



Broj/Broj: 03/1-50-14-7-8/11

Sarajevo/Sarajevo, 24. 11. 2011. godine

PREDMET: Izvještaj sa službenog puta, London i Tallinn 10. - 14.10.2011. g.

U periodu od 10.10.2011.-14.10.2011. obavljena je službena studijska posjeta predstavnika institucija iz Bosne i Hercegovine Velikoj Britaniji i Estoniji na temu Cyber sigurnost. Delegaciju BiH činili su predstavnici sljedećih institucija: Ministarstva sigurnosti, Zajedničke komisije za odbranu i sigurnost, Državne agencije za istrage i zaštitu, Ministarstva odbrane, Federalne uprave policije i Ministarstva unutrašnjih poslova RS.

U sklopu boravka u Velikoj Britaniji posjećen je Cabinet Office, gdje su predstavnici institucija Velike Britanije predstavili svoju organizaciju i iskustava na polju cyber sigurnosti. Održane su prezentacije predstavnika Centra za zaštitu nacionalne kritične infrastrukture, CERT-a (Computer Emergency Response Team-Tim za odgovore na računarske incidente) Ministarstva odbrane UK i Kancelarije za sigurnost i borbu protiv terorizma. Naglašeno je da svake godine Velika Britanija izdvaja oko 650 miliona funti za potrebe cyber sigurnosti.

U sklopu boravka u Estoniji posjećen je Estonski CERT gdje se delegacija BiH upoznala sa njihovom organizacijom, nadležnostima i oblastima djelovanja. U drugom dijelu boravka u Estoniji članovi delegacije BiH posjetili su NATO Centar izvrsnosti za pitanja cyber sigurnosti u Tallinnu. Bitno je naglasiti da je Estonija svoje kapacitete najviše razvila poslije destruktivnog napada na Estonske sisteme 2007. godine, kada je ključna vladina, bankarska i poslovna infrastruktura nekoliko dana bila izvan funkcije što je za posljedicu imalo nesagledive materijalne i nematerijalne gubitke.

S obzirom na sve veći broj automatizovanih i informatizovanih servisa i usluga, kako u državnom, tako i privatnom sektoru, koji mogu predstavljati moguće mete napada preko cyber prostora, uočeno je da su u Velikoj Britaniji i Estoniji pitanja cyber sigurnosti jedan od državnih prioriteta.

Obje države imaju razvijenu strategiju za cyber sigurnost kao osnovu za dalje aktivnosti, koja definiše kritičnu infrastrukturu koju je neophodno zaštititi sa definisanim mehanizmima zaštite i saradnje između institucija i drugih subjekata unutar države. Također je definisana i saradnja na regionalnom i međunarodnom planu.

Isti tako, Velika Britanija i Estonija imaju oformljena i dovoljno osnažena CERT tijela unutar države koja štite kritičnu infrastrukturu, tj imaju snažna preventivna tijela za borbu protiv

cyber prijetnji. „Više resursa za prevenciju=manje resursa za reakciju“. Svakako da imaju i jake zakonske mehanizme za cyber sigurnost.

U posljednje 2 godine pojavljuju se maliciozni softveri koji direktno nanose velike štete industriji i uređajima u industriji (npr STUXNET), dok je recimo prije nekoliko godina najveća šteta od malicioznih softvera šteta bila brisanje podataka. Za razliku od većine računarskih virusa koji su dizajnirani da nanesu štetu računarskim sistemima, STUXNET crv je recimo stvoren kako bi zarazio industrijske sisteme. Bio je izuzetno uspješan u svojoj misiji. 2010. godine kada je ovaj opasan i vrlo sposoban virus gotovo sabotirao iranski nuklearni program.

S obzirom na iznešeno, jasno su vidljiva velika interesovanja i ulaganja Velike Britanije i Estonije na polju cyber sigurnosti. Ove dvije države su u poodmakloj fazi razvoja kapaciteta za zaštitu od cyber napada, dok u Bosni i Hercegovini razvoj tih kapaciteta tek treba da se dešava. Jedan od koraka koje je Bosna i Hercegovina učinila na ovom polju je usvajanje Strategije za uspostavu CERT tijela u BiH usvojene od strane Vijeća Ministara BiH na 156. sjednici ove godine. U Republici Srpskoj je prije par mjeseci usvojen Zakon o informacijskoj sigurnosti gdje je definisana uspostava CERT tijela za zaštitu infrastrukture organa uprave u RS-u. CERT tijela unutar države moraju imati jaku saradnju i dobru razmjenu informacija između sebe, agencija za provođenje zakona, kao i sa drugim tijelima u inostranstvu, jer cyber prostor ne poznaje teritorijalne, etničke, rasne ili nacionalne granice. Uspostavom ovakvih tijela se u određenoj mjeri smanjuje rejting Bosne i Hercegovine kao zemlje visokog rizika kada su u pitanju strana ulaganja, obzirom da su danas svi biznis procesi zasnovani na informacionim tehnologijama i internetu.

U periodu od 09.-11. Novembra ove godine u Tesliću, u organizaciji Ministarstva sigurnosti, OSCE misije u Bosni i Hercegovini i NATO štaba u Sarajevu planirano je održavanje seminara o cyber sigurnosti. Cilj je da se kroz diskusije i prezentacije međunarodnih stručnjaka u kombinaciji s iskustvima i znanjem koje je prikupljeno iz ove studijske posjete i drugih iskustava, napravi sveobuhvatna rasprava o ovom pitanju.

Bosna i Hercegovina treba nastaviti razvijati kapacitete za zaštitu od cyber prijetnji koje će za nekoliko godina, a možda i prije, biti najopasnija prijetnja po nacionalne sigurnosti država u cijelom svijetu. Naredni korak je formiranje Radne grupe na Vijeću Ministara BiH koja će imati zadatak izvršiti sve pripreme za formiranje CERT tijela u BiH.

Također je na kraju veoma važno napomenuti da EU i NATO snažno podržavaju aktivnosti na razvoju kapaciteta za cyber sigurnost.

Član Zajedničke komisije

Mehmed Bradarić