EUROOPA
KOMISJON

Brüssel, 4.10.2017
COM(2017) 476 final

ANNEX 1

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

LISA

järgmise dokumendi juurde:

KOMISJONI TEATIS EUROOPA PARLAMENDILE JA NÕUKOGULE

Parimate tulemuste saavutamine võrgu- ja infoturbe direktiivi rakendamisel – jõupingutused direktiivi (EL) 2016/1148 (meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus) tulemuslikuks rakendamiseks

SISUKORD

LISA

1. Sissejuhatus

Käesoleva lisa eesmärk on edendada võrgu- ja infosüsteemide turvalisust kogu liidus käsitleva võrgu- ja infoturbe direktiivi (EL) 2016/1148[1] (edaspidi „võrgu- ja infoturbe direktiiv“ või „direktiiv“) tulemuslikku kohaldamist, rakendamist ja täitmist ning aidata liikmesriikidel tagada liidu õiguse tulemuslik rakendamine. Täpsemalt on sellel kolm erieesmärki: a) selgitada riigi ametiasutustele nende suhtes kohaldatavaid direktiivis sisalduvaid kohustusi, b) tagada nende direktiivis sätestatud kohustuste tulemuslik täitmine, mida kohaldatakse üksuste suhtes, kellel on turvanõuete ja intsidentidest teatamisega seotud kohustused, ning c) aidata üldiselt tagada õiguskindlus kõigi asjaomaste osalejate jaoks.

Selleks antakse käesolevas lisas suuniseid järgmiste küsimuste kohta, mis on olulised võrgu- ja infoturbe direktiivi eesmärgi saavutamiseks ehk ELi võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge taseme tagamiseks, mis toetab meie ühiskonna ja majanduse toimimist:

- liikmesriikide kohustus vastu võtta riiklik võrgu- ja infosüsteemide turvalisuse strateegia (punkt 2);
- riiklike pädevate asutuste, ühtsete kontaktpunktide ja küberturbe intsidentide lahendamise üksuste loomine (punkt 3);
- oluliste teenuste operaatorite ja digitaalse teenuse osutajate suhtes kohaldatavad turvanõuded ja intsidentidest teatamise kohustus (punkt 4) ning
- võrgu- ja infoturbe direktiivi ja muude õigusaktide vaheline seos (punkt 5).

Komisjon kasutas nende suuniste koostamisel direktiivi ettevalmistamise käigus kogutud teavet ja analüüse ning Euroopa Liidu Võrgu- ja Infoturbeameti (edaspidi „ENISA“) ja koostöörühma panust. Samuti kasutati konkreetsete liikmesriikide kogemusi. Komisjon võttis vajaduse korral arvesse liidu õiguse tõlgendamise juhtpõhimõtteid: võrgu- ja infoturbe direktiivi sõnastust, konteksti ja eesmärke. Kuna direktiiv on seni üle võtmata, ei ole Euroopa Liidu Kohus ega siseriiklikud kohtud selleteemalisi otsuseid veel teinud. Kohtupraktikast juhindumine ei ole seetõttu võimalik.

Teabe koondamine ühtsesse dokumenti võimaldab liikmesriikidel saada direktiivist hea ülevaate ja võtta seda teavet arvesse siseriiklike õigusaktide väljatöötamisel. Komisjon toonitab siiski, et käesolev lisa ei ole siduv ja selle eesmärk ei ole kehtestada uusi eeskirju. Lõplik pädevus liidu õiguse tõlgendamisel kuulub Euroopa Liidu Kohtule.

[1] Euroopa Parlamendi ja nõukogu 6. juuli 2016. aasta direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus. Direktiiv jõustus 8. augustil 2016.

2. Riiklik võrgu- ja infosüsteemide turvalisuse strateegia

Võrgu- ja infoturbe direktiivi artikli 7 kohaselt on liikmesriigid kohustatud vastu võtma riikliku võrgu- ja infosüsteemide turvalisuse strateegia, mida võib pidada samaväärseks mõistega „riiklik küberjulgeoleku strateegia“. Riikliku strateegia ülesanne on kindlaks määrata küberturvalisusega seotud strateegilised eesmärgid ning asjakohased regulatiivsed ja poliitikameetmed. Riikliku küberjulgeoleku strateegia mõistet kasutatakse laialdaselt nii rahvusvahelisel kui ka Euroopa tasandil, eelkõige ENISA koostöös liikmesriikidega riiklike strateegiate väljatöötamiseks, mille tulemusel avaldati hiljuti ajakohastatud riikliku küberjulgeoleku strateegia hea tava juhend[2].

Käesolevas punktis kirjeldab komisjon, kuidas võrgu- ja infoturbe direktiiv edendab liikmesriikide valmisolekut, nõudes tõhusate riiklike võrgu- ja infosüsteemide turvalisuse strateegiate kehtestamist (artikkel 7). Selles punktis käsitletakse järgmisi aspekte: a) strateegia kohaldamisala ning b) sisu ja vastuvõtmiskord.

Nagu allpool täpsemalt kirjeldatud, on võrgu- ja infoturbe direktiivi artikli 7 nõuetekohane ülevõtmine direktiivi eesmärkide saavutamiseks määrava tähtsusega ning selleks on vaja eraldada piisavad rahalised vahendid ja inimressursid.

2.1. Riikliku strateegia kohaldamisala

Artikli 7 sõnastuse kohaselt hõlmab riikliku küberjulgeoleku strateegia vastuvõtmise kohustus üksnes II lisas osutatud sektoreid (s.o energeetika, transport, pangandus, finantsturg, tervishoid, joogivee varustus ja jaotamine ning digitaalne taristu) ja III lisas osutatud teenuseid (internetipõhine kauplemiskoht, internetipõhine otsingumootor ja pilvandmetöötlusteenus).

Direktiivi artiklis 3 on konkreetselt sätestatud minimaalse ühtlustamise põhimõte, mille kohaselt liikmesriigid võivad vastu võtta või säilitada sätteid eesmärgiga saavutada võrgu- ja infosüsteemide turvalisuse kõrgem tase. Selle põhimõtte kohaldamine riikliku küberjulgeoleku strateegia vastuvõtmise kohustuse suhtes võimaldab liikmesriikidel hõlmata rohkem sektoreid ja teenuseid kui need, mida on nimetatud direktiivi II ja III lisas.

Lähtudes võrgu- ja infoturbe direktiivi eesmärgist saavutada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus,[3] on komisjoni arvates soovitatav välja töötada riiklik strateegia, mis hõlmab kõiki ühiskonna ja majanduse asjaomaseid mõõtmeid, mitte üksnes võrgu- ja infoturbe direktiivi II ja III lisas käsitletud sektoreid ja digitaalseid teenuseid. See on kooskõlas nii rahvusvaheliste parimate tavade (vt Rahvusvahelise Telekommunikatsiooni Liidu (ITU) suunised ja OECD analüüs, millele osutatakse edaspidi) kui ka võrgu- ja infoturbe direktiiviga.

[2] ENISA, „National Cyber-Security Strategy Good Practice“ (Riikliku küberjulgeoleku strateegia hea tava juhend), 2016. Avaldatud aadressil https://www.enisa.europa.eu/publications/ncss-good-practice-guide.
[3] Vt artikli 1 lõige 1.

Nagu edaspidi põhjalikumalt selgitatakse, puudutab see eelkõige haldusasutusi, kes vastutavad sektorite ja teenuste eest, mida ei ole direktiivi II ja III lisas loetletud. Haldusasutused võivad töödelda tundlikku teavet, mida tuleb hõlmata riikliku küberjulgeoleku strateegia ja halduskavadega, millega hoitakse ära teabelekked ja tagatakse teabe vajalik kaitse.

2.2. Riiklike strateegiate sisu ja vastuvõtmiskord

Vastavalt võrgu- ja infoturbe direktiivi artiklile 7 tuleb riiklikus küberjulgeoleku strateegias käsitleda vähemalt järgmisi küsimusi:

i) riikliku võrgu- ja infosüsteemide turvalisuse strateegia eesmärgid ja prioriteedid;
ii) juhtimisraamistik, mille toel riikliku strateegia eesmärgid ja prioriteedid ellu viia;
iii) valmisoleku-, reageerimis- ja taastemeetmete, sh avaliku ja erasektori koostöö kindlaksmääramine;
iv) asjakohaste haridus-, teadlikkuse suurendamise ja koolitusprogrammide kirjeldus;
v) teadus- ja arendustegevuse kavade kirjeldus;
vi) riskihindamiskava riskide kindlakstegemiseks ja
vii) mitmesuguste strateegia rakendamises osalevate osalejate loetelu.

Ei artiklis 7 ega sellele vastavas põhjenduses 29 ei ole sätestatud riikliku küberjulgeoleku strateegia vastuvõtmise nõudeid ega täpsustatud selle sisu. Mis puudutab protsessi ja riikliku küberjulgeoleku strateegia sisuga seotud täiendavaid elemente, siis komisjon peab kõnealuse strateegia vastuvõtmisel asjakohaseks allpool esitatud lähenemisviisi. See põhineb analüüsil, mis hindas liikmesriikide ja kolmandate riikide kogemusi selle kohta, kuidas liikmesriigid on oma strateegiaid välja töötanud. Täiendava teabe allikas on ENISA riikliku küberjulgeoleku strateegia koolitusvahend, mis koosneb videoklippidest ja mida saab alla laadida ameti veebisaidilt[4].

2.3. Protsess ja käsitlemist vajavad teemad

Riikliku strateegia väljatöötamise ja vastuvõtmise protsess on keeruline ja mitmekülgne ning nõuab tulemuslikkuse ja edukuse tagamiseks küberturvalisuse ekspertide, kodanikuühiskonna ja riigi poliitilise protsessi pidevat kaasamist. Vältimatu eeltingimus on kõrgema haldustasandi toetus vähemalt riigisekretäri tasandil või juhtministeeriumi samaväärsel tasandil ning poliitiline tugi. Riikliku küberjulgeoleku strateegia edukaks vastuvõtmiseks võib kaaluda järgmist viieetapilist protsessi (vt joonis 1).

Esimene etapp. **Strateegia juhtpõhimõtete ja strateegiliste eesmärkide kehtestamine**

Esmalt peavad riiklikud pädevad asutused kindlaks määrama mõned riikliku küberjulgeoleku strateegia olulised punktid, täpsemalt soovitud tulemused ehk direktiivi (artikli 7 lõike 1 punkt a) sõnastuses „eesmärgid ja prioriteedid“ ning selle, kuidas need tulemused täiendavad riiklikku sotsiaal- ja majanduspoliitikat ja kas need on kooskõlas Euroopa Liidu liikmesriigi staatusega kaasnevate eesõiguste ja kohustustega. Eesmärgid peaksid olema konkreetsed,

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

mõõdetavad, saavutatavad, realistlikud ja tähtajalised (nn SMART-põhimõte). Näiteks: „Me tagame, et see [tähtajaline] strateegia põhineb rangetel ja terviklikel parameetritel, millest lähtudes me mõõdame edusamme tulemuste saavutamisel“[5].

See hõlmab ka poliitilist hinnangut selle kohta, kas strateegia rakendamise rahastamiseks saadakse märkimisväärsed eelarvelised vahendid. Samuti hõlmab see strateegia kavandatud kohaldamisala ning erinevaid avaliku ja erasektori sidusrühmade kategooriaid, kes peaksid eesmärkide ja meetmete kavandamises osalema.

Esimese etapi läbiviimist toetavad sihipärased seminarid ministeeriumide kõrgematele ametnikele ja poliitikutele, mida juhivad professionaalsete kommunikatsioonioskustega küberspetsialistid, kes oskavad selgitada, millised tagajärjed on vähesel küberturvalisusel või selle puudumisel tänapäeva digitaalsele majandusele ja ühiskonnale.

Teine etapp. **Strateegia sisu väljatöötamine**

Strateegia peab sisaldama toetavaid meetmeid, ajapõhiseid meetmeid ja peamisi tulemusnäitajaid, mille alusel toimub pärast kindlaksmääratud rakendusperioodi hindamine, täiustamine ja parandamine. Need meetmed peavad toetama juhtpõhimõtetes nimetatud eesmärke, prioriteete ja tulemusi. Toetavate meetmete kaasamise vajadus on sätestatud võrgu- ja infoturbe direktiivi artikli 7 lõike 1 punktis c.

Strateegia koostamise juhtimiseks ja panuse andmise lihtsustamiseks on soovitatav moodustada juhtministeeriumi juhitav juhtrühm. Selle saavutamiseks võib kasutada asjaomastest ametnikest ja ekspertidest koosnevaid redaktsioonirühmasid, mis tegelevad peamiste teemavaldkondadega, nagu riskihindamine, erandolukorra plaanimine, intsidentide haldamine, oskuste arendamine, teadlikkuse suurendamine, uurimistegevus, tööstuslik areng jne. Igal sektoril (nt energeetika, transport jne) palutakse ka eraldi hinnata nende kaasamise, sealhulgas vahendite eraldamise mõju ning kaasata prioriteetide kindlakstegemisse ja strateegia koostamise kohta ettepanekute tegemisse määratud oluliste teenuste operaatorid ja peamised digitaalse teenuse osutajad. Valdkondlike sidusrühmade kaasamine on oluline ka selle poolest, et direktiivi on vaja ühetaoliselt rakendada kõigis sektorites, võttes siiski arvesse nende eripära.

Kolmas etapp. **Juhtimisraamistiku väljatöötamine**

Selleks et juhtimisraamistik oleks tõhus ja tulemuslik, peab see tuginema peamistele sidusrühmadele ja lähtuma strateegia koostamisel kindlakstehtud prioriteetidest ning riiklike haldus- ja poliitiliste struktuuride piirangutest ja taustast. Soovitatav on sisse seada otsene aruandlus poliitikatasandile, kusjuures raamistikul on otsuste tegemise ja ressursside eraldamise võimekus, ning saada sisendeid küberturvalisuse ekspertidelt ja tööstusharu sidusrühmadelt. Võrgu- ja infoturbe direktiivi artikli 7 lõike 1 punktis b osutatakse juhtimisraamistikule ja märgitakse konkreetselt, et „see hõlmab valitsusasutuste ning muude asjaomaste osalejate [...] vastutust“.

[5] Väljavõte Ühendkuningriigi riiklikust küberjulgeoleku strateegiast aastateks 2016–2021, lk 67.

Neljas etapp. **Strateegia kavandi koostamine ja läbivaatamine**

Selles etapis tuleb koostada strateegia kavand ja see läbi vaadata, kasutades SWOT-analüüsi, millega tehakse kindlaks sisu muutmise vajadus. Pärast ametisisest läbivaatamist tuleks konsulteerida sidusrühmadega. Oluline on ka läbi viia avalik konsultatsioon, et rõhutada kavandatava strateegia tähtsust üldsusele, saada kõikidest võimalikest allikatest sisendeid ja leida toetust strateegia rakendamise rahastamisele.

Viies etapp. **Ametlik vastuvõtmine**

Viimane etapp hõlmab strateegia ametlikku vastuvõtmist poliitilisel tasandil koos seda toetava eelarvega, mis näitab, kui tõsiselt asjaomased liikmesriigid küberturvalisusesse suhtuvad. Võrgu- ja infoturbe direktiivi eesmärkide saavutamiseks julgustab komisjon liikmesriike esitama teavet eelarve kohta, kui nad edastavad komisjonile riikliku strateegia kooskõlas artikli 7 lõikega 3. Strateegia ja direktiivi tulemuslikuks rakendamiseks on äärmiselt oluline täita eelarve ja vajalike inimressurssidega seotud kohustusi. Kuna küberturvalisus on ikka veel suhteliselt uus ja kiiresti laienev avaliku poliitika valdkond, on enamikul juhtudel vaja uusi investeeringuid, isegi kui riigi rahanduse üldine olukord nõuab kärpeid ja säästmist.

Nõuanded protsessi ja riiklike strateegiate sisu kohta on kättesaadavad erinevates avalikes ja akadeemilistes allikates, nagu ENISA,[6] ITU,[7] OECD,[8] kübereksperte ülemaailmne koostööfoorum ja Oxfordi Ülikool[9].

2.4. Konkreetsed sammud, mida liikmesriigid peavad astuma enne ülevõtmise tähtaega

Enne direktiivi vastuvõtmist olid peaaegu kõik liikmesriigid[10] avaldanud dokumendi, millele viidati kui riiklikule küberturvalisuse strateegiale. Käesoleva lisa punktis 6 loetletakse praegu liikmesriikides kehtivad strateegiad[11]. Tavaliselt hõlmavad need strateegilisi põhimõtteid,

[6] ENISA, „National Cyber-Security Strategy Good Practice“ (Riikliku küberjulgeoleku strateegia hea tava juhend), 2016. Avaldatud aadressil https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

[7] ITU, „National Cybersecurity Strategy Guide“ (Riikliku küberjulgeoleku strateegia juhend), 2011. Avaldatud aadressil http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf. ITU avaldab 2017. aastal ka riikliku küberturvalisuse strateegia töövahendi (vt esitlus aadressil http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf).

[8] OECD, „Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies“ (Küberturvalisuse poliitika kujundamise pöördepunkt: riiklike küberturvalisuse strateegiate uue põlvkonna analüüs), 2012. Avaldatud aadressil http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.

[9] Global Cyber Security Capacity Centre (ülemaailmne küberturvalisuse kompetentsikeskus) ja Oxfordi Ülikool, „Global Cybersecurity Capacity Maturity Model for Nations (CMM)“ (Küberjulgeolekualase suutlikkuse küpsusmudel riikidele), muudetud trükk, 2016. Avaldatud aadressil https://www.thegfce.com/binaries/gfce/documents/publications/2017/02/13/cybersecurity-cmm-for-nations/CMM+revised+edition.pdf.

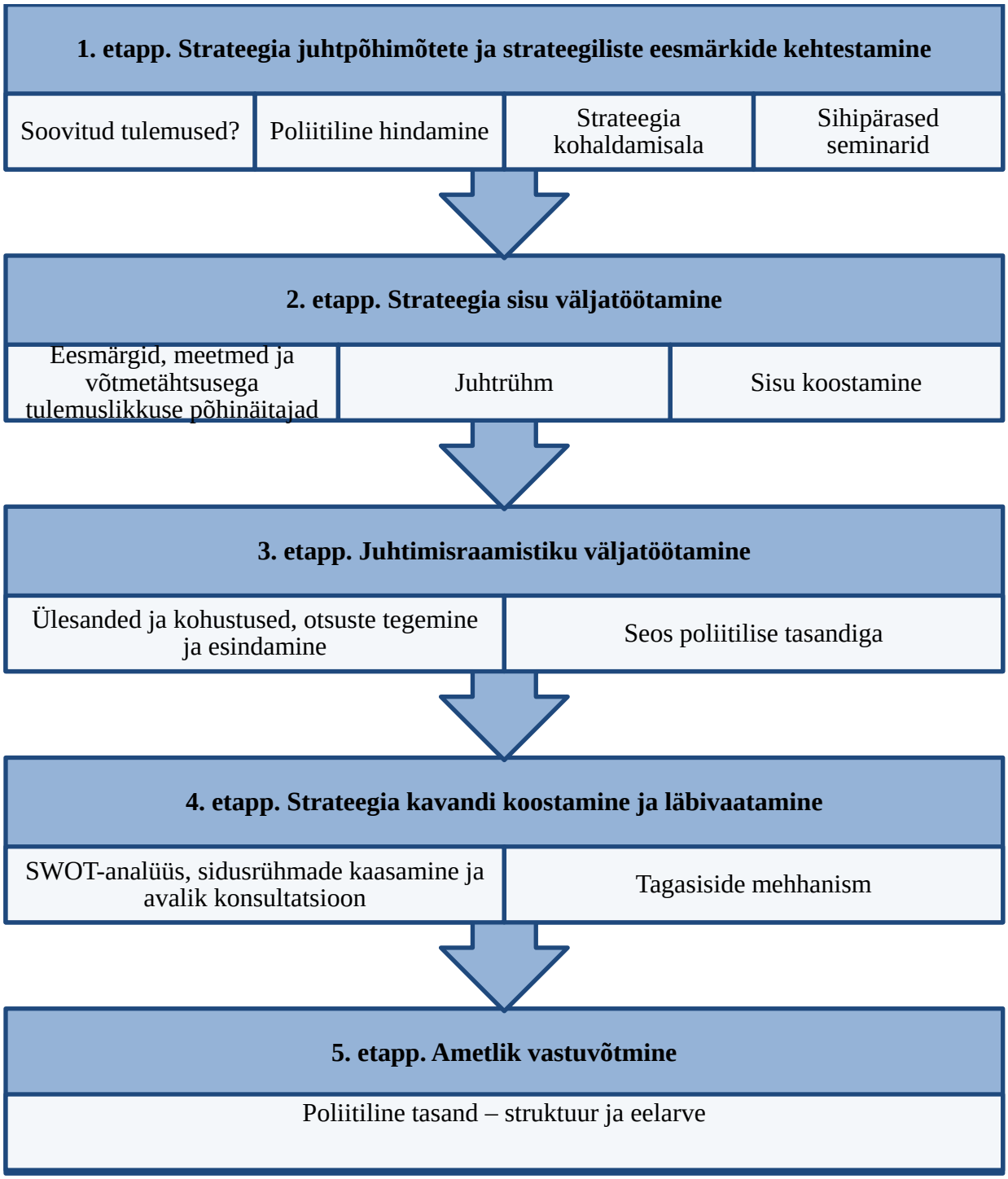
[10] Välja arvatud Kreeka, kus riiklik küberturvalisuse strateegia on alates 2014. aastast koostamisel (vt https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-greece/view).

[11] See teave põhineb ENISA esitatud riiklike küberturvalisuse strateegiate ülevaatel, mis on kättesaadav aadressil https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map.

suuniseid, eesmärke ja mõnel juhul konkreetseid meetmeid küberturvalisusega kaasnevate riskide maandamiseks.

Kuna mõned strateegiad võeti vastu enne võrgu- ja infoturbe direktiivi vastuvõtmist, ei pruugi need hõlmata kõiki artikli 7 elemente. Nõuetekohase ülevõtmise tagamiseks peavad liikmesriigid tegema lünkade analüüsi, võrreldes kõikide direktiivi II lisas loetletud sektorite ja III lisas loetletud teenuste puhul riikliku küberturvalisuse strateegia sisu artiklis 7 nimetatud seitsme selge nõudega. Liikmesriigid võivad kindlakstehtud lüngad kõrvaldada, muutes riiklikku küberturvalisuse strateegiat või vaadates täielikult läbi riikliku võrgu- ja infoturbe strateegia põhimõtted. Eespool esitatud riikliku küberturvalisuse strateegia vastuvõtmise suunised on asjakohased ka olemasoleva riikliku küberturvalisuse strateegia läbivaatamisel ja ajakohastamisel.

Joonis 1. Riikliku küberturvalisuse strateegia vastuvõtmise viieetapiline protsess



3. Võrgu- ja infoturbe direktiiv: riiklikud pädevad asutused, ühtsed kontaktpunktid ja küberturbe intsidentide lahendamise üksused (CSIRTid)

Artikli 8 lõike 1 kohaselt peavad liikmesriigid määrama ühe või mitu riiklikku pädevat asutust, kes hõlmavad vähemalt II lisas osutatud sektoreid ja III lisas osutatud teenuseid ning kelle ülesanne on jälgida direktiivi kohaldamist. Liikmesriigid võivad määrata selle ülesande ühele või mitmele olemasolevale asutusele.

Käesolevas punktis keskendutakse sellele, kuidas võrgu- ja infoturbe direktiiv edendab liikmesriikide valmisolekut, kohustades neid määrama tulemuslikud riiklikud pädevad asutused ja moodustama küberturbe intsidentide lahendamise üksused (CSIRTid). Täpsemalt hõlmab käesolev punkt riiklike pädevate asutuste määramise kohustust ja ühtse kontaktpunkti ülesandeid. Käsitletakse kolme teemat: a) võimalikud riiklikud juhtimisstruktuurid (nt tsentraliseeritud ja detsentraliseeritud mudelid jne) ja muud nõuded; b) ühtse kontaktpunkti roll ja c) küberturbe intsidentide lahendamise üksused.

3.1. Asutuste liik

Võrgu- ja infoturbe direktiivi artiklis 8 on sätestatud liikmesriikide kohustus määrata võrgu- ja infosüsteemide turbe vallas riiklikud pädevad asutused, tunnistades sõnaselgelt võimalust määrata „ühe või mitu riiklikku pädevat asutust“. Direktiivi põhjenduses 30 selgitatakse seda poliitikavalikut järgmiselt: „Arvestades riikide juhtimisstruktuuride erinevusi ning selleks, et kaitsta juba kehtivat valdkondlikku korda või liidu reguleerivaid ja järelevalveasutusi ning et vältida dubleerimist, peaksid liikmesriigid saama käesoleva direktiivi alusel nimetada oluliste teenuste operaatorite ja digitaalse teenuse osutajate võrgu- ja infosüsteemide turvalisusega seotud ülesannete täitmiseks rohkem kui ühe riikliku pädeva asutuse“.

Sellest tulenevalt on liikmesriikidel võimalik määrata üks keskne asutus, mis tegeleb kõigi direktiiviga hõlmatud sektorite ja teenustega, või mitu asutust, olenevalt näiteks sektori liigist.

Lähenemisviisi üle otsustamisel võivad liikmesriigid tugineda kogemustele, mis on saadud riiklikest lähenemisviisidest, mida kasutatakse elutähtsate infoinfrastruktuuride kaitset käsitlevate kehtivate õigusaktide kontekstis. Nagu selgub tabelist 1, otsustasid liikmesriigid kasutada elutähtsate infoinfrastruktuuride kaitse pädevuse määramisel riigi tasandil tsentraliseeritud või detsentraliseeritud lähenemisviisi. Riikide näiteid kasutatakse siin üksnes näitlikustamiseks ja eesmärgiga juhtida liikmesriikide tähelepanu olemasolevatele korralduslikele raamistikele. Komisjoni ei taha seega jätta muljet nagu tuleks asjaomastes riikides elutähtsate infoinfrastruktuuride kaitse puhul kasutatud mudelit kasutada ka võrgu- ja infoturbe direktiivi ülevõtmisel.

Liikmesriigid võivad otsustada ka erinevate segavariantide kasuks, mis hõlmavad nii tsentraliseeritud kui ka detsentraliseeritud lähenemisviiside elemente. Valiku võib teha kooskõlas direktiiviga hõlmatud erinevate sektorite ja teenuste varasema riikliku juhtimiskorraga; asjaomased asutused ning oluliste teenuste operaatorite ja digitaalse teenuse osutajatena identifitseeritud sidusrühmad võivad ka teha uue valiku. Liikmesriikide valikuid võivad mõjutada ka sellised olulised tegurid nagu küberturvalisuse alaste eriteadmiste olemasolu, rahastamiskaalutlused ning sidusrühmade ja riiklike huvide vahelised seosed (nt majanduse areng, avalik julgeolek jne).

3.2. Avalikustamine ja täiendavad asjaomased aspektid

Artikli 8 lõike 7 kohaselt peavad liikmesriigid teatama komisjonile riiklike pädevate asutuste määramisest ja nende ülesannetest. Seda tuleb teha ülevõtmise kuupäevaks.

Võrgu- ja infoturbe direktiivi artiklitega 15 ja 17 nähakse ette liikmesriikide kohustus tagada, et pädevatel asutustel oleksid nendes artiklites sätestatud ülesannete täitmiseks vajalikud õigused ja vahendid.

Lisaks sellele tuleb konkreetsete üksuste määramine riiklikuks pädevaks asutuseks avalikustada. Direktiivis ei täpsustata sellise avalikustamise viisi. Kuna selle nõude eesmärk on suurendada võrgu- ja infoturbega hõlmatud osalejate ja üldsuse teadlikkust, leiab komisjon teiste sektorite (telekommunikatsioon, pangandus, meditsiin) kogemustele tuginedes, et avalikustamine võiks toimuda näiteks laialdaselt reklaamitud portaali kaudu.

Võrgu- ja infoturbe direktiivi artikli 8 lõikes 5 on sätestatud, et sellistel asutustel peavad olema direktiivist tulenevate ülesannete täitmiseks „piisavad ressursid“.

Tabel 1. Riikide lähenemisviisid elutähtsate infoinfrastruktuuride kaitsele

ENISA avaldas 2016. aastal uuringu[12] liikmesriikide erinevate lähenemisviiside kohta elutähtsate infoinfrastruktuuride kaitsmisel. Selles kirjeldatakse kaht liikmesriikides elutähtsate infoinfrastruktuuride kaitse juhtimisel esinevat profiili, mida saab kasutada seoses võrgu- ja infoturbe direktiivi ülevõtmisega.

1. profiil. Detsentraliseeritud lähenemisviis – direktiivi II ja III lisas osutatud konkreetsete sektorite ja teenuste puhul on pädevad mitu valdkondlikku asutust

Detsentraliseeritud lähenemisviisi iseloomustavad:

(i) subsidiaarsuse põhimõte;
(ii) riigiasutustevaheline tihe koostöö;
(iii)valdkondlikud õigusaktid.

Subsidiaarsuse põhimõte

Üldise vastutusega ühtse asutuse loomise või määramise asemel järgib detsentraliseeritud lähenemisviis subsidiaarsuse põhimõtet. See tähendab, et rakendamise eest vastutab valdkondlik asutus, kes tunneb kohalikku sektorit kõige paremini ja kellel on väljakujunenud suhted sidusrühmadega. Selle põhimõtte kohaselt võetakse otsused vastu nende lähedal, keda need otsused mõjutavad.

Riigiasutustevaheline tihe koostöö

Kuna elutähtsate infoinfrastruktuuride kaitsega olid seotud erinevad riigiasutused, töötasid paljud liikmesriigid eri asutuste töö ja püüdluste kooskõlastamiseks välja koostöökavad. Need koostöökavad võivad olla mitteametlike võrgustike või institutsionaliseeritud foorumite või mehhanismide vormis. Koostöökavadel on siiski üksnes riigiasutuste vahel teabe vahetamise ja kooskõlastamise eesmärk ning neil puudub riigiasutuste üle mõjuvõim.

Valdkondlikud õigusaktid

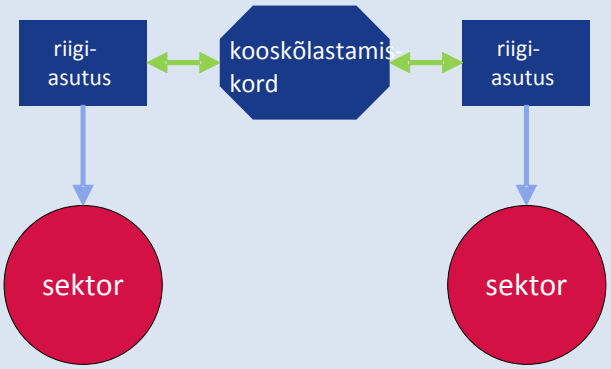
Riigid, kes järgivad elutähtsates sektorites detsentraliseeritud lähenemisviisi, hoiduvad sageli elutähtsate infoinfrastruktuuride kaitse alasest seadusandlikust tegevusest. Selle asemel on õigusnormide vastuvõtmine sektoripõhine ja võib seetõttu sektorite lõikes oluliselt erineda. Sellise lähenemisviisi eeliseks on võrgu- ja infoturbemeetmete ühtlustamine olemasolevate valdkondlike õigusaktidega, et sektor neid paremini vastu võtaks ja asjaomased asutused neid tulemuslikumalt täidaksid.

Direktiivi kohaldamisel paljude sektorite ja teenuste üleselt üksnes detsentraliseeritud lähenemisviisi kasutamisega kaasneb märkimisväärne järjepidevuse vähenemise oht. Sellisel juhul nähakse direktiiviga piiriülestes küsimustes sidepidamiseks ette ühtse kontaktpunkti

[12] ENISA, „Stocktaking, Analysis and Recommendations on the protection of CIIs“ (Elutähtsate infoinfrastruktuuride kaitse ülevaade, analüüs ja soovitused), 2016. Avaldatud aadressil https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis.

loomine ning asjaomane liikmesriik võib anda sellele ka ülesandeid seoses paljude riiklike pädevate asutuste vahelise kooskõlastamise ja koostööga kooskõlas direktiivi artikliga 10.

Joonis 2. Detsentraliseeritud lähenemisviis



Detsentraliseeritud lähenemisviisi näited

Rootsi on hea näide riigist, kus elutähtsate infoinfrastruktuuride kaitse puhul järgitakse detsentraliseeritud lähenemisviisi. Rootsi lähtub süsteemi vaatenurgast, mis tähendab seda, et erinevad asutused ja omavalitsused vastutavad elutähtsate infoinfrastruktuuride kaitse peamiste ülesannete eest, nagu elutähtsate teenuste ja infrastruktuuride kindlakstegemine, operaatorite töö koordineerimine ja toetamine, reguleerimisülesanded ning hädaolukorraks valmisoleku meetmed. Need asutused on muu hulgas Rootsi tsiviilhädaolukordade amet (MSB), Rootsi posti- ja telekommunikatsiooni amet (PTS) ning erinevad Rootsi kaitse-, militaar- ja õiguskaitseasutused.

Eri ametite ja avaliku sektori asutuste tegevuse koordineerimiseks on Rootsi valitsus välja töötanud koostöövõrgustiku, mis hõlmab konkreetsete ühiskondliku infoturbe kohustustega asutusi. See infoturbe koostöörühm (SAMFI) koosneb eri asutuste esindajatest ning kohtub mitu korda aastas, et arutada riigi infoturbega seotud küsimusi. SAMFI tegeleb eeskätt poliitilis-strateegiliste valdkondadega ning käsitleb tehnilisi küsimusi ja standardimist, riiklikke ja rahvusvahelisi arengusuundi infoturbe valdkonnas ning IT-intsidentide haldust ja ennetamist. (Rootsi tsiviilhädaolukordade amet (MSB), 2015).

Rootsi ei ole võtnud elutähtsate infoinfrastruktuuride kaitse kohta vastu keskvalitsuse seadusi, mida kohaldataks sektoriüleselt elutähtsate infoinfrastruktuuride operaatoritele. Selle asemel on asjaomaste avaliku sektori asutuste ülesanne vastu võtta õigusaktid, milles on sätestatud konkreetse sektori ettevõtjate kohustused. Näiteks on MSB-l õigus võtta infoturbe valdkonnas vastu valitsusasutustele kohaldatavaid õigusakte, samal ajal kui PTS võib nõuda operaatoritelt teatavate teisesel õigusel põhinevate tehniliste ja korralduslike turvameetmete rakendamist.

Selle profiili näitajatele vastab ka Iirimaa. Iirimaa järgib nn subsidiaarsuse doktriini, mille

kohaselt iga ministeerium vastutab oma sektoris elutähtsate infoinfrastruktuuride kindlakstegemise ja riskihindamise eest. Riiklikul tasandil ei ole elutähtsate infoinfrastruktuuride kaitse kohta vastu võetud ühtegi konkreetset õigusakti. Õigusaktid on valdkondlikud ning need on olemas peamiselt energeetika- ja telekommunikatsioonisektoris (2015). See profiil kehtib ka Austria, Küprose ja Soome kohta.

2. profiil. Tsentraliseeritud lähenemisviis – direktiivi II ja III lisas osutatud konkreetsete sektorite ja teenuste puhul on pädev üks keskne asutus

Tsentraliseeritud lähenemisviisi iseloomustavad:

i) sektoriülene keskne asutus;
ii) terviklikud õigusaktid.

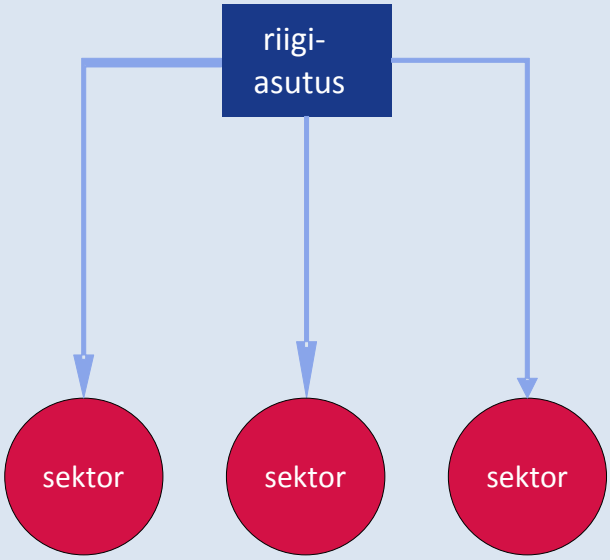
Sektoriülene keskne asutus

Tsentraliseeritud lähenemisviisi järgivad liikmesriigid on loonud asutused, kellel on kohustused ja laialdane pädevus mitmes sektoris või kõikides elutähtsates sektorites, või on laiendanud olemasolevate asutuste volitusi. Peamistel elutähtsate infoinfrastruktuuride kaitsega tegelevatel asutustel on mitu ülesannet, nagu erandolukorra plaanimine, hädaolukordade ohjamine, reguleerimisülesanded ja eraõiguslike operaatorite toetamine. Paljudel juhtudel on riiklik küberturbe intsidentide lahendamise üksus peamise elutähtsate infoinfrastruktuuride kaitsega tegeleva asutuse osa. Üleüldist küberturvalisuse alaste oskuste nappust arvesse võttes on tõenäoline, et kesksel asutusel on rohkem eriteadmisi küberturvalisuse valdkonnas kui valdkondlikel asutustel.

Terviklikud õigusaktid

Terviklike õigusaktidega kehtestatakse kohustused ja nõuded kõikidele elutähtsate infoinfrastruktuuride operaatoritele kõigis sektorites. Seda on võimalik saavutada uute terviklike õigusnormidega või olemasolevate valdkondlike õigusnormide täiendamisega. Selline lähenemisviis soodustaks võrgu- ja infoturbe direktiivi ühtset kohaldamist kõikide hõlmatud sektorite ja teenuste puhul. See hoiaks ära rakendamisel esinevate lünkade ohtu, mis võib tekkida, kui on mitu eripädevusega asutust.

Joonis 3. Tsentraliseeritud lähenemisviis



Tsentraliseeritud lähenemisviisi näited

ELi liikmesriikidest on tsentraliseeritud lähenemisviisi hea näide Prantsusmaa. Prantsusmaa Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) määrati 2011. aastal infosüsteemide kaitse peamiseks asutuseks. ANSSI täidab „elutähtsate operaatorite“ puhul tõhusat järelevalverolli: amet võib kohustada elutähtsaid operaatoreid järgima turvalisusmeetmeid ning ta on volitatud tegema turvalisusauditeid. Peale selle on see peamine ühtne kontaktpunkt elutähtsate operaatorite jaoks, kes on kohustatud teatama ametile turvaintsidentidest.

Turvaintsidentide puhul tegutseb ANSSI elutähtsate infoinfrastruktuuride kaitse hädaolukorra asutusena ning otsustab, milliseid meetmeid peavad operaatorid kriisiolukorras võtma. Valitsuse tegevust koordineeritakse ANSSI operatiivkeskuses. Ohtude avastamist ja intsidentidele reageerimist operatiivtasandil teostab CERT-FR, mis on ANSSI osa.

Prantsusmaa on kehtestanud elutähtsate infoinfrastruktuuride kaitse jaoks tervikliku õigusraamistiku. Peaminister andis 2006. aastal korralduse koostada elutähtsate infrastruktuuridega sektorite loetelu. Selle loetelu põhjal, mis sisaldas 12 elutähtsat sektorit, on valitsus kindlaks määranud ligikaudu 250 elutähtsat operaatorit. 2013. aastal võeti vastu militaarplaneerimise seadus[13]. Selles sätestatakse elutähtsate operaatorite erinevad kohustused, nagu intsidentidest teatamine ja turvameetmete rakendamine. Need nõuded on kohustuslikud kõikidele elutähtsatele operaatoritele kõigis sektorites (Prantsusmaa senat, 2013).

[13] La loi de programmation militaire.

3.3. Võrgu- ja infoturbe direktiivi artikkel 9: küberturbe intsidentide lahendamise üksused (CSIRTid)

Artikli 9 kohaselt on liikmesriigid kohustatud määrama ühe või mitu CSIRTi, kes vastutavad riskide ja intsidentide käsitlemise eest võrgu- ja infoturbe direktiivi II lisas loetletud sektorite ja III lisas loetletud teenuste puhul. Direktiivi artiklis 3 sätestatud minimaalse ühtlustamise nõuet arvestades võivad liikmesriigid kasutada CSIRTe ka direktiivi kohaldamisalasse mittekuuluvate sektorite puhul, nagu avalik haldus.

Liikmesriigid võivad luua CSIRTi pädeva asutuse osana[14].

3.4. Ülesanded ja nõuded

Määratud CSIRTide ülesanded, mis on sätestatud võrgu- ja infoturbe direktiivi I lisas, on järgmised:

- intsidentide seire riigis;
- riskide ja intsidentide kohta varajaste hoiatuste, hoiatusteadete ja teadaannete esitamine ning teabe levitamine asjakohastele sidusrühmadele;
- intsidentidele reageerimine;
- pidev riskide ja intsidentide analüüsimine ja teadlikkus olukorrast ning
- osalemine artikli 12 raames loodud riiklike CSIRTide võrgustikus.

Artikli 14 lõigetes 3, 5 ja 6 ning artikli 16 lõigetes 3, 6 ja 7 on sätestatud intsidentidest teatamisega seotud konkreetsed lisaülesanded juhuks, kui liikmesriik otsustab, et need ülesanded võib lisaks riiklikele pädevatele asutustele või nende asemel panna CSIRTidele.

Direktiivi ülevõtmisel on liikmesriikidel teatavad valikuvõimalused selles, milline on CSIRTide roll intsidentidest teatamise nõuete täitmisel. Nad võivad kehtestada kohustuse teatada küberturbe intsidentidest otse CSIRTidele, mille eeliseks on haldustõhusus, või otsustada, et intsidentidest tuleb teatada otse riiklikele pädevatele asutustele, kusjuures CSIRTidel on esitatud andmetele juurdepääsu õigus. CSIRTid on kokkuvõttes huvitatud probleemide lahendamisest, hoides ära ja avastades küberintsidente (sealhulgas neid, mis ei ole kohustuslikuks teatamiseks piisavalt olulised), reageerides neile ja vähendades nende mõju koostöös sidusrühmadega, ning riiklikud pädevad asutused vastutavad õigusnormidele vastavuse eest.

Direktiivi artikli 9 lõike 3 kohaselt peavad liikmesriigid ka tagama, et CSIRTidel oleks juurdepääs turvalisele ja töökindlale IKT-taristule.

[14] Vt artikli 9 lõike 1 viimane lause.

Direktiivi artikli 9 lõikes 4 kohustatakse liikmesriike teatama komisjonile, millised on CSIRTide volitused ja intsidentide käsitlemise protseduuri peamised elemendid.

Liikmesriikide määratud CSIRTidele kohaldatavad nõuded on esitatud võrgu- ja infoturbe direktiivi I lisas. CSIRT peab tagama oma sideteenuste laialdase kättesaadavuse. Üksuse ametiruumide ja tema tööd toetavate infosüsteemide asukoht peab olema turvaline ning tagama talitluspidevuse. Peale selle peab CSIRTil olema võimalik osaleda rahvusvahelistes koostöövõrgustikes.

3.5. Abi CSIRTide arendamisel

Euroopa ühendamise rahastu küberturvalisuse digitaalteenuste taristu programmi raames võib liikmesriikide CSIRTidele eraldada märkimisväärsed ELi vahendid nende suutlikkuse suurendamiseks ja teiste üksustega koostöö tõhustamiseks teabevahetuse koostöömehhanismi kaudu. SMART 2015/1089 projekti raames välja töötatava koostöömehhanismi eesmärk on lihtsustada liikmesriikide CSIRTide vabatahtlikku, kiiret ja tulemuslikku operatiivkoostööd, nimelt toetades CSIRTide võrgustikule direktiivi artikliga 12 pandud ülesannete täitmist.

Liikmesriikide CSIRTide suutlikkuse arendamisele suunatud asjakohaste konkursikutsete üksikasjad on avaldatud Euroopa Komisjoni Innovatsiooni ja Võrkude Rakendusameti (INEA) veebisaidil[15].

Euroopa ühendamise rahastu küberturvalisuse digitaalteenuste taristu haldusnõukogu näeb ette mitteametliku struktuuri liikmesriikide CSIRTidele poliitikatasandi suuniste koostamiseks ja abi andmiseks, eesmärgiga suurendada nende suutlikkust, ning vabatahtliku koostöömehhanismi rakendamiseks.

Äsja loodud või võrgu- ja infoturbe direktiivi I lisa ülesannete täitmiseks määratud CSIRT võib tulemuslikkuse parandamisel ja töö tõhustamisel tugineda ENISA nõuannetele ja eriteadmistele[16]. Seoses sellega tasub märkida, et liikmesriikide CSIRTid võivad juhinduda mõningatest ENISA uusimatest materjalidest. Käesoleva lisa punktis 7 on loetletud mitu ameti välja antud dokumenti ja uuringut, milles kirjeldatakse head tava ning antakse CSIRTi pädevuse ja teenustega seoses tehnilise tasandi soovitusi, mis hõlmavad CSIRTi küpsustaseme hindamist. Lisaks sellele jagavad CSIRTide võrgustikud suuniseid ja parimaid tavasid nii ülemaailmsel (FIRST[17]) kui ka Euroopa tasandil (Trusted Introducer, TI[18]).

3.6. Ühtse kontaktpunkti roll

Võrgu- ja infoturbe direktiivi artikli 8 lõike 3 kohaselt peab iga liikmesriik määrama riikliku ühtse kontaktpunkti, mis täidab sidepidamisfunktsiooni, et tagada piiriülene koostöö teiste liikmesriikide asjaomaste asutustega, aga ka selle direktiivi alusel loodud koostöörühma ja CSIRTide võrgustikuga[19]. Põhjenduses 31 ja artikli 8 lõikes 4 põhjendatakse seda nõuet

[15] Avaldatud aadressil https://ec.europa.eu/inea/en/connecting-europe-facility.
[16] Vt võrgu- ja infoturbe direktiivi artikli 9 lõige 5.
[17] Forum of Incident Response and Security Teams (intsidentidele reageerimise ja turvalisuse üksuste foorum) (https://www.first.org/).
[18] https://www.trusted-introducer.org/.
[19] Riikide CSIRTide võrgustik liikmesriikidevaheliseks operatiivkoostööks artikli 12 alusel.

vajadusega hõlbustada piiriülest koostööd ja suhtlust. Seda on eriti vaja, kuna liikmesriikidel võib olla rohkem kui üks riiklik asutus. Seega lihtsustab ühtne kontaktpunkt erinevate liikmesriikide asutuste identifitseerimist ja koostööd.

Ühtse kontaktpunkti sidepidamisülesanne hõlmab tõenäoliselt suhtlust koostöörühma sekretariaadi ja CSIRTide võrgustiku sekretariaadiga, kui riigi ühtne kontaktpunkt ei ole CSIRT ega koostöörühma liige. Lisaks sellele peavad liikmesriigid tagama, et ühtset kontaktpunkti teavitatakse oluliste teenuste operaatoritelt ja digitaalse teenuse osutajatelt saadud teadetest[20].

Direktiivi artikli 8 lõikes 3 on sätestatud, et kui liikmesriik võtab kasutusele tsentraliseeritud lähenemisviisi, st nimetab ainult ühe pädeva asutuse, siis on see pädev asutus ka ühtne kontaktpunkt. Kui liikmesriik otsustab detsentraliseeritud lähenemisviisi kasuks, võib ta määrata ühe pädevatest asutustest ühtseks kontaktpunktiks. Kui pädev asutus, CSIRT ja ühtne kontaktpunkt on erinevad üksused, on liikmesriigid valitud institutsioonilisest mudelist sõltumata kohustatud tagama nende tulemusliku koostöö, et täita direktiivis sätestatud kohustused[21].

Ühtne kontaktpunkt peab esitama koostöörühmale 9. augustiks 2018 ja seejärel igal aastal saadud teadete kohta koondaruande, milles esitatakse teadete arv, intsidentide laad ja asutuste võetud meetmed, nagu teiste mõjutatud liikmesriikide teavitamine intsidendist või asjakohase teabe edastamine teate esitanud ettevõtjale intsidendi käsitlemiseks[22]. Pädeva asutuse või CSIRTi taotlusel peab ühtne kontaktpunkt edastama oluliste teenuste operaatorite teated teiste intsidendist mõjutatud liikmesriikide ühtsetele kontaktpunktidele[23].

Liimesriigid peavad teatama komisjonile ühtse kontaktpunkti määramisest ja ülesannetest direktiivi ülevõtmise tähtajaks. Teave ühtse kontaktpunkti määramise kohta tuleb avalikustada samamoodi nagu riiklike pädevate asutuste andmed. Komisjon avaldab määratud ühtsete kontaktpunktide loetelu.

3.7. Karistused

Artiklis 21 jäetakse liikmesriikidele otsustusõigus kohaldatavate karistuste liigi ja laadi üle, tingimusel et need karistused oleksid tõhusad, proportsionaalsed ja hoiatavad. Teisisõnu on liikmesriikidel põhimõtteliselt vabadus otsustada oma siseriiklikes õigusaktides sätestatud karistuste maksimaalse määra üle, kuid valitud määr või protsent peab võimaldama riigi ametiasutustel rakendada igal konkreetsel juhul tõhusaid, proportsionaalseid ja hoiatavaid karistusi, võttes arvesse erinevaid tegureid, nagu rikkumiste tõsidus ja sagedus.

4. Üksused, kellel on turvanõuete ja intsidentidest teatamisega seotud kohustused

Ühiskonna ja majanduse jaoks olulist rolli omavad üksused, kellele osutatakse direktiivi artikli 4 lõigetes 4 ja 5 kui oluliste teenuste operaatoritele ja digitaalse teenuse osutajatele, on

[20] Vt artikli 10 lõige 3.
[21] Vt artikli 10 lõige 1.
[22] Sama.
[23] Vt artikli 14 lõige 5.

kohustatud võtma asjakohaseid turvameetmeid ja teatama tõsistest intsidentidest asjaomasele riigi ametiasutusele. Põhjus on selles, et selliste teenustega seotud turvaintsidentide mõju võib kujutada nendele teenustele suurt ohtu, mis võib põhjustada tõsiseid häireid majandustegevuses ja ühiskonnas laiemalt, vähendades kasutajate usaldust ja tekitades suurt kahju liidu majandusele[24].

Käesolevas punktis antakse ülevaade võrgu- ja infoturbe direktiivi II ja III lisaga hõlmatud üksustest ning loetletakse nende kohustused. Põhjalikumalt käsitletakse oluliste teenuste operaatorite identifitseerimist, arvestades selle protsessi tähtsust võrgu- ja infoturbe direktiivi ühtlustatud rakendamiseks kõikjal ELis. Samuti selgitatakse põhjalikult digitaalse taristu ja digitaalse teenuse osutajate määratlusi. Käsitletakse ka täiendavate sektorite kaasamise võimalust ja selgitatakse erilist lähenemisviisi seoses digitaalse teenuse osutajatega.

4.1. Oluliste teenuste operaatorid

Võrgu- ja infoturbe direktiivis ei ole täpselt määratletud, milliseid üksusi peetakse direktiivi kohaldamisalasse kuuluvateks oluliste teenuste operaatoriteks. Selle asemel esitatakse kriteeriumid, mida liikmesriigid peavad järgima identifitseerimisprotsessi läbiviimisel, mille tulemusena määratakse kokkuvõttes kindlaks, milliseid II lisas loetletud üksuste liigi alla kuuluvaid ettevõtjaid peetakse oluliste teenuste operaatoriteks, kes peavad seega täitma direktiivis sätestatud kohustusi.

4.1.1. Võrgu- ja infoturbe direktiivi II lisas loetletud üksuste liigid

Artikli 4 punktis 4 on oluliste teenuste operaator määratletud kui direktiivi II lisas osutatud liiki avaliku või erasektori üksus, mis vastab artikli 5 lõikes 2 sätestatud nõuetele. II lisas on loetletud sektorid, allsektorid ja üksuste liigid, mille puhul liikmesriigid peavad läbi viima identifitseerimisprotsessi vastavalt artikli 5 lõikele 2[25]. Need sektorid on energeetika, transport, pangandus, finantsturu taristud, tervishoid, joogivee varustus ja jaotamine ning digitaalne taristu.

Enamiku nn traditsioonilistesse sektoritesse kuuluvate üksuste kohta sisaldavad ELi õigusaktid väljakujunenud määratlusi, millele osutatakse II lisas. See ei kehti digitaalse taristu sektori kohta, mis on loetletud II lisa punktis 7 ning hõlmab interneti vahetuspunkte, domeeninimede süsteeme ja tippdomeeninimede registreid. Nende määratluste täpsustamiseks selgitatakse neid järgnevalt üksikasjalikult.

1) Interneti vahetuspunkt

Interneti vahetuspunkti mõiste on määratletud artikli 4 punktis 13 ja seda on täpsustatud põhjenduses 18; see on võrgustik, mis võimaldab rohkem kui kahe sõltumatu tehniliselt eraldiseisva süsteemi omavahelist ühendamist, eelkõige selleks, et hõlbustada internetiliikluse

[24] Vt põhjendus 2.
[25] Identifitseerimisprotsessi kohta vaata täpsemalt punkt 4.1.6.

vahetamist. Interneti vahetuspunkti võib kirjeldada ka kui füüsilist kohta, kus paljud võrgustikud vahetavad üksteisega kommutaatori kaudu internetiliiklust. Interneti vahetuspunkti peamine otstarve on võimaldada võrkude omavahelist otse ühendamist vahetuspunkti kaudu, ilma et liiklus peaks kulgema ühe või enama kolmanda osapoole võrgu kaudu. Interneti vahetuspunkti teenuse pakkuja tavaliselt internetiliiklust ei suuna. Internetiliiklust suunavad võrguteenuse pakkujad. Võrkude otse ühendamisel on palju eeliseid, millest peamised on maksumus, latentsusaeg ja ribalaius. Tavaliselt osapooled vahetuspunkti läbiva internetiliikluse eest tasu ei võta, samas kui liikluse eest ülesvoolu paikneva internetiteenuste osutajani võetakse. Võrkude otse ühendamisel, mis sageli toimub mõlema võrguga samas linnas, ei pea andmed ühest võrgust teise saamiseks liikuma kauge maa taha ja seetõttu väheneb latentsusaeg.

Tuleks märkida, et interneti vahetuspunkti määratlus ei hõlma füüsilisi punkte, kus ühendatakse omavahel ainult kaks füüsilist võrku (st sellised võrguteenuse osutajad nagu BASE ja PROXIMUS). Seega peavad liikmesriigid eristama direktiivi ülevõtmisel operaatoreid, kes lihtsustavad mitme võrguoperaatori vahelist internetiliiklust, nendest, kes on ühe võrgu operaatorid ja ühendavad füüsiliselt oma võrgud ühenduslepingute alusel. Viimasel juhul ei ole võrguteenuse osutajad artikli 4 punkti 13 määratlusega hõlmatud. Seda küsimust selgitatakse põhjenduses 18, kus on öeldud, et interneti vahetuspunkt ei paku juurdepääsu võrgule ega toimi transiiditeenuse osutaja ega edastajana. Teenuse osutajate viimasesse kategooriasse kuuluvad üldkasutatavaid sidevõrke ja/või -teenuseid pakkuvad ettevõtjad, kelle suhtes kohaldatakse direktiivi 2002/21/EÜ artiklites 13a ja 13b sätestatud turvalisuse tagamise ja teatamise kohustust ning kes seetõttu ei kuulu võrgu- ja infoturbe direktiivi kohaldamisalasse[26].

2) Domeeninimede süsteem

Domeeninimede süsteem on määratletud artikli 4 punktis 14 kui „hierarhilise jaotamise põhimõttel toimuv nimede andmise süsteem võrgus, mis edastab domeeninimede päringuid“. Täpsemalt saab domeeninimede süsteemi kirjeldada kui arvutitele, teenustele ja mis tahes muule internetti ühendatud ressursile hierarhilise jaotamise põhimõttel toimuvat nimede andmise süsteemi, mis võimaldab kodeerida domeeninimesid internetiprotokolli (IP) aadressideks. Süsteemi peamine ülesanne on transleerida määratud domeeninimed internetiprotokolli aadressideks. Selleks et selline domeeninimede transleerimine IP-aadressideks oleks võimalik, kasutab domeeninimede süsteem andmebaasi ning nimeservereid ja resolverit. Kuigi domeeninimede kodeerimine ei ole domeeninimede süsteemi ainus ülesanne, on see selle keskne ülesanne. Artikli 4 punktis 14 esitatud legaaldefinitsioon keskendub süsteemi peamisele ülesandele kasutaja seisukohast, laskumata tehnilistesse üksikasjadesse, nagu domeeninimeruum, nimeserverid, resolverid jne. Artikli 4 punktis 15 on määratletud, kes on domeeninimede süsteemi teenuse osutaja.

3) Tippdomeeninimede register

[26] Võrgu- ja infoturbe direktiivi ja direktiivi 2002/21/EÜ vahelise seose üksikasjade kohta vt punkt 5.2.

Tippdomeeninimede register on artikli 4 punktis 16 määratletud kui üksus, mis haldab ja teostab interneti domeeninimede registreerimist konkreetse tippdomeeni all. Domeeninimede haldamine ja juhtimine hõlmab tippdomeeninimede kodeerimist IP-aadressideks.

IANA (interneti numbrite määramise asutus) vastutab domeeninimede süsteemi juurtsooni haldamise, internetiprotokolli määramise ja muude internetiprotokolli ressursside ülemaailmse koordineerimise eest. Eelkõige vastutab IANA geneeriliste tippdomeenide (nt .com) ja riigidomeenide (nt .be) määramise eest operaatoritele (registritele) ning nende tehniliste ja haldusalaste üksikasjade eest. IANA peab määratud tippdomeenide ülemaailmset registrit ning osaleb selle loetelu teatavaks tegemises interneti kasutajatele üle maailma ja uute tippdomeenide loomises.

Registrite oluline ülesanne on määrata teise taseme domeeninimesid nende asjaomaste tippdomeenide raames registreerijatele. Need registreerijad saavad soovi korral ka ise määrata kolmanda taseme domeeninimesid. Riigidomeenid esindavad riiki või territooriumit vastavalt standardile ISO 3166-1. Geneerilistel tippdomeenidel ei ole tavaliselt geograafilist või riigi tähist.

Tuleks märkida, et tippdomeeninimede registri pidamine võib hõlmata domeeninimede süsteemi teenuste osutamist. Näiteks vastavalt IANA delegeerimiseeskirjadele peab riigidomeenidega tegelev määratud üksus muu hulgas tegema domeeninimede järelevalvet ja haldama selle riigi domeeninimede süsteemi[27]. Liikmesriigid peavad nende asjaoludega arvestama oluliste teenuste operaatorite identifitseerimisprotsessi läbiviimisel vastavalt artikli 5 lõikele 2.

4.1.2. Oluliste teenuste operaatorite identifitseerimine

Vastavalt direktiivi artikli 5 nõuetele peavad liikmesriigid identifitseerima kõik II lisas osutatud liiki üksused, kelle tegevuskoht on asjaomase liikmesriigi territooriumil. Hindamise tulemusel loetakse oluliste teenuste operaatoriteks kõik üksused, mis vastavad artikli 5 lõikes 2 sätestatud kriteeriumitele, ning nende suhtes kohaldatakse artikli 14 kohaseid turvalisuse tagamise ja teatamise kohustusi.

Liikmesriikidel on kõikide sektorite ja allsektorite operaatorite identifitseerimiseks aega 9. novembrini 2018. Liikmesriikide toetamiseks selle protsessi vältel töötab koostöörühm praegu välja juhenddokumenti, mis sisaldab asjakohast teavet oluliste teenuste operaatorite identifitseerimiseks vajalike sammude ja sellega seotud parimate tavade kohta.

Vastavalt artikli 24 lõikele 2 arutab koostöörühm nende riiklike meetmete protsessi, sisu ja liiki, mis võimaldavad identifitseerida oluliste teenuste operaatorid konkreetsetes sektorites. Liikmesriigid võivad enne 9. novembrit 2018 arutada koostöörühmas oma kavandatud riiklikke meetmeid, mis võimaldavad oluliste teenuste operaatorite identifitseerimist.

[27] Teave on avaldatud aadressil https://www.icann.org/resources/pages/delegation-2012-02-25-en.

4.1.3. Täiendavate sektorite kaasamine

Artiklis 3 sätestatud minimaalse ühtlustamise nõuet arvesse võttes võivad liikmesriigid vastu võtta või säilitada sätteid eesmärgiga saavutada võrgu- ja infosüsteemide turvalisuse kõrgem tase. Seoses sellega on liikmesriikidel üldiselt vabadus laiendada artikli 14 kohaseid turvalisuse tagamise ja teatamise kohustusi üksustele, mis kuuluvad teistesse sektoritesse ja allsektoritesse kui need, mis on loetletud võrgu- ja infoturbe direktiivi II lisas. Mitu liikmesriiki on otsustanud kaasata järgmised täiendavad sektorid või kaaluvad nende kaasamist.

i) Haldusasutused

Haldusasutused võivad pakkuda direktiivi II lisas nimetatud olulisi teenuseid, mis vastavad artikli 5 lõike 2 nõuetele. Sel juhul on neid teenuseid osutavad haldusasutused hõlmatud asjaomaste turvanõuete ja teatamiskohustusega. Kui aga haldusasutused pakuvad teenuseid, mis ei kuulu eespool nimetatud sätte kohaldamisalasse, ei ole need teenused asjaomaste kohustustega hõlmatud.

Haldusasutused vastutavad valitsusasutuste, piirkondlike ja kohalike omavalitsuste, ametite ja seotud ettevõtete pakutavate avalike teenuste nõuetekohase osutamise eest. Need teenused eeldavad sageli üksikisikuid ja organisatsioone käsitlevate isiku- ja organisatsiooni andmete loomist ja haldamist. Neid andmeid võib jagada ja teha kättesaadavaks paljudele avaliku sektori üksustele. Üldiselt on haldusasutuste kasutatavate võrgu- ja infosüsteemide turvalisuse kõrge tase kogu ühiskonna ja majanduse huvides. Seepärast on komisjon seisukohal, et liikmesriikidel oleks mõistlik kaaluda haldusasutuste kaasamist direktiivi ülevõtvate õigusaktide kohaldamisalasse, lisaks II lisas ja artikli 5 lõikes 2 sätestatud oluliste teenuste osutamisele.

ii) Postiteenuste sektor

Postiteenuste sektor hõlmab postiteenuste osutamist, nagu postisaadetiste kogumine, sortimine, transport ja jaotamine.

iii) Toidusektor

Toidusektor tegeleb põllumajanduslike toodete ja muude toiduainete tootmisega ning võib hõlmata olulisi teenuseid, nagu toiduga kindlustatuse ning toiduainete kvaliteedi ja toiduohutuse tagamist.

iv) Keemia- ja tuumatööstus

Keemia- ja tuumatööstus hõlmab eelkõige keemia- ja naftakeemiatööstuse toodete või tuumamaterjalide ladustamist, tootmist ja töötlemist.

v) Keskkonnasektor

Keskkonnasektori tegevus hõlmab keskkonna kaitseks ja ressursside haldamiseks vajalike kaupade ja teenuste pakkumist. Seepärast on tegevuse eesmärk hoida ära, vähendada ja likvideerida reostust ning säilitada olemasolevaid loodusressursse. Selle sektori raames võivad olulised teenused olla reostuse (nt õhu- ja veereostuse) ning meteoroloogiliste nähtuste seire ja kontroll.

vi) Kodanikukaitse

Kodanikukaitse sektori eesmärk on ennetada loodusõnnetusi ja inimtegevusest tingitud katastroofe, valmistuda nendeks ja neile reageerida. Selleks osutatavad teenused võivad olla hädaabinumbrite aktiveerimine ja meetmete rakendamine hädaolukordadest teavitamiseks, nende ohjamiseks ja neile reageerimiseks.

4.1.4. Jurisdiktsioon

Artikli 5 lõike 1 kohaselt peavad liikmesriigid identifitseerima oluliste teenuste operaatorid, kelle tegevuskoht on nende territooriumil. Selles sättes ei täpsustata tegevuskoha liiki, kuid põhjenduses 21 selgitatakse, et tegevuskoht eeldab liikmesriigis tegelikku ja tulemuslikku tegutsemist ning stabiilset tegevuskorraldust, kusjuures tegevuse õiguslik vorm ei ole määrav. See tähendab, et oluliste teenuste operaator kuulub liikmesriigi jurisdiktsiooni alla mitte ainult siis, kui tema peakontor asub selle liikmesriigi territooriumil, vaid ka siis, kui tal on seal näiteks filiaal või toimub tegevus muus õiguslikus vormis.

See omakorda tähendab, et sama üksus võib üheaegselt kuuluda mitme liikmesriigi jurisdiktsiooni alla.

4.1.5. Komisjonile esitatav teave

Võrgu- ja infoturbe direktiivi artikli 23 lõike 1 kohaseks komisjonipoolseks läbivaatamiseks peavad liikmesriigid esitama komisjonile 9. novembriks 2018 ning pärast seda iga kahe aasta tagant järgmise teabe:

- riiklikud meetmed, mis võimaldavad oluliste teenuste operaatorite identifitseerimist;
- oluliste teenuste loetelu;
- iga II lisas osutatud sektori puhul identifitseeritud oluliste teenuste operaatorite arv ning operaatori tähtsus asjaomases sektoris ja
- piirmäärad (kui need on olemas), mida on kasutatud teenuse osutamise taseme kindlakstegemiseks artikli 6 lõike 1 punktis a osutatud teenusest sõltuvate kasutajate arvu alusel või artikli 6 lõike 1 punktis f osutatud üksuse tähtsuse alusel.

Artikli 23 lõikes 1 sätestatud läbivaatamine, mis eelneb direktiivi ulatuslikule läbivaatamisele, näitab, kui oluliseks kaasseadusandjad peavad direktiivi nõuetekohast ülevõtmist seoses oluliste teenuste operaatorite identifitseerimisega, et hoida ära turu killustatust.

Selle protsessi võimalikult heaks teostamiseks julgustab komisjon liikmesriike seda teemat koostöörühmas arutama ning vahetama asjaomaseid kogemusi. Komisjon julgustab liikmesriike esitama komisjonile – vajaduse korral konfidentsiaalselt – identifitseeritud oluliste teenuste (mis lõpuks välja valiti) operaatorite loetelu lisaks teabele, mille liikmesriigid on direktiivi kohaselt kohustatud komisjonile esitama. Kui sellised loetelud on komisjonile kättesaadavad, siis on tal lihtsam hinnata identifitseerimisprotsessi järjepidevust ja tagada selle parem kvaliteet. Samuti võimaldab see tal võrrelda liikmesriikide lähenemisviise, soodustades seega direktiivi eesmärkide saavutamist.

4.1.6. Kuidas identifitseerimisprotsessi läbi viia?

Nagu on näha jooniselt 4, peaks riigi ametiasutus konkreetse üksuse identifitseerimisprotsessi läbiviimisel pöörama tähelepanu kuuele põhiküsimusele. Järgmises osas vastab iga küsimus etapile, mis tuleb läbida vastavalt artiklile 5 koostoimes artikliga 6, võttes arvesse ka artikli 1 lõike 7 kohaldatavust.

1. etapp. **Kas üksus kuulub direktiivi II lisas nimetatud sektorisse/allsektorisse ja vastab selles osutatud liigile?**

Riigi ametiasutus peab hindama, kas tema territooriumil asutatud üksus kuulub direktiivi II lisas loetletud sektorisse ja allsektorisse. II lisa hõlmab erinevaid majandussektoreid, mida peetakse siseturu nõuetekohase toimimise seisukohalt tähtsaks. II lisas osutatakse eelkõige järgmistele sektoritele ja allsektoritele:

- energeetika: elekter, nafta ja gaas;
- transport: lennu-, raudtee-, vee- ja maanteetransport;
- pangandus: krediidiasutused;
- finantsturu taristu: kauplemiskohad, kesksed vastaspooled;
- tervishoiusektor: tervishoiuasutused (k.a haiglad ja erakliinikud);
- vesi: joogivee varustus ja jaotamine;
- digitaalne taristu: interneti vahetuspunktid, domeeninimede süsteemi teenuse osutajad ja tippdomeeninimede registrid[28].

2. etapp. **Kas erinormid on kohaldatavad?**

Järgmisena peavad riigi ametiasutused hindama, kas artikli 1 lõikes 7 sätestatud erinormid on kohaldatavad. Selles sättes on eelkõige märgitud, et kui liidu õigusaktiga kehtestatakse digitaalse teenuse osutajatele või oluliste teenuste operaatoritele turva- ja/või teatamisnõuded, mis on toimelt vähemalt samaväärsed võrgu- ja infoturbe direktiivi asjaomaste nõuetega, kohaldatakse erinormides sätestatud kohustusi. Peale selle täpsustatakse põhjenduses 9, et kui artikli 1 lõikes 7 sätestatud nõuded on täidetud, peavad liikmesriigid kohaldama valdkondlike ELi õigusaktide sätteid, sealhulgas jurisdiktsiooniga seotud sätted. Sellisel juhul võrgu- ja infoturbe direktiivi asjaomaseid sätteid ei kohaldata. Sellisel juhul ei peaks pädev asutus artikli 5 lõike 2 kohast identifitseerimisprotsessi jätkama[29].

3. etapp. **Kas operaator pakub olulist teenust direktiivi tähenduses?**

Artikli 5 lõike 2 punkti a kohaselt peab identifitseeritav üksus osutama teenust, mis on oluline elutähtsa ühiskondliku ja/või majandustegevuse säilitamise seisukohast. Selle hindamisel peab liikmesriik arvesse võtma, et üks üksus võib osutada nii olulisi kui ka mitteolulisi teenuseid. See tähendab seda, et võrgu- ja infoturbe direktiivi turva- ja teatamisnõudeid kohaldatakse konkreetse operaatori suhtes üksnes oluliste teenuste osutamise ulatuses.

---

[28] Neid üksusi käsitletakse üksikasjalikumalt punktis 4.1.1.

[29] Erinormide kohaldatavust käsitletakse täpsemalt punktis 5.1.

Vastavalt artikli 5 lõikele 3 peab liikmesriik koostama kõikide oluliste teenuste operaatorite poolt tema territooriumil osutatavate oluliste teenuste loetelu. Loetelu tuleb esitada komisjonile 9. novembriks 2018 ja seejärel iga kahe aasta tagant[30].

4. etapp. **Kas teenuse osutamine sõltub võrgu- ja infosüsteemist?**

Samuti tuleb täpsustada, kas teenus vastab artikli 5 lõike 2 punktis b sätestatud teisele kriteeriumile ja eelkõige seda, kas olulise teenuse osutamine sõltub artikli 4 punktis 1 määratletud võrgu- ja infosüsteemidest.

5. etapp. **Kas turvaintsidendil on oluline häiriv mõju?**

Artikli 5 lõike 2 punktis c on sätestatud, et riigi ametiasutus peab hindama, kas turvaintsidendil on teenuse osutamisele oluline häiriv mõju. Artikli 6 lõikes 1 on sellega seoses sätestatud mitu sektoritevahelist tegurit, mida tuleb hindamisel arvesse võtta. Peale selle on artikli 6 lõikes 2 märgitud, et liikmesriigid võtavad asjakohasel juhul arvesse ka sektoripõhiseid tegureid.

Artikli 6 lõikes 1 loetletud **sektoritevahelised tegurid** on järgmised:

- asjaomase üksuse poolt osutatavatest teenustest sõltuvate kasutajate arv;
- muude II lisas osutatud sektorite sõltumine üksuse poolt pakutavast teenusest;
- intsidentide võimalik mõju (raskusaste ja kestus) majandus- ja ühiskondlikule tegevusele või avalikule julgeolekule;
- üksuse turuosa;
- intsidendist mõjutatud geograafilise ala võimalik ulatus;
- üksuse tähtsus teenuse piisava kvaliteedi säilitamisel, võttes arvesse alternatiivide olemasolu kõnealuse teenuse osutamiseks.

Põhjenduses 28 tuuakse **sektoripõhiste tegurite** kohta mõned näited (vt tabel 4), millest võib riigi ametiasutustel kasu olla.

Tabel 4. Näited sektoripõhiste tegurite kohta, mida tuleb intsidentide olulise häiriva mõju kindlakstegemisel arvesse võtta

Sektor	Sektoripõhiste tegurite näited
Energiatarnijad	liikmesriigi energiatootmise maht või osakaal
Naftatarnijad	päevane tarnemaht
Lennutransport (sh lennujaamad ja lennuettevõtjad) **Raudteetransport** **Meresadamad**	osakaal riigi liiklusmahus reisijate või kaubavedude arv aastas

[30] Vt artikli 5 lõike 7 punkt b.

Pangandus ja finantsturu taristud	süsteemne tähtsus koguvarade alusel koguvarade ja SKP suhtarv
Tervishoiusektor	teenuseosutaja hoole all olevate patsientide arv aastas
Vee tootmine, töötlemine ja veevarustus	maht ning kasutajate arv ja liik (sh näiteks haiglad, avalikke teenuseid osutavad organisatsioonid või üksikisikud) alternatiivsete veeallikate olemasolu samas geograafilises piirkonnas

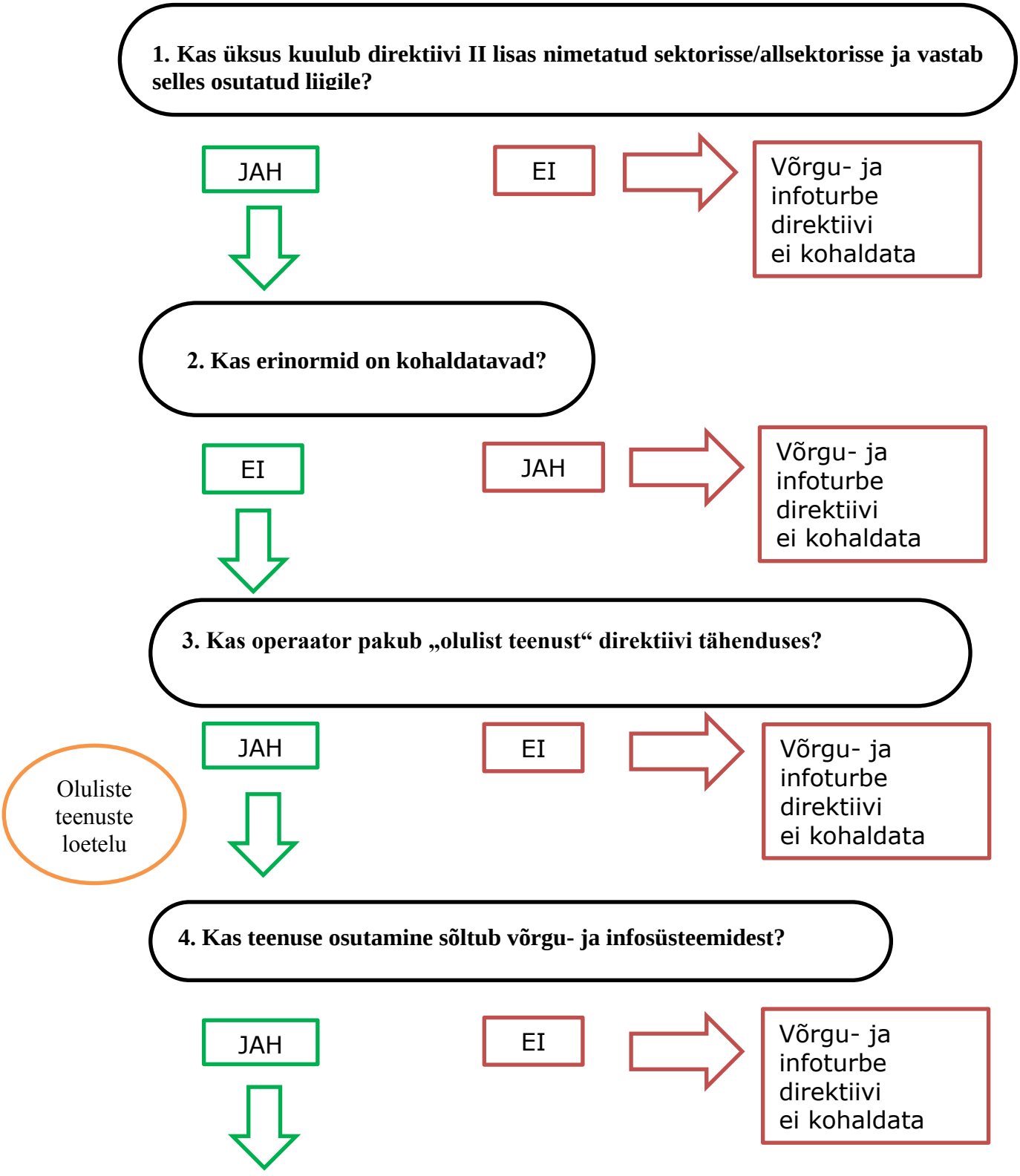
Tuleks märkida, et liikmesriigid ei tohiks artikli 5 lõike 2 kohase hindamise tegemisel lisada seal loetletud kriteeriumitele täiendavaid kriteeriume, kuna see võib vähendada identifitseeritud oluliste teenuste operaatorite arvu ja ohustada direktiivi artiklis 3 sätestatud oluliste teenuste operaatorite minimaalset ühtlustamist.

6. etapp. **Kas asjaomane operaator osutab olulisi teenuseid teistes liikmesriikides?**

6. etapp käsitleb juhtumeid, kus operaator osutab olulisi teenuseid kahes või enamas liikmesriigis. Artikli 5 lõikes 4 nõutakse, et enne identifitseerimisprotsessi lõpuleviimist peavad asjaomased liikmesriigid üksteisega konsulteerima[31].

[31] Konsultatsiooniprotsessi kohta vaata täpsemalt punkt 4.1.7.

Joonis 4. Kuueetapiline identifitseerimisprotsess



5. Kas turvaintsidendil on oluline häiriv mõju?

Sektoritevahelised tegurid (artikli 6 lõige 1)

- Teenustest sõltuvate **kasutajate arv**
- Teiste oluliste sektorite **sõltuvus** teenusest
- Intsidentide võimalik mõju **majandus- ja ühiskondlikule tegevusele** või **avalikule julgeolekule**
- Mõjutatud **geograafilise ala** võimalik **ulatus**
- Üksuse tähtsus **teenuse piisava kvaliteedi** säilitamisel

Sektoripõhised tegurid (põhjenduses 28 osutatud näited)

- **Energeetika**: liikmesriigi energiatootmise maht või osakaal
- **Transport**: osakaal riigi liiklusmahus ja vedude arv aastas
- **Tervishoiusektor:** teenuseosutaja hoole all olevate patsientide arv aastas

JAH

EI → Võrgu- ja infoturbe direktiivi ei kohaldata

6. Kas asjaomane operaator pakub olulisi teenuseid teistes liikmesriikides?

JAH

EI → Võrgu- ja infoturbe direktiivi ei kohaldata

Kohustuslik konsulteerimine

Riiklike meetmete võtmine (nt oluliste teenuste operaatorite loetelu, poliitika- ja õiguslikud meetmed)

4.1.7. Piiriülene konsulteerimine

Artikli 5 lõikes 4 on sätestatud, et juhul kui operaator osutab teenust kahes või enamas liikmesriigis, peavad kõnealused liikmesriigid üksteisega konsulteerima enne identifitseerimisprotsessi lõpuleviimist. Konsulteerimise eesmärk on aidata hinnata operaatori tähtsust piiriülese mõju seisukohast.

Konsulteerimisega soovitakse saavutada seda, et asjaomased riigi ametiasutused arutavad omavahel küsimust ja esitavad oma seisukohad ning jõuavad asjaomase operaatori identifitseerimisel parimal juhul samale tulemusele. Võrgu- ja infoturbe direktiiv ei välista siiski võimalust, et liikmesriigid jõuavad erinevatele järeldustele selles, kas konkreetne üksus identifitseeritakse oluliste teenuste operaatorina või mitte. Põhjenduses 24 nimetatakse liikmesriikide võimalust paluda selles protsessis abi koostöörühmalt.

Komisjoni arvates peaksid liikmesriigid püüdma jõuda nendes küsimustes konsensusele, et ei tekiks olukorda, kus samal ettevõtjal on eri liikmesriikides erinev õiguslik seisund. Lahknevus peaks olema erandlik olukord, näiteks kui ühes liikmesriigis oluliste teenuste operaatorina identifitseeritud üksuse tegevus teises liikmesriigis on vähetähtis.

4.2. Turvanõuded

Artikli 14 lõike 1 kohaselt peavad liikmesriigid tagama, et oluliste teenuste operaatorid võtavad tehnika taset arvesse võttes asjakohaseid ja proportsionaalseid tehnilisi ja korralduslikke meetmeid, eesmärgiga hallata riske, mis ohustavad nende töös kasutatavate võrgu- ja infosüsteemide turvalisust. Vastavalt artikli 14 lõikele 2 ennetavad ja minimeerivad asjakohased meetmed intsidentide mõju.

Koostöörühma spetsiaalse töösuuna raames valmistatakse praegu ette mittesiduvaid suuniseid oluliste teenuste operaatorite turvameetmete kohta[32]. Koostöörühma juhenddokument valmib 2017. aasta neljandaks kvartaliks. Komisjon julgustab liikmesriike koostöörühma koostatavat juhenddokumenti täpselt järgima, et turvanõudeid käsitlevad riiklikud sätted oleksid sellega võimalikult suures ulatuses kooskõlas. Nõuete ühtlustamine aitaks oluliste teenuste operaatoritel, kes sageli osutavad olulisi teenuseid rohkem kui ühes liikmesriigis, järgida nõudeid. See aitaks ka riiklikel pädevatel asutustel ja CSIRTidel täita oma järelevalveülesandeid.

4.3. Teatamisnõuded

Artikli 14 lõike 3 kohaselt peavad liikmesriigid tagama, et oluliste teenuste operaatorid teatavad „intsidentidest, millel on oluline mõju nende pakutavate oluliste teenuste järjepidevusele“. Järelikult ei peaks oluliste teenuste operaatorid teatama igast väiksemast intsidendist, vaid üksnes tõsistest intsidentidest, mis mõjutavad nende pakutavate oluliste

[32] Selle töösuuna edendamiseks levitati rahvusvaheliste standardite, hea tava ja riskihindamise/-juhtimise meetodite loetelusid kõikides võrgu- ja infoturbe direktiiviga hõlmatud sektorites ning neid kasutati kavandatavate turvavaldkondade ja -meetmete puhul taustinfona.

teenuste järjepidevust. Artikli 4 punkti 7 määratluse kohaselt on intsident „sündmus, mis tegelikult kahjustab võrgu- ja infosüsteemide turvalisust“. Artikli 4 punkti 2 määratluse kohaselt on võrgu- ja infosüsteemide turvalisus „võrgu- ja infosüsteemi võime panna teatava kindlusega vastu mis tahes tegevusele, mis seab ohtu salvestatud, edastatud või töödeldud andmete või nendega seotud, võrgu- ja infosüsteemi kaudu pakutavate või juurdepääsetavate teenuste kättesaadavuse, autentsuse, tervikluse ja konfidentsiaalsuse“. Sellest tulenevalt võib teatamiskohustus tekkida mis tahes sündmuse puhul, mis kahjustab mitte ainult andmete või seotud teenuste kättesaadavust, vaid ka nende autentsust, terviklust ja konfidentsiaalsust. Artikli 14 lõikes 3 osutatud teenuse järjepidevust rikutakse tegelikult mitte ainult füüsilise kättesaadavusega seotud juhtudel, vaid ka teenuse nõuetekohast osutamist mõjutavate muude turvaintsidentide korral[33].

Koostöörühma spetsiaalse töösuuna raames valmistatakse praegu ette mittesiduvaid suuniseid, mis käsitlevad intsidentidest teatamist olukordades, kus oluliste teenuste operaatorid peavad intsidentidest teatama vastavalt võrgu- ja infoturbe direktiivi artikli 14 lõikele 7, ning sellise teatamise vormi ja korda. Suunised peaksid valmima 2017. aasta neljandaks kvartaliks.

Erinevad riigisisesed teatamisnõuded võivad põhjustada piiriüleselt tegutsevate teenuse osutajate jaoks õiguslikku ebakindlust, keerukamaid ja koormavamaid menetlusi ning suuri halduskulusid. Seepärast toetabki komisjon koostöörühma tööd. Nagu turvanõuete puhulgi, julgustab komisjon liikmesriike koostöörühma koostatavat juhenddokumenti täpselt järgima, et intsidentidest teatamist käsitlevad riiklikud sätted oleksid sellega võimalikult suures ulatuses kooskõlas.

4.4. Võrgu- ja infoturbe direktiivi III lisa: digitaalse teenuse osutajad

Digitaalse teenuse osutajad on teine üksuste kategooria, mis on võrgu- ja infoturbe direktiiviga reguleeritud. Neid üksusi peetakse olulisteks majanduses osalejateks, kuna neid kasutavad teenuste osutamiseks paljud ettevõtjad ning digitaalse teenuse häired võivad mõjutada olulisi majandus- ja ühiskondlikke tegevusi.

4.4.1. Digitaalse teenuse osutajate kategooriad

Digitaalset teenust määratlevas artikli 4 punktis 5 osutatakse direktiivi (EL) 2015/1535 artikli 1 lõike 1 punktis b esitatud legaaldefinitsioonile, kitsendades kohaldamisala III lisas loetletud teenuseliikidele. Direktiivi (EL) 2015/1535 artikli 1 lõike 1 punkti b määratluse kohaselt on need teenused „kõik vahemaa tagant elektroonilisel teel ja teenusesaaja isikliku taotluse alusel ning tavaliselt tasu eest osutatavad teenused“ ning direktiivi III lisas on loetletud kolme liiki teenused: internetipõhine kauplemiskoht, internetipõhine otsingumootor ja pilvandmetöötlusteenus. Oluliste teenuste operaatoritega võrreldes ei nõuta direktiivis liikmesriikidelt nende digitaalse teenuse osutajate identifitseerimist, et siis nende suhtes kohaldada asjaomaseid kohustusi. Seetõttu kohaldatakse direktiivi asjaomaseid kohustusi, nimelt artiklis 16 sätestatud turva- ja teatamisnõudeid, kõikide direktiivi kohaldamisalasse kuuluvate digitaalse teenuse osutajate suhtes.

[33] See kehtib ka digitaalse teenuse osutajate kohta.

Järgnevates punktides esitatakse täiendavaid selgitusi direktiivi kohaldamisalaga hõlmatud kolme liiki digitaalsete teenuste kohta.

1. Internetipõhise kauplemiskoha pakkuja

Internetipõhine kauplemiskoht võimaldab väga paljudel ja väga erinevatel ettevõtjatel kaubelda tarbijatega ning luua ärisuhteid teiste ettevõtjatega. See annab ettevõtjatele alustaristu internetipõhiseks ja piiriüleseks kauplemiseks. Internetipõhise kauplemiskoha pakkujatel on majanduses oluline roll, kuna nad annavad eelkõige VKEdele juurdepääsu ELi digitaalsele ühtsele turule. Nende tegevus võib hõlmata ka kaugandmetöötluse teenuste osutamist, mis lihtsustavad kliendi majandustegevust, sealhulgas tehingute töötlemist ning ostjate, tarnijate ja toodete kohta teabe kogumist, aga ka vajalike toodete otsimise hõlbustamist, kaupade pakkumist, tehingutealast oskusteavet ning ostjate ja müüjate kokkuviimist.

Internetipõhine kauplemiskoht on määratletud artikli 4 punktis 17 ning seda on täpsustatud põhjenduses 15. Internetipõhist kauplemiskohta kirjeldatakse teenusena, mis võimaldab tarbijatel ja kauplejatel sõlmida kauplejatega internetipõhiseid müügi- või teenuse osutamise lepinguid ning see on selliste lepingute sõlmimise lõplik sihtkoht. Näiteks võib E-bay sarnast teenuse osutajat pidada internetipõhiseks kauplemiskohaks, kuna see võimaldab teistel luua tema platvormil poode, et teha oma tooted ja teenused tarbijatele või ettevõtjatele veebis kättesaadavaks. Internetipõhise kauplemiskoha määratluse alla kuuluvad ka rakenduste ja tarkvaraprogrammide levitamiseks mõeldud veebipõhised tarkvarapoed, kuna need võimaldavad rakenduste arendajatel müüa või turustada oma teenuseid tarbijatele või teistele ettevõtjatele. Artikli 4 punkti 17 määratlusega ei ole seevastu hõlmatud kolmanda osapoole teenuste vahendajad, nagu Skyscanner ja hinnavõrdlusteenused, mis suunavad kasutajad kaupleja veebisaidile, kus teenuse või tootega seotud tehing tegelikult sõlmitakse.

2. Internetipõhise otsingumootori pakkuja

Internetipõhine otsingumootor on määratletud artikli 4 punktis 18 ning seda on täpsustatud põhjenduses 16. Seda kirjeldatakse digitaalse teenusena, mis võimaldab kasutajatel teha mis tahes teemal otsinguid üldjuhul kõikidelt veebisaitidelt või konkreetses keeles veebisaitidelt. Määratlus ei hõlma veebisaidisiseste otsingutega piirduvaid otsingufunktsioone ega hinnavõrdluse veebisaite. Näiteks ei saa sellist otsingumootorit nagu EUR-Lex[34] pidada otsingumootoriks direktiivi tähenduses, kuna selle otsingufunktsioon piirdub konkreetse veebisaidi sisuga.

3. Pilvandmetöötlusteenuse osutaja

Artikli 4 punktis 19 esitatud määratluse kohaselt on pilvandmetöötlusteenus „digitaalne teenus, mis võimaldab juurdepääsu skaleeritavale ja paindlikule jagatavate andmetöötlusressursside kogumile“; andmetöötlusressursside ning skaleeritava ja paindliku kogumi mõisteid täpsustatakse põhjenduses 17.

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

Pilvandmetöötlust võib lühidalt kirjeldada teatud liiki andmetöötlusteenusena, mis kasutab jagatud ressursse nõudmispõhiseks andmete töötlemiseks. Jagatud ressursid on mis tahes riist- või tarkvara komponendid (nt võrgud, serverid või muu taristu, hoidlad, rakendused ja teenused), mis tehakse kasutajate nõudmisel neile andmete töötlemiseks kättesaadavaks. Termin „jagatav“ osutab andmetöötlusressurssidele, mille puhul paljud kasutajad kasutavad andmetöötluseks sama füüsilist taristut. Andmetöötlusressursse peetakse jagatavaks, kui teenuse osutaja kasutatavat ressursikogumit saab mis tahes hetkel kasutaja vajadustest olenevalt laiendada või vähendada. Seega saab andmekeskusi või ühe andmekeskuse üksikuid komponente lisada või ära võtta, kui andmetöötluse või -salvestuse kogumaht vajab ajakohastamist. Mõistet „paindlik kogum“ kirjeldatakse töökoormuse muutumisena, mille puhul suurendatakse ja vähendatakse automaatselt andmetöötlusressursside pakkumist, nii et kättesaadavad ressursid vastavad igal ajahetkel võimalikult täpselt hetkenõudlusele[35].

Praegu on olemas kolm põhilist pilveteenuse mudeli liiki, mida teenuse osutaja saab pakkuda:

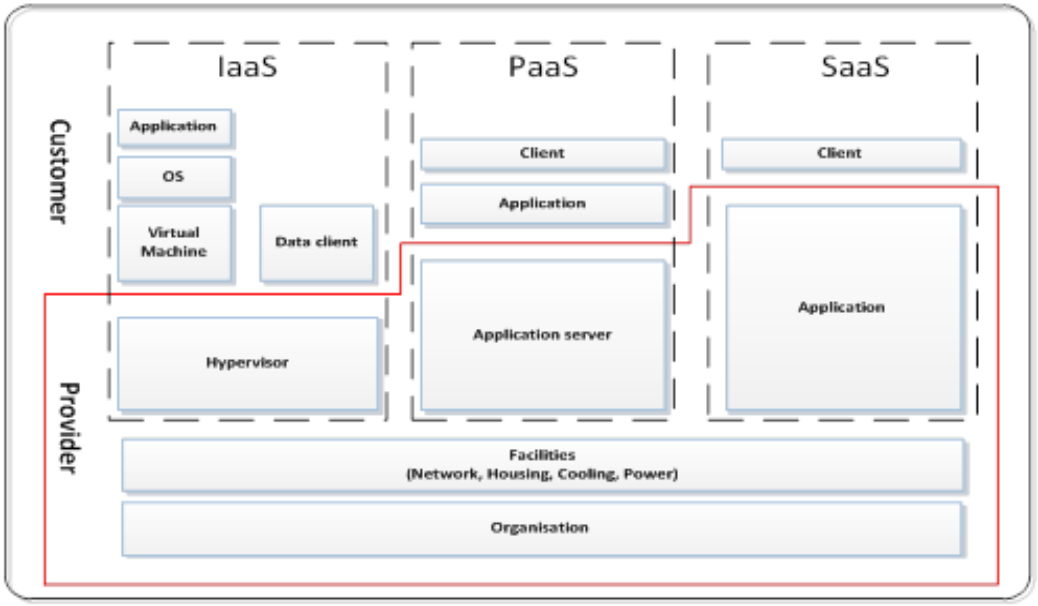
- taristu kui teenus (*Infrastructure as a Service*, IaaS) – pilveteenuse kategooria, kus kliendile pakutakse pilveteenusena taristut. See hõlmab andmetöötlusressursside virtuaalset pakkumist riistvara-, võrgu- või hoidlateenuse vormis. IaaS võimaldab kasutada servereid, andmete talletamist, võrke ja operatsioonisüsteeme. IaaS pakub ettevõtjale taristut, kus ta saab oma andmeid talletada ja kasutada rakendusi, mida ta oma igapäevatöös vajab;

- platvorm kui teenus (*Platform as a Service*, PaaS) – pilveteenuse kategooria, kus kliendile pakutakse pilveteenusena platvormi. See hõlmab veebipõhiseid andmetöötlusplatvorme, mis võimaldavad ettevõtjatel kasutada olemasolevaid rakendusi või luua ja katsetada uusi;

- tarkvara kui teenus (*Software as a service*, SaaS) – pilveteenuse kategooria, kus kliendile pakutakse pilveteenusena interneti kaudu kasutatavat rakendust või tarkvara. Seda pilveteenust kasutades ei ole lõppkasutajal vaja tarkvara osta, installeerida ega hallata ning tarkvarale pääseb juurde kõikjalt, kus on internetiühendus.

[35] Nikolas Roman Herbst, Samuel Kounev, Ralf Reussner, Karlsruhe tehnikainstituut, „Elasticity in Cloud Computing: What It Is, and What It Is Not“ (Pilvandmetöötluse paindlikkus: mis see on ja mis see ei ole), avaldatud aadressil https://sdqweb.ipd.kit.edu/publications/pdfs/HeKoRe2013-ICAC-Elasticity.pdf. Vt ka COM(2012) 529, lk 2–5.

Joonis 5. Pilvandmetöötluse teenusemudelid ja varad



ENISA on avaldanud põhjalikud suunised pilvandmetöötlusega seotud konkreetsetel teemadel[36] ning juhenddokumendi pilvandmetöötluse põhitõdede kohta[37].

4.4.2. Turvanõuded

Artikli 16 lõike 1 kohaselt peavad liikmesriigid tagama, et digitaalse teenuse osutajad võtavad asjakohaseid ja proportsionaalseid tehnilisi ja korralduslikke meetmeid, et hallata riske, mis ohustavad ettevõtjate poolt teenuste osutamiseks kasutavate võrgu- ja infosüsteemide turvalisust. Turvameetmetes tuleks arvesse võtta tehnika taset ning järgmist viit elementi: i) süsteemide ja rajatiste turvalisus; ii) intsidentide käsitlemine; iii) talitluspidevuse haldamine; iv) seire, auditeerimine ja testimine; v) vastavus rahvusvahelistele standarditele.

Seoses sellega on komisjonil vastavalt artikli 16 lõikele 8 õigus vastu võtta rakendusakte, et neid elemente täpsustada ja tagada digitaalse teenuse osutajate ühtlustamise kõrge tase. Komisjonil on plaanis rakendusakt vastu võtta 2017. aasta sügisel. Peale selle peavad liikmesriigid tagama, et digitaalse teenuse osutajad võtavad intsidentide mõju vältimiseks ja minimeerimiseks vajalikud meetmed, eesmärgiga tagada oma teenuste järjepidevus.

4.4.3. Teatamisnõuded

Digitaalse teenuse osutajad peaksid olema kohustatud teatama tõsistest intsidentidest pädevatele asutustele või CSIRTidele. Vastavalt võrgu- ja infoturbe direktiivi artikli 16 lõikele 3 tekib digitaalse teenuse osutajatel teatamiskohustus juhtudel, kui turvaintsidendil on teenuse osutamisele oluline mõju. Mõju kindlakstegemiseks on artikli 16 lõikes 4 loetletud viis konkreetset parameetrit, mida digitaalse teenuse osutaja peab arvesse võtma. Komisjonil

[36] Kättesaadav aadressil https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security.
[37] ENISA, „Cloud Security Guide for SMEs“ (Pilvandmetöötluse turvalisuse juhend VKEdele), 2015. Kättesaadav aadressil https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes.

on sellega seoses vastavalt artikli 16 lõikele 8 õigus vastu võtta rakendusakte, milles kirjeldatakse parameetreid täpsemalt. Kõnealuste parameetrite täpsustamine on osa punktis 4.4.2 nimetatud turvaelemente täpsustavast rakendusaktist, mille komisjon kavatseb sügisel vastu võtta.

4.4.4. Riskipõhine regulatiivne lähenemisviis

Artiklis 17 on sätestatud, et pädevad asutused võtavad digitaalse teenuse osutajate suhtes meetmeid järgneva järelevalve käigus. Liikmesriigid peavad tagama, et pädevad asutused võtavad meetmeid, kui neile esitatakse tõendid, et digitaalse teenuse osutaja ei täida direktiivi artiklis 16 sätestatud nõudeid.

Peale selle on komisjonil artikli 16 lõigete 8 ja 9 kohaselt õigus vastu võtta rakendusakte teatamis- ja turvanõuete kohta, mis edendavad ühtlustamist digitaalse teenuse osutajate jaoks. Artikli 16 lõike 10 kohaselt ei tohi liikmesriigid kehtestada digitaalse teenuse osutajate suhtes lisaks direktiiviga ette nähtutele täiendavaid turva- või teatamisnõudeid, välja arvatud juhul, kui need meetmed on vajalikud riigi põhifunktsioonide, eelkõige riigi julgeoleku tagamiseks ning kuritegude uurimise, avastamise ja nende eest vastutusele võtmise võimaldamiseks.

Digitaalse teenuse osutajate piiriülest olemust arvesse võttes ei järgi direktiiv mitme üheaegse jurisdiktsiooni mudelit, vaid lähenemisviisi, mis põhineb ettevõtja peamisel tegevuskohal liidus[38]. See võimaldab digitaalse teenuse osutajate suhtes kohaldada ühtset reeglistikku, kusjuures järelevalve eest vastutab üks pädev asutus – see on eriti oluline, sest paljud digitaalse teenuse osutajad pakuvad teenuseid korraga mitmes liikmesriigis. Sellise lähenemisviisi kohaldamine vähendab digitaalse teenuse osutajate koormust nõuete täitmisel ning tagab digitaalse ühtse turu nõuetekohase toimimise.

4.4.5. Jurisdiktsioon

Võrgu- ja infoturbe direktiivi artikli 18 lõike 1 kohaselt kuulub digitaalse teenuse osutaja selle liikmesriigi jurisdiktsiooni alla, kelle territooriumil on tema peamine tegevuskoht, nagu on eespool selgitatud. Artikli 18 lõikes 2 on sätestatud, et kui konkreetne digitaalse teenuse osutaja pakub teenuseid ELis, kuid tema asukoht ei ole liidu territooriumil, peab ta määrama oma esindaja liidus. Sellisel juhul käsitatakse digitaalse teenuse osutajat selle liikmesriigi jurisdiktsiooni alla kuuluvana, kus on esindaja asukoht. Juhul kui digitaalse teenuse osutaja pakub liikmesriigis teenuseid, kuid ei ole esindajat ELis määranud, võib liikmesriik põhimõtteliselt võtta digitaalse teenuse osutaja suhtes meetmeid, kuna see rikub direktiivist tulenevaid kohustusi.

4.4.6. Piiratud ulatusega digitaalse teenuse osutajate vabastamine turvanõuetest ja teatamiskohustusest

Artikli 16 lõike 11 kohaselt on digitaalse teenuse osutajad, kes on mikro- ja väikeettevõtjad komisjoni soovituse 2003/361/EÜ[39] tähenduses, vabastatud artiklis 16 sätestatud turvanõuetest ja teatamiskohustusest. Need nõuded ei ole seega siduvad ettevõtjatele, kus

[38] Vt eelkõige direktiivi artikkel 18.
[39] ELT L 24, 20.5.2003, lk 36.

töötab vähem kui 50 töötajat ja kelle aastakäive ja/või aasta bilansimaht ei ületa 10 miljonit eurot. Üksuse suuruse kindlakstegemisel ei ole oluline, kas asjaomane ettevõtja osutab üksnes võrgu- ja infoturbe direktiivis sätestatud digitaalseid teenuseid või ka muid teenuseid.

5. Võrgu- ja infoturbe direktiivi ja muude õigusaktide vaheline seos

Käesolevas punktis käsitletakse võrgu- ja infoturbe direktiivi artikli 1 lõikes 7 nimetatud erinorme, esitades kolm näidet komisjoni poolt seni hinnatud erinormide kohta ning täpsustades telekommunikatsiooniettevõtjate ja usaldusteenuse osutajate suhtes kohaldatavaid turva- ja teatamisnõudeid.

5.1. Võrgu- ja infoturbe direktiivi artikli 1 lõige 7: erinorme käsitlev säte

Võrgu- ja infoturbe direktiivi artikli 1 lõike 7 kohaselt ei ole digitaalse teenuse osutajate ja oluliste teenuste operaatorite suhtes kehtivaid turva- ja teatamisnõudeid käsitlevad direktiivi sätted kohaldatavad, kui sektoripõhises ELi õigusaktis sätestatud turva- ja/või teatamisnõuded on toimelt vähemalt samaväärsed võrgu- ja infoturbe direktiivi asjaomaste kohustustega. Liikmesriigid peavad artikli 1 lõiget 7 arvesse võtma direktiivi üldisel ülevõtmisel ning esitama komisjonile teabe erinormide kohaldamise kohta.

Metoodika

Sektoripõhiste ELi õigusaktide ja võrgu- ja infoturbe direktiivi asjaomaste sätete samaväärsuse hindamisel tuleks erilist tähelepanu pöörata küsimusele, kas sektoripõhiste õigusaktide turvanõuded hõlmavad meetmeid, mis tagavad võrgu- ja infosüsteemide turvalisuse, nagu on sätestatud direktiivi artikli 4 punktis 2.

Teatamiskohustuse kohta on võrgu- ja infoturbe direktiivi artikli 14 lõikes 3 ja artikli 16 lõikes 3 sätestatud, et oluliste teenuste operaatorid ja digitaalse teenuse osutajad peavad põhjendamatu viivituseta teatama pädevatele asutustele või CSIRTile intsidentidest, millel on oluline mõju teenuse osutamisele. Seoses sellega tuleb pöörata erilist tähelepanu operaatori / digitaalse teenuse osutaja kohustusele esitada teates teavet, mis võimaldab pädeval asutusel või CSIRTil kindlaks teha turvaintsidendi piiriülese mõju.

Praegu puuduvad digitaalse teenuse osutajate kategooriat reguleerivad sektoripõhised õigusaktid, mis näeksid ette võrgu- ja infoturbe direktiivi artiklis 16 sätestatud turva- ja teatamisnõuetega võrreldavad nõuded, millega saaks arvestada võrgu- ja infoturbe direktiivi artikli 1 lõike 7 kohaldamisel[40].

Mis puutub oluliste teenuste operaatoritesse, siis praegu kohaldatakse sektoripõhistest ELi õigusaktidest tulenevaid turva- ja/või teatamisnõudeid finantssektori ja eelkõige pangandus- ja finantsturu taristu suhtes, millele on osutatud II lisa punktides 3 ja 4. See on tingitud asjaolust, et finantsinstitutsioonide kasutatavate IT-süsteemide ning võrgu- ja infosüsteemide turvalisus

[40] See ei piira järelevalveasutuse teavitamist isikuandmetega seotud rikkumisest, mida käsitletakse isikuandmete kaitse üldmääruse artiklis 33.

ja terviklikkus on ELi õigusaktidega finantsinstitutsioonidele kehtestatud operatsiooniriskiga seotud nõuete oluline osa.

Näited

i) Teine makseteenuste direktiiv

Nn teise makseteenuste direktiiviga[41] on ette nähtud pangandussektori ja eelkõige määruse (EL) 575/2013 artikli 4 lõike 1 punktis 1 määratletud krediidiasutuste poolt makseteenuste osutamise puhul kohaldatavad turva- ja teatamisnõuded, mis on sätestatud direktiivi artiklites 95 ja 96.

Täpsemalt nõutakse artikli 95 lõikes 1 makseteenuse pakkujatelt asjakohaste leevendusmeetmete ja kontrollimehhanismide kehtestamist, et juhtida nende pakutavate makseteenustega seotud operatsiooni- ja turvariske. Need meetmed peaksid hõlmama tulemuslike intsidentide haldamise menetluste kehtestamist ja rakendamist, sealhulgas suurte operatsiooni- ja turvaintsidentide avastamise ja liigitamise menetlusi. Teise makseteenuste direktiivi põhjendustes 95 ja 96 täpsustatakse selliste turvameetmete laadi. Nende sätete põhjal on ilmne, et ettenähtud meetmete eesmärk on hallata makseteenuste osutamisel kasutatavate võrgu- ja infosüsteemidega seotud turvariske. Seepärast võib neid turvanõudeid pidada toimelt vähemalt samaväärseteks võrgu- ja infoturbe direktiivi artikli 14 lõigete 1 ja 2 vastavate sätetega.

Teatamisnõuete puhul nähakse teise makseteenuste direktiivi artikli 96 lõikes 1 ette makseteenuse pakkujate kohustus teavitada suurema turvaintsidendi korral põhjendamatu viivituseta pädevat asutust. Peale selle nõutakse teise makseteenuste direktiivi artikli 96 lõikes 2, mis on võrreldav võrgu- ja infoturbe direktiivi artikli 14 lõikega 5, et pädev asutus teavitaks teiste liikmesriikide pädevaid asutusi intsidendist, kui see on asjakohane. See kohustus tähendab ka seda, et turvaintsidentidest teatamine peab hõlmama teavet, mis võimaldaks asutustel hinnata intsidendi piiriülest mõju. Teise makseteenuste direktiivi artikli 96 lõike 3 punktiga a antakse Euroopa Pangandusjärelevalvele õigus töötada koostöös Euroopa Keskpangaga välja suunised intsidentidest teavitamise sisu ja vormi kohta.

Sellest tulenevalt võib järeldada, et kui krediidiasutused osutavad makseteenuseid, siis tuleks võrgu- ja infoturbe direktiivi artikli 1 lõike 7 kohaselt kohaldada võrgu- ja infoturbe direktiivi artikli 14 vastavate sätete asemel teise makseteenuste direktiivi artiklites 95 ja 96 sätestatud turva- ja teatamisnõudeid.

ii) Euroopa Parlamendi ja nõukogu 4. juuli 2012. aasta määrus (EL) nr 648/2012 börsiväliste tuletisinstrumentide, kesksete vastaspoolte ja kauplemisteabehoidlate kohta

Finantsturu taristuga seoses sisaldab määrus (EL) nr 648/2012 koostoimes komisjoni delegeeritud määrusega (EL) nr 153/2013 sätteid kesksetele vastaspooltele kehtivate turvanõuete kohta – seda võib käsitada erinormina. Nendes õigusaktides on eelkõige

[41] Direktiiv (EL) 2015/2366 (ELT L 337, 23.12.2015, lk 35).

sätestatud võrgu- ja infosüsteemide turvalisusega seotud tehnilised ja korralduslikud meetmed, mis lähevad üksikasjades kaugemale võrgu- ja infoturbe direktiivi artikli 14 lõigete 1 ja 2 nõuetest ning mida võib seetõttu turvanõuete puhul pidada vastavaks võrgu- ja infoturbe direktiivi artikli 1 lõike 7 tingimustele.

Määruse (EL) nr 648/2012 artikli 26 lõikes 1 on täpsemalt sätestatud, et üksusel peab olema „kindel juhtimiskord, mis hõlmab selgesti määratletud, läbipaistvate ja sidusate vastutusaladega selget organisatsioonilist struktuuri, tõhusaid protseduure riskide või võimalike riskide tuvastamiseks, juhtimiseks, jälgimiseks ja nendest teatamiseks ning piisavaid sisekontrollimeetmeid, sealhulgas usaldusväärset juhtimis- ja raamatupidamiskorda“. Artikli 26 lõike 3 kohaselt peab organisatsiooniline struktuur tagama, et teenuseid osutatakse ja tegevusi sooritatakse järjepidevalt ja korrektselt, kasutades asjakohaseid ja proportsionaalseid süsteeme, ressursse ja protseduure.

Lisaks sellele täpsustatakse artikli 26 lõikes 6, et „keskse vastaspoole IT-süsteemid peavad olema sellised, mis sobivad keeruliste eri liiki teenuste osutamiseks ja tegevuste sooritamiseks ning millega tagatakse turvalisuse kõrge tase ja säilitatava teabe terviklikkus ja konfidentsiaalsus“. Artikli 34 lõikes 1 kohustatakse looma, rakendama ja haldama piisavat talitluspidevuse kava ja avariitaastekava, mis peaksid tagama tegevuste kiire taastamise.

Need kohustused on täpsemalt määratletud komisjoni 19. detsembri 2012. aasta delegeeritud määruses (EL) nr 153/2013, millega täiendatakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 648/2012 seoses regulatiivsete tehniliste standarditega, mis käsitlevad kesksete vastaspoolte suhtes kohaldatavaid nõudeid[42]. Eelkõige pannakse selle artiklis 4 kesksele vastaspoolele kohustus töötada välja asjakohased riskijuhtimisvahendid, et juhtida kõiki asjaomaseid riske ja anda nende kohta aru, ning määrata kindlaks meetmete liigid (nt usaldusväärse teabe ja kindlate riskikontrollisüsteemide kasutamine, vahendite ja oskusteabe kättesaadavus ja juurdepääs kogu asjakohasele teabele riskijuhtimise funktsiooni täitmiseks, asjakohaste sisekontrollimehhanismide, nagu usaldusväärne haldus- ja raamatupidamiskord, kättesaadavus, et aidata keskse vastaspoole juhtorganil jälgida ja hinnata riskijuhtimise põhimõtete, protseduuride ja süsteemide asjakohasust ja tulemuslikkust).

Lisaks osutatakse artiklis 9 sõnaselgelt infotehnoloogiasüsteemide turvalisusele ning sätestatakse konkreetsed tehnilised ja korralduslikud meetmed seoses töökindla infoturberaamistikuga, mille abil hallatakse IT turbe riske. Need meetmed peaksid hõlmama mehhanisme ja menetlusi, mis tagavad teenuste kättesaadavuse ning andmete täpsuse, terviklikkuse ja konfidentsiaalsuse kaitse.

iii) Euroopa Parlamendi ja nõukogu 15. mai 2014. aasta direktiiv 2014/65/EL finantsinstrumentide turgude kohta ning millega muudetakse direktiive 2002/92/EÜ ja 2011/61/EL[43]

[42] ELT L 52, 23.2.2013, lk 41.
[43] ELT L 173, 12.6.2014, lk 349.

Kauplemiskohtadega seoses nõutakse direktiivi 2014/65/EL artikli 48 lõikes 1, et operaatorid tagaksid teenuste jätkuvuse kauplemissüsteemide häirete korral. Seda üldist kohustust on hiljuti täpsustatud ja täiendatud komisjoni 14. juuli 2016. aasta delegeeritud määrusega (EL) 2017/584,[44] millega täiendatakse Euroopa Parlamendi ja nõukogu direktiivi 2014/65/EL seoses regulatiivsete tehniliste standarditega, milles määratakse kindlaks kauplemiskohtade organisatsioonilised nõuded[45]. Eelkõige määruse artikli 23 lõikes 1 on sätestatud, et kauplemiskohad kehtestavad füüsilise ja elektroonilise turbe menetlused ja korra, mille eesmärk on kaitsta oma süsteeme väärkasutamise või loata juurdepääsu eest ning tagada andmete terviklikkus. Need meetmed peaksid võimaldama infosüsteemide vastaste rünnete riski vältida või minimeerida.

Artikli 23 lõikes 2 nõutakse, et operaatorite rakendatavad meetmed ja kord võimaldaksid riski viivitamatut tuvastamist ja juhtimist seoses loata juurdepääsuga, süsteemi häirimisega, mis takistab tõsiselt infosüsteemi toimimist või katkestab selle, ning andmetesse sekkumisega, mis hõlmab andmete kättesaadavust, terviklikkust või autentsust. Lisaks selle pannakse määruse artikliga 15 kauplemiskohtadele kohustus omada tõhusat talitluspidevuse korda, et tagada süsteemi piisav stabiilsus ja tegeleda häiretega. Need meetmed peaksid eelkõige võimaldama operaatoritel jätkata kauplemist kahe tunni jooksul või enam-vähem selle aja piires ning ühtlasi tagama, et kaduma läinud andmehulk on nullilähedane.

Artiklis 16 on samuti sätestatud, et meetmed, mis on tehtud kindlaks häirivate intsidentidega tegelemiseks ja haldamiseks, peaksid olema kauplemiskohtade talitluspidevuse kava osa, ning sellega nähakse ette konkreetsed elemendid, mida operaator peab talitluspidevuse kava vastuvõtmisel arvesse võtma (nt spetsiifilise turbetoimingute meeskonna loomine, mõjuhinnangu koostamine, milles tehakse kindlaks riskid, ja selle korrapärane läbivaatamine).

Nende turvameetmete sisu arvesse võttes tundub, et nende eesmärk on juhtida andmete või osutatavate teenuste kättesaadavuse, autentsuse, terviklikkuse ja konfidentsiaalsusega seotud riske ja nendega tegeleda; sellest võib järeldada, et eespool mainitud sektoripõhised ELi õigusaktid sisaldavad turvanõudeid, mis on toimelt vähemalt samaväärsed võrgu- ja infoturbe direktiivi artikli 14 lõigete 1 ja 2 vastavate kohustustega.

5.2. Võrgu- ja infoturbe direktiivi artikli 1 lõige 3: telekommunikatsioonieettevõtjad ja usaldusteenuse osutajad

Artikli 1 lõike 3 kohaselt ei kohaldata direktiivis sätestatud turva- ja teatamiskohustusi ettevõtjatele, kelle suhtes kohaldatakse direktiivi 2002/21/EÜ artiklites 13a ja 13b sätestatud nõudeid. Direktiivi 2002/21/EÜ artikleid 13a ja 13b kohaldatakse ettevõtjatele, kes pakuvad üldkasutatavaid sidevõrke või osutavad elektroonilise side teenuseid. Sellest tulenevalt peab ettevõtja järgima üldkasutatavate sidevõrkude pakkumisel või elektroonilise side teenuste osutamisel direktiivis 2002/21/EÜ sätestatud turva- ja teatamisnõudeid.

[44] ELT L 87, 31.3.2017, lk 350.
[45] http://ec.europa.eu/finance/securities/docs/isd/mifid/rts/160714-rts-7_en.pdf.

Kui sama ettevõtja osutab siiski ka muid teenuseid, näiteks võrgu- ja infoturbe direktiivi III lisas loetletud digitaalseid teenuseid (nt pilvandmetöötlus või internetipõhise kauplemiskoha teenus) või selliseid II lisa punkti 7 kohaseid teenuseid nagu domeeninimede süsteemi või interneti vahetuspunkti teenused, kohaldatakse ettevõtja suhtes nende konkreetsete teenuste osutamisel võrgu- ja infoturbe direktiivi turva- ja teatamisnõudeid. Tuleb märkida, et kuna II lisa punktis 7 loetletud teenuste osutajad kuuluvad oluliste teenuste operaatori kategooriasse, peavad liikmesriigid läbi viima artikli 5 lõike 2 kohase identifitseerimisprotsessi ja kindlaks tegema, millised domeeninimede süsteemi, interneti vahetuspunkti või tippdomeeninimede teenuseid osutavad ettevõtjad peaksid võrgu- ja infoturbe direktiivi nõudeid järgima. See tähendab seda, et hindamise järel on võrgu- ja infoturbe direktiivi nõudeid kohustatud järgima ainult need domeeninimede süsteemi, interneti vahetuspunkti või tippdomeeninimede teenuseid osutavad ettevõtjad, kes vastavad võrgu- ja infoturbe direktiivi artikli 5 lõike 2 kriteeriumidele.

Artikli 1 lõikes 3 on veel täpsustatud, et direktiivi turva- ja teatamisnõudeid ei kohaldata ka usaldusteenuse osutajatele, kelle suhtes kohaldatakse määruse (EL) nr 910/2014 artiklis 19 sätestatud sarnaseid nõudeid.

6. Avaldatud riiklikud küberturvalisuse strateegiadokumendid

	Liikmesriik	Strateegia pealkiri ja lingid
1	Austria	*Austrian Cybersecurity Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf (EN)
2	Belgia	*Securing Cyberspace* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ncss-be-fr (FR)
3	Bulgaaria	*Cyber Resilient Bulgaria 2020* (2016) http://www.cyberbg.eu/ (BG)
4	Horvaatia	*The national cyber security strategy of the republic of Croatia* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf (EN)
5	Tšehhi Vabariik	*National cyber security strategy of the Czech Republic for the period from 2015 to 2020* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (EN)
6	Küpros	*Cybersecurity Strategy of the Republic of Cyprus* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf (EN)
7	Taani	*The Danish Cyber and Information Security Strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/DK_NCSS.pdf (EN)
8	Eesti	*Cyber Security Strategy* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf (EN)
9	Soome	*Finland´s Cyber security Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf (EN)
10	Prantsusmaa	*French national digital security strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf (EN)
11	Iirimaa	*National Cyber Security Strategy 2015-2017* (2015)

		https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf (EN)
12	Itaalia	*National Strategic Framework for Cyberspace Security* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf (EN)
13	Saksamaa	*Cyber-security Strategy for Germany* (2016) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/ModerneVerwaltung-OeffentlicherDienst/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile (DE)
14	Ungari	*National Cyber Security Strategy of Hungary* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf (EN)
15	Läti	*Cyber Security Strategy of Latvia 2014–2018* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (EN)
16	Leedu	*The programme for the development of electronic information security (cyber-security) for 2011–2019* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf (EN)
17	Luksemburg	*National Cybersecurity Strategy II (2015)* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf (EN)
18	Malta	*National Cyber Security Strategy Green Paper* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGreenPaper.pdf (EN)
19	Madalmaad	*National Cyber Security Strategy 2* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf (EN)
20	Poola	*Cyberspace Protection Policy of the Republic of Poland* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf (EN)
21	Rumeenia	*Cybersecurity Strategy of Romania* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf (RO)
22	Portugal	*National Cyberspace Security Strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/portuguese-national-cyber-security-strategy/view

		(EN)
23	Slovakkia	*Cyber Security Concept of the Slovak Republic for 2015 – 2020* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 (EN)
24	Sloveenia	*Cyber Security Strategy establishing a system to ensure a high level of cyber security* (2016) http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf (EN)
25	Hispaania	*National Cyber Security Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf (EN)
26	Rootsi	*The Swedish National Cybersecurity Strategy* (2017) http://www.government.se/49edf4/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy.pdf (EN)
27	Ühendkuningriik	*National Cyber Security Strategy (2016-2021)* (2016) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf (EN)

7. Häid tavasid ja soovitusi sisaldavad ENISA materjalid

Intsidentidele reageerimine

- ✓ Intsidentidele reageerimise strateegiad ja küberkriiside alane koostöö[46]

Intsidentide käsitlemine

- ✓ Intsidentide käsitlemise automatiseerimise projekt[47]
- ✓ Intsidentide haldamise hea tava juhend[48]

Intsidentide klassifitseerimine ja taksonoomia

- ✓ Olemasolevate taksonoomiate ülevaade[49]
- ✓ Hea tava juhend taksonoomia kasutamisest intsidentide ennetamisel ja avastamisel[50]

CSIRTi küpsus

- ✓ Riiklike CSIRTide probleemid Euroopas 2016. aastal: CSIRTide küpsuse uuring[51]
- ✓ CSIRTide küpsuse uuring – hindamisprotsess[52]
- ✓ Suunised riiklikele CSIRTidele küpsuse hindamise kohta[53]

CSIRTi suutlikkuse arendamine ja koolitus

- ✓ Hea tava juhend koolitusmeetodite kohta[54]

Teabe leidmine CSIRTide kohta Euroopas. CSIRTide ülevaade riikide kaupa[55]

[46] ENISA, „Strategies for incident response and cyber crisis cooperation“, 2016. Avaldatud aadressil https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation.
[47] Lisateave aadressil https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation.
[48] ENISA, „Good Practice Guide for Incident Management“, 2010. Avaldatud aadressil https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management.
[49] Lisateave aadressil 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. Avaldatud aadressil 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. Avaldatud aadressil https://www.enisa.europa.eu/publications/study-on-csirt-maturity.
[52] ENISA, „Study on CSIRT Maturity – Evaluation Process“, 2017. Avaldatud aadressil 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. Avaldatud aadressil https://www.enisa.europa.eu/publications/csirt-capabilities.
[54] ENISA, „Good Practice Guide on Training Methodologies“, 2014. Avaldatud aadressil https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies.
[55] Lisainfo aadressil https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map.