EVROPSKA
KOMISIJA

Bruselj, 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

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU IN SVETU

Kako kar najbolje izkoristiti direktivo o varnosti omrežij in informacij – za učinkovito izvajanje Direktive (EU) 2016/1148 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji

SL

Uvod

Direktiva (EU) 2016/1148 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji[1] (v nadaljnjem besedilu: direktiva o varnosti omrežij in informacij ali Direktiva), sprejeta 6. julija 2016, je prvi horizontalni zakonodajni akt EU, ki obravnava izzive na področju kibernetske varnosti ter pomeni resnično prelomnico za kibernetsko odpornost in sodelovanje v Evropi.

Ima tri glavne cilje:

- izboljšanje nacionalnih zmogljivosti na področju kibernetske varnosti,
- krepitev sodelovanja na ravni EU in
- spodbujanje kulture obvladovanja tveganj in poročanja o incidentih med ključnimi gospodarskimi akterji, zlasti izvajalci, ki opravljajo bistvene storitve za vzdrževanje gospodarskih in družbenih dejavnosti, in ponudniki digitalnih storitev.

Direktiva o varnosti omrežij in informacij je temelj odziva EU na vse pogostejše kibernetske grožnje in izzive, ki spremljajo digitalizacijo našega gospodarstva in družbe, zato je njeno izvajanje ključni del svežnja o kibernetski varnosti, ki je bil predstavljen 13. septembra 2017. Učinkovitost odziva na ravni Unije bo omejena, dokler vse države članice EU ne bodo v celoti prenesle direktive o varnosti omrežij in informacij v svojo zakonodajo. To je bilo tudi priznano kot ključno v sporočilu Komisije iz leta 2016 o krepitvi odpornosti evropskega sistema kibernetske varnosti[2].

Zaradi novosti, ki jo pomeni direktiva o varnosti omrežij in informacij, ter nujnosti reševanja hitro spreminjajočih se kibernetskih groženj je treba posebno pozornost nameniti izzivom, s katerimi se spopadajo vsi akterji, ko želijo zagotoviti pravočasen in uspešen prenos Direktive. Glede na to, da je rok za prenos Direktive 9. maj 2018, rok za določitev izvajalcev bistvenih storitev pa 9. november 2018, Komisija podpira države članice pri prenosu Direktive in njihovo delo v skupini za sodelovanje v ta namen.

To sporočilo s prilogo temelji na pripravljalnem delu in analizi Komisije v zvezi z dosedanjim izvajanjem direktive o varnosti omrežij in informacij, na prispevku Evropske agencije za varnost omrežij in informacij (ENISA) in na razpravah z državami članicami v fazi prenosa Direktive, predvsem v okviru skupine za sodelovanje[3]. To sporočilo dopolnjuje znatna dosedanja prizadevanja, zlasti z:

- intenzivnim delom skupine za sodelovanje, ki se je dogovorila o delovnem načrtu, ki je usmerjen predvsem v prenos direktive o varnosti omrežij in informacij, zlasti v določitev izvajalcev bistvenih storitev ter njihovih obveznosti glede varnostnih zahtev in priglasitve incidentov. Medtem ko Direktiva državam članicam podeljuje

[1] Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji. Direktiva je začela veljati 8. avgusta 2016.
[2] COM(2016) 410 final.
[3] Mehanizem za strateško sodelovanje med državami članicami na podlagi direktive o varnosti omrežij in informacij (člen 11).

diskrecijsko pravico pri prenosu določb v zvezi z izvajalci bistvenih storitev, države članice priznavajo pomen usklajenega pristopa v tem oziru[4];

- vzpostavitvijo in hitrim delovanjem mreže, ki jo sestavljajo skupine za odzivanje na incidente na področju računalniške varnosti (skupine CSIRT), v skladu s členom 12(1) Direktive. Ta mreža je začela postavljati temelje za strukturirano operativno sodelovanje na evropski ravni.

Tako za raven oblikovanja politike kot tudi za operativno raven, ki ju predstavljata ti dve strukturi, je polno sodelovanje vseh držav članic bistveno za doseganje cilja visoke skupne ravni varnosti omrežij in informacijskih sistemov v Uniji.

To sporočilo s prilogo ta prizadevanja še krepi, tako da združuje in primerja najboljše prakse iz držav članic, ki so pomembne za izvajanje Direktive, zagotavlja dodatne smernice o tem, kako naj bi se Direktiva izvajala, in podrobneje pojasnjuje nekatere določbe. Glavni cilj je podpreti države članice, da bi dosegle učinkovito in usklajeno izvajanje direktive o varnosti omrežij in informacij po vsej EU.

Sporočilo bo nadalje dopolnila prihodnja izvedbena uredba Komisije o podrobnejši opredelitvi elementov in parametrov, povezanih z varnostnimi zahtevami in priglasitvijo incidentov za ponudnike digitalnih storitev, v skladu s členom 16(8) direktive o varnosti omrežij in informacij. Izvedbena uredba bo olajšala izvajanje Direktive v zvezi z obveznostmi glede ponudnikov digitalnih storitev[5].

V sporočilu so predstavljene ključne ugotovitve analize vprašanj, ki veljajo za pomembne referenčne točke in morebitni navdih z vidika prenosa Direktive v nacionalno zakonodajo. V ospredju so določbe o zmogljivostih in obveznostih držav članic glede subjektov, ki spadajo na področje uporabe Direktive. Priloga vsebuje podrobnejši pregled področij, za katera Komisija meni, da imajo največjo vrednost pri zagotavljanju praktičnih smernic za prenos z razlago in interpretacijo nekaterih določb Direktive ter predstavitvijo najboljših praks in doslej pridobljenih izkušenj z izvajanjem Direktive.

Za učinkovito izvajanje direktive o varnosti omrežij in informacij

Cilj direktive o varnosti omrežij in informacij je doseči visoko skupno raven varnosti omrežij in informacijskih sistemov v EU. To pomeni izboljšati varnost interneta ter zasebnih omrežij in informacijskih sistemov, na katerih temelji delovanje naše družbe in gospodarstva. Prvi pomemben element v tem oziru je pripravljenost držav članic, ki bi morala biti zagotovljena s sprejetjem nacionalnih strategij za kibernetsko varnost, kot je opisano v Direktivi, ter z delom skupin CSIRT in pristojnih nacionalnih organov.

[4] Skupina za sodelovanje pripravlja referenčne smernice, med drugim glede: meril za opredelitev ključnosti izvajalca v skladu s členom 5(2) Direktive, okoliščin, v katerih morajo izvajalci bistvenih storitev priglasiti incidente na podlagi člena 14(7) Direktive, in varnostnih zahtev za izvajalce bistvenih storitev v skladu s členom 14(1) in (2) Direktive.

[5] Osnutek izvedbene uredbe je na voljo za javno posvetovanje na spletni strani https://ec.europa.eu/info/law/better-regulation/have-your-say_sl.

Celovitost nacionalnih strategij

Pomembno je, da države članice prenos direktive o varnosti omrežij in informacij izkoristijo za revizijo svojih nacionalnih strategij za kibernetsko varnost ter preučijo vrzeli, najboljše prakse in nove izzive, ki so obravnavani v Prilogi.

Čeprav se Direktiva razumljivo osredotoča na podjetja in storitve, ki so posebnega ključnega pomena, je treba glede na vse večjo odvisnost od informacijske in komunikacijske tehnologije kibernetsko varnost gospodarstva in družbe obravnavati na celovit in dosleden način. Zato bi sprejetje celovitih nacionalnih strategij, ki presegajo minimalne zahteve direktive o varnosti omrežij in informacij (zajemajo več kot sektorje in storitve, navedene v prilogah II in III k Direktivi), povečalo splošno raven varnosti omrežij in informacijskih sistemov.

Ker je kibernetska varnost razmeroma novo in hitro rastoče področje javne politike, so v večini primerov potrebne nove naložbe, tudi kadar splošno stanje javnih financ zapoveduje omejevanje odhodkov in prihranke. Za doseganje ciljev Direktive so zato nujne ambiciozne odločitve za zagotovitev ustreznih finančnih in človeških virov, ki so nujno potrebni za učinkovito izvajanje nacionalnih strategij, kar vključuje zadostne vire pristojnih nacionalnih organov in skupin CSIRT.

Učinkovito izvajanje in izvrševanje predpisov

Potreba po določitvi pristojnih nacionalnih organov in enotnih kontaktnih točk je določena v členu 8 Direktive ter je ključni element za zagotovitev učinkovitega izvajanja Direktive in čezmejnega sodelovanja. Države članice uporabljajo tako centralizirane kot tudi decentralizirane pristope. Če države članice sprejmejo bolj decentraliziran pristop glede določitve pristojnih nacionalnih organov, je nujno treba zagotoviti tesno sodelovanje med različnimi organi in enotno kontaktno točko (*glej preglednico 1 v oddelku 3.2 Priloge*). To bi povečalo učinkovitost izvajanja in olajšajo izvrševanje predpisov.

Pretekle izkušnje glede zaščite kritične informacijske infrastrukture lahko pripomorejo k oblikovanju optimalnega modela upravljanja za države članice, ki bi zagotovil tako učinkovito sektorsko izvajanje direktive o varnosti omrežij in informacij kot tudi skladen horizontalni pristop (*glej oddelek 3.1 Priloge*).

Okrepljene zmogljivosti nacionalnih skupin CSIRT

Brez učinkovitih nacionalnih skupin CSIRT po vsej EU, ki imajo na voljo ustrezne vire, kot je določeno v členu 9 direktive o varnosti omrežij in informacij, bo EU še vedno preveč ranljiva za čezmejne kibernetske grožnje. Države članice bi zato morale preučiti možnost razširitve pooblastil skupin CSIRT, tako da ne bi obsegala le sektorjev in storitev, ki so vključeni v področje uporabe Direktive (*glej oddelek 3.3 Priloge*). Tako bi nacionalne skupine CSIRT

lahko zagotovile operativno podporo reševanju kibernetskih incidentov, ki prizadenejo podjetja in organizacije, ki ne spadajo na področje uporabe Direktive, a so prav tako pomembni za družbo in gospodarstvo. Poleg tega bi države članice lahko v celoti izkoristile dodatne možnosti financiranja, ki jih ponuja program infrastrukture digitalnih storitev za kibernetsko varnost Instrumenta za povezovanje Evrope ter so namenjene krepitvi zmogljivosti nacionalnih skupin CSIRT in sodelovanja med njimi (*glej oddelek 3.5 Priloge*).

Doslednost postopka določitve izvajalcev bistvenih storitev

Države članice morajo v skladu s členom 5 direktive o varnosti omrežij in informacij do 9. novembra 2018 določiti subjekte, ki se bodo šteli za izvajalce bistvenih storitev. Države članice bi lahko glede te naloge preučile možnost dosledne uporabe opredelitev in smernic, vključenih v to sporočilo, da bi zagotovile, da so podobne vrste subjektov s podobno vlogo na notranjem trgu dosledno opredeljene kot izvajalci bistvenih storitev tudi v drugih državah članicah. Države članice bi lahko razmislile tudi o razširitvi področja uporabe direktive o varnosti omrežij in informacij na javne uprave glede na vlogo, ki jo imajo za celotno družbo in gospodarstvo (*glej oddelka 2.1 in 4.1.3 Priloge*).

Kar največja uskladitev nacionalnih pristopov k določitvi izvajalcev bistvenih storitev, predvsem z upoštevanjem smernic, ki jih pripravi skupina za sodelovanje (*glej oddelek 4.1.2 Priloge*), bi bila zelo zaželena, saj bi privedla do bolj usklajene uporabe določb Direktive in tako zmanjšala tveganje razdrobljenosti trga. Kadar izvajalci bistvenih storitev zagotavljajo bistvene storitve v dveh ali več državah članicah, si je nujno treba prizadevati za dosego sporazuma med državami članicami na podlagi posvetovanja v skladu s členom 5(4) o dosledni določitvi subjektov (*glej oddelek 4.1.7 Priloge*), saj se tako prepreči drugačna regulativna obravnava istega subjekta pod pristojnostjo različnih držav članic.

Predložitev informacij o določitvi izvajalcev bistvenih storitev Komisiji

Države članice morajo v skladu s členom 5(7) Komisiji predložiti informacije o nacionalnih ukrepih, ki omogočajo določitev izvajalcev bistvenih storitev, seznam bistvenih storitev, število določenih izvajalcev bistvenih storitev in pomen teh izvajalcev za zadevni sektor. Poleg tega morajo države članice sporočiti morebitne pragove za določitev ustrezne ravni opravljanja storitev ali pomen zadevnega izvajalca za vzdrževanje ustrezne ravni opravljanja storitev. Države članice bi prav tako lahko preučile možnost, da Komisiji sporočijo sezname določenih izvajalcev bistvenih storitev, po potrebi na podlagi zaupnosti, saj bi to pripomoglo k večji natančnosti in kakovosti ocene Komisije (*glej oddelka 4.1.5 in 4.1.6 Priloge*).
Usklajeni pristopi glede varnostnih zahtev in priglasitve incidentov za izvajalce bistvenih storitev

V zvezi z obveznostmi glede varnostnih zahtev in priglasitve incidentov za izvajalce bistvenih storitev (člen 14(1), (2) in (3)) bi usklajen pristop k varnostnim zahtevam in priglasitvi incidentov, namenjen temu, da bi izvajalci bistvenih storitev lažje izpolnjevali predpise v čezmejnem kontekstu znotraj EU, v največji možni meri spodbujal enotni trg. Na tem

področju bodo referenčni dokument smernice, ki jih pripravlja skupina za sodelovanje (*glej oddelka 4.2 in 4.3 Priloge*).

V primeru velikih kibernetskih incidentov, ki prizadenejo več držav članic, je zelo verjetno, da obvezno priglasitev incidenta predloži izvajalec bistvenih storitev ali ponudnik digitalnih storitev v skladu s členom 14(3) in členom 16(3) ali drug subjekt, ki ni vključen v področje uporabe Direktive, prostovoljno v skladu s členom 20(1). V skladu s Priporočilom Komisije o usklajenem odzivu na velike kibernetske incidente in krize bi države članice lahko preučile možnost uskladitve svojih nacionalnih pristopov, da bi tako lahko čim prej predložile ustrezne informacije na podlagi teh priglasitev pristojnim organom ali skupinam CSIRT drugih zadevnih držav članic. Natančne in konkretne informacije bi bile ključne za zmanjšanje števila okužb ali obravnavanje šibkih točk, preden se zlorabijo.

Komisija namerava v duhu partnerstva, da bi z direktivo o varnosti omrežij in informacij dosegli kar največ, razširiti podporo v okviru Instrumenta za povezovanje Evrope na vse zadevne zainteresirane strani v skladu s to zakonodajo. Medtem ko je bil poudarek na krepitvi zmogljivosti skupin CSIRT in platformi, ki omogoča hitro in učinkovito operativno sodelovanje, za krepitev mreže skupin CSIRT, bo Komisija zdaj preučila, kako lahko financiranje v okviru Instrumenta za povezovanje Evrope koristi tudi pristojnim nacionalnim organom ter izvajalcem bistvenih storitev in ponudnikom digitalnih storitev.

Sklep

Glede na bližajoči se rok za prenos direktive o varnosti omrežij in informacij v nacionalno zakonodajo (9. maj 2018) ter rok za določitev izvajalcev bistvenih storitev (9. november 2018) bi morale države članice sprejeti ustrezne ukrepe za zagotovitev, da lahko določbe in modeli sodelovanja iz direktive o varnosti omrežij in informacij zagotovijo najboljša možna orodja na ravni EU za doseganje visoke skupne ravni varnosti omrežij in informacijskih sistemov po vsej Uniji. Komisija poziva države članice, naj pri tem preučijo ustrezne informacije, smernice in priporočila, ki jih vsebuje to sporočilo.

Sporočilo lahko dopolnijo drugi ukrepi, tudi tisti, ki jih pri svojem delu sprejme skupina za sodelovanje.