REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE
ZA INFORMACIJSKO VARNOST

URSIV

REPUBLIKA SLOVENIJA
URAD VLADE RS ZA KOMUNICIRANJE

Nacionalni komunikacijski načrt odzivanja v primeru kibernetskih incidentov

Druga verzija, januar 2026

VSEBINA

1. UVOD 3
2. KLJUČNI TERMINI 3
2.1 PODROBNA RAZVRSTITEV KIBERNETSKI INCIDENTOV 5
3. OPREDELITVE KOMUNICIRANJA PO ZAKONU O INFORMACIJSKI VARNOSTI 6
4. INTERNA IZMENJAVA INFORMACIJ MED KLJUČNIMI DELEŽNIKI V PRIMERU KIBERNETSKEGA INCIDENTA 7
5. OBVEŠČANJE JAVNOSTI 7
5.1 POTEK OBVEŠČANJA 8
5.1.1 STOPNJA INCIDENTA C1 DO C3 8
5.1.2 STOPNJA INCIDENTA C4 DO C6 8
5.2 OBVEŠČANJE TUJE JAVNOSTI 8
6. NALOGE IN AKTIVNOSTI URSIV IN UKOM 9
7. PREDVIDENA FINANČNA SREDSTVA ZA IZVAJANJE NAČRTA 9

1. UVOD

Nacionalni komunikacijski načrt odzivanja v primeru kibernetskih incidentov, s posebnim poudarkom na komuniciranju ob težjem kibernetskem incidentu, ki lahko preide v kritični kibernetski incident (C2), ter v primeru kritičnega kibernetskega incidenta (C1), je celota ukrepov na področju komuniciranja vseh odgovornih deležnikov z domačo in tujo javnostjo. Načrt je državni načrt in temelji na nalogah, za katere so odgovorni posamezni ključni deležniki.

Načrt je bil prvič pripravljen v letu 2024, druga prenovljena verzija načrta pa je pripravljena januarja 2026 in vključuje spremembe, ki temeljijo na sprejetju Zakona o informacijski varnosti (ZInfV-1), ki je stopil v veljavo junija 2025. Za načrt je odgovoren Urad Vlade Republike Slovenije za informacijsko varnost (URSIV), izvaja pa ga v sodelovanju z Uradom vlade za komuniciranje (UKOM) ter ministrstvi in drugimi državnimi organi skladno s svojimi zakonskimi pristojnostmi.

Ključno načelo obveščanja ob kibernetskih incidentih je, da mora biti javnost obveščena pravočasno, celovito in objektivno na način, ki je dostopen in razumljiv vsem.

2. KLJUČNI TERMINI

Zakon o informacijski varnosti (ZInfV-1) opredeljuje:

Informacijska varnost pomeni zaščito in varovanje omrežnih in informacijskih sistemov ter pripadajočih podatkov pred nedovoljenim dostopom, uporabo, razkritjem, motenjem, spreminjanjem ali uničenjem, in sicer za zagotavljanje zaupnosti, avtentičnosti, celovitosti in razpoložljivosti navedenih sistemov in podatkov.

Kibernetska grožnja je vsaka potencialna okoliščina, dogodek ali dejanje, ki bi lahko poškodovalo, prekinilo ali drugače škodljivo vplivalo na omrežja in informacijske sisteme, uporabnike takih sistemov in druge osebe.

Pomembna kibernetska grožnja je kibernetska grožnja, za katero se glede na njene tehnične značilnosti lahko domneva, da bi lahko resno negativno vplivala na omrežne in informacijske sisteme subjekta ali na uporabnike njegovih storitev, tako da bi povzročila znatno premoženjsko ali nepremoženjsko škodo.

Kibernetska obramba je celota ukrepov, dejavnosti in zmogljivosti državnih organov, organov lokalne samouprave, gospodarskih družb, zavodov in drugih organizacij ter državljanov in državljank, ki so potrebni za zaščito in varovanje kibernetskega prostora pred kibernetskimi grožnjami in incidenti.

Kibernetska varnost so dejavnosti, ki so potrebne za zaščito omrežnih in informacijskih sistemov, uporabnikov takih sistemov in drugih oseb, na katere vplivajo kibernetske grožnje.

Kibernetski prostor je globalno informacijsko okolje, ki ga tvorijo informacijski sistemi in omrežja, podatki, digitalne naprave in njihovi uporabniki.

Kriza je resna grožnja temeljnim vrednotam in družbenim normam, za katero so značilni časovni pritisk in negotove okoliščine, ki zahtevajo hitro odločanje in izvajanje ukrepov, ki odstopajo od običajnih in predpisanih institucionalnih poti ter zahtevajo uporabo mehanizmov kriznega upravljanja.

Incident je dogodek, ki je ogrozil razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali storitev, ki jih omrežni in informacijski sistemi zagotavljajo ali so prek njih dostopni.

Kibernetski incident velikih razsežnosti je incident, ki povzroči motnjo, ki presega zmožnost Republike Slovenije za odziv nanj, ali incident, ki pomembno vpliva na vsaj dve državi članici Evropske unije.

Skorajšnji incident je dogodek, ki bi lahko ogrozil razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali storitev, ki jih omrežni in informacijski sistemi zagotavljajo ali so prek njih dostopni, vendar se je uspešno preprečilo, da bi se ta dogodek uresničil, ali se ni uresničil.

Ranljivost je pomanjkljivost, dovzetnost ali napaka proizvoda ali storitve IKT, ki jo kibernetska grožnja lahko izkoristi.

Tveganje je možnost izgube ali motnje zaradi incidenta ter je izraženo kot kombinacija razsežnosti izgube ali motnje in verjetnosti, da bi se incident zgodil.

2.1 PODROBNA RAZVRSTITEV KIBERNETSKI INCIDENTOV

STOPNJEVANJE V SKLADU Z ZInfV-1	STOPNJEVANJE NA PODLAGI KAZALNIKOV	OPIS INCIDENTA
KRITIČNI	**KRITIČNI INCIDENT (C1)**	Pomemben incident, ki poleg vplivov C3 incidenta povzroči tudi oteženo delovanje države, še posebej izvajanje nalog obrambe, notranje varnosti ter zaščite in reševanja, ali delno onemogoči delovanje vsaj treh visoko kritičnih sektorjev ali enega v celoti.
TEŽJI	**INCIDENT (C2)**	Enkraten pomemben incident ali zaporedje več različnih incidentov v kratkem obdobju, kadar obstaja možnost, da preraste v kritični incident.
	INCIDENT (C3)	Enkraten pomemben incident ali zaporedje več različnih incidentov v kratkem obdobju, ki je glede na parametre določitve pomembnosti vpliva incidenta zadevnemu subjektu povzročil(-o) ali bi mu lahko povzročil(-o) znatne operativne motnje pri opravljanju storitev ali finančne izgube, je vplival(-o) ali bi lahko vplival(-o) na druge fizične ali pravne osebe s povzročitvijo precejšnje premoženjske ali nepremoženjske škode ali ima negativen medsektorski vpliv ali negativen vpliv na delovanje informacijskih sistemov obrambe, notranje varnosti ter sistema zaščite in reševanja.
LAŽJI	**INCIDENT (C4)**	Enkraten incident, ki glede na parametre določitve pomembnosti vpliva incidenta zadevnemu subjektu ni povzročil in ne more povzročiti znatne operativne motnje pri opravljanju storitev ali finančne izgube ter ni vplival in ne more vplivati na druge fizične ali pravne osebe s povzročitvijo precejšnje premoženjske ali nepremoženjske škode. Takšen incident ne sme imeti negativnega medsektorskega vpliva ali negativnega vpliva na delovanje informacijskih sistemov obrambe, notranje varnosti ter sistema zaščite in reševanja.
KIBERNETSKA GROŽNJA	**SKORAJŠNJI INCIDENT (C5)**	Dogodek, ki bi lahko ogrozil razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali storitev, ki jih omrežni in informacijski sistemi zagotavljajo ali so prek njih dostopni, vendar se je preprečilo, da bi se ta dogodek uresničil, ali se ni uresničil.
	DOGODEK (C6)	Zaznane kibernetske aktivnosti, ki nimajo negativnega vpliva na omrežje in informacijske sisteme ali informacijske sisteme zavezancev. Zaznan ali možen vpliv na posamezne fizične osebe ali posamezna podjetja v državi, ki niso zavezanci.

3. OPREDELITVE KOMUNICIRANJA PO ZAKONU O INFORMACIJSKI VARNOSTI

10. člen (pristojni nacionalni organ):

(2) Pristojni nacionalni organ izvaja naslednje naloge:

7. koordinira usposabljanje, vaje in izobraževanje na področju informacijske varnosti ter skrbi za okrepitev zavedanja javnosti o informacijski varnosti, lahko pa tudi sam organizira in izvaja usposabljanja s področja informacijske in kibernetske varnosti

12. za statistične namene in namene seznanjanja javnosti dvakrat letno pripravi anonimizirane informacije o priglašenih incidentih, te nato javno objavi na osrednjem spletnem mestu državne uprave.

13. strokovne in svetovalne naloge in naloge koordinatorja na področju odnosov z javnostmi, ki zajemajo komunikacijo z zunanjimi in notranjimi javnostmi ter **krizno komuniciranje v primeru incidenta**.

14. v sodelovanju s službo vlade, pristojno za komuniciranje z javnostmi, izdela in vzdržuje **nacionalni načrt komuniciranja v primeru incidentov**.

12. člen (organ za obvladovanje kibernetskih kriz):

(7) Če je treba v zvezi z izvajanjem tega člena obvestiti tudi javnost, pristojni nacionalni organ skupaj s službo vlade, pristojno za komuniciranje z javnostjo, **pripravi sporočilo za javno objavo, ki ga smejo mediji objaviti le v nespremenjeni obliki**.

30. člen (postopek priglasitve pomembnih incidentov):

(6) Kadar je ozaveščenost javnosti potrebna za preprečitev pomembnega incidenta ali obravnavo pomembnega incidenta, ki še poteka, ali kadar je razkritje pomembnega incidenta kako drugače v javnem interesu, **pristojni nacionalni organ po posvetovanju z zadevnim zavezancem obvesti javnost o pomembnem incidentu ali zahteva, da to stori zavezanec**. Predlog za takšno obveščanje lahko pristojnemu nacionalnemu organu poda tudi pristojna skupina CSIRT.

(7) Kadar je pristojni nacionalni organ prek enotne kontaktne točke obveščen o pomembnem čezmejnem ali medsektorsko pomembnem incidentu, ki ima vpliv tudi v Republiki Sloveniji, lahko po posvetovanju s subjektom, ki je priglasil incident, **obvesti javnost o pomembnem incidentu ali zahteva, da to stori zavezanec**, tudi kadar je bil incident priglašen v drugi državi članici Evropske unije.

37. člen (ocena ogroženosti)

(3) Če je ocena ogroženosti ovrednotena kot srednja, pristojni nacionalni organ o tem obvesti zavezance, pri tem jim lahko priporoči izvedbo dodatnih ukrepov za varnost omrežij ali informacijskih sistemov. Pristojni nacionalni **organ lahko o tem obvesti tudi splošno javnost na svojem spletnem mestu in v sredstvih javnega obveščanja** ter lahko hkrati priporoči tudi ustrezne ukrepe.

(4) Kadar je ocena ogroženosti ovrednotena kot kritična, pristojni nacionalni organ o tem nemudoma obvesti vlado, SNAV in osrednji organ za odzivanje na hibridne grožnje, lahko pa jih glede na presojo relevantnih okoliščin in informacij obvesti tudi, kadar je ogroženost ovrednotena kot visoka. O oceni ogroženosti visoka ali kritična pristojni nacionalni organ obvesti zavezance, lahko pa **obvesti tudi splošno javnost na svojem spletnem mestu in v sredstvih javnega obveščanja** ter lahko hkrati priporoči tudi ustrezne ukrepe. Pristojni nacionalni organ o preklicu ali spremembi ocene ogroženosti kritična ali visoka obvesti predhodno obveščene deležnike iz tega odstavka.

4. INTERNA IZMENJAVA INFORMACIJ MED KLJUČNIMI DELEŽNIKI V PRIMERU KIBERNETSKEGA INCIDENTA

Ključni deležniki so:

- URSIV,
- CSIRT skupini,
- ostali pristojni državni organi, glede na svoje pristojnosti,
- UKOM
- zavezanec po Zakonu o informacijski varnosti (ZInfV-1), ki ga je incident prizadel.

URSIV vse ključne deležnike obvešča o poteku incidenta in sporočilih za javnost, saj je usklajenost med deležniki nujna za učinkovito in ustrezno obveščanje javnosti.

Začetno obvestilo o kibernetskem incidentu stopnje C1 – C3 mora biti posredovano tudi UKOM. Oziroma tudi za nižje stopnje incidentov, v primeru povečanega zanimanja javnosti.

Začetno sporočilo UKOM-u posreduje URSIV.

URSIV obvešča UKOM po vrstnem redu in preneha obveščati, ko obvesti enega od naslednjih predstavnikov UKOM:

- direktorja UKOM
- vodjo Sektorja za vladno komuniciranje
- vodjo oddelka za odnose z domačimi in tujimi mediji
- dežurnega delavca.

5. OBVEŠČANJE JAVNOSTI

Z rednim obveščanjem in komuniciranjem prispevamo k umirjenemu reševanju kriznih razmer, ozaveščanju prebivalstva in preprečevanju težjih posledic za posameznika, družbo in gospodarstvo. V ospredju mora biti dostopnost do informacij za vsakega posameznika, ne glede na socialni status ali druge okoliščine, vključujoč ranljive skupine.

Usklajeno obveščanje javnosti o kibernetskih incidentih se izvede zaradi:

- ozaveščanja in opozarjanja na pretekle incidente – gre za seznanjanje javnosti s preteklimi izkušnjami, nevarnostmi in ukrepi za preprečevanje nastanka novih kibernetskih incidentov;

- preprečevanja stopnjevanja incidenta – gre za obveščanje javnosti o trenutnem kibernetskem incidentu, ki se že upravlja in zanj obstaja nevarnost, da preide v višjo stopnjo, kot je trenutno, na kar lahko vplivajo tudi aktivnosti javnosti v kibernetskem prostoru;

- nevarnosti novih enakih ali podobnih dogodkov – gre za obveščanje javnosti o kibernetskem incidentu, ki se trenutno upravlja, je ustavljen oziroma je v zaključnih fazah upravljanja in zanj obstaja nevarnost, da bi se zaradi aktivnosti javnosti razširil ali ponovil še pri katerem od zavezancev;

- umirjanja javnost in stabilizaciji splošnega nemira ob incidentu ter ustvarjanju zaupanja.

Pri presoji o obsegu in načinih obveščanja javnosti je treba upoštevati:

- načela zagotavljanja varnosti,
- varovanje podatkov o preiskavi incidenta,
- interes morebitnega predkazenskega oz. kazenskega postopka (za primere, ko ima incident zakonsko izpolnjene znake kaznivega dejanja),
- potrebe po ozaveščanju in varovanju osebnih podatkov prebivalstva,

- načela preprečevanja škodovanja dobremu imenu zavezanca, ki ga je kibernetski incident prizadel.

5.1 POTEK OBVEŠČANJA

Prvo sporočilo za javnost in vsa nadaljnja sporočila na državni ravni oblikuje in pošlje v objavo URSIV v sodelovanju z odzivnim centrom ter zavezancem, ki ga je incident prizadel. Pri večjih incidentih oziroma povečanem zanimanju javnosti se vključi tudi UKOM.

Sporočila za javnost objavi Sektor za mednarodne zadeve in odnose z javnostmi URSIV na spletišču GOV.SI in na svojih družbenih omrežjih oz. jih posreduje v objavo medijem.

5.1.1 STOPNJA INCIDENTA C1 DO C3

Nosilci obveščanja javnosti:
- URSIV v sodelovanju z UKOM, v kolikor je potrebno,
- ostali pristojni državni organi oziroma drugi zavezanci, glede na svoje pristojnosti.

Komunikacijske aktivnosti morajo potekati usklajeno. Vodilno koordinacijsko vlogo prevzameta UKOM oz. URSIV po dogovoru glede na potrebe medijskega odzivanja in zagotavljata usklajenost kriznega komuniciranja med ministrstvi in vladnimi službami ter opravljata naloge v skladu s svojimi pristojnostmi. Po potrebi se vključi tudi druge pristojne državne organe.

5.1.2 STOPNJA INCIDENTA C4 DO C6

Nosilci obveščanja javnosti:
- URSIV,
- ostali pristojni državni organi oziroma drugi zavezanci, glede na svoje pristojnosti.

Pri manj ogrožajočih incidentih se o poročanju javnosti dogovorita URSIV in zavezanec, ki ga je incident prizadel. Po potrebi se vključi tudi UKOM, v kolikor gre za povečano zanimanje javnosti.

5.2 OBVEŠČANJE TUJE JAVNOSTI

UKOM o dogajanju po potrebi celovito obvešča tudi tujo javnost, in sicer v sodelovanju s predstavniki za odnose z javnostmi URSIV in zavezancem, ki ga je incident prizadel.

6. NALOGE IN AKTIVNOSTI URSIV IN UKOM

UKOM in URSIV ter po potrebi zavezanec, ki ga je incident prizadel, v skladu z dogovorom, sodelujejo v sledečih fazah komuniciranja:
:

- priprava skupnih sporočil za javnost in posredovanje javnosti prek medijev, svetovnega spleta (preko spletnega mesta Vlade RS) in družbenih omrežij;
- obveščanje tuje javnosti, in sicer prek ustaljenih oblik komuniciranja, prek tujih dopisnikov v naši državi, prek neposrednih stikov s tujimi mediji ter prek Slovenske tiskovne agencije (STA) in TV izmenjave;
- organizacija novinarskega središča;
- organizacija novinarske konference za domače in tuje novinarje;
- spremljanje poročanja domačih in tujih medijev ter priprava izbora prispevkov, objavljenih v njih (t. i. klipinge);
- opravljanje drugih nalog iz svoje pristojnosti.

Glede na razsežnost kriznega dogodka, UKOM po potrebi imenuje operativno skupino za krizno komuniciranje, ki izvaja dejavnosti pravočasnega in usklajenega komuniciranja z javnostmi. Operativno skupino za krizno komuniciranje vodi direktor UKOM. Skupino sestavljajo predstavniki za odnose z javnostmi tistih ministrstev in vladnih služb, na katerih delovno področje se nanaša krizni dogodek. Po potrebi se v operativno skupino vključijo tudi predstavniki za odnose z javnostmi drugih državnih organov in zunanji strokovni sodelavci.

Direktor UKOM skliče vladno koordinacijo predstavnikov vladnih institucij za odnose z javnostmi, ki opravlja koordinativne in posvetovalne naloge na področju vladnih odnosov z javnostmi tudi v primeru kriznega komuniciranja.

7. PREDVIDENA FINANČNA SREDSTVA ZA IZVAJANJE NAČRTA

Finančna sredstva se določijo na podlagi letnih programov dela UKOM in URSIV v letnih proračunih UKOM in URSIV. V to so vključena sredstva za izvedbo rednih nalog, ki jih UKOM in URSIV opravljata tudi sicer.

Dodatna sredstva pa bi bila potrebna v primeru večjega obsega nesreče in posledično okrepljenih aktivnosti UKOM (organizacija medijskega središča, izvedba medijskih aktivnosti na terenu, letakov za obveščanje prebivalstva itd). V tem primeru bi UKOM vlado zaprosil za dodatna finančna sredstva.

Finančna sredstva so načrtovana tudi v okviru sredstev za usposabljanje, za sodelovanje na vajah ter udeležbo na seminarjih doma in v tujini. Cilj vseh tovrstnih aktivnosti je ustrezna pripravljenost zaposlenih za delo v kriznih razmerah.

Na podlagi ocene ogroženosti se predvidi sredstva, potrebna za delo v drugačnih (kriznih) razmerah – začasne pisarne, prostori za organizacijo medijskega središča, z namenom, da izvajanje dejavnosti ob izrednem dogodku poteka čim bolj nemoteno in da so omogočeni pogoji, ki zagotavljajo strokovno delo v skladu z načrti.

Priloge, ki jih redno posodabljata URSIV in UKOM:

- Telefonske številke pristojnih ustanov in njihovih predstavnikov
- Seznam predstavnikov za odnose z javnostmi v ministrstvih in vladnih službah

Načrt je bil sprejet 20.1. 2026.

Skrbnika načrta:

DIREKTORICA UKOM
Petra Bezjak Cirman

Petra Bezjak Cirman
Digitalno podpisal Petra Bezjak Cirman
Datum: 2026.01.27 18:28:47 +01'00'

DIREKTOR URSIV
Dr. Uroš Svete

Uroš Svete
Digitalno podpisal Uroš Svete
Datum: 2026.01.21 14:19:23 +01'00'