



EUROOPAN PARLAMENTTI

2009 - 2014

Teollisuus-, tutkimus- ja energiavaliokunta

2013/0027(COD)

19.12.2013

LAUSUNTO

teollisuus-, tutkimus- ja energiavaliokunnalta

sisämarkkina- ja kuluttajansuojavaliokunnalle

ehdotuksesta Euroopan parlamentin ja neuvoston direktiiviksi toimenpiteistä yhteisen korkeatasoisen verkko- ja tietoturvan varmistamiseksi koko unionissa (COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

Valmistelija(*): Pilar del Castillo Vera

(*) Valiokuntien yhteistyömenettely – työjärjestyksen 50 artikla

PA_Legam

LYHYET PERUSTELUT

Komissio antoi helmikuussa 2013 (Euroopan parlamentin Euroopan digitaalistrategiasta laatimassa valiokunta-aloitteisessa mietinnössä esitetyn pyynnön mukaisesti) ehdotuksen direktiiviksi toimenpiteistä yhteisen korkeatasoisen verkko- ja tietoturvan varmistamiseksi koko unionissa sekä ehdotuksen EU:n ensimmäiseksi verkkoturvallisuusstrategiaksi. Valmistelija suhtautuu hyvin myönteisesti ehdotukseen, pitäen mielessä, että saatavilla olevien tietojen tarkastelun perusteella voidaan arvioida, että tietotekniikkaan liittyvät vahingonteot voivat aiheuttaa yksinomaan pk-yrityksille suoraan yli 560 miljoonan euron suuruiset kulut vuosittain ja että erilaiset onnettomuudet (kuten tuotannon alkupään ympäristöongelmat tai luonnonkatastrofien kaltaiset fyysiset ongelmat) voivat aiheuttaa yli 2,3 miljardin euron suuruiset välittömät kustannukset.

Mitä tulee turvan rakenteeseen, valmistelija pitää kannatettavina useita ehdotetuista toimenpiteistä, kuten turvapoikkeamien raportointia koskevien säännösten laajentamista niin, että koskevat nykyisten vuoden 2009 puitedirektiivin 13 a artiklassa tarkoitettujen televiestintäpalveluiden tarjoajien ohella myös muita keskeisen infrastruktuurin aloja. Näin ollen ehdotukset – kuten sen vaatiminen, että kaikilla jäsenvaltioilla on oltava asianmukaisesti toimivia tietotekniikan kriisiryhmiä ja että niiden on nimettävä toimivaltainen viranomainen, joka on osa suojattua yleiseurooppalaista sähköistä tiedonjakoverkkoa, joka mahdollistaa verkkoturvallisuuteen liittyvien tietojen turvallisen jakamisen ja vaihtamisen – saavat myönteisen vastaanoton, ja niillä voidaan myötävaikuttaa merkittävästi direktiiviehdotuksen tavoitteen saavuttamiseen, eli verkko- ja tietoturvan yhteisen korkean tason varmistamiseen unionissa.

Valmistelija katsoo kuitenkin, että ehdotusta on mahdollista vielä parantaa, jos sitä tarkastellaan kahden peruseräteen, tehokkuuden ja luottamuksen prisman läpi.

Ensimmäinen periaate: tehokkuus

Ehdotuksessa asetetaan jäsenvaltioille velvoite nimetä toimivaltainen viranomainen, joka vastaa direktiivin soveltamisen valvomisesta ehdotuksen liitteessä II tarkoitetuilla aloilla, ja valmistelija katsoo tältä osin, että sen lisäksi, että kunkin jäsenvaltion on oltava vapaa valitsemaan tarkoituksenmukaisimmaksi katsomansa malli verkkoturvallisuuden hallinnointiin, on myös olennaisen tärkeää, että vältetään päällekkäiset institutionaaliset rakenteet, jotka voivat aiheuttaa toimivaltakiistoja ja häiritä yhteyksiä. Valmistelija katsoo siksi, että ei pitäisi kajota jo olemassa oleviin kansallisiin rakenteisiin, jotka toimivat tehokkaasti ja vastaavat asianomaisen jäsenvaltion tarpeita ja perustuslaillisia edellytyksiä. Valmistelija on kuitenkin sitä mieltä, että unionin tasolla tapahtuvan tietojenvaihdon, uhista varhaisessa vaiheessa varoittamisen ja yhteistyöverkostoon tehokkaasti osallistumisen varmistamiseksi kunkin jäsenvaltion on nimettävä keskitetty yhteyspiste.

Valmistelija katsoo samassa direktiiviehdotuksen tehokkuuden enimmäistämisen hengessä, että kansallisen tietotekniikan kriisiryhmän (CERT) perustamista koskevat toimenpide-ehdotukset eivät ehkä osoittaudu asianmukaisiksi vaatimuksiksi, kun otetaan huomioon, että niissä jätetään nykyisten CERT-ryhmien erilaiset luonteet ja kokoonpanot huomiotta. Sen lisäksi, että useimmilla jäsenvaltioilla on enemmän kuin yksi CERT-ryhmä, ne myös

käsitlevät erilaisia poikkeamia. Ryhmien toiminnan määrä ja tyyppi vaihtelee myös sen mukaan, toimivatko ne akateemisten tai tutkimuslaitosten, julkishallinnon vai yksityisen sektorin puitteissa ja johtamina. Käsiteltävänä oleva ehdotus rikkoisi myös nykyiset kansainväliset ja eurooppalaiset yhteistyöverkostot, joihin nykyiset CERT-ryhmät kuuluvat ja jotka ovat osoittautuneet tehokkaiksi turvapoikkeamia koskevien kansainvälisten ja eurooppalaisten vastatoimien koordinoimisessa. Valmistelija katsoo näin ollen, että sen sijaan, että direktiivissä säädetään yhdestä ainoasta kansallisesta CERT-ryhmästä, se olisi kohdistettava niihin CERT-ryhmiin, jotka tarjoavat palvelujaan liitteessä II tarkoitetuille aloilla, jolloin olisi esimerkiksi mahdollista, että yksi CERT-ryhmä palvelee kaikkia liitteessä II tarkoitettuja aloja tai useat CERT-ryhmät tarjoavat palveluja samalla alalla. Valmistelija katsoo kuitenkin, että jäsenvaltioiden on varmistettava CERT-ryhmiensä täysi toimintavalmius kaikkina aikoina ja huolehdittava, että ryhmillä on riittävät tekniset, taloudelliset ja inhimilliset resurssit voidakseen toimia asianmukaisesti ja osallistua kansainvälisiin ja unionin tason yhteistyöverkostoihin.

Tehokkuusperiaatteen soveltaminen edellyttää muutoksia myös direktiiviehdotuksen soveltamisalaan. Vaikka valmistelija on yhtä mieltä siitä, että raportointijärjestelmän velvoitteita on laajennettava niin, että ne koskevat myös energia-, liikenne-, terveys- ja rahoitusala, ehdotus ulottaa luvussa IV tarkoitettujen pakollisten toimenpiteiden Internet-talouden kaikkiin markkinatoimijoihin on kohtuuton ja mahdoton toteuttaa. Ehdotus on kohtuuton, koska uusien velvoitteiden summittainen määrääminen ”sellaisten tietoyhteiskunnan palvelujen tarjoajan, jotka mahdollistavat muiden tietoyhteiskunnan palvelujen tarjoamisen” kaltaiselle avoimelle ja määrittelemättömälle ryhmälle on paitsi käsittämätöntä myös riittämättömästi perusteltua, kun otetaan huomioon turvallisuuspoikkeamasta mahdollisesti aiheutuvan vahingon laajuus, ja koska se mahdollisesti lisää entisestään byrokratiasta teollisuudelle ja ennen muuta pk-yrityksille koituvaa rasitusta. Ehdotus on lisäksi mahdoton toteuttaa, sillä on syytä epäillä vakavasti, kykenevätkö toimivaltaiset viranomaiset käsittelemään kaikki mahdolliset ilmoitukset ennakoivasti tavalla, joka kannustaa kaksisuuntaiseen vuoropuheluun markkinatoimijoiden kanssa turvallisuusuhnan torjumiseksi.

Julkishallintojen osalta direktiivissä olisi löydettävä tasapaino yhtäältä tarpeen kehittää edelleen sähköisen hallinnon palveluja ja toisaalta julkishallinnoille jo asetettujen, niiden verkkojen ja tietojärjestelmien hallinnointia ja suojelua koskevien riittävän huolellisuuden velvoitteiden välillä. Valmistelija katsoo siksi, että vaikka 14 artiklassa vahvistettuja tietovaihtovaatimuksia olisi sovellettava täysimääräisesti julkishallintoihin, niille ei pitäisi asettaa 15 artiklassa tarkoitettuja velvoitteita.

Toinen periaate: luottamus

Valmistelijan mielestä suuri osa direktiivin onnistumisesta perustuu siihen, että sillä kyetään kannustamaan markkinatoimijoita osallistumaan, mikä johtaa siihen, että muodostuu luotettava verkko- ja tietoturva-ympäristö, jossa käytännön tason toimijat ovat halukkaita osallistumaan ennakoivasti. Mikäli direktiivillä ei päästä tähän, se on epäonnistunut. Valmistelija ehdottaa tältä osin sen varmistamista, että markkinatoimijoiden osallistumis- ja ilmoittamishalukkuutta ei heikennetä julkistamalla niiden ilmoittamat turvallisuuspoikkeamat tarpeettomasti tai säätämällä, että ne voidaan asettaa vastuuseen, mikäli toimivaltaiset viranomaiset tai keskitetyt yhteyspisteet menettävät tietoaan. Tämän lisäksi markkinatoimijoiden ja toimivaltaisten viranomaisten välinen kaksisuuntainen vuoropuhelu

on pidettävä avoinna ja markkinatoimijoita on rohkaistava osallistumaan kaikkiin foorumeihin, myös yhteistyöverkoston.

Valmistelija katsoo myös, että toimivaltaisten viranomaisten ja/tai keskitettyjen yhteyspisteiden osallistumisen olisi perustuttava luottamukseen erityisesti tietojenvaihdon osalta. Tämän takaamiseksi olisi direktiivin sisällettävä verkon luottamuksellisuutta ja turvallisuutta koskevia säännöksiä.

TARKISTUKSET

Teollisuus-, tutkimus- ja energiavaliokunta pyytää asiasta vastaavaa sisämarkkina- ja kuluttajansuojavaliokuntaa ottamaan huomioon seuraavat tarkistukset:

Tarkistus 1

Ehdotus direktiiviksi Johdanto-osan 1 kappale

Komission teksti

(1) Verkko- ja tietojärjestelmillä ja -palveluilla on elintärkeä tehtävä yhteiskunnassa. Niiden luotettavuus ja turvallisuus ovat olennaisen tärkeitä talouden toiminnalle ja sosiaaliselle hyvinvoinnille ja erityisesti sisämarkkinoiden toiminnalle.

Tarkistus

(1) Verkko- ja tietojärjestelmillä ja -palveluilla on elintärkeä tehtävä yhteiskunnassa. Niiden luotettavuus ja turvallisuus ovat olennaisen tärkeitä **EU:n kansalaisten vapaudelle ja kokonaisvaltaiselle turvallisuudelle sekä** talouden toiminnalle ja sosiaaliselle hyvinvoinnille ja erityisesti sisämarkkinoiden toiminnalle.

Tarkistus 2

Ehdotus direktiiviksi Johdanto-osan 2 kappale

Komission teksti

(2) **Tahallisten tai tahattomien** turvapoikkeamien laajuus ja **esiintymistiheys** kasvavat ja muodostavat merkittävän uhan verkko- ja tietojärjestelmien toiminnalle. Tällaiset

Tarkistus

(2) Turvapoikkeamien laajuus, **esiintymistiheys** ja **vaikutukset** kasvavat ja muodostavat merkittävän uhan verkko- ja tietojärjestelmien toiminnalle. **Nämä järjestelmät voivat olla myös helppo kohde**

turvapoikkeamat voivat toimia esteenä taloudelliselle toiminnalle, tuottaa huomattavia taloudellisia tappioita, heikentää käyttäjien luottamusta ja aiheuttaa merkittävää vahinkoa unionin taloudelle.

tahallisille haitallisille toimenpiteille, joiden tarkoituksena on vahingoittaa tai häiritä järjestelmien toimintaa. Tällaiset turvapoikkeamat voivat *uhata ihmisten terveyttä ja turvallisuutta*, toimia esteenä taloudelliselle toiminnalle, tuottaa huomattavia taloudellisia tappioita, heikentää käyttäjien *ja sijoittajien* luottamusta ja aiheuttaa merkittävää vahinkoa unionin taloudelle.

Perustelu

Pörssiyhtiöihin tehdään usein tietoverkkohyökkäyksiä ja ne kattavat niin rahoitusvarojen tai teollis- ja tekijänoikeuksien varkaudet kuin asiakkaiden tai liikekumppaneiden toiminnan keskeytymisen, mikä saattaa vaikuttaa yhtiöiden suhteisiin osakkeenomistajiin samoin kuin mahdollisten sijoittajien päätöksentekoon.

Tarkistus 3

Ehdotus direktiiviksi Johdanto-osan 3 kappale

Komission teksti

(3) Digitaaliset tietojärjestelmät, ensisijaisesti internet, ovat rajat ylittäviä viestintävälineitä, jotka helpottavat olennaisesti tavaroiden, palvelujen ja ihmisten liikkumista rajojen yli. Tämän ylikansallisen luonteen vuoksi näiden järjestelmien merkittävä häiriö yhdessä jäsenvaltiossa voi vaikuttaa myös muihin jäsenvaltioihin ja koko EU:hun. Verkko- ja tietojärjestelmien sietokyky ja vakaus on sen vuoksi olennaisen tärkeää sisämarkkinoiden moitteettomalle toiminnalle.

Tarkistus

(3) Digitaaliset tietojärjestelmät, ensisijaisesti internet, ovat *perinteiset* rajat ylittäviä viestintävälineitä, jotka helpottavat olennaisesti tavaroiden, palvelujen, *ajatuksien* ja ihmisten liikkumista rajojen yli. Tämän ylikansallisen luonteen vuoksi näiden järjestelmien merkittävä häiriö yhdessä jäsenvaltiossa voi vaikuttaa myös muihin jäsenvaltioihin ja koko EU:hun. Verkko- ja tietojärjestelmien sietokyky ja vakaus on sen vuoksi olennaisen tärkeää sisämarkkinoiden *samoin kuin ulkoisten markkinoidenkin* moitteettomalle toiminnalle.

Perustelu

Sisämarkkinoiden verkko- ja tietojärjestelmien sietokyky ja vakaus ovat myös olennaisen tärkeässä asemassa, jotta on mahdollista toimia vuorovaikutuksessa esimerkiksi Pohjois-Amerikan tai Aasian kaltaisten maailmanlaajuisten ja alueellisten markkinoiden kanssa.

Tarkistus 4

Ehdotus direktiiviksi Johdanto-osan 4 kappale

Komission teksti

(4) Olisi otettava käyttöön unionin tason yhteistyömekanismi, joka mahdollistaa verkko- ja tietoturvaan liittyvän tiedonvaihdon sekä koordinoitun havaitsemisen ja reagoinnin. Jotta tämä mekanismi olisi tehokas ja kaikkien jäsenvaltioiden käytettävissä, on olennaisen tärkeää, että kaikilla jäsenvaltioilla on vähimmäisvalmiudet ja strategia, joilla varmistetaan korkeatasoinen verkko- ja tietoturva niiden alueella. Vähimmäistason turvallisuusvaatimuksia olisi sovellettava myös **julkishallintoihin ja elintärkeän tietoinfrastruktuurin** operaattoreihin, jotta voidaan edistää riskinhallintakulttuuria ja varmistaa raportointi vakavimmista turvapoikkeamista.

Tarkistus

(4) Olisi otettava käyttöön unionin tason yhteistyömekanismi, joka mahdollistaa verkko- ja tietoturvaan liittyvän tiedonvaihdon sekä koordinoitun **ennaltaehkäisyyn**, havaitsemisen ja reagoinnin. Jotta tämä mekanismi olisi tehokas ja kaikkien jäsenvaltioiden käytettävissä, on olennaisen tärkeää, että kaikilla jäsenvaltioilla on vähimmäisvalmiudet ja strategia, joilla varmistetaan korkeatasoinen verkko- ja tietoturva niiden alueella. Vähimmäistason turvallisuusvaatimuksia olisi sovellettava myös **tietoinfrastruktuurin julkisiin ja yksityisiin** operaattoreihin ja **pörssiyhtiöihin**, jotta voidaan edistää riskinhallintakulttuuria ja varmistaa raportointi vakavimmista turvapoikkeamista. **Oikeudellisen kehyksen olisi perustuttava tarpeeseen suojata kansalaisten yksityisyyttä ja koskemattomuutta. Elintärkeiden infrastruktuureiden varoitusjärjestelmää (CIWIN) olisi laajennettava kattamaan erityisesti nämä operaattorit.**

Perustelu

Pörssiyhtiöiden tietoturvaloukkaukset saattavat vaikuttaa olennaisesti yhtiön tuotteisiin, palveluihin, suhteisiin asiakkaisiin tai toimittajiin sekä kokonaisvaltaisiin kilpailuoloihin, minkä vuoksi sisämarkkinoiden (ja ulkoisten markkinoiden) toimintaan kohdistuvat seuraukset voivat olla merkittäviä. Tästä syystä direktiivillä olisi katettava myös pörssiyhtiöt.

Tarkistus 5

Ehdotus direktiiviksi Johdanto-osan 4 a kappale (uusi)

Komission teksti

Tarkistus

(4 a) Tässä direktiivissä olisi painotettava elintärkeitä infrastruktuureja, jotka ovat välttämättömiä keskeisten taloudellisten ja sosiaalisten toimintojen ylläpitämiseksi energia-, liikenne- ja pankkialalla sekä rahoitusmarkkinainfrastruktuurien ja terveydenhuollon alalla.

Tarkistus 6

Ehdotus direktiiviksi Johdanto-osan 4 b kappale (uusi)

Komission teksti

Tarkistus

(4 b) Sen varmistamiseksi, että hallinnonalat eivät ylitä toimivaltaansa tai käytä sitä väärin, on olennaisen tärkeää, että julkisten viranomaisten tieto- ja turvajärjestelmät ovat avoimia, legitiimejä, asianmukaisesti määriteltyjä ja että ne on hyväksytty avoimen demokraattisen prosessin välityksellä.

Tarkistus 7

Ehdotus direktiiviksi Johdanto-osan 6 kappale

Komission teksti

Tarkistus

(6) Nykyiset valmiudet eivät riitä varmistamaan korkeatasoista verkko- ja tietoturvaa unionissa. Jäsenvaltioiden valmiudet ovat tasoltaan hyvin erilaisia, mikä johtaa hajanaisiin lähestymistapoihin eri puolilla unionia. Tämä johtaa

(6) Nykyiset valmiudet eivät riitä varmistamaan korkeatasoista verkko- ja tietoturvaa unionissa. Jäsenvaltioiden valmiudet ovat tasoltaan hyvin erilaisia, mikä johtaa hajanaisiin lähestymistapoihin eri puolilla unionia. Tämä johtaa

epätasaiseen suojaan kuluttajille ja yrityksille ja heikentää yleistä verkko- ja tietoturvan tasoa unionissa.

Julkishallintoja ja markkinatoimijoita koskevien yhteisten vähimmäisvaatimusten puuttuminen puolestaan merkitsee sitä, ettei unionin tasolla ole mahdollista luoda kokonaisvaltaista ja tuloksellista yhteistyömekanismeja.

epätasaiseen suojaan kuluttajille ja yrityksille ja heikentää yleistä verkko- ja tietoturvan tasoa unionissa.

Markkinatoimijoita koskevien yhteisten vähimmäisvaatimusten puuttuminen puolestaan merkitsee sitä, ettei unionin tasolla ole mahdollista luoda kokonaisvaltaista ja tuloksellista yhteistyömekanismeja, **mikä heikentää lisäksi kansainvälisen yhteistyön tehokkuutta ja häittää siten yleismaailmallisten turvahaasteiden torjumista ja heikentää unionin kansainvälistä johtoasemaa avoimen, tehokkaan ja turvallisen internetin turvaamisen ja edistämisen alalla.**

Tarkistus 8

Ehdotus direktiiviksi Johdanto-osan 7 kappale

Komission teksti

(7) Tehokas reagointi verkko- ja tietojärjestelmien turvallisuuden asettamiin haasteisiin edellyttää sen vuoksi unionin tason kokonaisvaltaista lähestymistapaa, joka kattaa yhteisten vähimmäisvalmiuksien luomista ja suunnittelua koskevat vaatimukset, tiedonvaihdon ja toimien koordinoinnin sekä yhteiset vähimmäisturvavaatimukset **kaikille kyseeseen tuleville markkinatoimijoille ja julkishallinnoille.**

Tarkistus

(7) Tehokas reagointi verkko- ja tietojärjestelmien turvallisuuden asettamiin haasteisiin edellyttää sen vuoksi unionin tason kokonaisvaltaista lähestymistapaa, joka kattaa yhteisten vähimmäisvalmiuksien luomista ja suunnittelua koskevat vaatimukset, **riittävien tietoverkkoturvallisuutta koskevien taitojen kehittämisen, tiedonvaihdon ja toimien koordinoinnin sekä yhteiset vähimmäisturvavaatimukset. Turvallisuuteen liittyviä vähimmäisnormeja olisi sovellettava tietoverkkoturvallisuuden koordinoinnista vastaavien Cyber Security Co-Ordination Groups (CSGC) -ryhmien antamien asianmukaisten suosituksien mukaisesti.**

Tarkistus 9

Ehdotus direktiiviksi Johdanto-osan 9 kappale

Komission teksti

(9) Verkko- ja tietoturvan yhteisen korkean tason saavuttamiseksi ja ylläpitämiseksi kullakin jäsenvaltiolla olisi oltava kansallinen verkko- ja tietoturvastrategia, jossa määritellään strategiset tavoitteet ja toteutettavat konkreettiset toimet. Kansallisella tasolla on tarpeen kehittää olennaiset vaatimukset täyttäviä verkko- ja tietoturvan yhteistyösuunnitelmia, jotta saavutetaan valmiudet ja reagointikyky sellaisella tasolla, että voidaan toimia tuloksellisesti yhteistyössä kansallisella ja unionin tasolla turvapoikkeamien sattuessa.

Tarkistus

(9) Verkko- ja tietoturvan yhteisen korkean tason saavuttamiseksi ja ylläpitämiseksi kullakin jäsenvaltiolla olisi oltava kansallinen verkko- ja tietoturvastrategia, jossa määritellään strategiset tavoitteet ja toteutettavat konkreettiset toimet. Kansallisella tasolla on tarpeen kehittää olennaiset vaatimukset täyttäviä **ja tässä direktiivissä asetettuihin vähimmäisvaatimuksiin perustuvia** verkko- ja tietoturvan yhteistyösuunnitelmia, jotta saavutetaan valmiudet ja reagointikyky sellaisella tasolla, että voidaan toimia tuloksellisesti yhteistyössä kansallisella ja unionin tasolla turvapoikkeamien sattuessa. **Tästä syystä jokainen jäsenvaltio olisi velvoitettava täyttämään yhteiset normit, jotka koskevat tiedon muotoa sekä jaettavan ja arvioitavan tiedon vaihdettavuutta. Jäsenvaltiot voivat pyytää tukea Euroopan unionin verkko- ja tietoturvavirastolta (ENISA) kehittäessään kansallisia verkko- ja tietoturvastrategioitaan yhteistä verkko- ja tietoturvastrategiaa koskevan vähimmäistason suunnitelman perusteella.**

Perustelu

Asianomaiset sidosryhmät ovat jo tunnustaneet ENISAn aseman erittäin pätevänä osaamiskeskuksena ja luotettavana välineenä, jolla edistetään tietoverkkoturvallisuutta EU:ssa. Tästä syystä EU:n olisi vältettävä toimenpiteiden ja rakenteiden päällekkäisyyttä hyödyntämällä ENISAn osaamista ja edellytettävä, että ENISA tarjoaa neuvontapalveluja niille jäsenvaltioille, joissa ei ole verkko- ja tietoturvasta vastaavia elimiä ja asiantuntemusta, sekä esitettävä tällaista tukea koskeva pyyntö.

Tarkistus 10

Ehdotus direktiiviksi Johdanto-osan 10 kappale

Komission teksti

(10) Jotta tämän direktiivin nojalla annetut säännökset voitaisiin panna tehokkaasti täytäntöön, kunkin jäsenvaltion olisi perustettava tai yksilöitävä elin vastaamaan verkko- ja tietoturvakysymysten koordinoinnista ja toimimaan keskuspuolella yhteistyölle rajojen yli unionin tasolla. Näille elimille olisi annettava riittävät tekniset, taloudelliset ja inhimilliset voimavarat, jotta ne voivat toteuttaa tehokkaasti ja tuloksettaasti niille osoitetut tehtävät ja siten saavuttaa tämän direktiivin tavoitteet.

Tarkistus

(10) Jotta tämän direktiivin nojalla annetut säännökset voitaisiin panna tehokkaasti täytäntöön, kunkin jäsenvaltion olisi perustettava tai yksilöitävä elin vastaamaan verkko- ja tietoturvakysymysten koordinoinnista ja toimimaan **yhtenäisenä keskuspuolella sekä sisäiselle koordinoinnille että** yhteistyölle rajojen yli unionin tasolla. **Nämä yhtenäiset kansalliset yhteyspuolella olisi nimettävä siten, että jokainen jäsenvaltio voi nimetä useamman kuin yhden kansallisen toimivaltaisen viranomaisen, joka vastaa verkon tietoturvasta, jäsenvaltioiden perustuslakiin, oikeudenkäyttöön tai hallintoon perustuvien vaatimusten mukaisesti; yhteyspuolella olisi kuitenkin annettava koordinointia koskeva toimivalta kansallisesti ja unionissa.** Näille elimille olisi annettava riittävät tekniset, taloudelliset ja inhimilliset voimavarat, jotta ne voivat toteuttaa **jatkuvasti**, tehokkaasti ja tuloksettaasti niille osoitetut tehtävät ja siten saavuttaa tämän direktiivin tavoitteet.

Tarkistus 11

Ehdotus direktiiviksi Johdanto-osan 10 a kappale (uusi)

Komission teksti

Tarkistus

(10 a) Koska kansallisissa hallintotirakenteissa on eroja ja jotta taataan jo olemassa olevien alakohtaisten järjestelyjen säilyttäminen ja vältetään päällekkäisyyksiä, jäsenvaltioiden olisi voitava nimetä useampi kuin yksi kansallinen toimivaltainen viranomainen,

joka vastaa markkinatoimijoiden verkkojen ja tietojärjestelmien turvallisuuteen liittyvistä tehtävistä tämän direktiivin mukaisesti. Sujuvan rajat ylittävän yhteistyön ja viestinnän varmistamiseksi on kuitenkin välttämätöntä, että kukin jäsenvaltio nimeää vain yhden kansallisen yhteyspisteen, joka vastaa rajat ylittävästä yhteistyöstä unionin tasolla. Jäsenvaltion olisi voitava nimetä vain yksi toimivaltainen viranomainen hoitamaan toimivaltaisen viranomaisen ja yhteyspisteen tehtäviä, jos sen perustuslaillinen rakenne sitä edellyttää.

Tarkistus 12

Ehdotus direktiiviksi Johdanto-osan 11 kappale

Komission teksti

(11) Kaikilla jäsenvaltioilla olisi oltava käytössään riittävät sekä tekniset että organisatoriset valmiudet, jotta voidaan ehkäistä ja havaita verkko- ja tietojärjestelmien turvapoikkeamia ja -riskejä, reagoida niihin ja lieventää niiden vaikutuksia. Tämän vuoksi kaikkiin jäsenvaltioihin olisi perustettava hyvin toimivat ja olennaiset vaatimukset täyttävät tietotekniikan kriisiryhmät (CERT), jotta voidaan taata toimivat ja yhteensopivat valmiudet turvapoikkeamien ja -riskien varalta ja varmistaa tehokas yhteistyö unionin tasolla.

Tarkistus

(11) Kaikilla jäsenvaltioilla **ja markkinatoimijoilla** olisi oltava käytössään riittävät sekä tekniset että organisatoriset valmiudet, jotta voidaan **milloin tahansa** ehkäistä ja havaita verkko- ja tietojärjestelmien turvapoikkeamia ja -riskejä, reagoida niihin ja lieventää niiden vaikutuksia. **Julkishallinnon turvajärjestelmien on oltava turvallisia sekä demokraattisen valvonnan ja seurannan alaisia. Yleisesti edellytetyjen laitteistojen ja valmiuksien olisi oltava yhteisesti hyväksytyjen teknisten normien ja standardinmukaisten toimintamenettelyjen (standards procedures of operation, SPO) mukaisia.** Tämän vuoksi kaikkiin jäsenvaltioihin olisi perustettava hyvin toimivat ja olennaiset vaatimukset täyttävät tietotekniikan kriisiryhmät (CERT), jotta voidaan taata toimivat ja yhteensopivat valmiudet turvapoikkeamien ja -riskien varalta ja varmistaa tehokas yhteistyö unionin

tasolla. *Näille tietotekniikan kriisiryhmille olisi annettava valtuudet toteuttaa vastavuoroisia toimia yhteisten teknisten normien ja standardinmukaisten toimintamenettelyjen pohjalta. Jäsenvaltioiden olisi varmistettava, ottaen huomioon nykyisten CERT-ryhmien erilaiset ominaispiirteet, jotka vastaavat eri alojen ja toimijoiden tarpeita, että ainakin yksi CERT-ryhmä tarjoaa palveluja kullakin liitteessä II tarkoitetulla alalla. Jäsenvaltioiden olisi huolehdittava CERT-ryhmien rajat ylittävän yhteistyön osalta, että ryhmillä on riittävät resurssit voidakseen osallistua jo toiminnassa oleviin kansainvälisiin ja eurooppalaisiin yhteistyöverkostoihin.*

Perustelu

Yhteentoimivuus on taattava.

Tarkistus 13

Ehdotus direktiiviksi Johdanto-osan 12 kappale

Komission teksti

(12) Euroopan jäsenvaltiofoorumilla (EFMS) on viety merkittävästi eteenpäin keskustelua ja tiedonvaihtoa hyvistä toimintamalleista, myös kehitetty periaatteita eurooppalaiselle kyberkriisejä koskevalle yhteistyölle. Jäsenvaltioiden olisi tätä edistystä hyödyntäen muodostettava verkosto, jonka kautta ne voivat olla jatkuvasti yhteydessä toisiinsa ja tukea yhteistyötään. Tämän turvatun ja tuloksellisen yhteistyömekanismin olisi mahdollistettava jäsennetty ja koordinoitu tiedonvaihto, havaitseminen ja reagointi unionin tasolla.

Tarkistus

(12) Euroopan jäsenvaltiofoorumilla (EFMS) on viety merkittävästi eteenpäin keskustelua ja tiedonvaihtoa hyvistä toimintamalleista, myös kehitetty periaatteita eurooppalaiselle kyberkriisejä koskevalle yhteistyölle. Jäsenvaltioiden olisi tätä edistystä hyödyntäen muodostettava verkosto, jonka kautta ne voivat olla jatkuvasti yhteydessä toisiinsa ja tukea yhteistyötään. Tämän turvatun ja tuloksellisen yhteistyömekanismin, **jonka osalta markkinatoimijoiden osallistuminen on varmistettu**, olisi mahdollistettava jäsennetty ja koordinoitu tiedonvaihto, havaitseminen ja reagointi unionin tasolla.

Tarkistus 14

Ehdotus direktiiviksi Johdanto-osan 13 kappale

Komission teksti

(13) Euroopan verkko- ja tietoturvaviraston (ENISA) olisi avustettava jäsenvaltioita ja komissiota antamalla asiantuntemusta ja neuvontaa ja helpottamalla parhaiden käytäntöjen vaihtamista. Komission olisi erityisesti kuultava ENISAA tämän direktiivin soveltamisesta. Jotta voidaan varmistaa toimiva ja oikea-aikainen tiedonsaanti jäsenvaltioille ja komissiolle, yhteistyöverkostossa olisi annettava varhaisvaroitukset turvapoikkeamista ja -riskeistä. Jotta voidaan kehittää valmiuksia ja tietämystä jäsenvaltioiden välillä, yhteistyöverkoston avulla olisi myös levitettävä parhaita toimintatapoja, avustettava sen jäseniä valmiuksien kehittämisessä sekä ohjattava vertaisarviointien ja verkko- ja tietoturvarajoitusten organisointia.

Tarkistus

(13) Euroopan verkko- ja tietoturvaviraston (ENISA) olisi avustettava jäsenvaltioita ja komissiota antamalla asiantuntemusta ja neuvontaa ja helpottamalla parhaiden käytäntöjen vaihtamista. Komission **ja jäsenvaltioiden** olisi erityisesti kuultava ENISAA tämän direktiivin soveltamisesta. Jotta voidaan varmistaa toimiva ja oikea-aikainen tiedonsaanti jäsenvaltioille ja komissiolle, yhteistyöverkostossa olisi annettava varhaisvaroitukset turvapoikkeamista ja -riskeistä. Jotta voidaan kehittää valmiuksia ja tietämystä jäsenvaltioiden välillä, yhteistyöverkoston avulla olisi myös levitettävä parhaita toimintatapoja, avustettava sen jäseniä valmiuksien kehittämisessä sekä ohjattava vertaisarviointien ja verkko- ja tietoturvarajoitusten organisointia.

Tarkistus 15

Ehdotus direktiiviksi Johdanto-osan 14 kappale

Komission teksti

(14) Arkaluonteisten ja luottamuksellisten tietojen vaihtamiseksi verkostossa olisi otettava käyttöön suojattu tiedonjakoinfrastruktuuri. Rajoittamatta velvollisuutta ilmoittaa yhteistyöverkostolle unionin kannalta merkittävistä turvapoikkeamista ja -riskeistä pääsy muista jäsenvaltioista tuleviin luottamuksellisiin tietoihin olisi annettava jäsenvaltioille vain, jos ne voivat

Tarkistus

(14) Arkaluonteisten ja luottamuksellisten tietojen vaihtamiseksi verkostossa olisi **ENISAn valvonnassa** otettava käyttöön suojattu tiedonjakoinfrastruktuuri. Rajoittamatta velvollisuutta ilmoittaa yhteistyöverkostolle unionin kannalta merkittävistä turvapoikkeamista ja -riskeistä pääsy muista jäsenvaltioista tuleviin luottamuksellisiin tietoihin olisi annettava jäsenvaltioille vain, jos ne voivat

näyttää toteen, että niiden tekniset, taloudelliset ja inhimilliset voimavarat ja prosessit sekä niiden viestintäinfrastruktuuri takaavat, että ne voivat osallistua verkostoon tehokkaasti, tuloksekkaasti ja turvallisesti.

näyttää toteen, että niiden tekniset, taloudelliset ja inhimilliset voimavarat ja prosessit sekä niiden viestintäinfrastruktuuri takaavat, että ne voivat osallistua verkostoon tehokkaasti, tuloksekkaasti ja turvallisesti. ***Jotta yhteistyöverkosto voi hoitaa tehtävänsä tehokkaasti, komission olisi luotava sille oma budjettikohta.***

Tarkistus 16

Ehdotus direktiiviksi Johdanto-osan 14 a kappale (uusi)

Komission teksti

Tarkistus

(14 a) Markkinatoimijoita voidaan myös tarvittaessa kutsua osallistumaan yhteistyöverkoston toimintaan.

Tarkistus 17

Ehdotus direktiiviksi Johdanto-osan 15 kappale

Komission teksti

Tarkistus

(15) Koska useimmat verkko- ja tietojärjestelmät ovat yksityisten ylläpitämiä, julkisen ja yksityisen sektorin välinen yhteistyö on olennaisen tärkeää. Markkinatoimijoita olisi kannustettava kehittämään omia epävirallisia yhteistyömekanismejaan verkko- ja tietoturvan varmistamiseksi. Niiden olisi myös tehtävä yhteistyötä julkisen sektorin kanssa sekä jaettava tietoa ja parhaita toimintatapoja vastineeksi operatiivisesta tuesta ***turvapoikkeamien tapauksessa.***

(15) Koska useimmat verkko- ja tietojärjestelmät ovat yksityisten ylläpitämiä, julkisen ja yksityisen sektorin välinen yhteistyö on olennaisen tärkeää. Markkinatoimijoita olisi kannustettava kehittämään omia epävirallisia yhteistyömekanismejaan verkko- ja tietoturvan varmistamiseksi. Niiden olisi myös tehtävä yhteistyötä julkisen sektorin kanssa sekä jaettava ***turvapoikkeamien tapauksessa keskenään*** tietoa ja parhaita toimintatapoja vastineeksi ***asiaankuuluvasta tiedosta, operatiivisesta tuesta ja strategisesti analysoiduista tiedoista. Tiedon ja parhaiden toimintatapojen jakamisen tosiasialliseksi kannustamiseksi on olennaisen tärkeää***

varmistaa, että markkinatoimijat, jotka osallistuvat mainittuun vaihtoon, eivät joudu yhteistyön seurauksena epäsuotuisaan asemaan. On annettava asianmukaisia turvatakuita sen varmistamiseksi, että tällaisella yhteistyöllä ei altisteta mainittuja toimijoita suuremmille säännösten laiminlyöntiin liittyville riskeille tai uusille velvoitteille muun muassa kilpailua, teollis- ja tekijänoikeuksia, tietosuojaa tai tietoverkkorikollisuutta koskevan lainsäädännön nojalla eikä lisääntyneille toiminta- tai turvallisuusriskeille.

Tarkistus 18

Ehdotus direktiiviksi Johdanto-osan 16 kappale

Komission teksti

(16) Avoimuuden varmistamiseksi ja EU:n kansalaisten ja markkinatoimijoiden informoimiseksi asianmukaisesti **toimivaltaisten viranomaisten** olisi perustettava yhteinen verkkosivusto, jolla julkaistaan ei-luottamukselliset tiedot turvapoikkeamista ja **-riskeistä**.

Tarkistus

(16) Avoimuuden varmistamiseksi ja EU:n kansalaisten ja markkinatoimijoiden informoimiseksi asianmukaisesti **yhteispisteiden** olisi perustettava yhteinen **unionin laajuinen** verkkosivusto, jolla julkaistaan ei-luottamukselliset tiedot turvapoikkeamista, **riskeistä** ja **keinoista riskien lieventämiseksi sekä annetaan mahdollisesti asianmukaisia ylläpitotoimia koskevia neuvoja**.

Tarkistus 19

Ehdotus direktiiviksi Johdanto-osan 17 kappale

Komission teksti

(17) Jos tietoja pidetään luottamuksellisina liikesalaisuuksia koskevien unionin ja

Tarkistus

(17) **Johdanto-osan 14 kappaleessa tarkoitettun tietojen luokittelua koskevan**

kansallisten sääntöjen mukaisesti, tällainen luottamuksellisuus on varmistettava tässä direktiivissä vahvistettujen toimien ja tavoitteiden toteuttamisen yhteydessä.

politiikan olisi oltava ENISAn suosittelman tiedon jakamiseen sovellettavan Information Sharing Traffic Light Protocol -järjestelmän mukainen. Kaikki vaihdetut tiedot on luokiteltava ja niitä on käsiteltävä tietolähteen määrittämä arkaluonteisuuden taso huomioon ottaen. Jos tietoja pidetään luottamuksellisina liikesalaisuuksia koskevien unionin ja kansallisten sääntöjen mukaisesti, tällainen luottamuksellisuus on varmistettava tässä direktiivissä vahvistettujen toimien ja tavoitteiden toteuttamisen yhteydessä.

Tarkistus 20

Ehdotus direktiiviksi Johdanto-osan 18 kappale

Komission teksti

(18) Erityisesti kansallisten kriisinhallintakokemusten perusteella ja yhteistyössä ENISAn kanssa komission ja jäsenvaltioiden olisi luotava unionin verkko- ja tietoturvan yhteistyösuunnitelma, jossa määritellään yhteistyömekanismit turvariskien ja -poikkeamien torjumiseksi. Tämä suunnitelma olisi otettava asianmukaisesti huomioon varhaisvaroitusten tekemisessä yhteistyöverkostossa.

Tarkistus

(18) Erityisesti kansallisten kriisinhallintakokemusten perusteella ja yhteistyössä ENISAn kanssa komission ja jäsenvaltioiden olisi luotava unionin verkko- ja tietoturvan yhteistyösuunnitelma, jossa määritellään yhteistyömekanismit, ***parhaat käytännöt ja toimintamallit*** turvariskien ja -poikkeamien ***ennaltaehkäisemiseksi, havaitsemiseksi, torjumiseksi ja niistä ilmoittamiseksi.*** Tämä suunnitelma olisi otettava asianmukaisesti huomioon varhaisvaroitusten tekemisessä yhteistyöverkostossa.

Tarkistus 21

Ehdotus direktiiviksi Johdanto-osan 19 kappale

Komission teksti

(19) Verkostossa tehtävää varhaisvaroitusta

AD\1013266FI.doc

Tarkistus

(19) Verkostossa tehtävää varhaisvaroitusta

17/66

PE519.596v02-00

olisi edellytettävä ainoastaan silloin kun turvapoikkeaman tai -riskin laajuus ja vakavuus ovat niin merkittäviä tai niistä voi tulla niin merkittäviä, että niistä on tarpeen antaa tietoa tai niihin on tarpeen reagoida unionin tasolla.

Varhaisvaroitukset olisi sen vuoksi rajoitettava sellaisiin **todellisiin tai mahdollisiin** turvapoikkeamiin tai -riskeihin, jotka leviävät nopeasti, ylittävät kansallisen reagointivalmiuden tai vaikuttavat useampaan kuin yhteen jäsenvaltioon. Asianmukaisen arvioinnin mahdollistamiseksi yhteistyöverkostolle olisi ilmoitettava kaikki tiedot, joilla on merkitystä turvariskin tai -poikkeaman arvioinnin kannalta.

olisi edellytettävä ainoastaan silloin kun turvapoikkeaman tai -riskin laajuus ja vakavuus ovat niin merkittäviä tai niistä voi tulla niin merkittäviä, että niistä on tarpeen antaa tietoa tai niihin on tarpeen reagoida unionin tasolla.

Varhaisvaroitukset olisi sen vuoksi rajoitettava sellaisiin turvapoikkeamiin tai -riskeihin, jotka leviävät nopeasti, ylittävät kansallisen reagointivalmiuden tai vaikuttavat useampaan kuin yhteen jäsenvaltioon. Asianmukaisen arvioinnin mahdollistamiseksi yhteistyöverkostolle olisi ilmoitettava kaikki tiedot, joilla on merkitystä turvariskin tai -poikkeaman arvioinnin kannalta.

Tarkistus 22

Ehdotus direktiiviksi Johdanto-osan 20 kappale

Komission teksti

(20) Saatuaan varhaisvaroituksen ja sen arvioinnin **toimivaltaisten viranomaisten** olisi sovittava koordinoitua reagoinnista unionin verkko- ja tietoturvan yhteistyösuunnitelman mukaisesti. Sekä **toimivaltaisille viranomaisille** että komissiolle olisi ilmoitettava toimenpiteistä, jotka kansallisella tasolla on toteutettu koordinoitun reagoinnin tuloksena.

Tarkistus 23

Ehdotus direktiiviksi Johdanto-osan 22 kappale

Tarkistus

(20) Saatuaan varhaisvaroituksen ja sen arvioinnin **yhteyspisteiden** olisi sovittava koordinoitua reagoinnista unionin verkko- ja tietoturvan yhteistyösuunnitelman mukaisesti. Sekä **yhteyspisteille, ENISAlle** että komissiolle olisi ilmoitettava toimenpiteistä, jotka kansallisella tasolla on toteutettu koordinoitun reagoinnin tuloksena.

Komission teksti

(22) Vastuu verkko- ja tietoturvan varmistamisesta lankeaa paljolti julkishallinnoille ja markkinatoimijoille. **Riskinhallintakulttuuria**, johon sisältyy riskinarviointi ja riskeihin suhteutettujen turvatoimenpiteiden toteuttaminen, olisi edistettävä ja kehitettävä asianmukaisten sääntelyllisten vaatimusten ja toimialojen vapaaehtoisten käytäntöjen kautta. Tasavertaisten toimintaedellytysten luominen on myös olennaista yhteistyöverkoston tehokkaan toiminnan kannalta, jotta voidaan varmistaa tuloksellinen yhteistyö kaikkien jäsenvaltioiden taholta.

Tarkistus 24

**Ehdotus direktiiviksi
Johdanto-osan 24 kappale**

Komission teksti

(24) Nämä velvollisuudet olisi laajennettava sähköisen viestinnän sektorin ulkopuolelle teknisiä standardeja ja määräyksiä ja tietoyhteiskunnan palveluja koskevia määräyksiä koskevien tietojen toimittamisessa noudatettavasta menettelystä 22 päivänä kesäkuuta 1998 annetussa Euroopan parlamentin ja neuvoston direktiivissä 98/34/EY²⁷ määriteltyjen sellaisten tietoyhteiskunnan palvelujen keskeisiin tarjoajiin, jotka tukevat loppukäyttäjille suunnattuja tietoyhteiskunnan palveluja tai verkkotoimintoja, kuten sähköisen kaupankäynnin alustoja, internet-välitteisiä maksupalveluja, verkkoyhteisöpalveluja, hakukoneita, pilvipalveluja ja **sovelluskauppoja. Häiriöt näissä tietoyhteiskunnan mahdollistavissa palveluissa estävät tarjoamasta muita**

Tarkistus

(22) Vastuu verkko- ja tietoturvan varmistamisesta lankeaa paljolti julkishallinnoille ja markkinatoimijoille. **Riskinhallinnan, tiiviin yhteistyön ja luottamuksen kulttuuria**, johon sisältyy riskinarviointi ja riskeihin suhteutettujen turvatoimenpiteiden toteuttaminen, olisi edistettävä ja kehitettävä asianmukaisten sääntelyllisten vaatimusten ja toimialojen vapaaehtoisten käytäntöjen kautta. Tasavertaisten **ja luotettavien** toimintaedellytysten luominen on myös olennaista yhteistyöverkoston tehokkaan toiminnan kannalta, jotta voidaan varmistaa tuloksellinen yhteistyö kaikkien jäsenvaltioiden taholta.

Tarkistus

(24) Nämä velvollisuudet olisi laajennettava sähköisen viestinnän sektorin ulkopuolelle **infrastruktuurien operaattoreihin, sillä ne ovat vahvasti riippuvaisia tieto- ja viestintäteknologiasta ja olennaisia elintärkeiden talouden ja yhteiskunnan toimintojen, kuten sähkön ja kaasun jakelun, liikenteen, luottolaitosten, rahoitusmarkkinoiden infrastruktuurien ja terveydenhuollon, ylläpitämiselle. Häiriö näissä verkko- ja tietojärjestelmissä vaikuttaisi sisämarkkinoihin. Vaikka tässä direktiivissä asetetut velvollisuudet eivät koskekaan** teknisiä standardeja ja määräyksiä ja tietoyhteiskunnan palveluja koskevia määräyksiä koskevien tietojen toimittamisessa noudatettavasta menettelystä 22 päivänä kesäkuuta 1998 annetussa Euroopan parlamentin ja

tietoyhteiskunnan palveluja, jotka ovat niistä keskeisesti riippuvaisia. Ohjelmistojen kehittäjät ja laitevalmistajat eivät ole tietoyhteiskunnan palvelujen tarjoajia, minkä vuoksi ne jäävät direktiivin soveltamisalan ulkopuolelle. Edellä mainitut velvollisuudet olisi laajennettava koskemaan myös julkishallintoja ja elintärkeiden infrastruktuurien operaattoreita, sillä ne ovat vahvasti riippuvaisia tieto- ja viestintäteknologiasta ja olennaisia elintärkeiden talouden ja yhteiskunnan toimintojen, kuten sähkön ja kaasun jakelun, liikenteen, luottolaitosten, pörssien ja terveydenhuollon, ylläpitämiselle. Häiriö näissä verkko- ja tietojärjestelmissä vaikuttaisi sisämarkkinoihin.

²⁷ EYVL L 204, 21.7.1998, s. 37.

neuvoston direktiivissä 98/34/EY²⁷ määriteltyjä sellaisten tietoyhteiskunnan palvelujen keskeisiä tarjoajia, jotka tukevat loppukäyttäjille suunnattuja tietoyhteiskunnan palveluja tai verkkotoimintoja, kuten sähköisen kaupankäynnin alustoja, internet-välitteisiä maksupalveluja, verkkoyhteisöpalveluja, hakukoneita, yleisiä tai sovelluskauppojen pilvipalveluja, *ne voivat ilmoittaa vapaaehtoisesti toimivaltaiselle viranomaiselle tai yhteyspisteelle sellaisista verkon tietoturvapoikkeamista, joista ilmoittamista ne pitävät asianmukaisena, ja toimivaltaisen viranomaisen tai yhteyspisteen olisi, mikäli se on kohtuullisesti mahdollista, toimitettava tietoturvapoikkeamasta ilmoittaneille markkinatoimijoille strategisesti analysoidut tiedot, joiden avulla turvallisuusuhka voidaan torjua.*

²⁷ EYVL L 204, 21.7.1998, s. 37.

Tarkistus 25

Ehdotus direktiiviksi Johdanto-osan 25 kappale

Komission teksti

(25) Julkishallinnoille ja markkinatoimijoille määrättävät tekniset ja organisatoriset toimenpiteet eivät saisi edellyttää jonkin tietyn kaupallisen tieto- ja viestintäteknologiatuotteen suunnittelua, kehittämistä tai valmistamista tietyllä tavalla.

Tarkistus

(25) Julkishallinnoille ja markkinatoimijoille määrättävät tekniset ja organisatoriset toimenpiteet eivät saisi edellyttää jonkin tietyn kaupallisen tieto- ja viestintäteknologiatuotteen suunnittelua, kehittämistä tai valmistamista tietyllä tavalla. *Toisaalta olisi edellytettävä tietoverkkoturvallisuutta koskevien kansainvälisten normien noudattamista.*

Tarkistus 26

Ehdotus direktiiviksi Johdanto-osan 28 kappale

Komission teksti

(28) Toimivaltaisten viranomaisten olisi kiinnitettävä asianmukaista huomiota epävirallisten ja luotettavien tiedonjakokanavien säilyttämiseen markkinatoimijoiden välillä ja julkisen ja yksityisen sektorin välillä. Toimivaltaisille viranomaisille raportoitujen turvapoikkeamien julkistamisessa olisi otettava asianmukaisesti ja tasapainoisesti huomioon yleisön yleinen etu saada tietoa uhista sekä mahdollinen turvapoikkeamista raportoivien **julkishallintojen ja** markkinatoimijoiden maineen vahingoittuminen ja niille koituva taloudellinen vahinko. Ilmoitusvelvoitteiden täytäntöönpanossa toimivaltaisten viranomaisten olisi kiinnitettävä erityistä huomiota tarpeeseen pitää tuotteiden haavoittuvuutta koskevat tiedot tiukasti luottamuksellisena ennen asianomaisten turvallisuuspäivitysten **julkistamista**.

Tarkistus

(28) Toimivaltaisten viranomaisten **ja yhteyspisteiden** olisi kiinnitettävä asianmukaista huomiota epävirallisten ja luotettavien tiedonjakokanavien säilyttämiseen markkinatoimijoiden välillä ja julkisen ja yksityisen sektorin välillä. **Haavoittuvuudesta tai turvapoikkeamista, jotka eivät ole aiemmin olleet tiedossa ja joista on raportoitu** toimivaltaisille viranomaisille, **olisi ilmoitettava kyseisten tieto- ja viestintätekniikan tuotteiden ja palvelujen valmistajille ja palveluntarjoajille. Toimivaltaisille viranomaisille ja yhteyspisteille** raportoitujen turvapoikkeamien julkistamisessa olisi otettava asianmukaisesti ja tasapainoisesti huomioon yleisön yleinen etu saada tietoa uhista sekä mahdollinen turvapoikkeamista raportoivien markkinatoimijoiden maineen vahingoittuminen ja niille koituva taloudellinen vahinko. **Luottamuksen ja tehokkuuden varmistamiseksi tietoturvapoikkeamat olisi julkistettava vasta sen jälkeen, kun poikkeamasta raportoineita tahoja on kuultu, ja vain, mikäli se on ehdottoman välttämätöntä tässä direktiivissä asetettujen tavoitteiden saavuttamiseksi.** Ilmoitusvelvoitteiden täytäntöönpanossa toimivaltaisten viranomaisten **ja yhteyspisteiden** olisi kiinnitettävä erityistä huomiota tarpeeseen pitää tuotteiden haavoittuvuutta koskevat tiedot tiukasti luottamuksellisena ennen asianomaisten turvallisuuspäivitysten **käyttöönottoa, joskaan ilmoittamista ei pidä viivyttää enempää kuin on pakollista. Yhteyspisteiden ei pääsääntöisesti tulisi julkistaa turvapoikkeamiin osallisten henkilöiden henkilötietoja. Yhteyspisteiden olisi julkaistava**

henkilötiedot vain tapauksissa, joissa se on välttämätöntä ja oikeasuhteista tavoitteen saavuttamiseksi.

Perustelu

Siinä tapauksessa, että viranomaiset ovat tietoisia tiettyjen tieto- ja viestintätekniikan alan tuotteiden tai palvelujen haavoittuvuudesta, niiden olisi ilmoitettava asiasta valmistajille ja palveluntarjoajille, jotta ne voivat nopeasti mukauttaa tuotteitaan ja palvelujaan.

Tarkistus 27

Ehdotus direktiiviksi Johdanto-osan 29 kappale

Komission teksti

(29) Toimivaltaisilla viranomaisilla olisi oltava tarvittavat keinot tehtäviensä suorittamiseen, mukaan lukien valtuudet saada riittävät tiedot markkinatoimijoilta **ja julkishallinnoilta** verkko- ja tietojärjestelmien turvatason arvioimiseksi sekä luotettavat ja kattavat tiedot verkko- ja tietojärjestelmien toimintaan vaikuttaneista tosiasiallisista turvapoikkeamista.

Tarkistus

(29) Toimivaltaisilla viranomaisilla **ja yhteyspisteillä** olisi oltava tarvittavat keinot tehtäviensä suorittamiseen, mukaan lukien valtuudet saada riittävät tiedot markkinatoimijoilta verkko- ja tietojärjestelmien turvatason arvioimiseksi **ja turvapoikkeamien määrän, laajuuden ja kohteiden mittaamiseksi** sekä luotettavat ja kattavat tiedot verkko- ja tietojärjestelmien toimintaan vaikuttaneista tosiasiallisista turvapoikkeamista.

Tarkistus 28

Ehdotus direktiiviksi Johdanto-osan 30 kappale

Komission teksti

(30) Turvapoikkeaman taustalla on usein rikollinen toiminta. Turvapoikkeamien rikollista luonnetta voidaan epäillä, vaikka sitä tukeva näyttö ei olisi riittävän selvä alusta alkaen. Toimivaltaisten viranomaisten ja lainvalvontaviranomaisten välisen yhteistyön olisi tällöin oltava osa tehokasta

Tarkistus

(30) Turvapoikkeaman taustalla on usein rikollinen toiminta **tai tietoverkkosota**. Turvapoikkeamien rikollista luonnetta voidaan epäillä, vaikka sitä tukeva näyttö ei olisi riittävän selvä alusta alkaen. Toimivaltaisten viranomaisten, **yhteyspisteiden** ja lainvalvontaviranomaisten välisen

ja kokonaisvaltaista reagoitua turvapoikkeamien uhkaan. Turvallisen, varman ja kestävämmän ympäristön kehittäminen edellyttää erityisesti, että turvapoikkeamista, joihin epäillään liittyvän vakavaa rikollisuutta, raportoidaan järjestelmällisesti lainvalvontaviranomaisille. Se, liittykö turvapoikkeamiin vakavaa rikollisuutta, olisi arvioitava tietoverkkorikollisuutta koskevan EU:n lainsäädännön perusteella.

yhteistyön *sekä Euroopan verkkorikostorjuntakeskuksen (EC3) ja ENISAn kanssa tehtävän yhteistyön* olisi tällöin oltava osa tehokasta ja kokonaisvaltaista reagoitua turvapoikkeamien uhkaan. Turvallisen, varman ja kestävämmän ympäristön kehittäminen edellyttää erityisesti, että turvapoikkeamista, joihin epäillään liittyvän vakavaa rikollisuutta, raportoidaan järjestelmällisesti lainvalvontaviranomaisille. Se, liittykö turvapoikkeamiin vakavaa rikollisuutta, olisi arvioitava tietoverkkorikollisuutta koskevan EU:n lainsäädännön perusteella.

Tarkistus 29

Ehdotus direktiiviksi Johdanto-osan 31 kappale

Komission teksti

(31) Turvapoikkeamat vaarantavat monissa tapauksissa henkilötiedot. Toimivaltaisten viranomaisten ja tietosuojaviranomaisten olisi tässä yhteydessä tehtävä yhteistyötä ja vaihdettava tietoa kaikista asiaankuuluvista seikoista, jotta voidaan puuttua turvapoikkeamista johtuviin henkilötietojen tietoturvaloukkauksiin. ***Jäsenvaltioiden on pantava täytäntöön velvollisuus ilmoittaa turvapoikkeamista tavalla, joka minimoi hallinnollisen rasitteen tapauksissa, joissa turvapoikkeama on myös yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta annetussa Euroopan parlamentin ja neuvoston asetuksessa²⁸ tarkoitettu henkilötietojen tietoturvaloukkaus. ENISA voisi tällöin toimia toimivaltaisten viranomaisten ja tietosuojaviranomaisten kanssa yhteistyössä kehittämällä tiedonvaihtomekanismeja ja -malleja, joiden avulla vältetään tarve kahdelle***

Tarkistus

(31) Turvapoikkeamat vaarantavat monissa tapauksissa henkilötiedot. ***Jäsenvaltioiden ja markkinatoimijoiden olisi suojeltava varastoituja, käsiteltyjä tai lähetettyjä henkilötietoja tahattomalta tai lainvastaiselta tuhoamiselta, tahattomalta katoamiselta tai muuttamiselta sekä luvattomalta tai lainvastaiselta varastoinnilta, käytöltä tai paljastamiselta, levittämiseltä tai käytöltä, sekä varmistettava henkilötietojen käsittelyä koskevan turvallisuuspolitiikan toteuttaminen.*** Toimivaltaisten viranomaisten, ***yhteyspisteiden*** ja tietosuojaviranomaisten olisi tässä yhteydessä tehtävä yhteistyötä ja vaihdettava tietoa kaikista asiaankuuluvista seikoista, jotta voidaan puuttua turvapoikkeamista johtuviin henkilötietojen tietoturvaloukkauksiin. Velvollisuus ilmoittaa turvapoikkeamista ***olisi hoidettava*** tavalla, joka minimoi hallinnollisen rasitteen tapauksissa, joissa

ilmoitusmallille. Yksi yhteinen ilmoitusmalli helpottaisi henkilötiedot vaarantaneista turvapoikkeamista raportoimista ja keventäisi yrityksille ja julkishallinnoille koituvaa hallinnollista taakkaa.

turvapoikkeama on myös henkilötietojen tietoturvaloukkaus, **josta on ilmoitettava sovellettavan lainsäädännön mukaisesti. ENISAn olisi tällöin avustettava toimivaltaisia viranomaisia ja tietosuojaviranomaisia** kehittämällä tiedonvaihtomekanismeja ja **yhden yhteisen ilmoitusmallin, joka** helpottaisi henkilötiedot vaarantaneista turvapoikkeamista raportoimista ja keventäisi yrityksille ja julkishallinnoille koituvaa hallinnollista taakkaa.

²⁸ SEC(2012) 72 final.

Perustelu

Mukautettu tietosuojadirektiiviluonnokseen.

Tarkistus 30

Ehdotus direktiiviksi Johdanto-osan 32 kappale

Komission teksti

(32) Turvallisuusvaatimusten standardointi tapahtuu markkinavetoisesti. Turvastandardien johdonmukaisen soveltamisen varmistamiseksi jäsenvaltioiden olisi edistettävä tiettyjen standardien noudattamista tai mukaisuutta, jotta voidaan varmistaa turvallisuuden korkea taso unionissa. Tätä varten voi olla tarpeen **laatia yhdenmukaistettuja standardeja**, jolloin olisi noudatettava 25 päivänä lokakuuta 2012 annettua Euroopan parlamentin ja neuvoston asetusta (EU) N:o 1025/2012 eurooppalaisesta standardoinnista, neuvoston direktiivien 89/686/ETY ja 93/15/ETY sekä Euroopan parlamentin ja neuvoston direktiivien 94/9/EY, 94/25/EY, 95/16/EY, 97/23/EY, 98/34/EY, 2004/22/EY, 2007/23/EY, 2009/23/EY ja 2009/105/EY

Tarkistus

(32) Turvallisuusvaatimusten standardointi tapahtuu markkinavetoisesti **vapaaehtois pohjalta siten, että markkinatoimijoiden olisi voitava käyttää vaihtoehtoisia keinoja, joilla saavutetaan vähintään samanlaisia tuloksia.** Turvastandardien johdonmukaisen soveltamisen varmistamiseksi jäsenvaltioiden olisi edistettävä tiettyjen **yhteentoimivien** standardien noudattamista tai mukaisuutta, jotta voidaan varmistaa turvallisuuden korkea taso unionissa. Tätä varten **on syytä harkita verkon tietoturva koskevien avoimien kansainvälisten standardien soveltamista tai kyseisten välineiden suunnittelemista.** Voi olla tarpeen **toteuttaa lisätoimenpide yhdenmukaistettujen standardien laatimiseksi**, jolloin olisi noudatettava

muuttamisesta ja neuvoston päätöksen 87/95/ETY ja Euroopan parlamentin ja neuvoston päätöksen N:o 1673/2006/EY kumoamisesta²⁹.

25 päivänä lokakuuta 2012 annettua Euroopan parlamentin ja neuvoston asetusta (EU) N:o 1025/2012 eurooppalaisesta standardoinnista, neuvoston direktiivien 89/686/ETY ja 93/15/ETY sekä Euroopan parlamentin ja neuvoston direktiivien 94/9/EY, 94/25/EY, 95/16/EY, 97/23/EY, 98/34/EY, 2004/22/EY, 2007/23/EY, 2009/23/EY ja 2009/105/EY muuttamisesta ja neuvoston päätöksen 87/95/ETY ja Euroopan parlamentin ja neuvoston päätöksen N:o 1673/2006/EY kumoamisesta²⁹.

Erityisesti ETSI (eurooppalainen telealan standardointijärjestö), CEN (Euroopan standardointikomitea) ja CENELEC (Euroopan sähkötekniikan standardointijärjestö) olisi valtuutettava ehdottamaan vaikuttavia ja tehokkaita EU:n avoimia turvallisuusstandardeja, joissa vältetään mahdollisuuksien mukaan tiettyjen teknisten ratkaisujen suosimista ja joiden olisi oltava pienten ja keskisuurien markkinatoimijoiden helposti hallinnoitavissa. Tietoverkkoturvallisuutta koskevia kansainvälisiä normeja olisi tarkasteltava huolellisesti sen varmistamiseksi, että niistä ei ole tingitty ja että niillä taataan asianmukainen turvallisuus, varmistaen näin, että noudattamalla tietoverkkoturvallisuutta koskevia normeja vaatimusten mukaisesti unionin tietoverkkoturvallisuutta parannetaan kokonaisvaltaisesti eikä heikennetä.

²⁹ EUVL L 316, 14.11.2012, s. 12.

²⁹ EUVL L 316, 14.11.2012, s. 12.

Tarkistus 31

Ehdotus direktiiviksi Johdanto-osan 33 kappale

Komission teksti

(33) Komission olisi tarkasteltava tätä direktiiviä säännöllisin väliajoin uudelleen erityisesti tekniikan ja markkinaolojen kehitykseen perustuvien muutostarpeiden selvittämiseksi.

Tarkistus

(33) Komission olisi tarkasteltava tätä direktiiviä säännöllisin väliajoin uudelleen, **kaikkia asianosaisia sidosryhmiä kuullen**, erityisesti **yhteiskunnan, politiikan**, tekniikan ja markkinaolojen kehitykseen perustuvien muutostarpeiden selvittämiseksi.

Tarkistus 32

**Ehdotus direktiiviksi
Johdanto-osan 34 kappale**

Komission teksti

(34) Yhteistyöverkoston moitteettoman toiminnan mahdollistamiseksi olisi komissiolle siirrettävä valta hyväksyä Euroopan unionin toiminnasta tehdyn sopimuksen 290 artiklan mukaisesti säädösvallan siirron nojalla annettavia delegoituja säädöksiä, joilla määritellään perusteet, jotka jäsenvaltion on täytettävä voidakseen osallistua suojattuun tiedonjakojärjestelmään, täsmennetään tarkemmin varhaisvaroituksen käynnistävät tapahtumat ja määritellään olosuhteet, joissa markkinatoimijoiden ja julkishallintojen on ilmoitettava turvapoikkeamista.

Tarkistus

Poistetaan.

Tarkistus 33

**Ehdotus direktiiviksi
Johdanto-osan 35 kappale**

Komission teksti

(35) On erityisen tärkeää, että komissio toteuttaa asiaa valmistellessaan asianmukaiset kuulemiset, **myös** asiantuntijatasolla. Komission olisi **delegoituja säädöksiä valmistellessaan ja**

Tarkistus

(35) On erityisen tärkeää, että komissio toteuttaa asiaa valmistellessaan asianmukaiset kuulemiset, **kaikki sidosryhmät mukaan luettuna ja erityisesti** asiantuntijatasolla. Komission

laatiessaan varmistettava, että asianomaiset asiakirjat toimitetaan Euroopan parlamentille ja neuvostolle yhtäaikaaisesti, hyvissä ajoin ja asianmukaisesti.

olisi varmistettava, että asianomaiset asiakirjat toimitetaan Euroopan parlamentille ja neuvostolle yhtäaikaisesti, hyvissä ajoin ja asianmukaisesti.

Tarkistus 34

Ehdotus direktiiviksi Johdanto-osan 36 kappale

Komission teksti

(36) Jotta voidaan varmistaa yhdenmukaiset edellytykset tämän direktiivin täytäntöönpanolle komissiolle olisi siirrettävä täytäntöönpanovaltaa siltä osin kuin on kyse *toimivaltaisten viranomaisten* ja komission välisestä yhteistyöstä yhteistyöverkostossa, *pääsystä suojattuun tiedonjakoinfrastruktuuriin*, unionin verkko- ja tietoturvan yhteistyösuunnitelmasta, *turvapoikkeamia koskevan julkisen tiedonmuodoista ja menettelyistä sekä verkko- ja tietoturvan kannalta merkityksellisistä standardeista ja/tai teknisistä eritelmistä*. Tätä valtaa olisi käytettävä yleisistä säännöistä ja periaatteista, joiden mukaisesti jäsenvaltiot valvovat komission täytäntöönpanovallan käyttöä, 16 päivänä helmikuuta 2011 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 182/2011³⁰ mukaisesti.

³⁰ EUVL L 55, 28.2.2011, s. 13

Tarkistus

(36) Jotta voidaan varmistaa yhdenmukaiset edellytykset tämän direktiivin täytäntöönpanolle komissiolle olisi siirrettävä täytäntöönpanovaltaa siltä osin kuin on kyse *yhteyspisteiden* ja komission välisestä yhteistyöstä yhteistyöverkostossa, *tämän rajoittamatta kansallisella tasolla olemassa olevia yhteistyömekanismeja, yleisiä yhteenliitettävyyys- ja turvallisuusstandardeja, jotka koskevat suojattua tiedonjakoinfrastruktuuria*, unionin verkko- ja tietoturvan yhteistyösuunnitelmaa sekä *muotoja ja menettelyjä, joita sovelletaan poikkeamiin, joilla on huomattavaa merkitystä*. Tätä valtaa olisi käytettävä yleisistä säännöistä ja periaatteista, joiden mukaisesti jäsenvaltiot valvovat komission täytäntöönpanovallan käyttöä, 16 päivänä helmikuuta 2011 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 182/2011³⁰ mukaisesti.

³⁰ EUVL L 55, 28.2.2011, s. 13.

Tarkistus 35

Ehdotus direktiiviksi Johdanto-osan 37 kappale

Komission teksti

(37) Komission olisi tämän direktiivin täytäntöönpanossa toimittava tarpeen mukaan yhteistyössä asiaankuuluvien alakohtaisten komiteoiden ja EU:n tasolla erityisesti energian, liikenteen ja terveyden alalla perustettujen elinten kanssa.

Tarkistus

(37) Komission olisi tämän direktiivin täytäntöönpanossa toimittava tarpeen mukaan yhteistyössä asiaankuuluvien alakohtaisten komiteoiden ja EU:n tasolla erityisesti **sähköisten viranomaispalvelujen**, energian, liikenteen ja terveyden alalla perustettujen elinten kanssa.

Tarkistus 36

**Ehdotus direktiiviksi
Johdanto-osan 38 kappale**

Komission teksti

(38) Tietoja, jotka toimivaltainen viranomainen katsoo liikesalaisuuksia koskevien unionin ja kansallisten sääntöjen mukaisesti luottamuksellisiksi, olisi vaihdettava komission **ja muiden** toimivaltaisten viranomaisten kanssa vain silloin kun se on ehdottoman välttämätöntä tämän direktiivin soveltamiseksi. Tällöin olisi toimitettava vain ne tiedot, jotka ovat merkityksellisiä ja laajuudeltaan oikein suhteutettuja kulloisenkin tiedonvaihdon tarkoituksen kannalta.

Tarkistus

(38) Tietoja, jotka toimivaltainen viranomainen **tai yhteyspiste** katsoo liikesalaisuuksia koskevien unionin ja kansallisten sääntöjen mukaisesti luottamuksellisiksi, olisi vaihdettava komission, **sen asiaan liittyvien virastojen, yhteyspisteiden ja/tai kansallisten** toimivaltaisten viranomaisten kanssa vain silloin kun se on ehdottoman välttämätöntä tämän direktiivin soveltamiseksi. Tällöin olisi toimitettava vain ne tiedot, jotka ovat merkityksellisiä, **välttämättömiä** ja laajuudeltaan oikein suhteutettuja kulloisenkin tiedonvaihdon tarkoituksen kannalta **noudattaen samalla ennalta määritellyjä kriteerejä, jotka koskevat luottamuksellisuutta sekä turvallisuus- ja luokittelujärjestelmiä ja joilla hallinnoidaan tiedonjakomenettelyä.**

Tarkistus 37

**Ehdotus direktiiviksi
Johdanto-osan 39 kappale**

(39) Turvariskejä ja -poikkeamia koskevien tietojen jakaminen yhteistyöverkostossa ja turvapoikkeamista kansallisille viranomaisille ilmoittamista koskevien vaatimusten noudattaminen voivat edellyttää henkilötietojen käsittelyä. Tällainen henkilötietojen käsittely on tarpeen, jotta voidaan saavuttaa tämän direktiivin tavoitteet, jotka liittyvät yleiseen etuun ja jotka ovat näin ollen perusteltuja direktiivin 95/46/EY 7 artiklan nojalla. Se ei näiden oikeutettujen tavoitteiden kannalta merkitse perusoikeuskirjan 8 artiklalla taattuun henkilötietojen suojaan puuttumista suhteettomalla ja kohtuuttomalla tavalla, joka loukkaisi tämän oikeuden keskeistä sisältöä. Tämän direktiivin soveltamiseksi olisi soveltuvin osin sovellettava Euroopan parlamentin, neuvoston ja komission asiakirjojen saamisesta yleisön tutustuttavaksi 30 päivänä toukokuuta 2001 annettua Euroopan parlamentin ja neuvoston asetusta (EY) N:o 1049/2001³¹. Kun tietoja käsittelevät unionin toimielimet ja muut elimet, kyseisessä tämän direktiivin täytäntöönpanemiseksi suoritettavassa tietojen käsittelyssä olisi noudatettava yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 18 päivänä joulukuuta 2000 annettua Euroopan parlamentin ja neuvoston asetusta (EY) N:o 45/2001.

³¹ EYVL L 145, 31.5.2001, s. 43.

Tarkistus 38

Ehdotus direktiiviksi Johdanto-osan 41 a kappale (uusi)

(39) Turvariskejä ja -poikkeamia koskevien tietojen jakaminen yhteistyöverkostossa ja turvapoikkeamista kansallisille viranomaisille *tai yhteyspisteille* ilmoittamista koskevien vaatimusten noudattaminen voivat edellyttää henkilötietojen käsittelyä. Tällainen henkilötietojen käsittely on tarpeen, jotta voidaan saavuttaa tämän direktiivin tavoitteet, jotka liittyvät yleiseen etuun ja jotka ovat näin ollen perusteltuja direktiivin 95/46/EY 7 artiklan nojalla. Se ei näiden oikeutettujen tavoitteiden kannalta merkitse perusoikeuskirjan 8 artiklalla taattuun henkilötietojen suojaan puuttumista suhteettomalla ja kohtuuttomalla tavalla, joka loukkaisi tämän oikeuden keskeistä sisältöä. Tämän direktiivin soveltamiseksi olisi soveltuvin osin sovellettava Euroopan parlamentin, neuvoston ja komission asiakirjojen saamisesta yleisön tutustuttavaksi 30 päivänä toukokuuta 2001 annettua Euroopan parlamentin ja neuvoston asetusta (EY) N:o 1049/2001³¹. Kun tietoja käsittelevät unionin toimielimet ja muut elimet, kyseisessä tämän direktiivin täytäntöönpanemiseksi suoritettavassa tietojen käsittelyssä olisi noudatettava yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 18 päivänä joulukuuta 2000 annettua Euroopan parlamentin ja neuvoston asetusta (EY) N:o 45/2001.

³¹ EYVL L 145, 31.5.2001, s. 43.

(41 a) Jäsenvaltiot ovat selittävistä asiakirjoista 28 päivänä syyskuuta 2011 annetun jäsenvaltioiden ja komission yhteisen poliittisen lausuman mukaisesti sitoutuneet perustelluissa tapauksissa liittämään ilmoitukseen toimenpiteistä, jotka koskevat direktiivin saattamista osaksi kansallista lainsäädäntöä, yhden tai useamman asiakirjan, josta käy ilmi direktiivin osien ja kansallisen lainsäädännön osaksi saattamiseen tarkoitettujen välineiden vastaavien osien suhde. Tämän direktiivin osalta lainsäätäjä katsoo tällaisten asiakirjojen toimittamisen olevan perusteltua.

Tarkistus 39

Ehdotus direktiiviksi

1 artikla – 2 kohta – b alakohta

Komission teksti

(b) luodaan jäsenvaltioiden välinen yhteistyömekanismi, jotta voidaan varmistaa tämän direktiivin yhtenäinen soveltaminen unionissa ja tarvittaessa verkko- ja tietojärjestelmiin vaikuttavien turvariskien ja -poikkeamien koordinoitu ja tehokas käsittely ja niihin reagoiminen;

Tarkistus

(b) luodaan jäsenvaltioiden välinen yhteistyömekanismi, **johon asianomaiset sidosryhmät osallistuvat**, jotta voidaan varmistaa tämän direktiivin yhtenäinen soveltaminen unionissa ja tarvittaessa verkko- ja tietojärjestelmiin vaikuttavien turvariskien ja -poikkeamien koordinoitu ja tehokas käsittely ja niihin reagoiminen;

Tarkistus 40

Ehdotus direktiiviksi

1 artikla – 6 kohta

Komission teksti

6. Tiedon jakaminen yhteistyöverkostossa III luvun mukaisesti ja verkko- ja tietoturvapoikkeamista 14 artiklan

Tarkistus

6. Tiedon jakaminen yhteistyöverkostossa III luvun mukaisesti ja verkko- ja tietoturvapoikkeamista 14 artiklan

mukaisesti tehtävät ilmoitukset voivat edellyttää henkilötietojen käsittelyä. Jäsenvaltion on hyväksyttävä tällainen käsittely, joka on välttämätöntä yleiseen etuun liittyvien tämän direktiivin tavoitteiden kannalta, direktiivin 95/46/EY 7 artiklan ja direktiivin 2002/58/EY, sellaisina kuin ne on pantu täytäntöön kansallisessa lainsäädännössä, mukaisesti.

mukaisesti tehtävät ilmoitukset voivat edellyttää **tiedoksi antamista luotettaville kolmansille osapuolille ja** henkilötietojen käsittelyä. Jäsenvaltion on hyväksyttävä tällainen käsittely, joka on välttämätöntä yleiseen etuun liittyvien tämän direktiivin tavoitteiden kannalta, direktiivin 95/46/EY 7 artiklan ja direktiivin 2002/58/EY, sellaisina kuin ne on pantu täytäntöön kansallisessa lainsäädännössä, mukaisesti. **Jäsenvaltioiden on hyväksyttävä lainsäädäntötoimia direktiivissä 95/46/EY olevan 13 artiklan mukaisesti, jotta varmistetaan, että julkishallintoja, markkinatoimijoita ja toimivaltaisia viranomaisia ei aseteta vastuuseen sellaisten henkilötietojen käsittelystä, jotka ovat tarpeen tietojen jakamiseksi yhteistyöverkon ja turvapoikkeamista ilmoittamisen kehyksessä.**

Tarkistus 41

Ehdotus direktiiviksi 2 artikla – 1 kohta

Komission teksti

Jäsenvaltioita ei estetä hyväksymästä tai pitämästä voimassa säännöksiä, joilla varmistetaan korkeampi turvataso, sanotun kuitenkin rajoittamatta niille unionin lainsäädännön nojalla kuuluvia velvoitteita.

Tarkistus

Jäsenvaltioita ei estetä hyväksymästä tai pitämästä voimassa säännöksiä, joilla varmistetaan korkeampi turvataso **EU:n perusoikeuskirjan mukaisesti**, sanotun kuitenkin rajoittamatta niille unionin lainsäädännön nojalla kuuluvia velvoitteita.

Perustelu

Jäsenvaltioille myönnettävä liikkumavara turvallisuusasioissa edellyttää Euroopan unionin perusoikeuskirjassa tunnustettujen oikeuksien kunnioittamista. Näitä oikeuksia ovat esimerkiksi oikeus yksityiselämän ja viestien kunnioittamiseen sekä henkilötietojen suojaan, oikeus elinkeinovapauteen ja oikeus tehokkaisiin oikeussuojakeinoihin.

Tarkistus 42

Ehdotus direktiiviksi

3 artikla – 1 kohta – 1 alakohta – b alakohta

Komission teksti

(b) yhtä tai useampaa laitetta tai yhteen kytkettyjen tai toisiinsa yhteydessä olevien laitteiden ryhmää, joka ohjelman avulla suorittaa automaattista *tietojenkäsittelyä* sekä

Tarkistus

(b) yhtä tai useampaa laitetta tai yhteen kytkettyjen tai toisiinsa yhteydessä olevien laitteiden ryhmää, joka ohjelman avulla suorittaa automaattista *digitaalisten tietojen käsittelyä* sekä

Tarkistus 43

Ehdotus direktiiviksi

3 artikla – 1 kohta – 1 alakohta – c alakohta

Komission teksti

(c) *sähköisiä* tietoja, joita a ja b alakohdassa mainituissa järjestelmissä varastoidaan, käsitellään, hankitaan tai välitetään niiden toimintaa, käyttöä, suojausta tai ylläpitoa varten.

Tarkistus

(c) *digitaalisia* tietoja, joita a ja b alakohdassa mainituissa järjestelmissä varastoidaan, käsitellään, hankitaan tai välitetään niiden toimintaa, käyttöä, suojausta tai ylläpitoa varten.

Tarkistus 44

Ehdotus direktiiviksi

3 artikla – 1 kohta – 2 alakohta

Komission teksti

(2) 'turvallisuudella' verkko- tai tietojärjestelmän kykyä suojautua tietyllä varmuudella onnettomuuksilta tai tahallisilta toimilta, jotka vaarantavat tallennettujen tai siirrettyjen tietojen ja muiden kyseisessä verkko- ja tietojärjestelmässä tai sen välityksellä tarjottujen tai välitettävien palvelujen saatavuuden, aitouden, eheyden ja luottamuksellisuuden;

Tarkistus

(2) 'turvallisuudella' verkko- tai tietojärjestelmän kykyä suojautua tietyllä varmuudella onnettomuuksilta tai tahallisilta toimilta, jotka vaarantavat tallennettujen tai siirrettyjen tietojen ja muiden kyseisessä verkko- ja tietojärjestelmässä tai sen välityksellä tarjottujen tai välitettävien palvelujen saatavuuden, aitouden, eheyden ja luottamuksellisuuden; *tässä määritely 'turvallisuus' kattaa asianmukaiset*

tekniset laitteet, ratkaisut ja toimintamenettelyt, joilla varmistetaan tässä direktiivissä vahvistettujen turvallisuusvaatimusten noudattaminen;

Tarkistus 45

Ehdotus direktiiviksi 3 artikla – 1 kohta – 4 alakohta

Komission teksti

(4) 'turvapoikkeamalla' mitä tahansa tilannetta tai tapahtumaa, joka tosiasiallisesti vaikuttaa kielteisesti turvallisuuteen;

Tarkistus

(4) 'turvapoikkeamalla' mitä tahansa **kohtuullisen helposti tunnistettavissa olevaa** tilannetta tai tapahtumaa, joka tosiasiallisesti vaikuttaa kielteisesti turvallisuuteen;

Perustelu

Alkuperäinen sanamuoto oli liian laaja-alainen ja olisi monimutkaistanut määritelmän soveltamista.

Tarkistus 46

Ehdotus direktiiviksi 3 artikla – 1 kohta – 5 alakohta

Komission teksti

(5) 'tietoyhteiskunnan palvelulla' direktiivin 98/34/EY 1 artiklan 2 alakohdassa tarkoitettua palvelua;

Tarkistus

Poistetaan.

Tarkistus 47

Ehdotus direktiiviksi 3 artikla – 1 kohta – 8 alakohta – a alakohta

Komission teksti

Tarkistus

(a) sellaisten tietoyhteiskunnan palvelujen tarjoajaa, jotka mahdollistavat muiden tietoyhteiskunnan palvelujen tarjoamisen; näistä palveluntarjoajista on ei-tyhjentävä luettelo liitteessä II;

Poistetaan.

Tarkistus 48

Ehdotus direktiiviksi 3 artikla – 1 kohta – 7 alakohta

Komission teksti

Tarkistus

(7) 'turvapoikkeamien käsittelyllä' kaikkia menettelyjä, jotka tukevat turvapoikkeaman analyysia, sen vaikutusten rajoittamista ja siihen reagointia;

(7) 'turvapoikkeamien käsittelyllä' kaikkia menettelyjä, jotka tukevat turvapoikkeaman **havaitsemista, ennaltaehkäisyä**, analyysia, sen vaikutusten rajoittamista ja siihen reagointia;

Tarkistus 49

Ehdotus direktiiviksi 3 artikla – 1 kohta – 8 alakohta

Komission teksti

Tarkistus

(a) sellaisten tietoyhteiskunnan palvelujen tarjoajaa, jotka mahdollistavat muiden tietoyhteiskunnan palvelujen tarjoamisen; näistä palveluntarjoajista on ei-tyhjentävä luettelo liitteessä II;

(b) sellaisten **elintärkeiden** infrastruktuurien ylläpitäjää, jotka ovat olennaisia elintärkeiden talouden ja yhteiskunnan toimintojen ylläpitämiselle energiahuollon, liikenteen, pankkitoimen, **pörssitoimen** ja terveydenhuollon aloilla; näistä operaattoreista on **ei-tyhjentävä**

(b) sellaisten **julkisten tai yksityisten** infrastruktuurien ylläpitäjää, jotka ovat olennaisia elintärkeiden talouden ja yhteiskunnan toimintojen ylläpitämiselle energiahuollon, liikenteen, pankkitoimen, **rahoitusmarkkinoiden** ja terveydenhuollon aloilla **ja joiden keskeytymisellä tai tuhoutumisella olisi merkittäviä kielteisiä**

luettelo liitteessä II;

vaikutuksia jäsenvaltioon siksi, että edellä mainittuja toimintoja ei voitaisi ylläpitää; näistä operaattoreista on luettelo liitteessä II;

Tarkistus 50

**Ehdotus direktiiviksi
3 artikla – 1 kohta – 8 a alakohta (uusi)**

Komission teksti

Tarkistus

(8 a) 'turvapoikkeamalla, jolla on merkittävä vaikutus' turvapoikkeamaa, joka vaikuttaa tietoverkon tai -järjestelmän turvallisuuteen ja jatkuvuuteen ja aiheuttaa vakavan häiriön elintärkeille talouden ja yhteiskunnan toiminnoille;

Tarkistus 51

**Ehdotus direktiiviksi
3 artikla – 1 kohta – 8 b alakohta (uusi)**

Komission teksti

Tarkistus

(8 b) 'palvelulla' markkinatoimijan tarjoamaa palvelua, pois lukien kaikki muut saman tahon palvelut;

Tarkistus 52

**Ehdotus direktiiviksi
3 artikla – 1 kohta – 11 a alakohta (uusi)**

Komission teksti

Tarkistus

*(11 a) 'säännellyllä markkinalla'
Euroopan parlamentin ja neuvoston*

*direktiivin 2004/39/EY^{28 a} 4 artiklan
14 kohdassa määriteltyä säänneltyä
markkinaa;*

*^{28 a} Euroopan parlamentin ja neuvoston
direktiivi 2004/39/EY, annettu 21 päivänä
huhtikuuta 2004, rahoitusvälineiden
markkinoista (EUVL L 45, 16.2.2005,
s. 18).*

Tarkistus 53

**Ehdotus direktiiviksi
3 artikla – 1 kohta – 11 b alakohta (uusi)**

Komission teksti

Tarkistus

*(11 b) 'monenkeskisellä
kaupankäyntijärjestelmällä' direktiivin
2004/39/EY 4 artiklan 15 kohdassa
määriteltyä monenkeskistä
kaupankäyntijärjestelmää;*

Tarkistus 54

**Ehdotus direktiiviksi
3 artikla – 1 kohta – 11 c alakohta (uusi)**

Komission teksti

Tarkistus

*(11 c) 'organisoidulla
kaupankäyntijärjestelmällä'
monenkeskistä järjestelmää, joka ei ole
sijoituspalveluyrityksen tai markkinoiden
ylläpitäjän ylläpitämä säännelty
markkina, monenkeskinen
kaupankäyntijärjestelmä tai
keskusvastapuoli ja jossa useiden
kolmansien osapuolten
joukkovelkakirjoja, strukturoituja
rahoitustuotteita, päästöoikeuksia tai
johdannaisia koskevat osto- ja myynti-
intressit voivat olla keskenään
vuorovaikutuksessa siten, että tuloksena
on sopimus direktiivin 2004/39/EY*

II osaston säännösten mukaisesti;

Tarkistus 55

**Ehdotus direktiiviksi
4 artikla – 1 kohta**

Komission teksti

Jäsenvaltioiden on varmistettava verkko- ja tietojärjestelmien korkea turvataso alueellaan tämän direktiivin mukaisesti.

Tarkistus

Jäsenvaltioiden on varmistettava verkko- ja tietojärjestelmien **pysyvä ja jatkuva** korkea turvataso alueellaan **EU:n perusoikeuskirjan ja** tämän direktiivin mukaisesti.

Perustelu

Jäsenvaltioille myönnettävä liikkumavara turvallisuusasioissa edellyttää Euroopan unionin perusoikeuskirjassa tunnustettujen oikeuksien kunnioittamista. Näitä oikeuksia ovat esimerkiksi oikeus yksityiselämän ja viestien kunnioittamiseen sekä henkilötietojen suojaan, oikeus elinkeinovapauteen ja oikeus tehokkaisiin oikeussuojakeinoihin.

Tarkistus 56

**Ehdotus direktiiviksi
5 artikla – 1 kohta – e a alakohta (uusi)**

Komission teksti

Tarkistus

(e a) Jäsenvaltiot voivat pyytää tukea Euroopan unionin verkko- ja tietoturvavirastolta (ENISA) kehittäessään kansallisia verkko- ja tietoturvastrategioitaan ja kansallisia verkko- ja tietoturva-alan yhteistyösuunnitelmia yhteistä verkko- ja tietoturvastrategiaa koskevan vähimmäistason yhteistyösuunnitelman perusteella.

Tarkistus 57

**Ehdotus direktiiviksi
5 artikla – 2 kohta – a alakohta**

Komission teksti

(a) *riskinhallintasuunnitelma* riskien *yksilöimiseksi* ja mahdollisten turvapoikkeamien vaikutusten *arvioimiseksi*,

Tarkistus

(a) *riskinhallintakehys, johon sisältyy* riskien *yksilöinti, priorisointi, arviointi* ja *käsittely*, mahdollisten turvapoikkeamien vaikutusten *arviointi, ehkäisy- ja valvontamahdollisuudet sekä mahdollisten vastatoimien valintaa koskevat kriteerit*;

Tarkistus 58

Ehdotus direktiiviksi
5 artikla – 2 kohta – b alakohta

Komission teksti

(b) *suunnitelman* täytäntöönpanoon osallistuvien eri toimijoiden tehtävien ja vastuiden määrittely,

Tarkistus

(b) *kehysten* täytäntöönpanoon osallistuvien eri *viranomaisten ja muiden* toimijoiden tehtävien ja vastuiden määrittely,

Tarkistus 59

Ehdotus direktiiviksi
6 artikla – otsikko

Komission teksti

Verkko- ja tietojärjestelmien turvallisuudesta *vastaava kansallinen toimivaltainen viranomainen*

Tarkistus

Verkko- ja tietojärjestelmien turvallisuudesta *vastaavat kansalliset toimivaltaiset viranomaiset ja yhteispisteet*

Tarkistus 60

Ehdotus direktiiviksi
6 artikla – 1 kohta

Komission teksti

1. Jokaisen jäsenvaltion on nimettävä verkko- ja tietojärjestelmien turvallisuudesta vastaava kansallinen

Tarkistus

1. Jokaisen jäsenvaltion on nimettävä *yksi tai useampi* verkko- ja tietojärjestelmien turvallisuudesta vastaava kansallinen

toimivaltainen viranomainen, jäljempänä
'toimivaltainen viranomainen'.

toimivaltainen viranomainen, jäljempänä
'toimivaltainen viranomainen'.

Tarkistus 61

Ehdotus direktiiviksi 6 artikla – 2 a kohta (uusi)

Komission teksti

Tarkistus

2 a. Jos jäsenvaltio nimeää useampia kuin yhden toimivaltaisen viranomaisen, sen on nimettävä kansallinen viranomainen, esimerkiksi toimivaltainen viranomainen, verkko- ja tietojärjestelmien turvallisuudesta vastaavaksi kansalliseksi yhteyspisteeksi (jäljempänä 'yhteyspiste'). Jos jäsenvaltio nimeää vain yhden toimivaltaisen viranomaisen, toimivaltainen viranomainen on myös yhteyspiste.

Tarkistus 62

Ehdotus direktiiviksi 6 artikla – 2 b kohta (uusi)

Komission teksti

Tarkistus

2 b. Jäsenvaltion toimivaltaiset viranomaiset ja yhteyspiste tekevät tiivistä yhteistyötä tässä direktiivissä vahvistettujen velvoitteiden täyttämiseksi.

Tarkistus 63

Ehdotus direktiiviksi 6 artikla – 2 c kohta (uusi)

Komission teksti

Tarkistus

2 c. Yhteyspiste varmistaa, että muiden yhteyspisteiden kanssa tehdään rajat ylittävää yhteistyötä.

Tarkistus 64

Ehdotus direktiiviksi 6 artikla – 3 kohta

Komission teksti

3. Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla on riittävät tekniset, taloudelliset ja henkilöstön voimavarat, jotta ne voivat suorittaa tehokkaasti ja tuloksekkaasti niille osoitetut tehtävät ja siten täyttää tämän direktiivin tavoitteet. Jäsenvaltioiden on varmistettava *toimivaltaisten viranomaisten* tuloksellinen, tehokas ja suojattu yhteistyö 8 artiklassa tarkoitetussa verkostossa.

Tarkistus

3. Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla **ja yhteyspisteillä** on riittävät tekniset, taloudelliset ja henkilöstön voimavarat, jotta ne voivat suorittaa tehokkaasti ja tuloksekkaasti niille osoitetut tehtävät ja siten täyttää tämän direktiivin tavoitteet. Jäsenvaltioiden on varmistettava **yhteyspisteiden** tuloksellinen, tehokas ja suojattu yhteistyö 8 artiklassa tarkoitetussa verkostossa.

Tarkistus 65

Ehdotus direktiiviksi 6 artikla – 4 kohta

Komission teksti

4. Jäsenvaltioiden on varmistettava, että toimivaltaiset viranomaiset saavat turvapoikkeamista ilmoitukset *julkishallinnoilta ja* markkinatoimijoilta siten kuin 14 artiklan 2 kohdassa säädetään sekä 15 artiklassa tarkoitetut täytäntöönpanovaltuudet ja täytäntöönpanon valvontavaltuudet.

Tarkistus

4. Jäsenvaltioiden on varmistettava, että toimivaltaiset viranomaiset **ja yhteyspisteet** saavat turvapoikkeamista ilmoitukset markkinatoimijoilta siten kuin 14 artiklan 2 kohdassa säädetään sekä 15 artiklassa tarkoitetut täytäntöönpanovaltuudet ja täytäntöönpanon valvontavaltuudet.

Tarkistus 66

Ehdotus direktiiviksi 6 artikla – 5 kohta

Komission teksti

5. Toimivaltaisten viranomaisten on

Tarkistus

5. Toimivaltaisten viranomaisten on

tarvittaessa kuultava *asiaankuuluvia kansallisia lainvalvontaviranomaisia ja tietosuojaviranomaisia ja* tehtävä yhteistyötä *niiden* kanssa.

kuultava *tietosuojaviranomaisia säännönmukaisesti ja tarvittaessa* tehtävä yhteistyötä *asiaankuuluvien kansallisten lainvalvontaviranomaisten* kanssa.

Perustelu

Turvallisuuden varmistamisen ja vapauksien turvaamisen välinen tasapaino järkkyy, jos vain yksi toimivaltainen viranomainen harjoittaa valvontavaltaa kansallisella tasolla ilman toisen kompensoivan viranomaisen kanssa tehtävää yhteistyötä.

Tarkistus 67

Ehdotus direktiiviksi 6 artikla – 5 kohta

Komission teksti

5. Toimivaltaisten viranomaisten on tarvittaessa kuultava asiaankuuluvia kansallisia lainvalvontaviranomaisia ja tietosuojaviranomaisia ja tehtävä yhteistyötä niiden kanssa.

Tarkistus

5. Toimivaltaisten viranomaisten *ja yhteyspisteiden* on tarvittaessa kuultava asiaankuuluvia kansallisia lainvalvontaviranomaisia ja tietosuojaviranomaisia ja tehtävä yhteistyötä niiden kanssa.

Tarkistus 68

Ehdotus direktiiviksi 6 artikla – 6 kohta

Komission teksti

6. Jokaisen jäsenvaltion on ilmoitettava komissiolle viipymättä *toimivaltaisen viranomaisen* nimeämisestä ja tehtävistä sekä mahdollisista myöhemmistä muutoksista näissä tiedoissa. Jokaisen jäsenvaltion on julkistettava *toimivaltaisen viranomaisen* nimeäminen.

Tarkistus

6. Jokaisen jäsenvaltion on ilmoitettava komissiolle viipymättä *toimivaltaisten viranomaisten ja yhteyspisteiden* nimeämisestä ja tehtävistä sekä mahdollisista myöhemmistä muutoksista näissä tiedoissa. Jokaisen jäsenvaltion on julkistettava *toimivaltaisten viranomaisten* nimeäminen.

Tarkistus 69

Ehdotus direktiiviksi 7 artikla – 1 kohta

Komission teksti

1. Jokaisen jäsenvaltion on perustettava tietotekniikan kriisiryhmä, jäljempänä 'CERT-ryhmä' (Computer Emergency Response Team), joka vastaa turvapoikkeamien ja -riskien käsittelystä hyvin määritellyn prosessin mukaisesti ja täyttää liitteessä I olevassa 1 kohdassa esitetyt vaatimukset. CERT-ryhmä voidaan perustaa toimivaltaisen viranomaisen yhteyteen.

Tarkistus

1. Jokaisen jäsenvaltion on perustettava ***kutakin liitteessä II tarkoitettua alaa varten vähintään yksi*** tietotekniikan kriisiryhmä, jäljempänä 'CERT-ryhmä' (Computer Emergency Response Team), joka vastaa turvapoikkeamien ja -riskien käsittelystä hyvin määritellyn prosessin mukaisesti ja täyttää liitteessä I olevassa 1 kohdassa esitetyt vaatimukset. CERT-ryhmä voidaan perustaa toimivaltaisen viranomaisen yhteyteen.

Tarkistus 70

**Ehdotus direktiiviksi
7 artikla – 5 kohta**

Komission teksti

5. ***CERT-ryhmän*** on toimittava toimivaltaisen viranomaisen valvonnassa, ja toimivaltaisen viranomaisen on säännöllisesti tarkastettava uudelleen ***sen*** voimavarojen riittävyyttä, ***toimeksiantoa*** ja turvapoikkeamien käsittelyprosessin tuloksekkua.

Tarkistus

5. ***CERT-ryhmien*** on toimittava toimivaltaisen viranomaisen ***tai yhteispisteen*** valvonnassa, ja toimivaltaisen viranomaisen ***tai yhteispisteen*** on säännöllisesti tarkastettava uudelleen ***niiden*** voimavarojen riittävyyttä, ***toimeksiantoja*** ja turvapoikkeamien käsittelyprosessin tuloksekkua.

Tarkistus 71

**Ehdotus direktiiviksi
7 artikla – 5 a kohta (uusi)**

Komission teksti

Tarkistus

5 a. Jäsenvaltioiden on varmistettava, että CERT-ryhmillä on riittävät henkilö- ja taloudelliset resurssit, jotta ne voivat osallistua aktiivisesti kansainvälisten ja erityisesti unionin tason

yhteistyöverkostojen toimintaan.

Tarkistus 72

Ehdotus direktiiviksi
7 artikla – 5 kohta – 1 alakohta (uusi)

Komission teksti

Tarkistus

(1) CERT-ryhmille annetaan valtuudet ja niitä rohkaistaan käynnistämään yhteisiä harjoituksia ja osallistumaan sellaisiin muiden CERT-ryhmien, kaikkien jäsenvaltioiden CERT-ryhmien ja muiden kuin jäsenvaltioiden asianomaisten toimielinten sekä Naton ja YK:n kaltaisten monikansallisten ja kansainvälisten instituutioiden CERT-ryhmien kanssa.

Tarkistus 73

Ehdotus direktiiviksi
7 artikla – 5 a kohta (uusi)

Komission teksti

Tarkistus

5 a. Kansallisia CERT-ryhmiään kehittäessään jäsenvaltiot voivat pyytää Euroopan verkko- ja tietoturvaviraston (ENISA) tai muiden jäsenvaltioiden tukea.

Tarkistus 74

Ehdotus direktiiviksi
8 artikla

Komission teksti

Tarkistus

1. Toimivaltaiset viranomaiset ja komissio

1. Yhteyspisteet, Euroopan verkko- ja

muodostavat verkoston, jäljempänä 'yhteistyöverkosto', **jotta voidaan tehdä** yhteistyötä verkko- ja tietojärjestelmiin vaikuttavien turvariskien ja -poikkeamien torjumiseksi.

2. Komissio ja **toimivaltaiset viranomaiset** ovat yhteistyöverkostossa pysyvästi yhteydessä toisiinsa. Euroopan verkko- ja tietoturvavirasto, jäljempänä 'ENISA', avustaa **pyynnöstä** yhteistyöverkostoa antamalla asiantuntemusta ja neuvontaa.

3. Yhteistyöverkostossa **toimivaltaisten viranomaisten** on

(a) annettava varhaisvaroituksia turvariskeistä ja -poikkeamista 10 artiklan mukaisesti,

(b) varmistettava koordinoitu reagointi 11 artiklan mukaisesti,

(c) julkaistava yhteisellä verkkosivustolla säännöllisesti ei-luottamukselliset tiedot voimassa olevista varhaisvaroituksista ja meneillään olevasta koordinoidusta reagoinnista,

(d) **jäsenvaltion tai komission pyynnöstä** yhdessä keskusteltava ja tehtävä arviointi yhdestä tai useammasta 5 artiklassa tarkoitettusta kansallisesta verkko- ja tietoturvastrategiasta ja kansallisesta verkko- ja tietoturvan yhteistyösuunnitelmasta tämän direktiivin soveltamisalan rajoissa,

(e) jäsenvaltion tai komission pyynnöstä

tietoturvavirasto (ENISA) ja komissio muodostavat verkoston, jäljempänä 'yhteistyöverkosto', **jossa ne tekevät** yhteistyötä verkko- ja tietojärjestelmiin vaikuttavien turvariskien ja -poikkeamien torjumiseksi.

2. Komissio ja **yhteyspisteet** ovat yhteistyöverkostossa pysyvästi yhteydessä toisiinsa. Euroopan verkko- ja tietoturvavirasto, jäljempänä 'ENISA', avustaa yhteistyöverkostoa antamalla asiantuntemusta ja neuvontaa.

Yhteistyöverkosto tekee tarvittaessa yhteistyötä tietosuojaviranomaisten kanssa.

3. Yhteistyöverkostossa **yhteyspisteiden** on

(a) annettava varhaisvaroituksia turvariskeistä ja -poikkeamista 10 artiklan mukaisesti,

(b) varmistettava koordinoitu reagointi 11 artiklan mukaisesti,

(c) julkaistava yhteisellä verkkosivustolla säännöllisesti ei-luottamukselliset tiedot voimassa olevista varhaisvaroituksista ja meneillään olevasta koordinoidusta reagoinnista,

(c a) keskusteltava yhdessä 14 artiklassa tarkoitetuista turvavaatimuksista ja turvapoikkeamista ilmoittamisesta sekä 15 artiklassa tarkoitettusta täytäntöönpanosta ja sen valvonnasta ja sovittava näiden yhteisestä tulkinnasta ja johdonmukaisesta soveltamisesta sekä koordinoitava toimenpiteitään;

(d) yhdessä keskusteltava ja tehtävä arviointi yhdestä tai useammasta 5 artiklassa tarkoitettusta kansallisesta verkko- ja tietoturvastrategiasta ja kansallisesta verkko- ja tietoturvan yhteistyösuunnitelmasta tämän direktiivin soveltamisalan rajoissa,

(e) **ENISAn**, jäsenvaltion tai komission

yhdessä keskusteltava ja tehtävä arviointi CERT-ryhmien tuloksellisuudesta erityisesti tehtäessä verkko- ja tietoturvarajoituksia unionin tasolla,

(f) tehtävä yhteistyötä ja vaihdettava tietoa kaikista asiaankuuluvista seikoista ***Europolin yhteydessä toimivan Euroopan verkkorikostorjuntakeskuksen kanssa ja*** muiden asianomaisten, erityisesti tietosuojan, energiahuollon, liikenteen, pankkitoimen, ***pörssitoimen*** ja terveydenhuollon alan eurooppalaisten elinten kanssa,

(g) vaihdettava tietoa ja parhaita toimintatapoja keskenään ja komission kanssa sekä avustettava toisiaan verkko- ja tietoturvalmiuksien kehittämisessä,

(h) järjestettävä säännöllisiä vertaisarviointeja valmiuksista ja varautumistasosta,

(i) järjestettävä verkko- ja tietoturvarajoituksia unionin tasolla ja tarvittaessa osallistuttava kansainvälisiin verkko- ja tietoturvarajoituksiin.

pyynnöstä yhdessä keskusteltava ja tehtävä arviointi CERT-ryhmien tuloksellisuudesta erityisesti tehtäessä verkko- ja tietoturvarajoituksia unionin tasolla ***ja toteutettava viipymättä toimenpiteitä havaittujen heikkouksien korjaamiseksi,***

(f) tehtävä yhteistyötä ja vaihdettava tietoa kaikista asiaankuuluvista ***verkko- ja tietoturvaa koskevista*** seikoista muiden asianomaisten, erityisesti tietosuojan, energiahuollon, liikenteen, pankkitoimen, ***rahoitusmarkkinoiden*** ja terveydenhuollon alan eurooppalaisten elinten kanssa,

(f a) keskusteltava yhdessä IV luvun säännöksistä ja sovittava niiden yhteisestä tulkinnasta, johdonmukaisesta soveltamisesta ja yhdenmukaisesta täytäntöönpanosta unionissa,

(g) vaihdettava tietoa ja parhaita toimintatapoja keskenään ja komission kanssa sekä avustettava toisiaan verkko- ja tietoturvalmiuksien kehittämisessä,

(h) järjestettävä säännöllisiä vertaisarviointeja valmiuksista ja varautumistasosta,

(i) järjestettävä verkko- ja tietoturvarajoituksia unionin tasolla ja tarvittaessa osallistuttava kansainvälisiin verkko- ja tietoturvarajoituksiin.

(i a) edistettävä aktiivisesti markkinatoimijoiden osallistumista, kuultava niitä ja vaihdettava tietoja niiden kanssa.

Komissio tiedottaa säännöllisesti yhteistyöverkostolle Horisontti 2020 -puiteohjelman turvallisuustutkimuksista ja muista asiaan liittyvistä ohjelmista.

3 a. Asianomaisia julkishallintoja ja markkinatoimijoita on tarvittaessa pyydettyä osallistumaan 3 kohdan c, g, h ja i alakohdassa tarkoitettuihin yhteistyöverkoston tehtäviin.

3 b. Kun yhteistyöverkostossa jaetaan tai julkistetaan tietoja, varhaisvaroituksia tai markkinatoimijoiden tai julkishallintojen parhaita käytäntöjä, jakamisen tai julkistamisen on tapahduttava alkuperäisen lähteen määrittämän tietoluokituksen mukaisesti 9 artiklan 1 kohdassa määritetyllä tavalla.

3 c. Komissio julkaisee vuosittain kertomuksen edeltävästä vuodesta. Kertomus perustuu verkoston toteuttamiin toimiin ja tämän direktiivin 14 artiklan 4 kohdan mukaisesti annettuun tiivistelmäraporttiin. Toimivaltaisille viranomaisille ja yhteyspisteille raportoitujen yksittäisten turvapoikkeamien julkistamisessa olisi otettava asianmukaisesti ja tasapainoisesti huomioon yleisön yleinen etu saada tietoa uhista sekä mahdollinen turvapoikkeamista raportoivien markkinatoimijoiden maineen vahingoittuminen ja niille koituva taloudellinen vahinko. Markkinatoimijoita on kuultava ennalta.

4. Komissio vahvistaa täytäntöönpanosäädöksissä tarvittavat säännöt 2 ja 3 kohdassa tarkoitetun **toimivaltaisten viranomaisten** ja komission välisen yhteistyön helpottamiseksi. Nämä täytäntöönpanosäädökset hyväksytään 19 artiklan 2 kohdassa tarkoitettua kuulemismenettelyä noudattaen.

4. Komissio vahvistaa täytäntöönpanosäädöksissä tarvittavat säännöt 2 ja 3 kohdassa tarkoitetun **yhteyspisteiden, ENISAn** ja komission välisen yhteistyön helpottamiseksi. Nämä täytäntöönpanosäädökset hyväksytään 19 artiklan 2 kohdassa tarkoitettua kuulemismenettelyä noudattaen.

Tarkistus 75

Ehdotus direktiiviksi 9 artikla – 1 kohta

Komission teksti

1. Arkaluonteisten ja luottamuksellisten tietojen vaihto yhteistyöverkostossa on toteutettava suojatun infrastruktuurin

Tarkistus

Arkaluonteisten ja luottamuksellisten tietojen vaihto yhteistyöverkostossa on toteutettava **ENISAn valvonnassa**

kautta.

ylläpidetyn suojatun infrastruktuurin kautta. *Jäsenvaltioiden on varmistettava, että muiden valtioiden tai komission jakamia arkaluonteisia tai salaisia tietoja ei jaeta kolmansien maiden kanssa tai käytetä väärään tarkoitukseen, esimerkiksi tiedustelupalvelun toimintoihin tai rahoituspäätöksiin.*

Tarkistus 76

Ehdotus direktiiviksi 9 artikla – 2 kohta – johdantokappale

Komission teksti

2. Siirretään komissiolle **18** artiklan mukaisesti valta antaa ***delegoituja säädöksiä***, joissa määritellään seuraaviin näkökohtiin liittyvät perusteet, jotka ***jäsenvaltion*** on täytettävä voidakseen osallistua suojattuun tiedonjakojärjestelmään:

Tarkistus

2. Siirretään komissiolle **19** artiklan mukaisesti valta antaa ***täytäntöönpanosäädöksiä***, joissa määritellään seuraaviin näkökohtiin liittyvät perusteet, jotka ***yhteispisteen*** on täytettävä voidakseen osallistua suojattuun tiedonjakojärjestelmään:

Tarkistus 77

Ehdotus direktiiviksi 9 artikla – 3 kohta

Komission teksti

3. Komissio hyväksyy täytäntöönpanosäädöksillä ***2 ja 3 kohdassa tarkoitettujen perusteiden nojalla päätökset jäsenvaltioiden pääsystä tähän suojattuun infrastruktuuriin***. Nämä täytäntöönpanosäädökset hyväksytään 19 artiklan 3 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

Tarkistus

3. Komissio hyväksyy täytäntöönpanosäädöksillä ***yleiset yhteenliitettävyyss- ja turvallisuusstandardit, joita yhteispisteiden on noudatettava tietojen vaihtamiseksi***. Nämä täytäntöönpanosäädökset hyväksytään 19 artiklan 3 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

Tarkistus 78

Ehdotus direktiiviksi 10 artikla

Komission teksti

1. *Toimivaltaisten viranomaisten* ja komission on annettava yhteistyöverkostossa varhaisvaroitukset turvariskeistä ja -poikkeamista, jotka täyttävät ainakin yhden seuraavista edellytyksistä:

(a) *ne leviävät tai voivat levitä nopeasti,*

(b) *ne ylittävät tai voivat* ylittää kansalliset reagointivalmiudet,

(c) *ne vaikuttavat tai voivat* vaikuttaa useampaan kuin yhteen jäsenvaltioon.

2. *Toimivaltaisten viranomaisten* ja komission on varhaisvaroituksissa annettava kaikki asiaankuuluvat hallussaan olevat tiedot, joista voi olla hyötyä turvariskin tai -poikkeaman arvioinnissa.

3. Komissio voi jäsenvaltion pyynnöstä tai omasta aloitteestaan pyytää jäsenvaltiota antamaan kaikki tarvittavat tiedot tietystä turvariskistä tai -poikkeamasta.

4. Jos turvariskiin tai -poikkeamaan, josta on tehty varhaisvaroitusta, epäillään liittyvän rikollisuutta, *toimivaltaisten viranomaisten* tai komission on *ilmoitettava tästä* Europolin yhteydessä *toimivalle* Euroopan *verkkorikostorjuntakeskukselle*.

Tarkistus

1. *Yhteyspisteiden* ja komission on annettava yhteistyöverkostossa varhaisvaroitukset turvariskeistä ja -poikkeamista, jotka täyttävät ainakin yhden seuraavista edellytyksistä:

(b) *yhteyspiste arvioi, että turvariski tai -poikkeama leviää tai voi levitä nopeasti ja voi* ylittää kansalliset reagointivalmiudet;

(c) *yhteyspisteet tai komissio arvioivat, että riski tai poikkeama* vaikuttaa useampaan kuin yhteen jäsenvaltioon.

2. *Yhteyspisteiden* ja komission on varhaisvaroituksissa annettava *viipymättä* kaikki asiaankuuluvat hallussaan olevat tiedot, joista voi olla hyötyä turvariskin tai -poikkeaman arvioinnissa. *Asianomaisen markkinatoimijan turvallisuusluokitelluiksi tai luottamuksellisiksi katsomat tiedot ja markkinatoimijan henkilöys ilmoitetaan vain siinä laajuudessa, kuin turvariskin tai -poikkeaman arviointi edellyttää.*

3. Komissio voi jäsenvaltion pyynnöstä tai omasta aloitteestaan pyytää jäsenvaltiota antamaan kaikki tarvittavat *turvaluokittelemattomat* tiedot tietystä turvariskistä tai -poikkeamasta.

4. Jos turvariskiin tai -poikkeamaan, josta on tehty varhaisvaroitusta, epäillään liittyvän *vakavaa* rikollisuutta, *yhteyspisteiden* tai komission on *tehtävä yhteistyötä kansallisten verkkorikosviranomaisten kanssa, jotta nämä voivat viipymättä tehdä yhteistyötä ja vaihtaa tietoja* Europolin yhteydessä *toimivan* Euroopan

verkkorikostorjuntakeskuksen kanssa.

4 a. Yhteistyöverkoston jäsenet eivät saa julkistaa 1 kohdan mukaisesti turvariskeistä ja -poikkeamista saamiaan tietoja ilman ilmoittavan yhteyspisteen etukäteen antamaa hyväksyntää.

4 b. Jos turvariskiinkin tai -poikkeamaan, josta on tehty varhaisvaroitus, epäillään liittyvän vakavia teknisiä rajaylittäviä piirteitä, yhteyspisteiden tai komission on ilmoitettava tästä ENISAlle.

5. Siirretään komissiolle **18** artiklan mukaisesti valta antaa *delegoituja säädöksiä*, joissa määritellään tarkemmin 1 kohdassa tarkoitetut varhaisvaroituksen käynnistävät turvariskit ja -poikkeamat.

5. Siirretään komissiolle **19** artiklan mukaisesti valta antaa *täytäntöönpanosäädöksiä*, joissa määritellään tarkemmin 1 kohdassa tarkoitetut varhaisvaroituksen käynnistävät turvariskit ja -poikkeamat *sekä markkinatoimijoihin liittyvien arkaluonteisten tietojen jakamista koskevat menettelyt.*

Tarkistus 79

Ehdotus direktiiviksi 11 artikla – 1 kohta

Komission teksti

1. Edellä 10 artiklassa tarkoitetun varhaisvaroituksen jälkeen *toimivaltaisten viranomaisten* on asiaankuuluvat tiedot arvioituaan sovittava koordinoidusta reagoinnista 12 artiklassa tarkoitetun unionin verkko- ja tietoturvan yhteistyösuunnitelman mukaisesti.

Tarkistus

1. Edellä 10 artiklassa tarkoitetun varhaisvaroituksen jälkeen *yhteyspisteiden* on asiaankuuluvat tiedot arvioituaan *viipymättä* sovittava koordinoidusta reagoinnista 12 artiklassa tarkoitetun unionin verkko- ja tietoturvan yhteistyösuunnitelman mukaisesti.

Tarkistus 80

Ehdotus direktiiviksi 12 artikla – 2 kohta – a alakohta – 1 luetelmakohta

Komission teksti

– muoto ja menettelyt sille, miten

Tarkistus

– muoto ja menettelyt sille, miten

toimivaltaiset viranomaiset keräävät ja jakavat yhteensopivaa ja vertailukelpoista tietoa turvariskeistä ja -poikkeamista,

yhteyspisteet keräävät ja jakavat yhteensopivaa ja vertailukelpoista tietoa turvariskeistä ja -poikkeamista,

Tarkistus 81

Ehdotus direktiiviksi 12 artikla – 3 kohta

Komission teksti

3. Unionin verkko- ja tietoturvan yhteistyösuunnitelma on vahvistettava vuoden kuluessa tämän direktiivin voimaantulosta, ja sitä on tarkistettava säännöllisesti.

Tarkistus

3. Unionin verkko- ja tietoturvan yhteistyösuunnitelma on vahvistettava vuoden kuluessa tämän direktiivin voimaantulosta, ja sitä on tarkistettava säännöllisesti. ***Kunkin tarkistuksen tuloksista raportoidaan Euroopan parlamentille.***

Tarkistus 82

Ehdotus direktiiviksi 12 artikla – 3 a kohta (uusi)

Komission teksti

Tarkistus

3 a. Komissio järjestää määrärahat unionin verkko- ja tietoturvan yhteistyösuunnitelman kehittämistä varten.

Tarkistus 83

Ehdotus direktiiviksi 13 artikla – 1 kohta

Komission teksti

Rajoittamatta yhteistyöverkoston mahdollisuutta epäviralliseen kansainväliseen yhteistyöhön unioni voi tehdä kolmansien maiden tai kansainvälisten järjestöjen kanssa

Tarkistus

Rajoittamatta yhteistyöverkoston mahdollisuutta epäviralliseen kansainväliseen yhteistyöhön unioni voi tehdä kolmansien maiden tai kansainvälisten järjestöjen kanssa

kansainvälisiä sopimuksia, joissa sallitaan ja organisoidaan niiden osallistuminen joihinkin yhteistyöverkoston toimiin. **Tällaisissa** sopimuksissa on **otettava huomioon tarve taata** yhteistyöverkostossa levitettävien henkilötietojen **riittävä suoja**.

kansainvälisiä sopimuksia, joissa sallitaan ja organisoidaan niiden osallistuminen joihinkin yhteistyöverkoston toimiin. Sopimuksissa **määrätään valvontamenettelyä, jota on noudatettava** yhteistyöverkostossa levitettävien henkilötietojen **riittävän suojan varmistamiseksi. Euroopan parlamentille on tiedotettava sopimuksia koskevista neuvotteluista ja taattava sopimusten sisällön avoimuus. Kaikki henkilötietojen siirrot unionin ulkopuolisissa maissa oleville vastaanottajille on tehtävä direktiivin 95/46/EY 25 ja 26 artiklan sekä asetuksen (EY) N:o 45/2001 9 artiklan mukaisesti.**

Perustelu

Muiden maiden tai turvallisuudesta huolehtivien elinten kanssa tehtäviin sopimuksiin on sisällytettävä mekanismi, jolla valvotaan kansalaisoikeuksien kunnioittamista. Lisäksi Euroopan parlamentin on toteutettava tehokkaasti sopimusten demokraattista valvontaa, ja parlamentille on tiedotettava määräajan kuluessa sopimusta koskevien neuvottelujen sisällöstä.

Tarkistus 84

Ehdotus direktiiviksi 14 artikla

Komission teksti

Tarkistus

1. Jäsenvaltioiden on varmistettava, että **julkishallinnot ja** markkinatoimijat toteuttavat tarkoituksenmukaiset tekniset ja organisatoriset toimenpiteet valvonnassaan olevien ja toiminnoissaan käyttämiensä verkko- ja tietojärjestelmien turvallisuuteen kohdistuvien riskien hallitsemiseksi. Näillä toimenpiteillä on voitava varmistaa riskiin suhteutettu turvallisuustaso ottaen huomioon **uusin tekniikka**. Erityisesti on toteutettava toimenpiteet, joilla ehkäistään ja minimoidaan niiden verkko- ja **tietojärjestelmään** niiden tarjoamissa keskeisissä palveluissa vaikuttavien turvapoikkeamien vaikutukset ja näin taataan näiden verkko- ja tietojärjestelmien tukemien palvelujen jatkuvuus.

2. Jäsenvaltioiden on **varmistettava**, että **julkishallinnot ja** markkinatoimijat ilmoittavat toimivaltaiselle viranomaiselle turvapoikkeamista, jotka vaikuttavat merkittävästi niiden tarjoamien keskeisten palvelujen turvallisuuteen.

1. Jäsenvaltioiden on varmistettava, että markkinatoimijat toteuttavat tarkoituksenmukaiset tekniset ja organisatoriset toimenpiteet valvonnassaan olevien ja toiminnoissaan käyttämiensä verkko- ja tietojärjestelmien turvallisuuteen kohdistuvien riskien **havaitsemiseksi ja** hallitsemiseksi **tehokkaasti**. Näillä **asianmukaisilla** toimenpiteillä on voitava varmistaa riskiin suhteutettu turvallisuustaso ottaen huomioon **teknologian kehitys**. Erityisesti on toteutettava toimenpiteet, joilla ehkäistään ja minimoidaan niiden verkko- ja **tietojärjestelmien turvallisuuteen** niiden tarjoamissa keskeisissä palveluissa vaikuttavien turvapoikkeamien vaikutukset ja näin taataan näiden verkko- ja tietojärjestelmien tukemien palvelujen jatkuvuus.

2. Jäsenvaltioiden on **pantava täytäntöön mekanismeja sen varmistamiseksi**, että markkinatoimijat ilmoittavat **viipymättä** toimivaltaiselle viranomaiselle **tai yhteyspisteelle** turvapoikkeamista, jotka vaikuttavat merkittävästi niiden tarjoamien keskeisten palvelujen turvallisuuteen **tai jatkuvuuteen. Ilmoittaminen ei lisää ilmoituksen tekvän osapuolen vahinkovastuuta. Turvapoikkeaman vaikutuksen merkittävyyttä arvioitaessa otetaan huomioon muun muassa seuraavat muuttujat.**

(a) niiden käyttäjien lukumäärä, joiden keskeisiin palveluihin turvapoikkeama vaikuttaa;

(b) turvapoikkeaman kesto;

(c) turvapoikkeaman vaikutusten maantieteellinen levinneisyys.

Nämä muuttujat on määriteltävä tarkemmin 8 artiklan 3 kohdan c a alakohdan (uusi) mukaisesti:

2 a. Liitteen II soveltamisalaan kuulumattomat toimijat voivat raportoida vapaaehtoisesti 14 artiklan 2 kohdassa

3. Edellä olevien 1 ja 2 kohdan vaatimuksia sovelletaan kaikkiin Euroopan unionissa palveluja tarjoaviin markkinatoimijoihin.

4. *Toimivaltainen viranomaisen* voi tiedottaa yleisölle *tai vaatia julkishallintoja ja markkinatoimijoita tiedottamaan yleisölle*, jos se katsoo turvapoikkeaman *julkistamisen olevan yleisen edun mukaista*. Toimivaltaisen viranomaisen on toimitettava yhteistyöverkostolle *vuosittain tiivistelmäraportti* vastaanotetuista ilmoituksista ja tämän kohdan mukaisesti

tarkoitetuista turvapoikkeamista.

2 b. Turvapoikkeamaa koskevan raportin vastaanottajan on ilmoitettava mahdollisimman pian turvapoikkeamasta raportoineelle toimijalle toteutetuista toimista, päätöksistä tai suosituksista sekä mahdollisista kolmansista osapuolista, joille asiasta on ilmoitettu, sekä tietojen jakamista koskevista turvallisuus- ja luottamuksellisuuskäytännöistä.

3. Edellä olevien 1 ja 2 kohdan vaatimuksia sovelletaan kaikkiin Euroopan unionissa palveluja tarjoaviin markkinatoimijoihin. *Markkinatoimijat, jotka eivät tarjoa palveluja Euroopan unionissa, voivat raportoida vapaaehtoisesti turvapoikkeamista.*

3 a. Jäsenvaltioiden on varmistettava, että markkinatoimijat ilmoittavat 1 ja 2 kohdassa tarkoitetuista turvapoikkeamista toimivaltaiselle viranomaiselle tai yhteyspisteelle siinä jäsenvaltiossa, jossa turvapoikkeama vaikuttaa keskeisiin palveluihin. Jos turvapoikkeama vaikuttaa keskeisiin palveluihin useammassa kuin yhdessä jäsenvaltiossa, ilmoituksen vastaanottanut yhteyspiste varoittaa muita asianomaisia yhteyspisteitä markkinatoimijoilta saamiensa tietojen perusteella. Markkinatoimijalle on ilmoitettava mahdollisimman pian muut yhteyspisteet, joille turvapoikkeamasta on ilmoitettu, sekä toteutetut toimet, tulokset tai muut turvapoikkeaman kannalta merkitykselliset tiedot.

4. *Yhteyspiste voi toimivaltaista viranomaista ja asianomaista markkinatoimijaa kuultuaan* tiedottaa yleisölle *yksittäisistä turvapoikkeamista*, jos se katsoo, *että kansalaisten on syytä olla tietoisia asiasta* turvapoikkeaman *ennalta ehkäisemiseksi tai meneillään olevaan turvapoikkeamaan reagoimiseksi tai jotta kansalaiset voivat lieventää julkisen tai markkinoilla toimivan*

toteutetuista toimista.

palvelun turvapoikkeamasta itseensä kohdistuvia riskejä tai tapauksissa, joissa turvapoikkeamaan osallinen markkinatoimija on kieltäytynyt korjaamasta turvapoikkeaman aiheuttanutta vakavaa rakenteellista puutetta viivyttämättä. Yhteyspisteen on perusteltava päätöksensä asianmukaisesti. Toimivaltaisen viranomaisen tai yhteyspisteen on, mikäli se on kohtuullisesti mahdollista, toimitettava tietoturvapoikkeamasta ilmoittaneille markkinatoimijoille strategisesti analysoidut tiedot, joiden avulla turvallisuusuhka voidaan torjua. Yhteyspisteen on toimitettava yhteistyöverkostolle kahdesti vuodessa tiivistelmäraportti vastaanotetuista ilmoituksista ja tämän kohdan mukaisesti toteutetuista toimista. Julkistettaessa yksittäisiä turvapoikkeamia, joista on raportoitu toimivaltaisille viranomaisille ja yhteyspisteille, olisi otettava asianmukaisesti ja tasapainoisesti huomioon yleisön yleinen etu saada tietoa uhista sekä mahdollinen turvapoikkeamista raportoivien markkinatoimijoiden maineen vahingoittuminen ja niille koituva taloudellinen vahinko. Markkinatoimijoita on kuultava ennalta. Kun on kyse turvapoikkeamista, joista on ilmoitettu 8 artiklassa tarkoitetulle yhteistyöverkostolle, muut toimivaltaiset kansalliset viranomaiset eivät julkista vastaanottamiaan tietoja riskeistä tai turvapoikkeamista ilman ilmoittavan toimivaltaisen viranomaisen hyväksyntää.

5. Siirretään komissiolle 18 artiklan mukaisesti valta antaa delegoituja säädöksiä, joissa määritellään olosuhteet, joissa julkishallintojen ja markkinatoimijoiden edellytetään ilmoittavan turvapoikkeamista.

6. Jollei 5 kohdan mukaisesti hyväksytyistä delegoiduista säädöksistä

6. Toimivaltaiset viranomaiset tai yhteyspisteet hyväksyvät suuntaviivat

muuta johdu, toimivaltaiset viranomaiset ***voivat hyväksyä suuntaviivoja ja tarvittaessa antaa ohjeita liittyen olosuhteisiin***, joissa ***julkishallintojen ja*** markkinatoimijoiden edellytetään ilmoittavan turvapoikkeamista.

7. Siirretään komissiolle valta määrittellä täytäntöönpanosäädöksillä muodot ja menettelyt 2 kohdan soveltamiseksi. Nämä täytäntöönpanosäädökset hyväksytään 19 artiklan 3 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

8. Edellä olevia 1 ja 2 kohtaa ei sovelleta mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä 6 päivänä toukokuuta 2003 annetussa komission suosituksessa 2003/361/EY³⁵ määriteltyihin mikroyrityksiin.

³⁵ EUVL L 124, 20.5.2003, s. 36.

olosuhteista, joissa markkinatoimijoiden edellytetään ilmoittavan turvapoikkeamista.

7. Siirretään komissiolle valta määrittellä täytäntöönpanosäädöksillä muodot ja menettelyt 2 kohdan soveltamiseksi. Nämä täytäntöönpanosäädökset hyväksytään 19 artiklan 3 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

8. Edellä olevia 1 ja 2 kohtaa ei sovelleta mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä 6 päivänä toukokuuta 2003 annetussa komission suosituksessa 2003/361/EY³⁵ määriteltyihin mikroyrityksiin.

³⁵ EUVL L 124, 20.5.2003, s. 36.

Tarkistus 85

Ehdotus direktiiviksi 14 artikla – 4 kohta – 1 alakohta (uusi)

Komission teksti

Tarkistus

Toimivaltaiselle viranomaiselle raportoimisen lisäksi markkinatoimijoita kannustetaan ilmoittamaan yritystä koskevista turvapoikkeamista tilinpäätöksissään vapaaehtoisesti.

Perustelu

Verkkoturvallisuuspoikkeamat voivat aiheuttaa merkittäviä taloudellisia tappioita ja huomattavia kuluja. Osakkaille ja sijoittajille olisi tiedotettava tällaisten turvapoikkeamien seurauksista. Kun yrityksiä rohkaistaan julkistamaan vapaaehtoisesti tiedot verkkoturvallisuuspoikkeamista, voidaan edistää alojen välistä keskustelua tulevien turvapoikkeamien todennäköisyydestä, riskien laajuudesta sekä verkkoturvaloukkauksien vähentämiseen tähtävien ehkäisevien toimien asianmukaisuudesta.

Tarkistus 86

Ehdotus direktiiviksi 15 artikla

Komission teksti

1. Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla on **kaikki** tarvittavat valtuudet **tutkia tapaukset, joissa julkishallinnot tai markkinatoimijat eivät ole noudattaneet** 14 artiklan mukaisia velvoitteitaan, sekä **näiden tapausten** vaikutukset verkko- ja tietojärjestelmien turvallisuuteen.

2. Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla on valtuudet vaatia markkinatoimijoita **ja julkishallintoja**

(a) antamaan tiedot, jotka tarvitaan niiden verkko- ja tietojärjestelmien turvallisuuden arvioimiseksi, mukaan lukien dokumentoidut turvallisuusohjeet,

(b) **läpikäymään** turvallisuustarkastuksen, jonka suorittaa pätevä ulkopuolinen elin tai kansallinen viranomainen, ja toimittamaan **sen tulokset** toimivaltaiselle viranomaiselle.

3. Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla on valtuudet antaa sitovia ohjeita markkinatoimijoille **ja julkishallinnoille**.

Tarkistus

1. Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla **ja yhteyspisteillä** on tarvittavat valtuudet **varmistaa** 14 artiklan **mukaisten velvoitteiden noudattaminen** sekä **velvoitteiden** vaikutukset verkko- ja tietojärjestelmien turvallisuuteen.

2. Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla **ja yhteyspisteillä** on valtuudet vaatia markkinatoimijoita

(a) antamaan tiedot, jotka tarvitaan niiden verkko- ja tietojärjestelmien turvallisuuden arvioimiseksi, mukaan lukien dokumentoidut turvallisuusohjeet,

(b) **esittämään todisteita turvatoimien tosiasiallisesta täytäntöönpanosta, kuten sisäisten tarkastajien, pätevän ulkopuolisen elimen tai kansallisen viranomaisen suorittaman** turvallisuustarkastuksen **tuloksia** ja toimittamaan **todisteet** toimivaltaiselle viranomaiselle **tai yhteyspisteelle. Toimivaltainen viranomainen tai yhteyspiste voi tarvittaessa pyytää lisätodisteita tai poikkeuksellisissa ja asianmukaisesti perustelluissa tapauksissa suorittaa lisätarkastuksen.**

Toimivaltaisten viranomaisten ja yhteyspisteiden on pyynnön esittäessään ilmoitettava, mihin tarkoitukseen ne tarvitsevat todisteita, ja täsmennettävä, mitä tietoja ne haluavat.

3. Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla **ja yhteyspisteillä** on valtuudet antaa sitovia ohjeita **kaikille liitteessä II tarkoitetuille**

4. Toimivaltaisten viranomaisten on ilmoitettava **turvapoikkeamista**, joihin epäillään liittyvän vakavaa rikollisuutta, **lainvalvontaviranomaisille**.

5. Toimivaltaisten viranomaisten on työskenneltävä tiiviisti yhteistyössä tietosuojaviranomaisten kanssa, kun ne käsittelevät henkilötietojen tietoturvaloukkauksiin johtaneita turvapoikkeamia.

6. Jäsenvaltioiden on varmistettava, että kaikkiin tämän luvun nojalla **julkishallinnoille ja** markkinatoimijoille määrättäviin velvoitteisiin voidaan hakea muutosta tuomioistuimessa.

Tarkistus 87

Ehdotus direktiiviksi 16 artikla

markkinatoimijoille.

4. Toimivaltaisten viranomaisten **ja yhteyspisteiden** on ilmoitettava **asianomaisille markkinatoimijoille mahdollisuudesta pyytää lainvalvontaviranomaisia nostamaan rikossyytteitä tapauksissa**, joihin epäillään liittyvän vakavaa rikollisuutta.

5. Toimivaltaisten viranomaisten **ja yhteyspisteiden** on työskenneltävä tiiviisti yhteistyössä tietosuojaviranomaisten kanssa, kun ne käsittelevät henkilötietojen tietoturvaloukkauksiin johtaneita turvapoikkeamia, **tämän vaikuttamatta tietosuojalainsäädännön soveltamiseen. Yhteyspisteet ja tietosuojaviranomaiset kehittävät yhteistyössä ENISAn kanssa tiedonvaihtomekanismeja ja yhden yhteisen mallin, jota käytetään sekä tämän direktiivin 14 artiklan 2 kohdan että yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta annetun Euroopan parlamentin ja neuvoston direktiivin 95/46/EY mukaisten ilmoitusten tekemiseen.**

Komissio voi hyväksyä täytäntöönpanosäädöksillä ja ottaen tarkoin huomioon yhteyspisteiden ja tietosuojaviranomaisten mahdollisesti kehittämät tiedonvaihtomekanismit ja yhteiset mallit yhteistyössä ENISAn kanssa tiedonvaihtomekanismeja ja yhden yhteisen mallin muotoa koskevia menettelyjä.

6. Jäsenvaltioiden on varmistettava, että kaikkiin tämän luvun nojalla markkinatoimijoille määrättäviin velvoitteisiin voidaan hakea muutosta tuomioistuimessa.

Komission teksti

1. Jäsenvaltioiden on 14 artiklan 1 kohdan johdonmukaisen täytäntöönpanon varmistamiseksi edistettävä verkko- ja tietoturvan kannalta merkityksellisten standardien ja/tai eritelmien käyttöä.

2. Komissio *laatii täytäntöönpanosäädöksillä* luettelon 1 kohdassa tarkoitetuista standardeista. Luettelo julkaistaan Euroopan unionin virallisessa lehdessä.

Tarkistus

1. Jäsenvaltioiden on 14 artiklan 1 kohdan johdonmukaisen täytäntöönpanon varmistamiseksi edistettävä verkko- ja tietoturvan kannalta merkityksellisten *ja EU:n lainsäädännön mukaisten avointen ja yhteentoimivien eurooppalaisten ja kansainvälisten* standardien ja/tai eritelmien käyttöä *ilman, että ne määräävät käyttämään mitään tiettyä teknologiaa.*

2. Komissio *valtuuttaa asianomaisen eurooppalaisen standardointielimen laatimaan yhdessä asiaan liittyvien sidosryhmien kanssa* luettelon 1 kohdassa tarkoitetuista standardeista *ja/tai eritelmistä.* Luettelo julkaistaan Euroopan unionin virallisessa lehdessä.

Tarkistus 88

**Ehdotus direktiiviksi
17 artikla – 1 kohta**

Komission teksti

1. Jäsenvaltioiden on säädettävä seuraamusjärjestelmästä, jota sovelletaan tämän direktiivin täytäntöönpanemiseksi annettujen kansallisten säännösten rikkomiseen, ja toteutettava kaikki tarvittavat toimenpiteet seuraamusten täytäntöönpanon varmistamiseksi. Seuraamusten on oltava tehokkaita, oikeasuhteisia ja varoittavia. Jäsenvaltioiden on annettava nämä säännökset tiedoksi komissiolle viimeistään päivänä, jona tämä direktiivi on saatettava osaksi kansallista lainsäädäntöä, ja kaikki niihin myöhemmin tehtävät muutokset viipymättä.

Tarkistus

1. Jäsenvaltioiden on säädettävä seuraamusjärjestelmästä, jota sovelletaan tämän direktiivin täytäntöönpanemiseksi annettujen kansallisten säännösten *tuottamukselliseen ja tahalliseen* rikkomiseen, ja toteutettava kaikki tarvittavat toimenpiteet seuraamusten täytäntöönpanon varmistamiseksi. Seuraamusten on oltava tehokkaita, oikeasuhteisia ja varoittavia. Jäsenvaltioiden on annettava nämä säännökset tiedoksi komissiolle viimeistään päivänä, jona tämä direktiivi on saatettava osaksi kansallista lainsäädäntöä, ja kaikki niihin myöhemmin tehtävät muutokset viipymättä.

Perustelu

On oltava selvää, että rikkomuksista määrättäviä seuraamuksia voidaan soveltaa ainoastaan, kun markkinatoimijat eivät ole toteuttaneet kaikkia niiltä kohtuudella odotettuja toimenpiteitä. Muutoin markkinatoimijat eivät haluaisi raportoida turvapoikkeamista.

Tarkistus 89

Ehdotus direktiiviksi 17 artikla – 1 a kohta (uusi)

Komission teksti

Tarkistus

1 a. Jäsenvaltioiden on varmistettava, että tämän artiklan 1 kohdassa tarkoitettuja seuraamuksia sovelletaan ainoastaan tapauksissa, joissa markkinatoimija on jättänyt täyttämättä luvun VI mukaiset velvoitteensa tahallisesti tai vakavan huolimattomuuden johdosta.

Tarkistus 90

Ehdotus direktiiviksi 18 artikla

Komission teksti

Tarkistus

18 artikla

Poistetaan.

Siirretyn säädösvallan käyttäminen

1. Siirretään komissiolle valta antaa delegoituja säädöksiä tässä artiklassa säädetyin edellytyksin.

2. Siirretään komissiolle valta antaa 9 artiklan 2 kohdassa, 10 artiklan 5 kohdassa ja 14 artiklan 5 kohdassa tarkoitettuja delegoituja säädöksiä. Komissio laatii siirrettyä säädösvaltaa koskevan kertomuksen viimeistään yhdeksän kuukautta ennen viiden vuoden pituisen kauden päättymistä.

Säädösvallan siirtoa jatketaan ilman eri toimenpiteitä samanpituisiksi kausiksi, jollei Euroopan parlamentti tai neuvosto

vastusta tällaista jatkamista viimeistään kolme kuukautta ennen kunkin kauden päättymistä.

3. Euroopan parlamentti tai neuvosto voi milloin tahansa peruuttaa 9 artiklan 2 kohdassa, 10 artiklan 5 kohdassa ja 14 artiklan 5 kohdassa tarkoitetun säädösvallan siirron.

Peruuttamispäätöksellä lopetetaan tuossa päätöksessä mainittu säädösvallan siirto. Päätös tulee voimaan sitä päivää seuraavana päivänä, jona se julkaistaan Euroopan unionin virallisessa lehdessä, tai jonakin myöhempänä, päätöksessä mainittuna päivänä. Päätös ei vaikuta jo voimassa olevien delegoitujen säädösten pätevyYTEEN.

4. Heti kun komissio antanut delegoidun säädöksen, komissio antaa sen tiedoksi yhtäaikaaisesti Euroopan parlamentille ja neuvostolle.

5. Edellä olevien 9 artiklan 2 kohdan, 10 artiklan 5 kohdan ja 14 artiklan 5 kohdan nojalla annettu delegoitu säädös tulee voimaan ainoastaan, jos Euroopan parlamentti tai neuvosto ei ole kahden kuukauden kuluessa siitä, kun asianomainen säädös on annettu tiedoksi Euroopan parlamentille ja neuvostolle, ilmaissut vastustavansa sitä tai jos sekä Euroopan parlamentti että neuvosto ovat ennen mainitun määräajan päättymistä ilmoittaneet komissiolle, että ne eivät vastusta säädöstä. Euroopan parlamentin tai neuvoston aloitteesta tätä määräaikaä jatketaan kahdella kuukaudella.

Tarkistus 91

**Ehdotus direktiiviksi
20 artikla – 1 kohta**

Komission teksti

Komissio tarkastelee **määräajoin** uudelleen tämän direktiivin toimintaa ja laatii kertomuksen Euroopan parlamentille ja neuvostolle. Ensimmäinen kertomus annetaan **kolmen** vuoden kuluessa 21 artiklassa tarkoitettuna osaksi kansallista lainsäädäntöä saattamiselle asetetusta määräpäivästä. Komissio voi tätä varten pyytää jäsenvaltioita antamaan tietoja ilman aiheetonta viivytyksiä.

Tarkistus

Komissio tarkastelee **kolmen vuoden välein** uudelleen tämän direktiivin toimintaa ja laatii kertomuksen Euroopan parlamentille ja neuvostolle. Ensimmäinen kertomus annetaan **kahden** vuoden kuluessa 21 artiklassa tarkoitettuna osaksi kansallista lainsäädäntöä saattamiselle asetetusta määräpäivästä. Komissio voi tätä varten pyytää jäsenvaltioita antamaan tietoja ilman aiheetonta viivytyksiä.

Perustelu

Verkkoturvallisuuden muuttuvien uhkien ja olosuhteiden vuoksi liitettä II on tarkistettava ja muokattava säännöllisesti.

Tarkistus 92

Ehdotus direktiiviksi
Liite 1 – otsikko 1

Komission teksti

Tietotekniikan **kriisiryhmän (CERT)** vaatimukset ja tehtävät

Tarkistus

Tietotekniikan **kriisiryhmien (CERT-ryhmät)** vaatimukset ja tehtävät

Tarkistus 93

Ehdotus direktiiviksi
Liite 1 – 1 kohta – johdantokappale

Komission teksti

CERT-ryhmän vaatimukset ja tehtävät on määriteltävä riittävästi ja selkeästi ja niiden on perustuttava kansalliseen politiikkaan ja/tai lainsäädäntöön. Niihin on sisällyttävä seuraavat:

Tarkistus

CERT-ryhmien vaatimukset ja tehtävät on määriteltävä riittävästi ja selkeästi ja niiden on perustuttava kansalliseen politiikkaan ja/tai lainsäädäntöön. Niihin on sisällyttävä seuraavat:

(Vastaava muutos tehdään kaikkialle liitteen I tekstiin.)

Tarkistus 94

Ehdotus direktiiviksi

Liite 1 – 1 kohta – 1 alakohta – a alakohta

Komission teksti

(a) **CERT-ryhmän** on varmistettava viestintäpalvelujensa korkea käytettävyys välttämällä yksittäisiä pisteitä, joiden toimintahäiriö keskeyttäisi koko palvelun, ja pitämällä käytössä useita kanavia, joiden kautta siihen voidaan ottaa yhteyttä ja joiden kautta se itse voi ottaa yhteyttä muualle. Viestintäkanavat on määriteltävä selkeästi, ja niiden on oltava hyvin käyttäjien ja yhteistyökumppanien tiedossa.

Tarkistus

(a) **CERT-ryhmien** on varmistettava viestintäpalvelujensa korkea käytettävyys välttämällä yksittäisiä pisteitä, joiden toimintahäiriö keskeyttäisi koko palvelun, ja pitämällä käytössä useita kanavia, joiden kautta siihen voidaan ottaa yhteyttä ja joiden kautta se itse voi ottaa yhteyttä muualle **kaikkina aikoina**. Viestintäkanavat on määriteltävä selkeästi, ja niiden on oltava hyvin käyttäjien ja yhteistyökumppanien tiedossa.

Tarkistus 95

Ehdotus direktiiviksi

Liite 1 – 1 kohta – 1 alakohta – c alakohta

Komission teksti

(c) **CERT-ryhmän** toimipaikka ja sitä tukevat tietojärjestelmät on sijoitettava suojattuihin paikkoihin.

Tarkistus

(c) **CERT-ryhmien** toimipaikka ja sitä tukevat tietojärjestelmät on sijoitettava suojattuihin paikkoihin, **joissa on suojatut verkkotietojärjestelmät**.

Tarkistus 96

Ehdotus direktiiviksi

1 artikla – 1 kohta – 2 alakohta – a alakohta – 1 luetelmakohta

Komission teksti

– turvapoikkeamien seuranta kansallisella tasolla,

Tarkistus

– turvapoikkeamien **havaitseminen ja** seuranta kansallisella tasolla,

Tarkistus 97

Ehdotus direktiiviksi

Liite 1 – 1 kohta – 2 alakohta – a alakohta – 5 a luetelmakohta (uusi)

Komission teksti

Tarkistus

– aktiivinen osallistuminen unionin tason ja kansainvälisiin CERT-ryhmien yhteistyöverkostoihin

Tarkistus 98

Ehdotus direktiiviksi

Liite II

Komission teksti

Tarkistus

Markkinatoimijoiden luettelo

Markkinatoimijoiden luettelo

1. Energia

1. Energia

(a) Sähkö

– Toimittajat

– Jakeluverkkojen operaattorit ja vähittäiskaupan toimittajat

– Sähkön siirtoverkot

– Sähkömarkkinatoimijat

(b) Öljy

– Öljysiirtoputkistot ja öljyvarastot

– Öljyn tuotanto-, jalostus- ja käsittelylaitteistojen operaattorit, varastointi ja siirto

(c) Kaasu

– Toimittajat

– Jakeluverkkojen operaattorit ja vähittäiskaupan toimittajat

– Maakaasun siirtoverkot ja varastointioperaattorit sekä nesteytetyn maakaasun operaattorit

– Maakaasun tuotanto-, jalostus- ja käsittelylaitteistojen operaattorit, varastointi ja siirto

2. Liikenne

– Kaasumarkkinatoimijat

2. Liikenne

(a) Maantieliikenne

(i) Liikenteenhallinnan ja -ohjauksen ylläpitäjät

(ii) Liitännäiset logistiikkapalvelut:

– varastot ja varastointi

– rahdinkäsittely ja

– muut liikenteen tukitoiminnot

(b) Rautatieliikenne

(i) Rautatiet (infrastruktuurin ylläpitäjät, integroituneet yritykset ja rautatieliikenteen harjoittajat)

(ii) Liikenteenhallinnan ja -ohjauksen ylläpitäjät

(iii) Liitännäiset logistiikkapalvelut:

– varastot ja varastointi

– rahdinkäsittely ja

– muut liikenteen tukitoiminnot

(c) Lentoliikenne

(i) Lentoliikenteen (rahti- ja matkustajaliikenteen) harjoittajat

(ii) Lentoasemat

(iii) Liikenteenhallinnan ja -ohjauksen ylläpitäjät

(iv) Liitännäiset logistiikkapalvelut:

– varastointi

– rahdinkäsittely ja

– muut liikenteen tukitoiminnot

(d) Meriliikenne

(i) Merenkulun (sisävesi-, meri- ja rannikkoliikenteen matkustaja- ja rahtiliikenteen) harjoittajat

(ii) Satamat

(iii) Liikenteenhallinnan ja -ohjauksen ylläpitäjät

3. Pankkitoimi: direktiivin 2006/48/EY 4 artiklan 1 kohdassa tarkoitetut luottolaitokset.

4. Finanssimarkkinoiden infrastruktuurit: *pörssit* ja keskusvastapuoliyhteisöt.

5. Terveysdenhuolto:
terveydenhuoltolaitokset (kuten sairaalat ja yksityisklinikat) sekä muut terveydenhuollon tarjoamiseen osallistuvat laitokset.

(iv) Liitännäiset logistiikkapalvelut:

– *varastot ja varastointi*

– *rahdinkäsittely ja*

– *muut liikenteen tukitoiminnot*

2 a. Vesihuoltopalvelut

3. Pankkitoimi: direktiivin 2006/48/EY 4 artiklan 1 kohdassa tarkoitetut luottolaitokset.

4. Finanssimarkkinoiden infrastruktuurit: *säännellyt markkinat, monenkeskiset kaupankäyntijärjestelmät, organisoidut kaupankäyntijärjestelmät, internetvälitteiset maksupalvelut* ja keskusvastapuoliyhteisöt.

5. Terveysdenhuolto:
terveydenhuoltolaitokset (kuten sairaalat ja yksityisklinikat) sekä muut terveydenhuollon tarjoamiseen osallistuvat laitokset.

6. Tieto- ja viestintäteknikka: Toimijan edellä 1–5 kohdassa lueteltujen palvelujen tarjoamiseksi käyttämät pilvipalvelut.

Tämä luettelo on tarkistettava kahden vuoden välein.

ASIAN KÄSITTELY

Otsikko	Yhteisen korkeatasoisen verkko- ja tietoturvan varmistaminen koko unionissa
Viiteasiakirjat	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)
Asiasta vastaava valiokunta Ilmoitettu istunnossa (pvä)	IMCO 15.4.2013
Lausunnon antanut valiokunta Ilmoitettu istunnossa (pvä)	ITRE 15.4.2013
Valiokuntien yhteistyö - ilmoitettu istunnossa (pvä)	12.9.2013
Valmistelija Nimitetty (pvä)	Pilar del Castillo Vera 23.5.2013
Valiokuntakäsittely	14.10.2013 4.11.2013
Hyväksytty (pvä)	16.12.2013
Lopullisen äänestyksen tulos	+: 36 -: 5 0: 0
Lopullisessa äänestyksessä läsnä olleet jäsenet	Amelia Andersdotter, Josefa Andrés Barea, Bendt Bendtsen, Fabrizio Bertot, Reinhard Bütikofer, Maria Da Graça Carvalho, Giles Chichester, Pilar del Castillo Vera, Christian Ehler, Vicky Ford, Adam Gierek, Norbert Glante, Robert Goebbels, Fiona Hall, Romana Jordan, Philippe Lamberts, Marisa Matias, Judith A. Merkies, Angelika Niebler, Jaroslav Paška, Vittorio Prodi, Miloslav Ransdorf, Herbert Reul, Teresa Riera Madurell, Paul Rübig, Amalia Sartori, Salvador Sedó i Alabart, Evžen Tošenovský, Claude Turmes, Marita Ulvskog, Vladimir Urutchev
Lopullisessa äänestyksessä läsnä olleet varajäsenet	Daniel Caspary, António Fernando Correia de Campos, Françoise Grossetête, Roger Helmer, Jolanta Emilia Hibner, Seán Kelly, Eija-Riitta Korhola, Holger Kraemer, Zofija Mazej Kukovič, Silvia-Adriana Țicău, Lambert van Nistelrooij
Lopullisessa äänestyksessä läsnä olleet sijaiset (187 art. 2 kohta)	María Auxiliadora Correa Zamora