Podpisnik: Marko Lotrič
Izdajatelj: Republika Slovenija
Št. cert.: d5 01 7a 17 00 00 00 00 56 7e 0e ba
Potek veljavnosti: 21.12.2027
Ref.št. dokumenta: 060-01-1/2024/36
Čas podpisa: 16:07, 24.01.2024

REPUBLIKA SLOVENIJA
DRŽAVNI SVET

Številka: 065-02-25/2023/7
Ljubljana, 24. 1. 2024

Državni svet Republike Slovenije je na 13. seji 24. 1. 2024, na podlagi 29. in 67. člena Poslovnika Državnega sveta (Uradni list RS, št. 70/08, 73/09, 101/10, 6/14, 26/15, 55/20, 123/20, 67/22 in 69/23), sprejel naslednji

S K L E P

Državni svet se je seznanil z Zaključki posveta *Odpornost in neprekinjenost delovanja ključnih organizacij imperativ moderne družbe* in na podlagi prvega in drugega odstavka 97. člena Poslovnika Državnega sveta poziva Vlado Republike Slovenije in Ministrstvo za obrambo, Ministrstvo za infrastrukturo, Ministrstvo za digitalno preobrazbo, Ministrstvo za gospodarstvo, turizem in šport, Ministrstvo za notranje zadeve, Ministrstvo za visoko šolstvo, znanost in inovacije in Ministrstvo za vzgojo in izobraževanje, da zaključke posveta proučijo in se do njih opredelijo v roku 30 dni.

* * *

Zaključki posveta se glasijo:

»Komisija Državnega sveta Republike Slovenije za državno ureditev je 27. 11. 2023 z Inštitutom za korporativne varnostne študije (ICS) in Slovenskim združenjem za korporativno varnost so-organizirala posvet *Odpornost in neprekinjenost delovanja ključnih organizacij imperativ moderne družbe*.

Pogovor o izzivih, ki jih prinaša zahtevno varnostno okolje z vključenimi varnostnimi grožnjami, je bil glavni namen posveta s področja zagotavljanja neprekinjenosti delovanja ključnih organizacij. Poplave poleti 2023 so pokazale, da bodo uspešno preživela samo tista organizacijska okolja, ki zagotavljajo ustrezen sistemski pristop pri zagotavljanju načrtovanja neprekinjenega delovanja. Takšne organizacije so bolj robustne in prožne na odzivanje v primeru celega niza kriz, ki si v zadnjem obdobju sledijo vedno pogosteje. Če v tem okviru izpostavimo organizacije, ki upravljajo s kritično infrastrukturo in bistvenimi storitvami, ki so ključne za delovanje širše družbene skupnosti, potem je pomen sistema neprekinjenega delovanja še pomembnejši. Posvet je opozoril na postopke prenosa dveh pomembnih evropskih direktiv s področja kritične infrastrukture in informacijske varnosti v slovenski pravni red (NIS-2 direktiva in CER direktiva). Obe direktivi se ukvarjata z zagotavljanjem ustrezne neprekinjenosti delovanja ključnih subjektov in storitev, njihove robustnosti

ter enotnih stresnih testov za preverjanje njihove sposobnosti delovanja ob kriznih razmerah. Posvet je bil namenjen razpravi in iskanju zaključkov, ki bodo strateškim institucijam v državi pomagale pri iskanju učinkovitih poti za integracijo omenjene zakonodaje v naš pravni red. V okviru posveta so bili predstavljeni tudi 3 ključni EU projekti s tega področja, ki predstavljajo primere dobre praske pri vpeljevanju in izgrajevanju ustreznega sistema neprekinjenega delovanja njihovih organizacij.

Udeležba vabljenih gostov, število udeležencev in poglobljenost razprav je pokazala aktualnost izbrane tematike posveta.

Udeležence posveta je uvodoma nagovoril predsednik Državnega sveta Republike Slovenije Marko Lotrič.

Posvet je potekal v 2 sklopih. V prvem delu je potekala moderirana okrogla miza o aktualnosti problematike, ki jo je povezoval izr. prof. dr. Denis Čaleta in na kateri so sodelovali: Boštjan Šefic, svetovalec v Kabinetu predsednika vlade/koordinator za odpravljanje posledic poplav; dr. Uroš Svete, direktor Urada za informacijsko varnost; mag. Boštjan Pavlin, generalni direktor direktorata za obrambne zadeve MORS; mag. Marko Mišmaš, direktor Agencije za komunikacijska omrežja in storitve Republike Slovenije (AKOS); mag. Aleksander Mervar, direktor ELES, d. o. o., in Aleš Skok, predsednik uprave Cinkarne Celje, d. d.

V drugem delu so predstavniki Inštituta za korporativne varnostne študije (ICS) predstavili rezultate 3 evropskih projektov s področja kritične infrastrukture. Dr. Jolanda Modic je v okviru prispevka z naslovom *Izboljšana odpornost kritične infrastrukture proti obsežnim nadnacionalnim in sistemskim tveganjem* predstavila projekt ATLANTIS. Aljoša Kandžič je v okviru prispevka z naslovom *Pripravljenost in uveljavljanje odpornosti na kaskadne kibernetsko-fizikalne grožnje in učinke za kritično infrastrukturo s poudarkom na okrožni ali regionalni zaščiti* predstavil projekt PRECINCT, in dr. Milan Tarman je v okviru prispevka *Strategije in tehnologije za združene in odporne kritične infrastrukture in vitalne storitve v Evropi, ki jo je prizadela pandemija,* predstavil projekt SUNRISE.

Posvet sta povezovala izr. prof. dr. Denis Čaleta, ICS, in Rajko Fajt, državni svetnik, predsednik Komisije Državnega sveta za državno ureditev.

V razpravi ob koncu posveta je z vprašanji sodeloval mag. Miroslav Gregorič, poslanec Državnega zbora.

* * *

Na podlagi predstavitev in razprave so bili oblikovani naslednji

z a k l j u č k i:

1. Proces odpravljanja posledic uničujočih poplav mora zagotavljati sistemske pristope, ki ne bodo zagotovili samo ustreznega saniranja posledic, temveč se bo uveljavil celovit metodološki model, ki bo zagotavljal, da se bo v prihodnje pri

gradnji infrastrukture upošteval nivo odpornosti na vedno bolj ekstremne vplive okolja.

2. Pred nami sta zaključni fazi implementacije dveh pomembnih evropskih direktiv - NIS-2 in CER, ki sta po vsebini usmerjeni v dvigovanje odpornosti in zagotavljanje neprekinjenega delovanja kritičnih subjektov ter s tem posledično tudi tistih procesov, ki pomembno vplivajo na odpornost družbe kot celote, zato je treba pospešiti sodelovanje med različnimi deležniki, ki lahko pripomorejo k večji učinkovitosti pripravljenih zakonskih predlogov. Posebej se je treba izogibati parcialnim pristopom silosnega delovanja[1], saj je treba procese implementacije razumeti kot enovit proces.

3. Proces implementacije direktiv je treba zgraditi tako, da bodo pristojnosti in odgovornosti v zakonodaji jasno začrtane. To pomeni tudi odločitev, v katerem delu bo država, zaradi nalaganja dodatnih zakonskih zahtev, ki bodo imele močan vpliv na dvigovanje odpornosti ključnih organizacij in družbe kot celote, pomagala tudi s finančnim vložkom.

4. Treba bo jasneje določiti, kateri koordinacijski center se bo v prihodnje gradil v smeri, da prevzame vse glavne koordinacijske funkcije v primeru večjih kriznih dogodkov. V tem trenutku stanje še vedno ni jasno oz. realnost odstopa od normativno predpisanih pričakovanj.

5. Izpostavljen je bil predlog, da se na področju zagotavljanja informacijske varnosti končno pristopi k oblikovanju sektorskih odzivnih centrov CSIRT[2], kot jih predvideva Zakon o informacijski varnosti. Od države se pričakuje, da bo aktivneje posredovala pri implementaciji te pomembne naloge. Energetski sektor je zaradi svoje evolucije razvoja na omenjenem področju prvi, ki bi bil lahko del tega projekta. To bo imelo pomembno vlogo pri dvigovanju koordinacijskih in komunikacijskih aktivnostih, ki so na področju zagotavljanja informacijske varnosti ključnega pomena, če želimo dvigniti odpornost celotnega elektroenergetskega sektorja na višji nivo. Ob dejstvu, da je omenjeni sektor v osnovi centralni sektor, od delovanja katerega so odvisni tudi vsi ostali sektorji kritične infrastrukture, je to izredno pomemben korak, ki ga je treba izvesti v čim krajšem času.

6. Na področju uvajanja novih pristopov, ki jih predvideva direktiva NIS-2, se ocenjuje, da se bo število zavezancev iz sedanjih 50 dvignilo na ocenjeno raven 1000 zavezancev. To pa za seboj potegne izredno zahtevne korake poenotenja ustreznih izhodišč za zagotavljanje višje stopnje njihove odpornosti. Tukaj je treba zagotoviti sodelovanje vseh državnih institucij, da ne bo celotno breme ostalo samo na Uradu Vlade Republike Slovenije za informacijsko varnost (URSIV).

[1] Delovanje brez nujnega sodelovanja med posameznimi procesi.
[2] Načrtovano je, da bi šlo za odzivne centre za kibernetsko varnost po posameznih sektorjih.

7. Zaradi različnih nacionalno pogojenih dejavnikov bo pri zagotavljanju neprekinjenega delovanja izvajalcev bistvenih storitev zelo težko zagotavljati pristop »ZERO trust«[3]. Zato bo treba vse sile usmeriti v zagotavljanje najboljšega približka omenjenim principom.

8. Posebej je bil izpostavljen problem pomanjkanja ustreznih kadrov na specifičnih strokovnih področjih. Na področju oblikovanja izobraževalnih programov, ki so financirani s strani javnih sredstev, bo treba hitro narediti ustrezno spremembo in programe prilagoditi trenutnim in bodočim potrebam zagotavljanja kibernetske varnosti v vseh sektorjih. Za pospešitev določenih korakov bodo soorganizatorji tega posveta v Državnem svetu organizirali nov posvet, ki bo namenjen iskanju dodatnih rešitev na področju izobraževanja kadra za zagotavljanje kibernetske varnosti in ostalih specialnih znanj.

9. Kadrovski izzivi so bili izpostavljeni tudi na področju določanja sektorskih koordinatorjev zaščite kritične infrastrukture. Omenjeni koordinatorji imajo izredno pomembno vlogo pri zagotavljanju ukrepov v posameznih sektorjih. Zaradi navedenega morajo biti na ta delovna mesta izbrani strokovni kadri, ki pa imajo tudi polno podporo na strateški ravni v resornih ministrstvih.

10. AKOS je pripravil predlog *Načrta za zagotavljanje delovanja mobilnih javnih komunikacijskih omrežij v primeru stanj ogroženosti* (v nadaljevanju: Načrt). Zavezanci bi bili skladno z Načrtom operaterji mobilnih javnih komunikacijskih omrežij, ki bi za izvajanje storitev dostopali do fizične infrastrukture oddajnih lokacij RTV Slovenije, določenih v Načrtu. Zato bi lahko v primeru popolnega ali delnega izpada vseh storitev na posameznih področjih, kot je bilo to v primeru poplav 2023, pomembno vlogo za zagotavljanje nujnih komunikacij (tako za državo kot za posameznika), lahko prevzele ravno navedene lokacije. Iz teh lokacij bi operaterji zagotovili vsaj delovanje govornih storitev, komunikacije v sili (112), javno obveščanje in alarmiranje (PWS), ki bi poleg obveščanja z FM in DAB radijskimi frekvencami RTV Slovenije pripomoglo k obveščenosti prebivalstva na prizadetih območjih. Na govornem delu bi se zagotovilo tudi delovanje omrežnih priključnih točk s prednostjo. Na približno tretjini lokacij so prisotni tudi oddajniki TETRE in druge komunikacijske naprave, ki jih za svoje potrebe uporabljata Ministrstvo za obrambo in Ministrstvo za notranje zadeve. Po oceni AKOS bi bilo Načrt mogoče uresničiti na 162 lokacijah, za kar bi bila nujna investicija v ustrezno zmogljive elektro generatorje, ki bodo v primeru izpada električnega napajanja zagotovili neprekinjeno delovanje opreme, ki je na lokacijah že nameščena. Če se ozremo v prihodnost, bi bilo mogoče s teh lokacij zagotavljati tudi delovanje PPDR (sistem javne varnosti, zaščite in reševanja), ko bo vzpostavljen sistem na ravni države.

[3] »Zero Trust« pomeni veliko več kot omogočanje zaupanja vrednih identitet uporabnikov, aplikacij, naprav, strojev in obremenitev. Gre za celovito strategijo varnosti podatkov, ki vključuje šifriranje podatkov v mirovanju in med prenosom, zajema pa tako javna kot zasebna oblak okolja.

11. Operaterjem, ki pokrivajo kritično infrastrukturo, je treba zagotoviti ustrezen komunikacijski sistem, ki bo zagotovil boljšo koordinacijo in komunikacijo v vseh fazah odzivanja na krizne razmere. Podan je bil predlog, da bi lahko država z razširitvijo uporabe komunikacijskega sistema ZARE (sistem radijskih zvez zaščite in reševanja) učinkovito rešila ta problem. Operaterji, ki pokrivajo kritično infrastrukturo, so pripravljeni tudi finančno sodelovati pri razširitvi tega sistema za njegovo uporabo.

12. Glede na kadrovski primanjkljaj na področju kibernetske varnosti je bil podan tudi predlog, da bi javna podjetja na področju kritične infrastrukture za nekatera delovna mesta lahko zaposlila in ustrezno plačala tudi osebe, ki formalno nimajo ustrezne izobrazbe, vendar pa imajo znanja, ki jih ta podjetja nujno potrebujejo. Z obstoječim načinom sistemizacije delovnih mest v javni upravi in državnih podjetjih teh kadrov ni mogoče pridobiti ali zadržati (nekatere države to že rešujejo na tak način). S tem bi se lahko deloma za posamezne kritične procese zagotovil dodaten strokovni kadrovski potencial.

13. Na področju nakupov za potrebe kritične infrastrukture, ki so nujni za zagotavljanje odpornosti in posledično neprekinjeno delovanje celotne družbene skupnosti, bo v postopkih javnega naročanja treba poiskati nove in ustrezne pristope, ki bodo pospešili postopke in jih naredili dovolj varne, da v fazi razpisnih postopkov ne pride do odkrivanja kritičnih informacij.

14. V prihodnosti bo zelo pomembno izvajanje ustreznih stresnih testov za različne segmente kritične infrastrukture, saj se bo le skozi takšne teste realneje ocenilo razkorak med načrtovanim in realnim stanjem v segmentih kritične infrastrukture. To bo pomemben korak pri zagotavljanju višje odpornosti vseh organizacijskih ravni v družbi.

15. Pri razumevanju pomembnosti neprekinjenega delovanja ključnih industrijskih organizacij se je treba zavedati, da je pri tem nujno tudi vključevanje lokalnih in nacionalnih organizacij in njihovo sodelovanje pri zagotavljanju neprekinjenega delovanja industrijskih organizacij oziroma podjetij. Z vključevanjem in sodelovanjem lokalne infrastrukture in ustanov se lahko izognemo možnim negativnim vplivom v primeru nesreč in drugih kriznih stanj za širšo lokalno skupnost.

16. Za konec je bil oblikovan sklep, da se je treba pri iskanju najbolj optimalnih rešitev pri zagotavljanju višje stopnje odpornosti in neprekinjenosti delovanja kritičnih procesov in organizacij nasloniti tudi na lastno znanje in izkušnje in ne le nekritično prenašati tujih praks v naše okolje.

17. V okviru pomembnih projektov EU na področju neprekinjenosti delovanja kritične infrastrukture, in sicer **ATLANTIS** - Izboljšana odpornost kritične infrastrukture na

obsežna transnacionalna in sistemska tveganja, **SUNRISE** - Strategije in tehnologije za združeno in odporno kritično infrastrukturo ter vitalne storitve v Evropi, prizadeti s pandemijo, in PRECINCT - Pripravljenost in odpornost kritične infrastrukture za kaskadne kibernetske - fizične grožnje tvorno sodelujejo tudi slovenski partnerji. Projekti prinašajo in predstavljajo veliko dobrih praks in novih znanj, ki jih je treba implementirati v operativni sistem zagotavljanja višje stopnje odpornosti slovenskih organizacij.

18. Strokovna združenja, ki se pri svojem delovanju ukvarjajo s področji, ki imajo neposredni vpliv na dvigovanje razumevanja pomena odpornosti organizacij in družbe kot celote, morajo tudi v prihodnje ostati eden od glavnih partnerjev države pri zagotavljanju višje stopnje varnostnega zavedanja vseh ključnih deležnikov, pri čemer so še posebej izpostavljeni pomembni gospodarski subjekti.«

Marko Lotrič
predsednik