Komentari na Nacrt prijedloga Zakona o kibernetičkoj sigurnosti

Zagreb, studeni 2023.

AmCham

American Chamber of Commerce in Croatia Američka gospodarska komora u Hrvatskoj

Uvod

Uz izrazito snažnu digitalnu transformaciju svih sfera naših života, a posebice digitalizacije poslovanja i upravljanja javnim institucijama, kibernetička sigurnost nadmašila je točku "reputacijske i financijske" odgovornosti i postala ključna odrednica sigurnosti. U današnje vrijeme kibernetička sigurnost predstavlja strateško pitanje funkcioniranja, ne samo poslovnih subjekata i državnih institucija, već i našeg načina života.

Američka gospodarska komora u Hrvatskoj (AmCham) prepoznaje važnost kibernetičke sigurnosti i pozdravlja nastojanja Europske unije i Hrvatske da ažurira postojeće zakonodavstvo i odgovori na brojne izazove.

AmCham pozdravlja napore Hrvatske u dijelu transponiranja Direktive o mjerama za visoku zajedničku razinu kibersigurnosti diljem Unije (Direktiva NIS2) u nacionalno zakonodavstvo.

Direktiva NIS2 (Direktiva EU2022/2555) je zakonodavstvo o kibernetičkoj sigurnosti unutar i na nivou Europske unije kroz koju se postavlja pravni okvir za povećanje ukupne razine sigurnosti EU. Direktivom se na razini država članica potiče međusobna suradnja na polju kibernetičke sigurnosti, potiče opremanje država članica odgovarajućom tehnologijom, timovima i nacionalnim tijelima koji prate i utječu na brzinu, kvalitetu i odgovor na računalne sigurnosne incidente. Također, potiče se razvoj kulture kibernetičke sigurnosti kroz sve svoje ekonomske sektore koji su bitni za gospodarstvo pojedine članice ali i cijele Europske unije.

Poduzeća koja su države članice utvrdile kao bitne i ključne morat će biti dio sustava koji će blisko surađivati sa nacionalnim tijelima za provedbu Direktive.

U tom kontekstu je nastao i Prijedlog Zakona o kibernetičkoj sigurnosti kao dio transponiranja NIS2 Direktive (Direktiva EU2022/2555) u nacionalno zakonodavstvo.

Komentar na Zakon

AmCham smatra da će Zakon o kibernetičkoj sigurnosti imati značajan utjecaj na hrvatsko gospodarstvo i institucije. Stoga je od posebne važnosti da se otklone sve potencijalne nejasnoće definicija i pojmova te izbjegnu pravne nesigurnosti u vidu implementacije Zakona. Najavljeno je i donošenje popratne Uredbe kojom bi trebalo pobliže definirati pojedinosti i otkloniti sve nedoumice. S obzirom na važnost navedenog zakonodavstva i utjecaja koji će imati na poslovni sektor ali i opću državu AmCham smatra kako bi u postupku donošenja Uredbe bilo potrebno da se kao članove radne skupine uključi i određeni broj neovisnih stručnjaka za kibernetičku sigurnost, kao i poduzetnika čije je poslovanje značajno povezano sa i koje će biti pogođeno stupanjem na snagu Zakona i donošenjem povezane Uredbe.

Uloga Sigurnosno-obavještajne agencije i ustrojstvo Nacionalnog centara za kibernetičku sigurnost

Člankom 63. predviđeno je osnivanje Nacionalnog centra za kibernetičku sigurnost (NCKS) unutar Sigurnosno-obavještajne agencije (SOA) te su ujedno poslovi Nadležnog tijela za provedbu zahtjeva kibernetičke sigurnosti (tj. SOA za enumerirane sektore u Prilogu III prijedloga Zakona) i poslovi Središnjeg državnog tijela za kibernetičku sigurnost preneseni na NCKS. Daljnjim pregledom zakona, a posebice provedbenog dijela u čl. 114. proizlazi da će NCKS biti organiziran kao interna ustrojbena jedinica SOA-e te kao takav neće imati posebnu osobnost niti formalnopravnu razdvojenost od SOA-e.

Vezano uz navedeno, ukazujemo na predloženo rješenje da se NCKS u Prilogu III Prijedloga Zakona navodi kao nadležni CSIRT za pojedine sektore, dok se istovremeno za veći dio istih sektora kao Nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti navodi Središnje državno tijelo za kibernetičku sigurnost, odnosno, SOA. U konkretnom se slučaju postavlja pitanje s kojim bi tijelom i na koji način bi trebao komunicirati pojedini subjekt-obveznik Zakona? Hoće li se formalna komunikacija sa NCKS ujedno smatrati komunikacijom sa SOA-om u ulozi Središnjeg državnog tijela za kibernetičku sigurnost i hoće li se komunikacija sa Središnjem državnim tijelom za kibernetičku sigurnost smatrati i obavještavanjem NCKS kao CSIRT-a? Napominjemo da su uzete u obzir odredbe čl. 37. i 38. prijedloga Zakona, no i navedenih odredaba se samo postavljaju dodatna pitanja jer se proceduralna pitanja obavještavanja nadležnih tijela planiraju tehnički i pravno-proceduralno urediti u budućnosti, dok se istovremeno prijedlogom Zakona (čl. 101. i 102.) predviđaju izrazito teške sankcije za subjekte, kao i za odgovorne osobe u subjektima.

Predmetnim se zakonodavnim rješenjem kod adresata zakona proizvodi nesigurnost i nejasnoća vezano uz tijelo ili tijela s kojima je adresat obvezan komunicirati, kao i

koje nadležnosti i ovlasti iz Zakona izvršava SOA, a koje NCKS kao nominalno (ali ne i pravno-formalno) zasebno tijelo.

Ukoliko je namjera zakonodavca da ustanovi NCKS kao zasebno i izdvojeno tijelo sa vlastitim ovlastima različitim od SOA-e, predlaže se pogodnije rješenje u vidu izdvajanja NCKS kao zasebnog tijela unutar sigurnosno-obavještajnog sustava po uzoru na Zavod za sigurnost informacijskih sustava. S druge strane, ako bi zakonodavac inzistirao na predloženom rješenju NCKS kao sastavnog dijela SOA-e, svakako se predlaže dodatno i jasnije uređenje međusobnog odnosa i koordinacije između NCKS i SOA-e u kontekstu Zakona o kibernetičkoj sigurnosti, a posebice u odnosu na jasnije uređenje odnosa između zakonom obuhvaćenih subjekata i NCKS/SOA-e kada se radi o sektorima gdje su navedeni kao nadležni CSIRT i nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti.

Usvajanje i implementacija Zakona o kibernetičkoj sigurnosti

Pored spomenute NIS2 Direktive na nivou EU trenutačno postoji cijeli set propisa koji predstavljaju novi zakonodavni okvir za informacijsku sigurnost i zaštitu kritičnih entiteta na razini EU. Neki su od tih propisa već stupili na snagu te će ih biti potrebno transponirati u zakonodavstvo Republike Hrvatske (CER direktiva) dok su neki propisi već izravno primjenjivi u Republici Hrvatskoj (CSA uredba i DORA uredba). Nadalje, važno je i istaknuti CRA (Cyber Resilience Act) uredbu, koja je u postupku donošenja a koja će se nadovezivati na okvir postavljen NIS2 direktivom u dijelu koji se odnosi na pitanja certificiranja i zaštite lanca dobave u odnosu na digitalne proizvode i proizvode s digitalnim komponentama.

Budući da je rok za transponiranje CER direktive isti kao i za NIS2 direktivu (listopad 2024. godine) te da se radi o srodnim propisima koji se međusobno nadovezuju i nadopunjuju, smatramo da postoji potreba da se dodatno i nedvosmisleno utvrdi međusobni odnos između provedbenog propisa NIS2 direktive (Zakon) i budućeg provedbenog propisa CER direktive. Navedeno je posebno bitno da se izbjegnu međusobna nepodudaranja ili proturječnosti, a posebice iz razloga što je stručni nositelj implementacije CER direktive (MUP) različit od stručnog nositelja implementacije NIS2 direktive (Ministarstvo hrvatskih branitelja).

U odnosu na spomenutu CRA uredbu, za očekivati je da će konačni tekst navedene uredbe koji se očekuje tijekom sljedeće godine imati utjecaja i na provedbu i implementaciju Zakona o kibernetičkoj sigurnosti sa aspekta pitanja certifikacije IKT proizvoda, usluga i sustava, kao i pitanja osiguravanja dobavnih lanaca entiteta obuhvaćenih Zakonom o kibernetičkoj sigurnosti. Budući da nije sigurno kada bi CRA uredba trebala stupiti na snagu, odnosno, da postoji vjerojatnost da će se pitanja certifikacija IKT proizvoda, usluga i sustava i utvrđivanja jedinstvenih sigurnosnih standarda sukcesivno uređivati tijekom sljedećih godina sukladno donošenju novih

propisa (CRA uredba) i utvrđivanja sigurnosnih shema EU za IKT proizvode, usluge i sustave, smatramo da bi do trenutka donošenja CRA uredbe i shema EU za IKT proizvode, usluge i sustave bilo uputno da se Zakonom, provedbenom Uredbom ili drugim podzakonskim aktima ili ekvivalentnim propisima (Zakon o provedbi kibernetičke sigurnosne certifikacije) nedvosmisleno urede kriteriji i standardi (ISO ili slični) koji bi služili kao stabilna osnova za implementaciju tehničkih i organizacijskih mjera od strane budućih obveznika Zakona.

Za dodatne informacije molimo kontaktirajte:
Američka gospodarska komora u Hrvatskoj
Andrea Doko Jelušić,
Izvršna direktorica T: 01 4836 777
E: andrea.doko@amcham.hr