

# AVAIN

UUTISET • 1. 2024



<b>Pääkirjoitus</b>	
<b>Pk-barometri</b>	<b>2</b>
.....	
<b>Puheenjohtajan palsta</b>	
<b>Vaikuttamisen merkitys</b>	<b>3</b>
.....	
<b>Kolumni Tieto on valtaa</b>	<b>4</b>
.....	
<b>Intersec 2024 – Dubai</b>	<b>6</b>
.....	
<b>Milloin työnantaja saa irtisanoa?</b>	<b>7</b>
.....	
<b>Turvallisuusala päjännyt hyvin</b>	<b>8</b>
.....	
<b>Kyberturvallisuusuutisia</b>	<b>10</b>
.....	
<b>Uusi kyberturvallisuus- direktiivi – NIS2</b>	<b>11</b>
.....	
<b>Lakipalsta: Henkilötietojen säilyttäminen</b>	<b>13</b>
.....	



# Pk-yritysten suhdanneodotukset heikentyneet

Pk-yritysten suhdanneodotukset ovat laskeutuneet selvästi viime syksystä. Tähän ovat vaikuttaneet etenkin ennätysnopea korkojen nousu, heikon taloustilanteen jatkuminen sekä Venäjän Ukrainaan kohdistuvan hyökkäyssodan pitkittyminen. Pk-yritysten investointihalukkuus on edelleen vähäistä, ja kysynnän epävakaus jarruttaa kasvua. Yritykset aikovat kuitenkin yhä pitää kiinni henkilöstöstään.

Poikkeukselliset viime vuodet ja talouden nykytilanteen epävarmuus vaikuttavat suoraan pk-yritysten suhdannenäkymiin. Kevään pk-yritysbarometrissa yritysten suhdanneodotukset laskivat tuntuvasti viime syksystä. Hieman yli puolet pk-yrityksistä arvio suhdanteiden kuitenkin pysyvän samana.

Pk-yritysbarometrin eli pk-barometrin julkistavat kaksi kertaa vuodessa Suomen Yrittäjät, Finnvera ja työ- ja elinkeinoministeriö. Tällä kertaa kyselyyn vastasi noin 5052 yritystä. Vastausaika oli joulukuun 2023 puolivälistä tammikuun 2024 puoliväliin.

## Kasvuhakuisuuden laskeva trendi huolestuttaa

Pk-yritysten kasvuhakuisuus on laskenut pitkään. Tämä on selvästi nähtävissä sekä kas-

vua tavoittelevien että voimakkaasti kasvuhakuisien yritysten määrissä. Kasvuhakuiset yritykset toimivat kasvun moottoreina ja kiihittäjinä muille yrityksille. Voimakkaasti kasvuhakuisien yritysten osuus on ennätyskellisen pieni, ja pidemmän aikavälin trendinomainen lasku herättää huolta.

## Epävarmuus heikentää haluja investoida, työvoimasta pidetään kiinni

Pk-yritysten investointihalukkuus on edelleen vaatimattomalla tasolla. Kaikilla päätoimialoilla on enemmän investointeja vähentäviä yrityksiä kuin niitä, joilla investointien odotetaan lisääntyvän.

Noin joka kymmenes pk-yrityksistä aikoo lisätä henkilökunnan määrää. Sen sijaan 14 prosenttia odottaa henkilöstönsä määrän vähentyvän. Suurin joukko, 74 prosenttia pk-yrityksistä, aikoo kuitenkin säilyttää nykyisen henkilöstönsä. Myös odotukset liikevaihdon ja vakavaraisuuden kehityksestä ovat laskeneet syksyn kyselystä.

## Epävarmuus on vähentänyt ulkoisen rahoituksen käyttöä

Talouden aktiviteetin hiipuminen, sen seurauksena heikentynyt yritysten luottokelpoi-

suus ja tiukka pankkitoiminnan sääntely näkyvät pk-yritysten ulkoisen rahoituksen käytössä. Finnvera on säilynyt merkittävänä rahoitustoimijana, vaikka sen rooli pankkilainojen vaihtoehtona ja täydentäjänä on hieman laskenut. Edelleen joka viides rahoituksen hakua suunnittelevista kertoo kääntyvänsä Finnveran puoleen.

Lisäksi Finnveran takauksella on keskeinen merkitys rahoituksen saannissa. Huomionarvoista on se, että erityisesti kasvuhakuiset yritykset ovat kiinnostuneita Finnverasta rahoittajana.

## Viidennes pk-yrityksistä kartoittanut liiketoiminnan ilmastovaikutuksia

Ajankohtaisaiheena barometrissä selvitettiin myös yritysten valmiuksia ilmastomuutoksen hillintään. Hieman alle puolet pk-yrityksistä näkee ilmastomuutoksen hillitsemistoimilla olevan vaikutuksia yritystoimintaansa. Osuus on laskenut kolme prosenttiyksikköä kahden vuoden takaisesta barometrasta. Noin neljäsnes osuus pk-yrityksistä näkee ilmastomuutoksen hillitsemistoimissa mahdollisuuk-

sia liiketoiminnalle eli samoin kuin kaksi vuotta sitten.

Kasvuhakuiset pk-yritykset tunnistavat ilmastomuutoksen hillitsemistoimien vaikutukset yrityksen toimintaan muita yrityksiä useammin.



Ona Gardemeister, toimitusjohtaja

# Vaikuttamisen merkitys

Ympäröivä maailma, elinympäristö ja yritysten toimintaympäristö muuttuvat ja kehittyvät. Tässä kehityksessä meillä jokaisella on mahdollisuus olla mukana sekä vaikuttaa kehityksen suuntaan ja siihen, miltä alamme toimintaympäristö tulee tulevaisuudessa näyttämään. Koemme helposti, että meidän omat toimmemme ovat riittäviä, kun ne kohdistuvat oman yrityksen kehitykseen ja menestymiseen. Kyse on kuitenkin laajemmasta muutoksesta, jonka vuoksi vaikuttamiseen tarvitaan lisää voimaa ja yhteistyötä. Yhteistyössä on voimaa! Näen, ettei kaikkea pidä ottaa annettuna, vaan omalla toiminnallamme pystymme vaikuttamaan suuntaan, johon toimiala on menossa. Ehkä emme pysty vaikuttamaan täysin haluamamme toimialan kehitys- ja muutossuuntaan, mutta voimme kuitenkin vaikuttamisen avulla pyrkiä muuttamaan nykyistä tilannetta paremmaksi ja ajaa meille tärkeitä tavoitteita sekä saavuttaa monia merkittäviä tuloksia ja muutoksia. Meillä on yhdessä mahdollisuus vaikuttaa asioihin, edistää asioita ja viedä niitä eteenpäin. Vaikuttamalla voimme pyrkiä esimerkiksi muuttamaan alan lakeja, sääntöjä tai käytäntöjä. Voimme edistää alan koulutuksiin liittyviä asioita ja yleisesti alan kehitystä. Vaikuttaminen voi olla voimakas työkalu positiivisten muutosten aikaansaa-

miseksi. On myös hyvä muistaa, että voimme sen avulla lisätä omaa tietoisuutta tärkeistä asioista tai ongelmasta, jotka saattavat muuten jäädä huomiotta.

Yhteistyötä ja vaikuttamista voi tehdä monella tapaa. Tähän saattaa riittää muutaman yksittäisen yrityksen yhteistyö tai alan konsolidaation mukanaan tuoma vahvuus. Näissä tapauksissa vaikuttaminen voi olla kuitenkin yksipuolista ja kanavat rajallisia. Tässä Turvaurakoitsijat ry:n vahvuus tulee esiin. Turvaurakoitsijat ry koostuu 80 jäsenliikkeestä ja yli 150 toimipaikasta ja meillä on 24 yhteistoimintajäsenyritystä. Jäsenemme koostuvat muutaman henkilön pienyrityksistä satoja henkilöitä työllistäviin yrityksiin ja yhteistoimintajäsenemme pienistä tavarantoimittajista jättikonserneihin. Turvaurakoitsijat ry pyrkii edistämään turvallisuusalan kehitystä Suomessa niin itsenäisesti kuin muiden alan järjestöjen kanssa yhteistyössä mm. Turvallisuusalan Foorumin ja Turvallisuusalan neuvottelukunnan kautta. Pohjoismaisella tasolla alan kehitystä edistetään Nordkeyn ja koko Euroopan laajuisesti Euroopan Lukkoseppäliitto ELFin kautta.

Turvaurakoitsijat järjestönä ajaa koko jäsenistön etua ja valitsee painopisteensä jäsen-

ten toiveiden ja tarpeiden mukaisesti. Tämän takia jäsenyritysten aktiivisuus on ensiluokkaisen tärkeää. Uusia ideoita ja ratkaisuja ongelmiin tarvitaan ja siksi onkin tärkeää, että olette mukana jakamassa tietoa tärkeistä asioista. Ilman jäsenistön ääntä Turvaurakoitsijoiden toiminnan suunta ei välttämättä kohtaa jäsenten toiveita ja tarpeita. Vaikka vaikuttaminen ei aina takaa välitöntä tai täydellistä muutosta, se on silti aina tehokas tapa edistää muutoksia ja tuoda esiin tärkeitä kysymyksiä. Vain osallistumalla voit vaikuttaa! Jatkuva sitoutuminen ja ponnistelut tuovat ajan myötä merkittäviä tuloksia meille kaikille.

Turvaurakoitsijat Ry:n vuosikokous järjestetään tänä vuonna Tampereella 11.4. hotelli Tornissa. Päivä koostuu vuosikokouksesta, yrityksiin kohdistuvien rikoksiin ja väärinkäytöksiin keskittyvästä seminaariesityksestä, sekä vanhaan tapaan yhteistoimintajäsenten tuote- ja palveluesittelystä. Ilta vietetään Tampereen Teatterissa Agatha Christien Idän pikajunan arvoituksen parissa. Ilmoittautuneita on tällä hetkellä yli 80. Jos et ole vielä ilmoittautunut, mutta tapahtuma kiinnostaa, niin ota yhteyttä Onaan sillä lisäpaikkoja saadaan varmasti järjestettyä vielä.

**Nähdään Tampereella.**

**Jyri Aho,**  
puheenjohtaja

# TIETO ON VALTAA

Voiko poliisille kertoa, että etsitty henkilö on sairaalahoitossa? Voiko passirekisterin tietoja käyttää törkeän rikoksen selvittämiseen? Miten poliisi voi hyödyntää laajoja tietomassoja? Tiedon käyttämiseen liittyviä kysymyksiä ja tiedonvaihdon haasteita ratkotaan nyt usean hankkeen voimin.

Englantilaisen yleisneron Sir Francis Baconin paljon siteerattu lausuma ”tieto on valtaa” on luonnollisesti irrotettu asiayhteydestään, kun sillä tavanomaisesti kuvataan tietoyhteiskunnan keskeisintä polttoainetta, tietoa. Bacon tarkoitti lauseellaan muuta. Ajat ovat toiset, eikä Baconilla voinut olla elinaikanaan 1500- ja 1600-luvulla aavistustakaan digitalisaatiosta.

Poliisi elää ja muuttuu yhteiskunnan mukana. Tietoa tarvitaan rikosten selvittämiseen ja vaarallisten tekojen estämiseen, viime kädessä myös yhteiskuntajärjestyksemme turvaamiseen. Ne ovat poliisin lakisääteisiä tehtäviä. Menetelmiä ovat esimerkiksi kotietsintä, telekuuntelu, televalvonta sekä tekninen kuuntelu, katselu ja seuranta.

## Tiedon hankkimisesta tiedon käyttämiseen

Kun koko yhteiskunta on kyllästetty tiedolla, tärkeää ei ole enää vain tiedon hankkiminen. Tärkeää on se, miten laillisesti hallussa olevaa tietoa saa käyttää.

Olennaisia kysymyksiä ovat tietomassan käsittely ja analysointi. Tärkeätä on myös tietojen turvallinen säilyttäminen ja tiedon tarvisijoille toimittaminen. Uudet uhkakuvat ovat nostaneet keskeiseksi kysymykseksi myös sen, miten laajasta tietomassasta löydetään ne pienet poikkeukset, joilla on merkitystä.

## Viranomaisetkin suojelevat yksityisyyttäsi

Jokainen meistä tekee arjessa valintoja sen suhteen, paljonko antaa vapaaehtoisesti tietojaan eri palveluntuottajille. Lisäksi altistumme erilaiselle tietojen kalastelulle. Osa toiminnasta on rikollista. On selvää, että kyse on kaiken aikaa myös yksityisyyden suojasta.

Meillä Suomessa viranomaisilla on lakisääteinen velvollisuus edistää perusoikeuksien toteutumista. Turvallisuus on perusoikeus, samoin yksityisyyden suoja. Samalla, kun poliisikin tarvitsee uutta tietoa tehtäviensä hoitamiseen, on kaiken tiedonhankinnan perustuttava oikeusvaltiossa lakiin. Tästä emme voi tinkiä, emmekä tingi.



On keskeistä huomata myös se, että kaikki eivät pelaa yhteisten pelisääntöjen mukaan. Rikolliset pyrkivät kiertämään kaiken sääntelyn. Maailmassa on myös valtiollisia toimijoita, joita yksityisyyden suoja koskevat säännökset eivät juuri rajoita.

## Yhteiskunnan on päätettävä rajanvedoista

Ollaan monessa kohdin vedenjakajalla. Tietotekninen kehitys on ollut niin nopeaa, että lainsäädännön on ollut vaikeaa pysyä kehityksessä mukana. Tekoälyn käyttö on tästä hyvä esimerkki. Euroopan unionissa on juuri valmistumassa yhteiset pelisäännöt tekoälyn käytölle.

On myös perinteisempiä asioita, joissa yhteiskunnan on tarpeen määritellä pelisäännöt. Missä määrin terveydenhoidon toimijoilla olevia hyvin luottamuksellisia terveystietoja ja poliisin hallussa olevia uhkakuvia voidaan ajaa yhteen? Voiko poliisille kertoa, että etsitty henkilö on sairaalassa hoidossa? Saako poliisi kertoa kaavoituksesta vastaavalle viranomaiselle, että rakennushankkeen takana on moottoripyöräjengin kerhotila?

Joiltakin osin on epäselvää sekin, saako poliisi käyttää sillä laillisesti olevia tietoja jonkin ilmiön analysoimiseen. Toisentyypinen kysymys on se, voiko viranomaisella laillisesti olevia tietoja saada käyttää toiseen käyttötarkoitukseen, kuten passirekisterin tietoja törkeiden rikosten selvittämiseen. Lähtökohteisesti tietoja voi käyttää vain alkuperäisen käyttötarkoituksen mukaisesti.

Avoimia kysymyksiä on lukuisia. Sen takia sisäministeriössä yhteistyössä muiden ministeriöiden kanssa selvitetään näitä kysymyksiä eri hankkeissa. Käynnissä on rikostiedusteluhanke, passirekisterin biometrisiä tietoja koskeva hanke sekä sisäministeriössä ja muuallakin valtioneuvostossa useita tiedonvaihtoa viranomaisten välillä koskevia hankkeita.

Tieto todella on valtaa. Samalla on hyvin tärkeää, että yhteiskunta piirtää rajan esimerkiksi rikostorjunnan tehokkuuden ja yksityisyyden suojan välille. Viime kädessä eduskunta asettaa tasapainon eri perusoikeuksien välille.



**Tomi Vuori**  
Poliisiosaston osastopäällikkö



# Taitotalo – innostuksesta osaamiseen!

Hyvä lukkoseppä/turvasuojaaja on asiakaspalvelun ammattilainen, jolta asennus- ja huoltotyöt sujuvat. Hyvällä lukkosepällä on laaja tietämys lukitus- ja turvallisuustekniikasta, lainsäädännöstä ja määräyksistä.

**Lukitus- ja turvajärjestelmäasentaja,  
sähkö- ja automaatioalan ammattitutkinto**  
aloitus syksyllä 2024

**Lukkoseppämestari,  
sähkö- ja automaatioalan erikoisammattitutkinto**  
aloitus 16.10.2024

Tutustu myös näihin koulutuksiin

**Tulityökoulutus yrityksille**

**Työturvallisuuskorttikoulutus yrityksille**

**Ensiavun peruskurssi**

**Turvallisuusvalvojan erikoisammattitutkinto**

KYSY LISÄÄ  
Jussi Venäläinen  
050 430 8281  
jussi.venalainen@taitotalo.fi

TAITOTALO  
Valimotie 8, 00380 Helsinki  
asiakaspalvelu@taitotalo.fi  
asiakaspalvelu 010 80 80 90

TAITOTALO

LUE LISÄÄ  
[taitotalo.fi/  
turvallisuuskoulutus](https://taitotalo.fi/turvallisuuskoulutus)





# Dubain Intersec 2024

**Dubain kansainväliset turvallisuusalan messut Intersec 2024 järjestettiin jo 25. kerran tammikuun puolivälissä entisestään laajentuneessa messukeskuksessa.**

Messuvieraita oli noin 47.500 yli 140 maasta kolmen messupäivän aikana tutustumassa noin 45.000 neliömetrin suuruiseen messualueeseen. Näytteilleasettajia oli yli tuhat ja he edustivat kuuttakymmentä maata, ensikertalaisia näytteilleasettajista oli neljännes. Messuilla oli myös 11 maapaviljonkia, jotka yhdistivät pk-yrityksiä, teknologiaa ja palveluntarjoajia eri puolilta maailmaa.

Intersec on selkeästi vakiinnuttanut asemansa turvallisuusinnovaatioiden lansee-

rauslustana viimeisten 25 vuoden aikana ja juhlavuonna oli tarjolla valtava määrä erilaisia seminaareja, työpajoja, tietoiskuja ja esityksiä, joissa käsiteltiin viimeisimpiä trendejä, haasteita ja uutuuksia eri turvallisuuden osa-alueilla.

Messujen kattaus oli todella laaja ja koostui viidestä eri kokonaisuudesta, joita olivat yritysturvallisuus, kyberturvallisuus, viranomais-toiminta, työ- ja terveysturvallisuus sekä palo- ja pelastusturvallisuus.

Monilla osastoilla oli tarjolla valvontatuotteita ja ratkaisuja, joita ei meille edes esitelty, kun kuultiin, että olimme Euroopasta, koska GDPR estää niiden myymisen täällä.

Kiinalaiset yritykset olivat palanneet messuille runsaslukuisesti koronapandemian jäl-

keen ja niitä olikin lukumääräisesti eniten, suomalaisista yrityksistä näytteilleasettajana oli Kaso Oy.

Seminaareissa korostettiin turvallisuusalan valtavia kasvumahdollisuuksia, jotka hyödyttävät niin loppukäyttäjiä kuin koko alaakin. Ongelmana on se, että turvallisuusala on kuitenkin edelleen hajanainen. Markkinoilla nähdään kuitenkin myös enemmän avoimuutta esimerkiksi valmistajien halukuutta kertoa enemmän visiostaan ja strategioistaan ja tehdä yhteistyötä.

Turvallisuusmaiseman muutoksia ei voi jättää huomiotta, varsinkin kun turvallisuustilanne ympäri maailmaa on merkittävästi muuttunut ihan lyhyen ajan sisällä. Olemme nähneet organisaatioiden turvallisuustarpei-

den ja -halujen muuttuvan vuosien saatossa. Sen lisäksi, että markkinoilla tapahtuu paljon muutoksia, myös toimialalla tunnustetaan, että muutos on tapahtumassa.

Helsingin ELF 2023 tapahtumassakin puhuneen **Lee Odessin** järjestämässä kaksipäiväisessä seminaarissa koko alan trendit ja tulevaisuus maalattiin loistavien esimerkkien saatelemana. Leen omassa esityksessä muistutettiin alamme olevan digitaalisen murroksen keskellä ja tämän positiivisesta vaikutuksesta yrityksille, jotka näkevät osoittajan ja nimittäjän muuttuneen ja osaavat hyödyntää tätä. Myös turvallisuusalalla niin pilvipalvelut kuin mobiilius raivaavat tietä tekoälyn käytölle.







Siirrytään lukitsemisesta ja pääsynhallinnasta kulkemisen helppouteen ja käyttäjäkokemuksen tärkeyteen.

Luonnollisesti tässä muutoksessa on voittajia ja häviäjiä, tärkeää on yritysten kyky toimia muutoksen keskellä ja uskallus hypätä uuteen ja tuntemattomaan. Muutos luo myös uusia yhteistyömahdollisuuksia alan yrityksille, joiden pitäisi myös ajatella luovasti, jotta muutos onnistuu mahdollisimman hyvin. Toki kaikkea vanhaa ei voi unohtaa, vaan se kulkee uuden rinnalla. Mitä olisimme valmiita uhraamaan uuden tieltä ja mitä emme?

Fokuksen siirtäminen ihmisestä ovelle ja nyt takaisin ihmiseen vaatii aivan toisenlaista ajattelua, suunnittelua ja kommunikointia.

Viestinnässä ja innovaatioissa pitäisi olla

kyse siitä, miten voimme lopulta tarjota erilaisia turvallisuuden tasoja vaivattomasti, koska mobiili- ja pilvipalveluiden hyödyntämisen läpimurto ja innovaatio ovat kääntäneet perinteisen arvolupauksemme pitää väärät ihmiset ulkona siihen, että oikeat ihmiset, kuten sinä, pääsevät sisään. Tärkeässä roolissa tulevat olemaan eri järjestelmien integraatiot, jotka mahdollistavat ihmisten saumattoman kulun yhdellä tunnisteella tarvitsemiinsa tiloihin ja resursseihin paremman käyttökokeemuksen saamiseksi.

Turvallisuusala voi hallita tätä turvallisuuden ja mukavuuden kohtaamista ja hyödyntämättömän lisäarvon luontia. Mutta tarvitaan tuoreita ideoita, innovaatioita ja johtajuutta, jotta sitä voidaan täysin hyödyntää.



## Tuotannolliset ja taloudelliset irtisanomisperusteet – milloin työnantaja saa irtisnoa?

Työsopimuslain mukaan työnantaja saa irtisnoa työsopimuksen, kun tarjolla oleva työ on vähentynyt taloudellisista, tuotannollisista tai työnantajan toiminnan uudelleenjärjestelyistä johtuvista syistä olennaisesti ja pysyvästi, eikä työnantajalla ole muuta työtä tarjolla. Käytännössä irtisanomisperusteena on usein toiminnan uudelleenjärjestely, kuten organisaatiomuutos tai tietyn toiminnan lopettaminen tai toimintojen yhdistäminen, ja näistä syistä työ loppuu tai olennaisesti vähenee osalla työntekijöistä.

Laissa ei ole säännöksiä siitä, miten työnantajan on valittava työn vähenemisen vuoksi irtisanottavat työntekijät. Lähtökohtaisesti irtisanominen on kuitenkin kohdistettava siihen työntekijään, jonka työ on tosiasiallisesti vähentynyt. Irtisanottavan korvaaminen toisissa tehtävissä työskentelevällä työntekijällä ei yleensä ole sallittua.

Sen sijaan, jos samoissa tehtävissä työskentelee useampi työntekijä, työnantaja voi valita irtisanottavat suhteellisen vapaasti, kunhan valintaa ei tehdä epäasiallisilla tai syrjivillä perusteilla tai työnantajaa mahdolli-

sesti velvoittavan työehtosopimuksen mukaisen irtisanomisjärjestyksen vastaisesti. Työehtosopimuksen mukaisen irtisanomisjärjestyksen noudattamatta jättäminen ei kuitenkaan tee irtisanomisesta laitonta, mutta voi johtaa hyvityssakkoon.

Myös tuotannollisin ja taloudellisin perustein tapahtuvaa irtisanomista koskee työsuopimuslain 7 luvun 1 §:ssä säädetty yleinen asiallisen ja painavan syyn vaatimus. Tämä tarkoittaa muun muassa sitä, että irtisanottavan valinta ei saa tapahtua epäasiallisilla tai syrjivillä perusteilla. Irtisanottavaa työntekijää ei siten saa valita esimerkiksi sukupuolen, raskauden tai perhevapaoikeuden käyttämisen taikka henkilön iän, terveydentilan tai seksuaalisen suuntautumisen perusteella.

Syrjivällä tai muutoin epäasiallisella perusteella tapahtuva irtisanottavan valinta tekee irtisanomisesta laittoman ja työnantaja on velvollinen suorittamaan työntekijälle korvusta työsuhteen perusteettomasta päättämisestä sekä mahdollisesti myös tasa-arvolain tai yhdenvertaisuuslain mukaista hyvitystä.

# Turvallisuusala pärjännyt hyvin toimintaympäristön muuttuessa

**Turvallisuusjärjestö Finnsecurityn vuosittain teettämän suhdannekatsauksen mukaan yksityisellä turvallisuusalalla niin kysyntä kuin tarjontakin ovat kasvaneet pandemiakriisin jälkeen. Myös turvallisuusalan yritysten lähiajan odotukset poikkeavat optimismillaan kotimaisen yrityskentän keskimääräisistä suhdanne-odotuksista.**

Alan kokonaisliikevaihdon voimakas kasvu ei kuitenkaan korreloi suoraan kannattavuuden kanssa, koska tuotantokustannukset ovat samalla nousseet.

Koko Suomen yrityskenttään verrattuna paljon suurempi osuus katsoo turvallisuusalalla kysyntätilanteen pysyvän ennallaan, eli kohtuullisen myönteisenä. Tätä selittää se, että monet turvallisuustuotteet ja -järjestelmät ovat asiakasyrityksissä ja -yhteisöissä niin sanottuja välttämättömyshyödykkeitä.

Niiden kysyntä on vähemmän riippuvaista suhdannevaihteluista tai lyhytaikaisista kriiseistä.

## **Turvajärjestelmien kysyntä ei erityisen suhdanneherkkää**

Suhdannekyselyn mukaan kysynnän määrän odotetaan olevan 2024 aikana parasta tietoturvatuotteissa (tuotteet, palvelut, ohjelmistot ja järjestelmät), oviautomaatiikassa ja tieto-

turvakoulutuksessa. Tätä mieltä oli kahdeksan kymmenestä vastanneista.

Yli puolet vastanneista uskoi, että kysynnän taso on hyvää myös sähköisissä lukitusjärjestelmissä, kameravalvontajärjestelmissä, etävalvontatuotteissa (järjestelmien tilan valvonta), hälytyskeskuspalveluissa sekä portti- ja puomiautomaatiikassa.

## **Tietoturva- ja paloriskit kärkihuolina**

Turvallisuusalan asiakaskyselyihin vastanneista kolme neljästä piti tietoturvallisuutta koskeviin uhkiin varautumista tärkeänä. Toiseksi tärkeimpänä turvallisuus- ja onnettomuusuhkana pidettiin toimitilojen paloturvallisuutta. Kolmannella sijalla olivat toimitilojen vesi- ja kosteusvahingot.

## **Innovaatioihin ja digitalisaatioon panostetaan**

Turvallisuusalan vuoden 2023 suhdannekyselyn mukaan yritystoiminnan keskeisiä kehittämistarpeita olivat laadunvalvonta, erottautuminen kilpailijoista sekä digitaalisen ympäristön hyödyntäminen liiketoiminnassa.

Näitä asioita pitivät erittäin tärkeinä tai tärkeinä kaikki vastanneet. Seuraavaksi tärkeimmät kehittämistarpeet koskivat henkilöstön kehittämistä, toimitusvarmuutta ja saavutettavuutta, palvelujen ja tuotteiden hinnoit-

telua sekä tarjouslaadinnan osaamista. Näitä piti erittäin tärkeänä yli 90 prosenttia vastanneista.

## **Kysyntää laadukkaasta ja ammattitaitoisesta työvoimasta**

Suhdannekyselyyn vastanneista vain neljä kymmenestä oli sitä mieltä, että ammattitaitoisen työvoiman saatavuus ja laatu yltävät edes kohtalaiselle tasolle, kun kaikki ammatitilat otetaan huomioon. Näkemykset tässä evät ole muuttuneet parin vuoden takaisesta kyselystä.

Turvallisuusalan ammatillisen tutkinnon ja AMK-tason tutkinnon suorittaneiden määriä ja työllistymistä sekä koulutuksen vetovoimaa tarkasteltiin seikkaperäisesti turvallisuusalan vuoden 2020 suhdanne- ja toimialaraportissa. Silloin erityistä huomiota kiinnitettiin ammatillisen koulutuksen kehittämiseen, koska ammatillisen koulutuksen uudistus ei ole kailta osin onnistunut.

Myös vuoden 2023 kyselystä kävi ilmi, että yli 40 prosenttia vastanneista ei ollut tyytyväinen ammatillisen koulutuksen ja työelämän vastaavuuteen.

## **Pandemia keskeytti kasvukehityksen**

Vuosina 2007–2019 vartiointi- ja turvallisuuspalveluiden liikevaihto oli Suomessa lähes kaksinkertaistunut ja henkilöstö kasvanut yli

50 prosenttia. Sen jälkeen liikevaihdon määrä on vähentynyt parilla ja henkilöstö kymmenellä prosentilla.

Turvallisuusalalla kasvuyritysten osuus on ollut perinteisesti suuri 2010-luvun alkuun ulottuvan mittaushistorian aikana. Vuonna 2023 voimakkaasti kasvuhakuisten yritysten osuus kuitenkin aleni selvästi ja aikaisempaa suurempi osa on tyytynyt säilyttämään asemansa, jos tilannetta verrataan pandemiaa edeltävään aikaan.

## **Maailmantilanteen epävarmuus heijastuu arvioista**

Asiakaskyselyihin vastanneet suhtautuvat lähitulevaisuuden turvallisuuskehitykseen hien myönteisemmin kuin viime vuosien toteutuneeseen kehitykseen. Vain kahdeksan prosenttia uskoi turvallisuustilanteen heikenevän seuraavan parin vuoden aikana.

Vajaa puolet arveli turvallisuustilanteen paranevan, joskin uudet haasteet, sumea taloustilanne ja epävarmuus tulevaisuudesta voivat hidastaa kehitystä. Liki yhtä suuri osuus oli sitä mieltä, että turvallisuustilanne pysyy ennallaan.

*Vuoden 2023 kyselyihin osallistui kaikkiaan 162 yritystä ja yhteisöä. Suhdanneraportin laati tutkija Pekka Lith Finnsecurity ry:n toimeksiannosta.*



# Kiinteistösi avaimeton tulevaisuus



dormakaban monipuolisesta ja laajasta tuotevalikoimasta löydät juuri sinulle sopivimman turvallisen mekaanisen tai elektro-mekaanisen lukitusratkaisun, joka kehittyy käyttöolosuhteiden vaatimusten mukaan.

Ota yhteyttä,  
autamme suunnittelussa!  
[www.dormakaba.com](http://www.dormakaba.com)

## Suojattu avain

dormakaba expert plus -avain on suojattu vuoteen 2033.

## Avaimeton kiinteistö

Kokonaisvaltainen, joustava kulunvalvontaratkaisu. Modulirakenteen ansiosta järjestelmä voidaan räätälöidä tarpeen mukaan. Mahdollistaa kustannustehokkaan dormakaba evolo -lukkojen käytön osana järjestelmää, koska ne eivät vaadi erillistä kaapelointia. Tuo tehokkuutta elinkaarikustannusten hallintaan.

## Yksi sähköinen avain kaikkialle

Älykäs, paikallinen kuluvalvontajärjestelmä, jonka laaja ovyksikkövalikoima sekä käytön helppous ja joustavuus vakuuttavat ominaisuuksillaan. Myös mekaaniset lukitusjärjestelmät ovat laajennettavissa kulunvalvonnaksi, joka voidaan integroida osaksi laajempaa on line -kulunvalvontajärjestelmää. dormakaba evolo on skaalattavissa käyttöympäristön mukaan.

**dormakaba** 



# Kyberturvallisuusuutisia

## Erilaisia rekrytointihuijauksia liikkeellä

Kyberturvallisuuskeskus on viime aikoina saanut ilmoituksia erilaisista rekrytointiin liittyvistä huijaustapauksista. Huijaukset eivät ole johtaneet varsinaisiin vahinkoihin, mutta ilmiö on mielenkiintoinen. Kyberturvallisuuskeskukselle voi ilmoittaa, mikäli vastaanotatte tai havaitsette rekrytointiin viittaavia huijauksia.

### Rekrytointihuijauksia on ollut monenlaisia:

- Esiintyminen esimerkiksi organisaation henkilöstöhallinnon nimissä, ja potentiaalisten hakijoiden lähestyminen.
- Organisaatioiden nimissä on tehty verkkopalveluun avoimia työpaikkailmoituksia, joita ei oikeasti ole olemassakaan.
- Kansalaiset ovat vastaanottaneet erilaisia työtarjouksia esimerkiksi WhatsAppin välityksellä.
- Organisaatioille on tullut poikkeuksellisen paljon hakemuksia avoimiin työpaikkailmoituksiin.
- Roskapostiltakaan ei ole välttytty; myös erilaisia koneellisesti tehtyjä viestejä on lapioitu avoimiin paikkoihin kottikärry-kaupalla.

## Tarkkana liitetiedostojen kanssa!

Vastaanotamme liitetiedostoja monien palveluiden kautta. Yleisesti yhdistämme liitetiedoston sähköpostiin, mutta niitä voi saapua esimerkiksi erilaisten verkkolomakkeiden tai palveluiden kautta. Organisaatiot ovat varautuneet esimerkiksi sähköpostitse tuleviin liitetiedostoihin tarkastamalla automaattisesti erilaisin suojautumismenetelmin liitetiedoston laatua. Osa haitallisista viesteistä päätyykin automaattisesti karanteeniin tai liite poistetaan matkalla ennen saapuneet-kansiota.

Huijarit osaavat naamioida liitetiedoston tai mahdollisesti paketoita sen toisen tiedoston sisään. Tällöin tiedosto saattaa tulla läpi erilaisten turvatoimien käyttäjän sähköpostiin tai palveluun tarkasteltavaksi. Tässä vaiheessa käyttäjien valvotuneisuus ja organisaation sisäinen tietoturvakoulutuksen laatu astuu esiin.

Liitetiedoston avulla voidaan levittää esimerkiksi haittaohjelmia, jotka pahimmassa tapauksessa voivat johtaa kiristyshaittaohjelmaan tai lievempiin tietoturvapoikkeamiin. Virustorjuntaohjelmistot saattavat myös asettaa liitetiedoston avanneen työaseman

karanteeniin, jolloin työasema voidaan joutua uudelleenasettamaan.

### Neuvoja liitetiedostojen varalle:

- Tarkastele sähköposti ja pohdi onko se liitetiedostoinen aito.
- Älä klikkaa esimerkiksi Office-liitetiedostoja tai .zip-paketteja auki automaattisesti.
- Kysy tarvittaessa kaverilta tai organisaation tietoturvasta vastaavalta henkilöltä liitetiedoston laadusta.
- Laatikaa organisaatiossa ohjeistus, miten liitetiedostojen kanssa tulee menetellä, mikäli niitä työtehtävissä tulee käsitellä.
- Älä hyväksy makroja tai muita liitetiedoston kysymiä lupia ilman varmuutta asiasta.
- Pidä tärkeät tiedostot tallessa sen varalta, mikäli liitetiedosto saastuttaa tietokoneen.
- Varmuuskopiot on syytä pitää ajan tasalla ja saatavilla myös niissä tapauksissa, missä työasema tai koko ympäristö saastuu liitetiedoston mukana tulleen haittaohjelman seurauksena.

Organisaation on hyvä olla tietoisia järjestelmistä, joista voidaan lähettää liite työntekijöiden käsiteltäväksi. On syytä testata, mitä tiedostoja on mahdollista välittää ja tämän jälkeen tehdä tarvittavia kovennuksia tietoturvan parantamiseksi. Kaikkia liitetiedostomuotoja ei ole syytä hyväksyä, ja on syytä laatia prosesseja niiden käsittelyyn.

Koulutus, kartoitus ja valppaus tulevat halvemiksi kuin kyberpoikkeama!



# NIS2

**NIS2 on Euroopan unionin uusi kyberturvallisuudsdirektiivi, jonka tarkoituksena on parantaa ja yhtenäistää koko EU:n kyberturvallisuuden tasoa. NIS2 korvaa aiemman NIS-direktiivin laajentaen huomattavasti sen vaatimuksia ja soveltamisalaa. Uuden direktiivin saattaminen osaksi kansallista lainsäädäntöä on tehtävä viimeistään 17.10.2024. Direktiivin vaatimukset koskettavat useita organisaatioita, ja valmistautuminen kannattaa aloittaa hyvissä ajoin.**

## Mitä toimialoja NIS2 koskee?

Direktiivi koskee automaattisesti kaikkia kriittisten toimialojen toimijoita, jotka työllistävät vähintään 50 henkilöä ja joilla on yli 10 miljoonan euron liikevaihto. Lisäksi direktiivi ulottuu koskemaan kaikkia toimijoita, jotka on kansallisesti määritelty kriittisiksi, riippumatta niiden koosta. Toimialat on jaettu kriittisiin ja muihin kriittisiin toimialoihin tarkemman määrittelyn ja seurannan vuoksi.

### Kriittisiä toimialoja:

- Pankki- ja finanssiala
- TVT-palvelun hallinta
- Energia
- Liikenne
- Avaruus
- Digitaalinen infrastruktuuri
- Julkishallinto
- Vesihuolto
- Terveystieteiden huolto.

### Muita kriittisiä toimialoja:

- Elintarvikeala
- Posti- ja kuriiripalvelut
- Jätehuolto
- Digitaaliset palvelut
- Kemikaalisektori
- Tutkimustoiminta
- Valmistava teollisuus.

## Mitä vaatimuksia NIS2 asettaa?

NIS2:n myötä vaatimukset riskienhallintatoimenpiteistä sekä olennaisten ja tärkeiden kokonaisuuksien raportoinnista kiristyvät. Direktiivin mukaan jokaisen EU:n jäsenvaltion on varmistettava, että eri toimijat toteuttavat teknisiä, toiminnallisia ja organisatorisia toimenpiteitä verkkojen ja tietojärjestelmien turvallisuuden kohdistuvien riskien hallitsemiseksi.

### Hallinnon vastuu

Direktiivi asettaa toimijoiden hallinnon vastuuseen organisaation kyberturvallisuusriskien hallintatoimenpiteistä, raportointivelvoitteista sekä kyberturvallisuuden toteutuksesta direktiivin vaatimalla tasolla. Vastuu mahdollistaa hallinnolle tietoon perustuvan päätöksenteon. Direktiivin asettamia vaatimuksia eri toimijoiden hallinnolle ovat muun muassa seuraavat:

- Kyberturvallisuusstrategian määrittely
- Kyberturvallisuusriskien hallintatoimenpiteiden hyväksyntä ja valvonta
- Velvollisuus osallistua kyberriskienhallinnan koulutukseen.

Hallintoa voidaan asettaa henkilökohtaisesti vastuuseen direktiivin velvoittamien kyberturvallisuusriskien hallintatoimenpiteiden rikkomisesta.

## Kyberturvallisuusriskien hallintatoimenpiteet

Direktiivin vaatimien kyberturvallisuusriskien hallintatoimenpiteiden tulee olla riski- ja suorituskykyperusteisia, eli niiden tason määrittämisessä täytyy huomioida muun muassa toimijoiden erilainen altistuminen riskeille sekä toimijan koko. Hallintatoimenpiteiden vaatimukset tarkentuvat direktiivissä, mutta ne sisältävät ainakin seuraavat:

- Riskianalyysit
- Tietojärjestelmien turvallisuuspolitiikat
- Liiketoiminnan jatkuvuuden ja kriisien hallinta
- Toimitusketjujen ja toimittajien turvallisuuden varmistaminen
- Kyberhygieniakäytännöt ja kyberturvallisuustietoisuus
- Tietoturvahäiriöiden käsittely ja raportointivelvoitteet
- Verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus
- Pääsynhallintaperiaatteet
- Omaisuudenhallinta
- Haavoittuvuuksien hallinnan periaatteet
- Henkilöstöturvallisuus
- Tiedon salauksen ja kryptografian periaatteet.

## Tietoturvahäiriöiden raportointivelvoite

Toimijoiden on raportoitava tietoturvahäiriöstä, joka vaarantaa tiedon saatavuuden, aitouden tai eheyden valvovalle viranomaiselle.

Aikarajat ja vaatimukset viranomaisilmoituksessa ovat seuraavat:

- 24 tunnin kuluessa on tehtävä ennakoilmoitus viranomaiselle, kun tieto häiriöstä on ensimmäisen kerran saatu
- 72 tunnin kuluessa on tehtävä ilmoitus viranomaiselle sisältäen tiedon häiriöstä, sen vakavuudesta ja vaikutuksista
- 1 kuukauden kuluessa on toimitettava häiriön loppuraportti.

# NIS2



# HENKILÖTIETOJEN SÄILYTTÄMINEN

Henkilötietojen säilyttämisen osalta on tärkeää ymmärtää Euroopan unionin yleisen tietosuoja-asetuksen (GDPR) asettamat vaatimukset ja periaatteet. Yritykset, jotka toimivat rekisterinpitäjinä, kohtaavat velvoitteita varmistaessaan, että henkilötietoja käsitellään lainmukaisesti, oikeudenmukaisesti ja läpinäkyvästi. Seuraavaksi keskeisiä vaatimuksia ja parhaita käytäntöjä henkilötietojen säilyttämiseen liittyen.

## Henkilötietojen säilytysajan suunnittelu ja perustelu

GDPR edellyttää, että rekisterinpitäjät säilyttävät henkilötietoja vain niin kauan kuin se on tarpeen tietojen käsittelyn tarkoituksia varten. Tämä tarkoittaa, että yritysten on arvioitava ja perusteltava henkilötietojen säilytysaikoja tapauskohtaisesti. Perusteluissa tulee ottaa huomioon muun muassa: Tietojen keräämisen ja käsittelyn tarkoitus, lakisääteiset velvoitteet, kuten kirjanpitolakiin perustuvat säilytysajat, yhtiön liiketoiminnan asettamat vaatimukset, sekä myös asiakassuhteiden mahdollisen päättymisen jälkeiset tarpeet, kuten reklamaatio-oikeudet.

## Dokumentointivelvoite ja osoitusvelvollisuus

Yritysten on dokumentoitava säilytysaikojen arviointiprosessit ja säilytysajat tavalla, joka mahdollistaa GDPR:n vaatimusten noudattamisen osoittamisen tarvittaessa esimerkiksi

niitä valvovalle viranomaiselle. Tämä osoitusvelvollisuus edellyttää, että yritykset pitävät kirjaa siitä, miten ne ovat päätyneet tiettyihin säilytysaikoihin, mukaan lukien käytetyt perusteet ja harkinnat. Suojatoimien on katettava niin tekniset kuin organisatoriset toimenpiteet, joilla taataan erityisesti tietojen minimoinnin periaatteen noudattaminen. Minimoinnin periaate edellyttää myös mahdollisimman lyhyttä säilytysaika. Henkilötietoja ei saa käsitellä, jos tarkoitukset on mahdollista toteuttaa anonyymeilla tiedoilla.

## Henkilötietojen poistaminen tai anonymisointi

Kun henkilötietoja ei enää tarvita alkuperäiseen tarkoitukseensa tai lakisääteisiin vaatimuksiin nähden, ne tulee joko poistaa tai anonymisoida siten, että henkilöt eivät ole enää tunnistettavissa. Yritysten on varmistettava, että niiden tietojärjestelmät ja prosessit mahdollistavat tietojen asianmukaisen poistamisen tai anonymisoinnin säilytysajan päättyessä.

GDPR antaa rekisteröidyille laajat oikeudet omiin tietoihinsa, mukaan lukien oikeus tulla unohdetuksi. Tämä tarkoittaa, että henkilö voi vaatia tietojensa poistamista tietyissä tilanteissa ennen säilytysajan päättymistä.

## Poikkeukset säilytysajoille

GDPR sallii henkilötietojen säilyttämisen alkuperäistä käyttötarkoitusta pidempään erityis-

tilanteissa, kuten yleisen edun mukaista arkistointia, tieteellistä tai historiallista tutkimusta tai tilastollisia tarkoituksia varten, kunhan noudatetaan asetuksen suojatoimia. Tämä edellyttää muun muassa, että tietojen minimointia ja mahdollisimman lyhyttä säilytysaika koskevat periaatteet toteutetaan.

## Tietosuojavaltuutetun linjaus

Tietosuojavaltuutettu on antanut ohjeistuksen henkilötietojen säilyttämisestä, joka toimii tärkeänä ennakkotapauksena GDPR:n periaatteiden soveltamisen ymmärtämiseksi tietyissä konteksteissa. 19. maaliskuuta 2021 tarkastellussa tapauksessa todettiin, että yksityisen pysäköintisakon yhteydessä kerätyt henkilötiedot, mukaan lukien ajoneuvosta otetut valokuvat ja pysäköintimaksuilmoitus, eivät täyttäneet kirjanpitolainsäädännössä viitattuja säilytyskriteereitä (erityisesti Kirjanpitolain säännökset kirjanpitoon tarvittavien asiakirjojen säilyttämisestä). Tietosuojavaltuutettu korosti, että ainoastaan rekisterinpitäjän kirjanpitovelvoitteiden mukaisiin kirjauksiin sisältyvät henkilötiedot voidaan säilyttää Kirjanpitolain määrittelemän ajan. Muita kuin näihin kriteereihin sopimattomia tietoja ei tulisi säilyttää mainitun lainsäädännön perusteella. Linjaus soveltuu muillekin toimialoille, eli ylimääräinen tieto tulee pyrkiä poistamaan mahdollisimman nopeasti.

Lisäksi valtuutettu korosti avoimuuden tärkeyttä koskien tietojen säilytysaikoja, kuten

Yleinen tietosuoja-asetus (GDPR) vaatii. Kun tietoja ei ole kerätty suoraan kyseiseltä henkilöltä, rekisterinpitäjän on informoitava henkilöä tietojen säilytysajasta tai, jos se ei ole mahdollista, käytetyistä kriteereistä tämän ajan määrittämiseksi. Kyseisessä tapauksessa todettiin, että rekisterinpitäjän tietosuojaseloste oli riittämätön, sillä siinä todettiin vain, että tietoja säilytetään lain vaatiman ajan ilman, että säilytysaika tai sen määrittämiseen käytettyjä kriteereitä oli määritelty.

Turvaurakoitsijalla voi olla perusteita säilyttää tietoa alan erityisten kriteerien nojalla, mutta ne kriteerit on syytä kirjata tietosuojaselosteeseen ja tarvittaessa konsultoida asiantuntijaa.

## Yhteenveto

Henkilötietojen säilyttäminen yrityksessä vaatii huolellista suunnittelua, dokumentointia ja perustelua. Yritysten on arvioitava säilytysaikoja säännöllisesti ja varmistettava, että ne ovat GDPR:n vaatimusten mukaisia. Lisäksi on tärkeää toteuttaa asianmukaiset toimenpiteet henkilötietojen poistamiseksi tai anonymisoinniksi, kun niitä ei enää tarvita. Näin yritykset voivat varmistaa, että ne kunnioittavat tietosuojavaatimuksia.



# Kokonaisratkaisu turvallisuuden ja kulkemisen hallintaan

Vie organisaatiosi tehokkuus, kulkemisen hallinta ja turvallisuus uudelle tasolle ja hyödynnä koko potentiaalisi **ABLOY OS** -kulunvalvonta- ja **PROTEC<sup>2</sup> CLIQ** -lukitusratkaisulla.

Kokonaisratkaisun avulla valjastat eduksesi Abloyn mekaanisen ja elektronisen osaamisen parhaat puolet ja hallitset kulkuoikeuksia, lukkoja, kulkutunnisteita ja koko turvallisuuden infrastruktuuria yhdestä ja samasta selainpohjaisesta käyttöliittymästä.

Lue lisää ja pyydä tarjous lähimmältä ABLOY- valtuutetulta lukkoliikkeeltäsi:  
[abloy.fi](http://abloy.fi)



# ABLOY