

Beograd, 2. februar 2012.

Komentari na Nacrt zakona o informacionoj bezbednosti

U članu 1. u drugom pasusu se koriste termini "tajni i drugi podaci bez oznake tajnosti, ,,", uobičajeno se koriste termini "klasifikovani i neklasifikovani podaci". - OK

U članu 1. u trećem pasusu se definiše informaciono-komunikacioni sistem i uvodi skraćenica "IKT sistem" - Logičnije je da se uvede skraćena oznaka "IK sistem".

U članu 2. (Značenje pojedinih termina), kod termina "informaciona bezbednost" treba umesto "zaštiti" da stoji "zaštiti".

U istom članu definicija pojma "informaciona bezbednost" je data veoma neprecizno, pa čak i netačno.

Deo da "informaciona bezbednost znači izvesnost da će IK sistem zaštititi tajnost, integritet, raspoloživost, autentičnost i neporecivost podataka kojima se rukuje putem tog sistema i da će taj sistem funkcionisati kako je predviđeno, kada je predviđeno i pod kontrolom ovlašćenih lica" je potpuno neadekvatna, jer informaciona bezbednost nikako ne može da znači izvesnost. Dalje, deo koji u definiciju uvodi i IK sistem i njegovo funkcionisanje je apsolutno nepotreban u definiciji pojma informacione bezbednosti jer postavlja fokus na IK sistem, a ne na zaštitu informacija i informacionih sistema od nekih nedozvoljenih radnji.

Uobičajena definicija informacione bezbednosti se oslanja na tri ključna principa (tzv. CIA triada) u vezi informacija, odnosno podataka : poverljivost (ili u našem dokumentu - tajnost, odn. Confidentiality), integritet (od. Integrity) i dostupnost (ili u našem dokumentu - raspoloživost, odn. Avialability).

Jedna od često korišćenih definicija se može naći na sajtu Legal Information Institute (Cornell University Law School) i uključena je u United States Code Definitions, a u prevedenom i izmenjenom obliku se koristi i u hrvatskom Zakonu o informacionoj sigurnosti iz 2007. godine, glasi:

(1) The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(C) availability, which means ensuring timely and reliable access to and use of information.

Definicija iz hrvatskog zakona:

Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda.

Iz teksta nije sasvim jasno sledeće:

Ko obavlja klasifikaciju podataka, ko dodeljuje sertifikate za pristup, kako se vrši zaštita neklasifikovanih podataka, planiranje rada u vanrednim situacijama, plan kontinuiteta poslovanja, edukacija i stručno usavršavanje i sertifikacija u vezi informacione bezbednosti, edukacija u vezi svesti o bezbednosti, procedure za postupanje u vezi incidenata, mere zaštite u oblasti poslovne saradnje, upravljanje rizikom informacione bezbednosti, nadzor mera i standarda u vezi informacione bezbednosti.

Od ukupno 26 stranica Predloga zakona Akreditaciji IK (predlažem ovu skraćenicu umesto IKT) sistema je posvećeno 6 stranica, Agenciji za KB i KEMZ 3 stranice, Akademskoj mreži Republike Srbije 6 stranica, državnoj komunikacionoj mreži pola stranice, a upravljanju rizikom samo jedan pasus.

Spominje se i Računarska mreža republičkih organa, a o njoj nisu dati nikakvi podaci. Pominju se i dva CERT-a, CERT republičkih organa i nacionalni CERT - Da li su potrebna dva? U vezi Inspekcije za informacionu bezbednost, između ostalih nejasnih činjenica nije jasno koliko ima inspektora.

Nigde se ne spominju usklađivanja sa međunarodnim standardima i preporukama, mere i standardi informacione bezbednosti su samo veoma površno dotaknuti, kao i oblasti informacione bezbednosti.

Smatram da bi zaista bilo potrebno da se produži rok.

Za bilo koje dodatne informacije stojim Vam na raspolaganju.

S poštovanjem,

Milan Vlahović CISSP, PMP

Rukovodilac sektora za informatiku,

Privredna komora Beograda