Huoltovarmuusorganisaatio

Kyberkypsyys toimialoilla 2025

Kansallisen toimialojen kyberkypsyys selvityshankkeen raportin lanseeraus

Antti Nyqvist

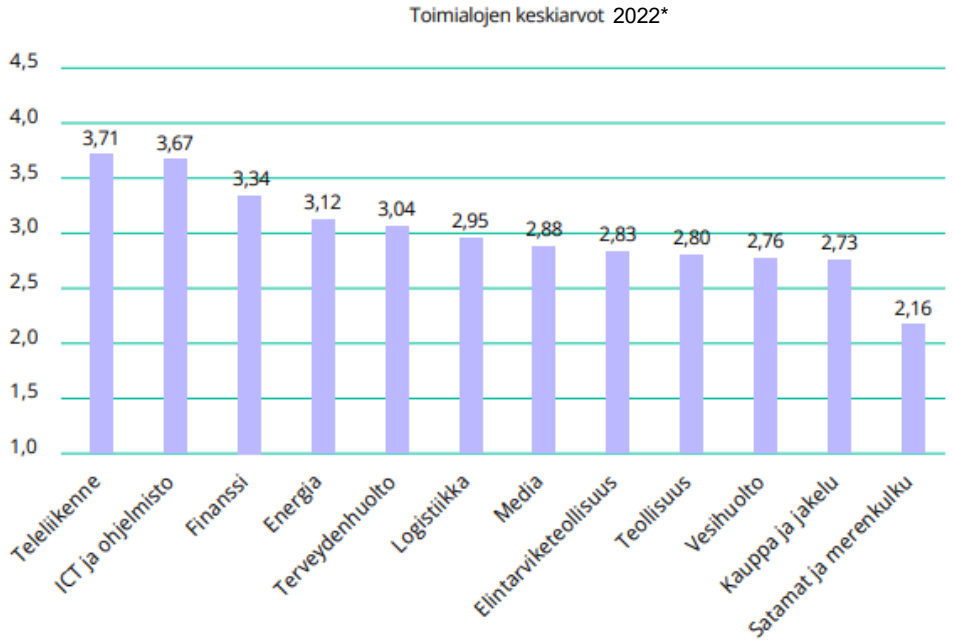
Valmiuspäällikkö, HVO Digipoolin
Poolisihteeri – Teknologiateollisuus ry

Selvityksen taustaa

- Elinkeinoelämän varautumista pyritään tukemaan tiedolla johtamisen keinoin
- Tilannetieto ja –ymmärrys on merkittävää oikeiden toimenpiteiden toteuttamiseksi ja vähäisten resurssien kohdistamiseksi
- Kybertilannekuva muodostuu yleisellä tasolla seuraavista:
  - Mitä yrityksistä raportoidaan
  - Mitä tietoa tiedonvaihtoverkostoissa jaetaan
  - Mitä tekniset järjestelmät havaitsevat
- Selvityksillä täydennetään ymmärrystä
- Huoltovarmuusorganisaation toimialojen tilannetta on arvioitu erilaisin keinoin historiassa
- Kyberturvallisuuden kypsyyttä on arvioitu 2013 vuodesta lähtien

KYBERTURVALLISUUDEN TILANNE ERI TOIMIALOJEN YRITYKSISSÄ
Toistuva selvitys

- Selvitykset n. 2 vuoden välein (2020, 2022, 2025)
- Kyberturvallisuuskeskuksen Kybermittari
  - (Perustuen NIST ja C2M2 malleihin)
- 40 toiminnon kypsyys (otos mallista)
  - Toimintojen kypsyys / Liiketoiminnan riskit toimialalla
  - CMM kypsyysmalli
  - Tuloksia puolen päivän työpajalla



- **Yritysraportti** – kyvykkyydet suhteessa liiketoimintariskeihin
- **Toimialaraportti** – yritykset suhteessa toisiinsa toimialalla (anonyymi)
- **Kansallisen tason raportti**
  - Kooste toimialoista – yritykset suhteessa toisiinsa (anonyymi)
  - Kyvykkyydet suhteessa kansalliseen uhka-arvioon

Tulosten käsittely toimialoittain -> johdetaan tuloksista priorisoituja toimenpide-ehdotuksia HVK kehitysohjelmiin

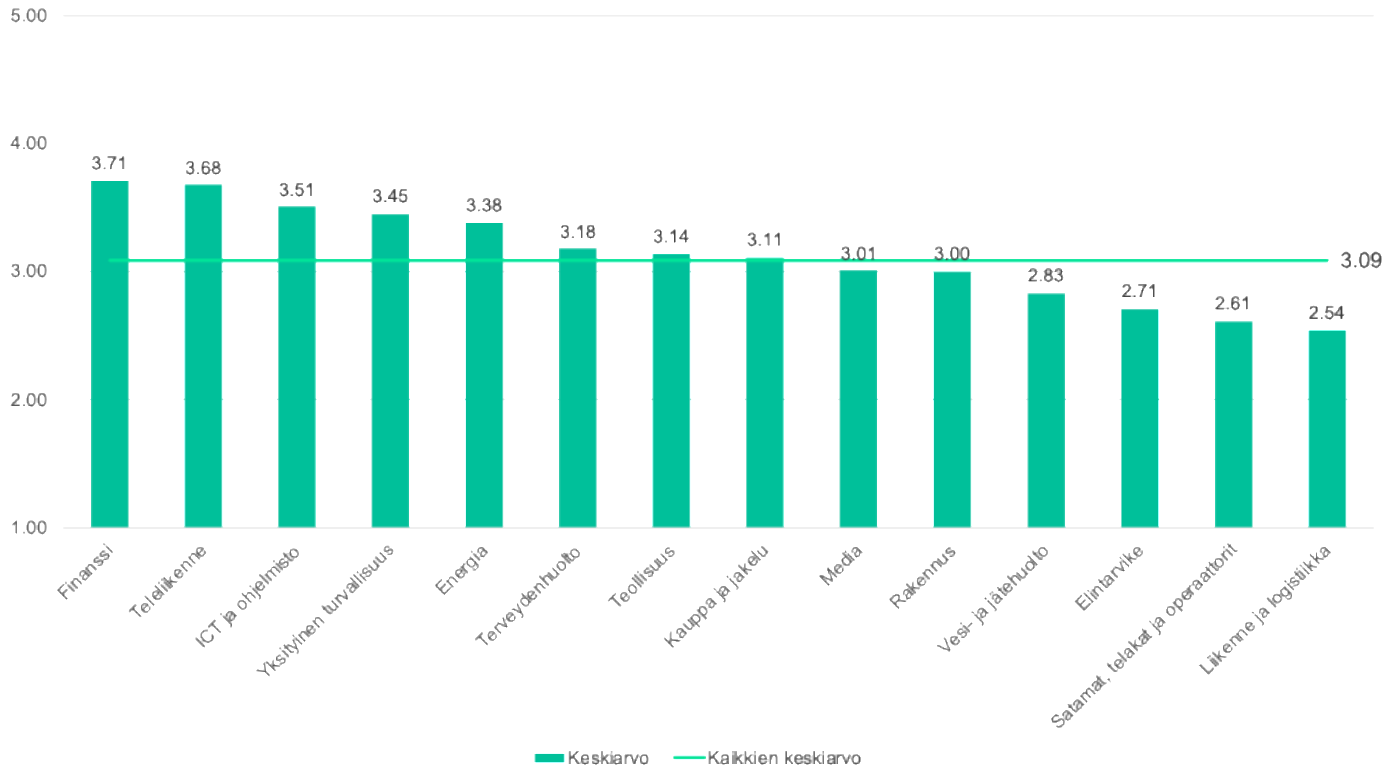
* 12 toimialaa; >120 yritystä

2025 Selvityksen Tulokset

Toimialojen vertailu

Päähavainnot

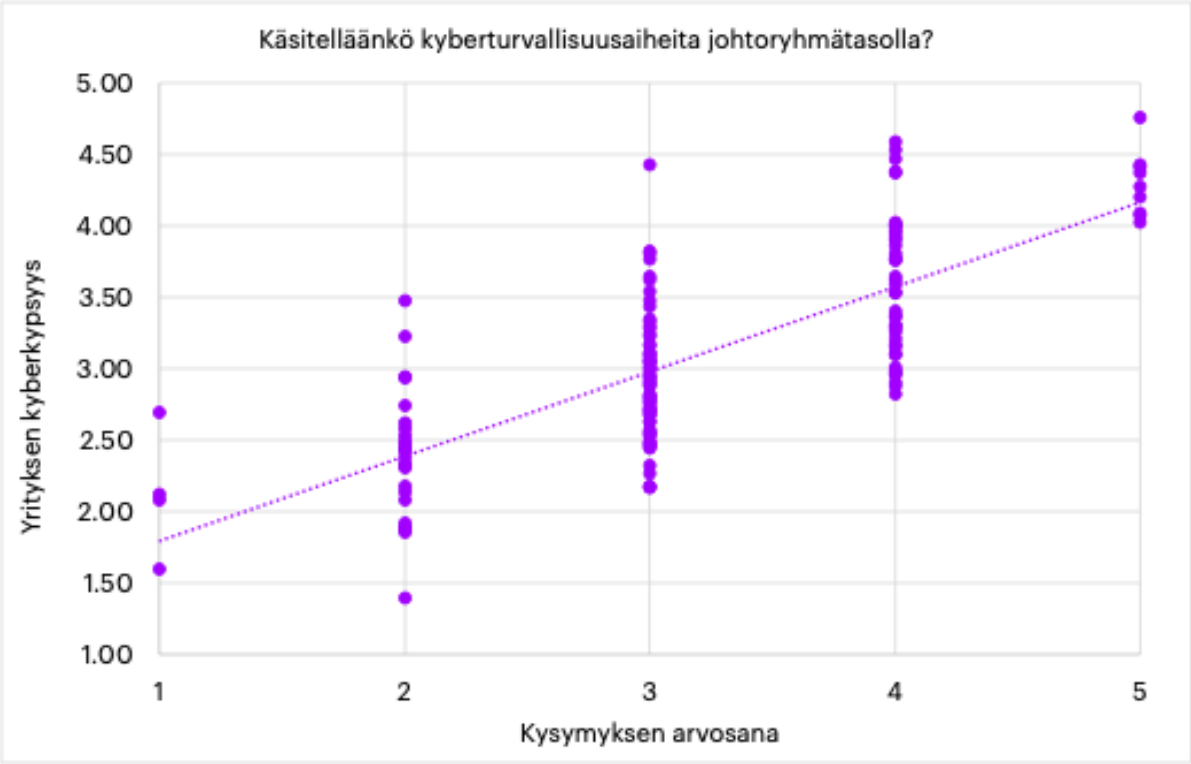
- Kriittisten toimialojen kyberkypsyys vaihtelee, mutta suurin osa ylittää perustasona pidetyn 3.00
- Vahvasti säännellyt toimialat menestyvät vertailussa parhaiten
- Erot ovat pääasiassa yrityskohtaisia ja jokaiselta toimialalta löytyy sekä korkeamman että matalamman kypsyystason yrityksiä
- Matalammilla kypsyystasoilla keskimääräistä enemmän pieniä ja keskisuuria yrityksiä
- NIS2-direktiivi ja sen kansallinen toimeenpano ovat käynnistäneet paljon kehitystoimia, erityisesti hallinnan systematisoinnissa, riskienhallinnassa ja toimitusketjujen kartoittamisessa – sääntelyn vaikutuksia kyberkypsyyteen liian aikaista arvioida



Otanta:

- Selvityksessä arvioitiin 14:sta kriittisen toimialan kyberkypsyyttä.
- Mukana on 146 yritystä pienistä suuryrityksiin, jotka ovat kriittisiä huoltovarmuuden tai yhteiskunnan kriisinkestävyyden kannalta. Yritykset toimivat maantieteellisesti kaikkialla Suomessa.

Yritysten välisiä kypsyyseroja selittävät tekijät



Kypsyyttä nostavat

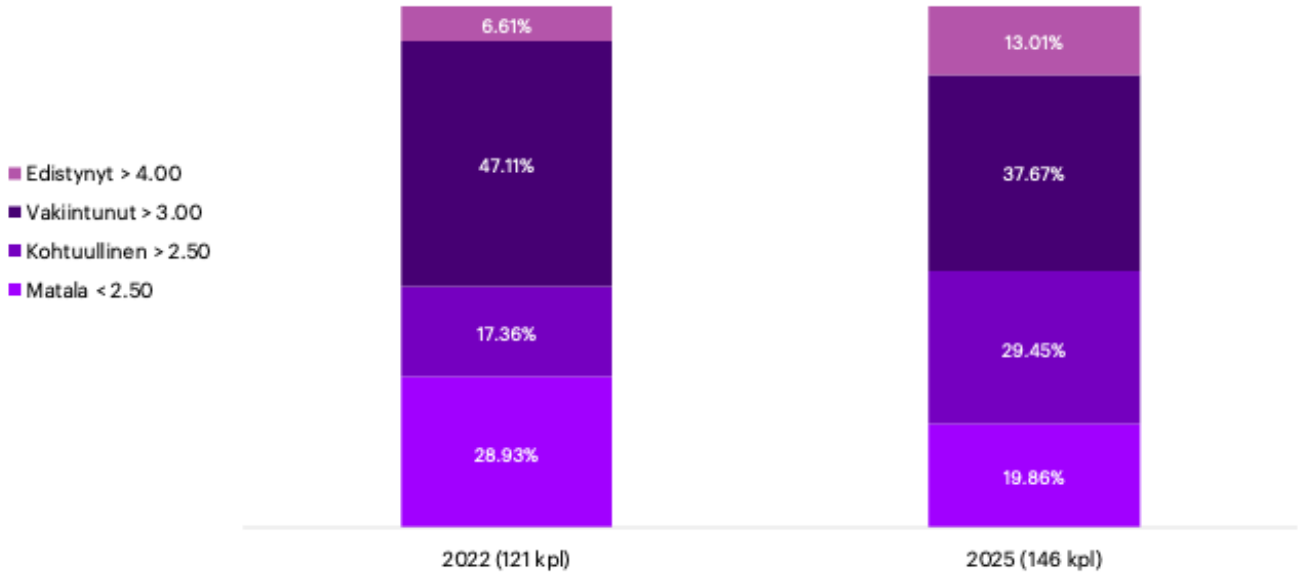
- Ylin johto käsittelee strategisen tason kybertilannekuvaa sekä merkittävimpiä kyberriskejä ja niiden hallintatoimia
- Jatkuvan poikkeamien havainnointi- ja reagointikyvyn ylläpito – monitasoinen ja ympärivuorokautinen valvontakyvykkyys
- Aktiivinen kyberresilienssin testaus harjoittelemalla eri tasoisten poikkeamatilanteiden hallintaa

Kypsyyttä laskevat

- Kirjaamattomat prosessit, jotka vähentävät toiminnan säännöllisyyttä, määrämuotoisuutta ja mitattavuutta
- Puutteet kyberturvallisuuteen liittyvässä henkilöresursoinnissa sekä avainhenkilöriskit
- Teknisen toteutuksen taso jää epäselväksi ilman säännöllisiä testaus- ja harjoittelukäytäntöjä

Muutos vuonna 2022 tehtyyn selvitykseen

”Vaikka yksittäisiä positiivisia kehityssuuntia on havaittavissa, kokonaisuutena toimialojen kyberkypsyystaso on pysynyt pitkälti ennallaan, eikä merkittävää edistystä ole havaittavissa uhkatilanteen kiristymisestä huolimatta.”



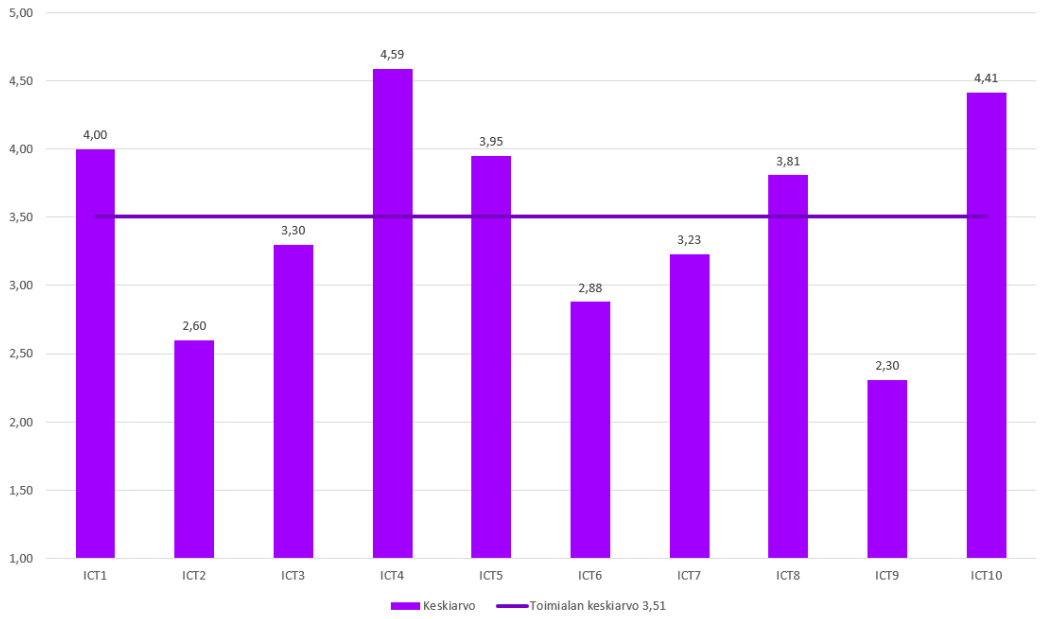
Päähavainnot

- Kaikkien toimialojen keskiarvo on noussut hieman (0.09) vuodesta 2022
- Haasteet resurssoinnissa ja kyberosaamisen niukkuudessa jatkuneet vuodesta 2022
- Vuoden 2022 tavoin vahvuudet ja kehityskohteet ovat edelleen lähinnä yrityskohtaisia, sillä saman toimialan sisällä voi olla täysin eritasoisia toteutuksia
- Yleisimpinä heikkouksina on vuoden 2022 tapaan häiriötilanteiden harjoittelun vähäisyys, riskienhallinta ja etenkin kolmansien osapuolten riskienhallinta
- Teollisuus- ja tuotantoympäristöjen (OT) hallinnan eriytyneisyys jatkuu kyberkypsyyttä laskevana trendinä sellaisilla toimialoilla, joita se koskee

Toimialakohtaisia havaintoja – ICT ala

Vertailu 2022–2025

- Vuoden 2025 ICT-toimialan kyberkypsyys on keskiarvoltaan 3,51, mikä on hieman laskenut vuoden 2022 tasosta 3,67.
- Riskienhallinta on kehittynyt, kun kyberriskit liitetään yhä useammin osaksi liiketoiminnan muuta riskienhallintaa, vaikka osa toimijoista painottaa edelleen asiakas- ja regulaatiovaatimuksia.
- Kolmansien osapuolten riskienhallinta on edistynyt NIS2-vaatimusten myötä, mutta seurantatoimenpiteet ja elinkaarenhallinta ovat edelleen haasteita.
- Henkilöstön kehittäminen on ainoa osa-alue, jonka keskiarvo on noussut.
- Heikoin osa-alue on tilannekuva, jossa valvonta ja tiedon hyödyntäminen johdon päätöksenteossa ovat edelleen puutteellisia. Kokonaisuutena kehitystä ohjaavat asiakas- ja regulaatiovaatimukset, mutta resurssien rajallisuus voi hidastaa pienempien toimijoiden kyvykkyyksien kehittämistä.



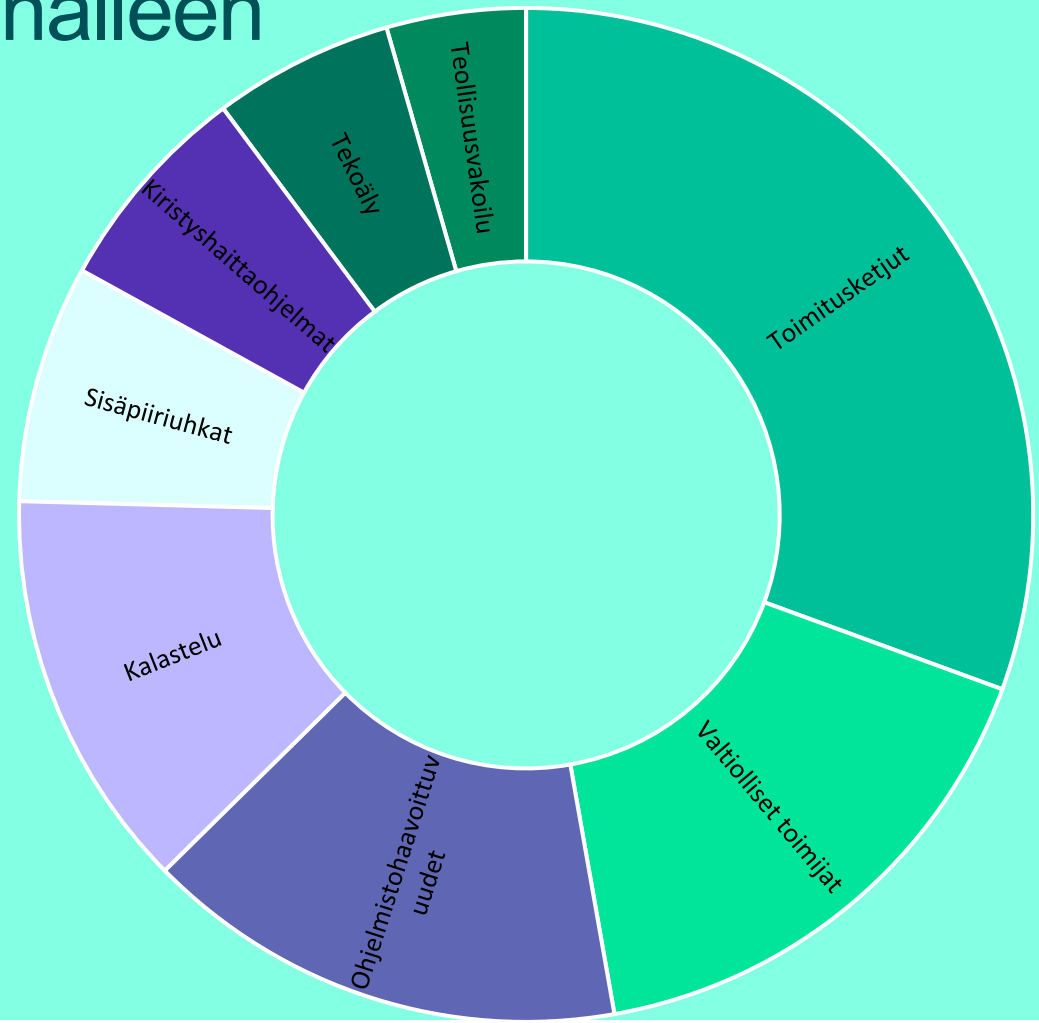
Alan Kehityskohteita

- Tilannekuvan muodostamisessa kehittämistarpeet liittyvät etenkin valvonnan kattavuuteen, ajantasaisen tiedon kokoamiseen ja sen hyödyntämiseen päätöksenteon tukena.
- Osalla toimijoista uhkatiedon hyödyntäminen on vielä satunnaista tai rajoittuu yksittäisiin lähteisiin. Sovellusturvallisuuteen tulisi kiinnittää lisää huomiota, sillä se on toimialan ydintoimintaa ja vain osalla yrityksistä turvallinen sovelluskehitys on huomioitu kattavasti.
- Riskinäkökulmasta myös kumppaniverkoston hallinnasta löytyi organisaatioilta kehitettävää esimerkiksi sopimusvaatimusten lisäämisen ja niiden säännöllisen päivittämisen osalta. Lisäksi tietoturvan toteutumisen seuranta ja auditointikäytäntöjen laajentaminen tukevat ketjun hallittavuutta ja läpinäkyvyyttä. Kehittämistarpeita havaittiin myös kyberhäiriön- ja jatkuvuudenhallinnan sekä testaamisen alueella. Prosesseja ja palautumissuunnitelmia on usein laadittu, mutta niiden testaaminen kaipaa osassa yrityksistä systemaattisuutta.

Kyberuhkat

Kyberuhkat tai –uhkatoimijat, joita selvitykseen vastanneet pitävät merkityksellisinä liiketoiminnalleen

- Selvitykseen osallistuneita yrityksiä pyydettiin nimeämään haastatteluhetkellä omalle liiketoiminnalleen merkittävimmät kyberuhkat*
- Uhkat on esitetty ympyräkaaviossa siten, että suurempi alue kertoo useamman yrityksen pitävän kyseistä uhkaa yhtenä merkittävimmistä
- Osallistujat eivät asettaneet uhkia kriittisyysjärjestykseen eikä niiden lukumäärää rajattu
- Kyberuhkien merkittävyys vaihtelee huomattavasti sen mukaan, mitä yritys tekee ja millä toimialalla se toimii



*Ympyräkaavioon on nostettu kahdeksan useimmin toistunutta kyberuhkaa tai –uhkatoimijaa kaikkien toimialojen haastatteluista

Johtopäätökset

Selvitysaineistoista on nostettavissa kolme pääteemaa

1. Kyberuhkatietoisuus jatkaa kehittymistään, mutta konkreettiset toimet jäävät jälkeen

Organisaatioiden kyberuhkatietoisuus on kasvanut ja johdon tietoisuus uhkista vahvistunut, mutta erityisesti matalamman kypsyystason yrityksissä kehitystä hidastavat resurssi- ja rakenteelliset puutteet sekä kyberturvallisuuden eriytyminen liiketoiminnasta.

2. Kyberriskienhallinnan kehitys on epätasaista, eikä sen tuottamaa tietoa kyetä hyödyntämään päätöksenteossa

Kyberriskienhallinnan taso vaihtelee merkittävästi eri toimialojen ja yritysten välillä. Korkeammalla tasolla se on liiketoimintalähtöistä ja arkipäiväistä, kun taas erityisesti PK-sektorilla riskienhallinta on useammin satunnaista tai reaktiivista.

3. Häiriötilanteisiin varautuminen on ottanut harppauksen eteenpäin

Valtaosa yrityksistä on laatinut varautumissuunnitelman ainakin kriittisille palveluille ja monissa yrityksissä suunnitelmien laatiminen on myös johtanut konkreettisiin toimenpiteisiin. Kehitys on kuitenkin usein reaktiivista, ei ennakoivaa, ja harjoittelua tehdään edelleen vain vähän.

Kyberuhkatietoisuus jatkaa kehittymistään, mutta konkreettiset toimet jäävät jälkeen

Päähavainnot

- Jo edellisellä selvityskierroksella vuonna 2022 havaittiin, että turvallisuusympäristöön vaikuttavat tapahtumat nostavat ainakin hetkellisesti organisaatioiden kyberturvatietoisuutta
- Kasvanut tietoisuus ei kuitenkaan edelleenkään näy yritysten arjen toimintamalleissa
- Yksi syy on, että monet matalamman tason yritykset arvioivat houkuttelevuuttaan hyökkäyskohteena varsin kapeasti
- Yrityksissä, joissa riippuvuus digitaalisista järjestelmistä on matalampi, taustalla saattaa olla tietoinen päätös rajata kyberturvallisuusinvestointeja, koska häiriöitä ei arvioida kriittiseksi uhkaksi
- Varautumisessa huomio ei kohdistu oman tai asiakkaiden tiedon suojaamiseen

”Verkostoituneessa yhteiskunnassa yksittäisen yrityksen korkea kypsyystaso ei riitä, vaan toimitusketjujen heikkoudet altistavat kaikki kyberuhkille.

Riski kasvaa entisestään, jos yritysten valmiustaso pääsee eriytymään”

Kyberriskienhallinnan kehitys on epätasaista, eikä sen tuottamaa tietoa kyetä hyödyntämään päätöksenteossa

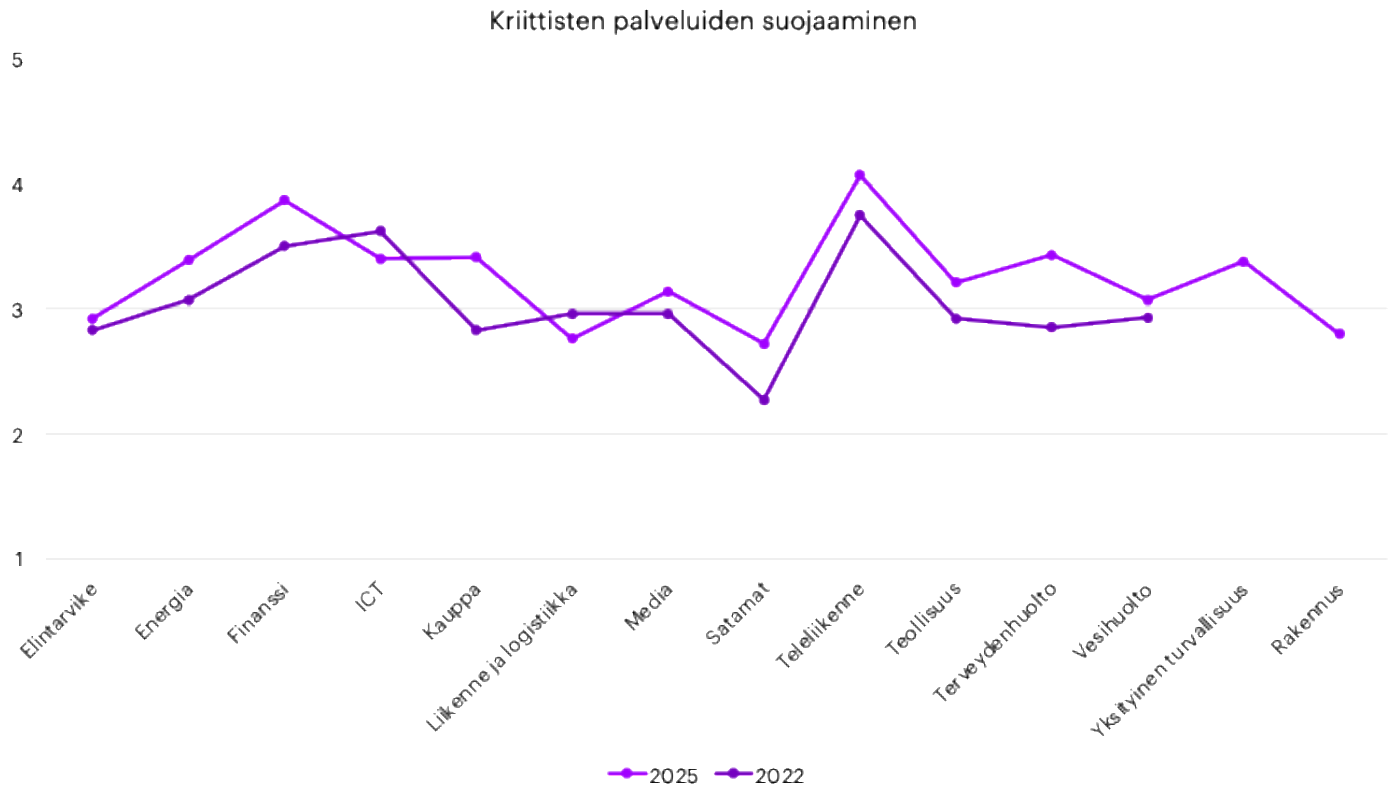
Päähavainnot

- Yritysten välisissä tuloksissa on merkittävää hajontaa kyberriskienhallinnassa
- Korkeammalla tasolla yritykset tekevät systemaattista ja kattavaa kyberriskienhallintaa sekä operatiivisella että strategisella tasolla
- Parhaimmillaan yrityksen johto on ottanut kyberriskien seurannan luonnolliseksi osaksi liiketoiminnan riskienhallintaa
- Matalammilla tasoilla kyberriskienhallinta puuttuu kokonaan tai sitä tehdään satunnaisesti, reaktiona jo toteutuneisiin uhkiin
- Kolmansien osapuolten riskienhallinta on selvityksessä kartoitetuista osa-alueista heikoin, vaikka 80 % selvitykseen osallistuneista yrityksistä on tunnistanut toimitusketjut yhtenä keskeisenä kyberuhkana

Häiriötilanteisiin varautuminen on harpannut eteenpäin

Päähavainnot

- Vaikka yleisessä kyberkypsyyden tasossa ei ole nähtävissä merkittävää nousua, yritysten varautuminen häiriötilanteisiin on lisääntynyt
- Valtaosa yrityksistä on laatinut varautumissuunnitelman ainakin kriittisiksi tunnistamilleen palveluille ja tehnyt konkreettisia varautumistoimenpiteitä (varavoima, tietoliikenneyhteyksien kahdennukset yms.)
- Kyberhäiriötilanteiden harjoittelua tehdään vielä verrattain vähän
- Yhteiskunnallisilla harjoituksilla on suuri merkitys erityisesti pienissä ja keskisuurissa yrityksissä, joissa yhteisharjoittelu on ainoita keinoja harjoitella häiriötilanteiden hallintaa käytännössä



Suosituksia

Yhteiskunnan kybervarautumista edistävät suositukset:

1. Toimitusketjujen kyberturvallisuus on huomioitava laajemmin

Kansallinen kyberkypsyyden hidas kehitys ja yritysten valmiustason eriytyminen voi uhata kaikkia kokonaisketjun yrityksiä kypsyystasosta riippumatta. Toimitusketjujen riskien- ja kyberturvallisuuden hallinta on keskeinen kehitettävä kyvykkyys yrityksen kyberkypsyystasosta riippumatta.

2. Yhteisharjoittelu yhteiskunnallisesti ja toimialoittain on tärkeää

Yhteisharjoitukset ovat monille pk-yrityksille ainoa tapa harjoitella jatkuvuuden hallintaa. Siksi ne ovat tärkeitä paitsi näille yrityksille, myös korkeamman kypsyystason organisaatioille, jotka voivat altistua toimitusketjun kyberturvapoikkeamille.

3. Kyberturvallisuuslain toimeenpano

NIS2-direktiivin kansallisen toimeenpanon valvonnassa tulee painottaa käytännön toteutusta. Yrityksiltä on vaadittava konkreettisia todisteita kyberturvatoimien jalkautumisesta, jotta laki nostaa todellista eikä näennäistä kypsyyttä.

4. Liiketoimintajohtajille suunnattu kyberturvallisuuskoulutus

Johdon kyberuhkatietoisuuden heijastuminen käytännön kyberkypsyyteen vaatii koulutusta, joka puhuttelee kohderyhmää ja kytkee kyberturvallisuuden suoraan liiketoiminnan jatkuvuuteen ja taloudelliseen menestykseen.

Liiketoiminnan jatkuvuutta edistävät suositukset

1. Johdon osallistuminen avain kyberkypsyystason nostoon

Tukea voi edistää aktiivisella yhteistyöllä ja seurattavilla mittareilla sekä kehittämällä johdon kyberturvallisuusosaamista kohdennetuin koulutuksin.

2. Kyberturvallisuusosaamisen kehittäminen

Yritysten tulisi organisaation koosta ja toimialasta riippuen varmistaa riittävä kyberturvallisuusosaamisen taso palkkaamalla asiantuntijoita, hyödyntämällä kumppaneita sekä tukemalla työntekijöiden uudelleenkouluttautumista.

3. Kokonaisvaltainen turvallisuusjohtaminen

Monissa organisaatioissa kyberturvallisuus, teollisuus- ja tuotantojärjestelmien (OT) turvallisuus sekä fyysinen turvallisuus johdetaan erillisinä kokonaisuuksina. Yhtenäinen tilannekuva parantaa kyberriskien ja resurssien priorisointia sekä auttaa tunnistamaan laajempia vaikuttamisyrityksiä.

4. Operatiivisen kyberriskienhallinnan sisällyttäminen liiketoiminnan riskienhallintaan

Erityisesti pienissä ja keskisuurissa yrityksissä kyberriskienhallinta on vähäistä, reaktiivista ja irrallista muusta liiketoiminnan riskienhallinnasta.

Toimialojen kyberkypsyysselvitys 2025

”Selvitys osoittaa, että kansallinen kyberkypsyyden taso on kehittynyt vuodesta 2022 vain maltillisesti. Samalla teknologian ja uhkakentän murros etenee merkittävästi nopeammin kuin organisaatioiden kyky uudistua ja investoida kyberturvallisuuteen.”

TOP 3 toimialat

- Finanssiala
- Teleliikenneala
- ICT ja ohjelmisto

Kehittyvät toimialat

- Liikenne ja logistiikka
- Satamat, operaattorit ja telakat
- Elintarvike
- Vesi- ja jätehuolto

Kypsyyttä nostavat

- Johdon tuki
- Liiketoimintalähtöinen kehittäminen
- Monitasoinen ja ympärivuorokautinen valvontakyvykkyys
- Aktiivinen häiriötilanteiden harjoittelu

Kypsyyttä laskevat

- Rajattu dokumentaatio
- Kyberturvallisuusosaamisen puute ja avainhenkilöriskit
- Testaus- ja harjoittelukäytäntöjen vähäisyys tai puuttuminen

Päähavaintoja hitaasti kehittyvän kyberkypsyyden taustalla:

Kyberturvallisuus nähdään tukitoimintona, joka ei lisää liiketoiminnan arvoa → investoinnit jäävät niukoiksi

Merkittävien kyberturvapoikkeamien riskiä pidetään pienenä → investointihalukkuus kasvaa vasta uhkien realisoituessa

Liiketoimintajohdon ymmärrys kyberturvallisuudesta on vähäinen, → kehitystoimet jäävät tietoturvapäättäjien vastuulle

Kiitos!

Huoltovarmuusorganisaatio

Iskunkestävä yhteiskunta - yhdessä.

Varmuuden vuoksi.

digipooli.fi @Digipooli