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

VSEBINA

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 v primeru kibernetskih incidentov. Načrt je državni načrt in temelji na nalogah, za katere so odgovorni posamezni ključni deležniki.

Načrt je pripravljen v letu 2024 za obveščanje javnosti v primeru kibernetskih incidentov, s posebnim poudarkom na primeru težjega kibernetskega incidenta, ki lahko preide v kritični kibernetski incident (C2), ter v primeru kritičnega kibernetskega incidenta (C1). Za načrt je odgovoren Urad Vlade Republike Slovenije za informacijsko varnosti (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, še posebej pa ob težjem kibernetskem incidentu, ki lahko preide v kritični kibernetski incident (C2), ter v primeru kritičnega kibernetskega incidenta (C1) je, da mora biti javnost o njej obveščena pravočasno, celovito in objektivno.

2. KLJUČNI TERMINI

Zakon o informacijski varnosti opredeljuje:

Kibernetska grožnja je možnost zlonamernega poskusa poškodovanja ali prekinitve računalniškega omrežja, sistema, storitev in podatkov.

Kibernetska obramba je celota ukrepov in dejavnosti države, s katerimi se odvrača, onemogoča, preprečuje ali odbija kibernetske napade v informacijskem okolju.

Kibernetska varnost je sposobnost zaščititi, varovati in braniti kibernetski prostor pred kibernetskimi grožnjami, incidenti in kibernetskimi napadi.

Kibernetski napad je napad prek kibernetskega prostora z namenom zlonamernega uničevanja, izpostavljanja, nadzorovanja ali spreminjanja, onemogočanja, zbiranja in oviranja kateregakoli dela kibernetskega prostora, vključno glede informacij, ki so bistvenega pomena za nemoteno delovanje države.

Kibernetski prostor je globalno informacijsko okolje, ustvarjeno s pomočjo elektronsko komunikacijskih omrežij in informacijskih sistemov. Kibernetski prostor omogoča nastanek, obdelavo in izmenjavo informacij.

2.1 PODROBNA RAZVRSTITEV KIBERNETSKI NAPADOV

STOPNJEVANJE V SKLADU Z ZInfV	STOPNJEVANJE NA PODLAGI KAZALNIKOV	OPIS INCIDENTA
KRITIČNI	KRITIČNI INCIDENT (C1)	Incident povzroči oteženo delovanje države, še posebej informacijskih sistemov obrambe, notranje varnosti ter sistema zaščite in reševanja. Povzročanje resne motnje delovanja osrednjih državnih storitev, motnja stabilnosti države. Ima velik negativni vpliv na omrežja in informacijske sisteme oziroma informacijske storitve zavezancev.
TEŽJI	ZELO POMEMBNI INCIDENT (C2)	Zaznan negativni vpliv na občutljive podatke in delovanje državne in kritične infrastrukture, ki je opredeljena v 5. in 6. členu ZInfV. Zaznan velik negativni vpliv na omrežja in informacijske sisteme oziroma informacijske storitve zavezancev. Negativno vpliva na delovanje informacijskih sistemov obrambe, notranje varnosti ter sistema zaščite in reševanja.
	POMEMBNI INCIDENT (C3)	Možen vpliv na izvajalce bistvenih storitev, dele državne infrastrukture in dobavno verigo za kritično infrastrukturo. Možen negativni medpodročni vpliv.
LAŽJI	SREDNJI INCIDENT (C4)	Zaznan majhen negativni vpliv na omrežja in informacijske sisteme oziroma informacijske storitve zavezancev. Vpliv na izvajalce bistvenih storitev ali vpliv na gospodarstvo in dele državne uprave ali dobavno verigo.
	LAŽJI INCIDENT (C5)	Možen vpliv na omrežja in informacijske sisteme oziroma informacijske storitve zavezancev ali priprave na napad na gospodarstvo ali državno infrastrukturo.
KIBERNETSKA GROŽNJA	VARNOSTNI DOGODEK (C6)	Zaznane kibernetske aktivnosti, ki nimajo vpliva na omrežja in informacijske sisteme oziroma informacijske storitve zavezancev. Zaznan ali možen vpliv na posamezne fizične osebe ali posamezna podjetja v državi, ki niso zavezanci.

Razpredelnica 1: Stopnje kibernetskih napadov, Vir: Nacionalni načrt odzivanja na kibernetske incidente

3. OPREDELITVE KOMUNICIRANJA PO ZAKONU O INFORMACIJSKI VARNOSTI

13. člen (priglasitev incidentov):

(8) Pristojni nacionalni organ lahko po posvetovanju z **izvajalcem bistvenih storitev**, ki je priglasil incident, obvesti javnost o posameznih incidentih, kadar je ozaveščenost javnosti potrebna za njegovo obravnavo ali zaradi preprečitve stopnjevanja incidenta ali novih incidentov.

(9) Pri obveščanju javnosti iz prejšnjega odstavka pristojni nacionalni organ upošteva ravnotežje med interesom javnosti, da je obveščena o nevarnostih, na eni strani, ter morebitno škodo za ugled in poslovanje izvajalcev bistvenih storitev, ki priglasijo incidente, na drugi strani.

14. člen (varnostne zahteve in priglasitev incidentov):

(10) Pristojni nacionalni organ lahko po posvetovanju z zadevnim **ponudnikom digitalnih storitev** obvesti javnost o posameznih incidentih ali zahteva, da to stori ponudnik digitalnih storitev, kadar je ozaveščenost javnosti potrebna za preprečitev incidenta ali obravnavo incidenta, ki že poteka, ali kadar je razkritje incidenta kako drugače v javnem interesu.

(11) Kadar javnost na podlagi prejšnjega odstavka obvešča pristojni nacionalni organ upošteva ravnotežje med interesom javnosti, da je obveščena o nevarnostih, na eni strani, ter morebitno škodo za ugled in poslovanje ponudnikov digitalnih storitev, ki priglasijo incidente, na drugi strani.

18. člen (priglasitev incidentov):

(5) Pristojni nacionalni organ lahko po posvetovanju z **organom državne uprave**, ki je priglasil incident, obvesti javnost o posameznih incidentih, kadar je ozaveščenost javnosti potrebna za preprečitev incidenta ali njegovo obravnavo.

(6) Pri obveščanju javnosti iz prejšnjega odstavka pristojni nacionalni organ upošteva ravnotežje med interesom javnosti, da je obveščena o nevarnostih, na eni strani ter morebitnim negativnim vplivom takšne objave na preiskovanje ali pregon kaznivih dejanj, javni red in mir, nacionalno varnost in obrambo države na drugi strani.

23. člen (obveščanje javnosti):

Če je v zvezi s sprejetimi ukrepi iz 21. ali prejšnjega člena tega zakona potrebno tudi obveščanje javnosti, pristojni nacionalni organ skupaj s službo vlade, pristojno za komuniciranje z javnostjo, pripravi sporočilo za javno objavo, ki ga mediji smejo objaviti le v nespremenjeni obliki.

25. člen (vodenje in vsebina seznamov):

(6) Pristojni nacionalni organ in nacionalni CSIRT ter CSIRT organov državne uprave na podlagi podatkov iz tretjega in četrtega odstavka tega člena za statistične namene in namene seznanjanja javnosti dvakrat letno pripravijo anonimizirane informacije, ki jih tudi javno objavijo na svojih spletnih straneh.

27. člen (pristojni nacionalni organ):

(7) Koordinira usposabljanje, vaje in izobraževanje na področju informacijske varnosti ter skrbi za dvig zavedanja javnosti o informacijski varnosti.

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

Ključni deležniki so:

- URSIV,
- Odzivni center,
- Ostali pristojni državni organi, glede na svoje pristojnosti,
- UKOM in
- Zavezanec po Zakonu o informacijski varnosti, 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 Uradu vlade za komuniciranje (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

Javnost mora biti o kibernetskem incidentu obveščena pravočasno, celovito in objektivno, na način, ki je dostopen in razumljiv vsem. 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,
- varovanja 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.

Podrobnosti žrtve napada bodo razkrite samo v primeru zakonskih zahtev, v primeru podajanja varnostnih napotkov glede kibernetskega incidenta pa se oblikujejo anonimizirani tehnični zapisi, ki se delijo z javnostjo v skladu s tem poglavjem. Po dogovoru s pristojnim odzivnim centrom se, kadar zavezanec to želi, zaradi zaščite strank ali posla lahko objavijo podrobni podatki o kibernetskem incidentu in napadenem zavezancu.

5.2 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 PR služba URSIV na spletišču GOV.SI in na svojih družbenih omrežjih oz. jih posreduje v objavo medijem.

5.2.1 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.

5.2.2 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.

5.3 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.

5.5 OBJAVA NUJNIH SPOROČIL V MEDIJIH

Po predpisih in na zahtevo državnih organov, javnih podjetij in zavodov morajo brez odlašanja in brezplačno objaviti nujno sporočilo v zvezi z resno ogroženostjo življenja, zdravja ali premoženja ljudi, povezano z resnim tveganjem za življenje, zdravje ali premoženje ljudi ter z ogrožanjem kulturne in naravne dediščine ter varnosti države (25. člen ZMed).

V takih primerih so za takojšnje posredovanje sporočil državnih organov javnosti pristojni:
– Televizija Slovenija,
– Radio Slovenija,
– Slovenska tiskovna agencija,
– po potrebi tudi drugi mediji.

7. NALOGE IN AKTIVNOSTI UKOM

UKOM v sodelovanju z URSIV, ter zavezancem, ki ga je incident prizadel, lahko sodeluje v sledečih fazah komuniciranja:
:

- koordinira pripravo skupnih sporočil za javnost in jih posreduje javnosti prek medijev, svetovnega spleta (preko spletnega mesta Vlade RS) in družbenih omrežij;
- obvešča tujo javnost, 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;
- po potrebi organizira in vodi novinarsko središče;
- organizira novinarske konference za domače in tuje novinarje;
- navezuje stike z redakcijami tujih medijev in novinarji, akreditiranimi v Sloveniji, ter skrbi, da imajo na razpolago informativno in drugo gradivo in da so jim dostopni informacijski viri;
- spremlja poročanje domačih in tujih medijev ter pripravlja izbor prispevkov, objavljenih v njih (t. i. klipinge) in
- opravlja druge naloge iz svoje pristojnosti.

Po potrebi UKOM izvede še naslednje naloge:

Glede na razsežnosti kriznega dogodka UKOM 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.

Da bi bilo obveščanje javnosti o razmerah na ogroženem območju, sprejetih ukrepih, izvajanju nalog zaščite, reševanja in pomoči čimbolj sprotno in celovito, UKOM po potrebi organizira novinarske konference, na katerih predstavniki vlade, pristojnih ministrstev, Štaba civilne zaščite RS in pooblaščeni izvedenci poročajo o razmerah, sprejetih ukrepih, izvajanju aktivnosti in svetujejo o ravnanju v nastalih razmerah.

UKOM da pobudo pristojnim na URSIV, in zavezancem, ki ga je incident prizadel, da zagotovijo (opremijo) posebno snemalno ekipo, ki bo zaščitena lahko zagotavljala slikovno oziroma filmsko gradivo za medije z območij, kjer bo dostop novinarjem, reporterjem in snemalcem zaradi ogroženosti prepovedan.

8. 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 22.11. 2024.

Skrbnika načrta:

DIREKTORICA UKOM
Petra Bezjak Cirman

Petra Bezjak Cirman
Digitalno podpisal Petra Bezjak Cirman
Datum: 2024.11.22 14:26:32 +01'00'

DIREKTOR URSIV
Dr. Uroš Svete

Uroš Svete
Digitalno podpisal Uroš Svete
Datum: 2024.11.22 14:32:00 +01'00'