EUROPSKA
KOMISIJA

Bruxelles, 4.10.2017.
COM(2017) 476 final

ANNEX 1

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

PRILOG

KOMUNIKACIJI KOMISIJE EUROPSKOM PARALMENTU 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

SADRŽAJ

PRILOG

1. Uvod

Cilj je ovog Priloga pridonijeti djelotvornoj primjeni, provedbi i izvršenju Direktive (EU) 2016/1148 o sigurnosti mrežnih i informacijskih sustava širom Unije[1] (dalje u tekstu: „Direktiva NIS" ili „Direktiva") i pomoći državama članicama da osiguraju djelotvornu primjenu prava EU-a. Konkretno, Prijedlog ima tri posebna cilja: (a) bolje objasniti nacionalnim tijelima obveze iz Direktive koje se na njih primjenjuju, (b) osigurati djelotvorno izvršenje obveza iz Direktive koje se primjenjuju na subjekte koji imaju obveze povezane sa sigurnosnim zahtjevima i obavješćivanjem o incidentima i (c) općenito pridonijeti stvaranju pravne sigurnosti za sve relevantne dionike.

U tu se svrhu u ovom Prilogu daju smjernice o sljedećim aspektima koji su od ključne važnosti za postizanje cilja Direktive NIS, odnosno za osiguranje visoke zajedničke razine sigurnosti mrežnih i informacijskih sustava u EU-u, na čemu se temelji funkcioniranje našeg društva i gospodarstva:

- obveza država članica da donesu nacionalnu strategiju o sigurnosti mrežnih i informacijskih sustava (odjeljak 2.),
- uspostava nacionalnih nadležnih tijela, jedinstvenih kontaktnih točaka i timova za odgovor na računalne sigurnosne incidente (odjeljak 3.),
- sigurnosni zahtjevi i zahtjevi za obavješćivanje o incidentima koji se primjenjuju na operatore ključnih usluga i pružatelje digitalnih usluga (odjeljak 4.) i
- odnos između Direktive NIS i drugih zakonodavnih akata (odjeljak 5.).

Komisija je izradila ove smjernice na temelju podataka i analize prikupljenih tijekom izrade Direktive, doprinosa Europske agencije za mrežnu i informacijsku sigurnost („ENISA") i skupine za suradnju. Iskoristila je i iskustva pojedinih država članica. Komisija je prema potrebi uzela u obzir vodeća načela za tumačenje prava EU-a: tekst, kontekst i ciljeve Direktive NIS. Budući da Direktiva nije prenesena u nacionalno zakonodavstvo, još nema presuda Suda Europske unije ili nacionalnih sudova. Stoga se sudska praksa ne može iskoristiti za smjernice.

Zahvaljujući objedinjenju tih informacija u jednom dokumentu države članice mogle bi dobiti dobar pregled Direktive i te informacije uzeti u obzir pri izradi svojeg nacionalnog zakonodavstva. Komisija također naglašava da ovaj Prilog nije obvezujući i da nije predviđeno da se njime stvaraju nova pravila. Sud EU-a ima konačnu nadležnost za tumačenje prava EU-a.

[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. Nacionalna strategija za sigurnost mrežnih i informacijskih sustava

U skladu s člankom 7. Direktive NIS države članice moraju donijeti nacionalnu strategiju za sigurnost mrežnih i informacijskih sustava koju se može smatrati jednakovrijednom nacionalnoj strategiji za kibersigurnost („NSK"). Nacionalnom strategijom definiraju se strateški ciljevi i odgovarajuće aktivnosti u području politike i regulatorne aktivnosti povezane s kibersigurnošću. Pojam nacionalna strategija za kibersigurnost upotrebljava se u međunarodnom kontekstu i u Europi, posebno u kontekstu suradnje ENISA-e i država članica na izradi nacionalnih strategija, zbog čega je nedavno ažuriran Vodič o dobroj praksi za nacionalne strategije za kibersigurnost[2].

U tom odjeljku Komisija opisuje kako se Direktivom NIS jača pripravnost država članica zahvaljujući zahtjevu za uspostavu čvrste nacionalne strategije o sigurnosti mrežnih i informacijskih sustava (članak 7.). Tim odjeljkom obuhvaćeni su sljedeći aspekti: (a) područje primjene strategije i (b) sadržaj i postupak donošenja.

Kako je opisano u nastavku, pravilno prenošenje članka 7. Direktive NIS od ključne je važnosti za ispunjenje ciljeva Direktive i u tu je svrhu nužno dodijeliti odgovarajuća financijska sredstva i ljudske resurse.

2.1. Područje primjene nacionalne strategije

U skladu s tekstom članka 7. obveza donošenja nacionalne strategije za kibersigurnost primjenjuje se samo na „sektore iz Priloga II. (tj. energetiku, prijevoz, bankarstvo, financijsko tržište, zdravstvo, opskrbu vodom za piće i njezinu distribuciju i digitalnu infrastrukturu) i na usluge navedene u Prilogu III." (internetsko tržište, internetsku tražilicu i usluge računalstva u oblaku).

Člankom 3. Direktive posebno je propisano načelo minimalnog usklađivanja u skladu s kojim države članice mogu donijeti ili zadržati odredbe čiji je cilj postizanje više razine sigurnosti mrežnih i informacijskih sustava. Primjenom tog načela na obvezu donošenja nacionalne strategije za kibersigurnost državama članicama se omogućuje da uključe više sektora i usluga od onih obuhvaćenih prilozima II. i III. Direktivi.

Prema mišljenju Komisije i s obzirom na cilj Direktive NIS, odnosno postizanje visoke zajedničke razine sigurnosti mrežnih i informacijskih sustava u Uniji[3], trebalo bi izraditi nacionalnu strategiju kojom su obuhvaćene sve relevantne dimenzije društva i gospodarstva, a ne samo sektori i digitalne usluge koji su obuhvaćeni prilozima II. i III. Direktivi NIS. To je u skladu s najboljom međunarodnom praksom (vidi smjernice ITU-a i analizu OECD-a dalje u tekstu) i s Direktivom NIS.

Kako je detaljnije objašnjeno u nastavku, to se posebno odnosi na javne uprave koje su odgovorne za sektore i usluge koji nisu navedeni u prilozima II. i III. Direktivi. Javne uprave

[2] ENISA, *Dobra praksa za nacionalne strategije za kibersigurnost*, 2016. Dostupno na https://www.enisa.europa.eu/publications/ncss-good-practice-guide

[3] Vidjeti članak 1. stavak 1.

mogu obrađivati osjetljive informacije, što opravdava njihovo uključivanje u nacionalnu strategiju za kibersigurnost i planove upravljanja kojima se sprječava neovlaštena objava i osigurava primjerena zaštita tih informacija.

2.2. Sadržaj i postupak donošenja nacionalnih strategija

U skladu s člankom 7. Direktive NIS nacionalna strategija za kibersigurnost treba uključivati barem sljedeće:

i) ciljeve i prioritete nacionalne strategije za sigurnost mrežnih i informacijskih sustava;
ii) upravljački okvir za postizanje ciljeva i prioriteta nacionalne strategije;
iii) opis mjera povezanih s pripravnošću, odgovorom i ponovnom uspostavom, uključujući mehanizme suradnje između javnog i privatnog sektora;
iv) popis programâ edukacije, podizanja razine svijesti i osposobljavanja;
v) popis istraživačkih i razvojnih planova;
vi) plan za procjenu rizika s ciljem prepoznavanja rizika; i
vii) popis različitih sudionika u provedbi strategije.

Ni u članku 7. ni u odgovarajućoj uvodnoj izjavi 29. nisu navedeni zahtjevi za donošenje nacionalne strategije za kibersigurnost niti je podrobnije određen sadržaj te strategije. Kada je riječ o postupku i dodatnim elementima povezanima sa sadržajem nacionalne strategije za kibersigurnost, Komisija smatra da je pristup opisan u nastavku prikladan za donošenje nacionalne strategije za kibersigurnost. To se temelji na analizi iskustava država članica i trećih zemalja u razvoju njihovih strategija. Dodatni izvor informacija jest ENISA-in alat za osposobljavanje za izradu nacionalnih strategija za kibersigurnost koji se sastoji od videozapisa i medija koji se mogu preuzeti na njezinu *web*-mjestu[4].

2.3. Postupak i pitanja koja je potrebno obuhvatiti

Postupak izrade i donošenja nacionalne strategije složen je i višedimenzionalan postupak čija učinkovitost i uspjeh ovise o kontinuiranom angažmanu stručnjaka za kibersigurnost, civilnog društva i nacionalnih političkih procesa. Od ključne je važnosti viša administrativna potpora barem na razini državnog tajnika ili jednakovrijednoj razini u nadležnom ministarstvu, kao i politička potpora. Za uspješno donošenje nacionalne strategije za kibersigurnost može se razmotriti sljedeći postupak od pet koraka (vidjeti grafikon 1.).

Prvi korak – **Utvrđivanje vodećih načela i strateških ciljeva koji proizlaze iz strategije**

Prvo, nacionalna nadležna tijela trebala bi definirati neke ključne elemente koji se moraju uključiti u nacionalnu strategiju za kibersigurnost, točnije željene rezultate ili kako se u Direktivi nazivaju (članak 7. stavak 1. točka (a)), „ciljeve i prioritete”, navesti kako se tim rezultatima dopunjavaju nacionalne socijalne i gospodarske politike i jesu li oni u skladu s povlasticama i obvezama koje proizlaze iz članstva u Europskoj uniji. Ciljevi bi trebali biti specifični, mjerljivi, ostvarljivi, realistični i vremenski ograničeni (SMART). Na primjer: *„Osigurat ćemo da se ova [vremenski ograničena] strategija temelji na strogim i*

[4] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-training-tool

sveobuhvatnim mjerilima s pomoću kojih mjerimo napredak prema rezultatima koje želimo ostvariti"[5]

Prethodno navedeno uključuje i političku procjenu u pogledu toga mogu li se pribaviti dostatna proračunska sredstva za provedbu strategije. To podrazumijeva i opis predviđenog područja primjene strategije i različite kategorije dionika iz javnog i privatnog sektora koji bi trebali sudjelovati u izradi nacrta različitih ciljeva i mjera.

Prvi korak mogao bi se ostvariti s pomoću ciljanih radionica s višim dužnosnicima i političarima koje će voditi stručnjaci za kibersigurnost s profesionalnim komunikacijskim vještinama koji mogu istaknuti kakve posljedice nedostatak ili slaba razina kibersigurnosti mogu imati za suvremeno digitalno gospodarstvo i društvo.

Drugi korak – **Razvoj sadržaja strategije**

Strategija bi trebala sadržavati potporne mjere, vremenski ograničene aktivnosti i ključne pokazatelje uspješnosti za kasniju evaluaciju, razradu i poboljšanje nakon određenog razdoblja provedbe. Tim mjerama trebali bi se podupirati cilj, prioriteti i rezultati utvrđeni kao vodeća načela. Potreba za uključivanjem potpornih mjera utvrđena je u članku 7. stavku 1. točki (c) Direktive NIS.

Preporučuje se osnivanje koordinacijske skupine koja će upravljati postupkom izrade mjera i olakšavati prikupljanje informacija, a kojom će predsjedati nadležno ministarstvo. To bi se moglo postići osnivanjem različitih skupina sastavljenih od relevantnih službenika i stručnjaka koji bi se bavili izradom mjera povezanih s ključnim generičkim temama, na primjer procjenom rizika, planiranjem za nepredviđene situacije, upravljanjem incidentima, razvojem vještina, podizanjem razine osviještenosti, istraživanjem i industrijskim razvojem itd. Svaki bi se sektor zasebno pozvalo (na primjer, energetiku, prijevoz itd.) da procijeni posljedice svojeg uključivanja, uključujući potrebne resurse, i da imenovane operatore ključnih usluga i pružatelje ključnih digitalnih usluga uključi u postupke utvrđivanje prioriteta i podnošenje prijedloga u postupak izrade mjera. Sudjelovanje dionika iz različitih sektora od ključne je važnosti i s obzirom na to da je potrebno osigurati usklađenu provedbu Direktive u različitim sektorima i istodobno dopustiti posebnosti različitih sektora.

Treći korak – **Razvoj upravljačkog okvira**

Da bi bio učinkovit i djelotvoran, upravljački okvir trebao bi se temeljiti na ključnim dionicima, utvrđenim prioritetima u postupku izrade i na ograničenjima i kontekstu nacionalnih upravnih i političkih struktura. Bilo bi poželjno da postoji izravno izvješćivanje političke razine, da okvir ima sposobnosti donošenja odluka i raspodjele sredstava te da mu pridonose stručnjaci za kibersigurnost i dionici iz industrije. U članku 7. stavku 1. točki (b) Direktive NIS spominje se upravljački okvir i posebno se zahtijevaju „odgovornosti vladinih tijela i drugih relevantnih sudionika".

[5] Izvadak iz Nacionalne strategije za kibersigurnost UK-a, 2016. – 2021., str. 67.

Četvrti korak – **Izrada nacrta strategije i njegova revizija**

U toj fazi trebalo bi izraditi nacrt strategije i revidirati ga primjenom analize prednosti, nedostataka, prilika i prijetnji (SWOT) kojom bi se moglo utvrditi treba li revidirati sadržaj. Nakon unutarnje revizije trebalo bi održati savjetovanje s dionicima. Važno je održati i javno savjetovanje kako bi se javnosti istaknula važnost predložene strategije, kako bi se prikupile informacije iz svih mogućih izvora i zatražila potpora za sredstva potrebna za naknadnu provedbu strategije.

Peti korak – **Službeno donošenje**

Taj završni korak uključuje službeno donošenje na političkoj razini s proračunom kojim se omogućuje provedba i koji pokazuje koliko ozbiljno predmetna država članica shvaća kibersigurnost. U cilju ispunjenja ciljeva Direktive NIS te pri dostavljanju dokumenta nacionalne strategije Komisiji u skladu s člankom 7. stavkom 3., Komisija potiče države članice da dostave informacije o proračunu. Preuzimanje obveza u pogledu proračuna i potrebnih ljudskih resursa od ključne je važnosti za djelotvornu provedbu strategije i Direktive. Budući da je kibersigurnost još uvijek novo područje javne politike koje se brzo širi, u većini slučajeva potrebna su nova ulaganja čak i ako su zbog općeg stanja javnih financija potrebni rezovi i uštede.

Savjeti o postupku izrade nacionalnih strategija i njihovu sadržaju dostupni su iz različitih javnih i akademskih izvora, na primjer od ENISA-e[6], ITU-a[7], OECD-a[8], Globalnog foruma stručnjaka za kibersigurnost i Sveučilišta u Oxfordu[9].

2.4. Konkretni koraci koje države članice moraju poduzeti prije roka za prenošenje

Prije donošenja Direktive gotovo sve države članice[10] već su objavile dokumente koji su definirani kao nacionalne strategije za kibersigurnost. U odjeljku 6. ovog Priloga nalazi se popis svih strategija koje trenutačno postoje u svakoj državi članici[11]. One obično uključuju

---

[6] ENISA, *Dobra praksa za nacionalne strategije za kibersigurnost*, 2016. Dostupno na https://www.enisa.europa.eu/publications/ncss-good-practice-guide

[7] ITU, Vodič za nacionalne strategije za kibersigurnost (2011.). Dostupno na http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf
ITU će 2017. objaviti i Skup alata za izradu nacionalnih strategija za kibersigurnost (vidjeti prezentaciju na http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf)

[8] OECD, *Politika kibersigurnosti na prekretnici: Analiza nove generacije nacionalnih strategija za kibersigurnost* (2012.). Dostupno na: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

[9] Globalni centar za kapacitete u području kibersigurnosti i Sveučilište u Oxfordu, *Globalni model zrelosti kapaciteta za kibersigurnost za države (CMM) – Revidirano izdanje* (2016.). Dostupno na: https://www.thegfce.com/binaries/gfce/documents/publications/2017/02/13/cybersecurity-cmm-for-nations/CMM+revised+edition.pdf

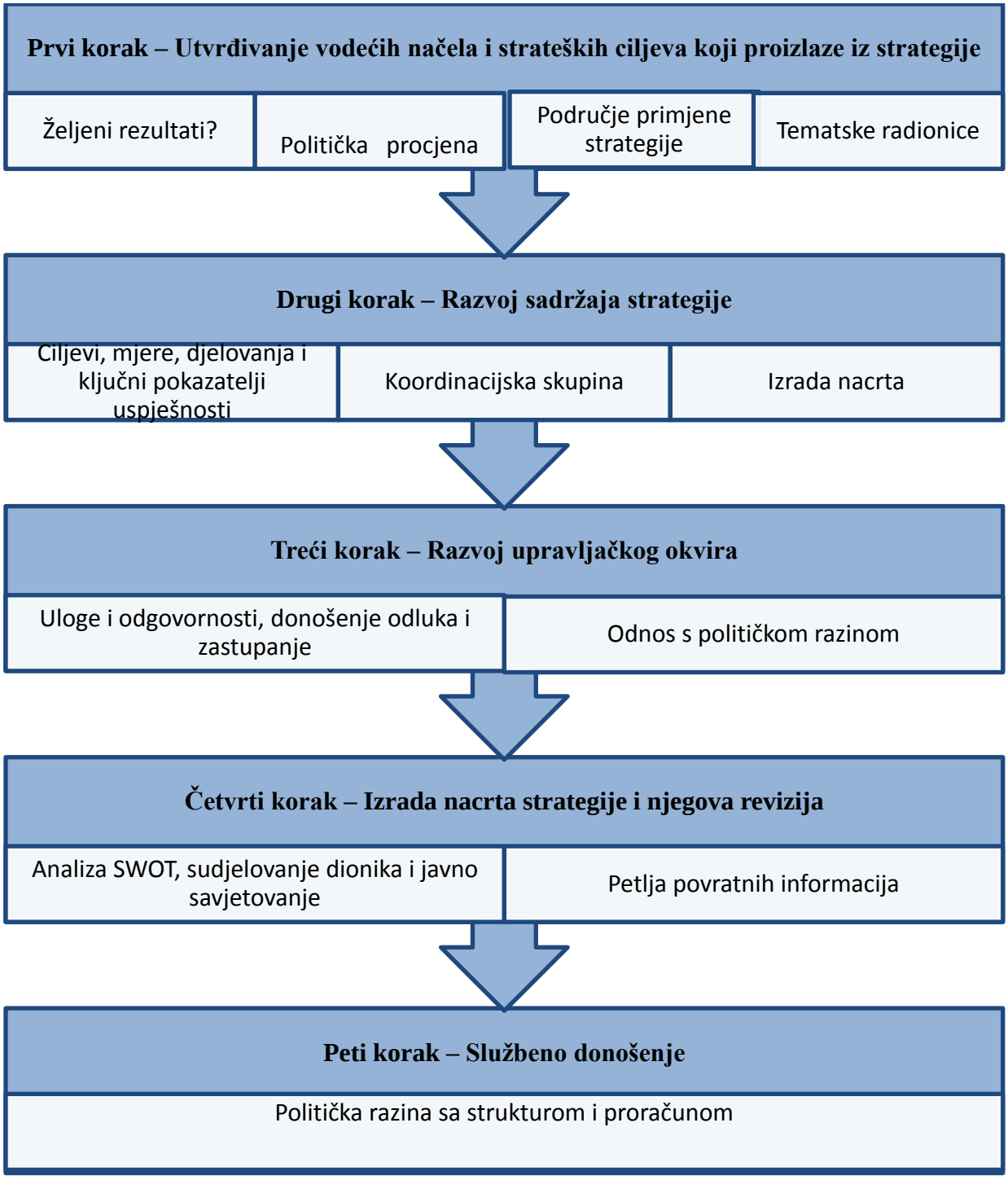
[10] Osim Grčke u kojoj je nacionalna strategija za kibersigurnost u izradi od 2014. (vidjeti na https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-greece/view)

[11] Navedene informacije temelje se na pregledu nacionalnih strategija za kibersigurnost koji je izradila ENISA, dostupnom na https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

strateška načela, smjernice, ciljeve i u nekim slučajevima posebne mjere za ublažavanje rizika povezanih s kibersigurnošću.

Budući da su neke od tih strategija donesene prije donošenja Direktive NIS, one nužno ne sadržavaju sve elemente navedene u članku 7. Kako bi se osiguralo pravilno prenošenje, države članice morat će provesti analizu nedostataka povezivanjem sadržaja svojih nacionalnih strategija za kibersigurnost sa sedam zasebnih zahtjeva iz članka 7. u svim sektorima navedenima u Prilogu II. Direktivi i u pogledu svih usluga iz Priloga III. Utvrđeni nedostaci mogu se zatim ukloniti revizijom njihovih postojećih strategija za kibersigurnost ili potpunom revizijom načela nacionalne strategije za mrežnu i informacijsku sigurnost. Prethodno navedene smjernice za postupak donošenja nacionalnih strategija za kibersigurnost relevantne su i za reviziju i ažuriranje postojećih strategija.

Grafikon 1.: Postupak od pet koraka za donošenje nacionalne strategije za kibersigurnost



3. Direktiva NIS: nacionalna nadležna tijela, jedinstvene kontaktne točke i timovi za odgovor na računalne sigurnosne incidente (CSIRT-ovi)

U skladu s člankom 8. stavkom 1. države članice moraju imenovati jedno ili više nacionalnih nadležnih tijela koja obuhvaćaju barem sektore iz Priloga II. i usluge iz Priloga III. Direktivi,

a koja će imati zadaću nadgledanja njezine primjene. Države članice mogu tu ulogu dodijeliti postojećem tijelu ili tijelima.

U tom se odjeljku usredotočuje na to kako se Direktivom NIS poboljšava pripravnost država članica uvođenjem zahtjeva za imenovanje djelotvornih nacionalnih nadležnih tijela i timova za odgovor na računalne sigurnosne incidente (CSIRT-ova). Drugim riječima, tim je odjeljkom obuhvaćena obveza imenovanja nacionalnih nadležnih tijela, uključujući ulogu jedinstvene kontaktne točke. Razmatraju se tri teme: (a) moguće nacionalne upravljačke strukture (npr. centralizirani, decentralizirani modeli itd.) i drugi zahtjevi; (b) uloga jedinstvene kontaktne točke i (c) timovi za odgovor na računalne sigurnosne incidente.

3.1. Vrsta nadležnih tijela

Člankom 8. Direktive NIS od država članica zahtijeva se imenovanje nacionalnih nadležnih tijela za sigurnost mrežnih i informacijskih sustava te se izričito priznaje mogućnost imenovanja „jednog ili više nacionalnih nadležnih tijela”. U uvodnoj izjavi 30. Direktive objašnjen je taj politički izbor: „S obzirom na razlike u nacionalnim upravljačkim strukturama i radi zaštite već postojećih sektorskih rješenja ili nadzornih i regulatornih tijela Unije te kako bi se izbjegla udvostručivanja, države članice trebale bi biti u mogućnosti odrediti više od jednog nadležnog nacionalnog tijela čija je odgovornost izvršavanje zadaća povezanih sa sigurnošću mrežnih i informacijskih sustava operatorâ ključnih usluga i pružateljâ digitalnih usluga u okviru ove Direktive.”

U skladu s time države članice mogu odlučiti imenovati jedno središnje tijelo koje će biti zaduženo za sve sektore i usluge obuhvaćene Direktivom ili nekoliko tijela, ovisno, na primjer, o vrsti sektora.

Kada odlučuju o pristupu, države članice mogu svoju odluku temeljiti na iskustvu stečenom primjenom nacionalnih pristupa koji se upotrebljavaju u kontekstu postojećeg zakonodavstva o zaštiti ključne infrastrukture (CIIP). Kako je opisano u tablici 1., u slučaju CIIP-a, države članice odlučile su pri dodjeli nadležnosti na nacionalnoj razini primijeniti centralizirani ili decentralizirani pristup. Nacionalni primjeri ovdje se navode samo radi ilustracije i kako bi se države članice upoznale s postojećim ustrojstvenim okvirima. Komisija stoga ne tvrdi da bi se model koji se u određenoj zemlji upotrebljava za CIIP trebao nužno upotrebljavati za prenošenje Direktive NIS.

Države članice mogu se odlučiti i za različita hibridna rješenja koja uključuju elemente centraliziranog i decentraliziranog pristupa. Izbor se može izvršiti u skladu s prethodnim nacionalnim upravljačkim rješenjima za različite sektore i usluge obuhvaćene Direktivom ili nadležna tijela i relevantni dionici koji su identificirani kao operatori ključnih usluga i pružatelji digitalnih usluga mogu utvrditi nove modele. Važni čimbenici na kojima će države članice temeljiti svoj izbor mogu uključivati i stručno znanje o kibersigurnosti, pitanja povezana s resursima, odnose između dionika i nacionalne interese (na primjer gospodarski razvoj, javna sigurnost itd.).

3.2. Objava i dodatni relevantni aspekti

U skladu s člankom 8. stavkom 7. države članice moraju obavijestiti Komisiju o imenovanju nacionalnih nadležnih tijela i o njihovim zadaćama. To se mora učiniti do roka za prenošenje.

Člancima 15. i 17. Direktive NIS zahtijeva se od država članica da osiguraju da nadležna tijela imaju posebne ovlasti i sredstva za izvršavanje zadaća utvrđenih u tim člancima.

Nadalje, imenovanje određenih subjekata nacionalnim nadležnim tijelima objavljuje se. Direktivom nije propisan način objave. Budući da je cilj tog zahtjeva postići visoku razinu osviještenosti dionika na koje utječe mrežna i informacijska sigurnost i opće javnosti te na temelju iskustava u drugim sektorima (telekomunikacije, bankarstvo, zdravstvo), Komisija smatra da bi se to moglo izvršiti, primjerice, s pomoću dobro oglašavanog portala.

Člankom 8. stavkom 5. Direktive NIS zahtijeva se da takva tijela imaju „odgovarajuće resurse” za provedbu zadaća koje su im dodijeljene Direktivom.

Tablica 1.: Nacionalni pristup zaštiti ključne informacijske strukture (CIIP)

ENISA je 2016. objavila studiju[12] o različitim pristupima država članica zaštiti njihovih ključnih informacijskih infrastruktura. Opisana su dva različita pristupa upravljanju ključnom informacijskom strukturom u državama članicama, koji se mogu primijeniti u kontekstu prenošenja Direktive NIS.

Profil 1.: Decentralizirani pristup – s više sektorskih tijela nadležnih za pojedine sektore i usluge navedene u prilozima II. i III. Direktivi

Decentralizirani pristup obilježava sljedeće:

(i) načelo supsidijarnosti
(ii) snažna suradnja javnih agencija
(iii)zakonodavstvo specifično za pojedini sektor

Načelo supsidijarnosti

Umjesto uspostave ili imenovanja jedinstvene agencije koja ima opću nadležnost, decentralizirani pristup temelji se na načelu supsidijarnosti. To znači da je za provedbu odgovorno sektorsko tijelo koje najbolje razumije lokalni sektor i ima već uspostavljeni odnos s dionicima. U skladu s tim načelom, odluke donose tijela koja su najbliža onima na koje mjere utječu.

Snažna suradnja javnih agencija

Budući da u zaštiti ključne informacijske infrastrukture sudjeluju različite javne agencije, mnoge države članice razvile su programe suradnje u cilju koordinacije rada i napora različitih tijela. Ti programi suradnje mogu biti u obliku neformalnih mreža ili institucionaliziranih foruma ili mehanizama. Međutim, svrha je tih programa suradnje samo razmjena informacija i koordinacija između različitih javnih agencija, ali oni nad njima nemaju ovlasti.

Zakonodavstvo specifično za pojedini sektor

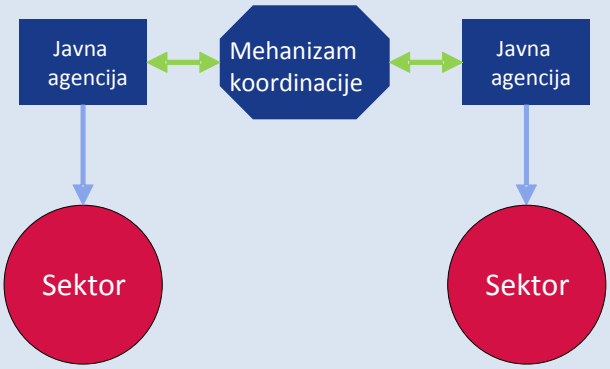
Države koje u ključnim sektorima primjenjuju decentralizirani pristup često ne donose zakonodavstvo za zaštitu ključne informacijske infrastrukture. Donošenje zakona i propisa specifično je za sektore i stoga se može znatno razlikovati od sektora do sektora. Prednost tog pristupa jest usklađivanje mjera povezanih s mrežnom i informacijskom sigurnošću s postojećim sektorskim propisima u cilju poboljšanja prihvaćenosti u sektoru i djelotvornosti izvršenja od strane predmetnog tijela.

Čisti decentralizirani pristup donosi znatan rizik od manje usklađene primjene Direktive u različitim sektorima i uslugama. U tom slučaju Direktivom je predviđena jedinstvena nacionalna kontaktna točka za vezu za prekogranična pitanja i, u skladu s člankom 10. Direktive, predmetna država članica mogla bi taj subjekt zadužiti i za unutarnju koordinaciju i

[12] ENISA, *Pregled stanja, analiza i preporuke za zaštitu ključne informacijske strukture* (2016.). Dostupno na: https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

suradnju različitih nacionalnih nadležnih tijela.

Grafikon 2. – Decentralizirani pristup



Primjeri decentraliziranog pristupa

Švedska je dobar primjer zemlje koja primjenjuje decentralizirani pristup u zaštiti ključne informacijske infrastrukture. Ta država upotrebljava „perspektivu sustava", što znači da su za glavne zadaće u okviru zaštite ključne informacijske infrastrukture, kao što su utvrđivanje ključnih usluga i ključne infrastrukture, koordinacija i potpora operatora, regulatorne zadaće i mjere pripravnosti u hitnim slučajevima, odgovorne različite agencije i općine. Među tim su agencijama i Švedska agencija za nepredviđene situacije (MSB), Švedska agencija za poštu i telekomunikacije (PTS) te nekoliko švedskih obrambenih i vojnih agencija i tijela kaznenog progona.

U cilju koordinacije djelovanja različitih agencija i javnih tijela, švedska vlada razvila je okvir za suradnju koji se sastoji od tijela „s posebnim odgovornostima za informacijsku sigurnost društva". Skupina za suradnju u području informacijske sigurnosti (SAMFI) sastoji se od predstavnika različitih tijela i sastaje se nekoliko puta godišnje kako bi razgovarala o pitanjima povezanima s nacionalnom informacijskom sigurnošću. SAMFI djeluje uglavnom u političko-strateškim područjima i bavi se pitanjima kao što su tehnička pitanja i normizacija, nacionalni i međunarodni razvoj u području informacijske sigurnosti ili upravljanje incidentima u području IT-a i njihovo sprječavanje. (Švedska agencija za nepredviđene situacije (MSB) 2015.).

Švedska nije objavila osnovni zakon o zaštiti ključne informacijske infrastrukture koji se primjenjuje na operatore ključne informacijske infrastrukture (CII) u svim sektorima. Umjesto toga, za donošenje propisa s obvezama za poduzeća u određenom sektoru odgovorna su odgovarajuća javna tijela. Na primjer, MSB ima pravo donositi propise za državna tijela u sektoru informacijske sigurnosti, a PTS može tražiti od operatora da provode određene tehničke ili ustrojstvene mjere sigurnosti na temelju sekundarnog zakonodavstva.

Još jedan primjer zemlje tog profila jest Irska. Irska slijedi „doktrinu supsidijarnosti" u skladu s

kojom je svako ministarstvo odgovorno za utvrđivanje ključne informacijske infrastrukture i za procjenu rizika u svojem sektoru. Nadalje, na nacionalnoj razini nisu doneseni posebni propisi za zaštitu ključne informacijske infrastrukture. Zakonodavstvo je sektorsko i postoji uglavnom u sektoru energetike i telekomunikacija (2015.). Ostali primjeri su Austrija, Cipar i Finska.

Profil 2.: Centralizirani pristup — s jednim središnjim tijelom koje je nadležno za sve sektore i usluge navedene u prilozima II. i III. Direktivi.

Centralizirani pristup obilježava sljedeće:

i) središnje tijelo nadležno za sve sektore
ii) sveobuhvatno zakonodavstvo

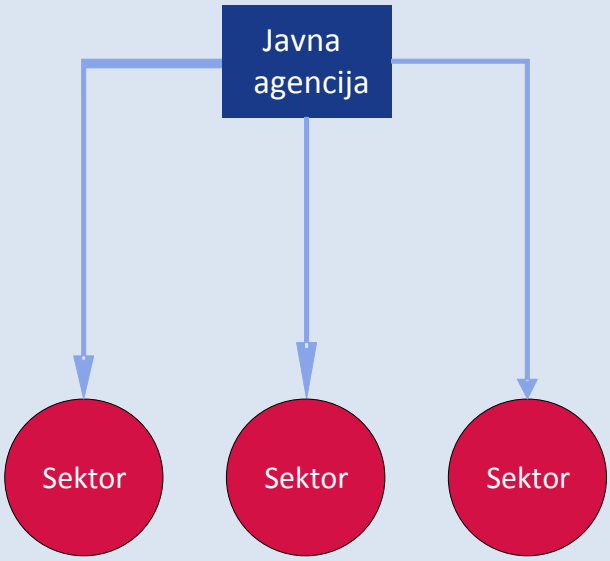
Središnje tijelo nadležno za sve sektore

Države članice koje primjenjuju centralizirani pristup osnovale su tijela s odgovornostima i širokim nadležnostima u nekoliko ključnih sektora ili svim ključnim sektorima ili su proširile ovlasti postojećih tijela. Ta glavna tijela za zaštitu ključne informacijske infrastrukture kombiniraju nekoliko zadaća kao što je planiranje za hitne slučajeve, upravljanje hitnim slučajevima, regulatorne zadaće i podupiranje privatnih operatora. U mnogim slučajevima nacionalni ili državni CSIRT dio je glavnog tijela za zaštitu ključne infrastrukture. Vjerojatnije je da će u središnjem tijelu postojati veća koncentriranost stručnjaka za kibersigurnost nego u više sektorskih nadležnih tijela, uzimajući u obzir opći manjak vještina u području kibersigurnosti.

Sveobuhvatno zakonodavstvo

Sveobuhvatnim zakonodavstvom utvrđuju se obveze i zahtjevi za sve operatore ključne informacijske infrastrukture u svim sektorima. To se može postići novim sveobuhvatnim zakonima ili dopunom postojećih sektorskih propisa. Takvim pristupom olakšala bi se dosljedna primjena Direktive NIS u svim sektorima i na sve obuhvaćene usluge. Izbjegao bi se rizik od nedostataka u provedbi koje bi mogle nastati u slučaju više nadležnih tijela s posebnim područjem nadležnosti.

Grafikon 3. – Centralizirani pristup



Primjeri centraliziranog pristupa

Francuska je dobar primjer države članice EU-a s centraliziranim pristupom. Francuska agencija *Agence Nationale de la Sécurité des Systèmes d'Information* (ANSSI) proglašena je 2011. glavnim nacionalnim tijelom za obranu informacijskih sustava. ANSSI ima snažnu nadzornu ulogu u pogledu „operatora od ključne važnosti" (OIV): može im naložiti da se pridržavaju sigurnosnih mjera i ovlaštena je nad njima provoditi revizije sigurnosti. Nadalje, ANSSI je glavna jedinstvena kontaktna točka za operatore od ključne važnosti, koji su joj dužni prijavljivati sigurnosne incidente.

U slučaju sigurnosnih incidenata, ANSSI djeluje kao agencija za zaštitu ključne informacijske infrastrukture u nepredviđenim situacijama i odlučuje o mjerama koje operatori moraju poduzeti kao odgovor na krizu. Djelovanja vlade koordiniraju se u operativnom centru ANSSI-ja. Za otkrivanje prijetnji i odgovor na incidente na operativnoj razini zadužen je CERT-FR, koji je dio ANSSI-ja.

Francuska je uspostavila sveobuhvatni pravni okvir za zaštitu ključne informacijske infrastrukture. Predsjednik vlade naložio je 2006. izradu popisa sektora ključne infrastrukture. Na temelju tog popisa na kojem se nalazilo dvanaest ključnih sektora, vlada je definirala otprilike 250 operatora od ključne važnosti. Godine 2013. donesen je Zakon o vojnom programiranju (LPM)[13]. U njemu su utvrđene različite obveze za operatore od ključne važnosti, kao što je izvješćivanje o incidentima ili provedba sigurnosnih mjera. Ti su zahtjevi obvezni za sve operatore od ključne važnosti u svim sektorima (francuski Senat, 2013.).

[13] *La loi de programmation militaire*.

3.3. Direktiva NIS, članak 9.: timovi za odgovor na računalne sigurnosne incidente (CSIRT-ovi)

U skladu s člankom 9. države članice moraju imenovati jednog ili više CSIRT-ova kojima se povjerava zadaća rješavanja rizika i incidenata u sektorima navedenima u Prilogu II. Direktivi NIS i u vezi s uslugama navedenima u Prilogu III. Uzimajući u obzir zahtjev minimalnog usklađivanja iz članka 3. Direktive, države članice mogu upotrebljavati CSIRT-ove i za druge sektore koji nisu obuhvaćeni Direktivom, kao što je javna uprava.

Države članice mogu odlučiti uspostaviti CSIRT unutar nacionalnog nadležnog tijela[14].

3.4. Zadaće i zahtjevi

Zadaće imenovanih CSIRT-ova, navedene u Prilogu I. Direktivi NIS, uključuju sljedeće:

- praćenje incidenata na nacionalnoj razini,
- pružanje ranih upozorenja i najava te informiranje relevantnih dionika o rizicima i incidentima,
- odgovaranje na incidente,
- pružanje dinamičke analize rizika i incidenata te pregleda situacije i
- sudjelovanje u mreži nacionalnih CSIRT-ova (mreža CSIRT-ova) uspostavljenoj u skladu s člankom 12.

Posebne dodatne zadaće navedene su u članku 14. stavcima 3., 5. i 6. i članku 16. stavcima 3., 6. i 7. u pogledu obavijesti o incidentima kada država članica odluči da CSIRT-ovi mogu preuzeti te uloge zajedno s nacionalnim nadležnim tijelima ili umjesto njih.

Države članice pri prenošenju Direktive imaju više mogućnosti u pogledu uloge CSIRT-ova u zahtjevima za obavješćivanje o incidentima. Moguće je izravno obvezno prijavljivanje CSIRT-ovima koje donosi prednosti administrativne učinkovitosti ili države članice mogu izabrati mogućnost izravnog prijavljivanja nacionalnim nadležnim tijelima pri čemu CSIRT-ovi imaju pravo pristupa prijavljenim informacijama. CSIRT-ovi su u konačnici zainteresirani za rješavanje problema odvraćanjem, otkrivanjem, odgovaranjem na kiberincidente i ublažavanjem njihova učinka (uključujući kiberincidente koji ne podliježu obveznom prijavljivanju) zajedno s dionicima, a za regulatornu usklađenost nadležna su nacionalna nadležna tijela.

U skladu s člankom 9. stavkom 3. Direktive države članice moraju osigurati i da CSIRT-ovi imaju pristup sigurnoj i otpornoj infrastrukturi IKT-a.

[14] Vidjeti članak 9. stavak 1. zadnja rečenica.

Člankom 9. stavkom 4. od država članica zahtijeva se da obavijeste Komisiju o mandatu i glavnim elementima postupka za rješavanje incidenata imenovanih CSIRT-ova.

Zahtjevi za CSIRT-ove koje imenuju države članice propisani su u Prilogu I. Direktivi NIS. CSIRT mora osigurati visoku razinu dostupnosti svojih komunikacijskih usluga. Njihovi prostori i informacijski sustavi za potporu smješteni su na sigurnim lokacijama i moraju moći osigurati kontinuitet rada. Nadalje, CSIRT-ovi moraju imati mogućnost sudjelovati u međunarodnim mrežama za suradnju.

3.5. Pomoć za razvoj CSIRT-ova

Programom Kibersigurnost infrastrukture za digitalne usluge (DSI) Instrumenta za povezivanje Europe (CEF) mogu se osigurati znatna sredstva EU-a kojima će se državama članicama pomoći da poboljšaju svoje sposobnosti i uzajamnu suradnju s pomoću mehanizma suradnje za razmjenu informacija. Mehanizmom suradnje koji se razvija u okviru projekta SMART 2015/1089 nastoji se olakšati brza i djelotvorna operativna suradnja na dobrovoljnoj osnovi između CSIRT-ova država članica, posebno radi potpore zadaćama koje su mreži CSIRT-ova povjerene u skladu s člankom 12. Direktive.

Pojedinosti o relevantnim pozivima na podnošenje prijedloga za jačanje kapaciteta CSIRT-ova država članica dostupni su na *web*-mjestu Izvršne agencije za inovacije i mreže (INEA) Europske komisije[15].

Upravljački odbor programa Kibersigurnost infrastrukture za digitalne usluge u okviru CEF-a osigurava neformalnu strukturu za smjernice na razini politike i pomoć CSIRT-ovima država članica za jačanje kapaciteta i za provedbu dobrovoljnog mehanizma suradnje.

Novoosnovani CSIRT ili CSIRT imenovan za izvršavanje zadaća iz Priloga I. Direktivi NIS može se oslanjati na savjete i stručno znanje ENISA-e kako bi poboljšao svoju uspješnost i učinkovitost svojeg rada[16]. U vezi s time vrijedi istaknuti da bi CSIRT-ovi država članica kao referencu trebali uzeti neke od aktivnosti koje je ENISA nedavno provela. Agencija je, kako je navedeno u odjeljku 7. ovog Priloga, posebno objavila niz dokumenata i studija s opisom dobre prakse, preporukama na tehničkoj razini i procjenama razine zrelosti CSIRT-ova u pogledu različitih sposobnosti i usluga CSIRT-ova. Nadalje, smjernice i najbolju praksu dijelile su i mreže CSIRT-ova na globalnoj (FIRST[17]) i europskoj razini (Trusted Introducer, TI[18]).

3.6. Uloga jedinstvene kontaktne točke

U skladu s člankom 8. stavkom 3. Direktive NIS svaka država određuje nacionalnu jedinstvenu kontaktnu točku koja izvršava funkciju povezivanja s ciljem osiguravanja prekogranične suradnje s relevantnim tijelima u drugim državama članicama te sa skupinom za suradnju i mrežom CSIRT-ova[19] koja je osnovana tom Direktivom. U uvodnoj izjavi 31. i

[15] Dostupno na: https://ec.europa.eu/inea/en/connecting-europe-facility
[16] Vidjeti članak 9. stavak 5. Direktive NIS.
[17] Forum timova za odgovor na računalne sigurnosne incidente (https://www.first.org/)
[18] https://www.trusted-introducer.org/
[19] Mreža nacionalnih CSIRT-ova za operativnu suradnju država članica u skladu s člankom 12.

članku 8. stavku 4. objašnjava se logička podloga tog zahtjeva, a to je olakšavanje prekogranične suradnje i komunikacije. To je posebno potrebno budući da države članice mogu odlučiti imenovati više nacionalnih tijela. Stoga bi se jedinstvenom kontaktnom točkom olakšala identifikacija i suradnja tijela iz različitih država članica.

Funkcija povezivanja jedinstvene kontaktne točke vjerojatno će uključivati komunikaciju s tajništvom skupine za suradnju i tajništvom mreže CSIRT-ova u slučajevima kada jedinstvena kontaktna točka nije ni CSIRT ni član skupine za suradnju. Nadalje, države članice moraju osigurati informiranje jedinstvene kontaktne točke o obavijestima o incidentima koje su zaprimile od operatora ključnih usluga ili pružatelja digitalnih usluga.[20]

U članku 8. stavku 3. Direktive navedeno je da ako država članica primjenjuje centralizirani pristup, odnosno ako imenuje jedno nadležno tijelo, to nadležno tijelo ima i ulogu jedinstvene kontaktne točke. Ako se država članica odluči za decentralizirani pristup, među tim različitim nadležnim tijelima može odabrati jedno koje će djelovati kao jedinstvena kontaktna točka. Neovisno o odabranom institucionalnom modelu, ako su nadležno tijelo, CSIRT i jedinstvena kontaktna točka različiti subjekti, države članice dužne su osigurati djelotvornu suradnju među njima u cilju ispunjavanja obveza propisanih Direktivom.[21]

Do 9. kolovoza 2018., a nakon toga svake godine, jedinstvena kontaktna točka mora skupini za suradnju podnijeti sažeto izvješće o zaprimljenim obavijestima, među ostalim o broju obavijesti i naravi incidenata te o radnjama koje su poduzela nadležna tijela, kao što su obavješćivanje drugih pogođenih država članica o incidentu ili pružanje odgovarajućih informacija za rješavanje incidenta poduzeću koje o njemu dostavilo obavijest.[22] Na zahtjev nadležnog tijela ili CSIRT-a jedinstvena kontaktna točka mora obavijesti operatora ključnih usluga proslijediti jedinstvenim kontaktnim točkama drugih država članica pogođenih incidentima.[23]

Države članice moraju do roka za prenošenje obavijestiti Komisiju o imenovanju jedinstvene kontaktne točke i o njezinim zadaćama. Imenovanje jedinstvene kontaktne točke objavljuje se na isti način kao i imenovanje nacionalnih nadležnih tijela. Komisija objavljuje popis imenovanih jedinstvenih kontaktnih točaka.

3.7. Sankcije

Člankom 21. državama članicama dopušta se da odluče o vrsti i prirodi primjenjivih sankcija uz uvjet da su učinkovite, proporcionalne i odvraćajuće. Drugim riječima, države članice u načelu mogu slobodno odlučiti o najvećem iznosu sankcija propisanom njihovim nacionalnim zakonodavstvom, ali odabranim iznosom ili postotkom trebalo bi se državama članicama omogućiti da u svakom pojedinačnom slučaju odrede učinkovite, proporcionalne i odvraćajuće sankcije, uzimajući u obzir različite čimbenike kao što su težina ili učestalost povrede.

[20] Vidjeti članak 10. stavak 3.
[21] Vidjeti članak 10. stavak 1.
[22] Isto.
[23] Vidjeti članak 14. stavak 5.

4. Subjekti koji imaju obveze u pogledu sigurnosnih zahtjeva i obavijesti o incidentima

Subjekti koji imaju važnu ulogu za društvo i gospodarstvo i koji se u članku 4. stavku 4. i članku 4. stavku 5. Direktive nazivaju operatorima ključnih usluga i pružateljima digitalnih usluga moraju poduzeti odgovarajuće sigurnosne mjere i ozbiljne incidente prijaviti relevantnim nacionalnim tijelima. Razlog tomu je to što učinci sigurnosnih incidenata povezanih s takvim uslugama mogu predstavljati veliku prijetnju funkcioniranju takvih usluga, što može u velikoj mjeri naštetiti gospodarskim djelatnostima i društvu općenito, narušiti povjerenje korisnika i nanijeti znatnu štetu gospodarstvu Unije[24].

Taj odjeljak sadržava pregled subjekata obuhvaćenih područjem primjene priloga II. i III. Direktivi NIS i popis njihovih obveza. Podrobno je opisana identifikacija operatora ključnih usluga zbog važnosti tog postupka za usklađenu provedbu Direktive NIS u cijelom EU-u. Podrobno su objašnjene i definicije digitalnih infrastruktura i pružatelja digitalnih usluga. Ispituje se i moguće uključivanje dodatnih sektora te se dodatno objašnjava poseban pristup u pogledu pružatelja digitalnih usluga.

4.1. Operatori ključnih usluga

Direktivom NIS ne definira se izričito koji će se subjekti smatrati operatorima ključnih usluga u okviru njezina područja primjene. Umjesto toga u njoj se navode kriteriji koje će države članice morati primjenjivati kako bi mogle provoditi postupak identifikacije kojim će se u konačnici utvrditi koja će se poduzeća koja se mogu razvrstati među subjekte iz Priloga II. smatrati operatorima ključnih usluga i stoga će imati obveze propisane Direktivom.

4.1.1. Vrste subjekata iz Priloga II. Direktivi NIS

Člankom 4. stavkom 4. operatori ključnih usluga definiraju se kao javni ili privatni subjekti tipa navedenog u Prilogu II. Direktivi, koji ispunjavaju kriterije utvrđene u članku 5. stavku 2. U Prilogu II. navedeni su sektori, podsektori i vrste subjekata u pogledu kojih svaka država članica mora provesti postupak identifikacije iz članka 5. stavka 2.[25] Sektori uključuju energetiku, prijevoz, bankarstvo, infrastrukture financijskog tržišta, zdravstvo, vodu i digitalnu infrastrukturu.

Većina subjekata iz „tradicionalnih sektora" dobro je definirana u zakonodavstvu EU-a i na te se definicije upućuje u Prilogu II. Međutim, to nije slučaj u pogledu sektora digitalne infrastrukture koji je naveden u Prilogu II. točki 7., uključujući središta za razmjenu internetskog prometa, sustave naziva domena i registre naziva vršnih domena. Stoga su te definicije u nastavku detaljno objašnjene u cilju pojašnjenja.

1) Središte za razmjenu internetskog prometa (IXP)

[24] Vidjeti uvodnu izjavu 2.
[25] Više pojedinosti o postupku identifikacije opisano je u nastavku u odjeljku 4.1.6.

Pojam središte za razmjenu internetskog prometa definiran je u članku 4. stavku 13. i dodatno pojašnjen u uvodnoj izjavi 18. i može se opisati kao mrežni instrument koji omogućuje međusobno povezivanje više od dvaju neovisnih tehnički autonomnih sustava, prvenstveno u svrhu olakšavanja razmjene internetskog prometa. Središte za razmjenu internetskog prometa može se opisati i kao fizička lokacija na kojoj više mreža može razmjenjivati internetski promet s pomoću prekidača. Glavna je svrha IXP-a omogućiti mrežama izravno međusobno povezivanje posredstvom središta za razmjenu, a ne posredstvom jedne ili više mreža treće strane. Pružatelj IXP-a u načelu nije odgovoran za preusmjeravanje internetskog prometa. Preusmjeravanje prometa obavljaju pružatelji mrežnih usluga. Postoje brojne prednosti izravnog međusobnog povezivanja, ali glavni razlozi su trošak, latencija i širina pojasa. Promet koji prolazi kroz središte za razmjenu u načelu ne naplaćuje nijedna strana, dok se promet prema pružatelju internetskih usluga na uzlaznom tržištu naplaćuje. Zahvaljujući izravnoj međusobnoj vezi, koja se često nalazi u istom gradu kao i obje mreže, izbjegava se potreba za dalekim putovanjem podataka iz jedne mreže u drugu, čime se smanjuje latencija.

Treba napomenuti da definicijom IXP-a nisu obuhvaćene fizičke točke na kojima se međusobno povezuju samo dvije fizičke mreže (tj. pružatelji mrežnih usluga kao što su BASE i PROXIMUS). Stoga pri prenošenju Direktive države članice moraju razlikovati između operatora koji olakšavaju razmjenu ukupnog internetskog prometa među više mrežnih operatora i oni koji su operatori jedne mreže i koji fizički međusobno povezuju svoje mreže na temelju sporazuma o međusobnom povezivanju. U potonjem slučaju pružatelji mrežnih usluga nisu obuhvaćeni definicijom iz članka 4. stavka 13. To je objašnjeno u uvodnoj izjavi 18. u kojoj je navedeno da IXP ne pruža pristup mreži odnosno ne djeluje kao pružatelj prijenosa ni kao nositelj prijenosa. Posljednja kategorija pružatelja su poduzeća koja pružaju javne komunikacijske mreže i/ili usluge koje podliježu sigurnosnim obvezama i obvezama prijave iz članaka 13.a i 13.b Direktive 2002/21/EZ i stoga su isključena iz područja primjene Direktive NIS[26].

2) Sustav naziva domena (DNS)

Pojam sustav naziva domena definiran je u članku 4. stavku 14. kao „hijerarhijsko raspoređeni sustav imenovanja na mreži koji šalje upite o nazivima domena". Drugim riječima, DNS se može opisati kao hijerarhijsko raspoređeni sustav imenovanja za računala, usluge i ostale resurse povezane na Internet kojim se omogućuje šifriranje naziva domena u IP adrese (adrese internetskog protokola). Glavna uloga sustava jest pretvaranje dodijeljenih naziva domena u IP adrese. U tu svrhu DNS upravlja bazom podataka i koristi se poslužiteljima naziva i rezolverom kako bi omogućio takav „prijevod" naziva domena u operativne IP adrese. Iako šifriranje naziva domena nije jedina zadaća DNS-a, to je njegova ključna zadaća. Pravna definicija iz članka 14. stavka 4. usmjerena je na glavnu ulogu sustava s gledišta korisnika i ne uključuje tehničke pojedinosti, kao što su na primjer upravljanje prostorom naziva domene, poslužiteljima naziva, rezolverima itd. Naposljetku, člankom 4. stavkom 15. pojašnjava se tko se smatra pružateljem DNS usluga.

[26] Više pojedinosti o odnosu između Direktive NIS i Direktive 2002/21/EZ navedeno je u odjeljku 5.2.

3) Registar naziva vršnih domena (registar naziva TLD-a)

Registar naziva vršnih domena definiran je u članku 4. stavku 16. kao subjekt koji upravlja i rukuje registracijom naziva internetskih domena za određenu vršnu domenu. Takvo upravljanje i rukovanje nazivima domena uključuje pretvaranje naziva vršnih domena u IP adrese.

IANA (Tijelo za dodjelu mrežnih brojeva na internetu) odgovorno je za globalnu koordinaciju korijenskog DNS-a, dodjelu adresa internetskog protokola i ostale resurse internetskog protokola. IANA je posebno odgovorna za dodjelu generičkih vršnih domena (gTLD), na primjer „.com", i nacionalnih vršnih domena (ccTLD), na primjer „.be", operatorima (registrima) i za održavanje njihovih tehničkih i administrativnih podataka. IANA održava globalni registar dodijeljenih TLD-ova i sudjeluje u širenju tog popisa korisnicima interneta u cijelom svijetu te u uvođenju novih TLD-ova.

Važna je zadaća registara dodjeljivati nazive druge razine takozvanim registrantima u okviru vlastitog TLD-a. Registranti mogu sami dodjeljivati nazive domene treće razine ako tako žele. Nacionalne vršne domene dodjeljuju se za predstavljanje države ili područja na temelju norme ISO 3166-1. Generičke vršne domene obično ne nose zemljopisnu oznaku ili oznaku države.

Treba napomenuti da upravljanje registrom TLD-ova može uključivati pružanje sustava naziva domena. Na primjer, u skladu s pravilima delegiranja IANA-e, imenovano tijelo koje se bavi nacionalnim vršnim domenama mora, među ostalim, nadzirati nazive domena i upravljati DNS-om te zemlje[27]. Države članice moraju uzeti u obzir te okolnosti kada provode postupak identifikacije operatora ključnih usluga u skladu s člankom 5. stavkom 2.

4.1.2. Identifikacija operatora ključnih usluga

U skladu sa zahtjevima iz članka 5. Direktive države članice moraju provesti postupak identifikacije u pogledu svih subjekata svih vrsta navedenih u Prilogu II. koji imaju poslovni nastan na njihovom državnom području. Nakon te procjene svi subjekti koji ispunjavaju kriterije propisane u članku 5. stavku 2. identificiraju se kao operatori ključnih usluga i podliježu obvezama u pogledu sigurnosti i obavješćivanja iz članka 14.

Države članice moraju do 9. studenoga 2018. identificirati operatore za svaki sektor i podsektor. Kako bi pomogla državama članicama u tom postupku, skupina za suradnju radi na razvoju dokumenta sa smjernicama koji sadržava potrebne informacije o nužnim koracima i najboljoj praksi identifikacije operatora ključnih usluga.

Nadalje, u skladu s člankom 24. stavkom 2. skupina za suradnju raspravlja o postupku, sadržaju i vrsti nacionalnih mjera za omogućivanje identifikacije operatora ključnih usluga u određenim sektorima. Država članica može, prije 9. studenoga 2018., zatražiti raspravu o

[27] Informacije su dostupne na sljedećoj poveznici: https://www.icann.org/resources/pages/delegation-2012-02-25-en

svojem nacrtu nacionalnih mjera za omogućivanje identifikacije operatora ključnih usluga u okviru skupine za suradnju.

4.1.3. Uključivanje dodatnih sektora

Uzimajući u obzir zahtjev minimalnog usklađivanja iz članka 3., države članice mogu donositi ili održavati zakonodavstvo kojim se osigurava viša razina sigurnosti mrežnih i informacijskih sustava. U tu svrhu države članice mogu proširiti obvezeu pogledu sigurnosti i obavješćivanja iz članka 14. na tijela iz sektora i podsektora koji nisu navedeni u Prilogu II. Direktivi NIS. Različite države članice odlučile su ili trenutačno razmatraju uključivanje nekih od sljedećih sektora:

i) Javne uprave

Javne uprave mogu pružati ključne usluge iz Priloga II. Direktivi u skladu s zahtjevima članka 5. stavka 2. U takvim slučajevima javne uprave koje pružaju takve usluge bile bi obuhvaćene relevantnim sigurnosnim zahtjevima i obvezama obavješćivanja. S druge strane, kada javne uprave pružaju usluge koje nisu obuhvaćene prethodno navedenim područjem primjene, takve usluge ne bi bile obuhvaćene relevantnim obvezama.

Javne uprave odgovorne su za pravilno pružanje javnih usluga koje pružaju javna tijela, tijela regionalne i lokalne vlasti, agencije i povezana poduzeća. Te usluge često podrazumijevaju prikupljanje osobnih i poslovnih podataka o pojedincima i organizacijama i upravljanje tim podacima, koji se mogu razmjenjivati i staviti na raspolaganje brojnim javnim tijelima. Općenito govoreći, visoka razina sigurnosti mrežnih i informacijskih sustava kojima se koriste javne uprave u interesu je društva i gospodarstva u cjelini. Komisija stoga smatra da bi države članice trebale razmotriti uključivanje javne uprave u područje primjene nacionalnog zakonodavstva za prenošenje Direktive, uz pružanje ključnih usluga iz Priloga II. i članka 5. stavka 2.

ii) Poštanski sektor

Poštanski sektor obuhvaća pružanje poštanskih usluga kao što su preuzimanje, razvrstavanje, prijevoz i dostava poštanskih pošiljaka.

iii) Prehrambeni sektor

Prehrambeni sektor obuhvaća proizvodnju poljoprivrednih i ostalih prehrambenih proizvoda i mogao bi uključivati ključne usluge kao što je osiguravanje sigurnosti hrane i jamstvo kvalitete i sigurnosti hrane.

iv) Kemijska i nuklearna industrija

Kemijska i nuklearna industrija obuhvaćaju posebno skladištenje, proizvodnju i preradu kemijskih i petrokemijskih proizvoda i nuklearnih materijala.

v) Sektor zaštite okoliša

Aktivnosti zaštite okoliša obuhvaćaju opskrbu robom i pružanje usluga nužnih za zaštitu okoliša i upravljanje njima. Aktivnosti su stoga usmjerene na sprječavanje, smanjenje i uklanjanje onečišćenja i očuvanje dostupnih prirodnih resursa. Ključne usluge u ovom sektoru mogle bi biti praćenje i kontrola onečišćenja (npr. zraka i vode) i meteoroloških pojava.

vi) Civilna zaštita

Cilj je sektora civilne zaštite spriječiti prirodne katastrofe i katastrofe koje uzrokuje čovjek te se pripremiti i odgovoriti na njih. Usluge koje se pružaju u tu svrhu mogu uključivati aktivaciju brojeva hitnih službi i obavljanje aktivnosti informiranja o hitnim slučajevima te njihovu kontrolu i odgovor na njih.

4.1.4. Nadležnost

U skladu s člankom 5. stavkom 1. svaka država članica mora identificirati operatore ključnih usluga s poslovnim nastanom na njezinu državnom području. Tom se odredbom ne opisuje dodatno vrsta poslovnog nastana, ali je u uvodnoj izjavi 21. objašnjeno da takav poslovni nastan podrazumijeva učinkovito i stvarno obavljanje djelatnosti u okviru stabilnih aranžmana, a pravni oblik takvih aranžmana ne bi trebao biti odlučujući čimbenik. To znači da država članica može biti nadležna za operatora ključnih usluga ne samo kada operator ima sjedište na njezinu državnom području već i u slučajevima kada operator na njezinu području ima, na primjer, podružnicu ili neku drugu vrstu zakonitog poslovnog nastana.

Posljedica toga je da nekoliko država članica može imati nadležnost nad istim subjektom.

4.1.5. Informacije koje se dostavljaju Komisiji

Za potrebe preispitivanja koje Komisija mora provoditi u skladu s člankom 23. stavkom 1. Direktive NIS države članice dužne su do 9. studenoga 2018. i svake dvije godine nakon toga Komisiji dostaviti sljedeće podatke:

- nacionalne mjere kojima se omogućuje identifikacija operatora ključnih usluga,
- popis ključnih usluga,
- broj operatora ključnih usluga identificiranih za svaki sektor naveden u Prilogu II. i relevantnost tih operatora za sektor i
- pragove, ako postoje, za određivanje odgovarajuće razine opskrbe prema broju korisnika koji se oslanjaju na tu uslugu kako je navedeno u članku 6. stavku 1. točki (a) ili u skladu s važnošću tog subjekta u skladu s člankom 6. stavkom 1. točkom (f).

Preispitivanje predviđeno člankom 23. stavkom 1., koje prethodi sveobuhvatnom preispitivanju Direktive, pokazuje koliku važnost suzakonodavci pridaju pravilnom prenošenju Direktive u pogledu identifikacije operatora ključnih usluga kako bi se izbjegla rascjepkanost tržišta.

Da bi se ovaj postupak mogao provesti na najbolji mogući način, Komisija potiče države članice da razgovaraju o toj temi i da razmjenjuju relevantno iskustvo u skupini za suradnju. Nadalje, Komisija potiče države članice da dostave Komisiji, prema potrebi na povjerljivoj osnovi, popis identificiranih operatora ključnih usluga (koji su u konačnici odabrani) zajedno sa svim podacima koje države članice moraju dostaviti Komisiji u skladu s Direktivom. Postojanjem takvih popisa olakšala bi se procjena dosljednosti postupka identifikacije i poboljšala njegova kvaliteta te bi se omogućila usporedba postupaka među državama članicama, čime bi se olakšalo postizanje ciljeva Direktive.

4.1.6. Kako provoditi postupak identifikacije?

Kako je prikazano na grafikonu 4., nacionalno tijelo trebalo bi ispitati šest ključnih pitanja kada provodi postupak identifikacije u pogledu određenog subjekta. Svako pitanje u sljedećem odlomku odgovara koraku koji treba poduzeti u skladu s člankom 5. u vezi s člankom 6. i uzimajući u obzir primjenjivost članka 1. stavka 7.

Prvi korak – **Pripada li subjekt sektoru/podsektoru i odgovara li vrsti obuhvaćenoj Prilogom II. Direktivi?**

Nacionalno tijelo trebalo bi procijeniti pripada li subjekt s poslovnim nastanom na njegovu državnom području sektorima i podsektorima navedenima u Prilogu II. Direktivi. Prilogom II. obuhvaćeni su različiti gospodarski sektori koji se smatraju ključnima za osiguravanje pravilnog funkcioniranja unutarnjeg tržišta. Prilog II. posebno se odnosi na sljedeće sektore i podsektore:

- energetika: električna energija, nafta, plin
- prijevoz: zračni, željeznički, vodni i cestovni promet
- bankarstvo: kreditne institucije
- infrastrukture financijskog tržišta: mjesta trgovanja, središnje druge ugovorne strane
- zdravstvo: pružatelji zdravstvene zaštite (uključujući bolnice i privatne klinike)
- vodoopskrba: opskrba vodom za piće i njezina distribucija
- digitalna infrastruktura središta za razmjenu internetskog prometa, pružatelji usluga sustava naziva domene, registri naziva vršnih domena[28]

Drugi korak – **Primjenjuje li se *lex specialis*?**

U sljedećem koraku nacionalno tijelo mora ocijeniti primjenjuje li se odredba o *lex specialisu* iz članka 1. stavka 7. U odredbi je posebno navedeno da ako se pravnim aktom EU-a pružateljima digitalnih usluga ili operatorima ključnih usluga određuju sigurnosni zahtjevi i/ili zahtjevi za obavješćivanje koji su barem jednaki obvezama iz Direktive NIS, primjenjuju se odredbe iz posebnog pravnog akta. Nadalje, u uvodnoj izjavi 9. objašnjeno je da bi države članice, ako su ispunjeni zahtjevi iz članka 1. stavka 7., trebale primjenjivati odredbe posebnog akta EU-a, uključujući odredbe o nadležnosti. S druge strane, relevantne odredbe Direktive NIS ne bi se primjenjivale. U tom slučaju nadležno tijelo ne bi trebalo nastaviti provoditi postupak identifikacije iz članka 5. stavka 2.[29]

Treći korak – **Pruža li operator ključnu uslugu u smislu Direktive?**

U skladu s člankom 5. stavkom 2. točkom (a) subjekt koji je predmet identifikacije mora pružati uslugu koja je ključna za održavanje ključnih društvenih i/ili ekonomskih djelatnosti. Pri obavljanju te procjene države članice trebale bi uzeti u obzir činjenicu da jedan subjekt može pružati ključne i sporedne usluge. To znači da će se sigurnosni zahtjevi i zahtjevi za

[28]Ti su subjekti detaljnije objašnjeni u odjeljku 4.1.1.

[29] Više pojedinosti od primjenjivosti *lex specialisa* navedeno je u odjeljku 5.1.

obavješćivanje iz Direktive NIS primjenjivati na određenog operatora samo ako on pruža ključne usluge.

U skladu s člankom 5. stavkom 3. država članica trebala bi sastaviti popis svih ključnih usluga koje operator ključnih usluga pruža na njezinu državnom području. Taj će se popis trebati dostaviti Komisiji do 9. studenoga 2018. i svake dvije godine nakon toga[30].

Četvrti korak – **Ovisi li usluga o mrežnom i informacijskom sustavu?**

Nadalje, treba objasniti ispunjava li ta usluga drugi kriterij iz članka 5. stavka 2. točke (b) i posebno ovisi li pružanje ključne usluge o mrežnim i informacijskim sustavima koji su definirani u članku 4. stavku 1.

Peti korak – **Bi li sigurnosni incident imao znatan negativan učinak?**

Člankom 5. stavkom 2. točkom (c) od nacionalnog tijela zahtijeva se da procjeni bi li incident imao znatan negativan učinak na pružanje usluge. U tom kontekstu u članku 6. stavku 1. propisano je nekoliko međusektorskih čimbenika koje treba uzeti u obzir u procjeni. Nadalje, člankom 6. stavkom 2. propisano je da bi tijekom procjene, prema potrebi, trebalo uzeti u obzir čimbenike specifične za određeni sektor.

Međusektorski čimbenici navedeni u članku 6. stavku 1. sljedeći su:

- broj korisnika koji se oslanjaju na usluge koje taj subjekt pruža,
- ovisnost drugih sektora iz Priloga II. o uslugama koje dotični subjekt pruža,
- mogući utjecaj incidenata, u pogledu njihova stupnja i trajanja, na gospodarske i društvene aktivnosti te na javnu sigurnost,
- tržišni udio tog subjekta,
- zemljopisna raširenost u smislu područja na koje bi incident mogao utjecati,
- važnost subjekta za održavanje dostatne razine usluge, uzimajući u obzir raspoloživost alternativnih sredstava za pružanje te usluge.

Kada je riječ o **čimbenicima specifičnima za određeni sektor,** u uvodnoj izjavi 28. navedeni su neki primjeri (vidjeti tablicu 4.) koji bi mogli poslužiti kao korisne smjernice nacionalnim tijelima.

Tablica 4.: Primjeri čimbenika specifičnih za određeni sektor koje treba uzeti u obzir pri utvrđivanju znatnog negativnog učinka u slučaju incidenta

Sektor	Primjer čimbenika specifičnih za određeni sektor
Dobavljači električne energije	količina ili udio proizvedene električne energije na nacionalnom tržištu
Dobavljači nafte	dnevna količina isporučene nafte

[30] Vidjeti članak 5. stavak 7. točku (b).

Zračni prijevoz (uključujući zračne luke i zračne prijevoznike) **Željeznički prijevoz** **Pomorske luke**	udio u opsegu nacionalnog prometa godišnji broj putnika ili prevezenog tereta
Bankarska infrastruktura ili infrastruktura financijskog tržišta	sustavna važnost koja se temelji na ukupnoj imovini omjer ukupne imovine i BDP-a
Zdravstveni sektor	godišnji broj pacijenata kojima se pruža zdravstvena skrb
Proizvodnja i prerada vode te vodoopskrba	količina te broj i vrste opskrbljenih korisnika (što primjerice uključuje bolnice, organizacije javnih službi ili pojedince) postojanje alternativnih izvora vode za isto zemljopisno područje

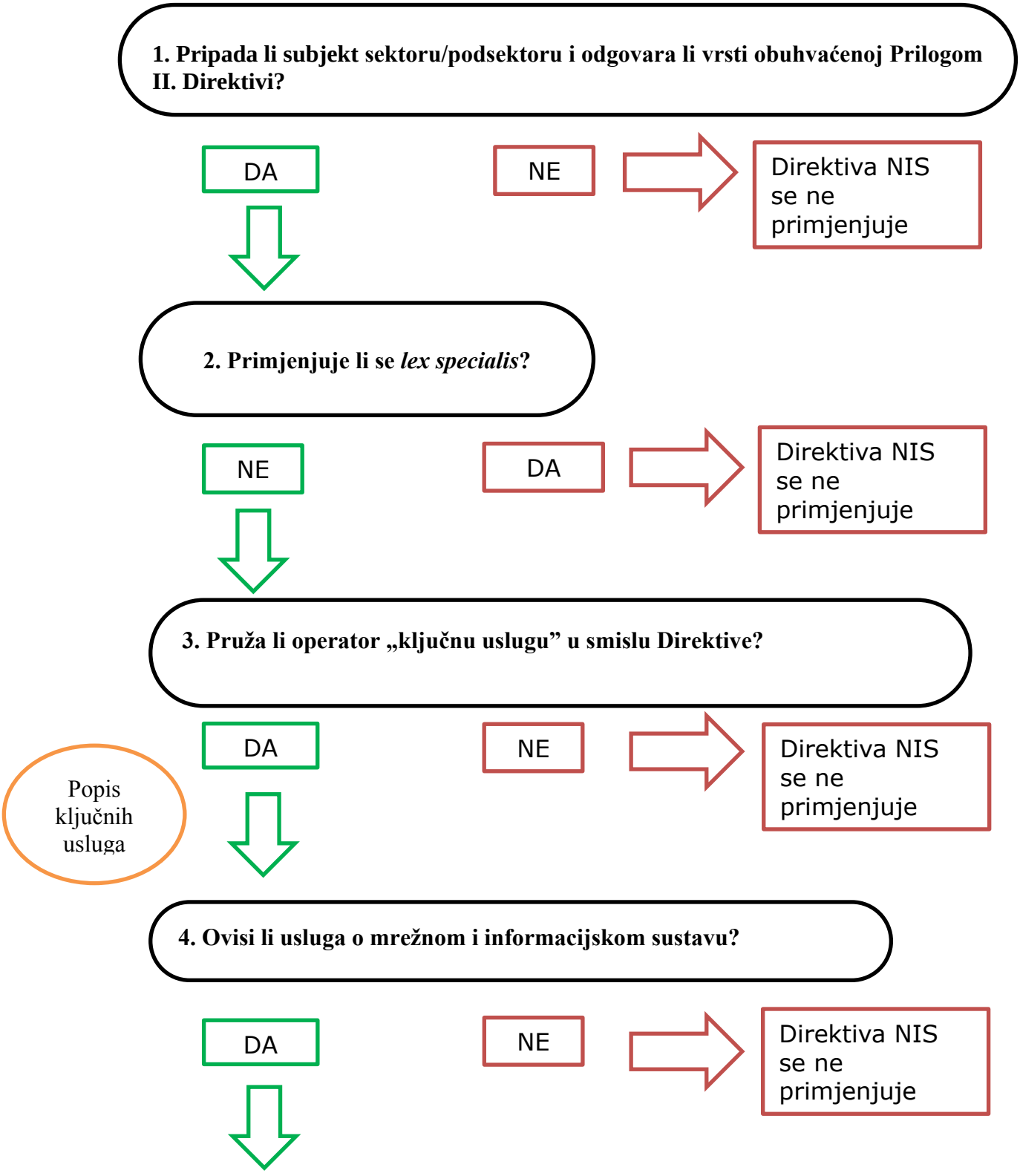
Trebalo bi istaknuti da države članice pri obavljaju procjene u skladu s člankom 5. stavkom 2. ne bi trebale dodavati dodatne kriterije osim navedenih u toj odredbi jer bi se tako mogao smanjiti broj identificiranih pružatelja ključnih usluga i ugroziti minimalno usklađivanje operatora ključnih usluga propisano u članku 3. Direktive.

Šesti korak - **Pruža li predmetni operator ključne usluge u drugim državama članicama?**

Šesti korak odnosi se na slučajeve kada operator pruža svoje ključne usluge u dvije ili više država članica. Člankom 5. stavkom 4. zahtijeva se od predmetnih država članica da se uključe u postupak savjetovanja prije dovršetka postupka identifikacije[31].

[31] Više pojedinosti o postupku savjetovanja navedeno je u odjeljku 4.1.7.

Grafikon 4.: Postupak identifikacije u 6 koraka



5. Bi li sigurnosni incident imao znatan negativan učinak?

Međusektorski čimbenici (članak 6. stavak 1.)

- **broj korisnika** koji se oslanjaju na usluge
- **ovisnost** drugih ključnih sektora o usluzi
- mogući utjecaj incidenata **na gospodarske i društvene aktivnosti te na javnu sigurnost**
- moguća **zemljopisna raširenost**
- važnost subjekta za održavanje dostatne **razine usluge**

na

Čimbenici specifični za pojedini sektor (primjeri navedeni u uvodnoj izjavi 28.)

- **energetika:** količina ili udio proizvedene električne energije na nacionalnom tržištu
- **promet**: udio u opsegu nacionalnog prometa i godišnji broj operacija
- **zdravstvo**: godišnji broj pacijenata kojima se pruža zdravstvena skrb

DA

NE → Direktiva NIS se ne primjenjuje

6. Pruža li predmetni operator ključne usluge u drugim državama članicama?

DA

NE → Direktiva NIS se ne primjenjuje

Obvezno savjetovanje s predmetnom državom

Donošenje nacionalnih mjera (npr. popis operatora ključnih usluga, mjere politike i zakonodavne mjere)

4.1.7. Prekogranično savjetovanje

Ako operator pruža ključne usluge u dvije ili više država članica, člankom 5. stavkom 4. propisano je da se te države članice moraju jedna s drugom savjetovati prije okončanja postupka identifikacije. Svrha je tog savjetovanja olakšati procjenu ključne prirode operatora u smislu prekograničnog učinka.

Željeni je rezultat savjetovanja razmjena argumenata i stajališta među uključenim nacionalnim tijelima i postizanje istog rješenja u pogledu identifikacije predmetnog operatora. Međutim, Direktivom NIS ne sprječavaju se države članice da donesu suprotne zaključke o tome hoće li određenog subjekta identificirati kao operatora ključnih usluga ili ne. U uvodnoj izjavi 24. spominje se da države članice mogu u tom pogledu zatražiti pomoć skupine za suradnju.

Komisija smatra da bi države članice trebale nastojati postići konsenzus o tim pitanjima kako bi se izbjegla situacija u kojoj isto trgovačko društvo ima drugačiji pravni položaj u različitim državama članicama. Različiti pravni položaj trebao bi biti stvarno iznimni slučaj, odnosno kada subjekt koji je određen kao operator ključne usluge u jednoj državi članici obavlja marginalne ili beznačajne djelatnosti u drugoj.

4.2. Sigurnosni zahtjevi

U skladu s člankom 14. stavkom 1. države članice moraju osigurati da operatori ključnih usluga, uzimajući u obzir najnovija postignuća, poduzimaju odgovarajuće i razmjerne tehničke i organizacijske mjere za upravljanje rizicima kojima su izloženi mrežni i informacijski sustavi kojima se organizacije služe u pružanju svojih usluga. U skladu s člankom 14. stavkom 2. učinak incidenta sprječava se i svodi na najmanju moguću mjeru odgovarajućim mjerama.

Posebna radna skupina unutar skupine za suradnju trenutačno radi na neobvezujućim smjernicama o sigurnosnim mjerama za operatore ključnih usluga[32]. Skupina će dovršiti dokument sa smjernicama do četvrtog tromjesečja 2017. Komisija potiče države članice da pažljivo prate dokument sa smjernicama koji će razviti skupina za suradnju kako bi nacionalne odredbe o sigurnosnim zahtjevima bile što usklađenije. Usklađivanjem takvih zahtjeva znatno bi se olakšala usklađenost operatora ključnih usluga koji često pružaju ključne usluge u više država članica i nadzornih zadaća nacionalnih nadležnih tijela i CSIRT-ova.

4.3. Zahtjevi za obavješćivanje

U skladu s člankom 14. stavkom 3. države članice moraju osigurati da operatori ključnih usluga obavješćuju o „incidentima koji imaju znatan učinak na kontinuitet ključnih usluga

[32] Za potrebe tih aktivnosti poslani su popisi međunarodni normi, dobre prakse i metodologija za procjenu rizika/upravljanje za sve sektore obuhvaćene Direktivom NIS i upotrijebit će se kao ulazne informacije za predložene sigurnosne domene i sigurnosne mjere.

koje pružaju". Stoga operatori ključnih usluga ne bi trebali prijavljivati manje incidente nego samo ozbiljne incidente koji utječu na kontinuitet pružanja ključne usluge. U članku 4. stavku 7. incident se definira kao „bilo koji događaj koji ima stvaran negativni učinak na sigurnost mrežnih i informacijskih sustava". Pojam „sigurnost mrežnih i informacijskih sustava" definira se u članku 4. stavku 2. kao „sposobnost mrežnih i informacijskih sustava da odolijevaju, na određenoj razini pouzdanosti, bilo kojoj radnji koja ugrožava dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih ili prenesenih ili obrađenih podataka ili srodnih usluga koje ti mrežni i informacijski sustavi nude ili kojima omogućuju pristup". Stoga bi svaki događaj koji ima negativan utjecaj ne samo na dostupnost nego i na autentičnost, cjelovitost ili povjerljivost podataka ili povezanih usluga mogao pokrenuti obvezu obavješćivanja. Kontinuitet usluge koji se spominje u članku 14. stavku 3. može se ugroziti ne samo u slučajevima fizičke dostupnosti, već i bilo kojim drugim sigurnosnim incidentom koji utječe na pravilno pružanje usluge[33].

Posebna radna skupina unutar skupine za suradnju priprema neobvezujuće smjernice o okolnostima u kojima su operatori ključnih usluga dužni obavješćivati o incidentima u skladu s člankom 14. stavkom 7. i o formatu i nacionalnom postupku obavješćivanja. Planira se da će smjernice biti dovršene do četvrtog tromjesečja 2017.

Različiti nacionalni zahtjevi za obavješćivanje mogu dovesti do pravne nesigurnosti, složenijih i opterećujućih postupaka i znatnih administrativnih troškova za pružatelje koji djeluju preko granica. Komisija stoga pozdravlja rad skupine za suradnju. Kao i u slučaju zahtjeva u pogledu sigurnosti, Komisija potiče države članice da pažljivo prate dokument sa smjernicama koji će izraditi skupina za suradnju kako bi nacionalne odredbe o prijavi incidenata bile što usklađenije.

4.4. Direktiva NIS, Prilog III.: pružatelji digitalnih usluga

Pružatelji digitalnih usluga (DSP-ovi) druga su kategorija subjekata uključenih u područje primjene Direktive NIS. Ti se subjekti smatraju važnim gospodarskim subjektima jer ih mnoga poduzeća upotrebljavaju za pružanje svojih usluga, a prekid u pružanju digitalnih usluga mogao bi utjecati na ključne gospodarske i društvene aktivnosti.

4.4.1. Kategorije pružatelja digitalnih usluga

U članku 4. stavku 5. u kojem se definiraju digitalne usluge upućuje se na pravnu definiciju iz članka 1. stavka 1. točke (b) Direktive 2015/1535 sužavanjem područja primjene na vrste usluge navedene u Prilogu III. U članku 1. stavku 1. točki (b) Direktive (EU) 2015/1535 te se usluge definiraju kao „svaka usluga koja se obično pruža uz naknadu, na daljinu, elektroničkim sredstvima te na osobni zahtjev primatelja usluga", a u Prilogu III. Direktivi navedene su tri posebne vrste usluga: internetsko tržište, internetska tražilica i usluge računalstva u oblaku. Za razliku od operatora ključnih usluga, Direktivom se ne traži od država članica da identificiraju pružatelje digitalnih usluga na koje bi se potom primjenjivale relevantne obveze. Stoga će se relevantne obveze iz Direktive, odnosno sigurnosni zahtjevi i

[33] Isto se primjenjuje na pružatelje digitalnih usluga.

zahtjevi za obavješćivanje utvrđeni u članku 16., primjenjivati na sve pružatelje digitalnih usluga unutar njezina područja primjene.

U sljedećim odjeljcima dodatno su objašnjene tri vrste digitalnih usluga koje su uključene u područje primjene Direktive.

1. Pružatelj usluga internetskog tržišta

Internetskim tržištem omogućuje se velikom broju različitih poduzeća da obavljaju svoje djelatnosti trgovine s potrošačima i da uspostavljaju odnose s drugim poduzećima. Njime se trgovačkim društvima osigurava osnovna infrastruktura za trgovinu na internetu i preko granica. Ona imaju važnu ulogu u gospodarstvu jer MSP-ovima omogućuju pristup širem jedinstvenom digitalnom tržištu EU-a. Pružanje računalnih usluga na daljinu kojima se olakšavaju gospodarske djelatnosti klijenta, uključujući obradu transakcija i prikupljanje informacija o kupcima, dobavljačima i proizvodima, može se također smatrati djelatnošću pružatelja usluga internetskog tržišta, kao i olakšavanje traženja odgovarajućih proizvoda, ponuda proizvoda, stručni savjet u pogledu transakcija i povezivanje kupaca i prodavača.

Pojam internetskog tržišta definiran je u članku 4. stavku 17. i dodatno objašnjen u uvodnoj izjavi 15. Opisuje se kao usluga kojom se potrošačima i trgovcima omogućuje da putem interneta sklapaju kupoprodajne ugovore ili ugovore o uslugama s trgovcima te je krajnje odredište za sklapanje tih ugovora. Na primjer, pružatelj kao što je *E-bay* može se smatrati internetskim tržištem jer omogućuje drugima da na njegovoj platformi uspostavljaju trgovine kako bi svoje proizvode ponudili potrošačima ili poduzećima na internetu. Nadalje, smatra se da su internetske trgovine aplikacija za distribuciju aplikacija i računalnih programa obuhvaćene definicijom internetskog tržišta jer razvojnim inženjerima aplikacija omogućuju da prodaju ili distribuiraju svoje usluge potrošačima ili drugim poduzećima. S druge strane, posrednici u pružanju usluga trećih strana, kao što su *Skycanner* i usluge usporedbe cijena, koji preusmjeravaju korisnika na *web*-mjesto trgovca na kojem se sklapa stvarni ugovor za pružanje usluge ili kupoprodaju proizvoda, nisu obuhvaćeni definicijom iz članka 4. stavka 17.

2. Pružatelj usluge internetske tražilice

Pojam internetske tražilice definiran je u članku 4. stavku 18. i dodatno objašnjen u uvodnoj izjavi 16. Opisuje se kao digitalna usluga koja korisniku omogućuje da vrši pretraživanja u načelu svih internetskih stranica ili internetskih stranica na određenom jeziku na temelju upita o bilo kojoj temi koji je u obliku ključne riječi Nisu obuhvaćene funkcionalnosti pretraživanja ograničene na pretraživanje unutar internetske stranice ili internetske stranice za uspoređivanje cijena. Na primjer tražilica kao ona koja se upotrebljava na stranicama EUR LEX-a[34] ne može se smatrati tražilicom u smislu Direktive jer je njezina funkcija pretraživanja ograničena na sadržaj tog konkretnog *web*-mjesta.

3. Pružatelj usluge računalstva u oblaku

[34] Dostupno na: http://eur-lex.europa.eu/homepage.html

U članku 4. stavku 19. usluga računalstva u oblaku definira se kao „digitalna usluga kojom se pruža pristup nadogradivom i elastičnom skupu djeljivih računalnih resursa", a u uvodnoj izjavi 17. navedena su dodatna pojašnjenja pojmova računalni resursi, nadogradiv i elastičan skup.

Ukratko, računalstvo u oblaku može se opisati kao posebna vrsta računalne usluge koja se koristi zajedničkim resursima za obradu podataka na zahtjev, a djeljivi resursi odnose se na bilo koju vrstu komponenti računalne opreme ili računalnih programa (npr. mreže, poslužitelji ili druga infrastruktura, skladištenje, aplikacije i usluge) koji se korisnicima daju na zahtjev radi obrade podataka. Pojmom djeljivi definiraju se računalni resursi kada se više korisnika koristi istom fizičkom infrastrukturom za obradu podataka. Računalni resurs može se smatrati djeljivim ako se skup resursa kojim se koristi pružatelj može u bilo kojem trenutku proširiti ili smanjiti, ovisno o zahtjevima korisnika. Stoga se podatkovni centri ili jedinstvene komponente unutar podatkovnog centra mogu dodavati ili uklanjati ako je potrebno ažurirati ukupnu količinu računalnog kapaciteta ili kapaciteta za pohranu. Pojam elastični skup može se opisati kao promjene radnog opterećenja automatskim povećanjem i smanjenjem resursa kako bi dostupni resursi u svakom trenutku bili što više usklađeni s trenutačnom potražnjom"[35].

Pružatelj trenutačno može ponuditi tri glavne vrste modela usluga u oblaku:

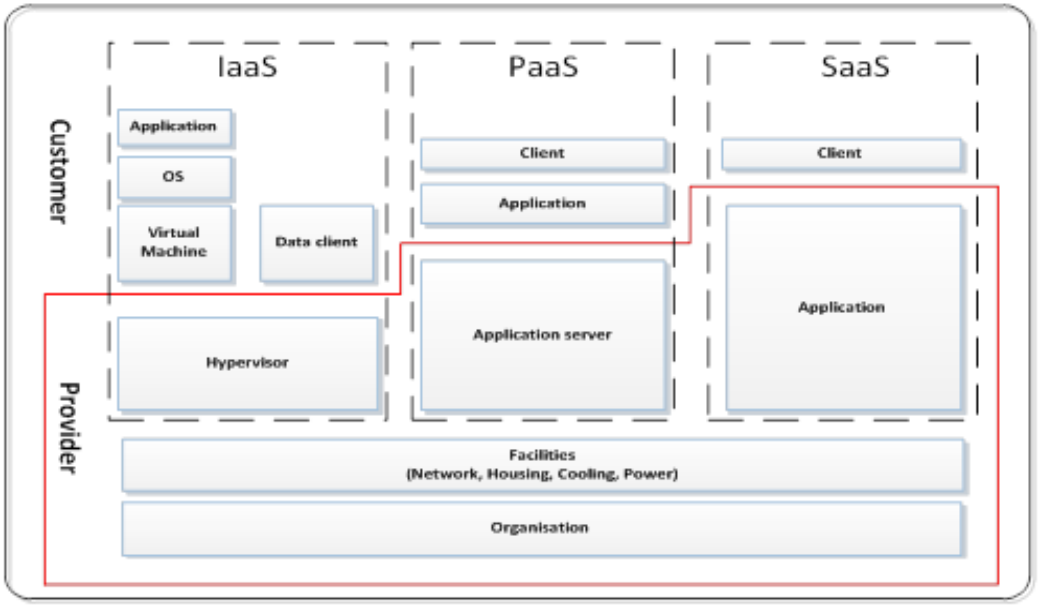
- infrastruktura kao usluga (IaaS): kategorija usluge u oblaku u kojoj se klijentu pruža infrastruktura kao vrsta kapaciteta u oblaku. Ona uključuje virtualno pružanje računalnih resursa u obliku računalne opreme, umrežavanja i usluge pohranjivanja. Infrastrukturom kao uslugom pokreću se poslužitelji, pohrana, mreže i operativni sustavi. Njome se osigurava poduzetnička infrastruktura u kojoj poduzeća mogu pohranjivati svoje podatke i pokretati aplikacije potrebne za njihov svakodnevni rad,

- platforma kao usluga (PaaS): kategorija usluge u oblaku u kojoj se klijentu pruža platforma kao vrsta kapaciteta u oblaku. Ona uključuje internetske računalne platforme kojima se trgovačkim društvima omogućuje da pokreću postojeće aplikacije ili da razvijaju i ispituju nove,

- softver kao usluga (SaaS): Kategorija usluge u oblaku u kojoj se klijentu kao vrsta kapaciteta u oblaku pružaju aplikacija ili softver koji se upotrebljava na internetu. Ovom vrstom usluge u oblaku uklanja se potreba krajnjeg korisnika da kupuje i instalira softver te da njime upravlja i omogućuje se dostupnost softvera s bilo kojeg mjesta gdje postoji internetska veza.

[35] Nikolas Roman Herbst, Samuel Kounev, Ralf Reussner, Karlsruhe Institute of Technology, „Elasticity in Cloud Computing: What It Is, and What It Is Not", dostupno na: https://sdqweb.ipd.kit.edu/publications/pdfs/HeKoRe2013-ICAC-Elasticity.pdf. Vidjeti isto stranice 2. – 5. COM(2012) 529.

Grafikon 5.: Modeli usluga i imovine u računalstvu u oblaku



EMISA je izradila sveobuhvatne smjernice o posebnim temama u području oblaka[36]i dokument sa smjernicama o osnovama računalstva u oblaku[37].

4.4.2. Sigurnosni zahtjevi

U skladu s člankom 16. stavkom 1. države članice moraju osigurati da operatori ključnih usluga poduzimaju odgovarajuće i razmjerne tehničke i organizacijske mjere za upravljanje rizicima kojima su izloženi mrežni i informacijski sustavi kojima se trgovačka društva služe u pružanju svojih usluga. Tim sigurnosnim mjerama trebalo bi uzeti u obzir najnovija postignuća i sljedećih pet elemenata: i. sigurnost sustava i objekata; ii. rješavanje incidenata; iii. upravljanje kontinuitetom poslovanja; iv. praćenje, reviziju i testiranje; v. usklađenost s međunarodnim standardima.

U tom pogledu Komisija, u skladu s člankom 16. stavkom 8., ima ovlasti donositi provedbene akte radi dodatnog utvrđivanja tih elemenata i osiguranja visoke razine usklađenosti tih pružatelja usluga. Očekuje se da će Komisija donijeti provedbeni akt u jesen 2017. Nadalje, zahtijeva se od država članica da osiguraju da pružatelji digitalnih usluga poduzimaju nužne mjere za sprječavanje učinaka incidenata i njihovo svođenje na najmanju moguću mjeru kako bi se osigurao kontinuitet njihovih usluga.

4.4.3. Obveze obavješćivanja

Od pružatelja digitalnih usluga trebalo bi tražiti da o ozbiljnim incidentima obavješćuju nadležna tijela ili CSIRT-ove. U skladu s člankom 16. stavkom 3. Direktive NIS, zahtjev za obavješćivanje primjenjuje se na pružatelje digitalnih usluga u slučajevima kada sigurnosni

[36] Dostupno na: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security
[37] ENISA, *Vodič o sigurnosti usluga u oblaku za MSP-ove* (2015.). Dostupno na: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

incident ima znatan učinak na pružanje usluge. U članku 16. stavku 4. navedeno je pet parametara koje pružatelji digitalnih usluga moraju uzeti u obzir pri utvrđivanju učinka. Komisija je u tu svrhu ovlaštena u skladu s člankom 16. stavkom 8. donijeti provedbene akte s podrobnijim opisima parametara. Ti parametri dodatno će se utvrditi provedbenim aktom u kojem će se utvrditi sigurnosni elementi iz točke 4.4.2., a koji Komisija planira donijeti u jesen.

4.4.4. Regulatorni pristup utemeljen na riziku

Člankom 17. propisano je da pružatelji digitalnih usluga podliježu *ex post* nadzoru nacionalnih nadležnih tijela. Države članice moraju osigurati da nadležna tijela poduzmu mjere kada dobiju dokaze da pružatelj digitalnih usluga ne ispunjava zahtjeve utvrđene u članku 16. Direktive.

Nadalje, u skladu s člankom 16. stavcima 8. i 9., Komisija ima ovlasti donositi provedbene akte u pogledu zahtjeva za obavješćivanje i sigurnosnih zahtjeva kojima će se povećati razina usklađenosti za pružatelje digitalnih usluga. Nadalje, u skladu s člankom 16. stavkom 10. države članice ne smiju pružateljima digitalnih usluga nametati nikakve dodatne sigurnosne zahtjeve ni zahtjeve za obavješćivanje uz one predviđene u Direktivi, osim ako su takve mjere nužne za zaštitu njihovih bitnih državnih funkcija, posebno radi zaštite nacionalne sigurnosti te kako bi se omogućila istraga, otkrivanje i kazneni progon kaznenih djela.

Naposljetku, uzimajući u obzir prekograničnu prirodu pružatelja digitalnih usluga, Direktiva ne slijedi model višestrukih usporednih nadležnosti već pristup utemeljen na kriteriju glavnog poslovnog nastana trgovačkog društva u EU-u.[38] Tim pristupom omogućuje se da se na pružatelje digitalnih usluga primjenjuje jedinstveni skup pravila s jednim nadležnim tijelom koje je odgovorno za nadzor, što je posebno važno jer mnogi pružatelji digitalnih usluga istodobno pružaju svoje usluge u mnogim državama članicama. Primjenom tog pristupa teret usklađivanja pružatelja digitalnih usluga svodi se na minimum i osigurava pravilno funkcioniranje jedinstvenog digitalnog tržišta.

4.4.5. Nadležnost

Kako je prethodno objašnjeno, u skladu s člankom 18. stavkom 1. Direktive NIS, smatra se da trgovačko društvo pripada nadležnosti države članice u kojoj ima glavni poslovni nastan. U slučajevima kada određeni pružatelj digitalnih usluga nudi usluge u EU-u, ali nema poslovni nastan na području EU-a, člankom 18. stavkom 2. pružatelju digitalnih usluga određuje se obveza da imenuje predstavnika u Uniji. U tom slučaju nadležnost nad trgovačkim društvom ima država članica u kojoj predstavnik ima poslovni nastan. Ako pružatelj digitalnih usluga pruža usluge u državi članici, ali nije imenovao predstavnika u EU-u, država članica može u načelu poduzeti mjere protiv pružatelja digitalnih usluga jer on krši svoje obveze koje ima u skladu s Direktivom.

[38] Vidjeti posebno članak 18. Direktive.

4.4.6. Izuzeće pružatelja digitalnih usluga ograničenog opsega iz područja primjene sigurnosnih zahtjeva i zahtjeva za obavješćivanje

U skladu s člankom 16. stavkom 11. pružatelji digitalnih usluga koji su mikropoduzeća i mala poduzeća u smislu Preporuke Komisije 2003/361/EZ39 isključeni su iz područja primjene sigurnosnih zahtjeva i zahtjeva za obavješćivanje utvrđenih u članku 16. To znači da tim zahtjevom nisu obvezana poduzeća koja zapošljavaju manje od 50 osoba i čiji godišnji promet i/ili čija ukupna godišnja bilanca nisu veći od 10 milijuna EUR. Pri utvrđivanju veličine subjekta nije relevantno pruža li predmetno trgovačko društvo samo digitalne usluge u smislu Direktive NIS ili i druge usluge.

5. Odnos između Direktive NIS i ostalog zakonodavstva

Ovaj odjeljak odnosi se na odredbe o *lex specialisu* iz Direktive NIS, članak 1. stavak 7., tri primjera *lex specialisa* koje je Komisija do sada ocijenila i pojašnjenje sigurnosnih zahtjeva i zahtjeva za obavješćivanje koji se primjenjuju na pružatelje telekomunikacijskih usluga i usluga povjerenja.

5.1. Direktiva NIS, članak 1. stavak 7.: odredba *lex specialisa*

U skladu s člankom 1. stavkom 7. Direktive NIS, odredbe o sigurnosnim zahtjevima i/ili zahtjevima za obavješćivanje za pružatelje digitalnih usluga ili operatore ključnih usluga u skladu s Direktivom ne primjenjuju se ako su pravnim aktom EU-a za pojedini sektor predviđeni sigurnosni zahtjevi i/ili zahtjevi za obavješćivanje koji su po učinku barem jednaki obvezama utvrđenima u Direktivi NIS. Države članice moraju pri prenošenju Direktive uzeti u obzir članak 1. stavak 7. i Komisiji dostaviti informacije o primjeni odredaba *lex specialisa.*

Metodologija

Pri procjenjivanju jednakovrijednosti pravnog akta EU-a za pojedini sektor s relevantnim odredbama Direktive NIS posebnu važnost treba posvetiti pitanju čine li sigurnosne obveze u pravnom aktu EU-a za pojedini sektor mjere kojima se osigurava sigurnost mrežnih i informacijskih sustava kako je definirana u članku 4. stavku 2. Direktive.

Kada je riječ o zahtjevima za obavješćivanje, člankom 14. stavkom 3. i člankom 16. stavkom 3. Direktive NIS propisano je da operatori ključnih usluga i pružatelji digitalnih usluga moraju bez odlaganja obavijestiti nadležna tijela ili CSIRT o incidentima koji imaju značajan/znatan učinak na pružanje usluge. Posebnu pozornost treba posvetiti obvezama operatora/pružatelja ključne usluge da u obavijest uključi informacije na temelju kojih nadležno tijelo ili CSIRT mogu utvrditi prekogranični učinak sigurnosnog incidenta.

Trenutačno ne postoji pravni akt specifičan za pojedini sektor za kategoriju pružatelja digitalnih usluga u kojem su predviđeni sigurnosni zahtjevi i zahtjevi za obavješćivanje koji

[39] SL L 24, 20.5..2003., str. 36.

su jednaki onima utvrđenima u članku 16. Direktive NIS koji se mogu uzeti u obzir u primjeni članka 1. stavka 7. Direktive NIS[40].

Kada je riječ o operatorima ključnih usluga, financijski sektor i posebno sektori bankarske infrastrukture i infrastrukture financijskog tržišta iz Priloga II. točaka 3. i 4. trenutačno podliježu sigurnosnim zahtjevima i/ili zahtjevima za obavješćivanje iz pravnih akata EU-a specifičnih za pojedini sektor. To je zato što su sigurnost i pouzdanost IT-a i mrežnih i informacijskih sustava kojima se koriste financijske institucije bitan dio zahtjeva operativnog rizika koji se u skladu sa zakonodavstvom EU-a određuju financijskim institucijama.

Primjeri.

i. Direktiva o platnim uslugama 2

U pogledu bankarskog sektora, a posebno u pogledu pružanja platnih usluga kreditnih institucija koje su definirane u članku 4. točki 1. Uredbe (EU) 575/2013, takozvanom Direktivom o platnim uslugama 2 (PSD 2)[41] predviđeni su sigurnosni zahtjevi i zahtjevi za obavješćivanje koji su utvrđeni u člancima 95. i 96. te Direktive.

Drugim riječima, člankom 95. stavkom 1. zahtijeva se od pružatelja platnih usluga da uspostave okvir s prikladnim mjerama ublažavanja i kontrolnim mehanizmima za upravljanje operativnim i sigurnosnim rizicima povezanima s platnim uslugama koje pružaju. Te mjere trebale bi uključivati uspostavu i održavanje djelotvornih postupaka upravljanja incidentima, uključujući postupke za otkrivanje i klasifikaciju značajnih operativnih i sigurnosnih incidenata. U uvodnim izjavama 95. i 96. PSD-a 2 dodatno je pojašnjena priroda takvih sigurnosnih mjera. Iz tih je odredaba razvidno da je cilj tih mjera osigurati upravljanje sigurnosnim rizicima povezanima s mrežnim i informacijskim sustavima koji se upotrebljavaju za pružanje usluga plaćanja. Stoga se ti sigurnosni zahtjevi mogu po učinku smatrati barem jednakovrijednima odgovarajućim odredbama članka 14. stavaka 1. i 2. Direktive NIS.

Kada je riječ o zahtjevima za obavješćivanje, u članku 96. stavku 1. PSD-a 2 predviđena je obveza pružatelja platnih usluga da bez nepotrebne odgode obavješćuju nadležno tijelo o ozbiljnim sigurnosnim incidentima. Nadalje, kao i člankom 14. stavkom 5. Direktive NIS, člankom 96. stavkom 2. PSD-a 2 zahtijeva se od nadležnog tijela da obavijesti nadležna tijela drugih država članica o tome je li incident relevantan za njih. Ta obveza istodobno znači da izvješćivanje o sigurnosnim incidentima mora uključivati informacije na temelju kojih nadležna tijela mogu procijeniti prekogranični učinak incidenta. Člankom 96. stavkom 3. točkom (a) PSD-a 2 ovlašćuje se EBA da u suradnji s ESB-om razvije smjernice o točnom sadržaju i formatu obavijesti.

[40] Time se ne dovodi u pitanje izvješćivanje nadzornog tijela o povredi osobnih podataka iz članka 13. Opće uredbe o zaštiti osobnih podataka.
[41] Direktiva (EU) 2015/2366, SL L 337, 23.12.2015., str..35.

Stoga se može zaključiti da bi se na pružanje usluga plaćanja kreditnih institucija u skladu s člankom 1. stavkom 7. Direktive NIS trebali primjenjivati sigurnosni zahtjevi i zahtjevi za obavješćivanje iz članaka 95. i 96. PSD-a 2 umjesto odgovarajućih odredaba članka 14. Direktive NIS.

ii. Uredba (EU) br. 648/2012 Europskog parlamenta i Vijeća od 4. srpnja 2012. o OTC izvedenicama, središnjoj drugoj ugovornoj strani i trgovinskom repozitoriju

Kada je riječ o infrastrukturi financijskog tržišta, Uredba (EU) 648/2012 u vezi s Delegiranom uredbom Komisije (EU)153/2013 sadržava odredbe o sigurnosnim zahtjevima za središnje druge ugovorne strane (CCP) koje se mogu smatrati *lex specialisom.* U pravnim aktima posebno su predviđene tehničke i organizacijske mjere povezane sa sigurnošću mrežnih i informacijskih sustava koje su čak detaljnije od zahtjeva iz članka 14. stavaka 1. i 2. Direktive NIS i stoga se može smatrati da ispunjavaju zahtjeve iz članka 1. stavka 7. Direktive NIS kada je riječ o sigurnosnim zahtjevima.

Drugim riječima, u članku 26. stavku 1. Uredbe (EU) br. 648/2012 propisano je da bi subjekt trebao imati „pouzdane sustave upravljanja s jasnom organizacijskom strukturom i dobro određenim, transparentnim i dosljednim linijama odgovornosti, učinkovite postupke za utvrđivanje, upravljanje, praćenje i izvješćivanje o rizicima kojima je središnja druga ugovorna strana izložena ili bi mogla biti izložena, te primjerene mehanizme unutarnje kontrole kao i odgovarajuće administrativne i računovodstvene postupke.” Člankom 26. stavkom 3. propisano je da se organizacijskom strukturom mora osigurati kontinuitet i pravilno funkcioniranje usluga i aktivnosti uporabom prikladnih i razmjernih sustava, resursa i postupaka.

Nadalje, u članku 26. stavku 6. objašnjeno je da CCP mora održavati „sustave informacijske tehnologije koji odgovaraju složenosti, raznovrsnosti i vrsti usluga i aktivnosti koje se obavljaju kako bi se osigurali visoki standardi sigurnosti i integriteta i povjerljivosti informacija”. Nadalje, člankom 34. stavkom 1. određuje se obveza uspostave, provedbe i održavanja primjerene politike kontinuiteta poslovanja i plana oporavka od kriznih situacija kojima bi trebalo osigurati pravovremeni oporavak operacija.

Te obveze detaljno su opisane u Delegiranoj uredbi Komisije EU/153/2013 od 19. prosinca 2012. o dopuni Uredbe (EU) br. 648/2012 Europskog parlamenta i Vijeća u vezi s regulatornim tehničkim standardima o zahtjevima za središnje druge ugovorne strane[42]. Posebno se člankom 4. te Uredbe CCP-u određuje obveza da razvije odgovarajuće alate za upravljanje rizicima kojima bi se omogućilo upravljanje svim relevantnim rizicima i izvješćivanje o njima te da dodatno opiše vrstu mjera (npr. uporaba snažnih informacijskih sustava i sustava kontrole rizika, dostupnost resursa, stručnosti i pristupa svim relevantnim informacijama za funkciju upravljanja rizikom, dostupnost prikladnih mehanizama unutarnje kontrole kao što su čvrsti administrativni i računovodstveni postupci kojima će se odboru

[42] SL L 52, 23.2..2013., str. 41.

CCP-a pomoći u praćenju i procjeni prikladnosti i djelotvornosti politika, postupaka i sustava za upravljanje rizikom).

Nadalje, u članku 9. posebno se spominje sigurnost sustava informacijske tehnologije i određuju se konkretne tehničke i organizacijske mjere povezane s održavanjem čvrstog okvira za informacijsku sigurnost za upravljanje rizikom informacijske sigurnosti. Takve mjere trebale bi uključivati mehanizme i postupke kojima se osigurava dostupnost usluga i zaštita autentičnosti, cjelovitosti i povjerljivosti podataka.

iii. Direktiva 2014/65/EU Europskog parlamenta i Vijeća od 15. svibnja 2014. o tržištu financijskih instrumenata i izmjeni Direktive 2002/92/EZ i Direktive 2011/61/EU[43]

U pogledu mjesta trgovanja, člankom 48. stavkom 1. Direktive 2014/65/EU zahtjeva se od operatora da osiguraju kontinuitet svojih usluga u slučaju prekida njihovih sustava za trgovanje. Ta opća obveza nedavno je dodatno opisana i dopunjena Delegiranom uredbom Komisije (EU) 2017/584[44] od 14. srpnja 2016. o dopuni Direktive 2014/65/EU Europskog parlamenta i Vijeća u pogledu regulatornih tehničkih standarda kojima se utvrđuju organizacijski zahtjevi za mjesta trgovanja[45]. Člankom 23. stavkom 1. te Uredbe posebno je propisano da mjesta trgovanja raspolažu postupcima i mehanizmima za fizičku i elektroničku sigurnost čija je namjena zaštititi njihove sustave od zlouporabe i neovlaštenog pristupa te osigurati cjelovitost podataka. Tim mjerama trebala bi se omogućiti zaštita od rizika od napada protiv informacijskih sustava i ti bi se rizici trebali svesti na minimum.

Člankom 23. stavkom 2. dalje je propisano da bi mjerama i mehanizmima koje poduzimaju operatori trebalo omogućiti brzu identifikaciju rizika povezanih s neovlaštenim pristupom i upravljanje njima, ometanja sustava koja ozbiljno ometaju ili prekidaju funkcioniranje informacijskog i ometanja podataka kojima se ugrožava dostupnost, cjelovitost ili autentičnost podataka. Nadalje, člankom 15. Uredbe mjestima trgovanja određuje se obveza da uspostave djelotvorne mehanizme za kontinuitet poslovanja kojima se osigurava dostatna stabilnost sustava i rješavaju incidenti koji uzrokuju prekide u radu. Tim mjerama posebno bi se trebalo omogućiti operatoru da nastavi trgovanje u roku od dva sata i osigurati da je količina izgubljenih podataka što bliže nuli.

U članku 16. dalje je navedeno da bi utvrđene mjere za rješavanje incidenata kojima se uzrokuju prekidi u radu i upravljanje njima trebale biti dio plana kontinuiteta poslovanja mjesta trgovanja i predviđeni su posebni elementi koje operator treba uzeti u obzir pri donošenju plana kontinuiteta rada (npr. uspostava posebne skupine za sigurnosne operacije, provođenje procjene učinka radi utvrđivanja rizika koja se povremeno preispituje).

Uzimajući u obzir sadržaj tih sigurnosnih mjera, čini se da je njihova svrha upravljanje rizicima koji se odnose na dostupnost, autentičnost, cjelovitost i povjerljivost podataka ili pruženih usluga i rješavanje tih rizika te da se posljedično može zaključiti da prethodno

[43] SL L 173, 12.6..2014., str. 349.
[44] SL L 87, 31.3..2017., str. 350.
[45] http://ec.europa.eu/finance/securities/docs/isd/mifid/rts/160714-rts-7_en.pdf

navedeni pravni akti EU-a specifični za pojedine sektore sadržavaju sigurnosne obveze čiji je učinak barem jednakovrijedan odgovarajućim odredbama iz članka 14. stavaka 1. i 2. Direktive NIS.

5.2. Direktiva NIS, članak 1. stavak 3.: pružatelji telekomunikacijskih usluga i usluga povjerenja

U skladu s člankom 1. stavkom 3. sigurnosni zahtjevi i zahtjevi za obavješćivanje predviđeni u Direktivi ne primjenjuju se na pružatelje koji podliježu zahtjevima iz članaka 13.a i 13.b Direktive 2002/21/EZ. Članci 13.a i 13.b Direktive 2002/21/EZ primjenjuju se na poduzeća koja pružaju javne komunikacijske mreže i javno dostupne elektroničke komunikacijske usluge. Stoga, kada je riječ o pružanju javnih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga, trgovačko društvo mora ispuniti sigurnosne zahtjeve i zahtjeve za obavješćivanje iz Direktive 2002/21/EZ.

Međutim, ako isto trgovačko društvo pruža i druge usluge kao što su digitalne usluge (npr. računalstvo u oblaku ili internetsko tržište) navedene u Prilogu III. Direktivi NIS ili usluge kao što su DNS ili IXP u skladu s Prilogom II. točkom 7. Direktive NIS, sigurnosni zahtjevi i zahtjevi za obavješćivanje iz Direktive NIS primjenjivali bi se na to trgovačko društvo u pogledu pružanja tih određenih usluga. Treba napomenuti i da, budući da pružatelji usluga iz Priloga II. točke 7. pripadaju kategoriji operatora ključnih usluga, države članice moraju provoditi postupak identifikacije u skladu s člankom 5. stavkom 2. i utvrditi koji pojedinačni pružatelji usluga DNS, IXP i TLD bi trebali ispunjavati zahtjeve iz Direktive NIS. To znači da će nakon takve procjene samo oni pružatelji DNS-a, IXP-a ili TLD-a koji ispunjavaju kriterije iz članka 5. stavka 2. Direktive NIS morati ispuniti zahtjeve iz Direktive NIS.

U članku 1. stavku 3. dalje je navedeno da se sigurnosni zahtjevi i zahtjevi za obavješćivanje Direktive ne primjenjuju na pružatelje usluga povjerenja koji podliježu sličnim zahtjevima u skladu s člankom 19. Uredbe (EU) br. 910/2014.

6. Objavljene nacionalne strategije za kibersigurnost

	Država članica	Naziv strategije i dostupne poveznice
1.	Austrija	*Austrijska strategija za kibersigurnost* (2013.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf (EN)
2.	Belgija	*Osiguravanje kiberprostora* (2012.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ncss-be-fr (FR)
3.	Bugarska	*Kiberotporna Bugarska 2020.* (2016.) http://www.cyberbg.eu/ (BG)
4.	Hrvatska	*Nacionalna strategija kibernetičke sigurnosti Republike Hrvatske* (2015.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf (EN)
5.	Češka	*Nacionalna strategija kibersigurnosti Češke Republike za razdoblje od 2015. do 2020.* (2015.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (EN)
6.	Cipar	*Strategija kibersigurnosti Republike Cipra* (2012.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf (EN)
7.	Danska	*Danska strategija kibernetičke i informacijske sigurnosti* (2015.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/DK_NCSS.pdf (EN)
8.	Estonija	*Strategija kibersigurnosti* (2014.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf (EN)
9.	Finska	*Finska strategija kibersigurnosti* (2013.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf (EN)
10.	Francuska	*Francuska nacionalna strategija digitalne sigurnosti* (2015.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf (EN)

11.	Irska	*Nacionalna strategija kibersigurnosti 2015. – 2017.* (2015.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf (EN)
12.	Italija	*Nacionalni strateški okvir za sigurnost kiberprostora* (2013.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf (EN)
13.	Njemačka	*Strategija kibersigurnosti za Njemačku* (2016.) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/ModerneVerwaltung-OeffentlicherDienst/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile (DE)
14.	Mađarska	*Nacionalna strategija kibersigurnosti Mađarske* (2013.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf (EN)
15.	Latvija	*Strategija kibersigurnosti Latvije 2014. – 2018.* (2014.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (EN)
16.	Litva	*Program za razvoj elektroničke informacijske sigurnosti (kibersigurnosti) za razdoblje 2011. – 2019.* (2011.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf (EN)
17.	Luksemburg	*Nacionalna strategija za kibersigurnost II. (2015.)* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf (EN)
18.	Malta	*Zelena knjiga Nacionalna strategija kibersigurnosti* (2015.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGreenPaper.pdf (EN)
19.	Nizozemska	*Nacionalna strategija kibersigurnosti 2. (2013.)* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf (EN)
20.	Poljska	*Politika zaštite kiberprostora Republike Poljske* (2013.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf (EN)
21.	Rumunjska	*Strategija kibersigurnosti Rumunjske* (2011.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf (RO)
22.	Portugal	*Nacionalna strategija sigurnosti kiberprostora* (2015.) https://www.enisa.europa.eu/topics/national-cyber-security-

		strategies/ncss-map/portuguese-national-cyber-security-strategy/view (EN)
23.	Slovačka	*Plan kibersigurnosti Slovačke Republike za razdoblje 2015. – 2020.* (2015.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 (EN)
24.	Slovenija	*Strategija kibersigurnosti kojom se uspostavlja sustav za osiguranje visoke razine kibersigurnosti* (2016.) http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf (EN)
25.	Španjolska	*Nacionalna strategija kibersigurnosti* (2013.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf (EN)
26.	Švedska	*Švedska nacionalna strategija kibersigurnosti* (2017.) http://www.government.se/49edf4/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy.pdf (EN)
27.	Ujedinjena Kraljevina	*Nacionalna strategija kibersigurnosti (2016. – 2017.)* (2016.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf (EN)

7. Popis dobre prakse i preporuka ENISA-e.

Za odgovore na incidente

- ✓ Strategije za odgovore na incidente i suradnju u slučaju kiberkriza[46]

Za rješavanje incidenata

- ✓ Projekt automatizacije rješavanja incidenata[47]
- ✓ Vodič dobre prakse za upravljanje incidentima[48]

Za razvrstavanje incidenata i taksonomiju

- ✓ Pregled postojećih taksonomija[49]
- ✓ Vodič dobre prakse za uporabu taksonomija za sprječavanje i otkrivanje incidenata[50]

Za zrelost CSIRT-ova

- ✓ Izazovi za nacionalne CSIRT-ove u Europi 2016.: Studija o zrelosti CSIRT-ova[51]
- ✓ Studija o zrelosti CSIRT-ova – Postupak evaluacije[52]
- ✓ Smjernice za nacionalne i državne CSIRT-ove tome kako procijeniti zrelost[53]

Za jačanje kapaciteta i osposobljavanje CSIRT-ova

- ✓ Vodič dobre prakse o metodologijama osposobljavanja[54]

Za informacije o postojećim CSIRT-ovima u Europi – Pregled CSIRT-ova po državama[55]

[46] ENISA, *Strategije za odgovore na incidente i suradnju u slučaju kiberkriza (2016.).* Dostupno na:https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation
[47] Više informacija na: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation
[48] ENISA, *Vodič dobre prakse za upravljanje incidentima (2010.).* Dostupno na:https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management
[49] Više informacija na: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies
[50] ENISA, *Vodič dobre prakse za uporabu taksonomija za sprječavanje i otkrivanje incidenata* (2017). Dostupno na:https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection
[51] ENISA, *Izazovi za nacionalne CSIRT-ove u Europi 2016.: Studija o zrelosti CSIRT-ova (2017.).* Dostupno na:https://www.enisa.europa.eu/publications/study-on-csirt-maturity
[52] *ENISA, Studija o zrelosti CSIRT-ova – Postupak evaluacije (2017.)* Dostupno na:https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process
[53] ENISA, sposobnosti CSIRT-ova. *Kako procijeniti zrelost? Smjernice za nacionalne i državne CSIRT-ove (2016.)* Dostupno na: https://www.enisa.europa.eu/publications/csirt-capabilities
[54] ENISA, *Vodič dobre prakse o metodologijama osposobljavanja* (2014.). Dostupno na:https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies
[55] Više informacija na: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map