 2025

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).

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 in incidentih kibernetske varnosti v Republiki Sloveniji. Dotično polletno poročilo je pripravljeno še v skladu s prej omenjenim zakonom. Naslednje polletno poročilo (julij – december 2025) pa bo pripravljeno v skladu z novo sprejetim Zakonom o informacijski varnosti (Uradni list RS, št, 40/25 v nadaljevanju: ZInfV-1), ki je stopil v veljavo 19. junija 2025. Le-ta 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 kibernetskih 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 *(angl. Slovenian Computer Emergency Response Team)* in SIGOV-CERT. SI-CERT je po ZInfV pristojni nacionalni odzivni center za kibernetsko varnost za zavezance kot izvajalce bistvenih storitev 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. SIGOV-CERT 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 JANUARJA DO JUNIJA 2025

V prvem polletju leta 2025 sta oba odzivna centra skupaj obravnavala 2786 varnostnih dogodkov in incidentov, kar predstavlja okoli petnajstodstotni porast v primerjavi z drugim polletjem 2024, ko je bilo zabeleženih 2419 dogodkov in incidentov. Med njimi je bilo največ prostovoljnih priglasitev s strani fizičnih oseb in subjektov, ki niso zavezanci po ZInfV. Najbolj izpostavljeni so bili raziskovalno-izobraževalni sektor, organi državne uprave in operaterji elektronskih komunikacij. Vrh polletnih prijav dogodkov in incidentov sta predstavljala mesec januar in februar, čemur je sledil trend padanja števila incidentov z manjšimi odstopanji do konca junija.

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

Mesec	SI-CERT	SIGOV-CERT	SKUPAJ 1. polletje 2025
januar 2025	304	199	503
februar 2025	340	169	509
marec 2025	332	95	427
april 2025	312	141	453
maj 2025	328	137	465
junij 2025	335	94	429
SKUPAJ	1951	835	**2786**

Vir: SI-CERT, SIGOV-CERT

SI-CERT je v prvem polletju obravnaval skupaj 1951 varnostnih dogodkov in incidentov, kar predstavlja 24-odstotni porast števila incidentov v primerjavi z drugim polletjem 2024, ko jih je bilo obravnavanih 1569. Pri tem je potrebno pojasniti, da v tabelo niso vključeni enostavni incidenti spletnega ribarjenja (ang. *phishing*), ki so bili prijavljeni in evidentirani na SI-CERT. Skupno število teh incidentov je znašalo 3129.

Tabela 2: Stopnje varnostnih dogodkov in incidentov

Oznaka	1. četrtletje 2025	2. četrtletje 2025	SKUPAJ
C1	0	0	0
C2	0	0	0
C3	1	1	2
C4	7	8	15
C5	42	46	88
C6	926	920	1846
SKUPAJ	**976**	**975**	**1951**

Vir: SI-CERT

Med obravnavanimi incidenti, ki so bili priglašeni na SI-CERT, je bilo največ lažjih varnostnih dogodkov oziroma incidentov, ki so bili označeni s stopnjo C6 (1846). Temu so sledili lažji incidenti označeni s stopnjo C5 (88), 15 incidentov stopnje C4 in dva incidenta označena s stopnjo C3.

Tabela 3: Kategorije in vrste incidentov

Kategorija	Skupaj
Druge goljufije	691
Drugo	235
Zloraba nepriviligiranega uporabniškega računa	189
Spletno nakupovanje	165
Izsiljevanje	121
Neželena sporočila	98
Trojanski konj	76
Phishing sporočilo	51
Goljufija z vnaprejšnjim plačilom	49
Phishing spletno mesto	31
Kraja identitete	30

Nepooblaščeno izkoriščanje virov	27
Ranljivi sistemi in naprave	15
Odgovorno razkrivanje	14
Izsiljevalski virus	14
Orodje za oddaljen nadzor (RAT)	13
Žaljiva vsebina	13
Porazdeljen napad onemogočanja (DDos)	12
Razkritje ranljivosti	12
Napad na aplikacijo	11
Nepooblaščeno spreminjanje podatkov	9
Nepooblaščen dostop do podatkov	8
Virus	6
Odtekanje informacij	6
Izpad delovanja naprav in omrežja	6
Odkrivanje potencialnih tarč in ranljivosti (skeniranje)	5
Poskusi prijav, bruteforce in napadi s slovarjem	5
Zloraba privilegiranega uporabniškega računa	5
Intelektualna lastnina in avtorske pravice	5
Nasilna vsebina	2
Črv	2
Nadzorni strežnik	1
Izkoriščanje znane ranljivosti	1
Socialni inženiring	1
Napad onemogočanja	1
Boti in botneti	1

Vir: SI-CERT

Med oblikami varnostnih dogodkov in kibernetskih incidentov so prevladovale različne oblike spletnih goljufij, kar je razvidno iz tabele 3. Žrtve le-teh so predvsem fizične in druge pravne osebe, ki incidente prijavljajo na podlagi prostovoljne prijave in niso zavezanci po ZInfV-1. Statistično gledano velja v tem obdobju poleg omenjenih incidentov izpostaviti tudi zlorabo neprivilegiranih uporabniških računov, incidenti povezani s spletnim nakupovanjem, izsiljevanje in neželena sporočila.

Tabela 4: Razdelitev incidentov po sektorjih

Skupina	Sektor	1. četrtletje 2025	2. četrtletje 2025	Skupaj
NIS	Energija	3	6	9
NIS	Digitalna infrastruktura	2	6	8
NIS	Zdravstvo	3	7	10
NIS	Promet	2	1	3
NIS	Bančništvo	2	2	4
NIS	Infrastruktura finančnih trgov	0	0	0
NIS	Ponudnik spletne tržnice	0	0	0
NIS	Ponudnik računalništva v oblaku	0	1	1

NIS	Varstvo okolja	0	0	0
NIS	Preskrba s hrano	0	0	0
NIS	Oskrba s pitno vodo	1	1	2
ZInfV	Državne ustanove	12	9	21
Ostalo	Operaterji elektronskih komunikacij	6	4	10
Ostalo	Raziskovalno-izobraževalni sektor	18	20	38
Ostalo	Druge pravne osebe	77	70	144
Ostalo	Fizična oseba	42	49	91
Ostalo	Drugo	5	7	12

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 v prvem polletju 2025

Kategorija	Skupaj v EUR
Druge goljufije	928.715,00
Phishing sporočilo	161.727,00
Nepooblaščeno izkoriščanje virov	51.018,00
Zloraba neprivilegiranega uporabniškega računa	21.863,00
Virus	20.000,00
Spletno nakupovanje	16.288,00
Drugo	3.750,00
Izsiljevanje	3.292,00
Nepooblaščeno spreminjanje podatkov	640,00
Phishing spletno mesto	385,00
Goljufija z vnaprejšnjim plačilom	320,00
SKUPAJ	**1.207.998,00**

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 z drugim polletnim obdobjem 2024, ko je neposredna finančna izguba prijavitelja znašala 1.821.367,00 EUR, se ugotavlja zmanjšanje skupne priglašene finančne izgube prijaviteljev v prvi polovici leta 2025, ko je ta znašala 1.207.998,00 EUR. Največja zabeležena finančna izguba se je izkazala na področju drugih goljufij v znesku 928.715,00 EUR. Dodatna velja izpostaviti tudi finančne izgube, zaradi sporočil spletnega ribarjenja v višini 161.727,00 EUR in nepooblaščenega izkoriščanja virov v višini 51.018,00 EUR. Ob tem ostale finančne izgube prav tako niso zanemarljive in predstavljajo breme predvsem za manjša in srednje velika podjetja ter primerljive organizacije. Velja opozoriti, da prijavitelji prostovoljno razkrijejo podatke o finančnih izgubah ob

prijavi incidenta na SI-CERT, zato je oškodovanje žrtev lahko tudi bistveno večje in posledično ne predstavlja dejanskega seštevka vseh oškodovanj.

S sprejemom Uredbe o izvajanju uredbe (EU) o digitalni operativni odpornosti za finančni sektor (ang. *DORA*) (Uradni list RS, št. 25/25), ki je stopila v veljavo 26. 4. 2025, se uvaja tudi obveznost poročanja finančnih subjektov pristojnim organom (Banka Slovenije, Agencija za zavarovalni nadzor, Agencija za trg vrednostnih papirjev) o večjih incidentih povezanih z informacijsko-komunikacijsko tehnologijo (IKT). Na podlagi prvega odstavka 4. člena omenjene uredbe morajo finančni subjekti o večjih incidentih povezanih z IKT poročati tudi pristojni CSIRT skupini. SI-CERT je v letu 2024 skladno z omenjeno uredbo skupaj z omenjenimi pristojnimi organi za bančni in finančni sektor vzpostavil protokol obveščanja in ga uspešno udejanjil z nastopom veljavnosti uredbe. V prvi polovici leta je SI-CERT na tej podlagi prejel 42 obvestil o incidentih, ki pa niso bili s področja kibernetske varnosti. Skladno s četrtim in petim odstavkom 4. člena uredbe morajo omenjeni pristojni organi tedensko poročati URSIV o večjih incidentih, povezanih z IKT, kot tudi o zaznavi večjega incidenta, ki bi finančnemu subjektu povzročil, ali bi mu lahko povzročil znatne operativne motnje pri opravljanju storitev ali finančne izgube ali bi lahko vplival na druge fizične ali pravne osebe s povzročitvijo precejšnje premoženjske ali nepremoženjske škode. V omenjenem obdobju Banka Slovenije, Agencija za zavarovalni nadzor in Agencija za trg vrednostnih papirjev URSIV niso poročale o večjem incidentu povezanim z IKT.

Tabela 6: Stopnje varnostnih dogodkov in incidentov

Oznaka	1. četrtletje 2025	2. četrtletje 2025	SKUPAJ
C1	0	0	0
C2	0	0	0
C3	1	0	1
C4	0	1	1
C5	463	370	833
C6	0	0	0
SKUPAJ	464	371	**835**

Vir: SIGOV-CERT

SIGOV-CERT je v drugem polletju prav tako zaznal povečanje priglašenih varnostnih dogodkov in kibernetskih incidentov glede na preteklo obdobje. Skupno je bilo obravnavanih 835 varnostnih dogodkov in incidentov, kar predstavlja manjši porast glede na prejšnje polletno obdobje (830). V prvem četrtletju je bil priglašen en incident klasificiran s stopnjo C3, ostali incidenti so bili klasificirani s stopnjo C5. V drugem četrtletju je bil priglašen en incident stopnje C4, ostalih 370 incidentov je bilo označenih s stopnjo C5, kar je razvidno v zgornji tabeli.

Tabela 7: Vrste dogodkov in incidentov

Vrsta incidenta	1. četrtletje 2025	2. četrtletje 2025	Skupaj
Žaljiva/zlonamerna vsebina	328	275	603
Zlonamerna koda	3	6	9
Zbiranje informacij	2	1	3
Poizkusi vdora	1	5	6
Vdori	0	0	0
Razpoložljivost	0	2	2

Varnost informacijskih virov	0	0	0
Goljufije	128	82	210
Ranljivost	0	0	0
Drugo	2	0	2
SKUPAJ	464	371	**835**

Vir: SIGOV-CERT

Pri analizi vrste dogodkov in incidentov je bilo ugotovljeno, da je bila najpogostejša oblika prijavljenega incidenta uporaba žaljive oziroma zlonamerne vsebine (603). Temu so sledile različne oblike goljufij (210) in uporaba zlonamerne kode (9), kar je podrobneje prikazano v zgornji tabeli.

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 prvem polletju 2025 je SI-CERT opozoril na izrabo treh VMware ranljivosti, ki je zlonamernim akterjem omogočala, da iz virtualnega sistema (t.i. *guest*) zlorabijo gostiteljski sistem (t.i. *host hipervizor*). Po podatkih proizvajalca naj bi se ranljivosti že izrabljale v posameznih kibernetskih incidentih. Broadcom je 4. marca 2025 objavil popravke za tri ranljivosti VMware produktov, ena od teh je bila ocenjena kot kritična (CVSS 9,3). Preko izrabe teh ranljivosti bi lahko zlonamerni akter, ki predhodno pridobi administratorske pravice (Administrator, root) na enem od virtualnih sistemov, zlorabil gostiteljski sistem (t.i. VM Escape), s čemer bi lahko prišlo do zlorabe celotnega virtualiziranega okolja. Posledica tega bi lahko bila zloraba podatkov in zagon poljubne kode, kot na primer v primeru incidenta z uporabo zlonamerne programske opreme (ang. *ransomware*). Proizvajalec je na podlagi tega izdal popravke, ki odpravljajo posamezne ranljivosti. Skrbnikom sistemov se je priporočila takojšnja namestitev popravkov in obveščanje o zaznanih zlorabah ranljivosti SI-CERT.

V juniju je SI-CERT opozoril na obvestilo ameriškega Nacionalnega inštituta za standarde in tehnologijo (ang. *National Institute of Standards and Technology - NIST*) o kritični ranljivosti CVE-2025-49113 sistema Roundcube Webmail. Slednji predstavlja priljubljen odprtokodni spletni vmesnik za elektronsko pošto. Verzije pred 1.5.10 ter različice 1.6.x pred 1.6.11 so vsebovale kritično ranljivost z oznako CVE-2025-49113. Izraba ranljivosti je zlonamernim akterjem omogočala izvajanje poljubne kode na sistemu. CVSS ocena ranljivosti je bila ocenjena kot 9,9 (od maksimalno 10). Proizvajalec je na podlagi tega izdal popravke ranljivosti. SI-CERT je skrbnikom sistema svetoval takojšnjo nadgradnjo sistema in obveščanje v primeru zaznave izrabe ranljivosti.

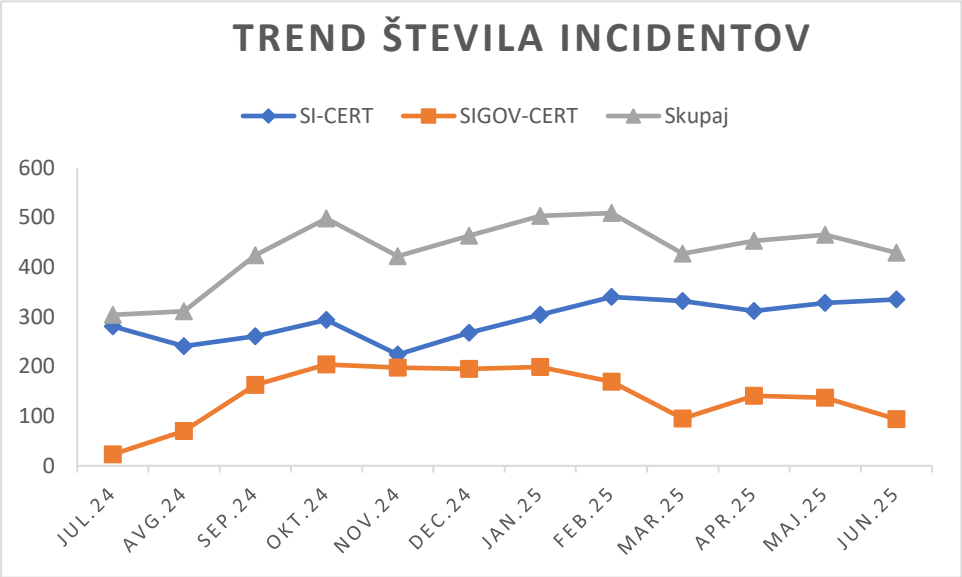
SIGOV-CERT je v omenjenem obdobju obvestil o aktivnem izkoriščanju ranljivosti v Ivanti EPMM (Endpoint and Policy Management), ki organizacijam omogoča upravljanje mobilnih naprav na način, da lahko podjetje preko njega nadzoruje varnost, aplikacije in nastavitve na službenih telefonih in drugih napravah. V zvezi s tem je bila priporočena izvedba začasnih ukrepov preprečitve dostopa do EPMM API in spremljanje dnevniških zapisov za morebitne anomalije. Ivanti je v zvezi z ranljivostjo izdal ustrezne popravke[1].

Prav tako je SIGOV-CERT v omenjenem obdobju opozoril na objavo kritične ranljivosti v navezavi s produkti podjetja Fortinet, in sicer FortiOS in FortiProxy. Ranljivost CVE-2024-55591 omogoča, da zlonamerni akter zaobide avtentikacijo z uporabo alternativne poti ali kanala (CWE-288). (https://nvd.nist.gov/vuln/detail/CVE-2024-55591) (https://app.opencve.io/cve/CVE-2024-55591) in pridobitve privilegiranih uporabniških pravic s pomočjo posebej oblikovanih zahtevkov do modula websocket v Node.js (https://nvd.nist.gov/vuln/detail/CVE-2024-55591). V zvezi z ranljivostjo so bila izdana priporočila za posodobitev programske opreme FortiOS na verzijo 7.0.17 ali novejšo ter FortiProxy na verzijo 7.0.20 ali 7.2.13 ali novejšo, uporaba varnostnih popravkov proizvajalca in spremljanje varnostnih opozoril.

[1] https://www.ivanti.com/blog/epmm-security-update

OCENA

Statistični pregled števila priglašenih varnostnih dogodkov in kibernetskih incidentov v prvi polovici leta 2025 kaže na skupno večji porast števila incidentov v primerjavi z drugo polovico leta 2024[2]. SI-CERT je v tem obdobju zabeležil večji porast števila incidentov glede na preteklo obdobje (24 odstotni). Trend rasti števila incidentov je zabeležil tudi SIGOV-CERT, ki je v tem obdobju prav tako poročal o povečanju števila incidentov. V spodnji tabeli je prikazana primerjalna krivulja števila obravnavanih incidentov v drugi polovici leta 2024 in prvem polletju 2025.



Graf 1: Število obravnavnih incidentov v letih 2024 in 2025, SI-CERT, SIGOV-CERT

V obravnavanem obdobju so med varnostnimi dogodki in kibernetskimi incidenti prevladovale različne oblike goljufij, zlorabe neprivilegiranih uporabniških računov, incidenti povezani s spletnim nakupovanjem, izsiljevanje in neželena sporočila. Med njimi se je zabeležil incident pri operaterju telekomunikacijskih storitev, kjer je zlonamerni akter povzročil razkritje internih dokumentov na temnem spletu. Poleg tega velja izpostaviti dogodek z okuženimi osebnimi izmenljivimi mediji (USB ključki), za katerega je bilo ocenjeno, da bi lahko imel negativen vpliv na centralno državno informacijsko-komunikacijsko omrežje, organizacije javnega sektorja in širše. Dogodek je opomnil na pomen tveganj v dobavnih verigah, vključno z možnostjo vpeljave zlonamerne kode že na nivoju proizvajalca. URSIV je zaradi omenjenega naznanil stanje povečane ogroženosti varnosti omrežij in informacijskih sistemov in o tem obvestil zavezance in operaterje elektronskih komunikacij. Na podlagi tega so bile izdane odločbe, s katerimi se je pozvalo k poročanju o stanju informacijskih sistemov in uvedbi dodatnih varnostnih ukrepov. Ob tem so bila podana tudi dodatna priporočila glede uvedbe dodatnih varnostno-tehničnih ukrepov in ukrepov za varnost dobavnih verig pri uporabi in nabavi osebnih izmenljivih medijev. Ugotovitve so pokazale, da incident ni bil del usmerjene kampanje zoper določen subjekt ali Republiko Slovenijo, je pa opozoril na pomen varnosti dobavnih verig in strogem preverjanju in nadzoru dobaviteljev pri nabavi informacijske opreme.

[2] V prvem polletnem obdobju 2025 je bilo skupaj obravnavanih 2786 incidentov, kar predstavlja okoli petnajstodstotno rast števila incidentov v drugi polovici leta 2024, ko je bilo zabeleženih 2419 incidentov.

URSIV je glede na pridobljene podatke in upoštevaje aktualne trende kibernetskih incidentov v Republiki Sloveniji ter širše dogajanje na kibernetskem področju ocenil, da je ogroženost srednja. Skladno s tem so bili zavezanci pozvani k izvajanju ukrepov iz 21. in 22. člena ZInfV-1.

Na ravni EU je bila v prvem in drugem četrtletnem obdobju 2025 stopnja kibernetske ogroženosti ocenjena kot srednja (ang. *substantial*). V obravnavanem obdobju so bile države članice in institucije EU ciljane s strani kibernetskih kriminalcev, državno povezanih akterjev in hektivističnih skupin. Omenjene zlonamerne skupine izkazujejo 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 skupine so nadaljevale s svojimi aktivnostmi zoper države članice, s posebnim fokusom na telekomunikacijski sektor in vladne institucije. Dodatno pozornost zahtevajo tudi kampanje kibernetskega vohunjenja, ki ciljajo na vladne organizacije, vključno konzularnimi predstavništvi držav članic in ministrstev za zunanje zadeve ter informacijske operacije, ki so poskušale vplivati na rezultate volilnih procesov držav članic. Kratkoročni in srednjeročni obeti glede groženj informacijski in kibernetski varnosti se tako na mednarodni ravni nakazujejo predvsem s strani državno povezanih skupin, ki se bodo po vsej verjetnosti nadaljevale s kampanjami kibernetskega vohunjenja zoper države članice s ciljem strateškega zbiranja podatkov. Dodatno se predvideva nadaljevanje izvajanja porazdeljenih napadov onemogočanja (ang. *Distributed Denial-of-Service - DDoS*), ki bodo usmerjeni v volilne procese držav članic. Goljufi še naprej uporabljajo napredne tehnike socialnega inženiringa, da pridobijo zaupne informacije od žrtev. Zlonamerna elektronska sporočila in spletno ribarjenje so postali bolj ciljno usmerjeni in osredotočeni na posameznika, kar je povečalo njihovo učinkovitost. Pri tem pomaga vse hitreje razvijajoča tehnologija umetne inteligence in tehnologija za izdelavo kompleksnih ponaredkov (ang. *Deepfake*), ki omogoča ustvarjanje zelo realističnih ponarejenih video vsebin. Tovrstnim primerom smo bili že priča tudi v našem prostoru, ko je bila zlorabljena podoba in glas naših najvišjih političnih predstavnikov. Aktivnosti, ki izkoriščajo ranljivosti v dobavni verigi, postajajo vse večja grožnja. Pogosto služijo kot vstopna točka za namestitev vohunske programske opreme ali kot izhodišče za zlonamerne kibernetske aktivnosti v primeru zaostrovanja že tako napetih odnosov med velikimi geopolitičnimi akterji.

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 (https://www.varninainternetu.si/) 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 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 Zakonu o informacijski varnosti (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 prvem polletnem obdobju 2025 velja izpostaviti, da je Evropska agencija za kibernetsko varnost (ang. *European Union Agency for Cybersecurity - ENISA*) objavila Tehnične smernice za izvajanje NIS2, ki ponujajo praktične in tehnične usmeritve za izvajanje Direktive (EU) 2022/2555 (direktiva NIS 2). Smernice predstavljajo pripomoček za vse tiste subjekte, ki so zavezanci ali sodelujejo pri implementaciji direktive v praksi. Med drugim smernice posebej obravnavajo tudi področje varnosti dobavnih verig, ki postaja čedalje pomembnejše področje z vidika upravljanja kibernetskih incidentov, saj prav ranljivosti v dobavnih verigah pogosto omogočajo izvajanje kibernetskih incidentov in povečujejo njihovo resnost. URSIV je februarja 2025 izdal tudi Priročnik kibernetske varnosti, ki je namenjen vsem zavezancem po ZInfV-1, kot tudi drugim organizacijam, ki želijo okrepiti varnost informacijsko-komunikacijskih sistemov.