REPUBLIKA SLOVENIJA
URAD VLADE RS ZA INFORMACIJSKO VARNOST

Ulica gledališča BTC 2, 1000 Ljubljana

T: 01 478 4778
E: gp.uiv@gov.si
W: http://www.uiv.gov.si
X: @URSIV_Slovenia

Številka: 386-21/2026-1544-82

Ljubljana, 28. 9. 2026

GENERALNI SEKRETARIAT VLADE REPUBLIKE SLOVENIJE
Gp.gs@gov.si

ZADEVA: Predlog sklepa o sprejemu Skupnega zaključnega poročila o vaji kibernetske varnosti ENISA »Cyber Europe 2026« (CE26) – predlog za obravnavo

1. Predlog sklepov vlade:

Na podlagi šestega odstavka 21. člena Zakona o Vladi Republike Slovenije (Uradni list RS, št. 24/05 – uradno prečiščeno besedilo, 109/08, 38/10 – ZUKN, 8/12, 21/13, 47/13 – ZDU-1G, 65/14, 55/17, 163/22 in 57/25 – ZF in 555/26) je Vlada Republike Slovenije na _____ seji dne _____ pod _____ točko dnevnega reda sprejela

S K L E P

Vlada Republike Slovenije je sprejela Skupno zaključno poročilo o vaji kibernetske varnosti ENISA »Cyber Europe 2026« (CE26), ki je priloga tega sklepa.

Mag. Janja Garvas
generalna sekretarka

Priloga:

– Skupno zaključno poročilo o vaji kibernetske varnosti ENISA »Cyber Europe 2026« (CE26).

Sklep prejmejo:

– Urad Vlade Republike Slovenije za informacijsko varnost,
– Ministrstvo za finance,
– Služba Vlade Republike Slovenije za zakonodajo,
– Generalni sekretariat Vlade Republike Slovenije.

2. Osebe, odgovorne za strokovno pripravo in usklajenost gradiva:

- dr. Niko Gamulin, v. d. direktorja Urada Vlade Republike Slovenije za informacijsko varnost,
- Katarina Janjič, sekretar, vodja Nacionalnega koordinacijskega centra za kibernetsko varnost.

3. Zunanji strokovnjaki, ki so sodelovali pri pripravi dela ali celotnega gradiva:

/

4. Predstavniki vlade, ki bodo sodelovali pri delu državnega zbora:

/

5. Kratek povzetek gradiva:

Agencija Evropske unije za kibernetsko varnost (ENISA) je 10. in 11. junija 2026 izvedla vajo kibernetske varnosti Cyber Europe 2026 (CE26) (v nadaljevanju: vaja). Na nacionalni ravni je vajo vodil Urad Vlade Republike Slovenije za informacijsko varnost (v nadaljevanju: URSIV), sodelovali pa so Akademska in raziskovalna mreža Slovenije – skupina CSIRT SI-CERT, Luka Koper, d.d., in Slovenske železnice, d.o.o. in URSIV.

Vaja je preverjala tehnične, organizacijske in komunikacijske zmogljivosti pri obvladovanju obsežnih kibernetskih incidentov ter sodelovanje na nacionalni in evropski ravni. Vsi zastavljeni mednarodni in nacionalni cilji vaje so bili doseženi. Kot ključne prednosti so bili prepoznani realističen scenarij, učinkovito sodelovanje med deležniki, preverjanje postopkov poročanja in kriznega komuniciranja ter sodelovanje v okviru CSIRT mreže in EU-CyCLONe.

Kot področja za nadaljnje izboljšave so bila izpostavljena dodatna pojasnila glede uporabe metodologije Zakona o informacijski varnosti (v nadaljnjem besedilu: ZInfV-1) in postopkov prijavljanja incidentov, jasnejša opredelitev komunikacijskih kanalov in vsebin na družbenih omrežjih ter razmislek o daljšem trajanju prihodnjih izvedb vaje.

Namen vaje je bil preveriti in izboljšati nacionalne postopke zaščite in obrambe kibernetskega prostora, odzivanje na kibernetske incidente ter sodelovanje med nacionalnimi organi, zavezanci po ZInfV-1 in ustreznimi mrežami Evropske unije.

6. Presoja posledic za:

a)	javnofinančna sredstva nad 40.000 EUR v tekočem in naslednjih treh letih	NE
b)	usklajenost slovenskega pravnega reda s pravnim redom Evropske unije	NE
c)	administrativne posledice	NE
č)	gospodarstvo, zlasti mala in srednja podjetja ter konkurenčnost podjetij	NE
d)	okolje, vključno s prostorskimi in varstvenimi vidiki	NE
e)	socialno področje	NE
f)	dokumente razvojnega načrtovanja: – nacionalne dokumente razvojnega načrtovanja – razvojne politike na ravni programov po strukturi razvojne klasifikacije programskega proračuna – razvojne dokumente Evropske unije in mednarodnih organizacij	NE

7.a Predstavitev ocene finančnih posledic nad 40.000 EUR:

I. Ocena finančnih posledic, ki niso načrtovane v sprejetem proračunu				
	Tekoče leto (t)	t + 1	t + 2	t + 3
Predvideno povečanje (+) ali zmanjšanje (**–**) prihodkov državnega proračuna				
Predvideno povečanje (+) ali zmanjšanje (**–**) prihodkov občinskih proračunov				
Predvideno povečanje (+) ali zmanjšanje (**–**) odhodkov državnega proračuna				
Predvideno povečanje (+) ali zmanjšanje (**–**) odhodkov občinskih proračunov				
Predvideno povečanje (+) ali zmanjšanje (**–**) obveznosti za druga javnofinančna sredstva				

II. Finančne posledice za državni proračun				
II.a Pravice porabe za izvedbo predlaganih rešitev so zagotovljene:				
Ime proračunskega uporabnika	Šifra in naziv ukrepa, projekta	Šifra in naziv proračunske postavke	Znesek za tekoče leto (t)	Znesek za t + 1
SKUPAJ				
II.b Manjkajoče pravice porabe bodo zagotovljene s prerazporeditvijo:				
Ime proračunskega uporabnika	Šifra in naziv ukrepa, projekta	Šifra in naziv proračunske postavke	Znesek za tekoče leto (t)	Znesek za t + 1
SKUPAJ				

II.c Načrtovana nadomestitev zmanjšanih prihodkov in povečanih odhodkov proračuna:		
Novi prihodki	Znesek za tekoče leto (t)	Znesek za t + 1
SKUPAJ		

OBRAZLOŽITEV:

I. Ocena finančnih posledic, ki niso načrtovane v sprejetem proračunu

V zvezi s predlaganim vladnim gradivom se navedejo predvidene spremembe (povečanje, zmanjšanje):

- prihodkov državnega proračuna in občinskih proračunov,
- odhodkov državnega proračuna, ki niso načrtovani na ukrepih oziroma projektih sprejetih proračunov,
- obveznosti za druga javnofinančna sredstva (drugi viri), ki niso načrtovana na ukrepih oziroma projektih sprejetih proračunov.

II. Finančne posledice za državni proračun

Prikazane morajo biti finančne posledice za državni proračun, ki so na proračunskih postavkah načrtovane v dinamiki projektov oziroma ukrepov:

II.a Pravice porabe za izvedbo predlaganih rešitev so zagotovljene:

Navedejo se proračunski uporabnik, ki financira projekt oziroma ukrep; projekt oziroma ukrep, s katerim se bodo dosegli cilji vladnega gradiva, in proračunske postavke (kot proračunski vir financiranja), na katerih so v celoti ali delno zagotovljene pravice porabe (v tem primeru je nujna povezava s točko II.b). Pri uvrstitvi novega projekta oziroma ukrepa v načrt razvojnih programov se navedejo:

- proračunski uporabnik, ki bo financiral novi projekt oziroma ukrep,
- projekt oziroma ukrep, s katerim se bodo dosegli cilji vladnega gradiva, in
- proračunske postavke.

Za zagotovitev pravic porabe na proračunskih postavkah, s katerih se bo financiral novi projekt oziroma ukrep, je treba izpolniti tudi točko II.b, saj je za novi projekt oziroma ukrep mogoče zagotoviti pravice porabe le s prerazporeditvijo s proračunskih postavk, s katerih se financirajo že sprejeti oziroma veljavni projekti in ukrepi.

II.b Manjkajoče pravice porabe bodo zagotovljene s prerazporeditvijo:

Navedejo se proračunski uporabniki, sprejeti (veljavni) ukrepi oziroma projekti, ki jih proračunski uporabnik izvaja, in proračunske postavke tega proračunskega uporabnika, ki so v dinamiki teh projektov oziroma ukrepov ter s katerih se bodo s prerazporeditvijo zagotovile pravice porabe za dodatne aktivnosti pri obstoječih projektih oziroma ukrepih ali novih projektih oziroma ukrepih, navedenih v točki II.a.

II.c Načrtovana nadomestitev zmanjšanih prihodkov in povečanih odhodkov proračuna:

Če se povečani odhodki (pravice porabe) ne bodo zagotovili tako, kot je določeno v točkah II.a in II.b, je povečanje odhodkov in izdatkov proračuna mogoče na podlagi zakona, ki ureja izvrševanje državnega proračuna (npr. priliv namenskih sredstev EU). Ukrepanje ob zmanjšanju prihodkov in prejemkov proračuna je določeno z zakonom, ki ureja javne finance, in zakonom, ki ureja izvrševanje državnega proračuna.

7.b Predstavitev ocene finančnih posledic pod 40.000 EUR:
(Samo če izberete NE pod točko 6.a.)

Sprejem Skupnega zaključnega poročila o vaji kibernetske varnosti ENISA »Cyber Europe 2026« (CE26) ne povzroča dodatnih javnofinančnih posledic v tekočem in naslednjih treh letih.

8. Predstavitev sodelovanja z združenji občin:

Vsebina predloženega gradiva (predpisa) vpliva na: - pristojnosti občin, - delovanje občin, - financiranje občin.	NE

Gradivo (predpis) ni bilo poslano v mnenje:
Skupnosti občin Slovenije SOS: NE

Združenju občin Slovenije ZOS: NE

Združenju mestnih občin Slovenije ZMOS: NE

Predlogi in pripombe združenj niso bili podani.

Bistvenih predlogov in pripomb, ki ne bi bili upoštevani, ni.

9. Predstavitev sodelovanja javnosti:

Gradivo je bilo predhodno objavljeno na spletni strani predlagatelja:	NE

Skladno s sedmim odstavkom 9. člena Poslovnika Vlade Republike Slovenije (Uradni list RS, št. 43/01,

23/02 – popr., 54/03, 103/03, 114/04, 26/06, 21/07, 32/10, 73/10, 95/11, 64/12, 10/14, 164/20, 35/21, 51/21 in 114/21) javnost ni bila povabljena k sodelovanju, ker gre za predlog sklepa vlade.
Dr. Niko Gamulin v. d. direktorja urada

Priloge:

- Skupno zaključno poročilo o vaji kibernetske varnosti ENISA »Cyber Europe 2026« (CE26),
- predlog sklepa o sprejemu Skupnega zaključnega poročila o vaji kibernetske varnosti ENISA »Cyber Europe 2026« (CE26),
- obrazložitev.

Priloga 1

Zaključno poročilo o vaji kibernetske varnosti ENISA »Cyber Europe 2026«

POVZETEK

Agencija Evropske unije za kibernetsko varnost (v nadaljevanju: ENISA) je med 10. in 11. junijem 2026 izvedla vajo kibernetske varnosti Cyber Europe 2026 (v nadaljevanju: vaja CE26), ki je omogočila preverjanje pripravljenosti organizacij na obvladovanje obsežnih kibernetskih incidentov in kibernetskih kriz. V okviru nacionalne izvedbe so sodelovali Urad Vlade Republike Slovenije za informacijsko varnost (v nadaljevanju: URSIV), Akademska in raziskovalna mreža Slovenije, skupina CSIRT (v nadaljevanju: SI-CERT), Luka Koper, d.d. in Slovenske železnice, d.o.o., pri čemer je bil poudarek na preverjanju tehničnih zmogljivosti, postopkov poročanja, kriznega komuniciranja ter sodelovanja na nacionalni in evropski ravni. Priprave na vajo so bile ocenjene kot kakovostne in dobro organizirane, saj so udeležencem zagotovile jasno razumevanje ciljev, scenarija in postopkov. Sam scenarij je realistično prikazal usklajeno kibernetsko kampanjo proti pomorskemu in železniškemu sektorju, ki je zahtevala tako tehnično analizo incidentov kot tudi izvajanje procesov kriznega upravljanja. Udeleženci so posebno vrednost vaje prepoznali v preverjanju internih postopkov, sodelovanja med deležniki, izmenjave informacij ter usklajenega odzivanja na incidente. Kot ključne dejavnike uspešnega odziva so izpostavili poznavanje internih postopkov, jasno določene odgovornosti, učinkovite komunikacijske kanale ter sodelovanje z nacionalnimi in evropskimi partnerji. Med glavnimi ugotovljenimi pomanjkljivostmi so vadbenci izpostavili potrebo po dodatnih pojasnilih glede postopkov prijavljanja incidentov in uporabe metodologije Zakona o informacijski varnosti (v nadaljevanju: ZInfV-1), večjo jasnost vsebin na družbenih omrežjih ter razmislek o podaljšanju trajanja vaje, ki bi omogočilo poglobljeno obravnavo tehničnih in procesnih izzivov.

1 UVOD

Vaja CE26 predstavlja osmo izvedbo vseevropske serije vaj, ki jih organizira ENISA. Vaja simulira obsežne kibernetske incidente, ki lahko prerastejo v kibernetske krize in vplivajo na delovanje kritične infrastrukture po vsej Evropi. Poleg držav članic Evropske unije je v vaji sodelovala tudi Velika Britanija. Namen vaje je preverjanje pripravljenosti, odzivnih zmogljivosti ter usklajenega delovanja organizacij in pristojnih organov na tehnični, operativni in strateški ravni.

Republika Slovenija je na vaji sodelovala v obdobju od 10. do 11. junija 2026, pri čemer je vajo na nacionalni ravni vodil URSIV. Poleg nacionalnih organov Evropske unije so v vaji sodelovale tudi različne organizacije iz kritične infrastrukture držav članic Evropske unije in Velike Britanije. V okviru nacionalne izvedbe so sodelovali URSIV, SI-CERT, Luka Koper in Slovenske železnice, ki so vajo izvajali v skladu s svojimi vlogami in pristojnostmi.

Scenarij vaje je temeljil na usklajeni in kompleksni kibernetski kampanji, usmerjeni proti pomorskemu in železniškemu sektorju v državah članicah Evropske unije. Poleg neposrednih napadov na prometno infrastrukturo je scenarij predvideval tudi vplive na javno upravo, ponudnike informacijskih storitev ter širše družbeno okolje, vključno z dezinformacijskimi kampanjami. Takšen pristop je omogočil preverjanje sposobnosti organizacij za zaznavanje, obravnavo in poročanje o kibernetskih incidentih ter učinkovito krizno upravljanje in medsebojno sodelovanje.

Glavni namen sodelovanja na vaji je bil preizkus nacionalnih postopkov zaščite in obrambe kibernetskega prostora, preverjanje učinkovitosti koordinacije med deležniki ter krepitev pripravljenosti organizacij na odzivanje ob kibernetskih incidentih. Poseben poudarek je bil namenjen preverjanju postopkov poročanja, izmenjavi informacij, kriznemu komuniciranju in sodelovanju med nacionalnimi ter evropskimi mehanizmi kibernetske varnosti.

To poročilo povzema aktivnosti, izvedene v okviru priprav in sodelovanja na vaji CE26, ter predstavlja ključne ugotovitve, izkušnje in priporočila za nadaljnje izboljšanje pripravljenosti in odpornosti sodelujočih organizacij na področju kibernetske varnosti.

1.1 Cilji vaje

Pred vajo so bili s Sklepom vlade o sodelovanju Republike Slovenije na vaji kibernetske varnosti ENISA »Cyber Europe 2026« (številka 87100-4/2026/4, z dne 23. 4. 2026) sprejeti mednarodni cilji vaje, določeni v načrtu vaje pripravljenem s strani ENISE, ter cilji vaje, ki so bili določili na nacionalni ravni.

Cilji vaje določeni v dokumentu Cyber Europe 2026 – Exercise Plan (Maj 2025):

- preizkusiti in izboljšati ustreznost in učinkovitost postopkov in procesov kibernetske varnosti, zagotoviti organizacijsko sposobnost preživetja, skladnost z načrtom za kibernetsko varnost in ustreznimi določbami in predpisi EU ter nacionalnimi določbami ter omogočiti povratne informacije o splošni učinkovitosti, ustreznosti in uporabnosti politik;
- sodelujočim subjektom zagotoviti priložnosti za ocenjevanje ravni ozaveščenosti o kibernetski varnosti in prepoznavanje vrzeli v znanju ali spretnostih v skladu s profili European Cybersecurity Skills Framework (ECSF), da se na podlagi ugotovljenih izkušenj ponudijo možnosti za izpopolnjevanje ali prekvalifikacijo;
- preizkusiti in izboljšati učinkovitost mehanizmov sodelovanja in usklajevanja ter komunikacijskih kanalov, zagotoviti nemoten pretok informacij in naraščajoče zaupanje med železniškim in pomorskim sektorjem ter nacionalnimi subjekti in mrežami na ravni EU;
- vzpostaviti in izboljšati zavedanje o situaciji železniških in pomorskih organizacij ter nacionalnih organov za kibernetsko varnost, kar jim omogoči odkrivanje, odzivanje in okrevanje po obsežnih kibernetskih incidentih, hkrati pa upoštevati morebitni vpliv na druge sektorje;
- zagotoviti železniškim in pomorskim organizacijam priložnosti za preizkušanje, odkrivanje vrzeli in izboljšanje njihovih zmogljivosti poročanja o incidentih, s čimer se zagotovi, da poročila o stanju vključujejo ustrezne in relevantne informacije ter so skladna z obveznostmi iz Direktive o varnosti omrežij in informacijskih sistemov (NIS2).

Nacionalni cilji vaje:

- preveriti odziv sistema Republike Slovenije na ogrožanja in varnostna tveganja v primeru kibernetskih incidentov v nacionalnem kibernetskem prostoru;
- vaditi postopke koordiniranja upravljanja kibernetskih incidentov na nacionalni ravni;
- vaditi postopke sodelovanja in morebitne asistence s strani mreže nacionalnih ekip za odzivanje na kibernetske incidente (EU CSIRT) in mreže za upravljanje velikih kibernetskih kriz na ravni vodstev držav (EU CyCLONe) v primeru kibernetskega napada;
- preveriti usklajevanje in funkcionalnost odzivanja na kibernetske incidente v sodelovanju z gospodarskim sektorjem;
- vaditi odzivanje na kibernetske incidente na področju kritične infrastrukture, v sektorjih javne uprave ter železniškega in pomorskega prometa;
- vaditi postopke poročanja vadbencev ob zaznavi kibernetskega incidenta s ciljem zmanjševanja njihovih negativnih učinkov in zagotavljanjem celovite situacijske slike kibernetske varnosti v državi.

2 PRIPRAVE

Priprave na vajo CE26 so potekale več mesecev pred izvedbo vaje in so bile usklajevane s strani URSIV v sodelovanju z ENISA. V pripravljalnem obdobju je bilo izvedenih več nacionalnih in mednarodnih sestankov, katerih namen je bil predstavitev ciljev, scenarija in načina izvedbe vaje ter uskladitev sodelovanja med vsemi vključenimi deležniki. V okviru priprav so bili organizirani uvodni in koordinacijski sestanki, na katerih so bili predstavljeni namen in cilji vaje, način izmenjave informacij, uporaba

komunikacijskih kanalov, postopki poročanja ter vloga posameznih sodelujočih ekip. Udeležencem so bila posredovana tudi potrebna gradiva za pripravo na vajo, med katerimi so bili navodila za sodelujoče, obrazci za prijavo incidentov, predstavitve scenarija in druga podporna dokumentacija.

V okviru priprav so načrtovalci vaje na mednarodni in nacionalni ravni izhajali iz zastavljenih ciljev ter temu ustrezno oblikovali scenarij in tehnične izzive. Ti so vadbencem omogočali izvajanje postopkov in aktivnosti, potrebnih za doseganje ciljev vaje.

Posebna pozornost je bila namenjena pripravi lokalnih trenerjev in načrtovalcev vaje, ki so v sodelovanju z organizatorji prilagodili scenarij potrebam posameznih organizacij ter zagotovili pogoje za čim bolj realistično izvedbo. Na evropski ravni so potekale tudi pripravljalne aktivnosti znotraj Evropske mreže za upravljanje velikih kibernetskih kriz na ravni vodstev držav (v nadaljevanju: EU-CyCLONe), kjer so bile obravnavane vloge nacionalnih organov pri upravljanju kibernetskih kriz ter postopki sodelovanja na mednarodni ravni.

Vadbenci so v splošnem ocenili, da so bile priprave na vajo kakovostno izvedene. Gradiva so bila ocenjena kot jasna, pregledna in dobro strukturirana, tehnični artefakti pa kot realistični ter primerni za obravnavo simuliranih incidentov. Pozitivno je bilo izpostavljeno tudi postopno posredovanje informacij in dokaznega gradiva, kar je omogočilo bolj realistično simulacijo dejanskega odzivanja na incidente. Pri pregledu povratnih informacij so se pokazala tudi nekatera področja za izboljšave. Del vadbencev je izpostavil potrebo po dodatnih pojasnilih glede klasifikacije resnosti incidentov in postopkov prijavljanja v skladu z zahtevami ZInfV-1. Prav tako je bilo predlagano, da bi bile v prihodnjih izvedbah vaje še natančneje opredeljene okoliščine, v katerih zbrani tehnični podatki oziroma artefakti predstavljajo zadostno podlago za uradno prijavo incidenta oziroma izdajo zgodnjega opozorila.

Na splošno so priprave zagotovile ustrezno podlago za učinkovito izvedbo vaje ter sodelujočim omogočile dobro razumevanje svojih nalog, odgovornosti in pričakovanega načina sodelovanja v času izvajanja scenarija.

3 IZVEDBA VAJE

Vaja CE26 je obsegala tehnični ter procesni del odzivanja na obsežne kibernetske incidente. Scenarij je postopoma stopnjeval intenzivnost dogodkov in udeležence postavil pred vrsto tehničnih, organizacijskih in komunikacijskih izzivov, ki so zahtevali usklajeno delovanje na nacionalni in mednarodni ravni. Vadbenci so obravnavali različne vrste kibernetskih incidentov, scenarij pa je vključeval tudi elemente kriznega in strateškega komuniciranja z javnostmi. Tehnični del vaje je temeljil na analizi artefaktov, ki so jih udeleženci prejemali postopoma skozi celotno trajanje vaje. Večina vadbencev je ocenila, da so bili tehnični izzivi zahtevni, realistični in primerljivi z naprednimi grožnjami, s katerimi bi se lahko srečali tudi v dejanskem okolju. Več vadbencev je izpostavilo, da je bilo za uspešno reševanje nalog potrebno tesno sodelovanje med varnostnimi strokovnjaki, sistemskimi inženirji ter zunanjimi partnerji. Nekateri udeleženci so ocenili, da bi bile v resničnem incidentu razpoložljive informacije bistveno bolj nepopolne in bi zahtevale dodatno usklajevanje z lastniki sistemov in dobavitelji tehnologije.

Na procesni ravni so vadbenci preigrali postopke zaznave, ocenjevanja in obravnave incidentov ter preverjali učinkovitost notranjih mehanizmov kriznega upravljanja. V okviru vaje so bili uporabljeni postopki zgodnjega obveščanja, prijave incidentov, priprave vmesnih in zaključnih poročil ter postopki za usklajevanje aktivnosti med organizacijami. Več udeležencev je izpostavilo, da jim je vaja omogočila preverjanje celotne obravnave incidenta, od prvih indikatorjev kompromitacije do priprave zaključnega poročila in načrtovanja aktivnosti za obnovo sistemov. Pomemben del vaje je predstavljalo tudi krizno komuniciranje. Udeleženci so pripravljali odzive na medijska vprašanja, osnutke javnih izjav in komunikacijo z različnimi deležniki. Po ocenah vadbencev so takšne aktivnosti pomembno prispevale k preverjanju pripravljenosti organizacij na komunikacijske izzive ob večjih kibernetskih incidentih.

Na nacionalni ravni je potekalo redno usklajevanje med sodelujočimi organizacijami in pristojnimi organi. Izvedeni so bili operativni sestanki za izmenjavo informacij, usklajevanje odzivnih aktivnosti in pripravo skupne situacijske slike. Hkrati je na evropski ravni potekalo sodelovanje v okviru mreže nacionalnih

ekip za odzivanje na kibernetske incidente (v nadaljevanju: CSIRT mreža) in EU-CyCLONe, kjer so države izmenjevale podatke o poteku incidentov, ocene vpliva ter informacije o sprejetih ukrepih.

Splošna ocena izvedbe vaje je bila zelo pozitivna. Vadbenci so ocenili, da je scenarij omogočil učinkovito preverjanje tehničnih in organizacijskih zmogljivosti, pri čemer so posebej izpostavili dobro komunikacijo med deležniki in realističnost podanih izzivov. Nekateri vadbenci so ob tem predlagali, da bi bile prihodnje izvedbe vaje lahko daljše, saj bi to omogočilo podrobnejšo obravnavo posameznih tehničnih scenarijev in izvedbo še zahtevnejših igral. Prav tako je eden izmed vadbencev omenil, da je junijski termin za izvedbo nekoliko neugoden.

4 ANALIZA

Vaja CE26 je udeležencem omogočila preverjanje tehničnih, organizacijskih in komunikacijskih zmogljivosti v razmerah simuliranega kibernetskega incidenta večjih razsežnosti. Scenarij je bil ocenjen kot realističen, dogodki pa so bili logično povezani in primerno stopnjevani, kar je ustvarilo okoliščine, primerljive z dejanskim odzivanjem ob zahtevnem kibernetskem incidentu. Več vadbencev je ocenilo, da je vaja predstavljala ustrezno ravnovesje med tehničnimi izzivi in procesnim delom obravnave incidentov. Posebno dodano vrednost je predstavljalo preverjanje internih postopkov, poročanja o incidentih, kriznega komuniciranja ter sodelovanja z nacionalnimi in evropskimi deležniki. Pozitivno je bilo ocenjeno tudi dejstvo, da se udeleženci niso osredotočali na problematiziranje scenarija, temveč na izvajanje nalog in postopkov v skladu s svojimi vlogami. Pomemben element vaje je bila vključitev strateškega komuniciranja, medijskih vsebin in aktivnosti na družbenih omrežjih, ki so dodatno povečale realističnost scenarija in prispevale h kompleksnosti odločanja. Prav tako je bila kot pomembna dodana vrednost izpostavljena vključitev mreže EU-CyCLONe in CSIRT mreže.

Po drugi strani so vadbenci opozorili, da je bilo časovno okno za izvedbo posameznih aktivnosti razmeroma omejeno. Časovni pritisk je sicer povečal realističnost scenarija, vendar je v določenih primerih omejeval možnost podrobnejše strokovne razprave ter obravnave zahtevnejših tehničnih in procesnih vprašanj. Nekateri vadbenci so zato predlagali podaljšanje prihodnjih izvedb vaje za dodatni dan.

Ugotovljena so bila tudi nekatera odprta vprašanja. Eden izmed vadbencev je izpostavil omejeno dostopnost določenih vsebin na družbenih omrežjih (težko je bilo oceniti, za katero državo oziroma incident gre), zaradi česar vseh informacij ni bilo mogoče neposredno analizirati. Prav tako so bili podani predlogi za dodatna pojasnila glede uporabe obrazcev za prijavo incidentov, klasifikacije stopenj resnosti ter razlikovanja med potrjenimi dejstvi in tehničnimi ugotovitvami v postopkih poročanja.

5 V NADALJEVANJU SO PREDSTAVLJENE KLJUČNE UGOTOVITVE VAJE CE26

- Vsi zastavljeni cilji so bili doseženi. Odprava manjših pomanjkljivosti, ki so jih znotraj svojih procesov identificirali posamezni vadbenci, bo v prihodnje omogočala hitrejše in učinkovitejše odzivanje v primeru kibernetskih incidentov.
- Scenarij vaje je bil ocenjen kot realističen, dobro strukturiran in vsebinsko naprednejši v primerjavi s preteklimi izvedbami.
- Tehnični izzivi so bili zahtevni in so ustrezno preverjali strokovne zmogljivosti sodelujočih ekip.
- Vaja je uspešno omogočila preizkus celotnega procesa obravnave incidentov, od zgodnjega obveščanja in prijave incidenta do kriznega komuniciranja in priprave zaključnih poročil.
- Rezultati vaje kažejo, da učinkovit odziv ni odvisen zgolj od tehničnih zmogljivosti, temveč predvsem od predhodno določenih odgovornosti, poznavanja postopkov ter sposobnosti hitrega vključevanja ustreznih strokovnjakov in odločevalcev.
- Pomembno vlogo pri uspešnem obvladovanju incidentov imajo jasno določene odgovornosti, učinkovita organizacija dela ter ustrezna razdelitev vlog med člani odzivnih ekip.
- Pri enem izmed vadbencev je bilo ugotovljeno delno neujemanje med pripravljenimi tehničnimi artefakti in dejansko infrastrukturo oziroma zaščitnimi sistemi organizacije, kar je oteževalo neposredno uporabo nekaterih ugotovitev pri obravnavi simuliranega incidenta.

- Vadbenci so kot posebej pomembno izpostavili vzpostavitev enotnega komunikacijskega kanala za izmenjavo informacij, dokumentacije in koordinacijo aktivnosti med sodelujočimi.
- Za učinkovito reševanje zahtevnejših tehničnih incidentov je pomembno vključevanje vseh razpoložljivih strokovnjakov ter sodelovanje z zunanjimi strokovnimi organizacijami in skupinami za odzivanje na incidente na področju računalniške varnosti.
- Komunikacija med sodelujočimi organizacijami, nacionalnimi organi ter evropskimi mehanizmi sodelovanja je bila ocenjena kot učinkovita in koristna za vzpostavljanje skupne situacijske slike.
- Vključitev strateškega komuniciranja, medijskih vsebin in aktivnosti na družbenih omrežjih je povečala realističnost vaje ter omogočila preverjanje postopkov komuniciranja z javnostmi.
- Pozitivno je bila ocenjena medsebojna povezanost posameznih delov scenarija, saj je omogočila boljše razumevanje vplivov kibernetskih incidentov med različnimi sektorji.
- Več vadbencev je predlagalo dodatna pojasnila glede uporabe metodologije ZInfV-1, določanja stopenj resnosti incidentov ter sprožilcev za obveščanje pristojnih organov.
- Časovna omejenost vaje je povečala intenzivnost in časovni pritisk ter s tem prispevala k realističnosti scenarija. Hkrati je omejevala možnost poglobljene strokovne razprave in obravnave zahtevnejših odločitev. Za prihodnje izvedbe je zato smiselno razmisliti o podaljšanju vaje za najmanj en dan.

6 ZAKLJUČEK

Vaja CE2026 je bila uspešno izvedena in je dosegla zastavljene mednarodne in nacionalne cilje. Sodelujočim je omogočila celovito preverjanje tehničnih, organizacijskih in komunikacijskih zmogljivosti pri odzivanju na obsežne kibernetske incidente ter preverjanje sodelovanja med organizacijami, pristojnimi nacionalnimi organi in evropskimi mehanizmi kibernetskega kriznega upravljanja.

Scenarij je bil ocenjen kot realističen, vsebinsko zahteven in primeren za preverjanje pripravljenosti organizacij. Kot pomembna dodana vrednost so bili izpostavljeni zlasti preizkus postopkov zgodnjega obveščanja in prijavljanja incidentov, vzpostavljanje skupne situacijske slike, krizno komuniciranje ter sodelovanje v okviru CSIRT mreže in EU-CyCLONe.

Vaja je hkrati omogočila prepoznavo področij za nadaljnje izboljšave, predvsem pri uporabi postopkov poročanja in metodologije ZInfV-1, jasnosti komunikacijskih kanalov ter prilagajanju tehničnih artefaktov dejanskemu okolju sodelujočih organizacij. Ugotovitve in naučene lekcije predstavljajo pomembno podlago za nadaljnje izboljševanje nacionalnih postopkov, krepitev medsektorskega sodelovanja ter povečanje pripravljenosti Republike Slovenije na obsežne kibernetske incidente in kibernetske krize.

Mag. Janja Garvas
generalna sekretarka

Priloga 2

OBRAZLOŽITEV

Vlada Republike Slovenije je s Sklepom o sodelovanju Republike Slovenije na vaji kibernetske varnosti ENISA »Cyber Europe 2026« (CE26), št. 87100-4/2026/4 z dne 23. 4. 2026 (v nadaljnjem besedilu: sklep), določila sodelovanje Republike Slovenije na vaji ter naloge Urada Vlade Republike Slovenije za informacijsko varnost (v nadaljnjem besedilu: URSIV) pri njeni pripravi, izvedbi in poročanju. V skladu s sklepom URSIV po končani vaji potrdi poročilo o vaji in ga pošlje v sprejem Vladi Republike Slovenije.

Vaja Cyber Europe 2026 je potekala 10. in 11. junija 2026. Na nacionalni ravni jo je vodil URSIV, sodelovali pa so Akademska in raziskovalna mreža Slovenije, skupina CSIRT SI-CERT, Luka Koper, d.d., in Slovenske železnice, d.o.o. in URSIV. Scenarij je simuliral usklajeno in kompleksno kibernetsko kampanjo proti pomorskemu in železniškemu sektorju, vključeval je tudi vplive na javno upravo, ponudnike informacijskih storitev, krizno komuniciranje in dezinformacijske aktivnosti.

Vaja je omogočila preverjanje tehničnih, organizacijskih in komunikacijskih zmogljivosti za zaznavanje, obravnavo in poročanje o kibernetskih incidentih ter preverjanje nacionalnega in evropskega sodelovanja. Udeleženci so preizkusili postopke zgodnjega obveščanja, prijave incidentov, priprave vmesnih in zaključnih poročil, kriznega upravljanja in komuniciranja z javnostmi. Na evropski ravni je sodelovanje potekalo v okviru CSIRT mreže in EU-CyCLONe.

Iz skupnega zaključnega poročila izhaja, da so bili vsi zastavljeni mednarodni in nacionalni cilji doseženi. Scenarij je bil ocenjen kot realističen, dobro strukturiran in vsebinsko napreden, komunikacija med sodelujočimi organizacijami, nacionalnimi organi in evropskimi mehanizmi pa kot učinkovita. Vaja je potrdila, da so za uspešen odziv poleg tehničnih zmogljivosti ključne jasno določene odgovornosti, poznavanje postopkov, učinkoviti komunikacijski kanali ter pravočasno vključevanje ustreznih strokovnjakov in odločevalcev.

Kot področja za nadaljnje izboljšave so bila izpostavljena dodatna pojasnila glede uporabe metodologije Zakona o informacijski varnosti, določanja stopenj resnosti incidentov in sprožilcev za obveščanje pristojnih organov, večja jasnost vsebin na družbenih omrežjih, prilagajanje tehničnih artefaktov dejanskemu okolju sodelujočih organizacij ter razmislek o podaljšanju prihodnjih vaj za najmanj en dan. Ugotovitve in naučene lekcije bodo podlaga za nadaljnje izboljševanje nacionalnih postopkov ter krepitev medsektorskega sodelovanja in kibernetske odpornosti.

S predlaganim sklepom se Vladi Republike Slovenije predlaga, da sprejme Skupno zaključno poročilo o vaji kibernetske varnosti ENISA »Cyber Europe 2026« (CE26). Sprejem poročila ne povzroča dodatnih javnofinančnih posledic.