WAHL

LAW FIRM

Kibernetička sigurnost u Republici Hrvatskoj: izazovi implementacije

7. studeni 2025. I Legal Alerts br. 25. I Usklađenost, korporativne istrage i krizno upravljanje

U digitaliziranom društvu, gdje su državne institucije, gospodarstvo i svakodnevni život građana u velikoj mjeri oslonjeni na digitalne tehnologije, pitanje kibernetičke sigurnosti postaje prioritet. Kibernetička sigurnost više nije isključiva odgovornost IT sektora – ona je zajednička briga svih sektora društva. Svaki pojedinac, institucija i organizacija, bez obzira na djelatnost, ima ulogu u očuvanju digitalne sigurnosti. Suradnja između tehničkih stručnjaka, upravljačkih struktura, obrazovnih ustanova i zakonodavnih tijela ključna je za stvaranje otpornog i sigurnog digitalnog okruženja.

Pojam kibernetičke sigurnosti i zašto je važna?

Ponedjeljak je ujutro. Upravo ste stigli na posao i pokušavate ući u aplikaciju svoje banke kako biste provjerili stanje na računu – no aplikacija ne radi. Pokušavate platiti kavu karticom – na POS uređaju piše da je plaćanje odbijeno. Pokušate kontaktirati korisničku podršku banke – nitko se ne javlja. Ubrzo se šire vijesti da je došlo do velikog kibernetičkog napada i da su bankarski sustavi hakirani, podaci kompromitirani, a transakcije blokirane.

Nešto što je prošlih desetljeća bilo rezervirano za futurističke romane, sad je već stvarnost. Sve češći hakerski napadi na ključne infrastrukture dovode u pitanje enormne razmjere potencijalnih negativnih posljedica digitalnog i globaliziranog društva.

U eri potpune ovisnost društva o ICT tehnologiji i značajnoj količini povjerljivih osobnih podataka na platformama poput digitalnih *one stop shopova* kao što su e-Građani ili e-Porezna – kibernetička sigurnost mora postati prioritet kako zakonodavca tako i nas koji te tehnologije svakodnevno koristimo.

Kibernetička sigurnost može se definirati kao skup aktivnosti (procesa, mjera i standarda) osmišljenih za zaštitu računalnih sustava, mreža, programa i podataka od neovlaštenog pristupa, napada, oštećenja ili krađe[1].

Njena svrha nije samo tehnička zaštita infrastrukture nego i očuvanje povjerenja građana i gospodarstva u digitalne usluge.

Zakonodavni okvir u Republici Hrvatskoj

U svrhu usklađenja s europskim standardima, Republika Hrvatska je implementirala Direktivu (EU) 2022/2025 od 14. prosinca 2022. godine (poznatija pod nazivom NIS 2 Direktiva) kojom se uspostavlja viša razina kibernetičke

[1] https://mpudt.gov.hr/kiberneticka-sigurnost/28695?lang=hr

sigurnosti unutar Europske unije. Direktiva NIS 2 implementirana je u hrvatsko zakonodavstvo Zakonom o kibernetičkoj sigurnosti ("Narodne novine" br. 14/24.) koji je stupio na snagu 15. veljače 2024. godine.

Zakon o kibernetičkoj sigurnosti uređuje obveze i mjere koje moraju provoditi subjekti iz javnog i privatnog sektora kako bi zaštitili svoje informacijske sustave od kibernetičkih prijetnji. Navedeni zakon obuhvaća širi krug organizacija, uključujući ključne i važne subjekte iz područja energetike, zdravstva, prometa, financija, digitalnih usluga i drugih sektora.

Zakon o kibernetičkoj sigurnosti propisuje obvezu provođenja:

- procjene rizika,
- uspostave sigurnosnih politika,
- imenovanja odgovornih osoba za kibernetičku sigurnost te
- izvještavanja o ozbiljnim incidentima.

Također je važno napomenuti da je Vlada Republike Hrvatske 21. studenog 2024. godine, na temelju članka 24. Zakona o kibernetičkoj sigurnosti, usvojila Uredbu o kibernetičkoj sigurnosti („Narodne novine“, br. 14/24.).

Uredba o kibernetičkoj sigurnosti propisuje kriterije za razvrstavanje subjekata prema posebnim parametrima radi njihove kategorizacije, definira mjere za upravljanje rizicima u području kibernetičke sigurnosti te način njihove primjene. Također, uređuje postupak provedbe samoprocjene kibernetičke sigurnosti, određuje uvjete za prepoznavanje značajnih kibernetičkih incidenata, način prijave tih incidenata, kao i ostale aspekte ključne za unaprjeđenje ukupne razine kibernetičke sigurnosti.

Važan dio regulatornog okvira kibernetičke sigurnosti u Republici Hrvatskoj predstavlja i Nacionalni program upravljanja kibernetičkim krizama koji je usvojen 9. svibnja 2025. godine.

Nacionalni program upravljanja kibernetičkim krizama predstavlja podzakonski akt Zakona o kibernetičkoj sigurnosti kojim se uspostavlja sveobuhvatan sustav odgovora na kibernetičke krize u Republici Hrvatskoj. Program definira ciljeve, kapacitete, resurse i postupke za učinkovito upravljanje krizama u skladu s europskim okvirom.

Razlike NIS 2 Direktive i Zakona o kibernetičkoj sigurnosti

Iako je Zakon o kibernetičkoj sigurnosti u velikoj mjeri usklađen s europskim okvirom, ipak uvodi i dodatne obveze koje nadilaze zahtjeve NIS 2 Direktive. Primjerice, Zakon o kibernetičkoj sigurnosti precizira obvezu samoprocjene kibernetičke sigurnosti za važne subjekte, koja se mora provoditi najmanje svake dvije godine, dok NIS 2 Direktiva takvu obvezu ne propisuje izričito. Također, Zakon o kibernetičkoj sigurnosti detaljnije definira nadzorne mehanizme, uključujući obvezu revizije kibernetičke sigurnosti za ključne subjekte najmanje jednom svake dvije godine te nadzor svakih 3 do 5 godina.

U pogledu obuhvata, Zakon o kibernetičkoj sigurnosti zadržava kriterije iz NIS 2 Direktive, ali s dodatnim naglaskom na subjekte registrirane u Republici Hrvatskoj. Izuzetak su pružatelji javnih elektroničkih komunikacijskih mreža i usluga, koji podliježu Zakonu o kibernetičkoj sigurnosti samo ako pružaju usluge u Republici Hrvatskoj, bez obzira na mjesto registracije. Zakon o kibernetičkoj sigurnosti također propisuje da nadležno tijelo obavještava ključne i važne subjekte najkasnije do veljače 2025. godine, a oni su dužni uskladiti se u roku od jedne godine od te obavijesti.

Što se tiče kazni, Zakon o kibernetičkoj sigurnosti predviđa strože sankcije u odnosu na NIS 2 Direktivu.

Kazne za ključne subjekte se kreću:

- između 10.000 i 10.000.000 eura ili između 0,5% i 2% godišnjeg prometa, ovisno o tome što je veće.
- Za članove višeg menadžmenta, kazne iznose između 1.000 i 6.000 eura.

Kazne za važne subjekte kreću se:

- između 5.000 i 7.000.000 eura ili između 0,2% i 1,4% godišnjeg prometa,
- dok su kazne za članove višeg menadžmenta između 500 i 3.000 eura.

Tko su ključni, a tko važni subjekti?

Prema Zakonu o kibernetičkoj sigurnosti, subjekti se dijele na ključne i važne – ključni su, primjerice, bolnice, energetske tvrtke i banke, dok su važni pružatelji digitalnih usluga ili logističke tvrtke. Kategorije se određuju prema vrsti, veličini ili djelatnosti i utjecaju, dok se zapravo glavna razlika temelji na potencijalnom utjecaju incidenta na društvo, gospodarstvo i nacionalnu sigurnost.

Izazovi implementacije NIS 2 Direktive

Svaka implementacija nosi za sobom određene izazove i nedostatke u provedbi te provedba NIS 2 Direktive nije ništa drugačija. Izazovi koje bismo posebno izdvojili su:

- *Financijski i organizacijski izazovi za mala i srednja poduzeća*
- *Nacionalna infrastruktura na hrvatskom jeziku*
- *Ishođenje vjerodajnica za prijavu*

Financijski i organizacijski izazovi za mala i srednja poduzeća

Usvajanje Zakona o kibernetičkoj sigurnosti nameće brojne obveze organizacijama, uključujući imenovanje odgovornih osoba, izradu procjene rizika, planove za incidente, IT revizije i edukaciju zaposlenika, kao i ulaganja u tehničku zaštitu.

Posebno su pogođena mala i srednja poduzeća, koja se suočavaju s manjkom stručnjaka i financijskih resursa. Iako nemaju kapacitete velikih subjekata, sve su češće meta kibernetičkih napada zbog slabije zaštite. Stoga je nužno da zakonodavne mjere prate konkretna podrška, edukacija i financijska pomoć kako bi i manji subjekti mogli ispuniti zakonske zahtjeve i povećati otpornost svojih sustava.

Nacionalna infrastruktura na hrvatskom jeziku

Uspostavom nacionalne platforme za prijavu kibernetičkih incidenata, Zakon o kibernetičkoj sigurnosti propisuje dvije ključne uloge: administratora i korisnika platforme. Administrator mora biti zaposlenik društva, pristupati putem ePoslovanja i upravljati ovlaštenjima putem eOvlaštenja, dok je korisnik platforme zadužen za prijavu incidenata, a može biti zaposlenik društva ili vanjskog pružatelja povezanih usluga.

Problem nastaje kada su direktor ili zaposlenici subjekta stranci koji ne govore hrvatski, jer je platforma dostupna isključivo na hrvatskom jeziku. U današnjem digitalnom okruženju, direktori imaju ključnu ulogu u osiguravanju spremnosti svojih organizacija na kibernetičke prijetnje. Iako Zakon o kibernetičkoj sigurnosti ne zabranjuje da stranci obnašaju ove uloge, zbog jezične barijere teško mogu izvršavati zakonske obveze, što povećava rizik od novčanih kazni.

Sigurnosno-obavještajna agencija (SOA) potvrdila je da je problem prepoznat i učestao, te da se radi na rješenju, uključujući i moguće uvođenje engleskog jezika u platformu.

Ishođenje vjerodajnica za prijavu

Jedan od sve izraženijih praktičnih problema u primjeni Zakona o kibernetičkoj sigurnosti odnosi se na ishođenje vjerodajnica za pristup nacionalnim digitalnim sustavima poput e-Ovlaštenja, e-Građani, NIAS i Pixi. Premda tehničke prirode, ovaj problem ozbiljno otežava

pristup sustavima, osobito za strane državljane u upravljačkim funkcijama u hrvatskim tvrtkama.

Za pristup je potrebno imati hrvatske vjerodajnice (e-osobna iskaznica, mToken hrvatske banke, FINA certifikat), koje strani državljani bez prebivališta u Republici Hrvatskoj uglavnom ne mogu pribaviti. Time im je onemogućeno formalno preuzimanje ovlasti i provedba zakonski propisanih mjera. Dodatno, činjenica da su svi sustavi dostupni isključivo na hrvatskom jeziku predstavlja dodatnu prepreku.

U kontekstu sve većeg udjela stranih investitora i međunarodnog kadra, ovaj nedostatak predstavlja ozbiljan sustavni izazov. Hitno je potrebno razmotriti izmjene zakonskog okvira, omogućavanje alternativnih metoda autentifikacije i uvođenje višejezične podrške, kako bi se osigurala zakonita i učinkovita provedba obveza i za organizacije s međunarodnim kadrom.

Rokovi određeni Zakonom o kibernetičkoj sigurnosti

Zakonom o kibernetičkoj sigurnosti jasno su definirane ključne vremenske točke koje obvezni subjekti moraju poštovati.

Prva obveza odnosi se na inicijalnu kategorizaciju subjekata, koja je morala biti izvršena do 4. travnja 2025. godine. Nakon toga slijedi rok za obavijest o kategorizaciji, koju nadležno tijelo dostavlja subjektima najkasnije do 5. svibnja 2025. godine.

Nakon primitka obavijesti o kategorizaciji, subjekti su dužni u roku od 30 dana uspostaviti sustav izvještavanja o incidentima putem nacionalne platforme te prijavljivati incidente nacionalnim CSIRT-ovima (Computer Security Incident Response Team).

Subjekti zatim imaju godinu dana od primitka obavijesti o kategorizaciji da izvrše inicijalnu provedbu mjera Zakona o kibernetičkoj sigurnosti, što konkretno znači do 4. travnja 2026. godine.

Zakon o kibernetičkoj sigurnosti također predviđa unaprjeđenje mjera kroz upravljanje rizikom u subjektima, prvu samoprocjenu za važne subjekte odnosno reviziju za ključne subjekte. Samoprocjena odnosno revizija se provodi jednom u dvije godine, a prva mora biti provedena do 4. travnja 2028. godine.

Nadalje, Zakon o kibernetičkoj sigurnosti propisuje obvezu redovitog provođenja stručnih nadzora nadležnih tijela, koji se moraju provoditi najmanje jednom u roku od tri do pet godina.

Ovi rokovi ukazuju na strogo strukturiran plan implementacije mjera kibernetičke sigurnosti, koji zahtijeva pravodobnu pripremu i aktivno upravljanje obvezama od strane svih subjekata. Neispunjavanje ovih rokova može imati ozbiljne posljedice, uključujući novčane kazne i regulatorne sankcije. Stoga je iznimno važno da subjekti već sada počnu s pripremama kako bi ispunili sve zakonske obveze unutar predviđenih rokova.

Ključne vremenske točke:

- *Prijava kategorizacije subjekata: do 4. travnja 2025. (dostava obavijest od strane nadležnog tijela do 5. svibnja 2025.)*
- *Godinu dana od primitka obavijesti od kategorizaciji – obveza izvršenja inicijalne provedbe mjera (što bi značilo do 4. travnja 2026.)*

Statistika inicijalne kategorizacije u Republici Hrvatskoj

U sklopu provedbe Zakona o kibernetičkoj sigurnosti, provedena je inicijalna kategorizacija subjekata u Republici Hrvatskoj koja predstavlja temelj za daljnju implementaciju mjera i obveza predviđenih zakonskim okvirom.

Prema dostupnim statističkim podacima, kategorizacija je obuhvatila ukupno 702

subjekta, od čega je 140 identificirano kao ključni subjekti, a 562 kao važni subjekti. Ova kategorizacija obuhvaća čak 41 sektor, podsektor i vrstu subjekta, što ukazuje na široki zahvat Zakona o kibernetičkoj sigurnosti u različite sfere gospodarstva i javnog sektora.

Poseban dio kategorizacije odnosi se na 28 registara hrvatskih internetskih domena, koji su ovlašteni od strane CARNET TLD-a. Iako nisu izravno obuhvaćeni Zakonom o kibernetičkoj sigurnosti, njihova je zadaća dostavljati podatke u registar posebnih subjekata, čime posredno pridonose sustavu kibernetičke sigurnosti.

Promjene u registru kategoriziranih subjekata očekuju se i u budućnosti, i to na dva načina – trajno i jednokratno.

Trajne promjene odnose se na manji broj novih kategorizacija ili dekategorizacija, najčešće uslijed zakonskih promjena, širenja poslovanja ili preuzimanja, dok se jednokratne promjene očekuju do kraja 2025. godine i odnose se uglavnom na male subjekte iz sektora upravljanja IKT uslugama.

Ovi podaci ukazuju na to da je Republika Hrvatska pristupila implementaciji Zakona o kibernetičkoj sigurnosti sustavno i sveobuhvatno, uzimajući u obzir složenost digitalnog okruženja i raznolikost aktera. Inicijalna kategorizacija stoga čini ključan korak prema učinkovitijem upravljanju rizicima i boljoj otpornosti na kibernetičke prijetnje. Sustavno ažuriranje registra i aktivno uključivanje dodatnih subjekata osigurat će da zakon prati tehnološki razvoj i promjene u poslovnom i institucionalnom okruženju.

Zaključak

Jasno je da kibernetička sigurnost u digitaliziranom društvu postaje ključni stup stabilnosti, otpornosti i povjerenja građana, poduzeća i institucija u digitalne usluge. Više nije riječ isključivo o tehničkom pitanju koje se tiče isključivo IT stručnjaka, već o strateškom izazovu koji zahtijeva angažman svih sudionika društva – od zakonodavaca, menadžmenta i operativnih timova, do krajnjih korisnika.

Implementacijom Zakona o kibernetičkoj sigurnosti i usklađenjem s NIS 2 Direktivom, Hrvatska je napravila značajan korak prema sustavnom pristupu zaštiti digitalne infrastrukture, pri čemu su jasno definirani zahtjevi, rokovi i sankcije za nepoštivanje obveza.

Međutim, uz normativni napredak, pred Republikom Hrvatskom stoje i brojni izazovi praktične provedbe, osobito u kontekstu jezičnih barijera, tehničke pristupačnosti i ograničenih resursa kod manjih subjekata. Da bi zakonodavni okvir bio djelotvoran, ključno je osigurati provedivu infrastrukturu, ciljanu edukaciju, te kontinuiranu podršku subjektima koji su uključeni u sustav kibernetičke sigurnosti. Samo uz takav pristup moguće je ostvariti glavni cilj – stvaranje sigurnog i otpornog digitalnog okruženja koje može odgovoriti na sve sofisticiranije kibernetičke prijetnje današnjice.

Samo sinergijom države, privatnog sektora i stručne zajednice moguće je izgraditi sigurnu digitalnu budućnost.

Kontakt:

Neven Marić
+385 1/5629-767
n.maric@wahl.hr

Matea Miljuš Beranek
+385 1/6535 327
m.miljus-beranek@wahl.hr

** U pripremi publikacije je sudjelovala i odvjetnička vježbenica Valentina Štih.*