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

Številka: 870-19/2021-74
Ljubljana, dne 18. 03. 2022
EVA (če se akt objavi v Uradnem listu RS)
GENERALNI SEKRETARIAT VLADE REPUBLIKE SLOVENIJE **gp.gs@gov.si**
GENERALNI SEKRETARIAT VLADE REPUBLIKE SLOVENIJE **gp.gs@gov.si**

ZADEVA: Poročilo o sodelovanju Republike Slovenije na Natovi vaji kibernetske obrambe »Cyber Coalition 2021 – CC21« – 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 in 44/21), 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 2021 – CC21«.

Mag. Janja Garvas Hočevar,
vršilka dolžnosti generalnega sekretarja

Prejmejo:

- Ministrstvo za obrambo,
- Ministrstvo za infrastrukturo,
- Ministrstvo za javno upravo,
- Ministrstvo za pravosodje,
- Ministrstvo za zdravje,
- Ministrstvo za zunanje zadeve,
- Ministrstvo za notranje zadeve,
- Slovenska obveščevalno varnostna agencija,
- Urad Vlade Republike Slovenije za informacijsko varnost,
- Agencija Republike Slovenije za kominikacijska omrežja in storitve,
- Agencija Republike Slovenije za energijo,
- ELES, d.o.o.,

- nacionalni odzivni center za omrežne incidente SI-CERT pri javnem zavodu ARNES.

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:

- mag. Matej Tonin, minister za obrambo,
- Tone Slak, državni sekretar na Ministrstvu za obrambo.

5. Kratek povzetek gradiva:

Vaja Cyber Coalition (CC, v nadaljevanju: vaja CC) je največja vaja Nata s področja kibernetske obrambe. V sodelovanju s predstavniki članic zavezništva jo pod okriljem Vojaškega odbora (Military Committee - MC) načrtuje in vodi Zavezniško poveljstvo za transformacijo (Allied Command Transformation - ACT). Vaja Cyber Coalition 21 (v nadaljevanju: vaja CC21) je, ob upoštevanju ukrepov za preprečevanje širjenja okužb s COVID-19, potekala od 29. 11. 2021 do 3. 12. 2021. Namen vaje CC je vaditi in preveriti zmogljivosti, postopke in orodja, ki jih Nato in zaveznice uporabljajo pri svojem rednem delu za zaščito in obrambi kibernetskega prostora, ne pa tekmovanje med vadbenci.

Sodelovanje Republike Slovenije (RS) na Natovi CC21 je bilo načrtovano z Načrtom vaj v obrambnem sistemu in sistemu varstva pred naravnimi in drugimi nesrečami v letu 2021 (sklepi Vlade RS, št. 84300-15/2020/4 z dne 7. 1. 2021, št. 84300-15/2020/8 z dne 19. 5. 2021 in št. 84300-15/2020/14 z dne 22. 9. 2021, v nadaljevanju: načrt vaj). Glede na načrtovano sodelovanje je Vlada RS sprejela Sklep o sodelovanju RS na Natovi vaji kibernetske obrambe »Cyber Coalition 2021 – CC21« (sklep Vlade RS, št. 87000-15/2021/3 z dne 14. 10. 2021, v nadaljevanju: sklep o sodelovanju). Skladno z navedenim sklepom Ministrstvo za obrambo RS pripravi poročilo o vaji CC21 ter ga pošlje v pregled in sprejem Vladi RS.

RS je skladno s sklepom o sodelovanju dopolnila Natove cilje vaje CC21 z nacionalnimi cilji, z namenom preveriti odzivanje nacionalno varnostnega sistema RS v primeru kompleksnih kibernetskih groženj. RS je Natov scenarij vaje CC21 dopolnila z nacionalnim scenarijem ter jo tako razširila in povezala z nacionalno kibernetsko vajo, v kateri so poleg državnih organov sodelovale tudi gospodarske družbe in agencije s področja telekomunikacij ter prenosa in distribucije električne energije.

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:
(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: /
Bistveni predlogi in pripombe, ki niso bili upoštevani./

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 in 10/14, 146/20, 35/21, 51/21 in 114/21) javnost ni bila povabljena k sodelovanju, saj gre za predlog sklepa Vlade RS.	
10. Pri pripravi gradiva so bile upoštevane zahteve iz Resolucije o normativni dejavnosti:	DA
11. Gradivo je uvrščeno v delovni program vlade:	NE
	Tone Slak **državni sekretar**

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

Poročilo
o sodelovanju Republike Slovenije na Natovi vaji kibernetske obrambe
»Cyber Coalition 2021 – CC21«

UVOD

Vaja Cyber Coalition (CC, v nadaljevanju: vaja CC) je največja vaja Nata s področja kibernetske obrambe. V sodelovanju s predstavniki članic zavezništva jo pod okriljem Vojaškega odbora (Military Committee - MC) načrtuje in vodi Zavezniško poveljstvo za transformacijo (Allied Command Transformation - ACT). Republika Slovenija (v nadaljevanju: RS) je z izvedbo vaje Cyber Coalition 2021 (v nadaljevanju: vaja CC21), ki je potekala od 29. 11. 2021 do 3. 12. 2021, uresničila v Načrtu vaj v obrambnem sistemu in sistemu varstva pred naravnimi in drugimi nesrečami v letu 2021 (sklepi Vlade RS, št. 84300-15/2020/4 z dne 7. 1. 2021, št. 84300-15/2020/8 z dne 19. 5. 2021 in št. 84300-15/2020/14 z dne 22. 9. 2021, v nadaljevanju načrt vaj) načrtovano vajo.

Osnovni scenarij vaje CC21 je temeljil na mednarodni misiji Nata na namišljenem otoku, ki se je v bližnji preteklosti razdelil na dve državi, med katerima prihaja do trenj. Misija Nata, v kateri so v okviru vaje CC21 v posameznih vojaških poveljstvih delovale vse države udeleženke vaje CC21, se je soočala z različnimi načini kibernetskega delovanja nasprotnika. Dogodki na vaji CC21 so bili proženi v skladu s scenarijem vaje CC21 in razvojem petih zgodb, in so se navezovali na pravna vprašanja, na katera so odgovarjali nacionalni pravni strokovnjaki. Celotno dogajanje na vaji CC21 je bilo umeščeno v zgodovinski kontekst, ki je bil izčrpno opisan v scenariju, potek pa so dodatno osmislile medijske objave pred in med izvajanjem vaje CC21.

Cilj Natove vaje CC21 je bil vaditi in preverjati zmogljivosti, postopke in orodja za reševanje kibernetskih incidentov, ki jih Nato in zaveznice uporabljajo pri svojem rednem delu. Osnovni namen vaje CC21 je temeljil na reševanju tehničnih problemov in vadbi postopkov sodelovanja ter skupnega reševanja problemov, ne pa tekmovanja med vadbenci.

RS je skladno s Sklepom o sodelovanju RS na vaji kibernetske obrambe »Cyber Coalition 2021 – CC21« (sklep Vlade RS, št. 87000-15/2021/3 z dne 14. 10. 2021, v nadaljevanju: sklep o sodelovanju) dopolnila Natove cilje vaje CC21 z nacionalnimi cilji, z namenom preveriti odzivanje nacionalno varnostnega sistema RS v primeru kompleksnih kibernetskih groženj in incidentov. RS je Natov scenarij vaje CC21 dopolnila z nacionalnim scenarijem, in tako Natovo vajo CC21 v RS razširila z nacionalno kibernetsko vajo. V skladu z nacionalnim scenarijem so na Natovi vaji CC21 in nacionalni vaji v RS poleg državnih organov sodelovale tudi gospodarske družbe in agencije s področja telekomunikacij ter prenosa in distribucije električne energije.

PRIPRAVE NA VAJO CC21

Sodelovanje RS na Natovi vaji CC21 z načrtom vaj. Glede na načrtovano sodelovanje je Vlada RS sprejela sklep o sodelovanju.

Vlada RS je s sklepom o sodelovanju določila vodstvo in vadbence na vaji CC21 v RS: Ministrstvo za obrambo (MO), Ministrstvo za infrastrukturo (MZI), Ministrstvo za javno upravo (MJU), Ministrstvo za pravosodje (MP), Ministrstvo za zdravje (MZ), Ministrstvo za zunanje zadeve (MZZ), Ministrstvo za notranje zadeve (MNZ), Slovensko obveščevalno varnostno

agencijo (SOVA), Urad Vlade Republike Slovenijo za informacijsko varnost (URSIV), Agencijo Republike Slovenije za komunikacijska omrežja in storitve (AKOS), Agencijo Republike Slovenije za energijo (AGEN), ELES d.o.o. in nacionalni odzivni center za omrežne incidente SI-CERT. Za vodjo vaje CC21 v RS je Vlada RS imenovala generalnega sekretarja na MO, za njegovega namestnika pa vodjo Službe za informatiko in komunikacije na istem ministrstvu. V skladu s svojimi pristojnostmi je vodstvo vaje CC21 v RS kot vadbence v vajo CC21 v RS vključilo še podjetja Elektro Ljubljana d.d. s področja preskrbe z električno energijo in komunikacijska podjetja A1 d.d., Telekom Slovenije d.d. in Telemach d.o.o.

Vodstvo vaje je sprejelo Navodilo za organizacijo in izvedbo vaje kibernetske obrambe Cyber Coalition 2021 (CC21) v RS (dokument MO, št. 870-19/2021-32 z dne 26. 11. 2021, v nadaljevanju navodilo). Z navodilom je vodstvo določilo vlogo in naloge vodstva, skupine za organizacijo in izvedbo vaje, imenovalo dva predstavnika RS v vodstvu vaje CC21 v Estoniji (SVN-EXCON), določilo naloge in imenovalo dva lokalna koordinatorja vaje CC21 v RS ter določilo vlogo in naloge vadbencev v RS. Z navodilom je vodstvo vaje med drugim opredelilo tudi način označevanja dokumentov, informacijsko in komunikacijsko podporo, ravnanje s tajnimi podatki, zbiranje prvih vtisov o vaji CC21, pripravo dnevih in zaključnih poročil ter obveščanje javnosti.

Skladno s sklepom o sodelovanju in navodilom je MO oblikovalo Skupino za organizacijo in izvedbo vaje, ki je bila odgovorna za pripravo nacionalnega scenarija, izdelavo nacionalnih dokumentov, usklajevanje priprav na vajo CC21 in zagotovitev pogojev za izvedbo. Skupina za organizacijo in izvedbo vaje je pripravila 6 lastnih sestankov, 4 sestanke vodstva, 15 medresorskih koordinacij in 3 udeležbe na načrtovalnih konferencah. Za skupno več kot 180 vadbencev iz RS, ki so prihajali iz 30 različnih organizacij, so pripravili 3 skupne priprave, zagotovili različne komunikacijske poti v RS in njihovo preverjanje, organizirali so preverjanje in seznanjanje z Natovim informacijskim vadiščem (angleško Cyber Range) ter seznanjanje in praktično usposabljanje na platformi za izmenjavo informacij o škodljivi kodi (angleško *Malware Information Sharing Platform* – MISP).

Nato je vajo CC21 pripravil v skladu z usmeritvami in zahtevami, podanimi v dokumentu *Exercise Cyber Coalition 2021 – exercise Specifications* (oznaka dokumenta ACT/CAPDEV/CAP/TT-3893/SER:NU0419 z dne 12. 4. 2021). V skladu s tem dokumentom je vajo načrtovalo in vodilo Zavezniško poveljstvo za preoblikovanje (angleško *Allied Command Transformation* - ACT) pod vodstvom Vojaškega odbora (angleško *Military Committee*).

Nato je v okviru priprav na vajo CC21 izvedel 4 načrtovalne konference. Začetna, planska in glavna konferenca CC21 so zaradi epidemioloških razmer potekale v obliki avdio video konferenc (AVK), zaključna konferenca pa ob strogih zaščitnih ukrepih v fizični obliki v Talinu v Estoniji. Na načrtovalnih konferencah so RS zastopali predstavniki MO iz Službe za informatiko in komunikacije in Direktorata za obrambne zadeve.

V okviru priprav na vajo CC21 je Nato pripravil več dokumentov, ki so bili osnova za izvedbo vaje (Storybook, Mission Description, MoU between Republic of Andwaria and Nato CNDF Contribution Nations, navodila za vadbence, tehnična navodila), razvil tehnične naloge oziroma incidente, pripravil medijske objave, kompleksno vadbeno okolje v informacijskem vadišču, seznanitev in praktično usposabljanje na platformi za izmenjavo informacij o škodljivi kodi (MISP) ter vnesel podrobne korake in proženje dogodkov vaje v orodju za vodenje vaj (JEMM).

IZVEDBA VAJE CC21

Epidemiološke razmere so narekovale izvedbo vaje CC21 z upoštevanjem ukrepov za preprečevanje širjenja okužb z virusom. Vsak izmed vadbencev se je organizacijsko in operativno prilagodil razmeram epidemije COVID-19.

Skladno z opredeljeno časovnico so na naslove vadbencev prihajala različna situacijska poročila oziroma informacije iz medijev, ki so bile skoncetrirano posredovane nekaj dni pred vajo CC21. Prihajajoče informacije so dopolnjevale zgodovinski razvoj dogodka in scenarij, ki so ga vadbenci preučili pred vajo CC21.

Vaja CC21 je tehnično nadgradila predhodne vaje CC, večina tehničnih scenarijev je bilo namreč umeščenih v informacijsko vadbišče (Cyber Range) vaje CC21. Informacijsko vadbišče vaje CC21 je omogočalo reševanje vseh razen enega tehničnega igrala. Okoliščine reševanje incidenta na informacijskem vadišču vaje CC21 so specifične in večini vadbencem neznane, zato je bilo potrebnih več koordinacij in napotkov. Vajo CC21 sta v največji meri koordinirala slovenska predstavnika v vodstvu vaje CC21 v Talinu, hkrati pa sta bila izrednega pomena lokalna trenerja v RS.

Vadbenci so za medsebojno koordinacijo, obveščanje in reakcijo uporabljali izjemno veliko število komunikacijskih poti s ciljem informiranja in reševanja incidentov. Neopredeljenost komunikacijskih kanalov oziroma platforme za reševanje kibernetskih tveganj je predstavljala procesno težavo vadbencem:

- vadbenci so za prenos stopnjevanih tajnih podatkov podatkov uporabljali: KIS MO Intranet, KIS NCKU ter depešni sistem MZZ (do vključno stopnje tajnosti INTERNO);
- SI NS NOAN omrežje (do vključno stopnje NATO SECRET).

Bistveno izhodišče skupine za organizacijo in izvedbo vaje je bilo, da je potrebno vajo CC21 umestiti v celoten spekter vplivov kibernetskih incidentov in njihovih posledic v družbi. Dosedanje vaje CC so v večini primerov od vadbencev terjale kompetence za reševanje tehničnih incidentov. V nacionalnem scenariju CC21 pa smo težišče dali predvsem na odgovornost upravljanja z incidentom in tudi upravljanja sekundarnih posledic, torej prekinitve delovanj. V tem cilju je vaja CC dobila zahtevano dimenzijo poleg tehničnega nivoja tudi taktičen, operativen in strateški vidik.

Ključne problematike ki so jih reševali vadbeni so bile:

- nedelovanje informacijskih sistemov Slovenske vojske (SV) na mednarodni operaciji in misiji (MOM);
- nepravilno delovanje brezpilotnega letala SV na MOM;
- problematika pristaniških terminalov v pristanišču na območju operacije;
- nedelovanje mobilnih telefonov za pripadnike in druge člane slovenskih delegacij na MOM na lokaciji napotitve;
- škodljiva koda v dveh sistemih elektro energentskga sektorja;
- izpad operacijskih sistemov in aplikacij na MZ in MP ter organih v strukturi.

Skladno s sklepom o sodelovanju so na vaji CC21 sodelovali vsi vadbenci. Z vidika procesa upravljanja kibernetskega incidenta in njegovih posledic je z vajo CC21 dosežen napredek s področja reševanja kibernetskih incidentov. Z vidika predkazenskega postopka so na vaji CC21 sodelovali tudi Vrhovno državno tožilstvo RS in Specializirano državno tožilstvo RS.

Težišče scenarija in posledično reševanja tehničnih incidentov je predstavljalo reševanje težav SV na MOM in elektroenergetskega sistema držav članic. Prav tako so se pravna vprašanja nanašala na reševanje težav SV na MOM.

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 CC21.

Nekateri udeleženci med izvajanjem vaje CC21 niso poznali okolja in začetnega stanja sistema na katerem se je vaja CC21 izvajala. Tekom vaje CC21 so zaznali šume v komunikaciji, saj so sporočili, da zaradi težav z dostopom do strežnikov ni bilo mogoče v celoti sodelovati.

Zadnji dan vaje CC21 je bilo pripravljeno tudi poročilo »Prve ugotovitve« (angleško *First Impression Report*), ki je bilo preko predstavnika RS v Natovem vodstvu vaje CC21, poslano organizatorju vaje CC21 v Natu.

V celoti je na CC21 v RS sodelovalo:

- MO
    - MO-CERT
    - SGS
    - OVS
    - GŠSV/PSSV
        - POVCEN
        - ESD
        - MIL-CERT
- MZI
    - ELES
    - Elektro Ljubljana
- MJU
    - GOV-CERT
    - in sodelujoči
- MNZ
    - POLICIJA
    - POL-VOC
    - UKP-CRP
- MZZ
- MZ
- MP
    - državno tožilstvo RS
    - vrhovno državno tožilstvo RS
    - specializirano državno tožilstvo RS

- SOVA
- URSIV
- AKOS
    - Telekom d.d.
    - A1 Slovenija d.d.
    - Telemach d.o.o.
- SI-CERT

- oblikovane oziroma aktivirane so bile različne medresorske delovne skupine, ki so bile formirane s strani Vlade RS ali ministrstev.

ANALIZA VAJE CC21 – Odprta vprašanja in predlogi za nadaljnje delo

Vaja CC21 in priprave nanjo so potekale v času zaostrene epidemije COVID-19, kar je otežilo priprave in izvedbo. Kljub temu udeleženci in vodstvo ocenjujejo, da je bila vaja CC21, ob upoštevanju vseh ukrepov in s prilagojenim načinom dela, predvsem z delom na daljavo, uspešno izvedena.

Na vaji CC21 so sodelovali vadbenci na različnih nivojih v strukturi kibernetskega prostora: strateški, operativni, taktični in tehnični nivo, kar je zahtevalo dodatne napore pri obvladovanju poteka celotne vaje CC21. Gospodarske družbe, ki so bile vključene v vajo CC21, so vključno s posameznimi vadbenimi skupinami organov državne uprave na vaji CC21 sodelovale kot izvajalci bistvenih storitev, taktično tehnični nivo so predstavljali varnostno operativni centri (angleško *Security Operations Center* – SOC) ter strateški nivo ministrstva in URSIV.

Prva analiza vaje CC21 je bila opravljena na skupnem AVK srečanju udeležencev in vodstva, vadbenci pa so poslali tudi končna poročila, v katerih so zbrali ugotovitve in predloge za izboljšave.

Vadbenci in vodstvo vaje CC21 v RS ocenjujejo, da je bila vaja CC21, kljub zelo oteženim pogojem dela zaradi epidemije COVID-19, dobro pripravljena in izvedena tako na nivoju Nata kot tudi v RS, ter, da so bili doseženi cilji vaje CC21 v RS:

- uspešno je bil preverjen odziv nacionalno varnostnega sistema RS na posredna in neposredna ogrožanja in varnostna tveganja v primeru kibernetske grožnje ali incidenta v kibernetskem prostoru;
- uspešno so bili vodeni postopki medresorskega usklajevanja pri pripravi predlogov za odločanje v RS in pripravi stališč za morebitno zaprosilo za pomoč Natu skladno z Memorandumom o soglasju med Republiko Slovenijo in Organizacijo Severnoatlantske pogodbe o sodelovanju pri kibernetski obrambi – NATO INTERNO (v nadaljevanju: memorandum);
- uspešno so bile sprejete odločitve za nudenje zaprošene pomoči v primeru kibernetske grožnje;
- uspešno so bile preverjene normativne podlage ter procesi in postopki usklajevanja in izvajanje postopkov zaščite in obrambe kibernetskega prostora;
- kot zadovoljivo je bilo ocenjeno odzivanje na kibernetske incidente v sektorju kritične infrastrukture s težiščem na področjih preskrbe z električno energijo ter komunikacijskih omrežij;

- uspešno je bilo preverjeno sodelovanje in funkcionalnost odzivanja na kibernetske incidente z gospodarskim sektorjem.

Vadbenci ocenjujejo, da je bila vaja CC21 nadgradnja vaj CC iz prejšnjih let ter glede na stanje epidemije COVID-19 zastavljena zelo ambiciozno.

Ključne ugotovitve, ki so jih vadbenci podali v analizi vaje CC21 in v zaključnih poročilih:

1. podrobneje je treba opredeliti postopek poročanja in vadbence opozoriti na težišče poročanja, kar je pomembno za kakovostno, usklajeno in pravočasno obravnavo kibernetskih incidentov ter zmanjševanja njihovih negativnih učinkov;
2. nekateri vadbenci opozarjajo na preveliko število komunikacijskih poti, ki zahtevajo redno in aktivno spremljanje, kar je veliko breme za vadbence pri reševanju incidentov;
3. nekateri udeleženci vaje CC21 iz RS niso bili dovolj dobro seznanjeni z informacijskim vadiščem, na katerem je potekala večina tehničnih problemov vaje CC21, in to kljub dokaj dolgemu testnemu obdobju pred vajo CC21, v katerem so se vadbenci lahko seznanjali in preizkušali informacijsko vadišče vaje CC21. Deloma je to posledica tudi dokaj pozne priprave tehnične dokumentacije informacijskega vadišča in njeno spreminjanje pred vajo CC21;
4. v okviru vaje CC21 so se izmenjali seznami kontaktnih oseb ključnih državnih inštitucij, odzivnih centrov na kibernetske incidente ter gospodarskih družb, ki bodo koristni tudi pri rednem delu;
5. na področju poročanja je ugotovljeno, da obstaja pomembna razlika v vsebini poročila (obrazca), ki ga v primeru zaznanega incidenta poročajo operaterji na AKOS in poročila, ki ga AKOS v skladu z Nacionalnim načrtom kriznega odzivanja (NOKI) pošlje na URSIV. Zaradi razlik se lahko določene vsebine tudi izgubijo oziroma se incidenti drugače klasificirajo;
6. zelo koristne so bile namizne vaje (angleško *table top exercise* – TTX) v času kolektivnih priprav vadbencev, v okviru katerih so vadbenci preigravali odzivanje na kompleksne incidente, ki so bili podobni incidentom, s katerimi so se potem srečali na vaji CC21. Vadbenci predlagajo, da se temu na naslednji vaji CC nameni še več pozornosti;
7. nekateri vadbenci so v vaji CC21 prvič priglasili incidente nacionalnemu odzivnemu centru za kibernetsko varnost SI-CERT, hkrati je bilo s strani posameznih vadbencem evidentno skopo poročanje o incidentih na URSIV;
8. AKOS je URSIV redno posredovala poročila o kibernetskih incidentih pri operaterjih. Ti incidenti s strani operaterjev niso bili ocenjeni z visoko stopnjo oceno po NOKI;
9. izvajalci bistvenih storitev (v nadaljevanju: IBS) so pri poročanju uporabljali NOKI obrazce. Kljub temu, da so bili obrazci, še posebej kar se tiče informacij glede situacijske slike, pomanjkljivo izpolnjeni, je bil dosežen namen seznanjanja z obrazci in obveščanjem po NOKI;
10. URSIV je v teku vaje CC21 pridobila situacijsko sliko vpliva kibernetskih incidentov pri IBS preko nosilca kritične infrastrukture za obravnavano področje, ki pa v danem trenutku ni bila tako kritična, kot je bilo zaznati v nekaterih vadbenih medijskih objavah. Posledično, glede na pomanjkanje informacij in nasprotujoče informacije,

URSIV ni uspelo sestaviti celovite, realne situacije kibernetske varnosti na nacionalnem nivoju;

11. vadbenci so pohvalili vlogo in delo lokalnih trenerjev, ki sta bila v stalnem stiku z vadbenci ter sta s pravo mero in na pravi na način spremljala in usmerjala potek vaje CC21. V prihodnje bi veljalo razmisliti o delitvi vlog lokalnih trenerjev in sicer na lokalnega trenerja za Nato del vaje CC ter na lokalnega trenerja določenega s strani URSIV, ki bi primarno spremljal in usmerjal nacionalni del vaje CC;
12. na URSIV so izvajali procese v skladu z Zakonom o informacijski varnosti (Uradni list RS, št. 30/18 in 95/21) in NOKI ter pri tem sledili ciljem vaje CC21 in preverjali ustreznost in pomanjkljivosti v nacionalnem sistemu kibernetske varnosti.

Predlogi za izboljšanje ugotovljenih pomanjkljivosti:

1. preveri naj se možnost zmanjšanja število komunikacijskih poti in preveri možnost vzpostavitve sistema digitalne varne in strukturirane izmenjave informacij na nacionalni ravni. v RS naj se vzpostavi nacionalni MISP, ki naj se smiselno poveže z MISP Nato in z MISP mednarodno mrežo CERT;
2. priporoča se premislek o posodobitvi NOKI s ciljem, da bo vključeval tudi specifike, ki so značilne za dejavnost operaterjev elektronskih komunikacij in z njihovo dejavnostjo povezanimi incidenti. NOKI praviloma obravnava kibernetske varnostne incidente, Zakon o elektronskih komunikacihah (Uradni list RS, št. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – odl. US, 81/15, 40/17 in 189/21 – ZDU-1M) pa vse tipe varnostnih incidentov (npr. tudi okvare, naravne nesreče);
3. na ravni telekomunikacijskih operaterjev bi bilo smiselno vzpostaviti koordinacijsko skupino za sodelovanje, s ciljem delitve informacij glede odpravljanja težav pri nedelovanju in razlogov za prekinitev delovanja;
4. pri organizaciji vaje CC22 naj se več pozornost nameniti testiranju in spoznavanju z okoljem informacijskega vadišča vaje CC;
5. v prihodnje naj se v pripravah na vajo CC izvede več različnih priprav za vadbence glede na nivo, ki ga predstavljajo v nacionalnem sistemu kibernetske varnosti (strateški, operativni, tehnični);
6. ključno je nadaljevati diskusijo in najti rešitve v odnosih med deležniki, ki jih zavezujeta Zakon o informacijski varnosti in Zakon o kritični infrastrukturi (Uradni list RS, št. 75/17 in 189/21 – ZDU-1M). Rešitve so predvsem potrebne pri koordinacijskih aktivnostih in usklajevanju omenjenih zakonov, ki predpisujeta podobne obveznosti istim zavezancem, vendar v odnosu do drugih državnih organov;
7. pregleda naj se memorandum in se po potrebi revidira oziroma dopolni kontaktne točke v RS.

ZAKLJUČEK

Vaja CC 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).

Letošnja vaja CC21 je pomenila določen preskok predvsem na nacionalnem nivoju, saj je bil v vajo vključen širši spekter deležnikov s področja kritične infrastrukture, gospodarskih družb, izvajalcev bistvenih storitev in tudi državnih organov, ki so na vaji CC sodelovali prvič. Skozi izvedbo tovrstnih vaj CC se tako krepi zavedanje o pomenu kibernetike in ustreznega odzivanja na kibernetske grožnje. Skozi izvedbo vaj CC se različni deležniki med seboj spoznajo in v realnih situacijah mnogo lažje in bolj učinkovito pristopajo k reševanju realnih oziroma vsakodnevnih težav s področja kibernetike.

Vaja CC21 je dosegla namen in cilje opredeljene v sklepu o sodelovanju. Vadbenci so v procesnem delu sledili aktivnostim in sodelovali pri izvedbi preverjanja odziva nacionalno varnostnega sistema RS na posredna ali neposredna ogrožanja in varnostna tveganja v primeru groženj in incidentov v kibernetskem prostoru.

Izvajalo se je kontinuirano medresorsko usklajevanje pri pripravi predlogov za odločanje v RS in pripravi stališč za Nato skladno z memorandumom ter preučevalo in odzivalo na kibernetske incidente v sektorju kritične infrastrukture s težiščem na področju preskrbe z električno energijo in informacijsko-komunikacijskih omrežij in sistemov, ki so imeli posreden ali neposreden vpliv na delovanje vadbencev.

V prihodnje je ključno:

- zavzeti stališče do MISP in ga implementirati skladno s cilji na nacionalnem nivoju;
- smiselna je digitalizacija NOKI, ki bo hkrati odpravila vsebinske pomanjkljivosti, ki jih zaznava področje telekomunikacijskih operaterjev;
- nujno je preučevanje sekundarnih posledic kibernetskega napada, kjer pride do prekinitev delovanj, posledice pa imajo učinke izven primarnega resorja ali organizacije. Smiselno je opredeliti upravljanje nastale situacije in odgovornosti v obdobju do stanja kompleksne krize in v nadaljevanju v kompleksni krizi. Vaja CC21 je pokazala, da je potreben premislek o odzivanju RS v primerih kibernetskega napada z izhodiščem problematike Nata, kjer zavezniške sile izvajajo vojaške aktivnosti na območju ali izven območja zavezništva;
- v prihodnjih vajah kibernetske obrambe povečati poudarek pripravam posameznih skupin vadbencem, torej ločeno izvesti priprave za tehnični in taktični nivo ter ločeno za operativno strateški nivo;
- v prihodnjih vajah CC se s ciljem usmerjanja vadbencev na nacionalnem delu vaje CC doda lokalni trener s strani URSIV.

S sodelovanjem RS na vaji CC21 so bile pridobljene dodatne izkušnje in spoznanja, ki bodo nedvomno pripomogla k nadgradnji sistema odzivanja na kibernetske incidente v realnem okolju. Na priprave na vajo CC21 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