TRAFICOM
Liikenne- ja viestintävirasto

Tekoälyn käyttö kriittisillä sektoreilla

Traficomin toteutti kyselyn huoltovarmuuskriittisille organisaatioille kevään 2026 aikana. Kyselyn avulla selvitettiin organisaatioiden tekoälyn käytön nykytilaa sekä tekoälyn hyödyntämiseen liittyviä kyberturvallisuuskysymyksiä. Kyselyn tulokset ovat suuntaa antavia.

Turvallisuusosaaminen ei kehity käyttöönoton tahdissa

Vastaajista 90 % käyttää tekoälyä.

- vain 41 % on uhkamallintanut järjestelmänsä
- vain 28 % kokee tekoälyn kyberturvallisuusosaamisensa riittäväksi

Strategiseen johtamiseen tulee panostaa lisää

Vastaajista 80 % organisaatioista on määritellyt käyttöpolitiikan.

- 52 %:lla ei ole tekoälystrategiaa
- 17 %:lla ei ole politiikkaa, hallintamallia eikä strategiaa

Näkyvyys tekoälyn luomiin uhkiin on vielä rajallinen

Vastaajista 28 % organisaatioista oli havainnut tekoälyllä toteutettuja hyökkäyksiä.

- tekoälyn luomien uhkien tunnistaminen on vielä vaikeaa
- organisaatioilla ei vielä ole riittäviä valmiuksia havaita uusia tekoälyavusteisia hyökkäyksiä

Johtopäätökset

Tekoälyä tullaan hyödyntämään yhä laajemmin kriittisissä prosesseissa. Kyselyn perusteella suhtautuminen tekoälyyn on pääosin myönteistä, ja käyttöönotto etenee nopeasti eri sektoreilla. Samalla tulokset osoittavat, että tekoälyn käyttöönoton vauhti on monin paikoin nopeampaa kuin organisaatioiden kyky kehittää siihen liittyviä turvallisuus- ja hallintakäytäntöjä.

Tuloksista nousee esiin epätasapaino tekoälyn hyödyntämisen ja turvallisuuskyvykkyyksien välillä. Monissa organisaatioissa tekoälyn käyttöä ohjataan käytännön tasolla, mutta kokonaisvaltainen strateginen johtaminen sekä yhtenäiset hallintamallit puuttuvat edelleen. Tämä lisää riskejä erityisesti silloin, kun tekoälyä käytetään yhteiskunnan kannalta kriittisissä toiminnoissa ilman selkeitä vastuita, riskienhallintaa tai uhkamallinnusta.

Kyselyyn vastanneista 35 % ei ole varmuutta onko organisaatiossa otettu tekoäly käyttöön riittävän turvallisesti. Tekoälyratkaisujen käyttöönotto voi synnyttää uusia haavoittuvuuksia ja riippuvuuksia, joita ei vielä tunnisteta tai osata ennakoida. Lisäksi 28 % organisaatioista ilmoitti havainneensa tekoälyllä toteutettuja hyökkäyksiä, mutta yhtä suuri osuus ei osannut arvioida, onko hyökkäyksiä tapahtunut. Tämä viittaa siihen, että tekoälyyn liittyvien uusien uhkien tunnistaminen ja havaitseminen on edelleen haastavaa.

Suositukset

- Organisaatioiden tulee varmistaa, että tekoälyn käyttöönoton rinnalla kehittyvät riittävästi myös osaaminen, hallintamallit, uhkamallinnus, riskienhallinta ja kyky tunnistaa uusia uhkia. Vastuu tekoälyn toiminnasta säilyy aina ihmisillä.
- Lähes kaikki tekoälyä hyödyntävät organisaatiot käyttävät tekoälyavustajia. On tärkeää varmistaa tietosuoja ja tietoturvallinen tiedonkäsittely, rajata käyttöoikeudet tarpeen mukaan, valvoa integraatioita sekä ylläpitää lokitusta.
- Tekoälyratkaisujen turvallisuutta ja toimintaa tulee testata säännöllisesti, ja vastuut sekä toimintaperiaatteet on määriteltävä selkeästi.
- Riskitaso kasvaa erityisesti silloin, kun käyttöön otetaan autonomisia tekoälyagentteja, joilla on päätöksentekovaltaa ja pääsy useisiin järjestelmiin. Näiden ratkaisujen turvalliseen käyttöön tulee kiinnittää erityistä huomiota.