EUROPSKA
KOMISIJA

Bruxelles, 4.10.2017.
COM(2017) 476 final

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU I VIJEĆU

Optimalno iskorištavanje potencijala Direktive NIS – prema učinkovitoj provedbi Direktive (EU) 2016/1148 o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije

HR

Uvod

Direktiva (EU) 2016/1148 o sigurnosti mrežnih i informacijskih sustava širom Unije[1] (dalje u tekstu: „Direktiva NIS ” ili „Direktiva”), donesena 6. srpnja 2016., prvi je horizontalni zakonodavni akt EU-a u području kibersigurnosnih izazova i istinska prekretnica kad je riječ o kibersigurnosnoj otpornosti i suradnji u Europi.

Direktiva ima tri glavna cilja:

- poboljšanje nacionalnih sposobnosti u području kibersigurnosti;
- uspostava suradnje na razini EU-a; i
- promicanje kulture upravljanja rizikom i izvješćivanja o incidentima među ključnim gospodarskim subjektima, prije svega operatorima ključnih usluga za održavanje gospodarskih i društvenih aktivnosti i pružatelja digitalnih usluga.

Direktiva NIS kamen je temeljac EU-ova odgovora na sve brojnije kiberprijetnje i kiberizazove koji su posljedica digitalizacije gospodarskog i društvenog života te je njezina provedba stoga ključan dio paketa za kibersigurnost predstavljenog 13. rujna 2017. Učinkovitost EU-ova odgovora bit će ograničena sve dok se Direktiva NIS u potpunosti ne prenese u zakonodavstvo svih država članica EU-a. Da je to kritična točka prepoznato je i u Komisijinoj Komunikaciji o jačanju europskog sustava kibernetičke sigurnosti[2] iz 2016.

Novìna Direktive NIS i potreba za hitnim rješavanjem problema sve dinamičnijeg razvoja kiberprijetnji zahtijevaju da se posebna pozornost posveti izazovima s kojima se suočavaju svi akteri pri osiguravanju pravovremenog i uspješnog prenošenja Direktive. S obzirom na to da je rok za prenošenje 9. svibnja 2018., a rok za identifikaciju operatora ključnih usluga 9. studenoga 2018., Komisija podupire postupak prenošenja u državama članicama, kao i njihove s tim povezane aktivnosti u skupini za suradnju.

Ova Komunikacija i njezin Prilog temelje se na Komisijinu pripremnom radu i analizi povezanima s dosadašnjom provedbom Direktive NIS, na mišljenju Europske agencije za mrežnu i informacijsku sigurnost (ENISA) i raspravama s državama članicama u fazi prenošenja Direktive, prije svega u okviru skupine za suradnju [3]. Komunikacijom se dopunjuju znatni napori koji su do sada uloženi, prije svega zahvaljujući:

- intenzivnom radu skupine za suradnju, koja se usuglasila oko plana rada usmjerenog uglavnom na prenošenje Direktive NIS, posebno na pitanje identifikacije operatora ključnih usluga i utvrđivanje njihovih obveza u pogledu sigurnosnih zahtjeva i obavješćivanja o incidentima. Iako je Direktivom predviđeno diskrecijsko pravo pri

[1] Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije. Direktiva je stupila na snagu 8. kolovoza 2016.
[2] COM(2016) 410 final.
[3] Mehanizam za stratešku suradnju država članica u skladu s člankom 11. Direktive NIS.

prenošenju odredaba koje se odnose na operatore ključnih usluga, države članice prepoznale su važnost usklađenog pristupa u tom području[4].

- uspostavi i brzom funkcioniranju mreže timova za odgovor na računalne sigurnosne incidente (CSIRT-ovi) u skladu s člankom 12. stavkom 1. Direktive. Mreža otada radi na uspostavi temelja za strukturiranu operativnu suradnju na europskoj razini.

Da bi se ostvario cilj visoke zajedničke razine sigurnosti mrežnih i informacijskih sustava u Uniji, ključna je potpuna angažiranost svih država članica i na razini politike i na operativnoj razini koje te dvije strukture predstavljaju.

Ovom Komunikacijom i njezinim Prilogom ti će se napori pojačati zahvaljujući prikupljanju i usporedbi najbolje prakse iz država članica relevantne za provedbu Direktive, pružanju smjernica o načinu provedbe Direktive te iscrpnijim objašnjenjima pojedinih odredaba. Sveukupni cilj jest poduprijeti države članice u učinkovitoj i usklađenoj provedbi Direktive NIS u EU-u.

Komunikaciju će dodatno dopuniti skora Provedbena uredba Komisije o dodatnom utvrđivanju elemenata i parametara povezanih sa zahtjevima za sigurnost i obavješćivanje o incidentima za pružatelje digitalnih usluga, u skladu s članom 16. stavkom 8. Direktive NIS. Provedbenom uredbom olakšat će se provedba Direktive u pogledu obveza pružatelja digitalnih usluga[5].

U Komunikaciji se iznose ključni zaključci analize pitanja koja se smatraju važnim referentnim točkama i potencijalnim izvorom nadahnuća s aspekta prenošenja u nacionalno zakonodavstvo. Naglasak se u prvom redu stavlja na odredbe koje se odnose na sposobnost i obveze država članica u pogledu subjekata koji su obuhvaćeni područjem primjene Direktive. U Prilogu se iscrpnije analiziraju područja za koja Komisija smatra da pružanje praktičnih smjernica za prenošenje, u obliku objašnjenja i njezina tumačenja određenih odredaba Direktive te primjera najbolje prakse i dosad stečenog iskustva s Direktivom, ima najveću vrijednost.

Prema učinkovitoj provedbi Direktive NIS

Direktivom NIS želi se ostvariti visoka zajednička razina sigurnosti mrežnih i informacijskih sustava unutar EU-a. To znači poboljšanje sigurnosti interneta i privatnih mreža, kao i informacijskih sustava na kojima se temelji funkcioniranje našeg društva i gospodarstva. Prvi važan element u tom pogledu jest pripravnost država članica, koju bi trebalo osigurati utvrđivanjem nacionalnih strategija za kibersigurnost u skladu s Direktivom, te radom CSIRT-ova i nadležnih nacionalnih tijela.

[4] Skupina za suradnju trenutačno radi na referentnim smjernicama kojima će među ostalim biti obuhvaćeno sljedeće: kriteriji za definiranje ključne uloge operatora u skladu s člankom 5. stavkom 2. Direktive; okolnosti u kojima su operatori ključnih usluga dužni obavijestiti o incidentu u skladu s člankom 14. stavkom 7. Direktive; i sigurnosni zahtjevi za operatore ključnih usluga, u skladu s člankom 14. stavcima 1. i 2.

[5] Nacrt Provedbene uredbe dostupan je za javno savjetovanje na adresi https://ec.europa.eu/info/law/better-regulation/have-your-say_en

Sveobuhvatnost nacionalnih strategija

Važno je da države članice prenošenje Direktive NIS u nacionalno zakonodavstvo iskoriste za preispitivanje nacionalne strategije za kibersigurnost uzimajući u obzir nedostatke, najbolje prakse i nove izazove koji su navedeni u Prilogu.

Razumljivo je da je Direktiva usmjerena na poduzeća i usluge od posebne ključne važnosti, no s obzirom na to da se sve više oslanjamo na IKT, potreban je holistički i dosljedan pristup pitanju kibersigurnosti gospodarstva i društva u cjelini. Stoga bi se donošenjem sveobuhvatnih nacionalnih strategija koje nadilaze minimalne zahtjeve propisane Direktivom NIS (npr. proširenje i na sektore i usluge koji nisu navedeni u Prilogu II. odnosno Prilogu III. Direktivi) povećala opća razina sigurnosti mrežnih i informacijskih sustava.

Budući da je kibersigurnost još uvijek relativno novo područje javne politike koje se snažno razvija, u mnogim slučajevima potrebna su nova ulaganja, čak i ako opće stanje javnih financija zahtijeva rezove i uštede. Stoga je donošenje ambicioznih odluka kojima se osiguravaju primjereni financijski i ljudski resursi neophodni za učinkovitu provedbu nacionalnih strategija, uključujući dostatne resurse za nacionalna nadležna tijela i CSIRT-ove, od ključne važnosti za postizanje ciljeva Direktive.

Učinkovitost provedbe i izvršenja

Obveza imenovanja nacionalnih nadležnih tijela i jedinstvenih kontaktnih točaka utvrđena je u članku 8. Direktive i ključan je element za osiguravanje učinkovite provedbe Direktive NIS i prekogranične suradnje. U tom pogledu postoje u većoj mjeri centralizirani i decentralizirani pristupi u državama članica. Ako države članice u pogledu imenovanja nacionalnih nadležnih tijela donesu pristup koji je u većoj mjeri decentraliziran, ključnim se pokazalo osiguravanje snažnih mehanizama suradnje između brojnih tijela i jedinstvene kontaktne točke (*vidjeti Tablicu 1. odjeljka 3.2. Priloga*). Time se povećava učinkovitost provedbe i olakšava izvršenje.

Oslanjanje na prethodno iskustvo u području zaštite kritične informacijske infrastrukture može pomoći u oblikovanju optimalnog modela upravljanja u državama članicama, kojim bi se osigurala i učinkovita sektorska provedba Direktive NIS i usklađeni horizontalni pristup (*vidjeti odjeljak 3.1. Priloga*).

Unaprijeđene sposobnosti nacionalnih CSIRT-ova

Ako se unutar EU-a ne osnuju učinkoviti nacionalni CSIRT-ovi s odgovarajućim resursima kako je utvrđeno u članku 9. Direktive NIS, EU će i dalje biti previše izložen prekograničnim kiberprijetnjama. Zato bi države članice trebale razmotriti proširenje opsega djelovanja CSIRT-ova i na sektore i usluge koji nisu uključeni u područje primjene Direktive (*vidjeti*

odjeljak 3.3. Priloga). Tako bi nacionalni CSIRT-ovi mogli pružati operativnu pomoć u slučaju kiberincidenata u poduzećima i organizacijama koji nisu obuhvaćeni područjem primjene Direktive, a važni su za društvo i gospodarstvo. Nadalje, države članice mogle bi u potpunosti iskoristiti dodatne mogućnosti financiranja u okviru programa kibersigurnosti infrastrukture digitalnih usluga (DSI) Instrumenta za povezivanje Europe, koji je namijenjen unaprjeđenju sposobnosti i suradnje nacionalnih CSIRT-ova (*vidjeti odjeljak 3.5. Priloga*).

Dosljednost postupka identifikacije operatora ključnih usluga

U skladu s člankom 5. Direktive NIS države članice dužne su do 9. studenoga 2018. identificirati subjekte koji će se smatrati operatorima ključnih usluga. U tom pogledu države članice mogu razmotriti mogućnost da se dosljednom primjenom definicija i smjernica iz ove Komunikacije osigura da slična vrsta subjekata koji imaju sličnu ulogu na unutarnjem tržištu budu dosljedno identificirani kao operatori ključnih usluga u drugim državama članicama. Države članice mogu razmotriti i mogućnost proširenja područja primjene Direktive NIS na javne uprave, s obzirom na njihovu ulogu u cjelokupnom društvu i gospodarstvu (*vidjeti odjeljke 2.1. i 4.1.3. Priloga*).

Maksimalno usklađivanje nacionalnih pristupa u području identifikacije operatora ključnih usluga, prije svega primjenom smjernica koje je razradila skupina za suradnju (*vidjeti odjeljak 4.1.2. Priloga*), bilo bi veoma korisno jer bi dovelo do usklađene primjene odredaba Direktive, a time i manjeg rizika od fragmentacije tržišta. U slučaju operatora ključnih usluga koji ključne usluge pružaju u dvije države članice ili više njih, neophodno je nastojati postići dogovor država članica u kontekstu postupka savjetovanja iz članka 5. stavka 4. o dosljednoj identifikaciji subjekata (*vidjeti odjeljak 4.1.7. Priloga*) jer će se tako izbjeći da isti subjekt u jurisdikcijama različitih država članica podliježe različitom regulatornom tretmanu.

Podnošenje informacija o identifikaciji operatora ključnih usluga Komisiji

U skladu s člankom 5. stavkom 7. države članice dužne su dostaviti Komisiji informacije o nacionalnim mjerama za identifikaciju operatora ključnih usluga, popis ključnih usluga, broj identificiranih operatora ključnih usluga i relevantnost tih operatora za sektor. Nadalje, države članice dužne su dostaviti pragove, ako postoje, upotrijebljene u postupku identifikacije za određivanje odgovarajuće razine opskrbe ili važnosti određenog operatora za održavanje dostatne razine opskrbe. Države članice mogu razmotriti i mogućnost dostavljanja popisa identificiranih operatora ključnih usluga Komisiji, po potrebi na povjerljivoj osnovi, jer bi se time pridonijelo poboljšanju točnosti i kvalitete Komisijine ocjene (*vidjeti odjeljke 4.1.5. i 4.1.6. Priloga*).

Usklađeni pristupi u pogledu zahtjeva za sigurnost i obavješćivanje o incidentima za operatore ključnih usluga

Kad je riječ o obvezama operatora ključnih usluga koje se odnose na sigurnosne zahtjeve i obavješćivanje o incidentima (članak 14. stavci 1., 2. i 3.), učinak jedinstvenog tržišta u najvećoj bi se mjeri potaknuo usklađenim pristupom u području sigurnosnih zahtjeva i obavješćivanja o incidentima kojim bi se olakšalo prekogranično usklađivanje operatora

ključnih usluga u državama članicama EU-a. U tom kontekstu referentan je i dalje rad na smjernicama skupine za suradnju (*vidjeti odjeljke 4.2. i 4.3. Priloga*).

U slučaju kiberincidenata velikih razmjera koji pogađaju nekoliko država članica vrlo je vjerojatno da obvezne obavijesti o incidentima podnosi operator ključnih usluga ili pružatelj digitalnih usluga u skladu s člankom 14. stavkom 3. i člankom 16. stavkom 3. ili drugi subjekt koji nije obuhvaćen područjem primjene Direktive na dobrovoljnoj osnovi u skladu s člankom 20. stavkom 1. U skladu s Preporukom Komisije o koordiniranom odgovoru na kiberincidentne i kiberkrize velikih razmjera države članice mogu razmotriti mogućnost usklađivanja svojih nacionalnih pristupa kako bi u što kraćem roku na temelju tih obavijesti mogle pružiti relevantne informacije nadležnim tijelima ili CSIRT-ovima drugih uključenih država članica. Točne i korisne informacije ključne su za smanjenje broja virusa i za uklanjanje slabih točaka prije nego što budu zlouporabljene.

U duhu partnerstva pri nastojanju da se Direktiva NIS iskoristi na najbolji način, Komisija namjerava proširiti potporu u okviru Instrumenta za povezivanje Europe na sve relevantne dionike na koje se odnosi to zakonodavstvo. Iako je naglasak do sada bio na izgradnji kapaciteta CSIRT-ova i na uspostavi platforme za brzu i učinkovitu operativnu suradnju, odnosno na jačanju mreže CSIRT-ova, Komisija će sada istražiti kako se financijska sredstva iz Instrumenta za povezivanje mogu upotrijebiti i u korist nacionalnih nadležnih tijela, kao i operatora ključnih usluga i pružatelja digitalnih usluga.

Zaključak

S obzirom na to da je rok za prenošenje Direktive NIS u nacionalno zakonodavstvo 9. svibnja 2018., a rok za identifikaciju operatora ključnih usluga 9. studenoga 2018., države članice trebale bi poduzeti odgovarajuće mjere kako bi odredbe Direktive NIS i njome predviđeni modeli suradnje mogli osigurati najbolje moguće alate na razini EU-a za postizanje visoke zajedničke razine sigurnosti mrežnih i informacijskih sustava u Uniji. Komisija poziva države članice da u tom postupku razmotre relevantne informacije, smjernice i preporuke iz ove Komunikacije.

Ovu Komunikaciju mogu dodatno dopuniti druge mjere, uključujući one koje proizađu iz tekućeg rada skupine za suradnju.