

Verkko- ja tietoturvadirektiivin kansallisessa täytäntöönpano Suomessa

Liikenne- ja viestintäministeriön lausuntopyyntöön [Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta annetuista laeista](https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=12066eaa-f177-40ca-98c6-b2676ffc46bc&proposalLanguage=da4408c3-39e4-4f5a-84db-84481bafc744) Microsoft Oy lausuu kunnioittaen seuraavaa:

Tietoisuus kyberhyökkäysten uhkasta sekä tarve suojella verkko- ja tietojärjestelmien turvallisuutta ovat nousseet strategisen tärkeiksi tekijöiksi niin kansallisella kuin eurooppalaisella ja kansainväliselläkin tasolla. Microsoft on nostanut verkko- ja tietojärjestelmien turvallisuuden prioriteettiensa kärkijoukkoon, sillä tavoitteena on suojella Microsoftin järjestelmiä käyttäviä asiakkaita ja organisaatioita sekä noudattaa samoja parhaita käytäntöjä koko toimialalla. Tavoitteeseen pyritään suojelemalla IT-infrastruktuuria, hyödyntämällä kyberhyökkäysten ehkäisemiseen ja niiltä suojautumiseen suunniteltua teknologiaa sekä käymällä kansallista, eurooppalaista ja globaalia vuoropuhelua instituutioiden ja organisaatioiden kanssa.

Verkko- ja tietoturvadirektiivin kansallinen täytäntöönpano Suomessa on erinomainen tilaisuus saada aikaan tehokas sääntelyjärjestelmä, joka on yhdenmukaistettu muiden EU-maiden kanssa eurooppalaisen lainsäädännön mukaisesti. Tavoitteena tulee olla puutteiden korjaaminen ja sellaisten nykyisten mekanismien edistäminen, jotka ratkaisevat kyberturvallisuuden käytäntöihin liittyviä ongelmia. Verkko- ja tietoturvadirektiivin vahvistaminen on Microsoftille mieluisa kehitysaskel, sillä Euroopan ja koko maailman yleistä verkko- ja tietoturvallisuutta on tarpeen parantaa pikaisesti. Microsoft antaa mielellään panoksensa direktiivin yhdenmukaiseen, selkeään ja tehokkaaseen toteutukseen.

## Digitaalisten palvelujen tarjoajien sääntely

Koska digitaalisten palvelujen tarjoajien toimintaympäristö, Euroopan unionin jäsenvaltiot, on ominaisuuksiltaan erityinen, yhdenmukaistettu sääntelyjärjestelmä on keskeisen tärkeä menestyksen kannalta. Digitaalisten palvelujen tarjoajien luokat – pilvipalvelut (etenkin julkiset pilvipalvelut), verkon hakukoneet ja verkossa toimivat markkinapaikat – edustavat digitaalitalouden kolmea erillistä osa-aluetta, joista jokaisella on erilaiset kriittisyystasot. Digitaalisten palvelujen tarjoajien velvoitteet (esimerkiksi tietoturvavaatimukset ja tapahtumiin liittyvät ilmoitukset) on siksi eriytettävä luokan ja siihen liittyvän kriittisyyden perusteella.

Pilvipalvelun määritelmä on liian väljä, eikä siinä erotella erityyppisten palvelujen kriittisyystasoja. Yksi tapa ottaa pilvipalvelun kriittisyys huomioon mahdollisimman selkeästi on perustaa määritelmä palvelutyyppiin (sovellus, käyttöympäristö tai infrastruktuuri) ja käyttöönottomalliin (yksityinen, yhteisö, hybridi tai julkinen) ISO17788:2014-standardin mukaisesti.

Infrastruktuuritoiminnot sisältävä tyyppi, josta usein käytetään nimitystä IaaS (Infrastructure-as-a-Service), vaikuttaa näissä olosuhteissa merkittävästi siihen, miten kriittisyys on otettava huomioon. Kuten ISO17789:2014-standardin kohdassa 10.2.1 (Service capabilities functional component) selitetään, sovellus (eli SaaS-ohjelma, Software-as-a-Service) voidaan ottaa käyttöön käyttöympäristössä (eli PaaS-ympäristössä, Platform-as-a-Service), joka puolestaan voi olla toteutettu IaaS-infrastruktuurissa. Koska pilvipalvelujen käyttämiseen ja hallintaan tarvitaan näiden peräkkäisten kerrosten välisiä liittymiä, IaaS-ongelma voi olla kriittisempi kuin PaaS- tai SaaS-ongelma. Julkiset pilvipalvelut ovat lisäksi periaatteessa kenen tahansa asiakkaan käytettävissä. Siksi julkinen pilvi on kriittisempi kuin yksityinen pilvi, kuten ISO17789:2014-standardin kohdassa 8.5.12.4 (Implications of cloud deployment models) todetaan. Näin pilvipalvelujen velvoitteita tulisi soveltaa verkko- ja tietoturvadirektiivin tavoitteiden mukaisesti ainoastaan julkisiin IaaS-pilvipalveluihin.

Tietoturvavaatimuksia ja tapahtumailmoituksia koskevissa velvoitteissa tulisi ottaa huomioon sekä IaaS-pilvipalvelujen että julkisten pilvipalvelujen aiheuttamat kriittisyyteen liittyvät seuraamukset, jotta Suomen resurssit voidaan kohdistaa järkevästi ja pilvipalvelujen riskienhallintaan pystytään tarttumaan tehokkaasti.

## Keskeisten palvelujen tarjoajat

Kansalliseen täytäntöönpanoon on sisällytettävä verkko- ja tietoturvadirektiivissä keskeiset kyberturvallisuuteen liittyvät toiminnalliset järjestelyt, joissa noudatetaan riskiperusteista ja tuloskeskeistä lähestymistapaa. Näin edistetään järjestelmien kyberturvallisuutta ja vakautta koko Euroopan unionissa. Tietoturvan vankka perustaso on kyberriskien tehokkaan hallintaympäristön tärkeä osatekijä niin julkisella kuin yksityiselläkin sektorilla. Tässä viitekehyksessä Microsoft suosittelee, että keskeisten palvelujen tarjoajat kehittävät riskienhallinnan standardointiprosessit sekä valvontatyökalut, joilla varmistetaan tietoturvan asianmukaiset perustasot. Lisäksi on suositeltavaa ottaa huomioon nykyiset kansainväliset parhaat käytännöt, esimerkiksi Yhdysvaltojen kansallisen standardoimisviraston (NIST) suositukset kyberturvallisuuden kehittämisestä (Framework for Improving Critical Infrastructure Cybersecurity).

Yhdenmukaistaminen on välttämätöntä myös kriittisten infrastruktuurien määrittelyssä. Kansallisessa täytäntöönpanossa on noudatettava lähestymistapaa, jonka perusteena on yksilöidä keskeisten palvelujen tarjoajien eri luokkien kriittiset infrastruktuurit verkko- ja tietoturvadirektiivissä määritetyllä tavalla. Näin noudatetaan direktiivillä suojeltua yhdenmukaisuuden soveltamisalaa. Samalla myös resurssien kanavointi keskeisessä infrastruktuurissa tehostuu. Verkko- ja tietoturvadirektiivin tehokas kansallinen täytäntöönpano edellyttää tietoturvan perustasojen yhdenmukaistamista koko EU:ssa, jotta vältytään soveltamisalan päällekkäisyyksiltä jäsenvaltioissa.

## Yhdenmukaistaminen jäsenvaltioissa sekä julkisen ja yksityisen sektorin yhteistyö

Kyberturvallisuuteen liittyvän yhteistyön ja tiedonvaihdon tehostaminen EU:n jäsenvaltioiden kesken on erittäin tärkeää, jotta tietojärjestelmien kyberturvallisuus ja vakaus paranevat koko Euroopan unionissa. Siksi Microsoft esittää, että kansalliset toimivaltaiset viranomaiset tekisivät yhteistyötä muissa jäsenvaltioissa olevien kollegoidensa sekä toimialan asiaankuuluvien toimijoiden kanssa. Kyberturvallisuus on monialainen kysymys, ja etenkin teknologiateollisuus on kyberuhkissa sekä kohde että ensimmäinen reagoija.

Kansallisten toimivaltaisten viranomaisten vapaaehtoista yhteistyötä ja tiedonvaihtoa on tehostettava ja tuettava. Vuoropuhelu ja keskinäinen luottamus eivät kuitenkaan vaikuta direktiivillä suojeltuun alueelliseen vastuullisuuteen digitaalisten palvelujen tarjoajia kohtaan. Alueellinen vastuu on toisin sanoen vain digitaalisten palvelujen tarjoajan päätoimipaikan mukaisella jäsenvaltion kansallisella toimivaltaisella viranomaisella. Siksi tapahtumiin liittyvää ilmoitusvelvollisuutta ei pidä yhdistää vapaaehtoiseen yhteistyöhän ja tiedonvaihtoon.

## Yhteenveto

Strategisen merkittävyytensä ansiosta verkko- ja tietoturvadirektiivi on tärkeä keino parantaa yleistä verkko- ja tietoturvallisuutta sekä Suomessa että koko EU:ssa. Verkko- ja tietoturvadirektiivin selkeä ja yhdenmukainen kansallinen täytäntöönpano on yhdistetyn sääntelyjärjestelmän peruspilari. Siksi asiaan on suhtauduttava positiivisesti, julkisten instituutioiden ja yksityisen sektorin vuoropuhelua tukien. Näin vältetään päällekkäinen sääntely sekä varmistetaan tehokas ja yhdenmukainen toimintaympäristö.