

PRIMEDBE NA NACRT ZAKONA O INFORMACIONOJ BEZBEDNOSTI

Upravni odbor Društva za informatiku Srbije je 17 jula 2015. održao proširenu sednicu na kojoj su razmatrane i usvojene **sljedeće primedbe na Nacrt zakona o informacionoj bezbednosti.**

Opšta pitanja:

- Već nekoliko godina **postoji izuzetno aktuelna potreba** da se usvoji Zakon o informacionoj bezbednosti i reguliše osnivanje CERT-a. Dobro je što je Radna grupa za izradu Zakona imala u vidu **aktuelnu regulativu EU** i predložila rešenja u okviru postojećih institucija.
- U Nacrtu zakona informaciona bezbednost se uglavnom svodi **samo na skup mera koje treba da sprovede rukovaoc IKT sistema.** Informaciona bezbednost nije samo skup „mera za...“, već je **to širi pojam** i obuhvata bezbednosne aspekte i principe za organizovanje i funkcionisanje pravnog lica i posebno u projektovanju, organizaciji, uspostavljanju infrastrukture i upravljanju informacionim sistemom.
- Za informacionu bezbednost treba da bude **odgovorno pravno lice**, a za sprovođenje propisanih mera rukovaoc IKT sistema.
- Velikom broju učesnika u javnoj diskusiji nije bio jasan obuhvat Zakona (da li se Zakon odnosi i na sva pravna lica u privredi, obrazovanju, nauci...)? **Zato je u čl.1. potrebno izričito navesti na koga se Zakon odnosi.**
- Regulisati bezbednosne aspekte **iznošenja** ličnih podataka, poslovnih podataka... u inostranstvo radi obrade, čuvanja... **Klasifikovati koji se podaci sa stanovišta bezbednosti uopšte ne mogu iznositi.**

Konkretna pitanja:

čl. 2/2 Pronaći adekvatniji naziv za termin **rukovalac IKT sistema.** Predlažemo da se upotrebi termin **rukovodilac IKT sistema**

čl. 2/17. Zašto su samo MTT, MUP, MIP i SB **samostalni rukovaoci IKT sistemima,** **zašto su oni izvan kontrole,** šta je njihova funkcija i u čemu su oni samostalni ?

Po primenjenoj logici u samostalno rukovanje IKT sistema **treba uključiti i APR, Katastar, Registar stanovništva, baze podataka NBS, statističke baze podataka, portal eUprava...**

čl.4. Navesti taksativno nadležnosti Ministarstva u oblasti informacione bezbednosti:

- Predlaže Vladi uredbe iz oblasti informacione bezbednosti,
- Predlaže podzakonske akte iz oblasti Informacione bezbednosti,
- Predlaže Nacionalnu Strategiju iz oblasti Informacione bezbednosti,
- Definiše kritičnu infrastrukturu iz oblasti Informacione bezbednosti,
- Propisuje obaveze vlasnika i upravljača kritične infrastrukture,
- Vršiti nadzor funkcionisanja sistema informacione bezbednosti u državnim organima i organizacijama kao i svim drugim delovima kritične infrastrukture,
- Donosi planove aktivnosti i razvoja iz oblasti informacione bezbednosti,
- Vršiti inspeksijski nadzor nad primenom zakonske regulative iz oblasti informacione bezbednosti i svih drugih zakonskih okvira koji direktno ili indirektno utiču na IB,
- Vršiti akreditaciju- sertifikaciju IKT sistema i svih drugih činilaca iz oblasti informacione bezbednosti,

čl.5. U Telo za koordinaciju treba uključiti i predstavnike: **privrede(PKS), obrazovanja, Narodne banke Srbije, RNIDS, Poverenik za zaštitu podataka o ličnosti...** Zakonom treba **definisati nadležnosti** Tela za koordinaciju jer to treba da budu zakonska ovlašćenja. Ako nema svoja ovlašćenja onda će to telo imati savetodavni karakter?

Alternativa: brisati čl.5 jer se postavlja i pitanje, da li Telo za koordinaciju treba da postoji ako postoje MTT kao nadležni organ i Nacionalni CERT i CERT republičkih organa. Za razvoj informacionog društva u Srbiji, **važnije je da se obrazuje Telo za koordinaciju razvoja informacionog društva.**

čl.6. Za bezbednost IKT sistema **mora da bude odgovorno pravno lice (odgovoran starešina organa uprave, direktor, vlasnik firme...)** a samo za organizaciju i sprovođenje mera zaštite su odgovorni rukovaoci IKT sistema.

čl. 7. Zakonom treba odrediti **koje podatke rukovalac IKT sistema mora** da stavi na raspolaganje, vodeći računa o svim zakonima koji su na snazi i koji uređuju postupanje sa podacima, Ovo je važno za usaglašavanje sa EU.

Alternativa: Bolje je brisati čl.7.

čl.8. Precizirati i nabrojati **sve sisteme od posebnog značaja**. U protivnom Vlada će često morati da dopunjava listu sistema.

čl.13. Koga o incidentu obavješavaju pravna lica?

Ako je incident od interesa za javnost ko to procenjuje i na osnovu kojih kriterijuma?

čl. 17.

dodaje se nova alineja u stavu 2.

1. neposredno preduzima mere u cilju otklanjanja incidenta ili predlaže mere drugim nadležnim organima.

čl. 35. Nedoovoljivo je da se čeka **12 meseci za sve podzakonske akte!** Neki podzakonski akti se mogu predložiti odmah uz Zakon.

NAPOMENE:

- Videti da li su neka krivična dela iz oblasti informacione bezbednosti predviđena u **KZ?**
- Za sprovođenje Zakona biće u 2016. godini **potrebna sredstva za nova radna mesta i stalnu obuku i stručno usavršavanje**. Dati aproksimaciju troškova i komparirati ih sa mogućim štetama od incidenata.
- U Obrazloženju dati kratku **Analzu stanja bezbednosti, potencijalne ugroženosti, dosadašnje i moguće štete**. Ovo može da motiviše i podstakne na brže usvajanje Zakona.
- Društvo za informatiku smatra da, ukoliko se pokaže da su mali izgledi da se Zakon usvoji do kraja 2015. godine, **onda MTT treba Vladi da predloži hitno usvajanje Uredbe o osnivanju Nacionalnog CERTA**.

Beograd, 17. jul 2015.

Upravni odbor Društva za informatiku Srbije