OIKEUSREKISTERIKESKUS
RÄTTSREGISTERCENTRALEN

Lausunto

06.08.2024 ORK/314/2024

Asia: VN/36693/2023

Lausuntopyyntö Suomen kyberturvallisuusstrategiasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Oikeusrekisterikeskus kiittää mahdollisuudesta lausua Suomen kyberturvallisuustrategiasta.

Kansalaisten yleisen digiosaamisen taso korreloi valveutumistason kautta käänteisesti erilaisten verkon huijauksien alttiuden kanssa. On tiedossa, että erityisesti kehittyneempiä kyberhyökkäyksiä tehtailevat rikollisryhmät ja valtiolliset toimijat hakevat hyökkäyksien valmistelun tueksi tietoja erilaisilla kohdennetuilla huijaus- ja kalastelukampanjoilla. Myöhemmässä vaiheessa hyökkäysketjua saatetaan alttiiden palvelujen loppukäyttäjien epätietoisella tuella suorittaa teknisiä hyökkäyksiä esimerkiksi ujuttamalla nollapäivähyökkäys kriittisen suojamekanismin ohitse suoraan kohdeympäristöön. Palveluiden käyttäjät ovat yksi tärkeimmistä puolustuslinjoista, jonka osaamisen kehittämiseen tulisi panostaa nykyistä enemmän. Digiosaaminen on myös tärkeää haitalliselta informaatiovaikuttamiselta suojautumisessa koska merkittävä osa kansalaisten saamasta informaatiosta on peräisin digitaalisista välineistä.

Vastaavasti yhteiskunnan tärkeimpien suojattavien tietoteknisten palveluiden onnistunut suojaaminen edellyttää osaamista. Tällä hetkellä on havaittavissa jonkin merkkejä siitä, että riittävällä osaamis- ja kokemustasolla varustetuista asiantuntijoista on pulaa. Viime vuosien trendinä turvallisuusominaisuuksia on alettu lisäämään tuotteisiin, joissa niitä ei ole aiemmin tarvittu, ja samalla sekä yritysmaailma että julkinen sektori on kasvattanut panoksiaan kyberturvallisuuteen. Vaikka turvallisuusosaajia koulutetaankin enenevissä määrin suomalaisissa korkeakouluissa, koulutusmäärät ovat jääneet jälkeen markkinoiden kysynnästä. Toisaalta muodostunutta vajetta voitaisiin kuroa umpeen tehokkaasti jatkuvan oppimisen malleilla, jossa muuten osaaville IT-alan asiantuntijoille annetaan lisää eväitä palvelujen suojaamiseen, jolloin erityisosaajien pula helpottaisi.

Kannattaa huomioida, että salausteknologioita käytetään ensisijaisesti verkostoissa, joissa tietoa vaihdetaan sekä kansallisesti että globaalisti eri toimijoiden kanssa. Tällöin yhteentoimivuus nousee ehdottomaksi vaatimukseksi. Kansallista salausalgoritmien osaamista tarvitaan erityisesti turvallisten jo valmiiden algoritmien valintaan, turvallisuuden todentamiseen sekä erityisesti salausalgoritmien kehitysprosesseihin osallistumiseen. Tulevien vuosien merkittävin haaste tulee olemaan kvanttiturvallisten salausalgoritmien käyttöönotto, mikä tulee koskemaan jokaista yhteiskunnan toimijaa. Muutos onnistuu luonnollisesti sitä paremmin mitä enemmän sitä ohjataan aktiivisesti mm. julkisen hallinnon normistoja kehittämällä.

Siinä missä tilanneymmärrys liittyy enemmänkin viranomaisten väliseen yhteistoimintaan ja laajempien teemojen hallintaan, tilannekuva liittyy tietoteknisten ympäristöjen ja palvelujen päivittäiseen turvallisuustilanteeseen. Tilannekuvan ja erityisesti teknisen tilannekuvan muodostamiselle ei ole selkeitä velvoitteita viranomaisilla. Toimivan tilannekuvan rakentaminen edellyttää laajaa joukkoa erilaisten sensoreiden ja mittarien kehittämistä, tiedon jalostamista sekä niiden ympärille tarvittavia toimintamalleja. Pääosa viranomaisista ei kykene rakentamaan kaikkea tarvittavaa itsenäisesti, vaan nykyistä jo työn alla olevaa kehityskokonaisuutta tulee jatkaa ja tehostaa entisestään aktiivisilla toimenpiteillä, kuten esimerkiksi sarjalla Valtion virastojen sekä Valtion tieto- ja viestintätekniikkakeskus Valtorin yhteisprojekteja. Strategiakaudella korostuu entisestään luonnoksessa mainittujen asioiden lisäksi tilannekuvan nopean tuottamisen merkitys koska sekä aktiiviset uhkatoimijat että tekniset ongelmat, kuten haavoittuvuudet aiheuttavat tarpeen erittäin nopeaan tilannekuvaan perustuvaan reagointikykyyn.

Kannattaa tiedostaa lisäksi, että yksi kivijaloista, joihin yksittäisten viranomaisten palvelujen tietoturvallisuus nojaa, on arviointipalvelut. Tällä hetkellä arviointilaitospalveluja ei ole mahdollista saada keskeisimpään tietoturvallisuuden julkista hallintoa ohjaavaan normiin, julkisen hallinnon arviointikriteeristöön. Kansalliseen turvallisuusauditointikriteeristöön perustuvia arviointeja puolestaan voi suorittaa, mutta ne onnistuvat käytännössä vain nk. perinnekonesaleihin. Kyberturvallisuusstrategian toimeenpanosuunnitelman valmistelun yhteydessä tulee varmistaa, että viranomaisilla on mahdollisuus hankkia arviointilaitospalveluja ajanhetken mukaisia tarpeita vastaaviin ympäristöihin ja palveluihin, mikä ei tällä hetkellä onnistu.

Harjoitustoiminta on hyvin huomioitu strategian luonnoksessa. Monipuolisten kansallisten yhteistoiminnallisten kyberharjoitusten kehittäminen ja jatkuvuuden varmistaminen on erittäin tärkeää. Jokaisen yhteiskunnan toimijan, jolla on vastuullaan yhteiskuntakriittisiä toimintoja, on nähdäksemme harjoiteltava toimimista laajoissa kyberpoikkeamatilanteissa. Riittävien harjoitusten puitteiden tarjoaminen on yksi kriittisistä kyberturvallisuusstrategian menestystekijöistä. Harjoitustoiminnan suunnittelussa kannattaa huomioida, että julkisen hallinnon palvelujen ulkoistusaste todennäköisesti kasvaa todennäköisesti strategiakauden aikana edelleen, jolloin palveluja tuottavia yrityksiä tulee harjoituttaa aiempaa enemmän.

Varautumisessa on keskeistä, että kukin toimija ymmärtää eri skenaarioissa oman tilanteensa suhteessa kokonaisuuteen. Tällä hetkellä puuttuu selkeä kriittisten tietojärjestelmien priorisointi eri tyyppisissä uhkamalleissa. Tietoisuus tästä tulisi olla ainakin yhteiskuntakriittisten palveluiden

omistajilla. Toisaalta ei-kriittisten palveluiden näkökulmasta olisi hyvä järjestää varautumisharjoittelua, jossa keskityttäisiin ratkomaan vaihtoehtoisia toimintakyvyn turvaamistoimenpiteitä silloin, kun kaikki resurssit ovat kiinni kriittisten palveluiden turvaamisessa. Valitettavan usein harjoitellaan yksittäisen palvelun toimintahäiriöstä selviytymistä olettaen, että joka tilanteessa kaikki resurssit ovat käytettävissä.

Kyberrikollisuuden torjunnassa ja tutkinnassa kansainvälisen yhteistyön merkitystä voisi korostaa strategiassa lisää, koska IT-alan toimintaympäristö on hyvin kansainvälistä ja myös valtionhallinnon palveluita tuotetaan koko ajan laajemmin ulkomailta käsin erilaisilta pilvipalvelualustoilta. Kyberrikollisuus ei tunne maarajoja ja se leviää nopeasti kaikkialle. Tämän vuoksi vaaditaan huomattavasti nopeampaa ja valmiiksi verkostoitunutta toimintaa sekä palveluntarjoajilta että rikostutkintaviranomaisilta. Erityisen merkityksellistä kansainvälinen yhteistyö on silloin kun rikollisen sijaintimaan viranomaiset eivät puutu rikolliseen toimintaan.

Toimenpidesuunnitelman toivomme sisältävän konkreettiset maininnat toimenpiteiden resursoinnista. Varsinkin valtion viranomaisten osaamistarpeeseen ja työnantajakilpailukykyyn liittyen tämä on erittäin keskeistä. Strategian toteutuksen onnistuminen tulee edellyttämään monen toimijan resurssien kohdentamista. Toimenpidesuunnitelman tulisi sisältää myös mekanismi toimenpiteiden vaikuttavuuden tarkasteluun.

Kivinen Jussi
Oikeusrekisterikeskus

Lehtisalo Mikko
Oikeusrekisterikeskus - Turvallisuuspalvelut