Microsoft

Lausunto

05.01.2021

Asia: VN/24348/2020

Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; työryhmän väliraportti

Lausunnonantajan lausunto

Ehdotukset poliittisiksi linjauksiksi, kommentit:

Microsoft Oy kiittää mahdollisuudesta lausua tietoturvan ja tietosuojan parantamiseksi yhteiskunnan eri sektoreilla koskevasta väliraportista. Pidämme hanketta erittäin ajankohtaisena ja hyvänä.

Kyperrikollisuus on jatkuva ja laajeneva haaste sekä julkiselle että yksityiselle sektorille ympäri maailmaa. Enää ei ole tehokasta tarkastella verkkorikollisuutta vain tietyn rikollisen tai rikostyypin linssin läpi. Se voi olla taloudellisesti motivoitunut, kansallisvaltio vetoinen tai molempia. Viimeisen 12 kuukauden maailmanlaajuiset tapahtumat ovat tuoneet ennennäkemättömän muutoksen fyysiseen ja digitaaliseen maailmaan. Olemme nähneet, että verkkorikolliset jatkavat – ja joskus eskaloituvat etenkin kriisiaikoina.

Verkkorikollisia vastaan puolustautuminen on monimutkaista, alati kehittyvää ja päättymätön haaste. Mutta tieto on valtaa ja jotta tietoturva-ammattilaiset voivat luoda onnistuneita puolustusstrategioita, he tarvitsevat enemmän monipuolista ja ajantasaista tietoa uhista, joita vastaan he puolustautuvat. Yhteistyön merkitys korostuu sillä yksikään toimija ei voi ratkaista näitä haasteita yksin. Näin ollen käyntänteiden ja sääntelyiden pitäisi tukea yhteistyötä yli rajojen eikä pelkästään viranomaissektorilla yksisuuntaisesti. Sääntelyt eivät saisi muodostua yhteistyön esteiksi. Tietoturvaloukkaukset eivät myöskään tunnista kansallisia rajoja.

Maailma oli IT:n näkökulmasta huomattavasti yksinkertaisempi kymmenen vuotta sitten. Organisaation rajat olivat tietoteknisessä mielessä helposti piirrettävissä, joten suojaukset oli mielekästä rakentaa näitä rajojen mukaillen. Näiden sisäisten muurien sisällä ylläpidettiin omaa sisäistä verkkoa, johon muurien sisällä toimivilla oli pääsy VPN ratkaisujen kautta sekä palomuurien säännöstöillä. Maailma on sittemmin muuttunut, eivätkä perinteiset keinot ole enää yhteensopivia

tämän päivän toimintaympäristön kanssa, jossa liikennevirrat ovat monitahoisia. Mm. IoT tuo verkkoon mukanaan miljardeja uusia laitteita. Kaikki mikä on verkkoon kytkettävissä, kytketään verkkoon ja näin kaikesta tehdään älykästä.

Muutoksesta kertoo mm se, että fyysisen sijainnin ja verkkoteknisten kontrollisen sijaan tulee keskittyä itse tiedon suojaamiseen modernin tietoturvan keinoin. Haastavaksi asian tekee jos tietoturvallisuuskriteeristöjen vaatimusten taustalla on ajatus siitä, että tieto sijaitsee jossain eksaktissa paikassa ja että siihen pystytään kohdistamaan hallintatoimia perustuen sen fyysiseen sijaintiin. Nykyinen toimintaympäristö ei ole yhteensopiva tämän perusolettamuksen kanssa. Nyt tieto on joka tapauksessa jatkuvassa liikkeessä, joten vaatimuksia asetettaessa tulisi painopiste siirtää enemmän tiedon elinkaaren ja käyttäjien identiteettien suojaamiseen ja hallintaan, ja luopua ristiriitaisista, omalta osaltaan turhaan rajoittavista vaatimuksista. Esimerkiksi monivaiheisen tunnistamisen käyttöönotolla voidaan torjua jopa 99 % tietojenkalasteluhyökkäyksistä. Vaatimukset tulisi näin kohdistaa suojattavan tiedon luottamuksellisuuden, eheyden ja saatavuuden varmistamiseen kulkipa tieto missä tahansa. Kun kontrollit rakennetaan suojattavan kohteeseen mukaan, voidaan esim. fyysiseen sijaintiin liittyvistä vaatimuksista luopua.

Kyberturvallisuudesta huolehtimiseen tarvitaan kokonaan uudenlainen ajattelutapa. Zero Trust -konseptin mukaan kaikki on lähtökohtaisesti epäluotettavaa, ja identiteetti on kaiken keskiössä. Kaikki suojaukset tulee rakentaa tämän lähtökohdan pohjalta. Näin pääsemme verkkotason luottamukseen perustuvasta puolustuksesta eroon, emme ole muurien rajoittamia, mutta suojaamme ns muurien sisällä olevan tiedon.

Koska teknologia kehittyy jatkuvasti, tänä päivänä tietosuojan tarvetta avittamaan on olemassa enemmän työkaluja ja menetelmiä kuin koskaan – kuten esimerkiksi Differential Privacy, Confidential Computing, Homomorphic Encryption, Federated Learning (koneoppimisen hajautettu malli), hajautettu identiteetinhallinta (DID) sekä muita teknologioita tietosuojan varmistamiseen ja hallinnointiin.

Kun kriittisille toimialoille määritellään selkeät ja oikeasuhtaiset tietoturvavaatimukset tulisi huomioida myös teknologian kehitys. Esimerkiksi KATAKRI ei ole yhteensopiva hyperskaalan, globaalin ja jatkuvasti muuttuvan pilvipalvelun kanssa. KATAKRI on alun perin tarkoitettu kansainvälisen turvallisuusluokitellun tiedon suojaamiseen ja perustuu mm. Suomea sitoviin kansainvälisiin tietoturvavelvoitteisiin. KATAKRI 2015 TLIII -vaatimukset pakottavat suljettuihin, julkisista verkoista erotettuihin pieniin ympäristöihin ja näin esim. julkipilven mahdollistamat joustavuus, ketteryys, kustannustehokkuus, helppokäyttöisyys ja uusimmat innovaatiot ovat käyttäjien ulottumattomissa. Samalla poissuljetaan tavat vastata moderniin uhkiin. KATAKRI 2015 TLIII on oma paikkansa ja tärkeätä onkin ymmärtää, että sääntely ja ohjeistukset eivät voi lähteä ns ”one size fits for all” ajattelusta. Olisi suotavaa löytää käytäntöjä, joilla estämme tahattomat liian rajoittavat toimenpiteet, jotka saattavat itse asiassa heikentää tietoturvakulttuuria.

Pilvipalvelujen tuotanto perustuu kansainvälisiin standardeihin. Paikallisen ja alueellisen arviointikriteeristön käyttäminen johtaa turhaan päällekkäisyyteen ja tehottomuuteen globaalissa toimintaympäristössä. Kansallisen lainsäädännön pitäisi hyödyntää tällaisten kansainvälisten sertifiointi- ja akkreditointijärjestelmien koko potentiaali.

Suositeltavaa olisi tunnistaa toimenpiteet jotka voidaan toteuttaa jo nykyisen sääntelyn puitteissa huomioiden niin kansallinen kuin EU sääntely, mutta myös meneillään olevat hankkeet ja etenkin tiettyjen kriittisten alojen jo hyvinkin tarkat säännökset. Tietoturva on tärkeä osa-alue ja sen pitäisi toimia kehityksen mahdollistajana, ei jarruttajana.

Osaaminen on ollut keskiössä jo tovin ja maailmanlaajuisesti sektorilla on osaajapula. Suomi ei ole tässä kohdin poikkeus. Siitäkin syystä olisi entistä tärkeämpää korostaa yhteistyötä ja löytää joustavia malleja osaamisen lisäämiseksi. Olisi suotavaa löytää keinoja stimuloida tätä osaamista Suomessa ja kannustaa keinoja mikro-oppimisesta syvällisempiin opintoihin. Tietoturva on kansainvälistä ja näin ollen niin ulkomaisen osaamisen houkutteleminen Suomeen on suotavaa kuin sellaisen osaamisen hyödyntäminen organisaatioiden verkostoissa. Esimerkiksi paikalliset sääntelyt, jotka eivät reflektoi kansainvälistä käytäntöä lisäävät etenkin pienempien toimijoiden haasteita hyödyntää organisaatiossaan mutta Suomen ulkopuolella olevaa osaamista.

Väliraportin muut osat, kommentit:

-

Mäkelä Susanna
Microsoft - Yhteiskuntasuhteet