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: 368-21/2026-1544-31

Ljubljana, 21. 4. 2026

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

ZADEVA: Novo gradivo št. 1 - Predlog sklepa o sodelovanju Republike Slovenije na 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 prvega odstavka 6. člena Pravilnika o vajah v obrambnem sistemu (Uradni list RS, št. 100/13 in 44/21), je Vlada Republike Slovenije na _____ seji dne _____ pod _____ točko dnevnega reda sprejela

S K L E P

Vlada Republike Slovenije je sprejela Sklep o sodelovanju Republike Slovenije na vaji kibernetske varnosti ENISA »Cyber Europe 2026« (CE26).

Barbara Kolenko Helbl
generalna sekretarka

Priloga:

- Sklep o sodelovanju Republike Slovenije na 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. Uroš Svete, direktor 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:

Od 10. do 11na. junija 2026 bo Republika Slovenije sodelovala na vaji kibernetske varnosti Cyber Europe 2026 (CE26), ki jo organizira Agencija Evropske unije za varnost omrežij in informacij (v nadaljnjem besedilu: ENISA) v Atenah, Grčija. Sodelovaje na vaji je predvideno v skladu z Načrtom vaj v obrambnem sistemu in sistemu varstva pred naravnimi in drugimi nesrečami v letu 2026 (Sklep Vlade Republike Slovenije 84300-2/2026/2, z dne 5. 2. 2026).

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

Vajo v Republiki Sloveniji organizira in vodi Urad Vlade Republike Slovenije za informacijsko varnost; kot vadbenci sodelujejo Urad Vlade Republike Slovenije za informacijsko varnost, Luka Koper d.d., Slovenske železnice d.o.o. in Akademska in raziskovalna mreža Slovenije, skupina CSIRT SI-CERT.

Sodelujoči organi in organizacije krijejo svoje stroške sami, zato gradivo nima dodatnih javnofinančnih posledic nad 40.000 EUR.

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
1544	1544-21-0001, Delovanje Urada Vlade RS za informacijsko varnost	221004, Materialni stroški	6.000 EUR	
SKUPAJ			**6.000 EUR**	
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.)

Sodelujoči organi in organizacije sami krijejo svoje stroške priprav in izvajanja vaje. Organizacija in izvedba vaje »Cyber Europe 2026« (CE26) ne povzroča dodatnih javnofinančnih obveznosti nad 40.000 EUR v tekočem in naslednjih treh letih, predviden je materialni strošek za službena potovanja v povezavi s pripravo in izvedbo vaje v višini 6.000,00 EUR.

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 RS (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.
Ni relevantno, ker gradivo ni bilo predhodno objavljeno in javnost ni bila vključena v pripravo gradiva.
Dr. Uroš Svete direktor urada

Prilogi:

- obrazložitev,
- predlog sklepa o sodelovanju Republike Slovenije na vaji kibernetske varnosti ENISA »Cyber Europe 2026« (CE26).

Priloga 1

OBRAZLOŽITEV

Republika Slovenija bo v skladu z Načrtom vaj v obrambnem sistemu in sistemu varstva pred naravnimi in drugimi nesrečami v letu 2026 sodelovala na vaji kibernetske varnosti Agencije Evropske unije za varnost omrežij in informacij (v nadaljnjem besedilu: ENISA) »Cyber Europe 2026« (CE26), ki bo potekala 10. in 11. junija 2026.

Namen vaje na nacionalni ravni je vaditi nacionalne postopke zaščite in obrambe kibernetskega prostora ter odzivanja na kibernetske incidente pri zavezancih iz Zakona o informacijski varnosti (ZInfV-1). Na mednarodni ravni je namen povečati pripravljenost in odpornost kritičnih sistemov Evropske unije in držav članic ter zagotoviti učinkovito sodelovanje, izmenjavo podatkov in strateško usklajenost med sektorji in državami članicami.

Cilji vaje v Republiki Sloveniji so predvsem preveriti odziv sistema Republike Slovenije na varnostna tveganja in kibernetske incidente, vaditi koordiniranje upravljanja incidentov na nacionalni ravni, sodelovanje z mrežama nacionalnih ekip za odzivanje na kibernetske incidente (v nadaljnjem besedilu: EU CSIRT) in mreže za upravljanje velikih kibernetskih kriz na ravni vodstev držav (v nadaljnjem besedilu: EU CyCLONe), usklajeno odzivanje z gospodarskim sektorjem ter poročanje o incidentih zaradi zmanjševanja njihovih negativnih učinkov in zagotavljanja celovite situacijske slike v državi.

Scenarij vaje temelji na usklajeni in prefinjeni kampanji napadov na pomorsko in železniško infrastrukturo po Evropi, ki povzroča obratovalne motnje, gospodarsko škodo, motnje potniškega in tovornega prometa ter dezinformacije na družbenih omrežjih. Vadbenci bodo reševali tehnične izzive, ki jih zagotovi ENISA, ter izvedli interne in nacionalne procese priglasitve incidentov, kriznega upravljanja in komuniciranja z javnostmi.

Vajo v Republiki Sloveniji vodi Urad Vlade Republike Slovenije za informacijsko varnost, ki organizira in usklajuje priprave ter po končani vaji potrdi poročilo o vaji in ga pošlje v sprejem Vladi Republike Slovenije. Kot vadbenci sodelujejo Urad Vlade Republike Slovenije za informacijsko varnost, Luka Koper d.d., Slovenske železnice d.o.o. in Akademska in raziskovalna mreža Slovenije, skupina CSIRT SI-CERT; glede na razvoj scenarija se lahko vključijo tudi drugi potrebni subjekti.

Vlada Republike Slovenije sprejme sklep o organizaciji vaje v okviru svojih tekočih poslov, ker gre za nujno in redno nalogo zagotavljanja pripravljenosti državnih organov na krizne situacije, zlasti na področju kibernetske varnosti ali drugih izrednih dogodkov. Takšne vaje so ključne za preverjanje delovanja sistemov, usklajenosti pristojnih institucij ter učinkovitosti odzivnih mehanizmov, zato njihova izvedba ne pomeni sprejemanja novih politik ali dolgoročnih strateških odločitev, temveč izvajanje že sprejetih obveznosti države. V skladu s 115. členom Ustave RS, ki vladi po prenehanju mandata omogoča opravljanje le tekočih poslov, organizacija tovrstne vaje predstavlja dopustno in potrebno aktivnost za nemoteno delovanje države ter zagotavljanje njene varnosti in odpornosti.

Priloga 2

VLADA REPUBLIKE SLOVENIJE PREDLOG

Številka: _____
Ljubljana, dne _____

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 prvega odstavka 6. člena Pravilnika o vajah v obrambnem sistemu (Uradni list RS, št. 100/13 in 44/21) je Vlada Republike Slovenije na _____. redni seji dne _____ pod _____ točko dnevnega reda sprejela naslednji

S K L E P

o sodelovanju Republike Slovenije na vaji kibernetske varnosti ENISA »Cyber Europe 2026« (CE26)

1. člen
(uvodna določba)

Republika Slovenija bo od 10. 6. 2026 do 11. 6. 2026 sodelovala na vaji kibernetske varnosti ENISA »Cyber Europe 2026« (v nadaljnjem besedilu: vaja), ki poteka v organizaciji Agencije Evropske unije za varnost omrežij in informacij (v nadaljnjem besedilu: ENISA) v Atenah, Grčija.

2. člen
(namen)

(1) Namen vaje na nacionalnem nivoju je vaditi nacionalne postopke zaščite in obrambe kibernetskega prostora ter odzivanja na kibernetske incidente pri zavezancih iz Zakona o informacijski varnosti.

(2) Namen vaje na mednarodnem nivoju je povečati pripravljenost in odpornost kritičnih sistemov Evropske unije (v nadaljnjem besedilu: EU) in članic ter zagotoviti ustrezno sodelovanje izmenjavo podatkov in strateško usklajenost med posameznimi sektorji znotraj držav članic in med državami članicami.

3. člen
(cilji vaje)

(1) V skladu z dokumentom Cyber Europe 2026 – Exercise Plan (Maj 2025), ki ga je pripravila ENISA, so cilji vaje naslednji:

- 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).

(2) Cilji vaje v Republiki Sloveniji so:

- 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 nacionalnem nivoju.
- 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.

4. člen
(osnovna zamisel za izvedbo)

(1) Osnovna zamisel temelji na usklajeni in prefinjeni kampanji po vsej Evropi, v kateri so pomorske in železniške infrastrukture hkrati tarča napadov zlonamernih akterjev, kar povzroča hude obratovalne motnje, obsežno gospodarsko škodo in stisko potnikov. Evropski pomorski transporti se soočajo s kritičnimi motnjami, saj so pristaniška logistika in navigacijski sistemi močno prizadeti, kar povzroča zaustavitev tovornega prometa in potencialne skorajšnje trke. Hkrati pa glavna železniška omrežja trpijo zaradi neposrednih motenj, zaradi česar se ustavljajo čezmejni vlaki, kar ustvarja logistični kaos, zaradi česar so ujeti tisoči potnikov in prihaja do zamud pri dobavi. Ravno tako so napadeni infrastrukturni in prometni organi državne uprave, kar povzroča administrativno paralizo, moti potniški promet in razkriva občutljive podatke o potnikih. Vsi dogodki iz scenarija pa posledično spodbujajo dezinformacije s strani hektivistov na družbenih omrežjih.

(2) Vadbenci bodo v procesu vaje s tehničnimi ekipami reševali tehnične izzive, ki jih zagotovi ENISA, v nadaljevanju pa bodo s svojimi skupinami za krizni management izvedli interne in nacionalne procese priglasitve kibernetskih incidentov, upravljanja in koordiniranja kibernetskih incidentov, komuniciranja z javnostmi in ostalih procesov kriznega upravljanja.

5. člen
(kraj in čas izvajanja)

(1) Republika Slovenija bo za čas izvedbe vaje v Atene napotila enega nacionalna predstavnika, in sicer predstavnika v vlogi nacionalnega načrtovalca.

(2) V Republiki Sloveniji vaja poteka na sedežih vadbencev.

(3) Vaja se izvaja v okviru rednega delovnega časa med 9. in 17. uro.

6. člen
(priprava, načrtovanje in izvedba)

Urad Vlade Republike Slovenije za informacijsko varnost organizira in usklajuje priprave na vajo in zagotovi izdelavo dokumentov, potrebnih za izvedbo vaje v državi. Vsi vadbenci vaje so dolžni sodelovati v pripravah na vajo, pri njeni izvedbi in uresničitvi zastavljenih ciljev.

7. člen
(vodstvo vaje)

(1) Vajo vodi Urad Vlade Republike Slovenije za informacijsko varnost.

(2) Urad Vlade Republike Slovenije za informacijsko varnost zagotovi ustrezne priprave in izvedbo vaje ter sodelovanje vadbencev pri uresničitvi zastavljenih ciljev.

(3) Urad Vlade Republike Slovenije za informacijsko varnost po končani vaji potrdi poročilo o vaji, ki ga pošlje v sprejem Vladi Republike Slovenije.

8. člen
(vadbenci)

(1) Vadbenci na vaji v Republiki Sloveniji so:
- Urad Vlade Republike Slovenije za informacijsko varnost,
- Luka Koper d.d.,
- Slovenske železnice d.o.o.,
- Akademska in raziskovalna mreža Slovenije, skupina CSIRT SI-CERT.

(2) Vsak vadbenec, ki razpolaga s tehnično ekipo, je dolžan zagotoviti tudi skupino za izvedbo procesnega dela vaje, za namen priglašanja incidentov, komuniciranja z javnostmi in kriznega upravljanja.

(3) Glede na razvoj scenarija vaje in skladno z odločitvijo Urada Vlade Republike Slovenije za informacijsko varnost, se po potrebi kot vadbenci v vajo vključijo tudi drugi subjekti, ki bi bili v sklopu kibernetske varnosti potrebni za uspešno izvedbo vaje.

(4) Vadbenci določijo število sodelujočih in organizacijo dela na vaji.

9. člen
(stroški priprave in izvedbe)

Sodelujoči vadbenci sami krijejo svoje stroške priprav in izvajanja vaje.

10. člen
(seznanitev vadbencev)

Urad Vlade Republike Slovenije za informacijsko varnost s tem sklepom seznani vadbence in ostale sodelujoče.

11. člen
(končna določba)

Ta sklep začne veljati naslednji dan po sprejetju.

Barbara Kolenko Helbl
generalna sekretarka