KOMENTARI CETIN doo Beograd, Novi Beograd

Nacrt pravilnika o opštoj metodologiji za procenu rizika u informaciono-komunikacionim sistemima od posebnog značaja

I. Opšti komentari i sugestije

Imajući u vidu član 11, stav 4., član 54. stav 1 i član 55. stav 4. Zakona o informacionoj bezbednosti, predlaže mo da dokument ne bude podzakonski akt, već smernice o opštoj metodologiji za procenu rizika u informaci ono-komunikacionim sistemima od posebnog značaja.

Obrazloženje:

Odredbom člana 11. stav 4. Zakona o informacionoj bezbednosti ("Službeni glasnik RS", broj 91/25, u daljem tekstu: ZIB), propisano je da se akt o proceni rizika izrađuje u skladu sa opštom metodologijom za procenu rizika u prioritetnim i važnim IKT sistemima od posebnog značaja koju donosi organ, odnosno organizacija u kojoj se obavljaju poslovi Nacionalnog CERT-a. Odredbom člana 54. stav 1 ZIB propisuje obavezu donošenja podzakonskih akata u roku od 12 meseci od donošenja ZIB, dok je odredbom člana 55. stav 4. definisana obaveza Nacionalnog CERT-a da u roku od devet meseci od dana stupanja na snagu ZIB, donese opštu metodologiju za procenu rizika u IKT sistemima od posebnog značaja.

Ukazujemo da ne postoji ovlašćujuća odredba za donošenje pravilnika, odnosno da ZIB-om nije izričito dato ovlašćenje Regulatornom telu za elektronske komunikacije i poštanske usluge, kao organizaciji u kojoj se obavljaju poslovi Nacionalnog CERT-a, da ovu materiju uredi podzakonskim aktom.

Pravilnik kao podzakonski akt ima obavezujući normativni karakter i može se donositi samo kada postoji jasan i izričit zakonski osnov, dok smernice služe za stručno usmeravanje, pojašnjenje i ujednačenu primenu zakona bez stvaranja novih obaveznih pravila. U prilog prethodno navedenom, i sam nacrt akta koristi izraze "preporučuje se" više puta.

U tom smislu, smatramo da su smernice pogodniji instrument jer omogućavaju fleksibilnost, praktičnu primenu i brže prilagođavanje tehničkim i organizacionim promenama u oblasti informacione bezbednosti. Time se istovremeno čuva pravna sigurnost, izbegava prekoračenje zakonskog ovlašćenja i obezbeđuje dosledna primena zakona u praksi.

Ukoliko bi predmetna materija bila uređena pravilnikom, to bi moglo dovesti do toga da nadzor nad svim IKT sistemima zahteva primenu ove metodologije u punom obimu, odnosno izradu analize rizika za sve elemente i na isti način kako je to predviđeno metodologijom, što bi u praksi bilo teško ostvarivo. U nacrtu pravilnika je izabrana metoda procene rizika zasnovane na sistemima, dok nisu opisane, odnosno predviđene metode procene rizika zasnovane na procesima i zasnovane na scenarijima. Smatramo da metode koje nisu obrađene u nacrtu pravilnika ne treba isključiti, jer će u određenim slučajevima biti prigodnije za izradu akta o proceni rizika.

II. **Pojedinačni članovi**

1. **Predlog**

Relevantni članovi: 4.1.1 Opis sistema i 4.1.2. Opis informacionih sistema

Predlog izmene: Brisanje delova 4. 1.1. Opis sistema i 4.1.2. Opis informacionih sistema

Obrazloženje (opis problema): Smatramo da navedeni delovi nisu u funkciji procene rizika, a izrada njihovog opisa (koji uključuje definisanje obima procene, uključenih komponenti i ograničenja u okviru kojih se procena sprovodi) bi predstavljao izuzetno velik administrativni posao koji najčešće neće imati dovoljan nivo tačnosti. Takođe predlažemo da ovi delovi ne budu sastavni deo Akta o proceni rizika, jer smatramo da je za potrebe Akta o proceni rizika dovoljno pobrojati sisteme, navesti vlasnike i nivo kritičnosti. Ovi podaci treba da postoje na nivou sistema nezavisno od procesa procene rizika.

---

2. **Predlog**

Relevantni član: 4.4. Analiza rizika – rangiranje i vrednovanje

Predlog izmene: Predlažemo da se termin „verovatnoća događanja“ zameni terminom „verovatnoća materijalizacije rizika“ ili „verovatnoća ostvarenja rizika“, zato što su ovi izrazi precizniji i stručno pravilniji u kontekstu upravljanja rizicima.

Obrazloženje (opis problema): Termin „verovatnoća događanja“ je previše opšti i može se odnositi na bilo koji događaj, dok u analizi rizika nije svako događanje relevantno, već samo ono koje vodi ka nastanku štetne posledice. Nasuprot tome, „verovatnoća materijalizacije rizika“ jasno ukazuje na mogućnost da se identifikovana pretnja ili neželjeni scenario stvarno ostvari, što bolje odražava suštinu procene rizika.

Takođe, termin „verovatnoća ostvarenja rizika“ je u skladu sa uobičajenom terminologijom koja se koristi u oblasti informacione bezbednosti, upravljanja rizicima i kontrole poslovnih procesa. Na taj način se obezbeđuje veća terminološka doslednost, jasnije tumačenje propisa i preciznija primena u praksi.

---

3. **Predlog**

Relevantni član: 4.5.5. Komuniciranje rizika

Predlog izmene: Predlažemo da se nivo rizika ne vezuje za rok realizacije na način kako je navedeno, već da za svaki identifikovani rizik postoji posebna odluka o načinu njegovog adresiranja, u kojoj će biti definisan i rok za realizaciju te odluke.

Obrazloženje (opis problema) : Crveni nivo rizika ne mora nužno da povlači automatsko ili hitno tretiranje rizika, jer su obim štete, verovatnoća ostvarivanja i posledice specifične za svaki pojedinačni slučaj. Upravljanje rizicima zahteva procenat prihvatljivog nivoa rizika, kapacitete organa i dostupne resurse, pa je opravdano da se rok za realizaciju mera ne određuje apriorno na osnovu samo nivoa rizika, već u okviru konkretnog odlučivanja o načinu adresiranja rizika. Time se osigurava racionalna i proporcionalna raspodela sredstava i pravovremeno, ali ne nužno hitno, rešavanje svakog rizika.