БОСНА И ХЕРЦЕГОВИНА
ПАРЛАМЕНТАРНА СКУПШТИНА
БОСНЕ И ХЕРЦЕГОВИНЕ
ДОМ НАРОДА
ПРЕДСТАВНИЧКИ ДОМ
Заједничка комисија за одбрану и безбједност
Босне и Херцеговине

BOSNA I HERCEGOVINA
PARLAMENTARNA SKUPŠTINA
BOSNE I HERCEGOVINE
DOM NARODA
PREDSTAVNIČKI DOM/ZASTUPNIČKI DOM
Zajednička komisija za odbranu i sigurnost
Bosne i Hercegovine
Zajedničko povjerenstvo za obranu i sigurnost
Bosne i Hercegovine

Broj: 03/1-50-14-7-9/11
Sarajevo, 21. 12. 2011. godine

Izvještaj sa seminara o cyber sigurnosti, Teslić 09. - 11.11.2011. g.

U periodu od 09.11.2011.-11.11.2011. u hotelu "Kardial" u Tesliću održan je seminar na temu "Cyber-sigurnost", u organizaciji Ministarstva sigurnosti, uz podršku OSCE misije u BiH, NATO štaba u Sarajevu i ambasade Velike Britanije u BiH.

Na seminaru su učestvovali eminentni stručnjaci iz oblasti cyber sigurnosti, cyber kriminala/terorizma i CERT-a (Computer Emergency Response Team – Tim za odgovore na računarske incidente).

Na seminaru su predstavljeni aktuelni izazovi u oblasti cyber sigurnosti. Prezentacije su održali predstavnici sljedećih institucija i organizacija:

- Ministarstvo sigurnosti,
- Ministarstvo unutrašnjih poslova Republike Srpske,
- DCAF (Democratic Control of Armed Forces – Demokratska kontrola oružanih snaga),
- Ministarstvo unutrašnjih poslova Republike Hrvatske,
- NATO štab iz Brisela,
- FIRST (Forum for Incident Response and Security Teams- Globalni forum za CERT timove),
- Trusted introducer – Forum za CERT timove u Evropi,
- Nacionalni CERT Austija,
- ENISA (European Network and Information Security Agency-Evropska agencija za mrežnu i informacionu sigurnost),
- Nacionalni CERT Republike Hrvatske,
- Nacionalni CERT Estonije,
- Nacionalni CERT Rumunije.

Ostali učesnici seminara su bili predstavnici Suda BiH, Ministarstva komunikacija i transporta, Vlade RS, Agencije za informaciono društvo RS, SIPA-e, Munistarstva unutrašnjih poslova FBiH, Policije Brčko Distrikta, Agencije za bankarstvo FBiH, Agencije za bankarstvo RS, Granične policije, Agencije za identifikaciona dokumenta i razmjenu podataka (IDDEEA), Ministarstva odbrane, Udruženja banaka BiH, BH Telecom-a, Direkcije za koordinaciju policijskih tijela, M:tel-a, Zajedničke komisije za odbranu i sigurnost Parlemantarne skupštine BiH.

Na kraju drugog dana Seminara učesnici su podijeljeni u tri grupe i to grupa 1 Prevencija, grupa 2 Istrage, procesuiranje i odbrana i grupa 3 Privatni sektor. Svaka grupa je usaglasila određene neobavezujuće zaključke i preporuke:

Grupa 1 – Prevencija:

- Iskazana je zabrinutost kada je u pitanju sve veći broj prijetnji koje dolaze iz cyber prostora,
- Shvaćena je ozbiljnost napada u cyber prostoru,
- Cyber sigurnost treba biti jedan od prioriteta Bosne i Hercegovine u narednom periodu, počev od danas, jer su prijetnje našim informacionim sistemima pred vratima, a neke i ulaze,
- Nastaviti razvoj kapaciteta za cyber sigurost u Bosni i Hercegovini (zakonski, organizaciono, kadrovski, materijalno, edukacijski),
- Potrebno je puno raditi na preventivnom dijelu, jer više resursa na prevenciji manje je resursa na reakciji i rješavanju problema nakon incidenata,
- Potrebna je konstantna informisanost o prijetnjama, ranjivostima i kulturi ponašanja u cyber prostoru svih učesnika u cyber prostoru u Bosni i Hercegovini kako bi oni mogli dobro zaštiti svoj dio cyber prostora,
- Konstantno raditi na podizanju svijesti o cyber sigurnosti, pogotovo kod mlađe populacije (npr u osnovnim školama),
- CERT tijela trebaju biti uspostavljena i nastavljen njihov razvoj organizacijski, legislativno i materijalno,
- Ojačati saradnju između svih aktera po pitanju cyber sigurnosti na interancionalnom, regionalnom i lokalnom planu.

Grupa 2 – Istrage, procesuiranje i odbrana:

1. **Jača saradnja bezbjednosnih intitucija**

Saradnja bezbjednosnih institucija je jedan od suštinskih temelja borbe protiv sajber kriminala. U BiH, borbu protiv sajber kriminala izvode entitetske policijske strukture. Saradnja između FUP i MUP RS na polju borbe protiv sajber kriminala ocijenjena je da je na izuzetno visokom nivou.

2. **Formiranje i jačanje struktura koje se bave ovom problematikom**

Istražne radnje u krivičnim djelima sajber kriminala možemo razvrstati u 2 grupe: istražne radnje korištenja sajber tehnologija u krivičnim djelima organizovanog, opšteg, privrednog i drugih oblika kriminaliteta (koje se prije svega ogleda u dokaznim radnjama pretresa i

vještačenja) i istrage krivičnih djela protiv bezbjednosti računarskih podataka: oštećenje računarskih podataka i programa, računarska sabotaža, računarska prevara, izrada i unošenje računarskih virusa, neovlašteni pristup i dr.

a. Pitanje: **da li sve policijske strukture imaju nadležnost u obavljanju istražnih radnji korištenja sajber tehnologija u drugim krivičnim djelima?**

Uočeno je da sve policijske strukture vrše istrage korištenja sajber tehnologija u okviru istraga krivičnih djela i postavljeno je pitanje da li sve policijske strukture imaju nadležnost obavljanja ove vrste istraga. Svi su se složili da u pitanju nisu istrage krivičnih djela protiv računarskih podataka koji su kao takvi regulisani entitetskim zakonima, te da radnje **dokazivanja su dužne da preduzimaju sve policijske strukture**. Dalje govoreći, zbog ograničenih kapaciteta na polju forenzičke opreme koju posjeduju bezbjednosne strukture bila bi poželjna **veća saradnja i korištenje raspoloživih resursa drugih bezb. struktura** po ovom pitanju.

b. Pitanje: **način postupanja i istraga ukoliko dođe do slučajeva sajber kriminala u zajedničkim institucijama BiH**?

Odgovor na ovo pitanje je izuzetno kompleksan imajući u vidu nadležnosti pravosudnih i policijskih tijela u BiH. Poštujući trenutni legislativni i institucionalni okvir BiH, entiteta i BDBiH preporuka je da se oformi zajednički tim policijskih i pravosudnih institucija/agencija u BiH. Na način i u skladu sa EU standardima i preporukama, jer je zajednička saradnja bitan temelj uspješnosti istraga sajber kriminala

3. Saradnja sa ISP i regulatornim tijelima

Saradnja sa ISP predstavlja jedno od osnovnih neophodnih uslova za borbu protiv ove vrste krimiminaliteta. Ta saradnja treba da bude u skladu sa zakonom, efektna i brza, u kojoj treba da budu jasno definisane obaveze svih strana. Regulatorna tijela treba da postave jasne **standarde po pitanju minimalne dužine čuvanja informacija o korisnicima**. Obaveza bezbjednosnih agencija i ISP trebala biti **regulisanje načina traženja, odnosno izdavanja traženih podataka u operativne svrhe,** putem memoranduma o razumijevanju i saradnji. Ova stavka je neophodna iz razloga što su krivična djela iz oblasti sajber kriminala često vremenski kritična.

4. **Izmjene zakonskih i podzakonskih akata**

Neophodno je izvršiti redefinisanje zakonskih i podzakonskih akata koji se odnose na ovu problematiku u cilju harmonizacije zakonskog postupanja sa praksom i iskustvom. To se u prvom redu odnosi na uvođenje rigoroznijih kazni za ovu vrstu krivičnih djela, na harmonizaciju puta dokaza, postupanjima sa dokazima. Poseban osvrt dat je na izmjenu regulative vezane za pretres i vještačenje.

Grupa 3 – Privatni sektor:

- Formirati CERT tijela u Bosni i Hercegovini sa sljedećim funkcijama:
  - Rano obavještavanje o potencijalnim problemima,
  - Regulative i procedure vezane za elektronsko poslovanje,
  - Opšta (građanstvo) i specifična (industrija) edukacija,
  - Međusektorska koordinacija pri odgovoru na napade.
- Što hitnije uraditi procjenu ugroženosti,
- Uticati na zakonodavce da zakon o elektronskom poslovanju postane operativan,
- Iznalaženje i pronalaženje organa - moderatora koje će biti inicijator svih aktivnosti vezan za privatni sektor.

Ovaj seminar je bio dobra prilika da se upoznaju osobe iz različitih agencija/institucija/organizacija koje rade na poslovima cyber sigurnosti, da se razmijene određena iskustva, predstave dosadašnje aktivnosti, dogovore određeni naredni koraci. Ukazana je potreba jačanja saradnje i koordinativnog djelovanja prema cyber izazovima, stvorena je platforma za dijalog i doneseni su opšti neobavezujući zaključci.

Član Zajedničke komisije

Mehmed Bradarić