PC Press [Serbia]

Page: 8
Reach: 25897
Country: SERBIA
Size: 426 cm2

03.09.2015

Semjuel Beket i nacionalna informaciona bezbednost

Zakon o informacionoj bezbednosti predstavlja okvir za formiranje domaćeg CERT-a, tela koje će brzo reagovati na eventualne probleme u funkcionisanju Interneta. Ovakvo telo imaju sve razvijene zemlje, a nama je bilo potrebno još pre više godina...

Dušan Stojičević

Ako se uzme u obzir činjenica da Slovenija ima nacionalni CERT *(Computer Emergency Response Team)* od 1995. godine i da sada slavi 20 godina njegovog postojanja, a da je SAD formirala *United States Cyber Command* – specijalni vojni rod za cyber ratove – još 2009. godine, neophodno je da naša zemlja usvoji Zakon o informacionoj bezbednosti i da formira nacionalni CERT... i to pre najmanje 10 godina.

Zakon o informacionoj bezbednosti

Uz mnogobrojna prethodna odlaganja, pred nama je konačno predlog Zakona o informacionoj bezbednosti, čime se Srbija najzad pomerila sa mrtve tačke u ovoj oblasti. Kada govorimo o samom predlogu Zakona, moram reći da on nije loš, ali da postoje izvesne manje i veće manjkavosti koje bi trebalo da se dorade. Prema burnoj javnoj raspravi koja je održana u PKS i komentarima koji su tada izneti, vidi se da se na ovaj zakon čekalo dugo i da je neophodan. U razgovorima sa finskim, slovenačkim i hrvatskim CERT-om uvideli smo koliko napada dolazi preko računara sa naše teritorije (finski CERT nam je pokazao lošu situaciju u *cyber* bezbednosti u Srbiji, i to u realnom vremenu, tokom RIPE SEE skupa održanog u aprilu ove godine u Beogradu), sasvim je sigurno da Srbija vapi za nacionalnim CERT-om, čak i bez donošenja Zakona.

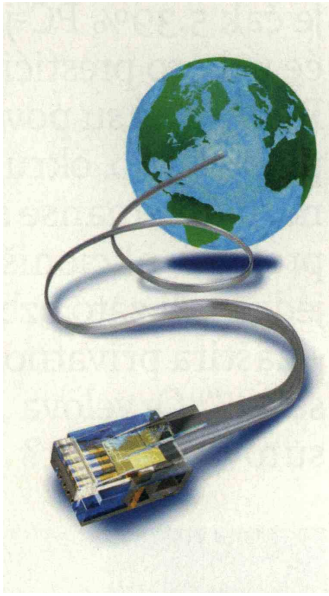
Glavna odlika ovog predloga Zakona jeste da se on najviše bavi državom i državnim službama, i kao takav je dovoljno dobar. Glavne predloge koje je RNIDS izneo u okviru komentara u javnoj raspravi tiču se upravo preusmerenja fokusa zakona sa državnog na nacionalni nivo, što bi trebalo da je i svrha ovog Zakona. Radi uspešnosti sprovođenja Zakona u njemu treba uvesti dobru praksu iz evropskih zemalja koje insistiraju na višepartnerskom modelu, na kome i počiva upravljanje Internetom u celini. Stoga smo predložili izmene koje se tiču učešća civilnog sektora (privatnih firmi, preduzetnika i drugih stručnih organizacija) u nacionalnoj informacionoj bezbednosti. Shodno tome da u predlogu Zakona nije definisana kritična infrastruktura, a da je u vlasništvu privatnih firmi skoro 90 odsto domaće infrastrukture, saradnja sa njima je neminovna, pogotovo ako se uzme u obzir potencijalna privatizacija Telekoma.

Druga glavna karakteristika predloga Zakona je opšti karakter, koji iziskuje izradu mnogobrojnih podzakonskih akata – čak 21 podzakonski akt, od kojih 19 treba da proizvede MTTT u narednih 12 meseci od donošenja Zakona. Ovo može predstavljati usko grlo, pošto je većina ovih podzakonskih akata usko-stručna. Čak i ovde je vidno da je potrebna saradnja sa civilnim sektorom koji ima znanja da pomogne u ovako obimnom zadatku.

Nacionalni CERT

Glavni cilj ovog predloga Zakona jeste formiranje nacionalnog CERT-a. Predlozi koje je RNIDS uputio na ovu temu odnose se na to da je nedovoljno precizno definisana njegova uloga, kao što je slučaj i sa ulogama ostalih tela. Prilikom definisanja uloga u oblasti nacionalne informacione bezbednosti, postoji tri nivoa: politički (vlada i ministarstva), strateški (obrazovan u višepartnerskom modelu) i operativni (nacionalni CERT koji kreira svoje veze na bazi poverenja). U predlogu Zakona imamo donekle izmešane ove oblasti u predloženim telima, a predlozi RNIDS-a su se odnosili na preciziranje uloga predloženih tela informacione bezbednosti.

U razgovorima sa finskim, slovenačkim i hrvatskim CERT-om prikupljene su informacije o brojnim napadima koji dolaze preko računara sa teritorije Srbije. Naša zemlja vapi za nacionalnim CERT-om, koji bi trebalo osnovati čak i pre donošenja Zakona



Shodno činjenici da svi oko nas, osim Bosne i Hercegovine (Crna Gora i Makedonija su u fazi formiranja), imaju nacionalni CERT, sa ili bez Zakona i strategija, neophodno je da što pre i mi imamo nacionalni CERT, možda i pre donošenja Zakona o nacionalnoj informacionoj bezbednosti. RNIDS, kao organizacija koja upravlja jednim kritičnim internet resursom – nacionalnim domenima .rs i .??? – upravo je u fazi formiranja CERT-a koji će se baviti informacionom bezbednošću u okviru ovih domena. Radna grupa završava svoj rad i očekujemo formiranje našeg CERT-a tokom ove ili naredne godine.

Dušan Stojičević je Predsednik Upravnog odbora Registra nacionalnog internet domena Srbije (RNIDS)