Huoltovarmuusorganisaatio

TIETO 24

Tämä esitys koostaa havaintoja TIETO24- harjoitukseen osallistuvista toimialoista.

Havainnot on tehty selvityksessä, jonka Digipoolin teetti toimialojen kyberturvallisuuden tilan ymmärtämiseksi.

Antti Nyqvist

Valmiuspäällikkö, Huoltovarmuusorganisaation Digipooli, Teknologiateollisuus ry

02.10.2024

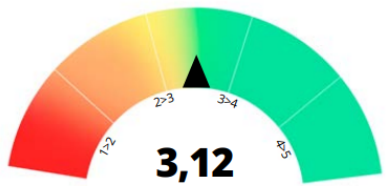
Energia

Suositukset toimialalle:

Energia-alan kypsyystaso on yleisesti hyvä. Vahva varautumiskulttuuri edistää kyberturvallisuutta. Alaan kohdistuvat uhkat ovat niin merkittäviä, että yritysten oma varautuminen ei välttämättä riitä, jolloin valtiotason ja sen ylittävien toimenpiteiden merkitys on suuri.

- OT-ympäristöjen kyberturvallisuuden hallinnan integroiminen osaksi johtamisjärjestelmää
- Kypsyystasojen hajonnan aiheuttaman riskin arviointi laajemmin toimialalla

Toimialan kokonaiskypsyys



Toimialan vahvuudet

Toimialan hyvä kokonaiskypsyys näkyy erityisesti seuraavissa osa-alueissa:

- Järjestelmällinen ja hallittu tietoturvan johtaminen, jota ohjaa liiketoiminta- ja riskitietoisuus
- Vahva kulttuuri varautumisen osalta sekä kattava jatkuvuussuunnittelu, jota tukee alan tiedonvaihto
- Pääsynhallinta, sekä fyysisten että loogisten oikeuksien osalta

Toimialan heikkoudet

Toimialan hyvästä kypsyystasosta huolimatta kehityskohteiksi tunnistettiin seuraavat:

- Alan vahva jakautuminen korkean ja matalan kypsyystason toimijoihin
- Tietoturvakulttuurin vaihteleva taso toimijoiden välillä
- Elinkaariajattelun puutteet niin kumppani- kuin identiteetinhallinnassa

Toimialan riskit ja uhkat

Merkittävimmät toimialalle tunnistetut riskit ja uhkat:

- Toimiala keskeinen vaikutusväline valtioiden välisessä vaikuttamisessa ja konflikteissa, kaikki riskit eivät yritysten hallittavissa
- Teknologian kehitys avaa integraatioita ja uhkavektoreita IT- ja OT-ympäristöjen välillä

Vertailu selvityksen 2019–2020 ja 2022 välillä

Energia-ala näyttäytyy edellisen selvityksen tavoin vahvasti jakautuneena yritysten kyberturvallisuuskyvykkyyksien sijoittuessa kypsyysasteikon kumpaankin päähän. Yhtenäistä selvityskierrosten tuloksissa on haasteet OT-turvallisuuden huomioimisessa.

Kehittyneet kyvykkyydet:

- Kyberturvallisuuden hallinta ja johtaminen
- Uhkatiedon jakaminen

Varautumiskulttuuri on perinteisesti keskittynyt tuotanto- ja jakeluhäiriöiden estämiseen ja esimerkiksi kyberturvallisuuden hallinta on jäänyt vähemmälle huomiolle. Edelliseen selvitykseen nähden tilanne on kehittynyt ja etenkin alan kypsät yritykset suhtautuvat kyberturvallisuuden kehittämiseen strategisesti ja entistä laaja-alaisemmin. Yhä useampi alan toimija kerää uhkatietoa, mutta haavoittuvuuksien hallinnassa nähdään edellisen selvityksen tavoin kehitysvaraa, etenkin matalamman kypsyyden yrityksissä.

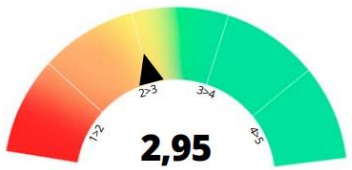
Logistiikka

Suositukset toimialalle:

Ala on jatkuvasti kehittyvä, altis kilpailulle ja herkkä toimitusketjussa tapahtuville muutoksille, jolloin kyberturvallisuuden kokonaisvaltaiseen hallintaan tulee kiinnittää erityistä huomiota.

- Tarve kokonaisvaltaiselle kyberturvallisuuden hallinnan kehittämiselle
- Tilannekuvan kehittäminen tukemaan ajantasaisen tilannekuvan muodostamista
- Tietoturvallisuuden huomioiminen kattavasti koko sovelluskehitysprosessin ajan ns. DevSecOps -mallin mukaisesti

Toimialan kokonaiskypsyys



Toimialan vahvuudet

Toimialan kokonaiskypsyys näkyy seuraavissa osa-alueissa:

- Kyberturvallisuuden vaikutusten huomioiminen liiketoimintastrategiassa
- Ymmärrys kriittisistä palveluista sekä niiden jatkuvuuden varmistaminen

Toimialan heikkoudet

Toimialan heikkoudeksi tunnistettiin seuraavat:

- Puutteet lokienhallinnan politiikkojen tai linjausten määrityksessä ja jalkautuksessa
- Järjestelmätason sekä OT-ympäristöjen valvonnan kattavuus ja varmistaminen
- Kolmansien osapuolten ja toimintojen välisten riippuvuuksien tunnistaminen

Toimialan riskit ja uhkat

Merkittävimmät toimialalle tunnistetut riskit ja uhkat:

- Erilaiset, maailmantilanteen muutoksen johdosta syntyvät uhkat näyttäytyen mm. kybertoiminnan ja hybridivaikuttamisen kasvuna
- Logistiikkaketjujen monimutkaisuus hankaloittaa niihin kohdistuvien riskien tunnistamista ja hallintaa
- Digitaalisten toimitusketjujen kasvu, altistaen uusille uhkavektoreille toimitusketjuissa

Vertailu selvityksen 2019–2020 ja 2022 välillä

Edellisestä selvityksestä poiketen vaihtelua osa-aluekohtaisissa kyvykkyyksissä nähdään merkittävästi vähemmän. Toimialan kyvykkyyserojen ollen lähinnä toimijoiden välisiä, ei osa-alueita myöskään voida järjestää vahvuuksiin ja heikkouksiin kaikkien ollessa lähes samalla tasolla.

Kehittyneet kyvykkyydet:

- Henkilöstön johtamisen ja kehittämisen osa-alue on kehittynyt tietoturvakoulutusten osalta, jotka olivat edellisen selvityksen aikaan entistä heikommin toteutettu.

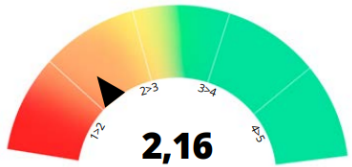
Satamat ja merenkulku

Suositukset toimialalle:

Satamat ja merenkulun toimialan kypsyystaso on matala. Erityisesti havaittu puute johdon tuessa estää mahdollisten kehitystarpeiden ja investointien tehokkaan edistämisen, joilla kyberturvallisuuden kokonaisuutta on mahdollista nostaa nykyisestä kypsyystasosta.

- Kyberturvallisuuden hallinnan kehittäminen pidemmän aikavälin strategialla, huomioiden liiketoimintalähtöisen kyberturvallisuusstrategian
- Johdon tuen lisääminen varmistamaan strategiaan pohjautuvien ja asetettujen kyberturvallisuuden tavoitteiden läpiviennin
- Kyberturvallisuusarkkitehtuuri osa-alueen kehittäminen huomioiden erityisesti selvityksessä havaitut puutteet tiedonsuojauksen prosesseihin liittyen

Toimialan kokonaiskypsyys



Toimialan vahvuudet

Toimialan matalan kokonaiskypsyyden huomioon ottaen voidaan kuitenkin havaita osa-alueita, jotka laadukkaasti kehitettyinä voivat nostaa osa-alueiden kypsyyttä seuraavalle kypsyystasolle:

- Identiteetin- ja pääsynhallinta
- Uhkien- ja haavoittuvuuksienhallinta

Yrityksillä on matalasta kokonaiskypsyydestä huolimatta hyviä käytäntöjä, joita jatkokehittämällä kokonaismaturiteettitasoa saadaan tulevaisuudessa nostettua.

Toimialan heikkoudet

Toimialan kypsyystasossa tunnistettiin seuraavat heikkoudet:

- Johdon tuen puute, estäen kehittämistarpeiden läpiviennin
- Puutteet kyberturvallisuuden hallinnan perustason määrittelyssä ja asetannassa

Toimialan riskit ja uhkat

Merkittävimmät toimialalle tunnistetut riskit ja uhkat:

- Kyberturvallisuuteen osoitettujen resurssien vähäisyys altistaa monivaikutteisille uhkille ja riskeille
- Liikenteen ja satamien häirintänä Ukrainan sodan seurauksena

Vertailu selvityksen 2019–2020 ja 2022 välillä

Satamat ja merenkulun toimialan kyberturvallisuuden tilanne ei ole merkittävästi muuttunut edellisestä, vuosina 2019-2020 toteutetusta toimialojen kyberturvallisuuden tilannekuvan selvittämishankkeesta.

Kehittyneet kyvykkyydet:

- Havaittavissa muutos tietoisuudessa ja suhtautumisessa tieto- ja kyberturvallisuuden pitkäjänteiseen kehittämiseen

Toimialaa koskettavat edelleen samat haasteet, kuten resurssoinnin vähäisyys, johdon sitoutumattomuus ja IT-palveluntuottajien kommunikoinnin puutteet. Toimialan kehittämistä tukee toimijoiden vahva sitoutuneisuus huoltovarmuusorganisaatioon. Toimialalle tämä linkki tarjoaa mahdollisuuden kehittää kyberturvallisuuden tilaa lisäämällä yhteistä tilannekuvaa ja organisoimalla yhteisiä tapoja kehittää kyvykkyyksiä.

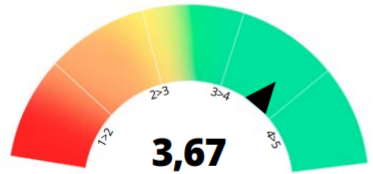
ICT ja Ohjelmistot

Suositukset toimialalle:

ICT- ja ohjelmistoalan hyvä kypsyystaso ja riskitietoisuus tuottaa nykyisellään kyvyn vastata uhkiin. Alan asema huoltovarmuuskriittisessä kokonaisketjussa ja datan käsittelijänä kuitenkin nostaa sen houkuttelevuutta kohteena ja asettaa vaatimuksen jatkuvasta kyvykkyyksien kehittämisestä. Kypsyystason kehittämiseksi suositellaan seuraavia:

- Toimitusketjujen sidonnaisuuksien tunnistaminen ja kumppanuuksien riskienhallinta laajemmin kuin suorien palveluntarjoajien osalta
- Toimialan sisäinen tiedonvaihto ja yhteinen jatkuvuusharjoittelu valtiollisten toimijoiden kyber- ja hybridiuhkien havaitsemisen ja torjumisen tueksi

Toimialan kokonaiskypsyys



Toimialan vahvuudet

Toimialan vahva kokonaiskypsyys näkyy erityisesti seuraavissa osa-alueissa:

- Kyberturvallisuuden kehittämisen priorisointi liiketoiminnan strategioissa, joka korreloi johdon tuen ja investointien kanssa
- ISO 27000 - tietoturvastandardiin pohjautuvien tietoturvallisuuden hallintamallien yleisyys

Toimialan heikkoudet

Toimialan hyvästä kypsyystasosta huolimatta kehityskohteiksi tunnistettiin seuraavat:

- Asiakasympäristöjen priorisointi ja sisäisten järjestelmien heikompi huomioiminen
- Legacy-järjestelmien suuri osuus sekä pilvisiirtymän hitaus johtuen epäselvyyksistä datan käsittelyyn liittyvästä regulaatiosta ja asiakkaiden varovaisuudesta

Toimialan riskit ja uhkat

Merkittävimmät toimialalle tunnistetut riskit ja uhkat:

- Henkilöstöön liittyvät riskit, kuten inhimilliset virheet, sisäpiiriuhkat, henkilöstön vaihtuvuus sekä osaavien kyberturvallisuusasiantuntijoiden saatavuushaasteet
- Toimitusketjuihin kohdistuvat uhkat
- Valtiollisten toimijoiden aiheuttamat kyber- ja hybridiuhkat

Vertailu selvityksen 2019–2020 ja 2022 välillä

ICT- ja ohjelmistoalan toimijoiden kehittyneet riskienhallinnan käytännöt ja jatkuvuusharjoittelu ovat vahvistaneet alan yritysten varautumisen tasoa. Toisaalta uhkatilanne on kehittynyt tai lähinnä konkretisoitunut, eli erilaiset, seuratut riskit ovat toteutuneet. Kypsyystaso on edelleen korkealla tasolla, mutta uhkaympäristön kehitys asettaa haasteita kaikille toimialayrityksille myös tulevaisuudessa.

Kehittyneet kyvykkyydet:

- Kyberriskienhallinta
- Kolmansien osapuolten riskienhallinta
- Käytännön jatkuvuusharjoittelu

Kyberriskienhallinnan käytännöt ja liiketoimintalähtöinen kyberturvallisuuden huomioiminen ovat selvästi kehittyneet edellisestä selvityksestä. Kolmansien osapuolten hallinta rajattuna suoriin kumppaneihin on myös parantunut, tosin kokonaisketjujen osalta havaittiin heikkouksia.

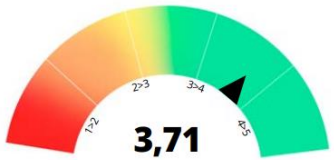
Teleliikenne

Suositukset toimialalle:

Teleliikenneala osoittaa vahvaa kypsyystasoa ja kykenee varautumisen kautta vastaamaan toimialan riski- ja uhkakenttään. Alan asema keskeisenä digitaalisen kyvykkyyksien tuottajana nostaa sen houkuttelevuutta kohteena, jolloin jatkuva kehitys ja parantaminen kyberturvallisuuden osalta on ratkaisevan tärkeää. Varautumistason kehittämiseksi nousevat seuraavat asiat esiin:

- Toimiala- ja viranomaisyhteistyön aktiivinen jatkaminen ja edelleen syventäminen
- Uhka- ja riskilähtöisen kyberturvallisuuden kehittämisen jatkaminen edelleen
- Toimitusketjujen riippuvuuksien ja kyberturvallisuuden hallinta

Toimialan kokonaiskypsyys



Toimialan vahvuudet

Toimialan vahva kokonaiskypsyys näkyy erityisesti seuraavissa osa-alueissa:

- Hyvä kypsyystaso läpi toimialan osoittaa alan varautumiskyvyn olevan korkea
- Liiketoiminta- ja riskilähtöinen kyberturvallisuuden hallinta, jolla vahva johdon tuki
- Keskeiset toiminnan turvaamisen liittyvät kyvykkyydet vahvoja kautta linjan

Toimialan heikkoudet

Toimialan heikoimmatkin kyvykkyydet ovat yli hyvän perustaso kolmen. Kriittisimmiksi kehitystoimiksi tunnistettiin:

- Kolmansien osapuolten kyberturvallisuuden hallinta
- Vaihteleva kyvykkyys kyberturvallisuuden tilannekuvan muodostamisessa toimialayritysten välillä

Toimialan riskit ja uhkat

Merkittävimmät toimialan tunnistamat riskit ja uhkat:

- Digitalisaatio ja teknologiariski, ml. pilvipalveluiden laajentuva käyttö
- Osaamisriski mm. ulkoistusten ja edelleen käytössä olevan legacy-infrastruktuurin osalta
- Kyberrikollisuuden ja -vaikuttamisen jatkuva kehittyminen ja monimuotoistuminen

Vertailu selvityksen 2019–2020 ja 2022 välillä

Vuoden 2019-20 ja 2022 selvitysten välillä Teleliikenneala on edelleen kyennyt kehittämään kypsyystasoaan. Vahvuudet edellisestä selvityksestä on kyetty säilyttämään ja erityisesti muutamia heikkouksina vuonna 19-20 mainittuja kyvykkyyksiä on parannettu, osaa merkittävästi.

Kehittyneet kyvykkyydet:

- Henkilöstön johtaminen ja kehittäminen, erityisesti kyberturvallisuushenkilöstön osaamisen kehittäminen
- Tilannekuvan kehittäminen, tietoturvavalvomo laajasti käytössä alan yrityksillä
- Omaisuudenhallinnan kehittyminen

Muut havainnot:

- Toimialan merkitys osana kansallista kyberturvallisuutta ja varautumista kohonnut geopolitiikan tapahtumien vuoksi