EUROOPAN TILINTARKASTUS-TUOMIOISTUIN

FI

Lehdistötiedote

Luxemburg, 29. maaliskuuta 2022

EU-elinten on kohennettava kyberturvallisuusvalmiuksiaan

EU-elimiin kohdistuvat kyberhyökkäykset ovat jyrkässä kasvussa. EU-elinten kyberturvallisuusvalmiudet vaihtelevat eikä valmiustaso kokonaisuutena ole oikeassa suhteessa yhä suurempiin uhkiin. Koska EU-elimet ovat vahvasti sidoksissa toisiinsa, heikkous yhdessä elimessä voi saattaa muutkin elimet alttiiksi turvallisuusuhkille. Tämän johtopäätöksen esittää Euroopan tilintarkastustuomioistuin erityiskertomuksessaan, jossa selvitetään, kuinka hyvin EU-elimet ovat valmistautuneet kyberuhkien varalta. Tarkastajat suosittavat, että käyttöön otetaan sitovat kyberturvallisuussäännöt ja että tietotekniikan kriisiryhmän (CERT-EU) resursseja lisätään. Tarkastajat katsovat, että Euroopan komission olisi myös edistettävä EU-elinten välisen yhteistyön lisäämistä. Samoin CERT-EU:n ja Euroopan unionin kyberturvallisuusviraston olisi suunnattava enemmän huomiota niihin EU-elimiin, joilla on vähemmän kokemusta kyberturvallisuuden hallinnasta.

EU-elimiin kohdistuneiden merkittävien kyberturvallisuuspoikkeamien määrä enemmän kuin kymmenkertaistui vuosina 2018–2021. Etätyö on lisännyt hyökkääjien mahdollisten sisäänpääsypaikkojen määrää huomattavasti. Merkittäviä poikkeamia aiheutetaan tyypillisesti monitahoisilla kyberhyökkäyksillä, joissa käytetään uusia menetelmiä ja teknologioita, ja niiden tutkimiseen ja niistä palautumiseen voi mennä viikkoja ellei kuukausia. Yksi esimerkki on Euroopan lääkevirastoon kohdistunut kyberhyökkäys, jossa paljastettiin viraston arkaluonteisia tietoja ja pyrittiin niitä manipuloimalla heikentämään luottamusta rokotteisiin.

"*EU:n toimielimet, elimet ja virastot ovat houkuttelevia kohteita mahdollisille hyökkääjille. Tämä koskee etenkin ryhmiä, jotka kykenevät toteuttamaan pitkälle kehittyneitä piilohyökkäyksiä kybervakoilua ja muita vahingollisia tarkoituksia varten*", toteaa tarkastusta johtanut Euroopan tilintarkastustuomioistuimen jäsen Bettina Jakobsen. "*Tällaisilla kyberhyökkäyksillä voi olla merkittäviä poliittisia vaikutuksia, ne voivat vahingoittaa EU:n yleistä mainetta ja heikentää luottamusta sen toimielimiin. EU:n on tehostettava organisaationsa suojausta.*"

Tarkastajien pääasiallinen havainto oli, että EU:n toimielimet, elimet ja virastot eivät aina ole hyvin suojattuja kyberuhkilta. EU-elimet eivät lähesty kyberturvallisuutta johdonmukaisesti, olennaiset kontrollit ja kyberturvallisuuden kannalta keskeiset hyvät käytännöt eivät aina ole käytössä eikä kyberturvallisuuskoulutusta tarjota järjestelmällisesti. Resurssien kohdentaminen kyberturvallisuuteen vaihtelee suuresti, ja useat EU-elimet käyttävät siihen huomattavasti

Lehdistötiedotteessa esitetään Euroopan tilintarkastustuomioistuimen erityiskertomuksen keskeiset tiedot. Kertomus löytyy kokonaisuudessaan sivustolta eca.europa.eu.

ECA Press

12, rue Alcide De Gasperi – L-1615 Luxembourg
E: press@eca.europa.eu @EUAuditors eca.europa.eu

vähemmän varoja kuin vertaisryhmänsä. Kyberturvallisuuden tasoeroja voitaisiin teoriassa perustella sillä, että organisaatioiden riskiprofiilit ovat erilaiset, eivätkä niiden käsittelemät tiedot ole yhtä arkaluonteisia. Tarkastajat painottavat kuitenkin, että kyberturvallisuuden heikkous yhdessä EU-elimessä voi altistaa useita muita organisaatioita kyberuhkille (kaikki EU-elimet ovat kytköksissä toisiinsa, ja usein ne ovat yhteydessä myös julkisiin ja yksityisiin organisaatioihin jäsenvaltioissa).

Tuesta kyberturvallisuuden alalla vastaavat EU:ssa pääasiassa tietotekniikan kriisiryhmä (CERT-EU) ja Euroopan unionin kyberturvallisuusvirasto (ENISA). Ne eivät ole kuitenkaan kyenneet antamaan EU-elimille kaikkea näiden tarvitsemaa tukea, koska resurssit ovat rajalliset tai muille osa-alueille on annettu etusija. Tarkastajien mukaan myös tiedonjako on puutteellista. Kaikki EU-elimet eivät esimerkiksi raportoi viivytyksettä haavoittuvuuksista ja merkittävistä kyberturvallisuuspoikkeamista, jotka ovat vaikuttaneet niihin ja voivat vaikuttaa muihin.

Taustaa

Tällä hetkellä EU:n toimielimillä, elimillä ja virastoilla ei ole oikeudellista kehystä, joka koskisi tietoturvaa ja kyberturvallisuutta. Niihin ei sovelleta EU:n laajinta kyberturvallisuutta koskevaa lainsäädäntöä, vuoden 2016 NIS-direktiiviä, eikä sen ehdotettua tarkistettua versiota, NIS2-direktiiviä. EU-elinten kyberturvallisuuteen käyttämien varojen määrästä ei myöskään ole saatavilla kattavaa tietoa. Kaikkiin EU-elimiin sovellettavat yhteiset säännöt tietoturvasta ja kyberturvallisuudesta esitetään tiedonannossa, jonka komissio julkaisi heinäkuussa 2020 EU:n turvallisuusunionistrategiasta kaudelle 2020–2025. Joulukuussa 2020 komissio julkaisi digitaalista vuosikymmentä koskevan EU:n kyberturvallisuusstrategian, jossa se ilmoitti ehdottavansa asetusta kaikkien EU-elinten yhteisistä kyberturvallisuussäännöistä. Komissio ehdotti myös, että CERT-EU:lle vahvistetaan uusi oikeusperusta, jossa kriisiryhmän toimivaltuuksia ja rahoitusta lisätään.

Erityiskertomus 05/2022 *EU:n toimielinten, elinten ja virastojen kyberturvallisuus: valmiustaso ei kokonaisuutena ole oikeassa suhteessa uhkiin* on saatavilla tilintarkastustuomioistuimen sivustolla. Tilintarkastustuomioistuin on käsitellyt EU:n kyberturvallisuuspolitiikan vaikuttavuuteen liittyviä haasteita myös katsauksessaan vuodelta 2019.

Lehdistö – yhteydenotot

Euroopan tilintarkastustuomioistuimen lehdistöpalvelu: press@eca.europa.eu

- Claudia Spiti: claudia.spiti@eca.europa.eu – matkapuhelin: (+352) 691 553 547
- Vincent Bourgeais: vincent.bourgeais@eca.europa.eu – matkapuhelin: (+352) 691 551 502
- Damijan Fišer: damijan.fiser@eca.europa.eu, matkapuhelin: (+352) 621 552 224