Bitka za Zakon o informacionoj bezbednosti Srbije

Zoran Živković dipl. Inž.
Predsednik Durštva za informacinu bezbednost Srbije

Značaj informacione bezbednosti

- Informaciona bezbednost Srbije je već dugo nacionalni resurs od najvećeg značaja, to je nacionalno blago 21 veka.
- Nacionalna bezbednost savremenih država počiva pre svega na Informacionoj bezbednosti kao zajedničkom imenitelju svih ostalih osnovnih kamena temeljaca bezbednosti.
- Ekonomska, vojna i diplomatska bezbednost se ne mogu više posmatrati samostalno bez Informacione bezbednosti.
- Počela je Druga digitalna revolucija – Infomaciono društvo je realnost.

Položaj IB-a u svetu

- Zemlje sveta su odavno shvatile značaj nacionalne informacione bezbednosti prepoznavši nezamenljivi značaj za opštu nacionalnu bezbednost.

- SAD je počela da se bavi IB 60-tih godina 20. veka. Da bi danas imali na snazi nešto manje od 20 zakona koji se bave delimično ili isključivo informacionom bezbednošću zemlje.

- Ruska Federacija je počela da razvija informacionu bezbednost svoje zemlje 90-ih godina 20. veka. Do sada su doneta tri zakona koja se isključivo bave IB, dva zakona koji je delimično obuhvataju i novi nacrt strategije o kiber bezbednosti koji uskoro treba da bude prihvaćen.

ZAŠTO JE VAŽAN ZAKON

- BEZ INFORMACIONOG DRUŠTVA NEMA NAPRETKA A PREMA TOME NI SAMOG DRUŠTVA.
- BEZ INFORMACIONE BEZBEDNOSTI NEMA NACIONALNE BEZBEDNOSTI.
- BEZ INFROMACIONE BEZBEDNOSTI NEMA NACIONALNOG KIBER PROSTORA.
- BEZ INFORMACIONE BEZBEDNOSTI NEMA OSNOVNIH VREDNOSTI SAVREMENOG SVETA NITI JEDNE SLOBODE ZAGARANTOVANE.

SAD

It is the policy of the United States to prevent or minimize disruptions to critical information infrastructures and thereby protect the people, the economy, the essential human and government services, and the national security of the United States.

1992. – Department of Defence Directive (DoDD) TS 3600.1 – "Informational Warfare"

1993. - MoP-30 – "Command and Control Warfare" (C2W)

1994. - DoD Science Committee – publikacije o specijalnim organizaciono-tehničkim merama zaštite informacione strukture

1996 - Department of the Army - FM-106. "Information Operations"

1998. – Presidential Decision Directive – PDD-63 – "Critical Infrastructure Protection"

2000. – Nationa Critical Infrastructure Plan

2002. – Cyber Security Enhancement Act, H.R.3482

2003. – National Strategy to Secure Cyberspace

2003. – National Strategy for Physical Protection of Critical Infrastructures and Key Assets

2003. – Inteligence Authorization Act For Fiscal Year 2003.

2003. – Homeland Security Information Sharing Act

RUSKA FEDERACIJA

Ruska Federacija informacionu bezbednost definiše kao

"stanje zaštićenosti životno važnih interesa ličnosti, društva i države u informacionoj sferi od spoljašnjih i unutrašnjih opasnosti (rizika), odnosno kao stanje zaštićenosti informacione sredine društva koje omogućava njeno formiranje, korišćenje i razvoj u interesu građana, organizacija, države."

Do sada je doneto pet zakona i jedan nacrt:

- 2000. - Nacionalni bezbednosni koncept Ruske Federacije
- 2000. - Doktrina informacione bezbednosti Ruske Federacije
- 2011. - Koncept aktivnosti oružanih snaga Ruske Federacije u informacionom prostoru
- 2013. - Koncept spoljne politike Ruske Federacije
- 2013. - Osnovni principi bezbednosne politike Ruske Federacije na polju međunarodne informacione bezbednosti
- 2014. - Nacrt koncepta strategije informacione bezbednosti Ruske Federacije

EU

- Prvi značajaniji dokument Evropske Unije donet je 2001. godine u Budimpešti – Kovencija o kiber kriminalu.

- Nakon toga je usvojena brojna regulativa koja uređuje oblast IB. Izdvajamo neke od najbitnijih:

  – Direktiva o obradi ličnih podataka i privatnosti elektronske komunikacije (2002)
  – Regulativa o zaštiti kritične informacione infrastrukture (2009)
  – Strategija o kiber bezbednosti EU (2013)
  – Direktiva o napadima na informacione sisteme (2013).

EU

Institucije na nivou EU koje se bave Informacionom bezbednošću.

- ENISA (European Union Agency for Network and Information Security)
- EC3 (European Cybercrime Centre) - Evropskoi centar za borbu protiv kiber kriminala
- CERT-EU (Computer Emergency Response Team EU)
- OEBS – OSAC

EU

- 1995. - Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- 2001. – Convention on Cyber Crime (Budapest Convention)
- 2002. - Directive 2002/58/EC on privacy and electronic communication
- 2009. – COM (2009) 149 - Critical Information Infrastructure Protection
- 2001. – Commission Decision 20/87/EU on standard contractual clauses for the transfer of personal data to processors established in third countries
- 2012. – COM (2012) 140 - Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre
- 2013. – Cyber security Strategy of the European Union
- 2013. – Directive 2013/40/EU on attacks against information systems

EU

Primer EU države koja je sledila sve preporuke EU

Češka Republika

- Formirali su neophodnu regulativu:
  - Nacionalne strategije o informacionoj bezbednosti
    - Strategija za period 2011.- 2015.
    - Strategija za period 2015.- 2020.
  - Zakon o informacionoj bezbednosti (2014.)

* Primetimo redosled aktivnosti

- Uspostavljena dva CERT-a
  - Civilni
  - Državni

EU

Primer EU države koja nije sledila sve preporuke EU

Rumunija

- Rumunija za sada ima usvojenu samo Strategiju o kiber bezbednosti. Usvojena je 2013. godine.

- Postoji zakon o zaštiti kritične infrastrukture ali taj zakon ne uređuje oblast IB. tj. ne postoji zakon o informacionoj bezbednosti

- Zakon o IB je donet 2014. godine i stupio je na snagu početkom 2015. Međutim, u roku od manje od mesec dana Ustavni sud ga je proglasio neustavnim.

- Suprotno preporukama Evropske Unije da nadzorno telo za kiber bezbednost bude iz civilnog domena, Rumunija je tu ulogu dodelila svojoj Agenciji za državnu bezbednost . Njena nadležnost je bila definisana tako da su prava građana bila ozbiljno narušena.

Društvo za informacionu bezbednost Srbije - DIBS

DIBS i borba za zakon

- Nakon nekoliko godina neformalnog rada u toku kojih je organizovano nekoliko okruglih stolova i dve konferencije Društvo za informacionu bezbednost Srbije (DIBS) formirano je formalno upisom u Registar Agencije za privredne registre, 10.02.2010. Osnovni cilj Društva je podizanje nivoa znanja iz IKT-a i Informacione bezbednosti u Republici Srbiji stalnim praćenjem i ocenjivanjem stanja informacione bezbednosti u svetu i Srbiji kao i aktivnim učešćem u kreiranju Nacionalne strategije i zakonske regulative iz domena rada.

- Do sada pet Konferencija, više okruglih stolova, preko 130 naučnih i stručnih radova iz domena IB od toga više od deset potpuno posvećenih Strategiji i Zakonu, preko dvadeset besplatnih kurseva i predavanja na fakultetima i školama širom Srbije , mnogobrojne analize, tekstovi u štampi, gostovanja u emisijama
    - **Sve to Srbiji s' ljubavlju – potpuno besplatno!**

DIBS i borba za zakon

Zaključci prve konferencije:

1. Srbija je jedna od tri evropske zemlje koja nema Strategiju IB niti Zakon o informacionoj bezbednosti,
2. Srbija je jedna od pet evropskih zemalja koja nema nacionali CERT (niti bilo koji drugi).

- Na svakoj narednoj konferenciji zaključci su bili identični sem u delu poređenja sa Evropom (broj zemalja koje nemaju zakon o informacionoj bezbednosti i nacionalni CERT se stalno smanjivao.)

- U vreme održavanja poslednje DIBS-e konferencije Srbija je bila jedina zemlja u Evropi koja nema zakon o informacionoj bezbednosti i nacionalni CERT.

DIBS i borba za zakon

- Nakon ove konferencije DIBS je odlučio da se redovne godišnje konferencije Informaciona bezbednost Srbije ne održavaju dok se ne donese predlog zakona i isti ne uđe u skupštinu Srbije.

- DIBS je nastavio da se bori za zakon kao i za sve ostale ciljeve iz domena IKT i Informacione bezbednosti organizacijom okruglih stolova, učešćem na domaćim i internacionalnim konferencijama, kroz predavanja na fakultetima, gostovanjima u emisijama, pisanjem članaka i stručnih radova i sličnim aktivnostima kao i aktivnim učešćem tokom javne rasprave Nacrta Zakona.

- DIBS nije pozvan da učestvuje u izradi predloga Zakona od strane vladinog tima.

Nacrt zakona o informacionoj bezbednosti

Akcioni plan i nacrt zakona

- Akcioni plan razvoja IKTa u Srbiji do 2020. godine propisuje da nacrt zakona o informacionoj bezbednosti treba biti donet do kraja drugog kvartala 2014. godine.

- Predlog nacrta zakona je predstavljen jula 2015. godine.

- Članovi DIBSa su predlog nacrta temeljno proučili i dostavili svoje primedbe i sugestije radnoj grupi.

- U raspravu oko Nacrta Zakona uključili su se Ministarstva, udruženja iz domena IKT a i drugi

Nacrt zakona o informacionoj bezbednosti Srbije – komentari

Komentari, sugestije, primedbe

- Na nacrt Zakona koji ima 36 članova dato je mnoštvo komentara, sugestija, primedbi.
- Dobar deo se odnosi na terminologiju (PODATAK, RUKOVAOC,IKT SISTEM I SLIČNO).
- Deo komentara je vezan za nadležnosti, posebno oko nadležnosti za pojedina ministarstva (nadležnosti MO i MTTT).
- INSPEKCIJA I KONTROLA (Ko kontroliše kontrolore ili Sertifikacija).
- Deo komentra je dat na osnovu važećih preporuka i zakona u EU (manje ili veće neusaglašenosti sa EU).

Nadležni organ

- Član 4: *“Organ državne uprave nadležan za bezbednost IKT sistema je ministarstvo nadežno za poslove informacionog društva.”*

Obaveza dostavljanja podataka

- Član 7: *“Na zahtev bezbednosnih službi i ministarstva nadležnog za unutrašnje poslove, rukovalac IKT sistema dužan je da stavi na raspolaganje podatke od značaja za informacionu bezbednost, koji su službama bezbednosti i ministarstvu nadležnom za unutrašnje poslove potrebni pri obavljanju poslova iz njihove nadležnosti u skaldu sa zakonom.”*

- Izuzetno bitan član za usaglašavanje sa regluativom EU.
- Treba precizno definisati ovaj član i usaglasiti ga sa zakonima koji su već na snazi a propisuju načine za rukovanje podacima.

Nacionalni CERT

- Član 16: *“Nacionalni centar za prevenciju bezbednosnih rizika u IKT sistemima (u daljem tekstu Nacionalni CERT) obavlja poslove koordinacije prevencije i zaštite od bezbednosnih rizika u IKT sistemima u republici Srbiji na nacionalnom nivou. Za poslove Nacionalnog CERT-a nadležna je Regulatorna agencija za elektronske komunikacije i poštanske usluge.”*
- Na konferenciji u Klubu poslanika prošlog meseca ministar Ljajić je izjavio da CERT ide u Upravu Vlade Srbije? Prvobitno je bilo planirano da ide u Ratel.

Hronologija

- Po našem mišljenju mnogo je bolje bilo da je prvo usvojena Strategiju razvoja koja bi poslužiti kao osnov za donošenje nacrta zakona.

Zaključak

SRBIJA ZASLUŽUJE DA IMA DOBAR ZAKON O INFORMACIONOJ BEZBEDNOSTI, ZAKON KOJI ĆE PRE SVEGA BITI U FUNKCIJI STRATEŠKIH CILJEVA NACIONALNE BEZBEDNOSTI I U INTERESU SVIH NJENIH GRAĐANA.

Hvala na pažnji!

Zoran Živković
Društvo za informacionu bezbednost Srbije