EUROPOS
KOMISIJA

Briuselis, 2017 10 04
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

PRIEDAS

prie

KOMISIJOS KOMUNIKATO EUROPOS PARLAMENTUI IR TARYBAI

Racionaliausias tinklų ir informacijos saugumas. Kaip veiksmingai įgyvendinti Direktyvą (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti

TURINYS

PRIEDAS

1. Įvadas

Šiuo priedu siekiama prisidėti prie veiksmingo Direktyvos (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti[1] (toliau – TIS Direktyva, arba Direktyva) taikymo, įgyvendinimo ir vykdymo užtikrinimo ir padėti valstybėms narėms užtikrinti, kad būtų veiksmingai taikoma ES teisė. Kalbant konkrečiau, juo siekiama trijų konkrečių tikslų: a) suteikti nacionalinėms institucijoms daugiau aiškumo dėl Direktyvoje joms nustatytų pareigų; b) užtikrinti, kad būtų veiksmingai vykdomos subjektams, turintiems su saugumo ir pranešimo apie incidentus reikalavimais susijusių pareigų, Direktyvoje nustatytos pareigos ir c) apskritai padėti suteikti visiems atitinkamiems subjektams teisinio tikrumo.

Šiuo tikslu šiame priede pateikiamos rekomendacijos dėl toliau nurodytų aspektų, kurie yra labai svarbūs norint pasiekti TIS direktyvos tikslą, t. y. užtikrinti aukštą bendrą tinklų ir informacinių sistemų saugumo lygį ES, kuris yra mūsų visuomenės ir ekonomikos veikimo pagrindas. Tai yra šie aspektai:

- valstybių narių pareiga priimti nacionalinę tinklų ir informacinių sistemų saugumo strategiją (2 skirsnis);
- nacionalinių kompetentingų institucijų, bendrųjų informacinių centrų ir reagavimo į kompiuterinius saugumo incidentus tarnybų įsteigimas (3 skirsnis);
- saugumo ir pranešimo apie incidentus reikalavimai, taikomi esminių paslaugų operatoriams ir skaitmeninių paslaugų teikėjams (4 skirsnis) ir
- TIS direktyvos ir kitų teisės aktų tarpusavio santykis (5 skirsnis).

Rengdama šias rekomendacijas, Komisija pasinaudojo rengiant Direktyvą surinkta informacija ir analizės rezultatais bei iš Europos Sąjungos tinklų ir informacijos apsaugos agentūros (ENISA) ir Bendradarbiavimo grupės gautais duomenimis. Ji taip pat pasinaudojo konkrečių valstybių narių įgyta patirtimi. Prireikus Komisija atsižvelgė į pagrindinius ES teisės aiškinimo principus: TIS direktyvos formuluotę, kontekstą ir tikslus. Turint omenyje, kad Direktyva nebuvo perkelta į nacionalinę teisę, Europos Sąjungos Teisingumo Teismas (toliau – Teisingumo Teismas) ar nacionaliniai teismai dar nėra priėmę jokių sprendimų. Todėl nėra galimybės kaip rekomendacijomis remtis teismų praktika.

Surinkus šią informaciją viename dokumente, valstybėms narėms bus parengta gera Direktyvos apžvalga, jos galės į šią informaciją atsižvelgti rengdamos nacionalinės teisės aktus. Kartu Komisija pabrėžia, kad šis priedas neturi privalomos galios ir jame nesiekiama

[1] 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti. Direktyva įsigaliojo 2016 m. rugpjūčio 8 d.

nustatyti naujų taisyklių. Pagrindinė ES teisės aiškinimo kompetencija priklauso Teisingumo Teismui.

2. Nacionalinė tinklų ir informacinių sistemų saugumo strategija

Pagal TIS direktyvos 7 straipsnį valstybės narės privalo priimti nacionalinę tinklų ir informacinių sistemų saugumo strategiją, kuri gali būti laikoma lygiaverte nacionalinei kibernetinio saugumo strategijai (toliau – NKSS). Nacionalinės strategijos funkcija – nustatyti kibernetinio saugumo strateginius tikslus ir tinkamą politiką bei reguliavimo priemones. NKSS koncepcija plačiai vartojama tarptautiniu mastu ir Europoje, visų pirma kai kalbama apie ENISA bendradarbiavimą su valstybėmis narėmis rengiant nacionalines strategijas; šio bendradarbiavimo rezultatas – neseniai parengtas NKSS gerosios patirties vadovas[2].

Šiame skirsnyje Komisija nurodo, kaip TIS direktyva reikalaujant priimti patikimas nacionalines tinklų ir informacinių sistemų saugumo strategijas stiprinama valstybių narių parengtis (7 straipsnis). Jame nagrinėjami šie aspektai: a) strategijos taikymo sritis ir b) strategijos turinys ir priėmimo tvarka.

Kaip paaiškinta toliau, Direktyvos tikslams pasiekti labai svarbu tinkamai perkelti TIS direktyvos 7 straipsnį į nacionalinę teisę, o tam reikia skirti pakankamai finansinių ir žmogiškųjų išteklių.

2.1. Nacionalinės strategijos taikymo sritis

Pagal 7 straipsnio formuluotę pareiga priimti NKSS taikoma tik II priede nurodytiems sektoriams (t. y. energetikos, transporto, bankininkystės, finansų rinkų, sveikatos priežiūros, geriamojo vandens tiekimo ir skirstymo ir skaitmeninės infrastruktūros sektoriams) ir III priede nurodytoms paslaugoms (elektroninei prekyvietei, interneto paieškos sistemai ir debesijos kompiuterijos paslaugai).

Direktyvos 3 straipsnyje įtvirtintas minimalaus suderinimo principas, pagal kurį valstybės narės gali priimti arba palikti galioti nuostatas aukštesniam informacinių sistemų tinklo saugumo lygiui užtikrinti. Taikydamos šį principą pareigai priimti NKSS, valstybės narės gali įtraukti daugiau sektorių ir paslaugų, negu nurodyta Direktyvos II ir III prieduose.

Komisijos nuomone, atsižvelgiant į TIS direktyvos tikslą užtikrinti aukštą bendrą tinklų ir informacinių sistemų saugumo lygį Sąjungoje[3], būtų tikslinga parengti nacionalinę strategiją, apimančią visus aktualius visuomenės ir ekonomikos aspektus, o ne tik atitinkamai TIS direktyvos II ir III prieduose nurodytus sektorius ir skaitmenines paslaugas. Tai atitinka tarptautinę gerąją patirtį (žr. toliau nurodytą Tarptautinės telekomunikacijų sąjungos (ITU) vadovą ir EBPO analizę) ir TIS direktyvos nuostatas.

[2] ENISA, „Nacionalinės kibernetinio saugumo strategijos rengimo geroji patirtis“ (angl. *National Cyber-Security Strategy Good Practice*), 2016 m. Paskelbta: https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

[3] Žr. 1 straipsnio 1 dalį.

Kaip paaiškinta toliau, tai ypač svarbu viešojo administravimo institucijoms, atsakingoms už sektorius ir paslaugas, neįtrauktus į Direktyvos II ir III priedus. Viešojo administravimo institucijos gali tvarkyti neskelbtiną informaciją, todėl šį aspektą reikia įtraukti į NKSS ir valdymo planus, kuriais užkertamas kelias informacijos nutekėjimui ir užtikrinama tinkama šios informacijos apsauga.

2.2. Nacionalinių strategijų turinys ir priėmimo tvarka

Pagal TIS direktyvos 7 straipsnį į NKSS turi būti įtraukti bent šie punktai:

i) nacionalinės tinklų ir informacinių sistemų saugumo strategijos tikslai ir prioritetai;
ii) valdymo sistema, skirta nacionalinės strategijos tikslams ir prioritetams įgyvendinti;
iii) parengties, reagavimo ir atkūrimo priemonių, įskaitant viešojo ir privačiojo sektorių bendradarbiavimą, nustatymas;
iv) švietimo, informuotumo didinimo ir mokymo programų nurodymas;
v) mokslinių tyrimų ir plėtros planų nurodymas;
vi) rizikos vertinimo planas, skirtas rizikai nustatyti ir
vii) subjektų, dalyvaujančių įgyvendinant strategiją, sąrašas.

Nei 7 straipsnyje, nei atitinkamoje 29 konstatuojamojoje dalyje nenurodyti NKSS priėmimo reikalavimai ir smulkiau neapibrėžta, koks turi būti NKSS turinys. Kalbant apie procesą ir papildomus elementus, susijusius su NKSS turiniu, Komisija mano, kad, priimant NKSS, reikia laikytis toliau išdėstyto požiūrio. Tai grindžiama valstybių narių ir trečiųjų valstybių įgytos patirties, susijusios su tuo, kaip valstybės narės parengė savo strategijas, analize. Išsamesnės informacijos galima gauti pasinaudojus ENISA mokomąja NKSS rengimo priemone, t. y. ENISA svetainėje pateiktais vaizdo įrašais ir atsisiųsdinama medžiaga[4].

2.3. Procesas ir spręstini klausimai

Nacionalinės strategijos projekto rengimas ir priėmimas yra sudėtingas ir daugialypis procesas, todėl, norint, kad jis būtų veiksmingas ir sėkmingas, jame turi nuolat dalyvauti kibernetinio saugumo ekspertai bei pilietinė visuomenė ir jis turi būti derinamas su nacionaliniu politiniu procesu. Būtina sąlyga – administracinė parama vadovams bent valstybės sekretoriaus arba atitinkamu lygmeniu pagrindinėje ministerijoje, taip pat politinė parama. Kad NKSS būtų sėkmingai priimta, galima apsvarstyti galimybę taikyti penkių etapų procesą (žr. 1 pav.).

Pirmasis etapas. **Pagrindinių principų ir strateginių tikslų nustatymas**

Visų pirma nacionalinės kompetentingos institucijos turėtų apibrėžti tam tikrus pagrindinius elementus, kurie turi būti įtraukti į NKSS, t. y. nurodyti, kokių rezultatų siekiama, Direktyvoje jie įvardyti kaip „tikslai ir prioritetai“, kaip tokiais rezultatais papildoma nacionalinė socialinė ir ekonominė politika ir ar jie suderinami su Europos Sąjungos valstybės narės privilegijomis ir įsipareigojimais. Tikslai turėtų būti konkretūs, išmatuojami, pasiekiami, realūs ir įvykdytini per nustatytą laiką. Tipinis pavyzdys: „Užtikrinsime, kad ši [per nustatytą laiką įvykdytina]

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

strategija būtų grindžiama griežtai apibrėžtais ir išsamiais rodikliais, pagal kuriuos vertinsime pažangą siekiant reikiamų rezultatų.“[5]

Pirmiau nurodytas procesas taip pat apima politinį vertinimą, ar galima gauti pakankamai lėšų strategijos įgyvendinimui finansuoti. Šiuo tikslu taip pat reikia apibrėžti numatomą strategijos taikymo sritį ir įvairias viešojo ir privačiojo sektorių suinteresuotųjų subjektų, kurie turėtų dalyvauti nustatant įvairius tikslus ir rengiant įvairias priemones, kategorijas.

Šį pirmąjį etapą būtų galima įgyvendinti rengiant vyresniesiems ministerijų pareigūnams ir politikams skirtus tikslinius praktinius seminarus, kuriuos vestų kibernetinio saugumo specialistai, turintys profesionalaus komunikavimo įgūdžių ir galintys išaiškinti menko kibernetinio saugumo arba jo nebuvimo padarinius šiuolaikinei skaitmeninei ekonomikai ir visuomenei.

Antrasis etapas. **Strategijos turinio rengimas**

Strategijoje turi būti nurodytos įgyvendinimo priemonės, veiksmai, kuriuos reikia atlikti per tam tikrą laiką, ir pagrindiniai veiklos rezultatų rodikliai, pagal kuriuos, praėjus nustatytam įgyvendinimo laikotarpiui, ją reikia vertinti, tobulinti ir gerinti. Šiomis priemonėmis turėtų būti padedama siekti tikslų, prioritetų ir rezultatų, kurie nustatyti kaip pagrindiniai principai. Poreikis įtraukti įgyvendinimo priemones nustatytas TIS direktyvos 7 straipsnio 1 dalies c punkte.

Rekomenduojama strategijos rengimo procesui valdyti ir nuomonių teikimui palengvinti sudaryti iniciatyvinę grupę, kuriai pirmininkautų vadovaujančioji ministerija. Tai būtų galima pasiekti iš atitinkamų pareigūnų ir ekspertų sudarius keletą strategijos rengimo grupių, kurios dirbtų pagrindinėse bendrosiose, pvz., rizikos vertinimo, nenumatytų atvejų planavimo, incidentų valdymo, gebėjimų ugdymo, informuotumo didinimo, mokslinių tyrimų ir pramonės plėtros, ir kitose srityse. Kiekvienas sektorius (pvz., energetikos, transporto ir kt.) atskirai taip pat būtų paragintas įvertinti savo dalyvavimo procese poveikį, be kita ko, išteklių skyrimą, ir bendradarbiauti su paskirtaisiais esminių paslaugų operatoriais bei pagrindiniais skaitmeninių paslaugų teikėjais nustatant prioritetus ir teikiant pasiūlymus strategijos rengėjams. Suinteresuotųjų subjektų dalyvavimas taip pat labai svarbus turint omenyje poreikį užtikrinti darnų Direktyvos įgyvendinimą įvairiuose sektoriuose, kartu atsižvelgiant į jų specifiką.

Trečiasis etapas. **Valdymo sistemos sukūrimas**

Kad būtų veiksminga ir efektyvi, valdymo sistema turėtų būti sukurta atsižvelgiant į pagrindinių suinteresuotųjų subjektų nuomones, rengiant strategiją nustatytus prioritetus ir nacionalinių administracinių bei politinių struktūrų apribojimus ir aplinkybes. Pageidautina, kad būtų atsiskaitoma tiesiogiai politiniam lygmeniui, o sistema galėtų priimti sprendimus ir skirstyti išteklius, taip pat kad būtų atsižvelgiama į kibernetinio saugumo ekspertų ir pramonės suinteresuotųjų subjektų nuomones. TIS direktyvos 7 straipsnio 1 dalies b punkte

[5] Ištrauka iš Jungtinės Karalystės 2016–2021 m. nacionalinės kibernetinio saugumo strategijos, p. 67.

kalbama apie valdymo sistemą ir konkrečiai reikalaujama, kad ji apimtų „valdžios įstaigų ir kitų atitinkamų subjektų [...] įsipareigojimus“.

Ketvirtasis etapas. **Strategijos projekto parengimas ir peržiūra**

Šiame etape strategijos projektas turėtų būti parengtas ir peržiūrėtas atliekant stiprybių, silpnybių, galimybių ir grėsmių (SSGG) analizę, pagal kurios rezultatus galėtų būti nustatyta, ar būtina persvarstyti turinį. Po vidaus peržiūros turėtų būti surengtos konsultacijos su suinteresuotaisiais subjektais. Taip pat būtų labai svarbu surengti viešas konsultacijas, per kurias visuomenei būtų išaiškinta siūlomos strategijos svarba, susipažinta su visų galimų šaltinių nuomonėmis ir būtų siekiama gauti paramą, reikalingą strategijai įgyvendinti.

Penktasis etapas. **Oficialus priėmimas**

Paskutiniame etape strategija turėtų būti oficialiai priimta politiniu lygmeniu ir jai turėtų būti skirtas pakankamas biudžetas, iš kurio būtų matyti, kad atitinkama valstybė narė rimtai vertina kibernetinį saugumą. Norėdama pasiekti TIS direktyvos tikslus Komisija ragina, kad valstybės narės, teikdamos Komisijai nacionalinės strategijos dokumentus pagal 7 straipsnio 3 dalį, pateiktų informaciją apie biudžetą. Įsipareigojimai dėl biudžeto ir būtini žmogiškieji ištekliai yra labai svarbūs strategijai ir Direktyvai veiksmingai įgyvendinti. Kadangi kibernetinis saugumas tebėra gana nauja ir sparčiai besiplečianti viešosios politikos sritis, daugeliu atvejų reikalingos naujos investicijos, net jeigu, atsižvelgiant į bendrą valstybės finansų padėtį, būtina mažinti išlaidas ir taupyti.

Patarimų dėl nacionalinių strategijų rengimo proceso ir turinio galima gauti iš įvairių viešųjų ir akademinių šaltinių, pvz., ENISA[6], ITU[7], EBPO[8], Visuotinio kibernetinio saugumo žinių forumo (angl. *Global Forum for Cyber Expertise*) ir Oksfordo universiteto[9].

[6] ENISA, „Nacionalinės kibernetinio saugumo strategijos rengimo geroji patirtis“ (angl. *National Cyber-Security Strategy Good Practice*), 2016 m. Paskelbta: https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

[7] ITU, Nacionalinės kibernetinio saugumo strategijos rengimo vadovas (angl. *National Cybersecurity Strategy Guide*), 2011 m. Paskelbta: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.
2017 m. ITU taip pat išleis Nacionalinės kibernetinio saugumo strategijos rengimo priemonių rinkinį (žr. pranešimą http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf).

[8] EBPO, „Lūžis kibernetinio saugumo politikos formavimo srityje. Naujos kartos nacionalinių kibernetinio saugumo strategijų analizė“ (angl. *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies*), 2012 m. Paskelbta: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.

[9] Visuotinio kibernetinio saugumo gebėjimų centras ir Oksfordo universitetas, „Valstybėms skirtas kibernetinio saugumo gebėjimų brandos modelis. Pataisytasis leidimas“ (angl. *Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition*), 2016 m. Paskelbta: https://www.thegfce.com/binaries/gfce/documents/publications/2017/02/13/cybersecurity-cmm-for-nations/CMM+revised+edition.pdf.

2.4. Konkretūs veiksmai, kurių valstybės narės turi imtis iki Direktyvos perkėlimo į nacionalinę teisę termino

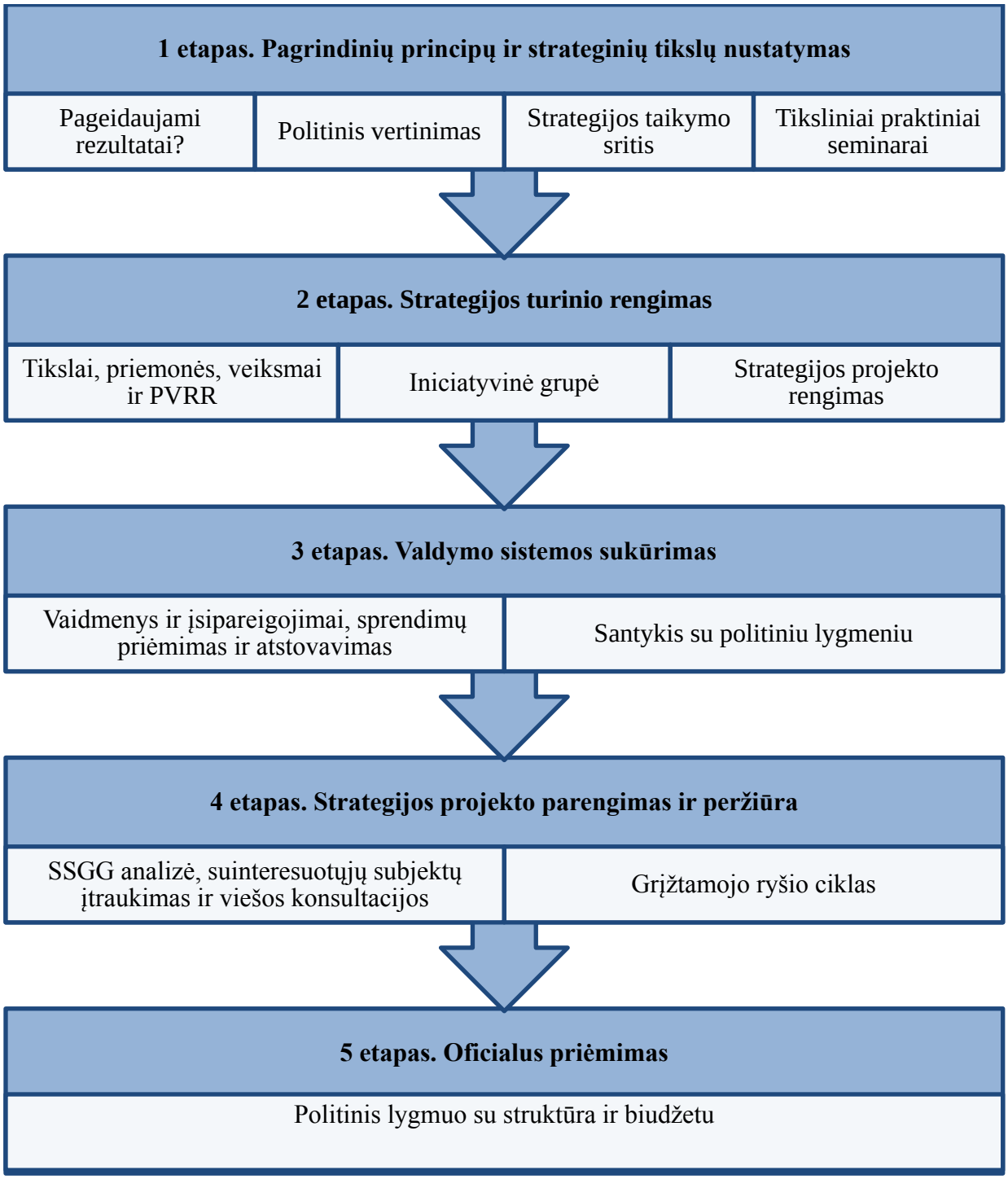
Prieš priimant Direktyvą, beveik visos valstybės narės[10] jau buvo paskelbusios dokumentus, nurodytus kaip NKSS. Šio priedo 6 skirsnyje pateiktas kiekvienoje valstybėje narėje šiuo metu taikomų strategijų sąrašas[11]. Jose paprastai nustatyti strateginiai principai, gairės ir tikslai, o kai kuriais atvejais – konkrečios su kibernetiniu saugumu susijusios rizikos mažinimo priemonės.

Atsižvelgiant į tai, kad kai kurios iš šių strategijų buvo priimtos iki TIS direktyvos priėmimo, jos nebūtinai apima visus 7 straipsnyje nurodytus elementus. Kad užtikrintų tinkamą Direktyvos perkėlimą į nacionalinę teisę, valstybės narės turės atlikti trūkumų analizę – savo NKSS turinį II priede išvardytų sektorių ir III priede išvardytų paslaugų srityse sulyginti su 7 straipsnyje nustatytais septyniais atskirais reikalavimais. Tada nustatytus trūkumus galima pašalinti atlikus esamos NKSS peržiūrą arba nusprendus visiškai peržiūrėti savo nacionalinės TIS strategijos principus. Pirmiau pateiktos NKSS priėmimo proceso gairės taip pat aktualios esamų NKSS peržiūrai ir atnaujinimui.

[10] Išskyrus Graikiją, kurioje nacionalinė kibernetinio saugumo strategija rengiama nuo 2014 m. (žr. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-greece/view).

[11] Ši informacija pagrįsta agentūros ENISA pateikta NKSS apžvalga, žr. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map.

1 pav. Penkių etapų NKSS priėmimo procesas



3. TIS direktyva. Nacionalinės kompetentingos institucijos, bendrieji informaciniai centrai ir reagavimo į kompiuterinius saugumo incidentus tarnybos (CSIRT)

Pagal Direktyvos 8 straipsnio 1 dalį jos taikymui stebėti valstybės narės privalo paskirti vieną ar daugiau nacionalinių kompetentingų institucijų, kurių veikla apima bent II priede nurodytus sektorius ir III priede nurodytas paslaugas. Valstybės narės šį vaidmenį gali paskirti esamai institucijai arba institucijoms.

Šiame skirsnyje dėmesys sutelktas į tai, kaip TIS direktyva, reikalaujant turėti veiksmingai veikiančias nacionalines kompetentingas institucijas ir reagavimo į kompiuterinius saugumo incidentus tarnybas (toliau – CSIRT), gerinama valstybių narių parengtis. Konkrečiau šiame skirsnyje aptariama pareiga paskirti nacionalines kompetentingas institucijas, taip pat bendrųjų informacinių centrų vaidmuo. Jame aptariamos trys temos: a) galimos nacionalinės valdymo struktūros (pvz., centralizuotas ir decentralizuotas modeliai ir t. t.) ir kiti reikalavimai; b) bendrojo informacinio centro vaidmuo ir c) reagavimo į kompiuterinius saugumo incidentus tarnybos.

3.1. Institucijų tipas

TIS direktyvos 8 straipsnyje reikalaujama, kad valstybės narės paskirtų nacionalines tinklų ir informacinių sistemų saugumo kompetentingas institucijas, t. y. aiškiai pripažįstama galimybė paskirti „vieną ar daugiau nacionalinių [...] kompetentingų institucijų“. Šis politinis sprendimas paaiškintas Direktyvos 30 konstatuojamojoje dalyje: „atsižvelgiant į nacionalinių valdymo struktūrų skirtumus ir siekiant išsaugoti jau veikiančias sektorių sistemas ar Sąjungos priežiūros ir reguliavimo įstaigas bei išvengti dubliavimo, valstybės narės turėtų turėti teisę paskirti daugiau nei vieną nacionalinę kompetentingą instituciją, atsakingą už užduočių, susijusių su esminių paslaugų operatorių bei skaitmeninių paslaugų teikėjų tinklų ir informacinių sistemų saugumu, vykdymą pagal šią direktyvą“.

Taigi valstybės narės gali laisvai pasirinkti, ar paskirti vieną centrinę instituciją, atsakingą už visus sektorius ir paslaugas, kurioms taikoma Direktyva, ar kelias institucijas, atsižvelgiant, pvz., į sektoriaus tipą.

Spręsdamos, kurį metodą taikyti, valstybės narės gali remtis nacionalinių metodų taikymo pagal esamus teisės aktus, kuriais reglamentuojama ypatingos svarbos informacinės infrastruktūros apsauga, patirtimi. Kaip nurodyta 1 lentelėje, valstybės narės, nacionaliniu lygmeniu skirstydamos atsakomybę už ypatingos svarbos informacinės infrastruktūros apsaugą, nusprendė taikyti centralizuotą arba decentralizuotą metodą. Nacionaliniai pavyzdžiai čia pateikti tik informaciniais tikslais, siekiant atkreipti valstybių narių dėmesį į esamas organizacines sistemas. Todėl Komisija neteigia, kad atitinkamų šalių naudotas ypatingos svarbos informacinės infrastruktūros apsaugos modelis būtinai turėtų būti naudojamas TIS direktyvai perkelti į nacionalinę teisę.

Valstybės narės taip pat gali nuspręsti taikyti įvairias hibridines sistemas, apimančias ir centralizuoto, ir decentralizuoto metodų elementus. Tokie sprendimai gali būti priimami atsižvelgiant į ankstesnes nacionalines įvairių sektorių ir paslaugų, kuriems taikoma Direktyva, valdymo sistemas arba juos turi iš naujo priimti atitinkamos institucijos ir suinteresuotieji subjektai, identifikuojami kaip esminių paslaugų operatoriai ir skaitmeninių paslaugų teikėjai. Priimdamos sprendimus, valstybės narės taip pat gali remtis tokiais svarbiais veiksniais kaip specialistų patirtis kibernetinio saugumo srityje, išteklių skyrimo galimybės, suinteresuotųjų subjektų ir nacionalinių interesų tarpusavio santykis (pvz., ekonominės plėtros, viešojo saugumo ir kt. srityse).

3.2. Viešinimas ir papildomi susiję aspektai

Pagal 8 straipsnio 7 dalį valstybės narės turi Komisijai pranešti apie nacionalinių kompetentingų institucijų paskyrimą ir jų užduotis. Tai turi būti padaryta, kol nesuėjo Direktyvos perkėlimo į nacionalinę teisę terminas.

TIS direktyvos 15 ir 17 straipsniuose reikalaujama, kad valstybės narės užtikrintų, jog kompetentingos institucijos turėtų reikiamus įgaliojimus ir priemones tuose straipsniuose nustatytoms užduotims atlikti.

Be to, apie konkrečių subjektų paskyrimą nacionalinėmis kompetentingomis institucijomis turi būti skelbiama viešai. Direktyvoje nenurodyta, kaip tokį viešinimą užtikrinti. Atsižvelgdama į šio reikalavimo tikslą užtikrinti aukštą subjektų, kuriems taikoma TIS direktyva, ir plačiosios visuomenės informuotumo lygį ir remdamasi kitų (telekomunikacijų, bankininkystės, farmacijos) sektorių patirtimi, Komisija mano, kad šį poreikį būtų galima patenkinti, pvz., sukūrus gerai išreklamuotą portalą.

TIS direktyvos 8 straipsnio 5 dalyje reikalaujama, kad tokios institucijos turėtų „tinkamų išteklių“ pagal Direktyvą paskirtoms užduotims atlikti.

1 lentelė. Nacionaliniai ypatingos svarbos informacinės infrastruktūros apsaugos užtikrinimo metodai

2016 m. ENISA paskelbė skirtingų metodų, kuriuos valstybės narės taiko savo ypatingos svarbos informacinei infrastruktūrai apsaugoti, tyrimą[12]. Yra du valstybėse narėse taikomi ypatingos svarbos informacinės infrastruktūros apsaugos valdymo profiliai, kuriais galima vadovautis perkeliant TIS direktyvą į nacionalinę teisę.

1 profilis. Decentralizuotas metodas – kelios sektorinės institucijos, atsakingos už konkrečius sektorius ir paslaugas, nurodytus atitinkamai Direktyvos II ir III prieduose.

Decentralizuotam metodui būdinga:

(i) subsidiarumo principas,
(ii) glaudus viešųjų įstaigų bendradarbiavimas,
(iii)konkretiems sektoriams skirti teisės aktai.

Subsidiarumo principas

Užuot įsteigus arba paskyrus vieną įstaigą, kuriai tektų visa atsakomybė, taikant decentralizuotą metodą laikomasi subsidiarumo principo. Tai reiškia, kad atsakomybė už įgyvendinimą tenka sektorinei institucijai, kuri geriausiai supranta vietos sektorių ir jau yra užmezgusi santykius su suinteresuotaisiais subjektais. Pagal šį principą sprendimus priima institucijos, esančios arčiausiai tų subjektų, kuriems daromas poveikis.

Glaudus viešųjų įstaigų bendradarbiavimas

Dėl viešųjų įstaigų, veikiančių ypatingos svarbos informacinės infrastruktūros apsaugos srityje, įvairovės daugelis valstybių narių parengė bendradarbiavimo sistemas, kad galėtų koordinuoti įvairių institucijų darbą ir pastangas. Šios bendradarbiavimo sistemos gali būti neoficialūs tinklai arba labiau institucionalizuoti forumai ar susitarimai. Vis dėlto šios bendradarbiavimo sistemos naudojamos tik įvairių viešųjų įstaigų tarpusavio keitimosi informacija ir veiksmų koordinavimo tikslais, tačiau neturi įgaliojimų priimti joms privalomų sprendimų.

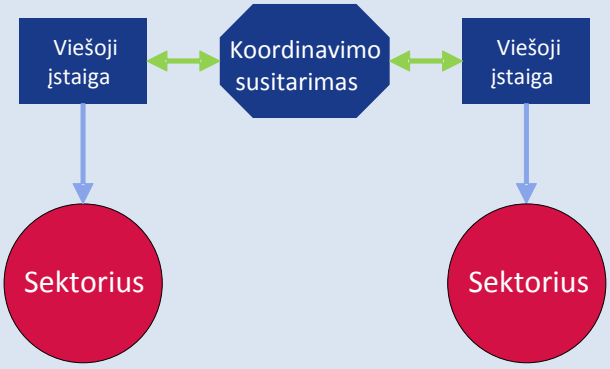
Konkretiems sektoriams skirti teisės aktai

Šalys, ypatingos svarbos sektoriams taikančios decentralizuotą metodą, dažnai vengia priimti ypatingos svarbos informacinės infrastruktūros apsaugai skirtus teisės aktus. Priimami konkretiems sektoriams skirti įstatymai ir kiti teisės aktai, todėl įvairiuose sektoriuose jie gali labai skirtis. Šis metodas pranašesnis tuo, kad jį taikant su TIS susijusios priemonės derinamos su galiojančiais konkretiems sektoriams skirtais teisės aktais ir taip siekiama didesnio sektoriaus pritarimo ir atitinkamos institucijos užtikrinamo veiksmingesnio šių priemonių įgyvendinimo.

[12] ENISA, „Ypatingos svarbos informacinės infrastruktūros apsaugos padėties apžvalga, analizė ir rekomendacijos“ (angl. *Stocktaking, Analysis and Recommendations on the protection of CIIs*), 2016 m. Paskelbta: https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

Kyla didelė rizika, kad, taikant išgrynintą decentralizuotą metodą, Direktyva įvairiems sektoriams ir paslaugoms bus taikoma ne taip nuosekliai. Šiuo atveju Direktyvoje ryšiams tarpvalstybiniais klausimais palaikyti numatytas bendrasis nacionalinis informacinis centras, atitinkama valstybė narė šiai įstaigai taip pat gali pavesti užtikrinti įvairių nacionalinių kompetentingų institucijų veiksmų vidaus koordinavimą ir jų tarpusavio bendradarbiavimą pagal Direktyvos 10 straipsnį.

2 pav. Decentralizuotas metodas



Decentralizuoto metodo taikymo pavyzdžiai

Geras šalies, taikančios decentralizuotą ypatingos svarbos infrastruktūros objektų apsaugos metodą, pavyzdys yra Švedija. Ši šalis taiko sisteminę perspektyvą, o tai reiškia, kad pagrindines ypatingos svarbos informacinės infrastruktūros apsaugos užduotis, pvz., gyvybiškai svarbių paslaugų ir ypatingos svarbos infrastruktūros objektų identifikavimą, operatorių veiksmų koordinavimą ir paramos jiems teikimą, reguliavimo užduotis, taip pat avarinės parengties priemonių taikymą, pavesta vykdyti skirtingoms įstaigoms ir savivaldybėms. Tarp šių įstaigų yra Švedijos civilinės saugos agentūra (MSB), Švedijos pašto ir telekomunikacijų agentūra (PTS) ir kelios Švedijos gynybos, karo reikalų ir teisėsaugos agentūros.

Siekdama koordinuoti įvairių įstaigų ir viešųjų subjektų veiksmus, Švedijos vyriausybė sukūrė bendradarbiavimo tinklą, sudarytą iš institucijų, turinčių specialius visuomeninius informacijos apsaugos užtikrinimo įgaliojimus. Šią bendradarbiavimo informacijos apsaugos klausimais grupę (toliau – SAMFI) sudaro įvairių institucijų atstovai, kurie susitinka kelis kartus per metus aptarti su nacionaliniu informacijos saugumu susijusių klausimų. SAMFI nagrinėjamos teminės sritys daugiausia susijusios su politinėmis ir strateginėmis sritimis ir apima tokias temas kaip techniniai klausimai ir standartizavimas, nacionalinė ir tarptautinė informacijos saugumo srities plėtra ar IT incidentų valdymas ir prevencija. (Švedijos civilinės saugos agentūra (MSB), 2015 m.).

Švedija nėra priėmusi bendro ypatingos svarbos informacinės infrastruktūros apsaugos įstatymo, kuris būtų taikomas visų sektorių ypatingos svarbos informacinės infrastruktūros

objektų operatoriams. Už teisės aktų, kuriais nustatomos konkrečių sektorių įmonių pareigos, priėmimą atsako atitinkamos valdžios institucijos. Pavyzdžiui, MSB turi teisę skelbti valdžios institucijoms skirtas informacijos saugumo taisykles, o PTS, remdamasi antrinės teisės aktais, gali reikalauti, kad operatoriai įgyvendintų tam tikras technines ar organizacines saugumo priemones.

Kitas šalies, kuriai būdingos šio profilio savybės, pavyzdys yra Airija. Airija laikosi subsidiarumo doktrinos, pagal kurią kiekviena ministerija atsako už ypatingos svarbos informacinės infrastruktūros objektų identifikavimą ir rizikos vertinimą savo sektoriuje. Be to, nacionaliniu lygmeniu nepriimta jokių konkrečių ypatingos svarbos informacinės infrastruktūros apsaugos teisės aktų. Teisės aktai ir toliau taikomi konkretiems sektoriams, daugiausia yra energetikos ir telekomunikacijų sektoriui skirtų teisės aktų (2015 m.). Kiti pavyzdžiai yra Austrija, Kipras ir Suomija.

2 profilis. Centralizuotas metodas – viena centrinė institucija yra kompetentinga klausimais, susijusiais su visais sektoriais ir paslaugomis, nurodytais atitinkamai Direktyvos II ir III prieduose.

Centralizuotam metodui būdinga:

i) už visus sektorius atsakinga centrinė institucija,
ii) išsamūs teisės aktai.

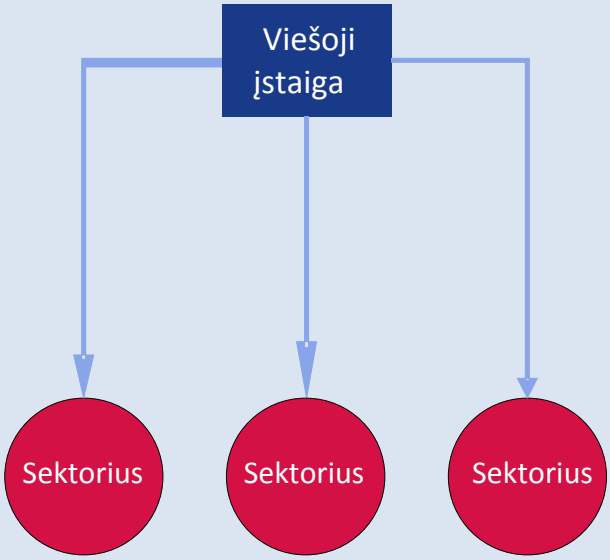
Už visus sektorius atsakinga centrinė institucija

Centralizuotą metodą taikančios valstybės narės yra įsteigusios institucijas, atsakingas už kelis arba visus ypatingos svarbos sektorius ir turinčias plačias kompetencijas tose srityse, arba yra išplėtusios esamų institucijų įgaliojimus. Šios pagrindinės už ypatingos svarbos informacinės infrastruktūros apsaugą atsakingos institucijos vykdo kelias užduotis, pvz., nenumatytų atvejų planavimą, ekstremaliųjų situacijų valdymą, reguliavimo užduotis ir paramos privatiems operatoriams teikimą. Daugeliu atvejų nacionalinės ar valstybinės CSIRT yra pagrindinės už ypatingos svarbos informacinės infrastruktūros apsaugą atsakingos institucijos dalis. Tikėtina, kad, atsižvelgiant į bendrą kibernetinio saugumo srities įgūdžių trūkumą, centrinėje institucijoje bus sutelkta daugiau kibernetinio saugumo srities žinių nei keliose sektorinėse institucijose.

Išsamūs teisės aktai

Išsamiais teisės aktais nustatomos visų ypatingos svarbos informacinės infrastruktūros objektų operatorių visuose sektoriuose pareigos ir jiems taikomi reikalavimai. Tai galima pasiekti priimant naujus išsamius įstatymus arba papildant esamus konkretiems sektoriams skirtus teisės aktus. Laikantis šio požiūrio, būtų sudarytos palankios sąlygos nuosekliai taikyti TIS direktyvą visiems į ją įtrauktiems sektoriams ir paslaugoms. Taip būtų išvengta įgyvendinimo trūkumų, galinčių atsirasti, kai yra daug specialius įgaliojimus turinčių institucijų, rizikos.

3 pav. Centralizuotas metodas



Centralizuoto metodo taikymo pavyzdžiai

Geras centralizuotą metodą taikančios ES valstybės narės pavyzdys yra Prancūzija. 2011 m. Prancūzija Nacionalinę informacinių sistemų saugumo agentūrą (pranc. *Agence Nationale de la Sécurité des Systèmes d'Information*, ANSSI) paskelbė pagrindine nacionaline informacinių sistemų apsaugos institucija. ANNSI atlieka svarbią ypatingos svarbos operatorių priežiūros funkciją: agentūra gali nurodyti ypatingos svarbos operatoriams laikytis saugumo priemonių ir yra įgaliota atlikti jų saugumo auditą. Be to, tai yra ypatingos svarbos operatorių, kurie privalo agentūrai pranešti apie saugumo incidentus, bendrasis informacinis centras.

Įvykus saugumo incidentui, ANNSI ypatingos svarbos informacinės infrastruktūros apsaugos srityje veikia kaip nenumatytų atvejų agentūra ir sprendžia, kokių priemonių operatoriai turi imtis reaguodami į krizę. Vyriausybės veiksmai koordinuojami ANNSI operacijų centre. Operatyviniu lygmeniu grėsmes nustato ir į incidentus reaguoja Prancūzijos Kompiuterinių incidentų tyrimo tarnyba (CERT-FR), kuri yra ANNSI dalis.

Prancūzija įdiegė išsamią teisinę ypatingos svarbos informacinės infrastruktūros apsaugos sistemą. 2006 m. ministras pirmininkas nurodė parengti ypatingos svarbos infrastruktūros sektorių sąrašą. Remdamasi šiuo sąrašu, kuriame identifikuota dvylika gyvybiškai svarbių sektorių, vyriausybė nustatė apie 250 ypatingos svarbos operatorių. 2013 m. paskelbtas Karinio planavimo įstatymas (LPM)[13]. Jame nustatytos įvairios ypatingos svarbos operatorių pareigos, pvz., pranešti apie incidentus arba įgyvendinti saugumo priemones. Šių reikalavimų privalo laikytis visi ypatingos svarbos operatoriai visuose sektoriuose (Prancūzijos Senatas, 2013 m.).

[13] *La loi de programmation militaire*.

3.3. TIS direktyvos 9 straipsnis. Reagavimo į kompiuterinius saugumo incidentus tarnybos (CSIRT)

9 straipsnyje reikalaujama, kad valstybės narės paskirtų vieną ar daugiau CSIRT, kurioms būtų pavesta valdyti su TIS direktyvos II priede nurodytais sektoriais ir III priede nurodytomis paslaugomis susijusią riziką ir incidentus. Atsižvelgdamos į Direktyvos 3 straipsnyje nustatytą minimalaus suderinimo reikalavimą, valstybės narės gali pavesti CSIRT vykdyti veiklą ir kituose sektoriuose, kuriems Direktyva netaikoma, pvz., viešojo administravimo sektoriuje.

Valstybės narės gali nuspręsti CSIRT įsteigti nacionalinėje kompetentingoje institucijoje[14].

3.4. Užduotys ir reikalavimai

TIS direktyvos I priede nustatytos tokios paskirtųjų CSIRT užduotys:

- stebėti incidentus nacionaliniu lygmeniu;
- teikti su įvairia rizika ir incidentais susijusius išankstinius įspėjimus, perspėjimus, skelbimus ir skleisti apie juos informaciją atitinkamiems suinteresuotiesiems subjektams;
- reaguoti į incidentus;
- užtikrinti operatyvią rizikos bei incidentų analizę ir informuotumą apie padėtį ir
- dalyvauti pagal 12 straipsnį sukurtame nacionalinių CSIRT tinkle.

14 straipsnio 3, 5 bei 6 dalyse ir 16 straipsnio 3, 6 bei 7 dalyse nustatytos specialios papildomos užduotys, susijusios su pranešimais apie incidentus, kai valstybė narė nusprendžia, kad CSIRT gali tokias funkcijas atlikti kartu su nacionalinėmis kompetentingomis institucijomis arba vietoj jų.

Perkeldamos Direktyvą į nacionalinę teisę, valstybės narės turi galimybę rinktis, kokį vaidmenį, susijusį su pranešimo apie incidentus reikalavimais, priskirti CSIRT. Pranešimai gali būti privalomai teikiami tiesiogiai CSIRT – taip būtų užtikrintas veiksmingas administravimas; valstybės narės taip pat gali pasirinkti, kad pranešimai būtų teikiami tiesiogiai nacionalinėms kompetentingoms institucijoms, o CSIRT turėtų teisę susipažinti su pranešimuose pateikta informacija. CSIRT visų pirma yra suinteresuotos kartu suinteresuotaisiais subjektais spręsti problemas, susijusias su kibernetinių incidentų (įskaitant tuos, kurie nėra itin svarbūs, kad apie juos būtų privaloma pranešti) prevencija, nustatymu, reagavimu į juos ir jų poveikio mažinimu, o užtikrinti, kad būtų laikomasi reikalavimų, privalo nacionalinės kompetentingos institucijos.

Pagal Direktyvos 9 straipsnio 3 dalį valstybės narės taip pat turi užtikrinti, kad tokios CSIRT turėtų prieigą prie saugios ir atsparios IRT infrastruktūros.

[14] Žr. 9 straipsnio 1 dalies paskutinį sakinį.

Direktyvos 9 straipsnio 4 dalyje reikalaujama, kad valstybės narės Komisiją informuotų apie paskirtųjų CSIRT incidentų valdymo proceso mastą ir pagrindinius elementus.

Valstybių narių paskirtoms CSIRT keliami reikalavimai pateikti TIS direktyvos I priede. CSIRT turi užtikrinti, kad jų ryšio paslaugos būtų lengvai prieinamos. CSIRT biurai ir pagalbinės informacinės sistemos veikia saugiose vietose ir gali užtikrinti veiklos tęstinumą. Be to, CSIRT turi turėti galimybę dalyvauti tarptautiniuose bendradarbiavimo tinkluose.

3.5. Pagalba steigiant CSIRT

Pagal Europos infrastruktūros tinklų priemonės (EITP) kibernetinio saugumo skaitmeninių paslaugų infrastruktūros (SPI) programą, siekiant padėti valstybių narių CSIRT gerinti savo gebėjimus ir tarpusavio bendradarbiavimą taikant keitimosi informacija mechanizmą, gali būti skiriamas didelis ES finansavimas. Pagal projektą SMART 2015/1089 rengiamu bendradarbiavimo mechanizmu siekiama sudaryti sąlygas greitam ir veiksmingam savanoriškam operatyviniam valstybių narių CSIRT bendradarbiavimui, t. y. taip siekiama padėti vykdyti pagal Direktyvos 12 straipsnį CSIRT tinklui pavestas užduotis.

Išsami informacija apie kvietimus teikti paraiškas dėl valstybių narių CSIRT gebėjimų stiprinimo pateikta Europos Komisijos Inovacijų ir tinklų programų vykdomosios įstaigos (INEA) svetainėje[15].

EITP kibernetinio saugumo SPI valdyba yra neoficiali struktūra, valstybių narių CSIRT teikianti politinio lygmens rekomendacijas ir pagalbą, kad padėtų joms stiprinti gebėjimus ir įgyvendinti savanoriško bendradarbiavimo mechanizmą.

Nauja įsteigta CSIRT arba TIS direktyvos I priede nurodytoms užduotims vykdyti paskirta CSIRT gali pasikliauti agentūros ENISA konsultacijomis ir patirtimi siekdama pagerinti savo veiklos rezultatus ir veiksmingai atlikti savo darbą[16]. Šiuo atžvilgiu verta pažymėti, kad valstybių narių CSIRT galėtų remtis tam tikru ENISA neseniai atliktu darbu. Visų pirma, kaip nurodyta šio priedo 7 skirsnyje, agentūra paskelbė nemažai su įvairiais CSIRT gebėjimais ir paslaugomis susijusių dokumentų ir tyrimų, kuriuose aprašoma geroji patirtis, pateikiamos techninio lygmens rekomendacijos ir CSIRT brandos lygio vertinimai. Be to, CSIRT tinklai taip pat keičiasi rekomendacijomis ir gerąja patirtimi ir pasauliniu (FIRST[17]), ir Europos („Trusted Introducer“, TI[18]) mastu.

3.6. Bendrojo informacinio centro vaidmuo

Pagal TIS direktyvos 8 straipsnio 3 dalį kiekviena valstybė narė turi paskirti nacionalinį bendrąjį informacinį centrą ryšiams palaikyti, kad būtų užtikrintas tarpvalstybinis bendradarbiavimas su kitų valstybių narių atitinkamomis institucijomis ir su Direktyva sukurta Bendradarbiavimo grupe bei CSIRT tinklu[19]. 31 konstatuojamojoje dalyje ir 8

[15] Paskelbta: https://ec.europa.eu/inea/en/connecting-europe-facility.
[16] Žr. TIS direktyvos 9 straipsnio 5 dalį.
[17] Reagavimo į incidentus ir saugumo tarnybų forumas (https://www.first.org/).
[18] https://www.trusted-introducer.org/
[19] Nacionalinių CSIRT tinklas, skirtas 12 straipsnyje nurodytam valstybių narių operatyviniam bendradarbiavimui palengvinti.

straipsnio 4 dalyje paaiškinta, kuo grindžiamas šis reikalavimas, t. y. reikalavimas palengvinti tarpvalstybinį bendradarbiavimą ir ryšių palaikymą. Tai ypač reikalinga turint omenyje, kad valstybės narės gali nuspręsti paskirti daugiau kaip vieną nacionalinę instituciją. Taigi įsteigus bendrąjį informacinį centrą būtų lengviau identifikuoti skirtingų valstybių narių institucijas ir su jomis bendradarbiauti.

Tais atvejais, kai nacionalinis bendrasis informacinis centras nėra nei CSIRT, nei Bendradarbiavimo grupės narys, bendrojo informacinio centro ryšių palaikymo vaidmuo veikiausiai apimtų bendravimą su Bendradarbiavimo grupės ir CSIRT tinklo sekretoriatais. Be to, valstybės narės turi užtikrinti, kad bendrasis informacinis centras būtų informuojamas apie pranešimus, gautus iš esminių paslaugų operatorių ir skaitmeninių paslaugų teikėjų[20].

Direktyvos 8 straipsnio 3 dalyje nurodyta, kad, jeigu valstybė narė taiko centralizuotą metodą, t. y. paskiria tik vieną kompetentingą instituciją, ta institucija taip pat vykdo bendrojo informacinio centro funkcijas. Jeigu valstybė narė nusprendžia taikyti decentralizuotą metodą, ji gali pasirinkti vieną iš įvairių kompetentingų institucijų, kad ši veiktų kaip bendrasis informacinis centras. Nesvarbu, kuris institucinis modelis buvo pasirinktas, jeigu kompetentinga institucija, CSIRT ir bendrasis informacinis centras yra skirtingi subjektai, valstybės narės privalo užtikrinti veiksmingą jų bendradarbiavimą, kad įvykdytų Direktyvoje nustatytus įpareigojimus[21].

Ne vėliau kaip 2018 m. rugpjūčio 9 d. ir vėliau kiekvienais metais bendrasis informacinis centras privalo Bendradarbiavimo grupei pateikti suvestinę ataskaitą apie gautus pranešimus, kurioje nurodomas pranešimų skaičius, incidentų pobūdis ir priemonės, kurių ėmėsi institucijos, pvz., kitų paveiktų valstybių narių informavimas apie incidentą arba atitinkamos informacijos suteikimas pranešančiajai įmonei, kad ši galėtų suvaldyti incidentą[22]. Kompetentingos institucijos arba CSIRT prašymu bendrasis informacinis centras turi esminių paslaugų operatorių pranešimus persiųsti kitų incidento paveiktų valstybių narių bendriesiems informaciniams centrams[23].

Valstybės narės turi Komisiją informuoti apie bendrojo informacinio centro paskyrimą ir jo užduotis iki Direktyvos perkėlimo į nacionalinę teisę termino. Apie bendrojo informacinio centro paskyrimą turi būti paskelbta viešai, taip pat turi būti viešai paskelbtos nacionalinės kompetentingos institucijos. Komisija paskelbia paskirtų bendrųjų informacinių centrų sąrašą.

3.7. Sankcijos

21 straipsnyje valstybėms narėms paliekama laisvė nuspręsti, kokios rūšies ir pobūdžio sankcijas taikyti, tačiau jos turi būti veiksmingos, proporcingos ir atgrasomosios. Kitaip tariant, iš principo valstybės narės gali laisvai nuspręsti, kokia turi būti didžiausia jų nacionalinės teisės aktuose nustatytų baudų suma, tačiau nustatant tokią sumą arba procentinę dalį nacionalinėms institucijoms turi būti suteikta galimybė kiekvienu konkrečiu atveju taikyti

[20] Žr. 10 straipsnio 3 dalį.
[21] Žr. 10 straipsnio 1 dalį.
[22] Ten pat.
[23] Žr. 14 straipsnio 5 dalį.

veiksmingas, proporcingas ir atgrasomąsias sankcijas atsižvelgiant į įvairius veiksnius, pvz., pažeidimo sunkumą arba dažnumą.

4. Subjektai, turintys su saugumo ir pranešimo apie incidentus reikalavimų vykdymu susijusių pareigų

Subjektai, turintys svarbią reikšmę visuomenei ir ekonomikai, Direktyvos 4 straipsnio 4 ir 5 punktuose įvardyti kaip „esminių paslaugų operatorius“ ir „skaitmeninių paslaugų teikėjas“, turi imtis atitinkamų saugumo priemonių ir apie pavojingus incidentus pranešti atitinkamoms nacionalinėms institucijoms. Tai grindžiama tuo, kad saugumo incidentai gali kelti didelę grėsmę tokių paslaugų teikimui, dėl to gali būti sutrikdyta ekonominė veikla ir plačiosios visuomenės gyvenimas ir gali būti pakirstas naudotojų pasitikėjimas ir padaryta didelė žala Sąjungos ekonomikai[24].

Šiame skirsnyje pateikta į TIS direktyvos II ir III priedus įtrauktų subjektų apžvalga ir nurodytos jų užduotys. Išsamiai apibūdintas esminių paslaugų operatorių identifikavimas, nes šis procesas labai svarbus siekiant užtikrinti darnų TIS direktyvos įgyvendinimą visoje ES. Taip pat šiame skirsnyje išsamiai paaiškintos skaitmeninės infrastruktūros ir skaitmeninių paslaugų teikėjo apibrėžtys. Be to, jame apsvarstyta galimybė įtraukti papildomus sektorius ir išsamiau paaiškintas specifinis požiūris į skaitmeninių paslaugų teikėjus.

4.1. Esminių paslaugų operatoriai

TIS direktyvoje aiškiai neapibrėžta, kurie konkretūs subjektai pagal jos taikymo sritį bus laikomi esminių paslaugų operatoriais. Tačiau joje nustatyti kriterijai, kuriuos valstybės narės turės taikyti vykdydamos identifikavimo procesą, – taip galiausiai bus nustatyta, kurios atskiros įmonės, priklausančios II priede išvardytų subjektų rūšiai, bus laikomos esminių paslaugų operatoriais ir atitinkamai joms bus taikomos Direktyvoje nustatytos pareigos.

4.1.1. TIS direktyvos II priede išvardytų subjektų rūšys

4 straipsnio 4 punkte esminių paslaugų operatoriai apibrėžiami kaip viešojo arba privačiojo sektoriaus subjektai, kurių rūšis nurodyta Direktyvos II priede ir kurie atitinka 5 straipsnio 2 dalyje nustatytus reikalavimus. II priede nurodyti sektoriai, subsektoriai ir subjektų rūšys, pagal kuriuos kiekviena valstybė narė turi atlikti 5 straipsnio 2 dalyje nustatytą identifikavimo procesą[25]. Sektoriai – energetika, transportas, bankininkystė, finansų rinkų infrastruktūra, sveikatos priežiūra, vandens tiekimas ir skaitmeninės infrastruktūra.

ES teisės aktuose pateikiamos gerai parengtos daugumos tradiciniams sektoriams priklausančių subjektų apibrėžtys, į kurias daroma nuoroda II priede. Tačiau to negalima pasakyti apie II priedo 7 punkte išvardytų skaitmeninės infrastruktūros objektų, įskaitant interneto duomenų srautų mainų taškus, domenų vardų sistemas ir aukščiausio lygio domenų

[24] Žr. 2 konstatuojamąją dalį.
[25] Išsamesnė informacija apie identifikavimo procesą pateikta 4.1.6 skirsnyje.

vardų registrus, apibrėžtis. Todėl, siekiant šio objektų apibrėžtis patikslinti, toliau pateikiami išsamūs jų paaiškinimai.

1) Interneto duomenų srautų mainų taškas (IXP)

Terminas „interneto duomenų srautų mainų taškas“ apibrėžtas 4 straipsnio 13 punkte ir papildomai paaiškintas 18 konstatuojamojoje dalyje; tai tinklo įrenginys, kuris sudaro sąlygas sujungti daugiau nei dvi techniškai nepriklausomas autonomines sistemas, visų pirma siekiant palengvinti interneto duomenų srautų mainus. Interneto duomenų srautų mainų tašką taip pat galima apibūdinti kaip fizinę vietą, kurioje naudojant perjungiklį įvairūs tinklai gali tarpusavyje vykdyti interneto duomenų srautų mainus. Pagrindinis IXP tikslas – sudaryti sąlygas tinklams susijungti tiesiogiai per interneto duomenų srautų mainų tašką, o ne per vieną ar daugiau trečiųjų šalių tinklų. IXP paslaugos teikėjas paprastai nėra atsakingas už interneto duomenų srautų nukreipimą. Duomenų srautų nukreipimo funkciją atlieka tinklo paslaugų teikėjai. Tiesioginis susijungimas turi daug pranašumų, tačiau pagrindinės jo naudojimo priežastys yra mažesnės sąnaudos, mažesnė delsa ir didesnis dažnių juostos plotis. Per interneto duomenų srautų mainų tašką einantys duomenų srautai paprastai nėra apmokestinami nė vienos šalies, o duomenų srautai per pirminį interneto paslaugų teikėją (IPT) yra apmokestinami. Esant tiesioginei jungčiai, kuri dažnai yra tame pačiame mieste kaip ir abu tinklai, duomenims nereikia keliauti ilgų atstumų, kad patektų iš vieno tinklo į kitą, todėl sumažėja delsa.

Reikėtų atkreipti dėmesį į tai, kad IXP apibrėžtis neapima fizinių taškų, kuriuose vienas su kitu sujungiami tik du fiziniai tinklai (t. y. tinklo paslaugų teikėjai, kaip antai BASE ir PROXIMUS). Todėl, perkeldamos Direktyvą į nacionalinę teisę, valstybės narės turi atskirti operatorius, kurie sudaro sąlygas daugeliui tinklų operatorių vykdyti bendrų interneto duomenų srautų mainus, ir pavienius tinklų operatorius, kurie fiziškai sujungia savo tinklus remdamiesi susitarimu dėl tinklų sujungimo. Pastariesiems tinklo paslaugų teikėjams 4 straipsnio 13 punkte pateikta apibrėžtis netaikoma. Paaiškinimą šiuo klausimu galima rasti 18 konstatuojamojoje dalyje, kurioje nurodyta, kad IXP nesuteikia prieigos prie tinklo ir nėra persiuntimo paslaugų teikėjas ar nešlys. Paskutinė paslaugų teikėjų kategorija yra įmonės, teikiančios viešųjų ryšių tinklų paslaugas ir (arba) elektroninių ryšių paslaugas, kurioms taikomi Direktyvos 2002/21/EB 13 straipsnio a ir b punktuose nustatyti saugumo ir pranešimo reikalavimai, todėl jos nepatenka į TIS direktyvos taikymo sritį[26].

2) Domeno vardų sistema (DNS)

Terminas „domeno vardų sistema“ 4 straipsnio 14 punkte apibrėžtas kaip „pagal hierarchiją suskirstyta vardų suteikimo sistema tinkle, kuris persiunčia domenų vardų užklausas“. Tiksliau DNS gali būti apibūdinta kaip pagal hierarchiją suskirstyta vardų suteikimo sistema, skirta kompiuteriams, sistemoms ar bet kuriam kitam prie interneto prijungtam ištekliui, kuriuo galima domenų vardus užkoduoti kaip IP (interneto protokolo) adresus. Pagrindinė

[26] Išsamesnė informacija apie TIS direktyvos ir Direktyvos 2002/21/EB santykį pateikta 5.2 skirsnyje.

sistemos funkcija – priskirtus domenų vardus paversti IP adresais. Šiuo tikslu DNS tokiam domenų vardų „vertimui“ į veikiančius IP adresus atlikti naudoja duomenų bazę ir vardų serverius bei vardų vertimo programą. Nors domenų vardų kodavimas nėra vienintelė DNS funkcija, tai yra viena svarbiausių sistemos užduočių. 4 straipsnio 14 punkte pateiktoje teisinėje apibrėžtyje dėmesys sutelkiamas į pagrindinį sistemos vaidmenį naudotojo požiūriu, nesileidžiant į techninio pobūdžio detales, kaip antai domeno vardo erdvė, vardų serveriai, vardų vertimo programos ir t. t. Galiausiai 4 straipsnio 15 punkte paaiškinama, ką reikėtų laikyti DNS paslaugų teikėju.

3) Aukščiausio lygio domenų vardų registras (ALD vardų registras).

Aukščiausio lygio domenų vardų registras 4 straipsnio 16 punkte apibrėžiamas kaip subjektas, kuris administruoja ir vykdo interneto domenų vardų registravimą pagal konkretų aukščiausio lygio domeną. Toks domenų vardų administravimas ir valdymas apima ALD vardų kodavimą į IP adresus.

IANA (Interneto numerių skyrimo tarnyba) yra atsakinga už visuotinį DNS pagrindinės zonos, interneto protokolo adresų sistemos ir kitų interneto protokolo išteklių koordinavimą. Visų pirma IANA atsako už bendrinių aukščiausio lygio domenų (bendrinių ALD) , pvz., „.com“, ir šalies kodo aukščiausio lygio domenų (šalies kodo ALD), pvz., „.be“, priskyrimą operatoriams (registrams) ir jų techninių bei administracinių duomenų priežiūrą. IANA tvarko priskirtųjų ALD visuotinį registrą ir prisideda prie šio sąrašo viešinimo interneto naudotojams visame pasaulyje, taip pat prie naujų ALD diegimo.

Svarbi registrų užduotis – priskirti antrojo lygio domeno vardus vadinamiesiems registruotojams pagal jų atitinkamą ALD. Jeigu pageidauja, šie registruotojai taip pat gali savarankiškai priskirti trečiojo lygio domenų vardus. Šalies kodo ALD skirti šaliai arba teritorijai žymėti pagal ISO 3166-1 standartą. Bendriniai ALD paprastai neturi geografinės ar šalies nuorodos.

Reikėtų atkreipti dėmesį į tai, kad ALD vardų registro tvarkymas gali apimti DNS paslaugos teikimą. Pavyzdžiui, pagal IANA delegavimo taisykles paskirtasis subjektas, atsakingas už poreikių, susijusių su šalies kodo ALD, tenkinimą, *inter alia*, turi vykdyti domenų vardų priežiūrą ir valdyti tos šalies DNS[27]. Valstybės narės turi atsižvelgti į tokias aplinkybes vykdydamos esminių paslaugų operatorių identifikavimo procesą pagal 5 straipsnio 2 dalį.

4.1.2. Esminių paslaugų operatorių identifikavimas

Pagal Direktyvos 5 straipsnio reikalavimus kiekviena valstybė narė turi identifikuoti visus II priede nurodytų rūšių subjektus, teisėtai įsisteigusius tos valstybės narės teritorijoje. Atlikus šį vertinimą, visi 5 straipsnio 2 dalyje nustatytus kriterijus atitinkantys subjektai identifikuojami kaip esminių paslaugų operatoriai ir jiems taikomi 14 straipsnyje nustatyti saugumo reikalavimai ir pareiga pranešimo apie incidentus.

[27] Informacijos galima rasti adresu https://www.icann.org/resources/pages/delegation-2012-02-25-en.

Valstybės narės kiekvieno sektoriaus ir subsektoriaus operatorius turi identifikuoti iki 2018 m. lapkričio 9 d. Siekdama padėti valstybėms narėms vykdyti šį procesą, Bendradarbiavimo grupė šiuo metu rengia rekomendacinį dokumentą, kuriame bus pateikta atitinkama informacija apie būtinuosius veiksmus ir geriausią patirtį, susijusius su esminių paslaugų operatorių identifikavimu.

Be to, pagal 24 straipsnio 2 dalį Bendradarbiavimo grupė turi aptarti nacionalinių priemonių, kuriomis sudaromos sąlygos identifikuoti esminių paslaugų operatorius konkrečiuose sektoriuose, taikymo procesą, turinį ir rūšį. Valstybė narė gali iki 2018 m. lapkričio 9 d. siekti Bendradarbiavimo grupėje aptarti savo nacionalinių priemonių, kuriomis sudaromos sąlygos identifikuoti esminių paslaugų operatorius, projektus.

4.1.3. Papildomų sektorių įtraukimas

Atsižvelgdamos į 3 straipsnyje nustatytą minimalaus suderinimo reikalavimą, valstybės narės gali priimti arba palikti galioti teisės aktus, kuriais užtikrinamas aukštesnis tinklų ir informacinių sistemų saugumo lygis. Šiuo atžvilgiu valstybės narės iš esmės gali 14 straipsnyje nustatytus saugumo ir pranešimo reikalavimus taikyti ir tiems subjektams, kurie priklauso į TIS direktyvos II priedą neįtrauktiems sektoriams ir subsektoriams. Įvairios valstybės narės jau nusprendė arba šiuo metu svarsto, ar į sąrašą įtraukti kai kuriuos iš toliau nurodytų sektorių.

i) Viešojo administravimo institucijos

Viešojo administravimo institucijos gali teikti Direktyvos II priede nurodytas esmines paslaugas, atitinkančias 5 straipsnio 2 dalies reikalavimus. Tokiais atvejais viešojo administravimo institucijoms, teikiančioms tokias paslaugas, būtų taikomi atitinkami saugumo reikalavimai ir pareiga pranešti. Ir priešingai – jeigu viešojo administravimo institucijos teikiamos paslaugos nepatenka į pirmiau minėtą taikymo sritį, tokioms paslaugoms atitinkami reikalavimai nebūtų taikomi.

Viešojo administravimo institucijos yra atsakingos už tai, kad valdžios įstaigos, regioninės ir vietos valdžios institucijos, agentūros ir asocijuotosios įmonės tinkamai teiktų viešąsias paslaugas. Teikiant šias paslaugas neretai renkami ir tvarkomi asmens duomenys ir įmonių duomenys apie fizinius asmenis ir organizacijas, kuriais gali būti keičiamasi ir kurie gali būti teikiami daugeliui viešųjų subjektų. Žvelgiant plačiau, aukštas viešojo administravimo institucijų naudojamų tinklų ir informacinių sistemų saugumo lygis svarbus visuomenei ir ekonomikai apskritai. Todėl Komisija laikosi požiūrio, kad valstybėms narėms būtų tikslinga apsvarstyti galimybę į nacionalinės teisės aktų, kuriais į nacionalinę teisę perkeliama Direktyva, taikymo sritį įtraukti ne tik tas viešojo administravimo institucijas, kurios teikia esmines paslaugas, kaip nustatyta II priede ir 5 straipsnio 2 dalyje.

ii) Pašto sektorius

Pašto sektorius apima pašto paslaugų, kaip antai pašto siuntų surinkimo, rūšiavimo, vežimo ir paskirstymo, teikimą.

iii) Maisto pramonės sektorius

Maisto pramonės sektorius yra susijęs su žemės ūkio ir kitų maisto produktų gamyba ir gali apimti esmines paslaugas, pvz., aprūpinimo maistu ir maisto kokybės bei saugos užtikrinimą.

iv) Chemijos ir branduolinė pramonė

Chemijos ir branduolinė pramonė visų pirma yra susijusi su cheminių ir naftos chemijos produktų arba branduolinių medžiagų laikymu, gamyba ir perdirbimu.

v) Aplinkos sektorius

Aplinkosaugos veikla apima aplinkai apsaugoti ir ištekliams valdyti būtinų prekių ir paslaugų teikimą. Todėl šios veiklos tikslas – taršos prevencija, mažinimas ir šalinimas, taip pat turimų gamtos išteklių išsaugojimas. Šiame sektoriuje esminės paslaugos galėtų būti taršos (pvz., oro ir vandens) ir meteorologinių reiškinių stebėjimas ir kontrolė.

vi) Civilinė sauga

Civilinės saugos sektoriaus tikslas – užkirsti kelią gaivalinėms nelaimėms ir žmogaus sukeltoms katastrofoms, joms pasirengti bei į jas reaguoti. Šiuo tikslu teikiamos paslaugos gali būti pagalbos telefono numerių aktyvinimas ir veiksmų, kuriais pranešama apie ekstremaliąsias situacijas, jos valdomos ir į jas reaguojama, įgyvendinimas.

4.1.4. Jurisdikcija.

Pagal 5 straipsnio 1 dalį kiekviena valstybė narė turi identifikuoti esminių paslaugų operatorius, kurie yra įsisteigę jos teritorijoje. Šioje nuostatoje konkrečiau nenurodyta teisinė įsisteigimo rūšis, tačiau 21 konstatuojamojoje dalyje paaiškinta, jog toks įsisteigimas reiškia, kad esminių paslaugų operatoriai veiksmingai vykdo realią veiklą remdamiesi stabiliomis struktūromis, o teisinė tokių struktūrų forma neturėtų būti lemiamas veiksnys. Tai reiškia, kad esminių paslaugų operatorius valstybės narės jurisdikcijai gali priklausyti ne tik tais atvejais, kai jos teritorijoje yra operatoriaus pagrindinė buveinė, bet ir tais atvejais, kai jos teritorijoje yra, pvz., operatoriaus filialas, ar jis yra kitaip joje įsisteigęs.

Todėl tas pats subjektas vienu metu gali priklausyti kelių valstybių narių jurisdikcijai.

4.1.5. Komisijai teiktina informacija

Kad Komisija galėtų atlikti peržiūrą pagal TIS direktyvos 23 straipsnio 1 dalį, valstybės narės privalo iki 2018 m. lapkričio 9 d. ir vėliau kas dvejus metus pateikti Komisijai šią informaciją:

- nacionalines priemones, kuriomis sudaromos sąlygos identifikuoti esminių paslaugų operatorius;
- esminių paslaugų sąrašą;
- kiekviename II priede nurodytame sektoriuje identifikuotų esminių paslaugų operatorių skaičių ir tų operatorių svarbą sektoriui ir
- ribas, jei jų esama, siekiant nustatyti tiekimo lygį atsižvelgiant į naudotojų, kurie priklauso nuo tos paslaugos, kaip nurodyta 6 straipsnio 1 dalies a punkte, skaičių arba subjekto svarbą, kaip nurodyta 6 straipsnio 1 dalies f punkte.

Iš 23 straipsnio 1 dalyje numatytos peržiūros, kuri atliekama prieš išsamią Direktyvos peržiūrą, matyti, kokią svarbą, siekdamos išvengti rinkos susiskaidymo, teisėkūros institucijos teikia tinkamam Direktyvos perkėlimui į nacionalinę teisę esminių paslaugų operatorių identifikavimo srityje.

Kad šis procesas būtų įgyvendintas kuo sėkmingiau, Komisija skatina valstybes nares aptarti šį klausimą, taip pat keistis atitinkama patirtimi Bendradarbiavimo grupėje. Be to, Komisija ragina valstybes nares, be visos informacijos, kurią valstybės narės pagal Direktyvą privalo pateikti Komisijai, (jei reikia, konfidencialiai) pasidalyti su Komisija identifikuotų esminių paslaugų operatorių (kurie galiausiai buvo atrinkti) sąrašais. Turint galimybę susipažinti su tokiais sąrašais, Komisijai būtų lengviau atlikti kokybiškesnį identifikavimo proceso vertinimą, be to, ji galėtų palyginti valstybių narių taikomus metodus, ir taip būtų užtikrintas geresnis Direktyvos tikslų įgyvendinimas.

4.1.6. Kaip vykdyti identifikavimo procesą?

Kaip parodyta 4 pav., nacionalinė institucija, vykdydama konkretaus subjekto identifikavimo procesą, turėtų atsakyti į šešis pagrindinius klausimus. Toliau pateiktas kiekvienas klausimas atitinka veiksmą, kurio reikia imtis pagal 5 straipsnį, skaitomą kartu su 6 straipsniu, taip pat atsižvelgiant į tai, ar taikoma 1 straipsnio 7 dalis.

1 etapas. **Ar subjektas priklauso sektoriui ir (arba) subsektoriui ir atitinka vieną iš Direktyvos II priede nustatytų subjektų rūšių?**

Nacionalinė institucija turėtų įvertinti, ar jos teritorijoje įsisteigęs subjektas priklauso vienam iš Direktyvos II priede nurodytų sektorių ir subsektorių. II priedas apima įvairius ekonomikos sektorius, kurie laikomi svarbiais siekiant užtikrinti tinkamą vidaus rinkos veikimą. Visų pirma II priede nurodyti šie sektoriai ir subsektoriai:

- energetika: elektros energija, nafta ir dujos;
- transportas: oro, geležinkelių, vandens ir kelių;
- bankininkystė: kredito įstaigos;
- finansų rinkų infrastruktūros objektai: prekybos vietos, pagrindinės sandorio šalys;
- sveikata: sveikatos priežiūros paslaugų teikėjai (įskaitant ligonines ir privačias klinikas);
- vanduo: geriamojo vandens tiekimas ir paskirstymas;
- skaitmeninė infrastruktūra: interneto duomenų srautų mainų taškai, domenų vardų sistemos ir aukščiausio lygio domenų vardų registrai[28].

2 etapas. **Ar taikomas *lex specialis*?**

Kitame etape nacionalinė institucija turi įvertinti, ar taikoma 1 straipsnio 7 dalyje įtvirtinta *lex specialis* nuostata. Visų pirma šioje nuostatoje nurodyta, kad, jeigu yra ES teisės aktas, kuriuo skaitmeninių paslaugų teikėjams arba esminių paslaugų operatoriams taikomi saugumo ir

[28]Jie išsamiau paaiškinti 4.1.1 skirsnyje.

(arba) pranešimo reikalavimai, kurie yra bent lygiaverčiai TIS direktyvoje nustatytiems atitinkamiems reikalavimams, turėtų būti taikomos to specialaus teisės akto nuostatos. Be to, 9 konstatuojamojoje dalyje paaiškinta, kad, jeigu 1 straipsnio 7 dalyje nustatyti reikalavimai įvykdyti, valstybės narės turėtų taikyti konkrečiam sektoriui taikomo ES teisės akto nuostatas, be kita ko, susijusias su jurisdikcija. Priešingu atveju atitinkamos TIS direktyvos nuostatos nebūtų taikomos. Šiuo atveju kompetentinga institucija neturėtų tęsti 5 straipsnio 2 dalyje nustatyto identifikavimo proceso[29].

3 etapas. **Ar operatorius teikia esminę paslaugą, apibrėžtą Direktyvoje?**

Pagal 5 straipsnio 2 dalies a punktą identifikuojamas subjektas turi teikti paslaugą, kuri yra būtina siekiant užtikrinti ypatingos svarbos visuomeninės ir (arba) ekonominės veiklos vykdymą. Atlikdamos šį vertinimą, valstybės narės turėtų atsižvelgti į tai, kad tas pats subjektas gali teikti ir esmines, ir neesmines paslaugas. Tai reiškia, kad TIS direktyvoje nustatyti saugumo ir pranešimo reikalavimai tam tikram operatoriui bus taikomi tik tokiu mastu, kokiu jis teikia esmines paslaugas.

Pagal 5 straipsnio 3 dalį valstybė narė turėtų sudaryti visų jos teritorijoje įsisteigusio esminių paslaugų operatoriaus teikiamų esminių paslaugų sąrašą. Šį sąrašą Komisijai reikės pateikti iki 2018 m. lapkričio 9 d., o vėliau – kas dvejus metus[30].

4 etapas. **Ar paslaugos teikimas priklauso nuo tinklų ir informacinių sistemų?**

Be to, turėtų būti išaiškinta, ar ši paslauga atitinka 5 straipsnio 2 dalies b punkto kriterijų ir visų pirma ar esminės paslaugos teikimas priklauso nuo tinklų ir informacinių sistemų, apibrėžtų 4 straipsnio 1 punkte.

5 etapas. **Ar saugumo incidentas turėtų didelį trikdomąjį poveikį?**

Pagal 5 straipsnio 2 dalies c punktą reikalaujama, kad nacionalinė institucija įvertintų, ar incidentas turės didelį trikdomąjį poveikį paslaugos teikimui. Šiuo tikslu 6 straipsnio 1 dalyje nustatyti keli visiems sektoriams bendri veiksniai, į kuriuos reikia atsižvelgti vertinime. Be to, 6 straipsnio 2 dalyje nustatyta, kad prireikus vertinime taip pat turėtų būti atsižvelgiama į konkretiems sektoriams būdingus veiksnius.

6 straipsnio 1 dalyje išvardyti šie **tarpsektoriniai veiksniai**:

- naudotojų, kurie priklauso nuo atitinkamo subjekto teikiamos paslaugos, skaičius;
- kitų II priede nurodytų sektorių priklausomybė nuo to subjekto teikiamos paslaugos;
- poveikis, kurį incidentai dėl savo masto ir trukmės galėtų daryti ekonominei ir visuomeninei veiklai arba viešajam saugumui;
- to subjekto užimama rinkos dalis;
- geografinė teritorijos, kurią galėtų paveikti incidentas, aprėptis;

[29] Išsamesnė informacija apie *lex specialis* taikymą pateikta 5.1 skirsnyje.
[30] Žr. 5 straipsnio 7 dalies b punktą.

- subjekto svarba pakankamam paslaugos lygiui išlaikyti, atsižvelgiant į esamas tos paslaugos teikimo alternatyvas.

28 konstatuojamojoje dalyje pateikti keli **konkretiems sektoriams būdingų veiksnių** pavyzdžiai (žr. 4 lentelę), kuriais nacionalinės institucijos galėtų pasinaudoti kaip gairėmis.

4 lentelė. Konkretiems sektoriams būdingų veiksnių, į kuriuos reikia atsižvelgti nustatant didelį trikdomąjį poveikį incidento atveju, pavyzdžiai

Sektorius	Konkretiems sektoriams būdingų veiksnių pavyzdžiai
Energijos tiekėjai	pagamintos nacionalinės energijos kiekis arba jos dalis
Naftos tiekėjai	tiekiamos naftos kiekis per dieną
Oro transportas (įskaitant oro uostus ir oro vežėjus) **Geležinkelių transportas** **Jūrų uostai**	nacionalinio eismo intensyvumo dalis; keleivių arba krovinių vežimo operacijų skaičius per metus
Bankų arba finansų rinkų infrastruktūros objektai	sisteminė svarba, grindžiama visu turtu; viso turto santykinė BVP dalis
Sveikatos priežiūros sektorius	sveikatos priežiūros paslaugų teikėjo pacientų skaičius per metus
Vandens gamyba, perdirbimas ir tiekimas	vandens kiekis ir vartotojų, kuriems vanduo tiekiamas, skaičius ir rūšis, įskaitant, pvz., ligonines, viešąsias paslaugas teikiančias organizacijas ar fizinius asmenis; alternatyvių vandens išteklių buvimas siekiant aptarnauti tą pačią geografinę vietovę

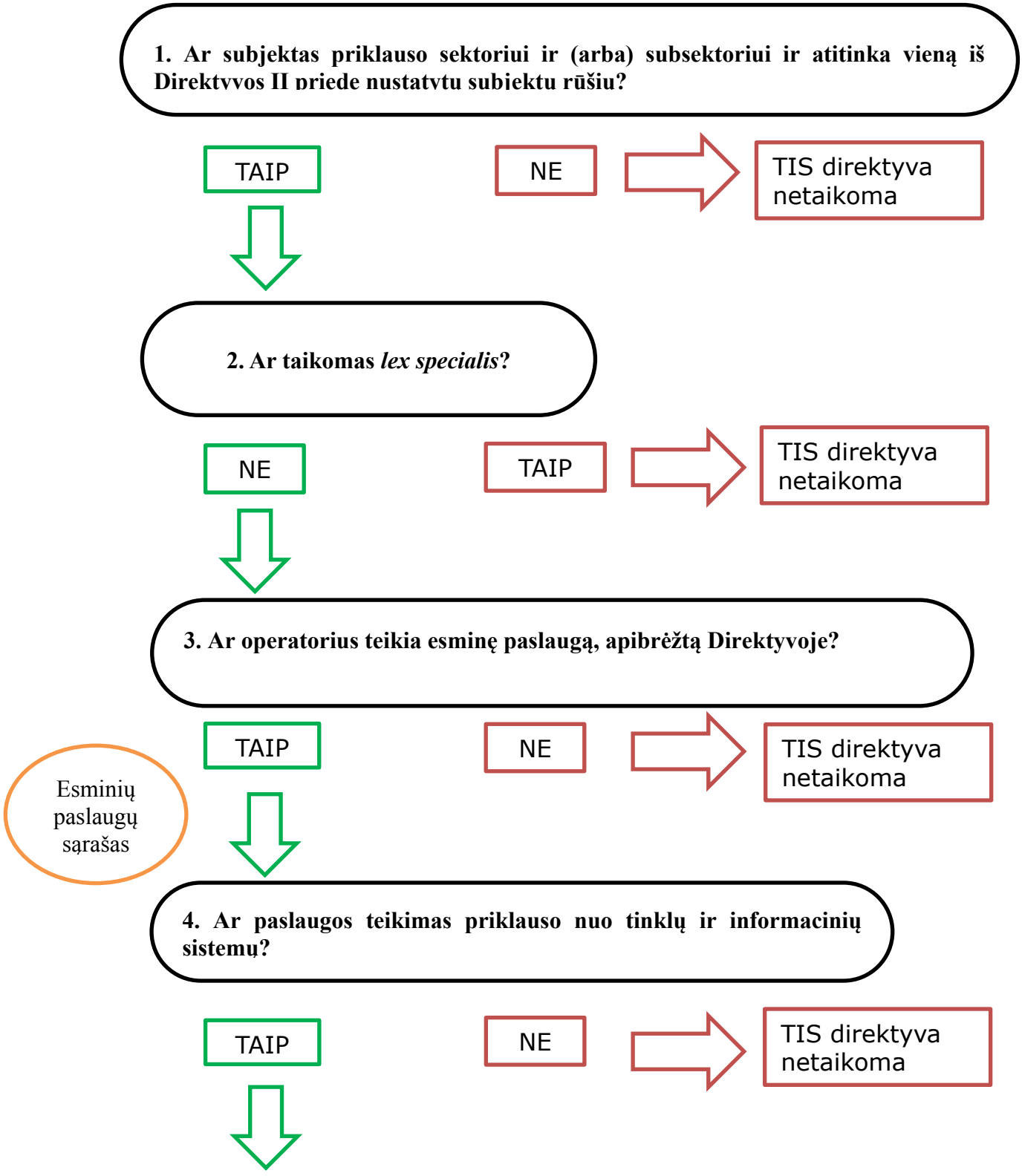
Reikėtų pabrėžti, kad, atlikdamos vertinimą pagal 5 straipsnio 2 dalį, valstybės narės neturėtų taikyti papildomų kriterijų be tų, kurie išvardyti toje nuostatoje, nes dėl to gali sumažėti identifikuotų esminių paslaugų teikėjų skaičius ir kilti rizika, kad, identifikuojant esminių paslaugų operatorius, nebus laikomasi Direktyvos 3 straipsnyje įtvirtinto minimalaus suderinimo reikalavimo.

6 etapas. **Ar atitinkamas operatorius teikia esmines paslaugas kitose valstybėse narėse?**

6 etape kalbama apie atvejus, kai operatorius teikia esmines paslaugas dviejose ar daugiau valstybių narių. 5 straipsnio 4 dalyje nustatyta, kad, prieš užbaigdamos identifikavimo procesą, atitinkamos valstybės narės konsultuojasi tarpusavy[31].

[31] Išsamesnė informacija apie konsultavimosi procesą pateikta 4.1.7 skirsnyje.

4 pav. Šešių etapų identifikavimo procesas



5. Ar saugumo incidentas turėtų didelį trikdomąjį poveikį?

Tarpsektoriniai veiksniai (6 straipsnio 1 dalis)

- **Naudotojų**, kurie priklauso nuo paslaugų, **skaičius**
- Kitų esminių sektorių **priklausomybė** nuo paslaugos
- Poveikis, kurį incidentai galėtų daryti **ekonominei ir visuomeninei veiklai** arba **viešajam saugumui**
- Galima **geografinė aprėptis**
- Subjekto svarba pakankamam **paslaugos lygiui** išlaikyti

Konkretiems sektoriams būdingi veiksniai (28 konstatuojamojoje dalyje pateikti pavyzdžiai)

- **Energetika**: pagamintos nacionalinės energijos kiekis arba jos dalis
- **Transportas**: nacionalinio eismo intensyvumo dalis ir operacijų skaičius per metus
- **Sveikata**: sveikatos priežiūros paslaugų teikėjo pacientų skaičius per metus

TAIP

NE → TIS direktyva netaikoma

6. Ar atitinkamas operatorius teikia esmines paslaugas kitose valstybėse narėse?

TAIP

NE → TIS direktyva netaikoma

Privaloma konsultacija su atitinkama (-omis) valstybe (-ėmis) nare (-ėmis)

Nacionalinių priemonių (pvz., esminių paslaugų operatorių sąrašo sudarymas, politikos ir teisinės priemonės) priėmimas

4.1.7. Tarpvalstybinis konsultavimosi procesas

5 straipsnio 4 dalyje nustatyta, kad, jeigu operatorius esmines paslaugas teikia dviejose ar daugiau valstybių narių, tos valstybės narės, prieš užbaigdamos identifikavimo procesą, turi konsultuotis tarpusavyje. Šios konsultacijos tikslas – padėti įvertinti operatoriaus ypatingą svarbą tarpvalstybinio poveikio požiūriu.

Šia konsultacija siekiama, kad susijusios nacionalinės institucijos išsakytų savo argumentus ir poziciją ir idealiu atveju pasiektų tą patį rezultatą identifikuodamos atitinkamą operatorių. Tačiau pagal TIS direktyvą valstybėms narėms nedraudžiama prieiti prie skirtingų išvadų, ar konkretus subjektas yra esminių paslaugų operatorius, ar ne. 24 konstatuojamojoje dalyje nurodyta, kad valstybės narės gali šiuo klausimu prašyti Bendradarbiavimo grupės paramos.

Komisijos nuomone, valstybės narės turėtų stengtis šiais klausimais susitarti ir išvengti situacijos, kai ta pati bendrovė įvairiose valstybėse narės turi skirtingą teisinį statusą. Teisinis statusas turėtų skirtis tik tikrai išskirtiniais atvejais, pvz., kai vienoje valstybėje narėje kaip esminių paslaugų operatorius identifikuotas subjektas kitoje valstybėje narėje vykdo tik nereikšmingą ir nedidelės apimties veiklą.

4.2. Saugumo reikalavimai

Pagal 14 straipsnio 1 dalį valstybės narės privalo užtikrinti, kad esminių paslaugų operatoriai, remdamiesi naujausiais technikos laimėjimais, imtųsi tinkamų ir proporcingų techninių ir organizacinių priemonių, kad galėtų valdyti riziką, kylančią tinklų ir informacinių sistemų, kuriais organizacijos naudojasi teikdamos savo paslaugas, saugumui. Pagal 14 straipsnio 2 dalį reikia imtis tinkamų priemonių, kad būtų išvengta incidento ir būtų kuo labiau sumažintas jo poveikis.

Bendradarbiavimo grupėje šiuo metu veikia speciali darbo grupė, rengianti neprivalomas gaires dėl saugumo priemonių, kurių turėtų imtis esminių paslaugų operatoriai[32]. Grupė turėtų baigti rengti rekomendacinį dokumentą iki 2017 m. ketvirtojo ketvirčio. Komisija ragina valstybes nares atidžiai laikytis rekomendacinio dokumento, kurį turi parengti Bendradarbiavimo grupė, kad nacionalinės teisės nuostatos dėl saugumo reikalavimų būtų kuo labiau suderintos. Suderinus tokius reikalavimus, esminių paslaugų operatoriams, kurie dažnai esmines paslaugas teikia daugiau nei vienoje valstybėje narėje, būtų daug lengviau laikytis saugumo reikalavimų, o nacionalinėms kompetentingoms institucijoms ir CSIRT būtų lengviau vykdyti priežiūros užduotis.

4.3. Pranešimo reikalavimai

Pagal 14 straipsnio 3 dalį valstybės narės turi užtikrinti, kad esminių paslaugų operatoriai praneštų „apie incidentus, kurie turi didelį poveikį jų teikiamų esminių paslaugų tęstinumui“.

[32] Kad darbo grupė galėtų įvykdyti savo užduotį, buvo išplatinti visų sektorių, kuriems taikoma TIS direktyva, tarptautinių standartų sąrašai, informacija apie gerąją patirtį ir rizikos vertinimo ir (arba) valdymo metodikos, ir jais buvo naudojamasi rengiant rekomendacijas dėl siūlomų saugumo sričių ir saugumo priemonių.

Taigi esminių paslaugų operatoriai neturėtų pranešti apie nereikšmingus incidentus, o tik apie didelius incidentus, turinčius poveikį esminės paslaugos tęstinumui. 4 straipsnio 7 punkte kaip incidentas apibrėžiamas kaip „įvykis, turintis faktinį neigiamą poveikį tinklų ir informacinių sistemų saugumui“. Terminas „tinklų ir informacinių sistemų saugumas“ 4 straipsnio 2 punkte išsamiau apibrėžiamas kaip „tinklų ir informacinių sistemų pajėgumas tam tikru patikimumo lygiu išlikti atspar[iom]s bet kuriems veiksmams, keliantiems pavojų saugomų, perduodamų ar tvarkomų duomenų, arba atitinkamų teikiamų ar per tas tinklų ir informacines sistemas gaunamų paslaugų prieinamumui, autentiškumui, vientisumui ar konfidencialumui“. Taigi bet koks įvykis, turintis neigiamą poveikį ne tik duomenų ar susijusių paslaugų prieinamumui, bet ir jų autentiškumui, vientisumui ar konfidencialumui, gali būti pagrindas atsirasti pareigai apie jį pranešti. Iš tiesų pavojus paslaugos teikimo tęstinumui, nurodytam 14 straipsnio 3 dalyje, gali kilti ne tik dėl fizinio paslaugos neprieinamumo, bet ir įvykus bet kokiam kitam saugumo incidentui, turinčiam neigiamą poveikį tinkamam paslaugos teikimui[33].

Bendradarbiavimo grupėje šiuo metu veikia speciali darbo grupė, rengianti neprivalomas pranešimų teikimo gaires dėl aplinkybių, kuriomis esminių paslaugų operatoriai privalo pranešti apie incidentus pagal 14 straipsnio 7 dalį, taip pat dėl nacionalinių pranešimų formato ir jų teikimo procedūros. Gairės turėtų būti baigtos rengti iki 2017 m. ketvirtojo ketvirčio.

Dėl skirtingų nacionalinių pranešimo reikalavimų taikymo paslaugų teikėjai, vykdantys veiklą tarpvalstybiniu mastu, gali patirti teisinį netikrumą, susidurti su sudėtingesnėmis varžančiomis procedūromis ir turėti didelių administracinių sąnaudų. Todėl Komisija palankiai vertina Bendradarbiavimo grupės darbą. Kaip ir rengiant saugumo reikalavimus, Komisija ragina valstybes nares atidžiai laikytis rekomendacinio dokumento, kurį turi parengti Bendradarbiavimo grupė, kad nacionalinės teisės nuostatos dėl pranešimo apie incidentus būtų kuo labiau suderintos.

4.4. TIS direktyvos III priedas. Skaitmeninių paslaugų teikėjai

Skaitmeninių paslaugų teikėjai yra antroji į TIS direktyvos taikymo sritį įtrauktų subjektų kategorija. Šie subjektai laikomi svarbiais ekonomikos dalyviais, nes daugelis įmonių jų paslaugomis naudojasi savo paslaugoms teikti, todėl skaitmeninės paslaugos teikimo sutrikimas gali turėti poveikį svarbiai ekonominei ir visuomeninei veiklai.

4.4.1. Skaitmeninių paslaugų teikėjų kategorijos

4 straipsnio 5 punkte, kuriame apibrėžiama skaitmeninė paslauga, daroma nuoroda į Direktyvos (ES) 2015/1535 1 straipsnio 1 dalies b punkte pateiktą teisinę apibrėžtį ir apibrėžties aprėptis susiaurinama, į ją įtraukiant tik III priede išvardytų rūšių paslaugas. Tiksliau, Direktyvos (ES) 2015/1535 1 straipsnio 1 dalies b punkte šios paslaugos apibrėžiamos kaip „paprastai už atlyginimą per atstumą, elektroninėmis priemonėmis ir asmenišku paslaugų gavėjo prašymu teikiama paslauga“, o Direktyvos III priede išvardytos trijų konkrečių rūšių paslaugos: elektroninė prekyvietė, interneto paieškos sistema ir debesijos kompiuterijos paslauga. Palyginti su nuostatomis dėl esminių paslaugų operatorių,

[33] Tas pats pasakytina ir apie skaitmeninių paslaugų teikėjus.

Direktyvoje nereikalaujama, kad valstybės narės identifikuotų skaitmeninių paslaugų teikėjus, kuriems būtų taikomos atitinkamos pareigos. Todėl atitinkamos Direktyvoje nustatytos pareigos, t. y. 16 straipsnyje nustatyti saugumo ir pranešimo reikalavimai, bus taikomi visiems skaitmeninių paslaugų teikėjams, kurie patenka į jos taikymo sritį.

Tolesniuose skirsniuose pateikiami papildomai paaiškinamos trys į Direktyvos taikymo sritį įtrauktos paslaugų rūšys.

1. Elektroninės prekyvietės paslaugos teikėjas

Elektroninėje prekyvietėje daugybė įvairių įmonių gali siūlyti savo prekes ir paslaugas vartotojams ir palaikyti tarpusavio santykius. Joje įmonėms suteikiama pagrindinė infrastruktūra, kad jos galėtų prekiauti internetu ir tarpvalstybiniu mastu. Elektroninės prekyvietės atlieka svarbų vaidmenį ekonomikoje, visų pirma naudodamosi jomis MVĮ turi prieigą prie platesnės ES bendrosios skaitmeninės rinkos. Elektroninės prekyvietės paslaugos teikėjo veiklai gali būti priskiriamos ir nuotolinės kompiuterijos paslaugos, kuriomis klientui sudaromos sąlygos vykdyti savo ekonominę veiklą, įskaitant sandorių tvarkymo ir informacijos apie pirkėjus, tiekėjus ir produktus rinkimo paslaugas, taip pat galimybė atlikti atitinkamų produktų paiešką, produktų tiekimas, sandorių tvarkymo paslaugos ir pirkėjų suvedimas su pardavėjais.

Terminas „elektroninė prekyvietė“ apibrėžtas 4 straipsnio 17 punkte ir išsamiau paaiškintas 15 konstatuojamojoje dalyje. Jis apibūdintas kaip paslauga, kuria sudaromos sąlygos vartotojams ir komercinės veiklos subjektams sudaryti elektroninės prekybos arba paslaugų sutartis su komercinės veiklos subjektais, ir yra tokių sutarčių sudarymo galutinė paskirties vieta. Pavyzdžiui, toks skaitmeninių paslaugų teikėjas kaip „E-bay“ gali būti laikomas elektronine prekyviete, nes sudaro sąlygas kitiems asmenims kurti parduotuves jo platformoje, kad šie galėtų internetu teikti savo produktus ir paslaugas vartotojams ar įmonėms. Elektroninės prekyvietės apibrėžtis apima ir internetines taikomųjų programų parduotuves, kuriose platinamos taikomosios programos ir programinė įranga, nes jose programų kūrėjai gali parduoti ar teikti savo paslaugas vartotojams arba kitoms įmonėms. Ir priešingai, trečiųjų šalių paslaugų teikimo tarpininkams, pvz., „Skyscanner“, ir kainų palyginimo paslaugoms, kuriomis pasinaudojęs naudotojas nukreipiamas į komercinės veiklos subjekto svetainę, kurioje ir sudaroma sutartis dėl paslaugos ar produkto, 4 straipsnio 17 punkte pateikta apibrėžtis netaikoma.

2. Interneto paieškos sistemos paslaugų teikėjai

Terminas „interneto paieškos sistema“ apibrėžtas 4 straipsnio 18 punkte ir išsamiau paaiškintas 16 konstatuojamojoje dalyje. Jis apibūdintas kaip skaitmeninė paslauga, kuria sudaromos sąlygos naudotojams vykdyti paiešką iš esmės visose svetainėse arba svetainėse konkrečia kalba, remiantis bet kurio dalyko užklausa. Paieškos funkcijoms, kurios apsiriboja paieška konkrečios svetainės viduje, ir kainų palyginimo svetainėms ši apibrėžtis netaikoma.

Pavyzdžiui, EUR LEX[34] svetainės paieškos sistema negali būti laikoma paieškos sistema, apibrėžta Direktyvoje, nes jos paieškos funkcija apsiriboja tos konkrečios svetainės turiniu.

3. Debesijos kompiuterijos paslaugų teikėjas

4 straipsnio 19 punkte debesijos kompiuterijos paslauga apibrėžta kaip „skaitmeninė paslauga, kuri suteikia prieigą prie kintamo masto pritaikomos bendrų kompiuterijos išteklių bazės“, o 17 konstatuojamojoje dalyje išsamiau paaiškinti terminai „kompiuterijos ištekliai“, „kintamo masto“ ir „pritaikoma bazė“.

Trumpai debesijos kompiuteriją galima apibūdinti kaip kompiuterijos paslaugą, kurią teikiant duomenims apdoroti naudojami bendri ištekliai, o bendri ištekliai yra aparatinės ar programinės įrangos komponentai (pvz., tinklai, serveriai ar kita infrastruktūra, kaupikliai, taikomosios programos ir paslaugos), kurie prireikus tiekiami naudotojams, kad šie galėtų apdoroti duomenis. Bendrais vadinami tokie kompiuterijos ištekliai, kai įvairūs naudotojai naudojasi ta pačia fizine duomenų tvarkymo infrastruktūra. Kompiuterijos išteklius gali būti apibrėžiamas kaip bendras, jeigu paslaugų teikėjo naudojama išteklių bazė bet kuriuo metu gali būti išplėsta arba sumažinta atsižvelgiant į naudotojų poreikius. Taigi duomenų centrai arba atskiri vieno duomenų centro komponentai gali būti pridedami arba pašalinami, jeigu reikia atnaujinti bendrą duomenų saugojimo ar atmintinės talpą. Terminas „pritaikoma bazė“ gali būti apibūdintas kaip darbo krūvio pokyčiai automatiškai pridedant ir šalinant išteklius taip, kad bet kuriuo metu turimi ištekliai kuo geriau atitiktų esamą paklausą[35].

Šiuo metu yra trijų pagrindinių rūšių debesijos paslaugos modeliai, kuriuos gali siūlyti paslaugų teikėjas.

- Paslauginė infrastruktūra (IaaS) – debesijos paslaugų kategorija, kai klientui kaip debesijos paslauga yra teikiama infrastruktūra. Ji apima virtualų kompiuterijos išteklių – aparatinės įrangos, tinklaveikos ir duomenų saugojimo paslaugų – teikimą. IaaS užtikrinamas serverių, kaupiklių, tinklų ir operacinių sistemų veikimas. Teikiant šią paslaugą sukuriama įmonės infrastruktūra, kurioje įmonė gali saugoti savo duomenis ir naudotis savo kasdienei veiklai reikalingomis taikomosiomis programomis.

- Paslauginė platforma (PaaS) – debesijos paslaugų kategorija, kai klientui kaip debesijos paslauga yra teikiama platforma. Ji apima internetines kompiuterijos platformas, kuriose įmonės gali naudotis esamomis taikomosiomis programomis arba kurti ar išbandyti naujas.

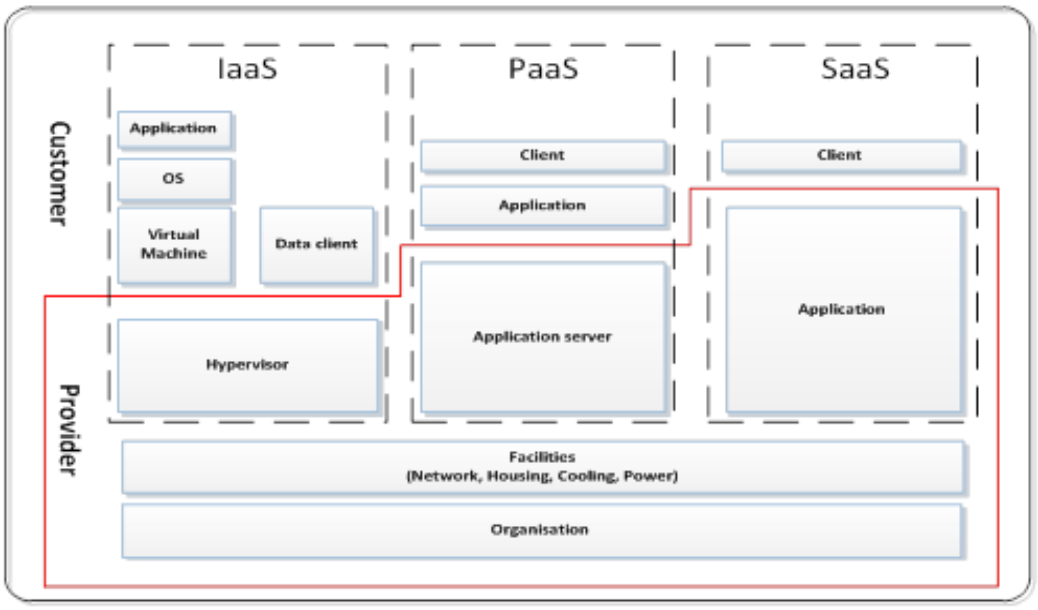
- Paslauginė programinė įranga (SaaS) – debesijos paslaugų kategorija, kai klientui kaip debesijos paslauga yra teikiama taikomoji programa arba programinė įranga, kuria naudojamasi prisijungus internetu. Naudojantis šios rūšies debesijos paslaugomis,

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

[35] Nikolas Roman Herbst, Samuel Kounev, Ralf Reussner, Karlsrūhės technologijų institutas, „Elasticity in Cloud Computing: What It Is, and What It Is Not“, paskelbta: https://sdqweb.ipd.kit.edu/publications/pdfs/HeKoRe2013-ICAC-Elasticity.pdf. Taip pat žr. COM(2012) 529, p. 2–5.

galutiniam naudotojui nebereikia įsigyti, diegti ir valdyti programinės įrangos, o jos pranašumas yra tas, kad programinė įranga yra prieinama iš bet kurios vietos, kur yra interneto ryšys.

5 pav. Debesijos kompiuterijos paslaugų modeliai ir ištekliai



ENISA yra parengusi išsamias gaires konkrečiais debesijos klausimais[36] ir debesijos kompiuterijos rekomendacinį dokumentą[37].

4.4.2. Saugumo reikalavimai

Pagal 16 straipsnio 1 dalį valstybės narės privalo užtikrinti, kad skaitmeninių paslaugų teikėjai imtųsi tinkamų ir proporcingų techninių ir organizacinių priemonių, kad galėtų valdyti riziką, kylančią tinklų ir informacinių sistemų, kuriais įmonės naudojasi teikdamos savo paslaugas, saugumui. Tos saugumo priemonės turėtų remtis naujausiais technikos laimėjimais ir jomis atsižvelgiama į šiuos penkis elementus: i) sistemų ir įrenginių saugumą; ii) incidentų valdymą; iii) veiklos tęstinumo valdymą; iv) stebėseną, auditą ir bandymus; v) atitiktį tarptautiniams standartams.

Šiuo atžvilgiu pagal 16 straipsnio 8 dalį Komisija yra įgaliota priimti įgyvendinimo aktus, kuriais patikslinami šie elementai ir užtikrinamas aukštas šiems paslaugų teikėjams taikomų reikalavimų suderinimo lygis. Numatoma, kad Komisija įgyvendinimo aktą priims 2017 m. rudenį. Be to, valstybės narės privalo užtikrinti, kad skaitmeninių paslaugų teikėjai imtųsi

[36] Paskelbta: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security
[37] ENISA, Debesijos saugumo vadovas MVĮ (angl. *Cloud Security Guide for SMEs*) (2015 m.). Paskelbta: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

reikalingų priemonių, kad būtų išvengta incidentų poveikio ir jis būtų kuo labiau sumažintas, siekiant užtikrinti tų paslaugų tęstinumą.

4.4.3. Pranešimo reikalavimai

Turėtų būti reikalaujama, kad skaitmeninių paslaugų teikėjai apie didelius incidentus praneštų kompetentingoms institucijoms arba CSIRT. Pagal TIS direktyvos 16 straipsnio 3 dalį skaitmeninių paslaugų teikėjai apie saugumo incidentą turės pranešti tais atvejais, kai jis turi didelį poveikį paslaugos teikimui. 16 straipsnio 4 dalyje išvardyti penki parametrai, pagal kuriuos nustatomas poveikio mastas ir į kuriuos visų pirma turi atsižvelgti skaitmeninių paslaugų teikėjai. Pagal 16 straipsnio 8 dalį Komisija yra įgaliota priimti įgyvendinimo aktus, kuriais išsamiau apibūdinami šie parametrai. Šie parametrai bus konkrečiau apibūdinti įgyvendinimo akte, kuriame patikslinami 4.4.2 nurodyti saugumo elementai ir kurį Komisija ketina priimti rudenį.

4.4.4. Rizika pagrįstas reglamentavimo metodas

17 straipsnyje nustatyta, kad nacionalinės kompetentingos institucijos skaitmeninių paslaugų teikėjams turi taikyti *ex post* priežiūros priemones. Valstybės narės privalo užtikrinti, kad kompetentingos institucijos imtųsi veiksmų, kai gauna įrodymų, kad skaitmeninių paslaugų teikėjas nesilaiko Direktyvos 16 straipsnyje nustatytų reikalavimų.

Be to, pagal 16 straipsnio 8 ir 9 dalis Komisija yra įgaliota priimti su saugumo ir pranešimo reikalavimais susijusius įgyvendinimo aktus, kuriais bus užtikrinamas aukštesnis skaitmeninių paslaugų teikėjams taikomų reikalavimų suderinimo lygis. Be to, pagal 16 straipsnio 10 dalį valstybėms narėms neleidžiama nustatyti jokių papildomų saugumo ar pranešimo reikalavimų skaitmeninių paslaugų teikėjams, nei tie, kurie nustatyti Direktyvoje, išskyrus atvejus, kai tokios priemonės būtinos siekiant apsaugoti jų esmines valstybines funkcijas, visų pirma užtikrinti nacionalinį saugumą ir sudaryti sąlygas tirti bei išaiškinti nusikalstamas veikas ir už jas patraukti baudžiamojon atsakomybėn.

Galiausiai, atsižvelgiant į tarpvalstybinį skaitmeninių paslaugų teikėjų veiklos pobūdį, Direktyvoje nesilaikoma daugelio lygiagrečių jurisdikcijų modelio; joje laikomasi požiūrio, grindžiamo bendrovės pagrindinės verslo vietos buvimo ES kriterijumi[38]. Laikantis šio požiūrio, skaitmeninių paslaugų teikėjui taikomas vienas taisyklių rinkinys, o už priežiūrą atsako viena kompetentinga institucija; tai ypač svarbu, nes daugelis skaitmeninių paslaugų teikėjų savo paslaugas vienu metu teikia daugelyje valstybių narių. Laikantis šio požiūrio, skaitmeninių paslaugų teikėjams labai sumažinama reikalavimų laikymosi našta ir užtikrinamas tinkamas bendrosios skaitmeninės rinkos veikimas.

4.4.5. Jurisdikcija

Kaip paaiškinta pirmiau, pagal TIS direktyvos 18 straipsnio 1 dalį skaitmeninių paslaugų teikėjas priklauso valstybės narės, kurioje yra jo pagrindinė verslo vieta, jurisdikcijai. 18 straipsnio 2 dalyje nustatyta, kad tais atvejais, kai konkretus skaitmeninių paslaugų teikėjas teikia paslaugas ES, tačiau nėra įsisteigęs ES teritorijoje, jis privalo paskirti atstovą Sąjungoje.

[38] Žr. visų pirma Direktyvos 18 straipsnį.

Tokiu atveju bendrovė priklauso valstybės narės, kurioje yra įsisteigęs jos atstovas, jurisdikcijai. Tais atvejais, kai skaitmeninių paslaugų teikėjas teikia paslaugas valstybėje narėje, tačiau nėra paskyręs savo atstovo ES, valstybė narė iš esmės gali imtis prieš jį veiksmų, nes paslaugų teikėjas nevykdo įpareigojimų, nustatytų Direktyvoje.

4.4.6. Saugumo ir pranešimo reikalavimų netaikymas riboto masto skaitmeninių paslaugų teikėjams

Pagal 16 straipsnio 11 dalį skaitmeninių paslaugų teikėjams, kurie yra mikroįmonės ar mažosios įmonės, apibrėžtos Komisijos rekomendacijoje 2003/361/EB39, netaikomi 16 straipsnyje nustatyti saugumo ir pranešimo reikalavimai. Tai reiškia, kad įmonės, kuriose dirba mažiau nei 50 darbuotojų ir kurių metinė apyvarta ir (arba) metinis balansas neviršija 10 mln. EUR, neprivalo laikytis tokių reikalavimų. Nustatant subjekto dydį, nesvarbu, ar atitinkama įmonė teikia tik skaitmenines paslaugas, apibrėžtas TIS direktyvoje, ar ji teikia ir kitas paslaugas.

5. TIS direktyvos ir kitų teisės aktų tarpusavio santykis

Šiame skirsnyje daugiausia dėmesio skiriama TIS direktyvos 1 straipsnio 7 dalies nuostatoms dėl *lex specialis*, taip pat pateikiami trys iki šiol Komisijos įvertinti *lex specialis* pavyzdžiai ir paaiškinami saugumo ir pranešimo reikalavimai, taikomi telekomunikacijų ir patikimumo užtikrinimo paslaugų teikėjams.

5.1. TIS direktyvos 1 straipsnio 7 dalis. *Lex specialis* nuostata

Pagal TIS direktyvos 1 straipsnio 7 dalį Direktyvos nuostatos dėl saugumo ir (arba) pranešimo reikalavimų, taikomų skaitmeninių paslaugų teikėjams arba esminių paslaugų operatoriams, netaikomos, jeigu konkrečiam sektoriui skirtame ES teisės akte yra nustatyti saugumo ir (arba) pranešimo reikalavimai, kurių poveikis yra bent lygiavertis TIS direktyvoje nustatytų pareigų poveikiui. Perkeldamos Direktyvą į nacionalinę teisę, valstybės narės turi apsvarstyti 1 straipsnio 7 dalį ir pateikti Komisijai informaciją apie *lex specialis* nuostatų taikymą.

Metodika

Vertinant konkrečiam sektoriui skirto ES teisės akto ir atitinkamų TIS direktyvos nuostatų lygiavertiškumą, visų pirma reikėtų atkreipti dėmesį į klausimą, ar konkrečiam sektoriui skirtame teisės akte nustatytos saugumo užtikrinimo pareigos apima priemones, kuriomis užtikrinamas tinklų ir informacinių sistemų saugumas, apibrėžtas Direktyvos 4 straipsnio 2 punkte.

Pranešimo reikalavimus reglamentuojančiose TIS direktyvos 14 straipsnio 3 dalyje ir 16 straipsnio 3 dalyje nustatyta, kad esminių paslaugų operatoriai ir skaitmeninių paslaugų teikėjai turi be nepagrįsto delsimo pranešti kompetentingai institucijai arba CSIRT apie incidentą, kuris turi didelį poveikį paslaugos teikimui. Šiuo atveju būtina atkreipti ypatingą

[39] OL L 24, 2003 5 20, p. 36.

dėmesį į operatoriaus ir (arba) skaitmeninių paslaugų teikėjo pareigas pranešime pateikti informaciją, kuria remdamasi kompetentinga institucija arba CSIRT galėtų nustatyti tarpvalstybinį saugumo incidento poveikį.

Šiuo metu nėra skaitmeninių paslaugų teikėjų kategorijai skirtų sektorinių teisės aktų, kuriais nustatomi saugumo ir pranešimo reikalavimai, kurie būtų panašūs į TIS direktyvos 16 straipsnyje nustatytus reikalavimus ir į kuriuos būtų galima atsižvelgti taikant TIS direktyvos 1 straipsnio 7 dalį[40].

Kalbant apie esminių paslaugų operatorius, finansų sektoriui ir visų pirma bankininkystės ir finansų rinkų infrastruktūros sektoriui, nurodytiems II priedo 3 ir 4 punktuose, šiuo metu taikomi sektoriniuose ES teisės aktuose nustatyti saugumo ir (arba) pranešimo reikalavimai. Taip yra todėl, kad finansų įstaigų naudojamų IT ir tinklų bei informacinių sistemų saugumas ir patikimumas yra esminė ES teisės aktais finansų įstaigoms nustatytų operacinės rizikos reikalavimų dalis.

Pavyzdžiai

i) Antroji mokėjimo paslaugų direktyva

Bankų sektoriuje, o ypač kredito įstaigų, apibrėžtų Reglamento (ES) Nr. 575/2013 4 straipsnio 1 punkte, teikiamoms mokėjimo paslaugoms taikomi saugumo ir pranešimo reikalavimai nustatyti Antrosios mokėjimo paslaugų direktyvos (toliau – MPD 2)[41] 95 ir 96 straipsniuose.

Tiksliau tariant, 95 straipsnio 1 dalyje reikalaujama, kad mokėjimo paslaugų teikėjai nustatytų atitinkamas rizikos mažinimo priemones ir kontrolės mechanizmus, kuriuos taikant galima valdyti operacinę ir saugumo riziką, susijusią su jų teikiamomis mokėjimo paslaugomis. Šios priemonės turėtų apimti veiksmingų incidentų valdymo procedūrų, įskaitant didelių operacinių ir saugumo incidentų nustatymo ir klasifikavimo procedūras, diegimą ir priežiūrą. MPD 2 95 ir 96 konstatuojamosiose dalyse išsamiau paaiškintas tokių saugumo priemonių pobūdis. Iš šių nuostatų matyti, kad numatytomis priemonėmis siekiama valdyti saugumo riziką, susijusią su tinklų ir informacinėmis sistemomis, naudojamomis teikiant mokėjimo paslaugas. Todėl šių saugumo reikalavimų poveikį galima laikyti bent lygiaverčiu atitinkamų TIS direktyvos 14 straipsnio 1 ir 2 dalių nuostatų poveikiui.

Kalbant apie pranešimo reikalavimus, MPD 2 96 straipsnio 1 dalyje numatyta, kad mokėjimo paslaugų teikėjai privalo nepagrįstai nedelsdami apie didelius saugumo incidentus pranešti kompetentingai institucijai. Be to, panašiai kaip TIS direktyvos 14 straipsnio 5 dalyje, MPD 2 96 straipsnio 2 dalyje reikalaujama, kad kompetentinga institucija apie incidentą informuotų kitų valstybių narių kompetentingas institucijas, jeigu incidentas joms yra svarbus. Kartu ši pareiga reiškia, kad į pranešimus apie saugumo incidentus turi būti įtraukta informacija, pagal kurią institucijos gali įvertinti incidento tarpvalstybinį poveikį. MPD 2 96 straipsnio 3 dalies a

[40] Tai nepažeidžia Bendrojo duomenų apsaugos reglamento 33 straipsnio nuostatų dėl pranešimo priežiūros institucijai apie asmens duomenų saugumo pažeidimą.
[41] Direktyva (ES) 2015/2366, OL L 337, 2015 12 23, p. 35.

punkte Europos bankininkystės institucijai suteikiami atitinkami įgaliojimai bendradarbiaujant su ECB parengti gaires dėl tikslaus pranešimų turinio ir formato.

Taigi galima padaryti išvadą, kad pagal TIS direktyvos 1 straipsnio 7 dalį kredito įstaigų teikiamoms mokėjimo paslaugoms turėtų būti taikomi MPD 2 95 ir 96 straipsniuose nustatyti saugumo ir pranešimo reikalavimai, o ne atitinkamos TIS direktyvos 14 straipsnio nuostatos.

ii) 2012 m. liepos 4 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 648/2012 dėl ne biržos išvestinių finansinių priemonių, pagrindinių sandorio šalių ir sandorių duomenų saugyklų

Kalbant apie finansų rinkų infrastruktūrą, Reglamente (ES) Nr. 648/2012 ir Komisijos deleguotajame reglamente (ES) 153/2013 įtvirtintos nuostatos dėl pagrindinėms sandorio šalims taikomų saugumo reikalavimų, kurios gali būti laikomos *lex specialis.* Visų pirma šiais teisės aktais nustatytos su tinklų ir informacinių sistemų saugumu susijusios techninės ir organizacinės priemonės, kurios yra netgi išsamesnės už TIS direktyvos 14 straipsnio 1 ir 2 dalyse nustatytus reikalavimus, todėl saugumo reikalavimų atžvilgiu gali būti laikomos atitinkančiomis TIS direktyvos 1 straipsnio 7 dalies nuostatas.

Tiksliau tariant, Reglamento (ES) Nr. 648/2012 26 straipsnio 1 dalyje nustatyta, kad subjektas turėtų turėti „tvirtą valdymo tvarką, įskaitant aiškią organizacinę struktūrą su tiksliai apibrėžta, skaidria ir nuoseklia atsakomybe, veiksmingus rizikos, su kuria ji[s] susiduria arba gali susidurti, nustatymo, valdymo, stebėjimo ir pranešimo apie tokią riziką procesus ir tinkamus vidaus kontrolės mechanizmus, įskaitant patikimas administracines ir apskaitos procedūras“. 26 straipsnio 3 dalyje nustatyta, kad, naudojant tinkamas ir proporcingas sistemas, išteklius ir procedūras, organizacinė struktūra turi užtikrinti tęstinumą ir tinkamą veikimą teikiant paslaugas ir vykdant veiklą.

26 straipsnio 6 dalyje taip pat paaiškinta, kad pagrindinė sandorio šalis turi naudoti „informacinių technologijų sistemas, kurios yra tinkamos atsižvelgiant į teikiamų paslaugų ir vykdomos veiklos sudėtingumą, įvairovę ir rūšis, siekiant užtikrinti griežtus apsaugos standartus ir saugomos informacijos vientisumą ir konfidencialumą“. Be to, 34 straipsnio 1 dalyje nustatyta, kad turi būti parengta, įdiegta ir taikoma tinkama veiklos tęstinumo politika ir veiklos atkūrimo planas, kuriais turėtų būti užtikrinama, kad būtų laiku atkurta veikla.

Šios pareigos tiksliau nustatytos 2012 m. gruodžio 19 d. Komisijos deleguotajame reglamente (ES) Nr. 153/2013, kuriuo Europos Parlamento ir Tarybos reglamentas (ES) Nr. 648/2012 papildomas nuostatomis dėl pagrindinėms sandorio šalims taikomų reikalavimų techninių reguliavimo standartų[42]. Visų pirma Reglamento (ES) Nr. 153/2013 4 straipsnyje pagrindinėms sandorio šalims nustatoma pareiga parengti tinkamas rizikos valdymo priemones, kad jos galėtų valdyti visą svarbią riziką ir apie ją teikti ataskaitas, ir toliau nurodomos tų priemonių rūšys (pvz., naudoti atsparias informacines ir rizikos kontrolės sistemas, turėti rizikos valdymui užtikrinti būtinus išteklius, kompetenciją ir galimybę susipažinti su visa svarbia informacija, turėti tinkamus vidaus kontrolės mechanizmus, kurie

[42] OL L 52, 2013 2 23, p. 41.

padeda pagrindinių sandorio šalių valdybai stebėti ir vertinti jos rizikos valdymo politikos, procedūrų ir sistemų tinkamumą ir veiksmingumą, pvz., patikimas administracines ir apskaitos procedūras).

Be to, 9 straipsnyje aiškiai kalbama apie informacinių technologijų sistemų saugumą ir nustatomos konkrečios techninės ir organizacinės priemonės, susijusios su patikimos informacijos saugumo sistemos, skirtos IT saugumo rizikai valdyti, priežiūra. Tokios priemonės turėtų apimti mechanizmus ir procedūras, kuriais garantuojama galimybė naudotis paslaugomis ir užtikrinamas duomenų autentiškumas, vientisumas ir konfidencialumas.

iii) 2014 m. gegužės 15 d. Europos Parlamento ir Tarybos direktyva 2014/65/ES dėl finansinių priemonių rinkų, kuria iš dalies keičiamos Direktyva 2002/92/EB ir Direktyva 2011/61/ES[43].

Kalbant apie prekybos vietas, Direktyvos 2014/65/ES 48 straipsnio 1 dalyje reikalaujama, kad operatoriai užtikrintų savo paslaugų tęstinumą, jei įvyktų bet koks jų prekybos sistemų gedimas. Ši bendroji pareiga neseniai buvo išsamiau apibrėžta ir papildyta 2016 m. liepos 14 d. Komisijos deleguotajame reglamente (ES) 2017/584[44], kuriuo Europos Parlamento ir Tarybos direktyva 2014/65/ES papildoma techniniais reguliavimo standartais, kuriais patikslinami prekybos vietoms taikomi organizaciniai reikalavimai[45]. Visų pirma, šio reglamento 23 straipsnio 1 dalyje nustatyta, kad prekybos vietos turi turėti fizinio ir elektroninio saugumo procedūras ir priemones, kurių paskirtis – apsaugoti savo sistemas nuo netinkamo naudojimo ar neteisėtos prieigos ir užtikrinti duomenų vientisumą. Šiomis priemonėmis turėtų būti sudarytos sąlygos išvengti išpuolių prieš informacines sistemas arba kuo labiau sumažinti jų riziką.

23 straipsnio 2 dalyje taip pat reikalaujama, kad operatorių taikomomis priemonėmis ir tvarka būtų sudarytos sąlygos greitai nustatyti ir valdyti riziką, susijusią su neteisėta prieiga, sistemos trukdžiais, dėl kurių labai sutrikdomas arba nutraukiamas informacinių sistemų veikimas, ir duomenų trukdžiais, dėl kurių kyla pavojus duomenų prieinamumui, vientisumui ir autentiškumui. Be to, reglamento 15 straipsnyje prekybos vietoms nustatyta pareiga įdiegti veiksmingas veiklos tęstinumo priemones, skirtas pakankamam sistemos stabilumui užtikrinti ir trukdžių sukeliantiems incidentams pašalinti. Visų pirma šiomis priemonėmis operatoriui turėtų būti sudarytos sąlygos prekybą atnaujinti per dvi arba beveik dvi valandas ir kartu užtikrinti, kad prarastų duomenų kiekis būtų artimas nuliui.

16 straipsnyje taip pat nurodyta, kad nustatytos trukdžių sukeliančių incidentų sprendimo ir valdymo priemonės turėtų būti įtrauktos į prekybos vietų veiklos tęstinumo planą, ir numatyti konkretūs elementai, kuriuos operatorius turi apsvarstyti priimdamas veiklos tęstinumo planą (pvz., specialios saugumo operacijų grupės sukūrimas, poveikio vertinimo, kurio metu nustatoma sutrikdymo rizika, atlikimas ir periodinė peržiūra).

[43] OL L 173, 2014 6 12, p. 349.
[44] OL L 87, 2017 3 31, p. 350.
[45] http://ec.europa.eu/finance/securities/docs/isd/mifid/rts/160714-rts-7_en.pdf

Šių saugumo priemonių turinys rodo, kad jos skirtos su duomenų ar teikiamų paslaugų prieinamumu, autentiškumu, vientisumu ir konfidencialumu susijusiai rizikai valdyti ir šalinti, taigi galima padaryti išvadą, kad pirmiau nurodytais sektoriniais ES teisės aktais nustatomos saugumo užtikrinimo pareigos, kurių poveikis yra bent lygiavertis TIS direktyvos 14 straipsnio 1 ir 2 dalyse nustatytų pareigų poveikiui.

5.2. TIS direktyvos 1 straipsnio 3 dalis. Telekomunikacijų ir patikimumo užtikrinimo paslaugų teikėjai

Remiantis 1 straipsnio 3 dalimi, Direktyvoje nustatyti saugumo ir pranešimo reikalavimai netaikomi paslaugų teikėjams, kuriems taikomi Direktyvos 2002/21/EB 13a ir 13b straipsniuose nustatyti reikalavimai. Direktyvos 2002/21/EB 13a ir 13b straipsniuose nustatyti reikalavimai taikomi įmonėms, teikiančioms viešųjų ryšių tinklų paslaugas arba viešai prieinamas elektroninių ryšių paslaugas. Taigi viešųjų ryšių tinklų paslaugas arba viešai prieinamas elektroninių ryšių paslaugas teikianti įmonė turi laikytis Direktyvoje 2002/21/EB nustatytų saugumo ir pranešimo reikalavimų.

Tačiau, jeigu ta pati įmonė teikia ir kitas paslaugas, kaip antai TIS direktyvos III priede nurodytas skaitmenines paslaugas (pvz., debesijos kompiuterijos ar elektroninės prekyvietės) arba tokias paslaugas kaip DNS ar IXP pagal TIS direktyvos II priedo 7 punktą, teikdama šias konkrečias paslaugas ji turės laikyti TIS direktyvoje nustatytų saugumo ir pranešimo reikalavimų. Reikėtų pažymėti, jog dėl to, kad II priedo 7 punkte nurodytų paslaugų teikėjai priklauso esminių paslaugų operatorių kategorijai, valstybės narės privalo vykdyti identifikavimo procesą pagal 5 straipsnio 2 dalį ir nustatyti, kurie konkretūs DNS, IXP ar ALD paslaugų teikėjai turėtų laikytis TIS direktyvos reikalavimų. Tai reiškia, kad, atlikus tokį vertinimą, TIS direktyvos reikalavimų privalės laikytis tik tie DNS, IXP ar ALD paslaugų teikėjai, kurie atitiks TIS direktyvos 5 straipsnio 2 dalyje nustatytus kriterijus.

Be to, 1 straipsnio 3 dalyje nurodyta, kad Direktyvoje nustatyti saugumo ir pranešimo reikalavimai taip pat netaikomi patikimumo užtikrinimo paslaugų teikėjams, kuriems taikomi panašūs Reglamento (ES) Nr. 910/2014 19 straipsnyje nustatyti reikalavimai.

6. Paskelbti nacionalinių kibernetinio saugumo strategijų dokumentai

	Valstybė narė	Strategijos pavadinimas ir susijusios nuorodos
1.	Austrija	Austrijos kibernetinio saugumo strategija (angl. *Austrian Cybersecurity Strategy*) (2013 m.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf (EN)
2.	Belgija	Kibernetinės erdvės saugumo užtikrinimas (angl. *Securing Cyberspace*) (2012 m.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ncss-be-fr (FR)
3.	Bulgarija	Strategija iki 2020 m. „Kibernetiniams išpuoliams atspari Bulgarija“ (angl. *Cyber Resilient Bulgaria 2020*) (2016 m.) http://www.cyberbg.eu/ (BG)
4.	Kroatija	Kroatijos Respublikos nacionalinė kibernetinio saugumo strategija (angl. *The national cyber security strategy of the republic of Croatia*) (2015 m.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf (EN)
5.	Čekija	2015–2020 m. Čekijos nacionalinė kibernetinio saugumo strategija (angl. *National cyber security strategy of the Czech Republic for the period from 2015 to 2020*) (2015 m.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (EN)
6.	Kipras	Kipro Respublikos kibernetinio saugumo strategija (angl. *Cybersecurity Strategy of the Republic of Cyprus*) (2012 m.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf (EN)
7.	Danija	Danijos kibernetinio ir informacijos saugumo strategija (angl. *The Danish Cyber and Information Security Strategy*) (2015 m.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/DK_NCSS.pdf (EN)
8.	Estija	Kibernetinio saugumo strategija (angl. *Cyber Security Strategy*) (2014 m.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf (EN)

9.	Suomija	Suomijos kibernetinio saugumo strategija (angl. *Finland's Cyber security Strategy*) (2013 m.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf (EN)
10.	Prancūzija	Prancūzijos nacionalinė skaitmeninio saugumo strategija (angl. *French national digital security strategy*) (2015 m.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf (EN)
11.	Airija	2015–2017 m. nacionalinė kibernetinio saugumo strategija (angl. *National Cyber Security Strategy 2015–2017*) (2015 m.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf (EN)
12.	Italija	Nacionalinė strateginė kibernetinės erdvės saugumo programa (angl. *National Strategic Framework for Cyberspace Security*) (2013 m.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf (EN)
13.	Vokietija	Vokietijos kibernetinio saugumo strategija (angl. *Cyber-security Strategy for Germany*) (2016 m.) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/ModerneVerwaltung-OeffentlicherDienst/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile (DE)
14.	Vengrija	Vengrijos nacionalinė kibernetinio saugumo strategija (angl. *National Cyber Security Strategy of Hungary*) (2013 m.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf (EN)
15.	Latvija	2014–2018 m. Latvijos kibernetinio saugumo strategija (angl. *Cyber Security Strategy of Latvia 2014–2018*) (2014 m.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (EN)
16.	Lietuva	Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa (angl. *The programme for the development of electronic information security (cyber-security) for 2011–2019*) (2011 m.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf (EN)
17.	Liuksemburgas	2-oji nacionalinė kibernetinio saugumo strategija (angl. *National Cybersecurity Strategy II*) *(2015 m.)* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf (EN)
18.	Malta	Nacionalinės kibernetinio saugumo strategijos žalioji knyga (angl.

		National Cyber Security Strategy Green Paper) (2015 m.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGreenPaper.pdf (EN)
19.	Nyderlandai	2-oji nacionalinė kibernetinio saugumo strategija (angl. *National Cyber Security Strategy 2*) (2013 m.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf (EN)
20.	Lenkija	Lenkijos Respublikos kibernetinės erdvės apsaugos politika (angl. *Cyberspace Protection Policy of the Republic of Poland*) (2013 m.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf (EN)
21.	Rumunija	Rumunijos kibernetinio saugumo strategija (angl. *Cybersecurity Strategy of Romania*) (2011 m.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf (RO)
22.	Portugalija	Nacionalinė kibernetinio saugumo strategija (angl. *National Cyberspace Security Strategy*) (2015 m.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/portuguese-national-cyber-security-strategy/view (EN)
23.	Slovakijos Respublika	2015–2020 m. Slovakijos Respublikos kibernetinio saugumo koncepcija (angl. *Cyber Security Concept of the Slovak Republic for 2015 – 2020*) (2015 m.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 (EN)
24.	Slovėnija	Kibernetinio saugumo strategija, kuria nustatoma aukšto lygio kibernetinio saugumo užtikrinimo sistema (angl. *Cyber Security Strategy establishing a system to ensure a high level of cyber security*) (2016 m.) http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf (EN)
25.	Ispanija	Nacionalinė kibernetinio saugumo strategija (angl. *National Cyber Security Strategy*) (2013 m.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf (EN)
26.	Švedija	Švedijos nacionalinė kibernetinio saugumo strategija (angl. *The Swedish National Cybersecurity Strategy*) (2017 m.) http://www.government.se/49edf4/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy.pdf (EN)

27.	Jungtinė Karalystė	2016–2021 m. nacionalinė kibernetinio saugumo strategija (angl. *National Cyber Security Strategy (2016-2021)* (2016 m.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf (EN)

7. ENISA paskelbtos gerosios patirties ir rekomendacijų sąrašas

Reagavimas į incidentus

- ✓ Reagavimo į incidentus ir bendradarbiavimo kilus kibernetinei krizei strategijos[46]

Incidentų valdymas

- ✓ Incidentų valdymo automatizavimo projektas[47]
- ✓ Incidentų valdymo gerosios patirties vadovas[48]

Incidentų klasifikacija ir taksonomija

- ✓ Esamų taksonomijų apžvalga[49]
- ✓ Taksonomijų naudojimo incidentų prevencijos ir nustatymo srityje gerosios patirties vadovas[50]

CSIRT branda

- ✓ 2016 m. nacionalinių CSIRT uždaviniai Europoje. CSIRT brandos tyrimas[51]
- ✓ CSIRT brandos tyrimas – vertinimo procesas[52]
- ✓ Nacionalinėms ir valstybinėms CSIRT skirtos brandos vertinimo gairės[53]

CSIRT gebėjimų stiprinimas ir mokymas

- ✓ Mokymo metodikų gerosios patirties vadovas[54]

Informacija apie Europoje veikiančias CSIRT – CSIRT apžvalga pagal šalis[55]

[46] ENISA, *Strategies for incident response and cyber crisis cooperation* (2016 m.). Paskelbta:https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation

[47] Daugiau informacijos: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation.

[48] ENISA, *Good Practice Guide for Incident Management* (2010 m.). Paskelbta:https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management.

[49] Daugiau informacijos: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies.

[50] ENISA, *A good practice guide of using taxonomies in incident prevention and detection* (2017 m.). Paskelbta:https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection.

[51] ENISA, *Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity* (2017 m.). Paskelbta:https://www.enisa.europa.eu/publications/study-on-csirt-maturity.

[52] ENISA, *Study on CSIRT Maturity – Evaluation Process* (2017 m.). Paskelbta:https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process.

[53] ENISA, *CSIRT Capabilities*. *How to assess maturity? Guidelines for national and governmental CSIRTs* (2016 m.) Paskelbta: https://www.enisa.europa.eu/publications/csirt-capabilities.

[54] ENISA, *Good Practice Guide on Training Methodologies* (2014 m.). Paskelbta:https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies.

[55] Daugiau informacijos: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map.