CRNA GORA
MINISTARSTVO JAVNE UPRAVE

INFORMACIJA
O STEPENU REALIZACIJE METODOLOGIJE IZBORA KRITIČNE INFORMATIČKE INFRASTRUKTURE

Podgorica, april 2017. godine

1 UVODNE NAPOMENE

Dok tradicionalni pristup bezbjednosti prikazuje vojne prijetnje kao najveće opasnosti po društva i države, savremeni bezbjednosni izazovi i rizici dolaze iz potpuno nove sfere - informatičke sfere.

Koncept nacionalne bezbjednosti se redefinisao, pa vojne, obavještajne i druge operacije zavise od sajber bezbjednosti. U prilog tome svjedoči i i odluka na NATO Samitu u Varšavi, jula 2016. godine, da se sajber prostor proglasi zvaničnim operativnim domenom ratovanja, zajedno sa vazduhom, morem, zemljom i svemirom.

Stalne i brze promjene u međunarodnim odnosima, porast bezbjednosnih izazova, rizika i prijetnji, kao i deficit bezbjednosti, uslovljavaju da globalna bezbjednosna slika postaje kompleksna, a kritična infrastruktura odnosno kritična informatička infrastruktura (**KII**) dobija nove dimenzije i sve veći značaj na nacionalnom i međunarodnom nivou.

Glavna komponenta infrastrukture informacione bezbjednosti jeste sposobnost nacije da spriječi, otkrije, istraži bezbjednosne prijetnje kao što su terorizam i organizovani kriminal, ali i medicinske, vojne, ekološke, ekonomske i druge prijetnje. Tim prije što napad na KII može imati kaskadni efekat i uticati na veliki broj građana, odnosno ugroziti vitalne funkcije društvene zajednice, ali i bezbjednost zemalja u regionu i šire. Stoga, prijetnje jedne zemlje ili nacije u domenu KII predstavljaju potencijalnu opasnost za druge, pa njihovo identifikovanje i blagovremeno reagovanje postaju sve značajniji faktor upravljanja bezbjednošću.

Pojedine države tretiraju KII u okviru kritične infrastrukture na liniji izraženog stava da je praktično nemoguće govoriti o kritičnoj infrastrukturi, a ne uzeti u obzir informatičke sisteme na kojima se danas sve više zasniva funkcionisanje, kontrola i generalno rad fizičkih sistema. NATO je kritičnu infrastrukturu definisao kao: sredstva, objekti, mreže i usluge, čiji bi kvar ili uništenje ozbiljno uticalo na zdravlje, bezbjednost, ekonomsko stanje, socijalnu zaštitu i funkcionisanje države.

Evropska unija (EU) je u avgustu 2016. godine ratifikovala Direktivu o mrežnoj i informacionoj bezbjednosti koja sadrži dvadeset i četiri člana koji precizno uređuju oblast kritične informatičke infrastrukture. Značaj KII, aktivnosti i pravci kretanja vezani za uređenje ove oblasti obrađuju se i u drugim strateškim dokumentima EU: Strategija sajber bezbjednosti, Jedinstveni digitalni market EU, Digitalna Agenda Evrope.

EU definiše kritičnu infrastrukturu kao: (a) imovinu, sistem ili njegov dio koji se nalazi na teritoriji zemlje članice i koji je neophodan za održavanje ključnih društvenih funkcija, zdravstva, bezbjednosti, mira, ekonomskog ili socijalnog blagostanja, a čije bi ometanje ili uništenje imalo značajan uticaj na zemlju članicuò; dok (b)òEvropska kritična infrastruktura ï podrazumijeva kritičnu infrastrukturu lociranu na teritoriji zemlje članice, čije bi ometanje ili

uniġtenje imalo znaļajan uticaj na bar dvije zemlje ļlanice. Znaļaj poremeĺaja u funkcionisanju elemenata kritiļne infrastrukture treba da se procijeni na osnovu kriterijuma meĽuzavisnosti. To podrazumijeva efekte nastale kao rezultat meĽusektorske zavisnosti od drugih tipova infrastrukture.ò

Polazeĺi od navedenih smjernica, a imajuĺi u vidu da su tipovi kritiļne infrastrukture od drġave do drġave veoma razliļiti i da zavise od stavova nadleġnih u pogledu toga ġta se podrazumijeva pod kritiļnom infrastrukturom, postoji potreba za sveobuhvatnim pristupom u oblasti zaġtite kritiļne infrastrukture.

2 AKTIVNOSTI NA PLANU REALIZACIJE METODOLOGIJE IZBORA KRITIČNE INFORMATIČKE INFRASTRUKTURE

Strategijom sajber bezbjednosti Crne Gore (u daljem tekstu Strategija) koja je usvojena za period od 2013. do 2017. godine, a kroz strateġki cilj broj dva: *„Zaštita kritične informatičke infrastrukture u Crnoj Gori“,* predviĽeno je definisanje i sistematska zaġtita Kritiļne informatiļke infrastrukture[1] (u daljem tekstu KII).

Prateĺi pomenuti strateġki cilj, 16.10.2014. godine na 85. sjednici, Vlada Crne Gore je usvojila **Metodologiju izbora kritične informatičke infrastrukture** sa prateĺim akcionim planom, kroz zakljuļak broj 08-2417/3.

Metodologijom su definisani kritiļni sektori kao i organi pod ļiju nadleġnost pripadaju (*Tabela 1*).

	KRITIČNI SEKTORI	**NOSIOCI KRITIČNOG SEKTORA**
1	Informacione i komunikacione tehnologije	Ministarstvo javne uprave
2	Bankarstvo i finansije	Ministarstvo finansija
3	Energetika	Ministarstvo ekonomije
4	Zdravstvo	Ministarstvo zdravlja
5	Poljoprivreda, bezbijednost hrane, ġumarstvo i vodoprivreda	Ministarstvo poljoprivrede i ruralnog razvoja

[1] Na osnovu Strategije donijet je Zakon o izmjenama i dopunama zakona o informacionoj bezbjednosti ("Sluġbeni list Crne Gore, broj 40/2016" od 30.6.2016. godine) kojim je formalno-pravno definisana Kritiļna informatiļka infrastruktura kao: Ă***informacioni sistemi organa čijim bi se prekidom rada ili uništenjem ugrozili život, zdravlje, bezbjednost građana i funkcionisanje države i od čijeg funkcionisanja zavisi vršenje djelatnosti od javnog interesa***ñ.

6	Nacionalna odbrana i bezbjednost	Ministarstvo odbrane / Ministarstvo unutrašnjih poslova / Ministarstvo pravde/ Agencija za nacionalnu bezbjednost
7	Transport	Ministarstvo saobraćaja i pomorstva
8	Državni organi/Usluge Vlade CG	Ministarstvo javne uprave

Tabela 1: Nosioci sektora kritične informatičke infrastrukture

U skladu sa pomenutim zaključkom (broj 08-2417/3), tačka 3, Ministarstvo javne uprave dobilo je zadatak da koordinira aktivnostima na ovom polju.

Na toj liniji, formirana je inter-resorna Radna grupa (u daljem tekstu RG) u čijem sastavu su bili predstavnici:

- Agencije za nacionalnu bezbjednost;
- Ministarstva ekonomije;
- Ministarstva finansija;
- Ministarstva odbrane;
- Ministarstva poljoprivrede i ruralnog razvoja;
- Ministarstva pravde;
- Ministarstva saobraćaja i pomorstva;
- Ministarstva unutrašnjih poslova;
- Ministarstva javne uprave i
- Ministarstva zdravlja;

Na osnovu Metodologije u okviru I faze članovi RG izradili su detaljnu analizu informacionih sistema organa kojima pripadaju. U okviru pomenute analize imenovani su svi informacioni sistemi kao i njihovi administratori, broj korisnika tih sistema i uraĎena je analiza zavisnosti u odnosu na druge informacione sisteme i servise.

U okviru II faze članovi RG izradili su detaljnu analizu informacionih sistema državnih institucija u njihovoj nadležnosti. S obzirom da su kroz metodologiju definisani kritični sektori, nadležni organi iz Tabele 1 su identifikovali sve državne institucije iz sektora njihove nadležnosti, a zatim saradnji sa identifikovanim organima, odnosno službenicima zaduženim za oblast informatike, izradili analizu informacionih sistema tih organa kao što je to uraĎeno u fazi I.

U okviru III faze članovi RG proslijedili su prethodno definisani upitnik i instrukcije privatnom sektoru na osnovu kojeg je dobijena analiza informacionih sistema u njihovom posjedu, a po ugledu na prethodne analize iz faze I i II.

U okviru IV faze na osnovu matriksa kritičnosti i drugih mjerila kritičnosti, članovi RG su u okviru svojih sektora, odnosno informacionih sistema prethodno analiziranih u fazama I, II i III, pristupili identifikaciji liste kritičnih informatičkih sistema.

Kroz TAIEX misije korišćene su usluge eksperata na planu konsultacija, dobijanja preporuka i razmjene mišljenja s ciljem finalizacije Analize predviđene Metodologijom i donošenja konačne liste kritičnih informatičkih sistema.

Uredbom o izmjenama i dopunama Uredbe o organizaciji i načinu rada državne uprave ("Sl. list CG", br. 73/2016) koju je Vlada Crne Gore donijela, u petak, 25. novembra 2016. godine, Ministarstvo javne uprave je preuzelo nadležnosti u ovoj oblasti od Ministarstva za informaciono društvo i telekomunikacije i nastavilo sa koordinacijom aktivnosti RG u pravcu finalizacije Analize kritične informatičke infrastrukture, a na osnovu matriksa kritičnosti.

3 ZAKLJUČNE NAPOMENE

Kritična informatička infrastruktura je prepoznata kao jedan od prioriteta u procesima integracija, ali proces identifakcije, poštetna ulaganja, kao i tehnička pomoć nedovoljni su za optimalno osiguranje kritične informatičke infrastrukture. Stoga je nephodno osmisliti programe i zaštititi ključne resurse za upravljanje KII.

Kako su informacioni sistemi u velikoj mjeri međusobno povezani ili povezani s javnim sistemima, kritična informatička infrastruktura u današnje vrijeme postaje sve izloženija, ne samo otkazima i havarijama, već i raznim vrstama namjernih napada. Osnovni problem iz kojeg proizilazi nužnost prepoznavanja kritične infrastrukture, predstavlja činjenica da napad na određenu kritičnu infrastrukturu sam po sebi multiplicira štetu, jer relativno mali napad na jedan infrastrukturni sistem može imati ogroman uticaj i prouzrokovati štetu na čitavom nizu međusobno povezanih infrastrukturnih sistema, tzv. kaskadni efekat.

S tim u vezi, upravljanje kritičnom informatičkom infrastrukturom treba da bude sastavni dio razvojnih programa, a kategorije poput sigurnosti i prevencije rizika od nepogoda i katastrofa, moraju se integrisati u sve relevantne dokumente Vlade, tim prije što Evropska komisija zahtijeva od država članica da definišu osnovne uslove nephodne za postojanje adekvatnog nivoa sposobnosti i kapaciteta nacionalnih kritičnih informatičkih infrastruktura.