Euroopan unionin neuvosto

Bryssel, 18. joulukuuta 2020
(OR. en)

14150/20
ADD 3

Toimielinten välinen asia:
2020/0359(COD)

CYBER 281
JAI 1119
DATAPROTECT 155
TELECOM 270
MI 581
CSC 368
CSCI 97

SAATE

Lähettäjä:	Euroopan komission pääsihteeri, allekirjoittajana johtaja Martine DEPREZ
Saapunut:	16. joulukuuta 2020
Vastaanottaja:	Jeppe TRANHOLM-MIKKELSEN, Euroopan unionin neuvoston pääsihteeri
Kom:n asiak. nro:	SWD(2020) 344 final
Asia:	KOMISSION YKSIKÖIDEN VALMISTELUASIAKIRJA TIIVISTELMÄ VAIKUTUSTENARVIOINNISTA Oheisasiakirja ehdotukseen EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVIKSI toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoamisesta

Valtuuskunnille toimitetaan oheisena asiakirja SWD(2020) 344 final.

Liite: SWD(2020) 344 final

EUROOPAN
KOMISSIO

Bryssel 16.12.2020
SWD(2020) 344 final

KOMISSION YKSIKÖIDEN VALMISTELUASIAKIRJA

TIIVISTELMÄ VAIKUTUSTENARVIOINNISTA

Oheisasiakirja

ehdotukseen

EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVIKSI

toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoamisesta

{COM(2020) 823 final} - {SEC(2020) 430 final} - {SWD(2020) 345 final}

Tiivistelmä

Toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa 6 päivänä heinäkuuta 2016 annetun direktiivin (EU) 2016/1148, jäljempänä ’NIS-direktiivi’ uudelleentarkasteluun liittyvä vaikutustenarviointi.

A. Toiminnan tarpeellisuus

Mikä on ongelmana ja miksi se on ongelma EU:n tasolla?

NIS-direktiivi, josta on toki ollut paljon hyötyä, kun se johti merkittävään muutokseen suhtautumisessa institutionaaliseen ja sääntelyajatteluun kyberturvakysymyksissä monissa EU-maissa, on myös osoittautunut monissa kohdin puutteelliseksi. Yhteiskuntien digitalisaatio (jota covid-19-kriisi edelleen on vahvistanut) on laajentanut tilannekuvaa uhkista ja luo uusia haasteita, jotka vaativat tarkemmin suunnattuja ja entistä innovatiivisempia puolustuskeinoja. Kyberhyökkäykset lisääntyvät. Ne ovat entistä sofistikoituneempia ja tulevat hyvin monista lähteistä sekä EU:n sisältä että sen ulkopuolelta.

NIS-direktiivin toimivuuden selvityksen perusteella vaikutustenarvioinnissa todettiin seuraavat ongelmat: EU:ssa toimivien yritysten heikko kyberuhkien sietokyky, erot häiriönsietokyvyssä jäsenvaltioiden ja toimialojen välillä ja heikko yhteinen tilannetietoisuus ja kyky yhteiseen reagointiin. Jotkin näistä ongelmista ja tekijöistä ovat johtaneet esimerkiksi tilanteeseen, jossa jossain EU-maassa tietyt suuret sairaalat eivät kuulu NIS-direktiivin soveltamisalaan eikä niiltä siten edellytetä direktiivin mukaisia turvatoimia, kun taas toisessa EU-maassa lähes joka ikinen sairaala kuuluu direktiivin tietoturvavaatimusten piiriin.

Mitä on tarkoitus saada aikaan?

NIS-direktiivin tarkistuksella pyritään kolmeen yleistavoitteeseen:

1. **Parannetaan kattavasti kaikilla asiaan liittyvillä toimialoilla Euroopan unionissa toimivien yritysten kykyä torjua kyberuhkia** ottamalla käyttöön säännöt, joilla varmistetaan, että kaikilta talouden ja koko yhteiskunnan kannalta tärkeitä toimintoja hoitavilta sisämarkkinoilla toimivilta julkisilta ja yksityisiltä toimijoilta edellytetään asianmukaisia kyberturvatoimia.
2. **Vähennetään epäjohdonmukaisuuksia häiriönsietokyvyssä sisämarkkinoilla direktiivin jo kattamilla toimialoilla** edelleen yhdenmukaistamalla 1) tosiasiallista soveltamisalaa, 2) turvallisuus- ja poikkeamaraportointivaatimuksia, 3) kansallisen tason valvontaa ja täytäntöönpanoa koskevia säännöksiä ja 4) jäsenvaltioiden toimivaltaisten viranomaisten valmiuksia.
3. **Parannetaan yhteistä tilannekuvaa ja yhteisiä valmiuksia valmistautua ja reagoida** lisäämällä luottamusta toimivaltaisten viranomaisten välillä, jakamalla enemmän tietoa ja laatimalla säännöt ja menettelyt laajamittaisten poikkeamien tai kriisien varalta.

Mitä lisäarvoa saadaan toimimisesta EU:n tasolla (toissijaisuusperiaate)?

Kyberturvallisuustoiminta unionissa ei voi olla tuloksellista, jos asiaa lähestytään hajanaisesti kansallisten tai alueellisten siilojen näkökulmasta. NIS-direktiivillä haluttiin korjata tätä puutetta luomalla puitteet verkkojen ja tietojärjestelmien tietoturvalle kansallisella ja unionitasolla. Sen täytäntöönpano ja toteutus paljasti kuitenkin myös tiettyjen säännösten ja lähestymistapojen sisälähtöisiä heikkouksia. Tällainen on esimerkiksi direktiivin soveltamisalan epäselvä rajaus. Lisäksi Euroopan taloudesta on covid-19-kriisin myötä tullut riippuvaisempi verkoista ja tietojärjestelmistä, ja eri toimialat ja palvelut ovat enenevässä määrin sidoksissa toisiinsa. Tässä tilanteessa NIS-direktiivin ensimmäinen säännönmukainen

uudelleentarkastelu loi tilaisuuden EU-tason lisätoimille. Nykyistä NIS-direktiiviä vahvempi EU-tason sääntely on perusteltavissa erityisesti seuraavilla seikoilla: i) ongelma on luonteeltaan maiden rajat ylittävä ii) EU-tason toimilla voidaan parantaa ja helpottaa tuloksellista toimintaa kansallisella tasolla ja iii) yhtenäisellä ja yhteistyöhön perustuvalla verkko- ja tietoturvatoiminnalla voidaan tuloksellisesti tukea tietosuojaa ja yksityisyyden suojaa.

B. Ratkaisut

Millä vaihtoehdoilla tavoitteet saavutettaisiin? Onko jokin vaihtoehto arvioitu parhaaksi? Ellei, miksi?

Vaikutustenarvioinnissa analysointiin neljä toimintavaihtoehtoa: 0) nykytilanteen säilyttäminen 1) kansallisen soveltamisen yhdenmukaistaminen muutoin kuin lainsäädännöllisin toimin 2) NIS-direktiivin vähäiset muutokset soveltamisen yhdenmukaistamiseksi 3) systeemiset ja rakenteelliset muutokset NIS-direktiiviin. Vaihtoehto 1 hylättiin jo varhaisessa vaiheessa, koska se ei juurikaan poikkea nykytilanteen säilyttämisestä. Vaikutustenarvioinnissa **parhaaksi** valitaan vaihtoehto 3 (**systeemiset ja rakenteelliset muutokset NIS-puitteisiin**), koska sillä pyritään perusteellisempaan muutokseen niin, että katetaan laajempi osa taloudesta koko unionissa, ja kohdennetummalla valvonnalla keskitytään oikeassa suhteessa suuriin ja avainasemassa oleviin yrityksiin ja kyetään selkeästi määrittelemään direktiivin soveltamisala. Se myös sujuvoittaisi ja edelleen yhdenmukaistaisi yritysten tietoturvavelvoitteita, loisi operatiiviselle tasolle tuloksellisemmat puitteet sekä muodostaisi selkeän perustan eri osapuolten yhteisvastuulle ja vastuuvelvollisuuksille ja kannustaisi tiedonvaihtoon.

Mitkä ovat sidosryhmien näkemykset? Mitkä toimijat kannattavat mitäkin vaihtoehtoa?

Enemmistö toimivaltaisista viranomaisista ja yrityksistä antoi tukensa NIS-direktiivin tarkistamiselle. Useissa kuulemisissa ne antoivat ymmärtää, että tarkistetun NIS-direktiivin olisi katettava uusia toimialoja ja alasektoreita, ja sillä olisi yhdenmukaistettava tai sujuvoitettava edelleen tietoturvatoimenpiteitä ja raportointivelvollisuuksia. Sidosryhmien taholta tuli tukea myös uusille toimintamalleille, joita oli ainoastaan valitussa vaihtoehdossa (esim. tarjontaketjulähtöinen turvallisuuspolitiikka, EU:n operatiivisen kriisinhallintamallin institutionalisointi).

C. Parhaaksi arvioidun vaihtoehdon vaikutukset

Mitkä ovat parhaaksi arvioidun vaihtoehdon hyödyt (jos parhaaksi arvioitua vaihtoehtoa ei ole, päävaihtoehtojen hyödyt)?

Parhaaksi arvioitu vaihtoehto toisi merkittäviä hyötyjä: NIS-direktiivin uudelleentarkastelun tueksi tehdyssä selvityksessä kehitetyn taloudellisen mallinnuksen arvioiden mukaan parhaaksi katsottu vaihtoehto voisi alentaa kyberturvapoikkeamista aiheutuvia kustannuksia 11,3 miljardilla eurolla.

NIS-kehyksen kattamia toimialoja tulisi huomattavasti lisää, mutta edellä mainittujen hyötyjen lisäksi NIS-vaatimuksista erityisesti valvontanäkökulmasta mahdollisesti aiheutuva rasite myös tasapainottuisi sekä soveltamisalan piiriin tulevien uusien toimijoiden että toimivaltaisten viranomaisten osalta. Tämä perustuisi siihen, että uudessa NIS-kehyksessä noudatettaisiin kaksitasoista lähestymistapaa, jossa keskityttäisiin suuriin avaintoimijoihin, sekä eriytettyä valvontajärjestelmää, jossa sallittaisiin ainoastaan jälkikäteisvalvonta (eli reaktiivinen valvonta ilman yleistä sääntöjenmukaisuuden systemaattista dokumentointivelvoitetta) hyvin monien toimijoiden osalta ja varsinkin ’tärkeiksi’ mutta ei ’keskeisiksi’ katsottujen toimijoiden osalta.

Kokonaisuudessaan voidaan todeta, että parhaaksi arvioitu vaihtoehto johtaisi tehokkaisiin kompromisseihin ja synergioihin ja tarjoaisi kaikista analysoiduista toimintavaihtoehdoista parhaat

mahdollisuudet varmistaa, että keskeisten toimijoiden kyky sietää kyberturvallisuusuhkia paranisi ja olisi yhdenmukainen kaikkialla unionissa, mikä johtaisi lopulta kustannussäästöihin sekä yrityksille että yhteiskunnalle.

Mitkä ovat parhaaksi arvioidun vaihtoehdon kustannukset (jos parhaaksi arvioitua vaihtoehtoa ei ole, päävaihtoehtojen kustannukset)?

Parhaaksi arvioitu vaihtoehto aiheuttaisi jäsenvaltioiden viranomaisille tiettyjä vaatimustenmukaisuuden varmistamiseen ja valvontaan liittyviä kustannuksia (resurssitarpeen kokonaiskasvuksi arvioitiin 20–30 %). Toisaalta uusi kehys toisi myös huomattavia hyötyjä, kun kokonaiskuva avainyrityksistä ja yhteydenpito niiden kanssa paranisi, EU-maiden välinen operatiivinen yhteistyö tehostuisi ja käyttöön saataisiin keskinäisen avunannon ja vertaisarvioinnin mekanismeja. Tämä parantaisi kyberturvan kokonaisvalmiuksia jäsenvaltioissa.

Uuden NIS-kehyksen soveltamisalaan tulevien yritysten osalta arvioidaan, että niiden olisi kasvatettava nykyisiä tieto- ja viestintätekniikan turvallisuuteen liittyviä menojaan enintään 22 % NIS-kehyksen ensimmäisinä vuosina (jo nykyisen NIS-direktiivin soveltamisalaan kuuluvien yritysten osalta luku olisi 12 %). Tämä keskimääräinen kulujen kasvu tuottaisi myös kohtuullisen tuoton näille investoinneille, varsinkin kun kyberturvapoikkeamien kustannukset laskisivat merkittävästi (arviolta 11,3 miljardia euroa kymmenen vuoden aikana).

Mitkä ovat vaikutukset pk-yrityksiin ja kilpailukykyyn?

Parhaaksi arvioidussa vaihtoehdossa NIS-kehystä ei sovellettaisi pien- ja mikroyrityksiin. Keskisuurten yritysten osalta voidaan olettaa, että tieto- ja viestintätekniikan turvallisuuteen liittyvät kulut kasvaisivat uuden NIS-kehyksen ensimmäisinä vuosina Samalla tietoturvavaatimusten tiukentaminen tällaisten toimijoiden osalta loisi niille kannustimia parantaa kyberturvavalmiuksiaan ja auttaisi parantamaan niiden tieto- ja viestintäteknisten riskien hallintaa.

Kohdistuuko jäsenvaltioiden budjettiin ja julkishallintoon merkittäviä vaikutuksia?

Jäsenvaltioiden budjettiin ja julkishallintoon kohdistuisi vaikutuksia: lyhyellä ja keskipitkällä aikavälillä lisäresurssitarpeeksi arvioidaan 20–30 %.

Onko toimenpiteellä muita merkittäviä vaikutuksia?

Muita merkittäviä negatiivisia vaikutuksia ei odoteta olevan. Parhaaksi katsotun vaihtoehdon oletetaan johtavan parempiin kyberturvavalmiuksiin, joten tätä kautta se vähentäisi merkittävämmin poikkeamien, myös tietoturvaloukkausten, määrää ja vakavuutta. Se auttaa myös todennäköisesti turvaamaan NIS-kehyksen piiriin kuuluvien toimijoiden tasavertaiset toimintaedellytykset eri jäsenvaltioissa ja vähentämään epäsuhtia kyberturvatiedon saatavuudessa.

Suhteellisuusperiaate

Parhaaksi arvioitu vaihtoehto ei ylitä sitä, mikä on tarpeen sen erityistavoitteiden saavuttamiseksi tyydyttävällä tavalla. Kaavaillut turvatoimien ja raportointivelvoitteiden yhdenmukaistamis- ja sujuvoittamistoimet perustuvat EU-maiden ja yritysten pyyntöihin parantaa nykyjärjestelmää.

D. Seuranta

Milloin asiaa tarkastellaan uudelleen?

Ensimmäinen uudelleentarkastelu suoritettaisiin 54 kuukauden kuluttua säädöksen voimaantulosta. Komissio laatisi uudelleentarkastelusta raportin Euroopan parlamentille ja neuvostolle. Uudelleentarkastelu suoritettaisiin ENISAn ja yhteistyöryhmän tuella.