REPUBLIKA SLOVENIJA
DRŽAVNI ZBOR
Poslanska skupina Slovenske demokratske stranke

Šubičeva ulica 4, 1000 Ljubljana
t: 01 478 95 30, f: 01 478 98 77, e: ps-sds@dz-rs.si, www.dz-rs.si

Ljubljana, 16. januar 2019

DRŽAVNI ZBOR REPUBLIKE SLOVENIJE
Odbor za obrambo

g. Samo Bevk, predsednik

ZADEVA: **ZAHTEVA ZA SKLIC NUJNE SEJE ODBORA ZA OBRAMBO**

Poslanska skupina Slovenske demokratske stranke zahteva, da se na podlagi drugega odstavka 48. člena, v povezavi z 32. členom Poslovnika DZ, skliče nujna seja Odbora za obrambo z obravnavo naslednje točke:

»STANJE NA PODROČJU KIBERNETSKE ZAŠČITE REPUBLIKE SLOVENIJE«

I. Obrazložitev:

V sodobnem svetu se uporaba informacijskih sistemov in omrežij vseskozi povečuje, zato se povečuje tudi pomen, ki ga imajo ti sistemi za uspešen razvoj gospodarskih in negospodarskih dejavnosti ter življenje in blaginjo celotne družbe. Vedno hitrejši razvoj informacijsko-komunikacijskih tehnologij po eni strani prinaša koristi za moderno družbo, po drugi strani pa vpliva na pojav vedno novih in tehnološko vse bolj dovršenih kibenetskih groženj. Po prvotnem razmahu spletnega kriminala posameznikov pred desetletji, so ključno vlogo na spletu začele prevzemati države s svojimi strukturami z namenom zaščite državljanov ter državne suverenosti. V zadnjih dveh desetletjih se opaža eksponenten razmah uporabe kibenetskih sredstev za doseganje ciljev na meddržavnem strateškem nivoju, ki je v preteklosti škodoval in še danes škoduje tako državljanom, kot gospodarskim družbam in državnim (pod)sistemom. Varnost omrežij in informacij tako prispeva h krepitvi pomembnih vrednot in ciljev v družbi, kot so človekove pravice in temeljne svoboščine, demokracija, pravna država, ter gospodarska in politična stabilnost.

Vsakodnevno se v tujih in domačih medijih pojavljajo novice incidentov s področja kibernetske varnosti, ki kažejo na to, da danes pred grožnjami in napadi ni varen več nihče. Kraje bančnih in drugih osebnih podatkov so ena izmed vidnejših manifestacij razmaha kibenetskih napadov na individualni ravni. Paralizacija Gruzije leta 2008, kolaps estonskega bančnega sistema leta 2008, onesposobljenje ukrajinske električne infrastrukture leta 2015 in 2017, vdiranje v volilne skrinjice posameznih zveznih držav ZDA leta 2016, WannaCry Virus leta 2017 in »man in the middle« napad na vitalen interes RS v arbitražnem postopku med RS in Republiko Hrvaško pa kažejo na dejstvo, da je postala uporaba kibemetskih sredstev s strani suverenih držav in njenih

parastruktur sredstvo za doseganje strateških ciljev. Nepripravljenost posameznikov, gospodarskih družb in držav na prej omenjene incidente opozarja, da življenje v balončku brezskrbnosti ni več mogoče in da je le vprašanje časa kdaj bodo napadi v informacijsko—kibemetskem prostoru imeli konkretnejše vplive tudi na našo družbo.

Eden izmed zaključkov srečanja tri tisoč ključnih svetovnih posameznikov s področja politike, gospodarstva, znanosti in drugih področij v Davosu je bila ocena največjih groženj, ki nas čakajo v naslednjih desetih letih. Največje grožnje človeštvu naj bi izhajale s področja ekstremnih vremenskih razmer ter naravnih katastrof. Na tretje mesto, pred pomanjkanje vode in hrane, migracije, teroristične napade in širjenje nalezljivih bolezni, so svetovni voditelji postavili grožnjo večjih kibenetskih napadov zaradi vse večjega zanašanja posameznikov, gospodarskih družb in držav na digitalne sisteme. Da se v letošnjem letu pričakuje večja možnost groženj in napadov v informacijsko-kibernetskem prostoru sta ocenili skoraj dve tretjim voditeljev. S to oceno se strinjajo tudi vodilne univerze, institucije in strokovnjaki s področja informacijske varnosti.

V Davosu so prav tako naznanili ustanovitev nove koordinacijske skupine na globalni ravni s sedežem v Ženevi, ki bo z relevantnimi institucijami in podjetji delila informacije o grožnjah v kibernetskem prostoru, z namenom izboljšanja digitalne varnosti, kar kaže na zavedanje voditeljev po potrebi za vzpostavitev struktur, ki bi se spopadle z naraščajočim številom in obsegom kibemetskih groženj.

Slovenija ni znotraj predvidevanj voditeljev nobena izjema, saj se tudi v našem kibernetskem prostoru že dlje časa spopadamo z grožnjami in napadi različnih obsegov. Večji kibernetski incidenti so se pri nas lani pokazali z vplivom WannaCry izsiljevalskega virusa na večdnevno ustavitev proizvodnje Revoza ter krajo kriptokovancev podjetja NiceHash v vrednosti preko 60 milijonov evrov. Oba incidenta in mnogi drugi (o katerih se v javnosti ni poročalo), so povzročili večjo materialno škodo posameznikom in gospodarskim družbam, ter načela javno podobo Republike Slovenije kot varnega pristana v času globalnih kibemetskih groženj. Temu je sledilo tudi večje zanimanje medijev za to področje, kar je o tej problematiki ozavestilo tudi državljane. Razvoj groženj v zadnjih letih kaže na to, da bo Slovenija brez močne, obsežne in izkušene strukture, ki bi v državi velikosti Republike Slovenije združila sile države, gospodarskih družb, inštitutov ter univerz, ostala zgolj nema opazovalka groženj in napadov na svoje državljane, gospodarske družbe in državne strukture.

Analiza obstoječega stanja:

Trenutno v Republiki Sloveniji (še) nimamo vzpostavljenega celovitega in učinkovitega sistema informacijske varnosti in kibernetske obrambe, čeprav v zahodnem svetu to postaja nacionalnovamostna prioriteta najvišje stopnje. V Sloveniji je bilo v preteklosti že pripravljenih nekaj predlogov sistemske ureditve področja kibernetske varnosti, vendar do izvedbe nikoli ni prišlo. Kljub temu je prevladalo spoznanje, da država potrebuje strategijo kibernetske varnosti, ki bo združila in usmerila prizadevanja vseh deležnikov za okrepitev in sistemsko ureditev tega pomembnega področja. Na podlagi zavedanja o pomenu informacijske varnosti in kibernetske obrambe ter mednarodnih zavez danih zvezi NATO in EU je Vlada Republike Slovenije na seji dne 25. 2. 2016 sprejela tako imenovano Strategijo kibernetske varnosti Republike Slovenije, ki govori o krepitvi sistema zagotavljanja kibernetske vamosti in sistemski ureditvi tega področja.

V okviru Natovega procesa obrambnega načrtovanja je Republika Slovenija sprejela cilj zmogljivosti E5308, ki se nanaša na informacijsko varnost in kibernetske obrambo. Prav tako je določen tudi cilj zmogljivosti E6202, ki se nanaša neposredno na kibernetsko obrambo in na Natovo politiko kibernetske obrambe iz leta 2014. Slednja je bila podkrepljena na vrhu zveze

NATO leta 2016 v Varšavi, kjer so se predsedniki držav in vlad zavezali h krepitvi kibernetske obrambe nacionalne infrastrukture in omrežij.

EU je sprejela več direktiv, ki se posredno ali neposredno nanašajo na informacijsko varnost in kibernetsko obrambo. Ena zadnjih neposrednih dimktiv je Direktiva EU 2016/1148 Evropskega Parlamenta in Sveta z dne 6. julija 2016, ki v 24. členu določa, da mora biti tudi v Republiki Sloveniji najkasneje do maja 2018 vzpostavljen delujoč sistem infomacijske varnosti in kibernetske obrambe, vendar nam ga doslej še ni uspelo vzpostaviti.

Nosilci operativnih zmogljivosti:
Trenutno so operativne zmogljivosti za odzivanje na kibernetske grožnje porazdeljene v SI-CERT kot nacionalen odzivnem centru za omrežne incidente, v Sektorju za informacijsko varnost v okviru Direktorata za informatiko na Ministrstvu za javno npravo, na Ministrstvu za obrambo za sisteme na področju obrambe in varstva pred naravnimi in drugimi nesrečami, v SOVA na področju protiobveščevalnega delovanja ter na Policiji, v Uradu za informatiko in telekomunikacije in Upravi kriminalistične policije, predvsem v Centru za računalniško preiskovanje z zmogljivostmi za zatiranje kibernetskega kriminala. Razen Policije, ki je v zadnjih petih letih izboljšala svoje kapacitete za preiskovanje in preprečevanje kibernetske kriminalitete, so drugi organi podhranjeni na kadrovskem, materialno-tehničnem in organizacijskem področju. Kljub pomanjkljivostim, zmogljivosti na operativni ravni obstajajo, ne obstaja pa koordinacijsko telo, ki bi na strateški ravni povezovalo navedene deležnike.

Sodelovanje med deležniki:
Po podatkih SI-CERT je bilo leta 2014 v Sloveniji obravnavanih 2060 incidentov, kar je skoraj 6,4-kratno povečanje glede na leto 2008. Naraščajoči trend glede na zgoraj omenjeno podhranjenost sistema zagotavljanja kibernetske varnosti vzbuja skrb. Sodelovanje deležnikov pri zagotavljanju kibernetske varnosti ni fornalizirano, ampak predvsem med odzivnimi centri poteka neformalno, razen kadar za to obstaja pravna podlaga. Pri tem gre za obveščanje o incidentih in pomoč pri njihovem reševanju, izmenjavo izkušenj ali pa uporabo obstoječih zmogljivosti. Priložnost za vzpostavitev sodelovanja so med drugim skupna sodelovanja pri izvedbi mednarodnih vaj iz kibernetske varnosti, ki jih organizira Agencija EU za varnost omrežij in informacij (ENISA). Tako je bilo v preteklosti sodelovanje že vzpostavljeno z nekaterimi bankami, telekomunikacij skimi ponudniki in distributerji električne energije.

Ozaveščanje:
Na področju ozaveščanja potekata dva projekta. SI-CERT od leta 2011 izvaja nacionalni program ozaveščanja in izobraževanja Varni na internetu. Projekt, ki je namenjen najširši slovenski javnosti, poseben sklop vsebin pa tudi malim podjetjem, obrtnikom in samostojnim podjetnikom, si za ključen cilj zastavlja dvig stopnje informiranosti o varni rabi interneta. Projekt, ki ga financira Ministrstvo za izobraževanje, znanost in šport, sodeluje tudi v kampanjah evropskega meseca kibernetske varnosti.

V okviru Centra za varnejši internet, ki ga vodi konzorcij, sestavljen iz Fakultete za družbene vede Univerze v Ljubljani, Arnes, Zveze prijateljev mladine Slovenije in Zavoda MISSS, financirata pa ga Generalni direktorat Connect pri Evropski komisiji in Ministrstvo za izobraževanje, znanost in šport, se izvajajo programi SAFE.SI, TOM telefon in Spletno oko. Program SAFE.SI deluje kot nacionalna točka ozaveščanja otrok in najstnikov o varni rabi interneta in mobilnih naprav. Program TOM telefon otrokom in mladostnikom med drugim svetuje tudi o varni rabi interneta in mobilnih naprav. Spletno oko pa je spletna prijavna točka, ki v partnerstvu s policijo, tožilstvom, Uradom varuha za človekove pravice, ponudniki internetnih storitev, javnimi in drugimi zainteresiranimi vladnimi in nevladnimi organizacijami omogoča anonimno prijavno domnevno nezakonitega gradiva s spolnimi zlorabami otrok in sovražnega govora na spletu ter ozavešča o

problematiki nezakonitih spletnih vsebin.

Izobraževanje:
Na izobraževalnem področju je informacijska oziroma kibemetska varnost vključena v visokošolski študijski program »informacijska vamost« na Fakulteti za varstvene vede Univerze v Mariboru, kot predmet je vključena v predmetnike študijskih programov na Fakulteti za računalništvo in informatiko ter Fakulteti za družbene vede Univerze v Ljubljani, Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru, Fakulteti za vede o zdravju Univerze na Primorskem, Fakulteti za informacijske študije v Novem mestu in samostojnem visokošolskem zavodu GEA College, kot del predmeta korporativna varnost tudi na nekaterih drugih visokošolskih izobraževalnih ustanovah. Na osnovnošolski in srednješolski ravni predmet s tega področja ne obstaja.

Udeležba na vajah:
Skladno z možnostmi Slovenija sodeluje na mednarodnih vajah iz kibernetske varnosti. Na vajah Cyber Europe, ki jih organizira ENISA, je tako 2010 sodelovala kot opazovalka, v letih 2012 in 2014 pa tudi kot aktivna udeleženka. Prav tako od leta 2013 naprej aktivno sodeluje na vajah kibernetske obrambe Cyber Coalition v okviru zveze NATO. Sodelovanje na vajah se je izkazalo kot dobra priložnost za preverjanje zmogljivosti in vzpostavitev novih povezav med deležniki. Do sedaj še ni bila izvedena nacionalna vaja iz kibernetske varnosti.

II. Odboru za obrambo predlagamo, da po končani razpravi sprejme naslednja sklepa:

1. Odbor za obrambo se je seznanil s stanjem na področju kibernetske zaščite Republike Slovenije.

2. Odbor za obrambo predlaga Vladi Republike Slovenije, da v roku treh mesecev pripravi poročilo o stanju na področju kibernetske zaščite Republike Slovenije in o ukrepih, ki jih namerava v namen njene krepitve sprejeti.

III. Poslanska skupina SDS predlaga, da na nujno sejo Odbora za obrambo povabite:
- Karl Viktor Erjavec, minister za obrambo
- Boštjan Poklukar, minister za notranje zadeve
- generalmajorka Alenka Ermenc, načelnica GŠ SV
- Dobran Božič, bivši direktor Urada Vlade RS za varovanje tajnih podatkov
- Bojan Križ, bivši generalni direktor Direktorata za informacijsko družbo
- Erik Kopač, svetovalec za nacionalno varnost bivšega predsednika Vlade RS
- Rajko Kozmelj, direktor Sove
- Zoran Klemenčič, bivši direktor Sove
- Dejan Matijevič, generalni direktor OVS

Danijel Krivec
Vodja poslanske skupine SDS