Komentari SHARE Fondacije na Nacrt zakona o informacionoj bezbednosti

Uvod

Donošenje novog Zakona o informacionoj bezbednosti je značajno za Republiku Srbiju iz više razloga i u vezi sa tim pozdravljamo inicijativu za unapređenjem ovog propisa. Inicijalna intencija izrade i usvajanja novog zakona, kako je navedeno u obrazloženju uz Nacrt zakona, jeste usklađivanje sa okvirom Evropske unije (EU) u oblasti informacione bezbednosti, tj. Direktivom 2022/2555 (NIS2 direktiva) i Uredbom 2019/881 (Akt o sajber bezbednosti). Međutim, fokus ne bi trebalo da bude samo nominalno usklađivanje sa EU propisima, već da se pored toga građanima omogući bezbednije digitalno okruženje, kao i da se osigura da svi ključni IKT sistemi u Republici Srbiji budu adekvatno spremni da odgovore na bezbednosne incidente i izazove.

Prethodnih godina svedočili smo bezbednosnim incidentima velikih razmera koji su pogodili javne IKT sisteme, kao što su ransomver napadi na novosadsko javno preduzeće Informatika i Republički geodetski zavod, a koji su ostali bez epiloga u pogledu utvrđivanja odgovornosti, pa možemo reći i pouka u pogledu prevencije i efikasnije mitigacije takvih incidenata. Incident koji je u toku pandemije COVID-19 kao kritičnog događaja uznemirio javnost bilo je objavljivanje pristupnih kredencijala za Informacioni sistem COVID-19 na javnoj stranici jedne zdravstvene ustanove, koje je SHARE Fondacija otkrila sasvim slučajno, tokom pretrage propisa usvojenih u cilju borbe protiv pandemije. Reakcija nadležnih organa na incident bila je efikasna, ali je ovaj propust pokazao nedovoljnu svest o rizicima i praktične implikacije nedovoljnih kapaciteta u sferi informacione bezbednosti. U medijima su se nedavno pojavili i navodi da se pristup službenim mejlovima državnih organa može ostvariti kupovinom kredencijala na *dark web* sajtovima.

Javna rasprava jeste dobra prilika da operatori IKT sistema od posebnog značaja, javne institucije, posebni CERT-ovi, stručna javnost i ostali zainteresovani akteri kroz razmenu mišljenja i informacija prilagode konačni tekst zakona, kako bi se u što potpunijoj formi koja realistično može da podigne nivo informacione bezbednosti našao pred narodnim poslanicima.

Transparentnost

Razumljivo je da određene informacije ne mogu javno dostupne, ali nacrtom zakona nije dovoljno izražen potencijal za transparentnost kada je reč o ovoj veoma važnoj društvenoj oblasti. Recimo,

član 9 Nacrta zakona predviđa da je Evidencija operatora IKT sistema od posebnog značaja tajni podatak u skladu sa zakonom kojim se uređuje tajnost podataka, koja se tako nalazi u režimu veoma osetljivih podataka jedne države, gde su sa druge strane posebni uslovi za njihovo pristupanje itd. U tom smislu, možemo postaviti pitanje da li je opravdano da kompletna Evidencija bude tajna, umesto samo konkretnih tehničkih podataka o IKT sistemima od posebnog značaja (npr. opsezi IP adresa) koji se mogu zloupotrebiti za njihovu enumeraciju i eventualne tehničke napade.

Takođe, kada je reč o obaveštavanju javnosti o incidentima, član 13, stav 6 Nacrta predviđa da Nacionalni CERT može uz konsultaciju sa operatorom IKT sistema objaviti informacije o incidentu "kada je neophodno da javnost bude upoznata sa incidentom ili kada je incident takav da je od interesa za javnost". Smatramo da bi bilo efektnije da se ova odredba precizira i više prilagodi tekstu iz NIS2 direktive (član 23) koji predviđa obaveštavanje javnosti u slučaju gde je "neophodna svest javnosti da bi se reagovalo na aktivan značajni incident", "kako bi se značajni incident sprečio" ili "ako je objavljivanje informacija o značajnom incidentu na drugi način u javnom interesu". Nacrtom bi moglo da se podstakne proaktivno objavljivanje *post mortem* analiza incidenta, bez otkrivanja osetljivih tehničkih informacija o samom IKT sistemu, koja bi sadržala informacije od značaja za druge IKT sisteme zarad prevencije budućih incidenata: indikatore kompromitacije, uočene taktike i tehnike napadača, savete za zaštitu od sličnih napada i mitigaciju i tome slično. Baza ranjivosti koja je predviđena da se uspostavi članom 27 Nacrta jeste dobar primer razmene informacija i transparentnosti, ali je Nacrt ipak predvideo da ona bude na dobrovoljnoj bazi.

Osnivanje Kancelarije za informacionu bezbednost (KIB) u okviru koje će biti i Nacionalni CERT otvara pitanja u vezi sa mogućnošću političkog uticaja, transparentnošću rada KIB i obezbeđivanjem dovoljno stručnog kadra za adekvatan nivo kapaciteta. U pogledu unapređenja transparentnosti, moguće je predvideti obavezu da KIB objavljuje detaljan godišnji izveštaj o radu koji bi uključivao statističke podatke, ali i detaljne tehničke analize najznačajnijih incidenata, bez navođenja odgovornosti i konkretnog IKT sistema od posebnog značaja gde se incident dogodio. Ovo bi omogućilo praćenje trendova na duži rok kada je reč o incidentima, kako na sektorskom, tako i nacionalnom nivou.

Član 19 Nacrta zakona predviđa da Kancelarijom za informacionu bezbednost rukovodi direktor, koga imenuje Vlada. Kao uslov navedeno je da lice koje se imenuje za direktora mora biti lice "odgovarajuće stručnosti" sa radnim iskustvom od najmanje 5 godina na poslovima rukovođenja. Imajući u vidu kompleksnost zaduženja i širok spektar nadležnosti KIB, kao i sve naprednije izazove sa kojima se suočavamo u digitalnom okruženju, smatramo da je od izuzetne važnosti da se

zakonom propiše da imenovano lice dodatno poseduje znanja, iskustvo i kompetencije u oblasti bezbednosti informacionih tehnologija.

Takođe, članom 21, st. 1, tač. 7 Nacrta zakona predviđeno je da Kancelarija u okviru njene nadležnosti "u saradnji sa nadležnim organima učestvuje u razvoju i sprovođenju programa obuka i stručnog usavršavanja lica koja rade na poslovima informacione bezbednosti u organima". Smatramo da bi reči "u saradnji sa nadležnim organima" trebalo isključiti iz navedene tačke, imajući u vidu značaj saradnje sa svim zainteresovanim akterima na edukaciji i podizanju nivoa znanja, pre svega civilnim sektorom i akademskom zajednicom. Član 28 Nacrta koji se bavi zaštitom dece pri korišćenju IKT predviđa jedinstveno mesto za pružanje saveta i prijem prijava u vezi bezbednosti dece na internetu, gde je navedeno da se podaci o licima koja podnose prijave čuvaju u rokovima predviđenim propisima koji uređuju kancelarijsko poslovanje. Kako kancelarijsko poslovanje uređuju podzakonski akti, napominjemo da se pitanja obrade i zaštite podataka o ličnosti moraju urediti zakonom, te da bi navedenu odredbu trebalo preformulisati na način da se ne poziva na akte niže pravne snage.

Nadzor nad sprovođenjem zakona

Izazovi i problemi sa primenom važećeg Zakona o informacionoj bezbednosti imaju pre svega sistemske korene. Usvajanje novog zakona neće u velikoj meri uticati da se postigne viši nivo primene odredbi dok se sistemski i strateški dugoročno ne adresiraju prepreke u opštem društvenom kontekstu. Iskustva iz zaštite podataka o ličnosti kao srodne oblasti nam govore da postupci utvrđivanja prekršajne odgovornosti za incidente, pa čak i najveće povrede poput slučaja Agencije za privatizaciju, gotovo po pravilu zastarevaju, dok izrečene kazne i mere ne deluju dovoljno odvraćajuće kako bi se među obveznicima zakona i građanima podigla svest o rizicima i odgovornosti za poštovanje zakona. Kada je reč o sankcijama za informacionu bezbednost, za sada nema javno poznatih slučajeva da je određeni entitet prekršajno kažnjen za kršenje odredbi zakona, a sva je prilika da je takvih situacija bilo, imajući u vidu potencijalni broj IKT sistema od posebnog značaja na teritoriji Republike Srbije.

Iako su članom 38 Nacrta inspektorima dodeljena tri dodatna ovlašćenja, što je veoma značajno, sedam godina od usvajanja prvog zakona broj inspektora za informacionu bezbednosti je i dalje nedovoljan i nedopustivo mali, što se donekle može razumeti usled ograničenih kapaciteta i resursa (nalaženje, zapošljavanje i zadržavanje dovoljno stručnog kadra) i internih procedura u javnom sektoru. Mera koja bi Kancelariji omogućila da ima širu sliku stanja od starta bila bi obaveza da operatori IKT sistema od posebnog značaja Kancelariji dostavljaju akte o bezbednosti

i akte o proceni rizika, što bi takođe ministarstvu kao nadležnom organu omogućilo da efikasnije sprovodi inspekcijski nadzor.

Dugoročno gledano, zakonom bi trebalo omogućiti da se slično odredbama NIS2 direktive (članovi 32 i 33) koje se odnose na mere nadzora nad operatorima IKT sistema od posebnog značaja usvoje mere koje bi potencijalno doprinele da obveznici imaju povećanu svest o sprovođenju nadzora. U zavisnosti od kapaciteta i resursa ministarstva kao nadležnog organa, te mere mogu biti terenske posete, nasumične kontrole, redovne bezbednosne revizije sistema, *ad hoc* revizije sistema i tome slično.

Zaključak

Nacrt zakona bi u trenutnoj formi u značajnoj meri približio pravni okvir Republike Srbije standardima Evropske unije, što je naročito važno imajući u vidu koliko se oblast informacione bezbednosti brzo razvija. Ipak, ono što je od strateškog značaja jeste da se unaprede kapaciteti ministarstva kao nadležnog organa, Kancelarije za informacionu bezbednost i Nacionalnog CERT-a, kao i svih drugih javnih institucija u čiju nadležnost makar i delimično spadaju poslovi zaštite informacione bezbednosti.

Ovim putem takođe pozivamo Ministarstvo informisanja i telekomunikacija da sa Ministarstvom pravde pokrene konsultacije o izmenama Zakona o prekršajima, kako bi se kroz izuzetke propisale više kazne za kršenje Zakona o informacionoj bezbednosti. Najviša kazna propisana Nacrtom zakona je 2.000.000 dinara, što jeste maksimum određen Zakonom o prekršajima, ali iz pozicije velikih korporativnih sistema koji posluju u Srbiji to nije iznos koji će delovati odvraćajuće na operatore i navesti ih da ulože resurse u adekvatnu primenu mera zaštite i drugih obaveza propisanih zakonom.

U tom smislu, trenutna verzija zakona, iako otvorena za unapređenja, predstavlja značajnu polaznu tačku i omogućava Republici Srbiji da ide u korak sa globalno naprednim standardima zaštite informacione bezbednosti. Predložene mere se mogu dodatno unaprediti najviše kroz povećanu transparentnost prema svim zainteresovanim akterima i široj javnosti, kao i mogućnost za efikasnije sprovođenje nadzora, bez čega ne možemo da očekujemo stvarno unapređenje stanja informacione bezbednosti.

Beograd,
30. avgust 2023.

SHARE Fondacija
Kapetan Mišina 6a, 11000 Beograd, Srbija
www.sharefoundation.info | info@sharedefense.org