

Tekoäly tukee yritysten lakisääteistä varautumista – mahdollisuus vai uusi riski?

3.6.2026

Suomalaiset yritykset toimivat yhä epävarmemmassa toimintaympäristössä. Pitkittyneet toimitusketjujen häiriöt, kyberuhkat, sään ääri-ilmiöt ja geopoliittiset kriisit ovat tehneet varautumisesta ajankohtaisemman kuin pitkään aikaan. Samalla lainsäädäntö edellyttää monilta yrityksiltä konkreettisia toimia toimintakyvyn turvaamiseksi myös vakavissa häiriö- ja poikkeustilanteissa.

Yksi kiinnostavimmista uusista välineistä tässä kokonaisuudessa on tekoäly. Oikein hyödynnettynä se voi tukea yritysten lakisääteistä valmiussuunnittelua, mutta huolimattomasti käyttöönotettuna se voi myös lisätä riskejä.

Mitä lakisääteinen valmiussuunnittelu tarkoittaa yrityksille?

Suomessa huoltovarmuus perustuu julkisen sektorin, elinkeinoelämän ja järjestöjen yhteistoimintaan. Huoltovarmuuden turvaamisesta annettu laki (1390/1992) ja valtioneuvoston huoltovarmuuspäätökset edellyttävät, että yhteiskunnan toiminnan kannalta kriittiset yritykset turvaavat toimintansa jatkuvuuden häiriö- ja poikkeusoloissa. Tämä koskee erityisesti energia-, logistiikka-, elintarvike-, ICT- ja rahoitussektoria, mutta myös muita yrityksiä välillisesti osana toimitusketjuja (Huoltovarmuuskeskus, n.d.; Valtioneuvosto, 2024).

Lisäksi pelastuslaki (379/2011) velvoittaa kaikkia yrityksiä omatoimiseen varautumiseen. Tämä tarkoittaa onnettomuuksien ehkäisyä, riskien tunnistamista sekä tarvittaessa pelastus- ja varautumissuunnitelmien laatimista myös normaaliolojen häiriötilanteita varten (Finlex, 2011).

Käytännössä varautuminen ei ole yksittäinen asiakirja, vaan jatkuva prosessi, jossa toimintaympäristöä seurataan, riskejä arvioidaan ja toimintamalleja päivitetään.

Mihin tekoäly istuu valmiussuunnittelussa?

Valmiussuunnittelun keskeinen haaste on monimutkaisuus. Yritysten toiminta on yhä verkottuneempaa, ja yksittäinen häiriö voi heijastua nopeasti koko arvoketjuun. Tekoäly tarjoaa tähän kolme keskeistä tukiroolia:

1. Riskien ennakointi ja analyysi
Tekoäly pystyy käsittelemään suuria tietomääriä ja tunnistamaan heikkoja signaaleja, jotka viittaavat tuleviin häiriöihin – esimerkiksi toimitusketjujen pullonkauloihin tai kyberturvallisuuden poikkeamiin.

2. Tilannekuvan muodostaminen
Häiriötilanteessa päätöksenteon tueksi tarvitaan ajantasaista ja kokonaisvaltaista tilannekuvaa. Tekoäly voi yhdistää tietoa eri järjestelmistä ja tuottaa johdolle selkeitä näkymiä tilanteen kehittymisestä.

3. Suunnittelun ja harjoittelun tuki
Erilaisia skenaarioita voidaan simuloida etukäteen: mitä tapahtuu, jos kriittinen järjestelmä kaatuu, henkilöstö ei ole saatavilla tai energiantuotanto keskeytyy? Tämä tukee jatkuvuus- ja valmiussuunnitelmien realistisuutta.

Case-esimerkki: tekoäly osana energia-alan varautumista

Case-esimerkki on havainnollistava ja perustuu julkisiin käytäntöihin energia-alalla – ei yksittäisen yrityksen salassa pidettäviin ratkaisuihin.

Suomalaiset energiayhtiöt toimivat toimialalla, jossa toimintavarmuus on sekä yhteiskunnan että lainsäädännön näkökulmasta kriittistä. Energiasektorilla digitalisaatio ja tekoälyä hyödyntävä analytiikka ovat yleistyneet erityisesti sähköverkon valvonnassa ja kunnossapidossa.

Havainnollisena esimerkkinä voidaan tarkastella tilannetta, jossa energiayhtiö hyödyntää tekoälyä sähköverkon tilannekuvan parantamiseen. Koneoppimismallit analysoivat historiallista ja reaaliaikaista mittausdataa, sääennusteita ja vikahistoriaa tunnistaakseen alueet, joissa sähkökatkoksen riski kasvaa merkittävästi.

Tällainen ratkaisu tukee valmiussuunnittelua monella tavalla:

- se auttaa ennakoimaan häiriöitä ennen niiden toteutumista
- se tukee pelastus- ja korjausresurssien ennakkosijoittelua

- se parantaa viranomaisyhteistyötä tarjoamalla selkeämpää tilannekuvaa

Samalla tekoälyn tuottama tieto täydentää perinteistä valmiussuunnittelua, mutta ei korvaa sitä: lopullinen vastuu päätöksistä säilyy ihmisillä ja organisaation johdolla.

Entä riskit ja sääntely?

Tekoäly ei ole neutraali työkalu. Euroopan unionin **tekoälyasetus (AI Act)** asettaa vaatimuksia tekoälyjärjestelmien riskienhallinnalle, läpinäkyvyydelle ja luotettavuudelle erityisesti kriittisissä käyttökohteissa (ENISA, 2024).

EU:n kyberturvallisuusvirasto **ENISA** on todennut, että tekoälyllä on kaksijakoinen rooli: se voi parantaa turvallisuutta, mutta samalla se voi synnyttää uusia haavoittuvuuksia, jos järjestelmiä ei suojata ja hallita asianmukaisesti (ENISA, 2025).

Yritysten näkökulmasta tämä tarkoittaa, että tekoäly on nähtävä osana **kokonaisvaltaista varautumista**, ei irrallisena teknisenä ratkaisuna.

Lopuksi: tekoäly tukee, mutta ei vapauta vastuusta

Tekoäly tarjoaa suomalaisille yrityksille merkittäviä mahdollisuuksia vahvistaa lakisääteistä valmiussuunnitteluaan. Se voi parantaa ennakointia, tilannekuvaa ja päätöksentekoa tilanteissa, joissa toimintakyky on vaakalaudalla.

Samalla tekoäly korostaa perinteisen varautumisen ydintä: vastuut, roolit ja toimintamallit on määriteltävä selkeästi, ja teknologiaa on käytettävä harkiten. Valmiussuunnittelu on lopulta ennen kaikkea **johtamisen ja yhteistyön kysymys** – tekoäly on yksi työkalu tämän tueksi, ei itse tarkoitus.

Beata Taijala
KTL, Ins., Sertifioitu Projektiosaaja (IPMA Level D)
SEAMK

Kirjoittaja toimii asiantuntijana vAI:lla tuottavuutta -hankkeessa. Hankkeen yhtenä tavoitteena on herättää alueen toimijoissa tietoisuus ja kyvykkyys hyödyntää tekoälyteknologiaa tuottavuuden parantamiseksi.

vAI:lla tuottavuutta? -hanke on Euroopan unionin osarahoittama. Lisää tietoa hankkeesta löydät hankkeen verkkosivuilta: vAI:lla tuottavuutta?

Lähteet

European Union Agency for Cybersecurity. (2024). *Artificial intelligence and next generation technologies*.

https://www.enisa.europa.eu/topics/artificial-intelligence-and-next-gen-technologies

European Union Agency for Cybersecurity. (2025). *ENISA AI threat landscape 2025*. https://www.enisa.europa.eu*Pelastuslaki 379/2011*. https://finlex.fi/fi/lainsaadanto/2011/379*Valtioneuvoston päätös huoltovarmuuden tavoitteista 568/2024*. https://finlex.fi/fi/lainsaadanto/2024/568

Huoltovarmuuskeskus. (i.a.). *Huoltovarmuuden keinot ja yritysten varautuminen*. https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/keinot

Valtioneuvosto. (2024). *Valtioneuvoston päätös huoltovarmuuden tavoitteista muuttuneessa turvallisuusympäristössä*. https://valtioneuvosto.fi