

Asia: VN/36693/2023

Lausuntopyyntö Suomen kyberturvallisuusstrategiasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Microsoft kiittää mahdollisuudesta lausua Suomen Kyberturvallisuusstrategia 2024 – 2035 luonnokseen.

Kyberturvallisuus on aikamme ratkaiseva haaste. Kyberturvallisuusympäristö kehittyy jatkuvasti ja muuttuu yhä monimutkaisemmaksi. Viimeisten vuosien aikana olemme nähneet merkittävää kasvua vihamielisten valtioiden kyberasekyvykkyydessä ja samalla myös kyberrikollisuuden eri ulottuvuuksien laajamittaisen kasvun. Uhkien rintama on ennennäkemättömän laaja, vastustajat käyttävät yhä kehittyneempiä ja monipuolisempia tekniikoita ja hyökkäykset kohdennetaan laajasti valtion kriittiseen infrastruktuuriin, yrityksiin ja yksittäisiin kansalaisiin.

Microsoft toimii kyberrauhan ja turvallisuuden puolustuksen etulinjassa joka päivä. Microsoftin yli 10 000 tietoturva-asiantuntijaa analysoi päivittäin yli 65 miljardia signaalia tekoälyn avulla ja Threat Intelligence -tiimimme seuraavat satoja uhkatoimijaryhmiä ympäri maailmaa. Tietoturvaekosysteemiimme kuuluu yli 15 000 tietoturvakumppania sekä tietoturvatutkijoista ja testaajista koostuva maailmanlaajuinen avoin yhteisö. Tämä laaja, syvä ja monipuolinen tietoturvaekosysteemi on tehokkaan puolustuksen edellytys .

Myös tekoälyteknologiat muuttavat kyberturvallisuutta. Näemme epäilemättä hyökkääjien käyttävän tekoälyä työkaluna, mutta tekoäly on myös kriittinen osa onnistunutta puolustusta. Esimerkiksi Ukrainassa näimme tekoälyteknologian ensimmäisen onnistuneen käytön Venäjän kyberhyökkäyksiltä suojautumisessa. Tulevina vuosina tekoälypohjaisen kyberpuolustuksen innovaatiot auttavat kääntämään kyberhyökkäysten aallon laajemmin. Tekoälyteknologian tehokas käyttöönotto puolustajien hyödyksi on siksi ratkaisevan tärkeää, jotta voidaan pysyä vastustajien edellä ja edistää kyberrauhaa ja -turvallisuutta.

Suomi on monelta osin digitalisaation kärkimaita ja digitaalinen transformaatio on myös laajasti koko Suomalaista yhteiskuntaa läpileikkaava. Digitalisaation syventyessä myös kyberuhkien potentiaalinen tarttumapinta laajenee. Laaja digitaalinen transformaatio tuo mukanaan myös vastuun tehokkaasti suojautua kyberuhkia vastaan.

Kokonaisturvallisuus ja puolustus on jo vuosikymmenien ajan toiminut suomalaisen yhteiskunnan turvallisuuden perustana ja konaisturvallisuuden merkitys korostuu entisestään digitaalisessa yhteiskunnassa. Kyberpuolustus ja turvallisuus on erottamaton osa suomalaisen yhteiskunnan kokonaisturvallisuutta ja puolustusta.

Kyberturvallisuuden toteutuminen on jaettu vastuu, jonka tehokas toteutus vaatii laajaa ja syvää yhteistyötä yksityisen ja julkisen sektorin välillä. Tarvitsemme enemmän ja syvempiä liittoutumia yksityisellä sektorilla sekä vahvempia kumppanuuksia yksityisen ja julkisen sektorin välillä. Julkisen ja yksityisen sektorin kumppanuudet ovat olennaisen tärkeitä - koko kyberturvallisuuden ja puolustuksen onnistuneen toteutuksen edellytys.

Suosituks:

- Julkisen ja yksityisen sektorin kumppanuudet ovat olennaisen tärkeitä, jotta voidaan vastata kyberturvallisuuden monimutkaisiin ja dynaamisiin haasteisiin ja luoda turvallisempi digitaalinen ympäristö kaikille. Microsoftin näkemyksen mukaan Suomen kyber strategian tavoitetilan kuvaillussa olisi tärkeää tuoda julkisen ja yksityisen sektorin kumppanuuden kriittisyys vahvemmin esiin, niin, että se tuodaan osaksi itse tavoitetilaa.

Ehdotamme, kumppanuustavoitteen lisäämistä tavoitetilatekstiin seuraavasti:

“Suomi edistää kyberturvallisuutta aktiivisesti ja määrätietoisesti julkisen ja yksityisen sektorin syvien ja laaja-alaisten kumppanuuksien sekä tiiviin kansallisen ja kansainvälisen yhteistoiminnan ja tiedovaihdon kautta.”

- Microsoft kannattaa tavoitetta edistää kyberturvallisuus osaamista kansalaistaitona. Jotta voidaan varmistaa että kaikissa suomalaisissa kouluissa kyberturvallisuuden ja tietoturvan perusteita opetetaan kansalaistaitoina, tulisi kyberturvallisuuteen liittyvät opetuskokonaisuudet liittää osaksi kansallista opetussuunnitelmaa oppilaiden tasavertaisuuden turvaamiseksi.

- Näkemyksemme mukaan kriittisten laskentakuormien siirtämistä pilveen olisi nopeutettava, sillä pilven tietoturva- ja kyberpuolustusinnovaatiot ovat vaikuttavimpia. Pilvessä voi tehokkaasti hyödyntää tekoälyä kyberhyökkäysten torjuntaan, hallita ja suojata tietoja paremmin ja palautua häiriöistä nopeammin. Pilvipalvelut ovat siksi monella tavalla kyberturvallisuusnäkökulmasta turvallisempi vaihtoehto kuin omat palvelimet tai datakeskukset. Pilvi siirtymä parantaisi kriittisen infrastruktuurin ja palvelujen häiriönsietokykyä ja turvallisuutta erityisesti terveydenhuollon, energian, rahoituksen, puolustuksen ja julkishallinnon kaltaisilla aloilla. Lisäksi pilvisiirtymä

mahdollistaa tulevaisuudessa uusien teknologioiden nopean ja turvallisen käyttöönoton. Strategiassa olisi hyvä käsitellä ja linjata kriittisten alojen nopean pilvisiirtymän tärkeyttä ja määritellä konkreettiset askeleet sen saavuttamiseksi. Strategiassa olisi hyvä käsitellä ja linjata kriittisten alojen nopean pilvisiirtymän tärkeyttä.

- Tekoälyn hyödyntämistä kyberuhkien havaitsemisessa, ehkäisemisessä ja niihin vastaamisessa tulisi edistää täysimääräisesti. Microsoft puoltaa Suomen tavoitetta olla edelläkävijä näiden teknologioiden adaptoimisessa kyberturvallisuuden ja puolustuksen saralla.

Microsoftille turvallisuus on kriittinen tekijä, joka on kaiken toimintamme keskiössä ja erottamaton osa toiminta kulttuuriamme, tuotteitamme ja toimintatapojamme. Microsoft on sitoutunut työskentelemään Suomen hallituksen, viranomaisten ja muiden sidosryhmien kanssa kyberturvallisuus strategian tavoitteiden saavuttamiseksi sekä Suomen kyberturvallisuuden ja puolustuksen tukemiseksi ja vahvistamiseksi.

Karppinen Juha
Microsoft Oy