REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

Vojkova cesta 55, 1000 Ljubljana

T: 01 471 23 73
F: 01 471 29 78
E: gp.mo@gov.si
E: glavna.pisarna@mors.si
www.mo.gov.si

PRILOGA 1

Številka: 870-18/2020-58
Ljubljana, dne 06. 04. 2021
EVA (če se akt objavi v Uradnem listu RS)
GENERALNI SEKRETARIAT VLADE REPUBLIKE SLOVENIJE **gp.gs@gov.si**

ZADEVA: Poročilo o sodelovanju Republike Slovenije na Natovi vaji kibernetske obrambe »Cyber Coalition 2020 (CC20«) – 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 in 55/17) in v povezavi z drugim odstavkom 12. člena Pravilnika o vajah v obrambnem sistemu (Uradni list RS, št. 100/13), je Vlada Republike Slovenije na____ seji dne_____ pod točko dnevnega reda_____sprejela naslednji

S K L E P

Vlada Republike Slovenije je sprejela Poročilo o sodelovanju Republike Slovenije na Natovi vaji kibernetske obrambe »Cyber Coalition 2020 (CC20)«.

mag. Janja Garvas Hočevar
v. d. GENERALNE SEKRETARKE

Prejmejo:

- Ministrstva,
- Urad Vlade Republike Slovenije za varovanje tajnih podatkov,
- Urad Vlade Republike Slovenije za komuniciranje,
- Slovenska obveščevalno varnostna agencija,
- nacionalni odzivni center za omrežne incidente SI-CERT pri javnem zavodu ARNES,
- Telekom Slovenije d.d.,
- Kontrola zračnega prometa Slovenije d.o.o.,
- Javna agencija za civilno letalstvo Republike Slovenije,
- Slovenske železnice d.o.o.

2. Predlog za obravnavo predloga zakona po nujnem ali skrajšanem postopku v državnem zboru z obrazložitvijo razlogov:

/

3.a Osebe, odgovorne za strokovno pripravo in usklajenost gradiva:

- Mag. Marko Doblekar, generalni sekretar v Ministrstvu za obrambo

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

/

4. Pri obravnavi gradiva bosta sodelovala:

/

5. Kratek povzetek gradiva:

Sodelovanje Republike Slovenije na Natovi vaji kibernetske obrambe Cyber Coalition 2020 (CC 20) je bilo načrtovano z Načrtom vaj v obrambnem sistemu in sistemu varstva pred naravnimi in drugimi nesrečami v letu 2020 (sklep Vlade RS, št. 84300-1/2020/3 z dne 23. 1. 2020 z dopolnitvami št. 84300-1/2020/9 z dne 11. 4. 2020 in 84300-1/2020/9 z dne 18. 6. 2020). Glede na načrtovano sodelovanje je Vlada RS sprejela Sklep o sodelovanju Republike Slovenije na Natovi vaji kibernetske obrambe »Cyber Coalition 2020 (CC20)«, (VRS št. 87000-10/2020/3, z dne 17. 9. 2020). Skladno z navedenim sklepom, Ministrstvo za obrambo Republike Slovenije poročilo o vaji pošlje v sprejem na Vlado Republike Slovenije.

Vaja Cyber Coalition je redna letna in hkrati največja vaja Nata na področju kibernetske obrambe, ki jo načrtuje in v sodelovanju s predstavniki članic vodi Zavezniško poveljstvo za transformacijo (Allied Command Transformation - ACT) pod okriljem Vojaškega odbora (Military Committee - MC).

Vaja je, ob upoštevanju ukrepov pristojnih institucij za preprečevanje širjenja okužb s COVID-19, potekala od 16. 11. do vključno 20. 11. 2020. Namen vaje CC20 je bil izboljšati sodelovanje in okrepiti sposobnost Nata in zaveznic pri zaščiti in obrambi kibernetskega prostora. Republika Slovenija si je v skladu z zgoraj navedenim Sklepom o sodelovanju Republike Slovenije na Natovi vaji kibernetske obrambe poleg sodelovanja pri izpolnjevanju Natovih ciljev zadala tudi cilj izboljšanje sodelovanja med nacionalnimi deležniki in krepitve nacionalnih zmogljivosti na področju kibernetske obrambe. Natov scenarij vaje je bil nadgrajen z nacionalnim scenarijem, s katerim so se v reševanje kibernetskih incidentov vključile tudi gospodarske družbe in agencije, katerih dejavnost je posebnega pomena za obrambo države. Poglavitni cilj nacionalnega dela scenarija je bil preveriti ustreznost rešitev obravnavanja kibernetskih incidentov po osnutku predloga Nacionalnega načrta odzivanja na kibernetske incidnete, ki ga je pripravila Uprava Republike Slovenije za informacijsko varnost.

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	NE

	načrtovanja – razvojne politike na ravni programov po strukturi razvojne klasifikacije programskega proračuna – razvojne dokumente Evropske unije in mednarodnih organizacij	

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

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		

/

7.b Predstavitev ocene finančnih posledic pod 40.000 EUR:

Gradivo nima finančnih posledic.

8. Predstavitev sodelovanja z združenji občin:

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

Gradivo (predpis) je bilo poslano v mnenje:
– Skupnosti občin Slovenije SOS: NE
– Združenju občin Slovenije ZOS: NE
– Združenju mestnih občin Slovenije ZMOS: NE

Predlogi in pripombe združenj so bili upoštevani:
– v celoti,
– večinoma,
– delno,
– niso bili upoštevani.

Bistveni predlogi in pripombe, ki niso bili upoštevani.
/

9. Predstavitev sodelovanja javnosti:

Gradivo je bilo predhodno objavljeno na spletni strani predlagatelja:	NE
V skladu 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, 80/13 in 10/14) javnost ni bila povabljena k sodelovanju, ker gre za predlog sklepa vlade.	
10. Pri pripravi gradiva so bile upoštevane zahteve iz Resolucije o normativni dejavnosti:	NE
11. Gradivo je uvrščeno v delovni program vlade:	NE
	Mag. Matej Tonin **minister**

Poslano:
- naslovniku,
- DOZ,
- OVS,
- SGS.

Poročilo

o sodelovanju Republike Slovenije na Natovi vaji kibernetske obrambe »Cyber Coalition 2020 (CC20)«.

UVOD

Kibernetska vaja Cyber Coalition je redna letna vaja Nata na področju kibernetske obrambe, ki jo načrtuje in v sodelovanju s predstavniki članic vodi Zavezniško poveljstvo za transformacijo (Allied Command Transformation - ACT) pod okriljem Vojaškega odbora (Military Committee - MC) in je tudi največja vaja zavezništva na področju kibernetske obrambe. Republika Slovenija (v nadaljevanju besedila: RS) je z izvedbo vaje Cyber Coalition 2020 (v nadaljevanju besedila: CC20), ki je potekala od 16. 11. do 20. 11. 2020, uresničila v Načrtu vaj v obrambnem sistemu in sistemu varstva pred naravnimi in drugimi nesrečami v letu 2020 (sklep Vlade RS, št. 84300-1/2020/3 z dne 23. 1. 2020 z dopolnitvami št. 84300-1/2020/9 z dne 11. 4. 2020 in 84300-1/2020/9 z dne 18. 6. 2020) načrtovano vajo.

Natov osnovni scenarij vaje je temeljil na namišljeni Natovi misiji na visokem severu na fiktivnem otoku Icebergen. Na njem je zavezništvo, na podlagi povabila države gostiteljice Andvarije, vzpostavilo misijo Collective Nordic Deffence Force (CNDF). V njej je s popolnjenvanjem zračne komponente sodelovala tudi RS. Pripadniki Slovenske vojske (SV) so pri svojem delu uporabljajli komunikacijski sistem brez stopnje tajnosti, ki pa je bil podvržen kibernetskim aktivnostim neznanih akterjev. Nadgradnja s slovenskim delom scenarija je temeljila na dodatni satelitski komunikacijski povezavi med Andvarijo in prestolnico, poleg tega pa so bili dodani še ostali elementi, ki so omogočili vključitev v vajo tudi ostalim vadbencem v RS.

Namen vaje CC20 na nivoju Nata je bil izboljšati sodelovanje in okrepiti sposobnost Nata in zaveznic pri zaščiti in obrambi kibernetskega prostora ter izvajanju vojaških operacij v kibernetskem prostoru.

RS je s sodelovanjem na vaji vadila mehanizme sodelovanja ter izmenjavo dobrih praks med zaveznicami in Natom, izmenjavo podatkov in obveščanja, splošno razumevanje in situacijsko zavedanje o grožnjah v kibernetskem prostoru ter sodelovala pri preverjanju tehničnih zmogljivosti in ustreznosti postopkov pri obrambi statičnih in premestljivih komunikacijsko informacijskih omrežjih.

Nadgradnja Natovega scenarija z nacionalnim scenarijam vaje je v RS v reševanje tehničnih in organizacijsko postopkovnih izzivov omogočilo vključitev ministrstev, agencij, vladnih služb in izvajalcev bistvenih storitev. Z ustanovitvijo Uprave RS za informacijsko varnost (URSIV) se je koordinacija in celovito upravljanje področja informacijske varnosti, pod katero spada tudi kibernetska obramba, vzpostavila nacionalna entiteta, ki zagotavlja celovitost in sistematičnost pri zaznavi, obravanavi in odzivanju na kibernetske incidente. Preveriti odziv na kibernetske incidente po predlogu Nacionalnega načrta odzivanja na kibernetske incidente (v nadaljevanju besedila: NOKI) in ga ob uspešni uporabi implementirati v normativnem dokumentu, je bil eden izmed osrednjih ciljev vaje CC20. Poleg tega se je preverjalo tudi odziv nacionalno varnostnega sistema RS na posredna ali neposredna ogrožanja in varnostna tveganja v primeru kibernetske grožnje ali incidenta v kibernetskem prostoru, preverjalo in vadilo izmenjavo podatkov in obveščanja o kibernetskih incidentih z

uporabo nacionalne platforme za izmenjavo informacij o škodljivi kodi (angl. Malware Information Sharing Platform – MISP) in analiziralo kibernetski incident skozi dobavno verigo.

PRIPRAVE NA VAJO

Sodelovanje RS na Natovi vaji kibernetske obrambe CC20 je bilo načrtovano z Načrtom vaj v obrambnem sistemu in sistemu varstva pred naravnimi in drugimi nesrečami v letu 2020. Glede na načrtovano sodelovanje je Vlada RS sprejela Sklep o sodelovanju Republike Slovenije na Natovi vaji kibernetske obrambe »Cyber Coalition 2020 (CC20«) (sklep Vlade RS, št. 87000-10/2020/3, z dne 17. 9. 2020).

V okviru priprav na vajo je bilo na ravni Nata izvedenih več načrtovalnih konferenc, ki so zaradi epidoemioloških razmer potekale v obliki avdio video konferenc (v nadaljevanju besedila: AVK). Konferenc so se udeleževali predstavniki Ministrstva za obrambo iz Službe za informatiko in komunikacije ter Direktorata za obrambne zadeve. Priprave na vajo in sama vaja je potekala v skladu z Natovim scenarijem, opredeljenim v dokumentu EXERCISE CYBER COALITION 2020 - EXERCISE SPECIFICATION (št. ACT/CD/CAP/TT-3022/Ser: NU:0080 z dne 30. 7. 2020) ter smernicami Nato akcijskega načrta opredelitve kibernetskega prostora kot samostojne planske in operativne domene.

Vlada RS je z zgoraj navedenim sklepom določila vadbence v državi, in sicer: Generalni sekretariat Vlade RS, Ministrstvo za obrambo, Ministrstvo za notranje zadeve, Ministrstvo za javno upravo, Ministrstvo za zunanje zadeve, Ministrstvo za pravosodje, Urad Vlade Republike Slovenije za varovanje tajnih podatkov, Urad Vlade Republike Slovenije za komuniciranje, Slovensko obveščevalno varnostno agencijo, nacionalni odzivni center za omrežne incidente SI CERT pri javnem zavodu ARNES ter Telekom Slovenije d.d. V okviru vadbneca Ministrstva za javno upravo je posebno vlogo imela URSIV kot nacionalno pristojni organ za informacijsko varnost, poleg tega pa je ministrstvo na vaji opravljalo vlogo odzivnega centra za kibernetsko varnost državne uprave (SIGOV-CERT). Vlada RS je za vodjo vaje imenovala generalnega sekretarja sekretariata na Ministrstvu za obrambo ter za njegovega namestnika vodjo Službe za informatiko in komunikacije na istem ministrstvu.

S sklepom vodstva vaje so se v sodelovanje na vaji vključili še Ministrstvo za infrastrukturo vključno z Agencijo RS za civilno letalstvo, Kontrola zračnega prometa RS d.o.o. ter Slovenske železnice d.o.o.

Določena sta bila tudi nacionalna predstavnika Slovenije (EXCON), ki sta svoji vlogi opravljala na daljavo iz RS.

Ministrstvo za obrambo je vodilo in izvajalo priprave na vajo. Za učinkovito izvajanje vaje je vodja vaje izdal Navodilo za organizacijo in izvedbo Natove vaje CC20 v Republiki Sloveniji (MO; št. 870-18/2020-37 z dne 13. 11. 2020), s katerim je opredelil vlogo glede na scenarij vaje in določil naloge SVNKON CNDF CC20, Tehnične skupine Mil-CERT, CIRT-MO, lokalnih koordinatorjev vaje (angl. Local Trainers), Skupine za pripravo nacionalnega scenarija, Skupine za koordinacijo ter Skupine za načrtovanje in pripravo vaje CC20. Določen je bil način pošiljanja dnevnih poročil in končnega poročila vadbencev. Skupino za pripravo nacionalnega scenarija je vodil URSIV.

Za uvod na priprave na vajo je bil julija 2020 sklican posvet vseh udeležecev vaje. Tekom priprav se je sestalo vodstvo vaje, posebej pa se je sestajala skupina za pripravo nacionalnega scenarija vaje, ki je izhajal iz osnovnih predlog igral Natovega navodila za vajo (CC20 Player Instructions Handbook). Izvedena so bila tudi številna usklajevanja in informativni sestanki v različnih kombinacijah manjših sestav skupin za pripravo scenarija vaje. Udeležba na sestankih je bila velikokrat okrnjena zaradi bolniških odsotnosti ključnih udeležencev skupine za izdelavo scenarija vaje, kar je povzročilo operativne težave pri oblikovanju scenarija.

Na pripravah na vajo so bila vadbencem predstavljena igrala, ki so imela specifične ranljivosti, tehnične pomanjklivosti ali škodljivo kodo in bi vključena v informacijski sistem ogrožala razpoložljivost, celovitost ali zaupnost podatkov.

Poleg organizacijskih priprav na vajo v RS je Ministrstvo za obrambo za vajo izvedlo tudi tehnične priprave, ki so vključevale zagotovitev skupinskih elektronskih naslovov za vadbence Ministrstva za obrambo, preverjanje delovanja podatkovnih in avdio komunikacij ter upravljanje s slovenskim delom kibernetskega vadbišča.

Analize predhodnih vaj so pokazale, da manjka platforma, ki bi omogočala izmenjavo informacij o škodljivi kodi oz. ostalih tehničnih informacijah o reševanju kibernetskih incidentov. Sprejeta je bila odločitev, da se na vaji preizkusi uporaba MISP platforme. Za uporabo sta bili določeni dve platformi, ločeno za nacionalni in Nato nivo.

V okviru priprav na vajo so bili vadbenci večkrat opozorjeni na skrbno ravnanje s tajnimi podatki. Posebnih priprav za delo s tajnimi podatki v okviru vaje ni bilo.

IZVEDBA VAJE

Epidemiološke razmere so narekovale izvedbo vaje z upoštevanjem ukrepov za preprečevanje širjenja okužb z virusom. Natovo vodstvo vaje ni usmerjalo iz Tartuja v Estoniji ampak iz različnih lokacij članic zavezništva. Slovenski član vodstva vaje je deloval v RS.

Vsak izmed vadbencev se je organizacijsko in operativno prilagodil razmeram epidemije COVID-19. Odziv je bil večinoma skladen z veljavnimi načrti odzivanja na kibernetske incidente. Skupine, ki so bile oblikovane pri vadbencih, so večinoma delovale razpršeno (angl. virtual teams). Brez fizičnih stikov, z uporabo omrežnih orodij so kljub oddaljenosti, lahko delili svoje ideje, informacije in rezultate z drugimi člani skupine. Za medsebojno komuniciranje ter koordinacijo z lokalnima koordinatorjema so uporabljale AVK sistem, ki ga je zagotovilo Ministrstvo za obrambo.

Vadbenci so za prenos podatkov uporabljali različna omrežja, ki so omogočala prenos stopnjevanih tajnih podatkov:

- internet (za podatke in informacije brez stopnje tajnosti);
- KIS MO Intranet, KIS NCKU ter depešni sistem MZZ (do vključno stopnje tajnosti Interno);
- SI NS NOAN omrežje (do vključno stopnje NATO SECRET).

V RS se je vsak izmed vadbencev, ki so bili vključeni v reševanje kibernetskega incidenta, že v pripravah na vajo seznanil z okvirnim scenarijem incidentov. Igrala so prejeli v začetku vaje in ob proženju incidenta tudi pričeli s tehničnem reševanjem incidenta. Igrala so bila vadbencem dodeljena skupaj z vsebinskim ozadjem, pripravljenim za scenarij posameznih incidentov. Vzpostavljena je bila tudi komunikacija za poročanje v okviru CNDF operacije, kjer mora SVNKON v Poveljstvo zračne komponente (angl. Air Component Command – ACC) posredovati dnevno tehnično in operativno poročilo.

Igrala so bila v RS dodeljena glede na področje dela vadbenca oziroma organizacijsko strukturo SV.

Skupno je bilo na vaji sedem različnih varnostnih dogodkov (igral), za katere so bili odgovorni posamezni vadbenci:

- Varnostni dogodek na kibernetskem vadbišču Cyber Range – odziv odzivni center SV (Mil – CERT);
- Motnje v delovanju satelitskih komunikacij – odziv Telekom Slovenije;
- Zlonamerna aplikacija na pametnem telefonu – odziv Sove;
- Zloraba medijskega portala MOM – odziv MO-CERT;
- Okužen računalnik (ob sodelovanju na logistični konferenci) – odziv SIGOV-CERT, Ministrstvo za infrastrukturo, Policija, Slovenske železnice d.o.o.;
- Nabavna veriga – odziv URSIV, SIGOV-CERT, Slovenske železnice, d.o.o., KZPS;
- Dezinformacija, ki ne doseže javnosti – odziv Ministrstva za zunanje zadeve (MZZ).

Večina vadbencev je z dnevnimi poročili podajala informacije o napredku pri reševanju kibernetskih incidentov, na podlagi katerih je bilo pripravljeno tudi dnevno zbirno poročilo za vse aktivne dneve vaje. Poročilo je bilo prvi dan poslano vsem vadbencem v seznanitev, naslenje dni pa po sprejeti odločitvi samo vodstvu vaje.

URSIV je večinoma prejemal informacije o incidentih skladno z osnutkom NOKI. Potencialno ranljivost prenosnikov je ovrednotila z oceno C2, kar pomeni kritični incident z možnostjo vpliva na občutljive podatke in delovanje državne in kritične infrastrukture ali delovanje informacijskih sistemov obrambe, notranje varnosti ter varstva pred naravnimi in drugimi nesrečami. Zaradi incidenta je bila sklicana tudi koordinacijska skupina za usklajevanje kibernetske varnosti na nacionalnem nivoju.

Zadnji dan vaje je bilo pripravljeno tudi poročilo Prve ugotovitve (angl. First Impressions), ki je bilo preko predstavnika RS v Natovem vodstvu vaje CC20 poslano organizatroju vaje v Natu.

ANALIZA VAJE - Odprta vprašanja in predlogi za nadaljnje delo

Priprave na vajo kot tudi vaja je bila izvedena v času izvajanja ukrepov za preprečevanje širjenja okužb s COVID-19, kar je otežilo optimalno pripravo nacionalnega scenarija in tudi samo izvedbo vaje. S prilagoditvami dela, vzpostavitvijo medsebojnega komuniciranja na daljavo, ki je nadomestilo timsko delo s fizično prisotnostjo udeležencev, je bila vaja kibernetske obrambe CC20 uspešno izvedena.

Na vaji so sodelovali vadbenci na različnih nivojih v strukturi kibernetskega prostora: strateški, taktični in tehnični nivo, kar je zahtevalo dodatne napore pri obvladovanju poteka celotne vaje. Gospodarske družbe, ki so bile vključene v vajo, so vključno s posameznimi vadbenimi skupinami organov državne uprave na vaji sodelovale kot izvajalci bistvenih storitev, taktično tehnični nivo so bili varnostno operativni centri (angl. Security Operations Center – SOC) ter strateški nivo ministrstva in URSIV.

Prva analiza vaje je bila opravljena na skupnem AVK srečanju udeležencev in vodstva, nato pa so vadbenci poslali tudi končna poročila, v katerih so zbrali ugotovitve in predloge za izboljšave.

RS je bila v uspešnosti reševanja tehničnih izzivov na nivoju Nata uspešnejša kakor prejšnja leta, zahvaljujoč sodelovanju večjega števila strokovnjakov na vaji.

Prevlada splošna ocena, da je bila vaja dobro pripravljena in cilji vaje CC20 v RS doseženi:

- uspešno se je preveril in preizkusil odziv nacionalno varnostnega sistema na posredna in neposredna ogrožanja in varnostna tveganja v primeru kibernetske grožnje ali incidneta v kibernetskem prostoru;
- URSIV je uspešno izvedel medresorsko usklajevanje preko koordinacijske skupine za primer kritičnega incidenta;
- Predlog NOKI se je izkazal kot dobra osnova, na kateri bodo na podlagi izkušenj, pridobljenih na vaji, opravljeni popravki in prilagoditve ter pred dokončno uveljavitvijo usklajene z vsemi deležniki;
- MISP platforma se je izkazala kot zelo uporabna platforma za tehnični nivo reševanja kibernetskih incidentov, za procesni (situacijski) del kot so izmenjave podatkov glede vpliva, posledic in sprejemanja ukrepov za preprečevanje posledic incidenta pa je potrebna nadaljnja razprava o uporabnosti;
- V manjši meri se je preverilo normativne podlage in procese za usklajevanje in izvajanje postopkov kibernetske obrambe, ki so pokazale določene pomanjkljivosti v poznavanju predpisanih postopkov v primeru zaznave kibernetskega incidenta;
- Analiza kibernetskega incidenta skozi dobavno verigo ostaja segment, kateremu bo potrebno v prihodnosti nameniti več pozornosti, tudi s poglobljenim ozadjem zgodbe;
- Sodelovanje in funkcionalnost odzivanja na kibernetske incidente z gospodarskim sektorjem je bila uspešno preverjena.

Podan je bil predlog, da se varnostno operativni centri (SOC) označujejo z oznako, iz katere je razvidna strokovnost kadrovske popolnjenosti centra (OC-P – prometni podatki; OC-A – analiza škodljive kode).

Ključne ugotovitve, podane na analizi vaje in v poročilih vadbencev:

a) Izrazita deficitarnost specifičnega kadra za reševanje tehničnih incidentov s področja škodljive kode v nasprotju s številom strokovnjakov s področja analize prometnih podatkov, katerih je v tem trenutku zadostno.
b) Preveliko število komunikacijskih kanalov za poročanje o napredku pri odpravi kibernetskega incidenta (tehnični vidik) in upravljanja le-tega (situacijski ali procesni vidik) s prioriteto odziva in ob upoštevanju dejstva, da je za nacionalni sistem

odzivanja na kibernetske incidente in napade ključno medresorsko sodelovanje in izmenjava podatkov.

c) Situacijsko upravljanje incidenta je odvisno od pridobljenih informacij o poteku in stopnji obvladovanja incidenta in ne od prejemanja tehničnih informacij.
d) Prepletanje Nato in nacionalnega nivoja vaje predstavlja bistveno bolj kompleksen izziv.

Predlogi za izboljšanje ugotovljenih pomanjkljivosti:

a) Pripoznanje kadrovskega deficita s strokovnim znanjem za reševanje tehničnih incidentov s področja škodljive kode in poziv Vladi RS k vzpodbujanju zaposlovanja tovrstnih kadrov.
b) Po predhodno opravljeni analizi komunikacijsko informacijskih sistemov v RS preučitev možnosti medsebojne povezljivosti omrežij iste stopnje tajnosti s ciljem vključenosti čim večjega števila deležnikov s področja informacijske varnosti, kar bo omogočalo široko medresorsko sodelovanje in izmenjavo podatkov.
c) Prilagoditev modela situacijskega upravljanja incidentov nacionalno pristojnega organa, ki bi temeljil na informaciji o poteku in stopnji obvladovanja incidenta.
d) Slovenija nima resursov za pripravo tehničnih igral kot jih pripravi NATO skupnost, zato je pomembno, da v RS izkoristimo to možnost s ciljem nadgrajevanja nacionalne varnosti v kibernetski domeni. V cilju kvalitetne umeščenosti nacionalnega dela vadbenega okvirja v prihodnjih vajah CC naj MO pred načrtovanjem aktivnosti organizira posvetovalni sestanek z vsemi nacionalnimi deležniki o umestitvi nacionalnega scenarija v NATO vajo Cyber Coalition.

Za čim hitrejše odzivanje in tehnično obvladovanje kibernetskih incidentov bi morali vzpostaviti nacionalno MISP platformo, v katero bi bili vključeni vsi ključni odzivni centri v RS.

ZAKLJUČEK

Vaja Cyber Coalition je redna letna in hkrati največja vaja Nata na področju kibernetske obrambe, ki jo načrtuje in v sodelovanju s predstavniki članic vodi Zavezniško poveljstvo za transformacijo (Allied Command Transformation - ACT) pod okriljem Vojaškega odbora (Military Committee - MC).

V primerjavi s prejšnjimi se je v letošnji vaji več pozornosti posvetilo umeščenosti nacionalno pristojnega organa za odzivanje na kibernetske incidente URSIV v kibernetskem prostoru RS. Državnim organom so se pridružile tudi gospodarske družbe kot izvajalke bistvenih storitev po Zakonu o informacijski varnosti (Uradni list RS, št. 30/18), kar je omogočilo preigravanje postopkov obveščanja, ukrepanja, tehničnega odzivanja in koordinacije po vertikalni liniji sistema odzivanja na kibernetske incidente. Za prepoznane pomanjkljivosti, ki bi v primeru realne situacije pomenile motnjo v odzivanju na incident, so nakazane možnosti rešitev, ki se bodo odrazile v načrtih odzivanja na kibernetske incidente.

Cilji vaje v RS so bili doseženi. Uspešno se je preveril in preizkusil odziv nacionalno varnostnega sistema na posredna in neposredna ogrožanja in varnostna tveganja zaradi groženj ali incidentov v kibernetskem prostoru. URSIV je na vaji preizkusil odzivanje na

kibernetske incidente po predlogu načrta in izvedel medresosrko usklajevanje za primer kritičnega incidenta. Z uporabo MISP platforme se je preverilo tudi njeno primernost za tehnični in situacijski nivo reševanja incidentov, pri čemer se je za slednji nivo izkazala potreba po nadaljnji razpravi o njeni uporabnosti. Uspešno je bila preverjeno tudi sodelovanje in funkcionalnost odzivanja na kibernetske incidente z gospodarskim sektorjem.

S sodelovanjem RS na Natovi vaji kibernetske obrambe CC20 so bile pridobljene dodatne izkušnje in spoznanja, ki bodo nedvomno pripomogla k nadgradnji odzivanja na kibernetske incidente v realnem okolju. Na priprave na vajo in njeno izvedbo je vplivala zaostrena zdravstvena situacija, ki je preprečevala optimalno izvedbo, vendar jo je kljub temu organizatorjem uspelo pripeljati do zaključka.

MINISTRSTVO ZA OBRAMBO