

AVAIN

UUTISET • 3.2025



Pääkirjoitus Tilaukoulutus ajaa turva-alan ahtaalle	2
Puheenjohtajan palsta Turvaurakoitsijat jäsenten ja toimialan tukena	3
Työturvallisuus – osa ammattitilpeyttä	5
NIS2-direktiivi tulee	7
Kyberturvallisuus 2025	8
Tekoäly ja turvallisuus- järjestelmät	10
PK-yrityksen varautuminen – kilpailukyky kriiseissä	11
Palkka-avoimuusdirektiivi ja sen vaikutukset	12
Lakipalsta Työlainsäädäntö elää	13

Tilauuskoulutus ajaa turva-alan ahtaalle

Yksityinen turva-ala on kriisin partaalla. Valtion suunnittelemat uudistukset voivat romahduttaa lakisääteisen koulutuksen saatavuuden – ja viedä yrityksiltä toimintaedellytykset.

Vuodenvaihteessa on tarkoitus poistaa valtionosuusrahoitteinen henkilöstökoulutus ja korvata se tilauuskoulutuksella. Mallissa yritykset voisivat tilata tarvitsemansa koulutuksen itse. Ajatus kuulostaa ensi kuulemalta houkuttevalta: se antaisi vapautta ja mahdollisuuden räätälöidä koulutusta ammatillisen koulutuksen säädösten puitteissa. Vapaus kuitenkin maksaa liikaa.

Tilauuskoulutuksen kustannukset näyttävät jäävän kokonaan yritysten maksettaviksi ja nousevan nopeasti kohtuuttomiksi. Yhden vastaavan hoitajan koulutus voi jatkossa maksaa yritykselle vähintään 7400 euroa – summa, joka monelle pienelle toimijalle on yksinkertaisesti mahdoton. Kun koulutusta ei pystytä toteuttamaan, vaarantuu koko alan osaamisen kehittäminen ja yritysten mahdollisuus toimia elinkeinoluvan mukaisesti.

Lain (LYTP) mukaan jokaisessa turva-alan yrityksessä on oltava vähintään yksi vastaava hoitaja. Hänellä tulee olla suoritettuna turvallisuusvalvojan tai lukkoseppämestarin erikoisammattitutkinto. Kyse ei ole paperinpyö-

rityksestä: ilman pätevyyden suorittanutta vastaavaa hoitajaa yritys menettää elinkeinolupansa.

Ongelma syvenee, koska Suomessa ei ole lukitus- ja turvajärjestelmäasentajille perus-

koulutusta. Alan osaaminen rakentuu ammatillisten tutkintojen ja perinteisen mestarikisälli -mallin varaan. Turvaurakoitsijat ry:n jäsenyrityksissä noin 60 prosenttia henkilöstöstä on suorittanut ammatti- tai erikoisammatti-

tutkinnon. Kun nämä työntekijät eläköityvät tai siirtyvät muihin tehtäviin, tarvitaan uusia osaajia tilalle. Tutkinnot eivät vain tuo uusia osaajia alalle – ne pitävät myös nykyiset työntekijät motivoituneina ja koko alan elinvoimaisena.

Tilanne vaikeutuu entisestään, sillä valtio on vähentänyt kouluttajan saamaa valtionosuutta toisen tutkinnon suorittavilta. Tämä tekee opilaitoksille vähemmän kannattavaksi kouluttaa henkilöitä, joilla on jo aiempi tutkinto – vaikka juuri heistä moni hakeutuu turva-alalle.

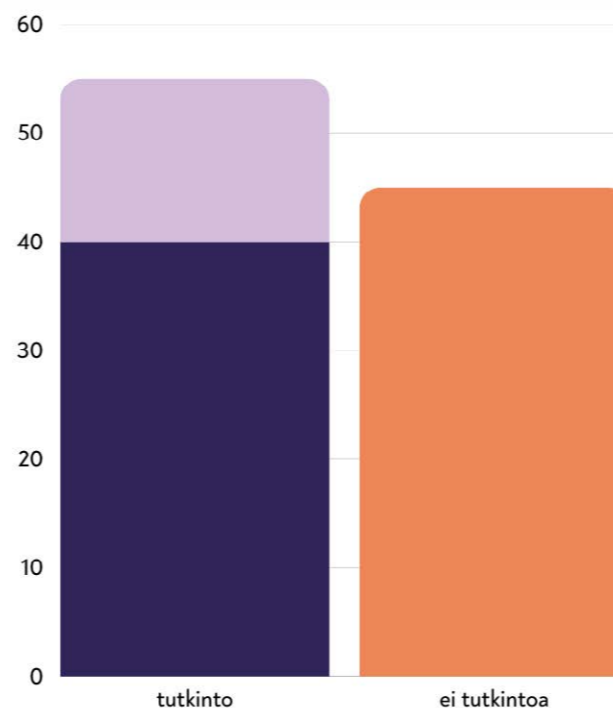
Turvaurakoitsijat ry haluaa nostaa nämä epäkohdat esiin, jotta koulutusmalleja ja niiden rahoitusta voitaisiin vielä kehittää yhteistyössä. Vain näin voidaan varmistaa, että Suomi säilyttää huoltovarmuutensa ja yhteiskunnan kokonaisturvallisuuden – ja että yksityiset turva-alan yritykset voivat jatkossakin toimia lain edellyttämällä tavalla.

Olisi koko alamme kannalta erittäin tärkeää, että päättäjät löytäisivät tähän ongelmaan ratkaisun – sillä ilman osaajia yksityinen turva-ala ei voi turvata yhteiskuntaa.

*Ona Gardemeister,
toimitusjohtaja*

Turvaurakoitsijat ry:n jäsenyritysten henkilöstön koulutustausta (toukokuu 2025)

● ammattitutkinto ● erikoisammattitutkinto ● ei tutkintoa



Turvaurakoitsijat ry

– jäsenten ja toimialan tukena muuttuvassa markkinassa



Jyri Aho, puheenjohtaja

Paljon on vettä virrannut Vantaanjoessa siitä, kun Suomen Lukkoseppäliikkeiden liitto perustettiin vuonna 1970. Järjestön idea oli valvoa ja suojella lukkoseppien yhteisiä ammattietuja. Ajateltiin, että yhdessä olemme enemmän ja sitä kautta päästään vahvemmin vaikuttamaan lukkoseppiä koskeviin asioihin. Perustamisvaiheessa jäsenenä oli 26 lukkoseppäliikettä. Näistä ajoista järjestö ja sen jäsenistö on mukautunut ja muuttunut ajan hengessä sekä asiakkaiden tarpeiden mukana

Vuosien saatossa lukkoseppien työ laajeni perinteisestä lukituksesta monipuoliseen turvatekniikkaan. Vuonna 1994 nimi muutettiin kuvaamaan tätä kehitystä paremmin: syntyi Suomen Turvaurakoitsijaliitto. Vuonna 2019 nimi hiottiin nykyiseen muotoonsa, Turvaurakoitsijat ry.

Vuonna 2004 järjestössä puhalsivat uudet tuulet, kun jäsenistön toiveena oli tehdä enemmän yhteistyötä alan muiden toimijoiden kanssa, perinteiset kumppanit olivat siihen asti olleet Abloy, Primo ja Björkboda, joista kaksi jälkimmäistä valmistsivat tuotteita Abloylle. Kyseisenä vuonna hyväksyttiin 11

uutta yrityskumppania ja näin syntyi käsite yhteistoimintajäsen. Tämä oli merkittävä uudistus, sillä suuri osa yrityksistä toimi esimerkiksi kulunvalvonnan, automaation sekä ohjelmistojen kanssa. Tänä päivänä meillä on 28 yhteistoimintajäsentä, joista alkuperäisiä on yrityskauppojen jälkeen mukana vielä kahdeksan, sekin kertoo omaa tarinaansa alan konsolidaatiosta.

Vuonna 2019 saavutettiin merkittävä virstanpylväs jäsenkunnan kehityksessä: ensimmäistä kertaa mukaan liittyi yritys, jonka toiminta ei liity lukitukseen, vaan yksinomaan turvatekniikkaan keskittyvä Secureplan Oy. Tämä trendi on sittemmin vahvistunut ja varmasti jatkuu myös tulevaisuudessa. Tällä hetkellä lähes 10 % jäsenistä edustaa muuta kuin perinteistä lukitusalan toimijaa. Yhteistoimintajäsenten osalta muutos näkyy vielä vahvemmin – noin 70 % niistä tarjoaa jotakin muuta kuin lukitustuotteita.

Jäsenten ja yhteistoimintajäsenten muuttunut rooli kuvaa koko alan kehitystä. Muutosta ohjaavat asiakkaiden tarpeet sekä tekniikan kehittyminen ja yleistyminen. Meidän tehtävämme on pysyä tässä muutoksessa

mukana ja varmistaa, että jäsenemme saavat parhaat mahdolliset työkalut tulevaisuuden mahdollisuuksiin tarttumiseen. Toivottamme tervetulleiksi kaikki uudet jäsenet ja yhteistoimintajäsenet, jotka tuovat mukanaan laaja-alaista osaamista turvamarkkinan.

Turvaurakoitsijat ry jatkaa työtään jäsentensä ja koko toimialan tukena. Markkina muuttuu – ja me muutamme sen mukana. Yhdessä rakennamme entistä vahvempaa ja turvallisempaa tulevaisuutta.

Turvaurakoitsijat ry on mukana Finnsec-messuilla 8.–9.10.2025. Lanseeraamme osastollamme mm. EN 16005 oviautomatiikka-standardiin liittyvän dokumentaatiopankin ja koulutuskokonaisuuden, joiden ansiosta dokumentaatio, riskienarviointi ja CE-merkintä täyttävät vaatimukset.

Lisäksi järjestämme mielenkiintoisen seminaarikokonaisuuden Messukeskuksen kongressi-siiven tilassa 209 keskiviikkona 8.10.2025 klo 9.30–15.30. Puheenvuorojen aiheet ja aikataulu on nähtävissä seuraavalla sivulla. **Nähdään Finnsec-messuilla!**



Mukana messuilla!



Teknologia, vastuullisuus ja resilienssi – turvallisuuden avaintekijät 2025

Turvallisuusala elää murrosta, jossa teknologia, vastuullisuus ja yhteiskunnan resilienssi kietoutuvat yhteen. Tekoäly tuo uusia mahdollisuuksia kameravalvontaan, pilvipalvelut muuttavat toimintamalleja ja kyberturvallisuus haastaa yritykset kaikilla tasoilla. Samaa aikaan vastuullisuuden ja huoltovarmuuden merkitys kasvaa – turvallisuus on koko yhteiskunnan selkäranka.

Finnsec-seminaari kokoaa yhteen alan asiantuntijat, jotka avaavat ajankohtaisia ilmiöitä tekoälystä hybridiuhkiin ja käytännön ratkaisuista vastuulliseen turvatekniikkaan. Päivän aikana saat tiiviin tilannekuvan ja tulevaisuuden näkymiä, jotka auttavat varautumaan, kehittämään ja tekemään oikeita valintoja niin yrityksen kuin koko yhteiskunnan turvallisuuden kannalta.

FINNSEC-SEMINAARI 8.10.2025, kongressisiipi, tila 209

9.30–10.00	Turvallisuusala tänään ja huomenna – Jyri Paasonen, Turvallisuus & Riskienhallinta -lehti
10.00–10.30	Tekoäly kameravalvonnan apuna – Timo Miettinen, HikVision
10.30–11.00	Pilviratkaisut, niiden vahvuudet ja heikkoudet – Eero Viilo, Saltosystems Oy
11.00–11.30	Current Fire Industry trends are moving faster towards Remote Connectivity – Paul Pope, Global Head of Fire & Life Safety Business, Ajax Systems
11.30–12.00	Häiriötön sähkönsyöttö turvallisuuden selkärankana – Aaro Myöhänen, FSM
12.00–12.30	TAUKO
12.30–13.00	Ajankohtaista digihuijauksista – muuttuuko jokin, kun pikamaksut ja "verification of payee" tulevat voimaan? – Niko Saxholm, Finanssiala
13.00–13.30	Mobiilitunnisteet kulunvalvonnassa – Anssi Liski, Schneider Electric
13.30–14.00	Kyberturvallisuuden tilannekuva pk-yrityksissä – Mika Lindberg, Opsec
14.00–14.30	Vastuullisuus turvatekniikan palveluntuottajalla – Mirva Viljakainen, Certego Oy
14.30–15.00	Standardien ja toimintojen harmonia – turvallisten ovien ydin – Juha Pekka Hirvonen, dormakaba Suomi
15.00–15.30	Hybridiuhat ja yhteiskunnan resilienssit – Heikki Kärkkäinen, Milestone Systems

CDVI täyttää 40 vuotta – kulunvalvontaa neljän vuosikymmenen ajalta

Vuonna 1985 pariisilaisesta verstaasta alkunsa saanut CDVI on kasvanut neljässä vuosikymmenessä kansainväliseksi kulunvalvonnan toimijaksi. Yrityksellä on nykyisin 11 tytäryhtiötä, yli 300 työntekijää ja toimintaa yli 100 maassa.

Tunnetuin tuote on Digicode®-näppäimistö, joka kuuluu edelleen monen kohteen arkeen. Vuonna 2025 se sai myös erityisen huomionosoituksen, kun Ranskan valtio valitsi sen kansalliseen postimerkkisarjaan muiden merkittävien keksintöjen rinnalle.

Perheyriyksestä kansainväliseksi toimijaksi

Yrityksen perusti **David Benhammou**, ja hänen veljensä **Yoram** on toiminut toimitusjohtajana vuodesta 2016. Pitkäjänteisyys ja henkilöstön pysyvyys ovat olleet osa CDVI:n identiteettiä – ensimmäinen työntekijä vuodelta 1985 työskentelee yhä yrityksessä.

Ratkaisuja vaativiin kohteisiin

CDVI:n tuotteita hyödynnetään esimerkiksi terveydenhuollossa ja kriittisessä infrastruktuurissa. Tuotteiden pitkä käyttöikä ja kattava takuu ovat olleet yksi kilpailuvaltti. Yritys on myös laajentanut toimintaansa yritysostoin, muun muassa hankkimalla SERSYSin, joka valmistaa paloturvallisia ja ilkeivallalta suojattuja lukitusjärjestelmiä.

lisia ja ilkeivallalta suojattuja lukitusjärjestelmiä.

Panostuksia tutkimukseen ja kestävyteen

Noin viidennes liikevaihdosta käytetään tutkimukseen ja tuotekehitykseen. CDVI on ollut mukana biometriaan ja äänentunnistukseen liittyvissä kehityshankkeissa yhdessä kansainvälisten tutkimuslaitosten kanssa.

Yritys on myös pyrkinyt vähentämään ympäristökuormitustaan #CDVIgoesgreen-ohjelman avulla. Se on sisältänyt mm. vähähiilisen alumiinin käyttöönottoa, pakkausmateriaalien vähentämistä ja digitaalisia käyttöohjeita paperin sijaan.

Riippumaton ja eurooppalainen toimija

CDVI on pysynyt itsenäisenä, vaikka suuri osa turvallisuusalan yrityksistä on sulautunut osaksi kansainvälisiä konserneja. Yrityksen pääkonttori sijaitsee Ranskassa, ja sen eurooppalainen identiteetti korostuu siinä, että suunnittelu, tuotanto ja asiakastuki on haluttu pitää lähellä asiakkaita.

Työturvallisuus on osa ammattitilpeyttä

– miksi turvallinen työympäristö on elintärkeää turvaurakointialalla

Turvallisuus on turvaurakointiyriytsten ydinosaamista. Mutta kuinka usein pysähdymme miettimään työntekijöiden omaa turvallisuutta? Työturvallisuus ja työhyvinvointi eivät ole pelkkiä lakisääteisiä velvoitteita – ne ovat liiketoiminnan kivijalka, ammatillisen uskottavuuden tae ja parhaimmillaan myös kilpailuetu.

Työturvallisuuslaki ei ole muodollisuus – se suojaa ihmistä ja liiketoimintaa

Turvaurakointialalla työtä tehdään usein haastavissa ympäristöissä: rakennustyömaila, asennuskohteissa, sähkölaitteiden parissa, yksin tai asiakkaiden tiloissa. Jokainen tilanne tuo omat riskinsä.

Työturvallisuuslain noudattaminen – kuten vaarojen arviointi, opastus, suojainten käyttö

ja työn suunnittelu – ei ole byrokratiaa, vaan elintärkeää ennaltaehkäisevää turvallisuustyötä. Lain avulla ehkäistään tapaturmia, ammattitauteja ja pitkää sairauspoissaolojen ketjua, joka kuormittaa työntekijöitä ja työnantajaa.

Turvallinen työ – parempi työ

Turvallinen työympäristö tukee työhyvinvointia ja lisää työn merkityksellisyyttä. Kun työntekijä kokee olevansa turvassa ja arvostettu, hän sitoutuu työhönsä paremmin. Turvallisuus luo pohjan avoimelle työskentelylle ja auttaa ennaltaehkäisemään paitsi fyysisiä, myös henkisiä kuormitustekijöitä.

Hyvinvoiva työntekijä tekee laadukkaampaa työtä, pystyy keskittymään ja edustaa yritystä positiivisesti asiakastilanteissa.

Turvallisuuskulttuuri ei synny sattumalta

Työturvallisuus ei ole pelkkä yksittäinen tarkastus tai suojakypärä – se on osa jokapäiväistä toimintaa. Vahva turvallisuuskulttuuri tarkoittaa, että:

- vaaratilanteet raportoidaan ja käsitellään oppimismahdollisuuksina
- työohjeet ovat ajan tasalla ja työntekijät saavat riittävästi koulutusta
- työvälineet ovat kunnossa ja ergonomiset
- työn suunnittelussa otetaan huomioon myös henkinen kuormitus
- turvallisuus on johdon ja esihenkilöiden prioriteetti.

Jäsenyrityksissämme on käytössä **ISO 45001 -sertifioitu työterveys- ja työturvallisuusjärjestelmä**. Sen osana myös **läheltä piti**

-tilanteiden kirjaaminen ja käsittely ovat tärkeä työkalu ennakoivassa turvallisuustyössä. Kyse ei ole syyllistämisestä, vaan oppimisesta ja siitä, että vastaavat tilanteet voidaan jatkossa välttää – kaikkien parhaaksi.

Turvaurakointiliikkeen uskottavuus rakentuu omalla esimerkillä

Turvaurakointiyriytset rakentavat asiakkaille turvallisuutta – lukitus-, kulunvalvonta- ja järjestelmäpalveluiden muodossa. Omien työntekijöiden turvallisuudesta huolehtiminen on osa samaa kokonaisuutta.

Yritys, joka panostaa työturvallisuuteen ja henkilöstön hyvinvointiin, näyttää esimerkkiä niin työntekijöilleen kuin asiakkailleen ja yhteistyökumppaneille. Turvallisuudesta huolehtiminen on osa ammattitilpeyttä – ja sitä, miten koko ala nähdään ulospäin.



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**

27.10.2025–5.3.2027

Tutustu myös:

Turvallisuusjärjestelmien suunnittelijan pätevyys -tentti

Rakenteellisen turvasuojauksen pätevyys, lukkoseppäkoe

taitotalo.fi/lukitusala

KYSY LISÄÄ

Jussi Venäläinen

050 430 8281

jussi.venalainen@taitotalo.fi

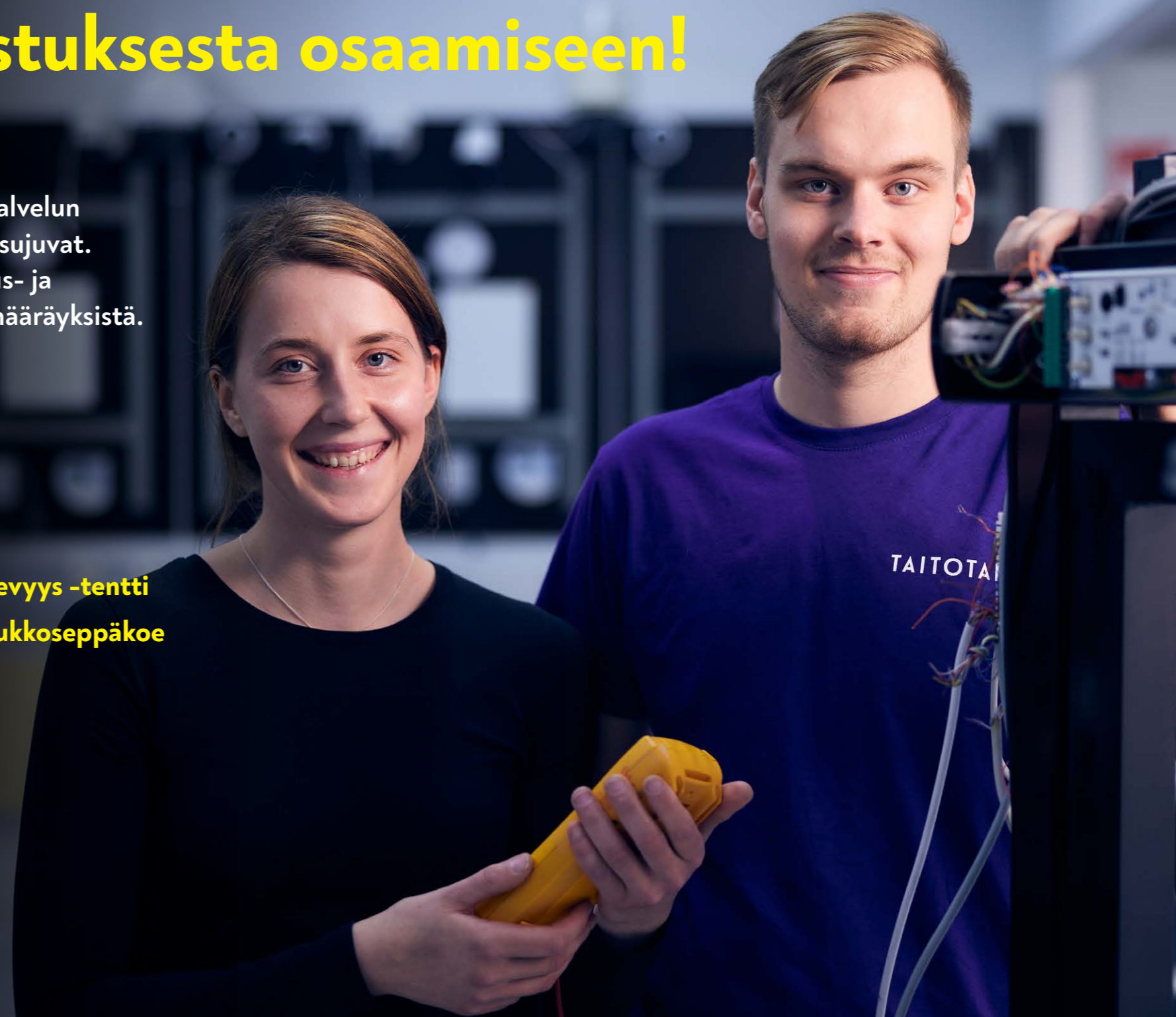
TAITOTALO

Valimotie 8, 00380 Helsinki

asiakaspalvelu@taitotalo.fi

asiakaspalvelu 010 80 80 90

TAITOTALO



NIS2-direktiivi tulee – mitä se tarkoittaa pienille turvallisuusalan yrityksille?

Euroopan unionin uusi NIS2-direktiivi (Network and Information Security Directive) tuo mukanaan merkittäviä velvoitteita kyberturvallisuuteen. Vaikka monet pienet turvallisuusalan yritykset eivät kuulu direktiivin suoraan sääntelyyn, sen vaikutukset ulottuvat laajasti koko toimialaan.

Mikä NIS2 on?

NIS2 on EU:n kyberturvallisuusedirektiivi, joka päivittää ja laajentaa aiemman NIS-direktiivin vaatimuksia. Tavoitteena on parantaa kriittisten toimialojen ja toimitusketjujen kykyä ehkäistä ja hallita kyberuhkia. Direktiivi koskee muun muassa energia-, vesihuolto-, terveys-, liikenne- ja digitaalipalveluita – ja erityisesti niiden toimittajia ja alihankkijoita.

Miksi turvallisuusyritysten kannattaa välittää?

Vaikka pieni turvatekniikkaliike ei olisikaan suoraan NIS2:n kohde, moni sen asiakas on. Esimerkiksi sairaalat, kaupungit, logistiikkakeskukset tai sähkölaitokset voivat edellyttää, että myös heidän toimittajansa täyttävät kyberturvallisuuden perusvaatimukset – mukaan lukien lukkoliikkeet ja järjestelmäasentajat.

Toimitusketjujen turvallisuus on nyt kaikkien asia.

Mitä pienet yritykset voivat tehdä?

1 Tarkista perusturva omassa IT-ympäristössä

- Käytetäänkö ajantasaisia virustorjunta- ja palomuuriratkaisuja?
- Onko ohjelmistot ja laitteet päivitetty?
- Käytetäänkö kaksivaiheista tunnistautumista?

2 Dokumentoi kyberturvallisuuskäytännöt

NIS2 painottaa riskienhallintaa ja vastuullisuutta. Pienellä yrityksellä tämä voi tarkoittaa esimerkiksi:

- tietoturvasuunnitelman laatimista
- varmuuskopiointikäytäntöjen dokumentointia
- selkeitä ohjeita työntekijöille salasanojen, asiakasdatan ja etäyhteyksien käytöstä.

3 Keskustele asiakkaiden kanssa – proaktiivisesti

Moni tilaaja kaipaa nyt tietoa siitä, miten heidän toimittajansa huolehtivat kyberturvasta. Hyvin laadittu tietoturvaluvaus tai vaikkapa yksi PowerPoint-sivu voi tehdä yrityksestä uskottavamman ja luotettavamman kumppanin.

4 Pidä huolta henkilöstön osaamisesta

Kyberturva ei ole vain teknologiaa – se on ennen kaikkea ihmisten toimintaa. Yksinkertainen koulutus tai muistilista voi estää inhimillisiä virheitä, jotka ovat edelleen yleisin tietomurtojen syy.

Ei uhka, vaan mahdollisuus?

NIS2 voi alkuun tuntua hankalalta, mutta se tarjoaa myös mahdollisuuden erottautua. Pienet turva-alan yritykset voivat profiloitua vastuullisina ja kyberturvallisuudesta huolehtivina ammattilaisina – ja samalla vahvistaa omaa kilpailukykyään yhä vaativammilla markkinoilla.

”NIS2 on signaali: nyt kaikki toimijat – myös pienet – ovat osa kyberturvallisuuden ekosysteemiä.”

NIS2-tietoturvalista pienelle turvayritykselle

1 Tietoturvaperusteet kunnossa?

- Käytössä on ajantasainen virustorjunta ja palomuuuri
- Kaikki käyttöjärjestelmät ja ohjelmistot pidetään päivitettyinä
- Laitteet suojataan vahvoilla salasanoilla ja/tai laitekohtaisilla PIN-koodeilla
- Kaksivaiheinen tunnistautuminen (2FA) on otettu käyttöön tärkeimmissä palveluissa

2 Varmuuskopiointi ja palautus

- Tiedostot varmuuskopioidaan säännöllisesti (esim. päivittäin tai viikoittain)
- Varmuuskopiot säilytetään erillisessä sijainnissa (pilvessä tai offline)
- Palautusprosessi on testattu: tiedetään, miten tiedot palautetaan tarvittaessa

3 Asiakasdata ja sopimukset

- Asiakas- ja projektitiedot säilytetään turvallisesti, ei esimerkiksi suojaamattomissa sähköposteissa
- Sopimuksissa huomioidaan tietoturvavelvoitteet (esim. vastuut, luottamuksellisuus)
- Pääsy asiakastietoihin on rajattu vain niille, jotka niitä tarvitsevat

4 Sisäinen ohjeistus ja osaaminen

- Yrityksellä on kirjallinen ohje tietoturvasta (lyhytkin riittää)
- Henkilöstölle on annettu ohjeistus salasanoista, sähköpostin liitteistä ja verkkourkinnasta
- Työntekijät tietävät, mitä tehdä, jos epäilevät tietomurtoa tai virushyökkäystä

5 Valmius asiakkaiden kysymyksiin

- Yrityksellä on lyhyt tietoturvaluvaus, jonka voi liittää tarjouksiin tai sopimuksiin
- Mahdolliset asiakasauditoinnit tai kyselyt on varauduttu hoitamaan (esim. kuka vastaa?)

VINKKI:

Tulosta tämä lista ja käy se läpi yhdessä henkilöstön kanssa – vaikka osana viikkopalaveria tai koulutuspäivää.

Kyberturvallisuus 2025 – kasvavat uhat ja yritysten haasteet

Lokakuu on kansainvälinen kyberturvallisuuskuukausi, ja sen sanoma on ajankohtaisempi kuin koskaan. Suomalaiset yritykset ovat entistä riippuvaisempia digitaalisista järjestelmistä, mutta samalla kyberuhat ovat kasvaneet sekä määrällisesti että laadullisesti. Kyberrikollisuus ei ole enää satunnaista häirintää, vaan liiketoimintaa, joka uhkaa yritysten jatkuvuutta ja koko yhteiskunnan turvallisuutta.

Hyökkäykset ammattimaistuvat

Viime vuosien aikana kyberhyökkäykset ovat siirtyneet yksittäisistä hakkereista järjestäytyneiden rikollisverkostojen ja valtiollisten toimijoiden käsiin. Hyökkäykset ovat huolellisesti suunniteltuja, pitkäkestoisia ja kohdistuvat sekä suuryrityksiin että pk-sektoriin. Erityisen haavoittuvia ovat yritykset, jotka toimivat kriittisen infrastruktuurin tai huoltovarmuuden kannalta keskeisillä aloilla – kuten turvallisuustekniikan parissa.

Pk-yritykset etulinjassa

Pk-yritykset muodostavat suuren osan Suomen elinkeinoelämästä, mutta niiden kyvykyys torjua kyberuhkia vaihtelee suuresti. Resurssipula, osaajavaje ja puutteelliset prosessit tekevät monista pienistä yrityksistä helppoja kohteita. Hyökkäystavat – tietojenkäsitelmä, palvelunestohyökkäykset ja kiristysohjelmat – voivat hetkessä pysäyttää liiketoiminnan.



Sääntely kiristyy

EU:n uusi **NIS2-direktiivi** astui Suomessa voimaan keväällä 2025 kyberturvallisuuslakina. Se tuo tiukkoja veloitteita erityisesti kriittisiä palveluja tarjoaville yrityksille: riskienhallinnan kehittäminen, poikkeamien raportointi

ja toimitusketjun tietoturvan varmistaminen eivät ole enää suosituksia, vaan lakisääteisiä vaatimuksia. Myös pk-yritykset joutuvat väistämättä mukaan, koska suuremmat tilaajat edellyttävät korkeaa tietoturvan tasoa sopimuskumppaneiltaan.

Inhimillinen tekijä yhä suurin riski

Teknologiset ratkaisut kehittyvät vauhdilla, mutta suurin osa tietomurroista saa alkunsa ihmisistä. Heikot salasanat, huolimattomuus sähköpostiliitteiden kanssa tai päivittämättömät ohjelmistot avaavat oven hyökkääjille. Yksi klikkaus voi maksaa yritykselle maineen, asiakassuhteet ja taloudellisen toimintakyvyn. Siksi henkilöstön jatkuva koulutus ja tietoturvatietoisuuden vahvistaminen ovat kriittisiä.

Mitä yritysten tulisi tehdä?

- **Perusta kuntoon:** palomuurit, varmuuskopiot, päivitykset.
- **Henkilöstön koulutus:** tunnista tietojenkäsitelmäyritykset ja raportoi niistä.
- **Harjoittele:** testaa säännöllisesti, miten organisaatio reagoi kyberhäiriöön.
- **Verkostoidu:** hyödynnä alan yhteistyötä ja jaa kokemuksia muiden kanssa.

Kyberturvallisuus ei ole enää erillinen IT-asia, vaan yrityksen riskienhallinnan ja liiketoiminnan jatkuvuuden ydin. Lokakuu tarjoaa hyvän tilaisuuden pysähtyä arvioimaan omaa valmiutta – sillä kyse ei ole siitä, *joutuuko* yritys hyökkäyksen kohteeksi, vaan siitä, *milloin*.

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

Suojattu avain

dormakaba expert plus -avain on suojattu vuoteen 2033.

Avaimeton kiinteistö

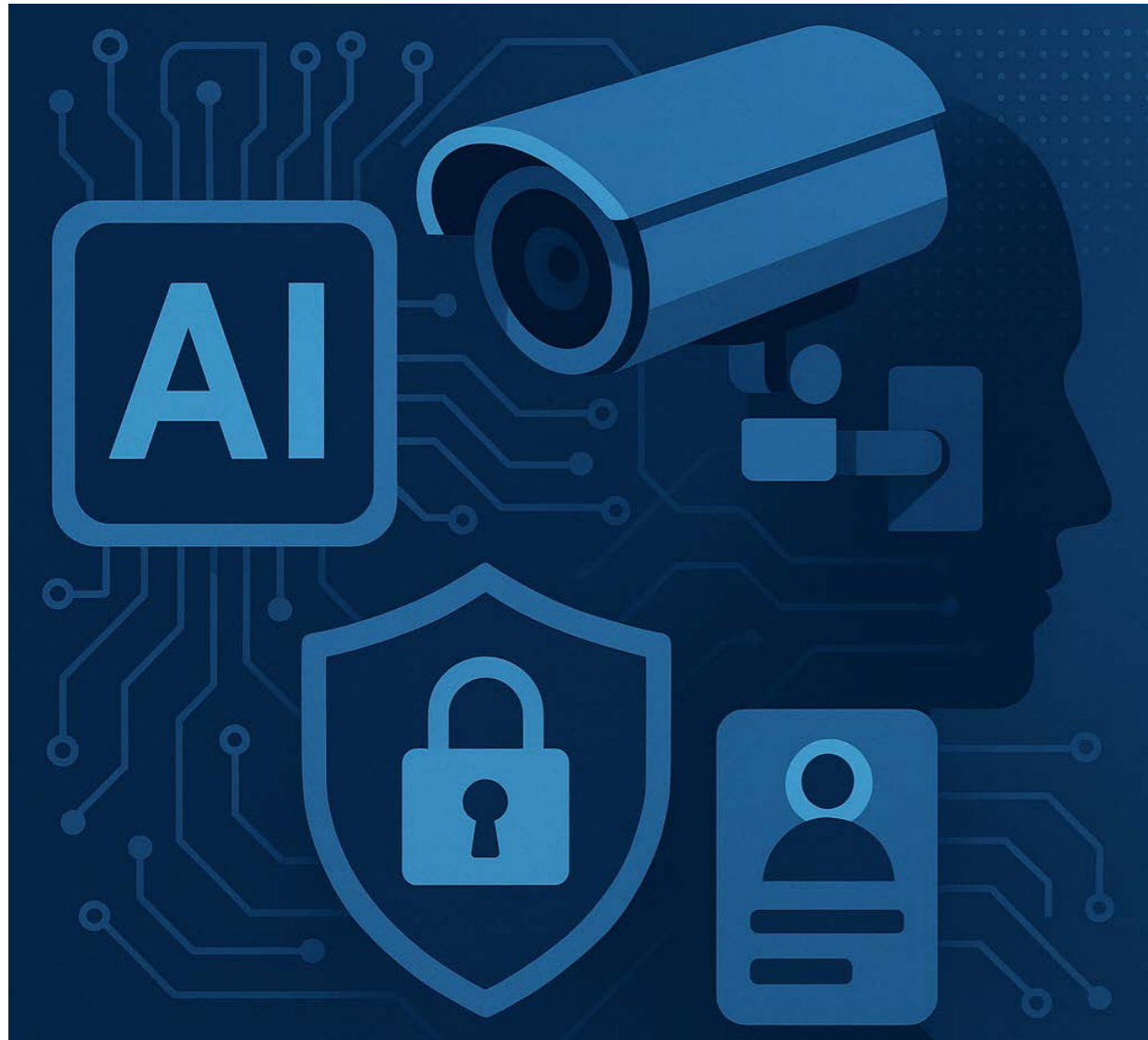
Kokonaisvaltainen, joustava kulunvalvontaratkaisu. Modulirakenteen ansiosta järjestelmä voidaan räätälöidä tarpeen mukaan. Mahdollistaa kustannustehokkaan dormakaba evolo -lukkojen käytön osana järjestelmää, koska ne eivät vaadi erillistä kaapelointia. Tuo tehokkuutta elinkaarikustannusten hallintaan.

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 

Tekoäly ja turvallisuusjärjestelmät – hypeä vai realismia?



Tekoäly on noussut yhdeksi kuumimmista trendeistä myös turvallisuusallalla. Lupaukset ovat suuria: tekoäly voi tunnistaa poikkeavaa käyttäytymistä, vähentää väärin hälytysten määrää ja jopa ennustaa järjestelmän huoltotarpeita. Mutta mitä tämä kaikki tarkoittaa käytännössä turva-urakoitsijoille ja asiakkaille?

Videovalvonta älykkäämmäksi

Yksi konkreettisimmista tekoälyn sovelluksista löytyy videovalvonnasta. Perinteinen kamera tallentaa kaiken, mutta tekoälypohjainen järjestelmä osaa erottaa ihmiset, ajoneuvot ja jopa tunnistaa epänormaalin liikkeen. Näin vartijat tai käyttäjät eivät huku

kuvavirtaan, vaan saavat hälytyksen juuri silloin, kun jotain olennaista tapahtuu.

Kulunvalvonta ja älylukitus – tekoälyn seuraava askel?

Kulunvalvontajärjestelmissä tekoäly voi tulevaisuudessa oppia tunnistamaan poikkeamia henkilöstön normaaleista kulkureiteistä ja -ajoista. Jos työntekijä käyttää kulkukorttia epätavalliseen kellonaikaan tai pyrkii alueelle, jossa hänellä ei yleensä ole asiaa, järjestelmä voi antaa ennakkohälytyksen tai pyytää lisävarmistusta (esim. biometrinen tunnistus).

Elektronisissa lukitusjärjestelmissä tekoäly voi auttaa optimoimaan pääsyoikeuksia ja reagoimaan dynaamisesti riskeihin. Kuvitellaan tilanne, jossa toimitilassa havaitaan tietoturvapoikkeama – järjestelmä voisi tekoälyn avulla automaattisesti rajata pääsyoikeuksia kriittisiin tiloihin ja suojata näin yritystä inhimillisiltä virheiltilä.

Integroidut turvajärjestelmät – tekoäly kokonaisuuden hallinnassa

Tulevaisuudessa tekoäly ei ehkä näy yksittäisissä laitteissa, vaan koko turvajärjestelmän ”selkärankana”. Kun kulunvalvonta, lukitus, kameravalvonta ja hälytysjärjestelmät yhdistyvät samaan alustaan, tekoäly voi yhdistellä eri lähteistä saatua tietoa ja tunnistaa uhkia aiemmin kuin yksittäinen järjestelmä.

Esimerkiksi jos kamera havaitsee henkilön liikkuvan kohteessa normaalien työaikojen

ulkopuolella ja kulunvalvonta osoittaa, että ovesta on tultu väärällä kulkukortilla, tekoäly voi yhdistää nämä tiedot ja nostaa hälytystason välittömästi. Tämä vähentää väärin hälytysten määrää ja auttaa kohdistamaan resurssit oikeisiin tilanteisiin.

Hypeä vai realismia?

Vaikka tekoäly tarjoaa monia hyötyjä, siihen liittyy myös riskejä ja epärealistisia odotuksia. Algoritmit tarvitsevat paljon laadukasta dataa toimiakseen, ja väärin koulutettu järjestelmä voi johtaa virheellisiin tuloksiin. Lisäksi tekoälyn hyödyntäminen ei poista ihmisen vastuuta: lopulliset päätökset kuuluvat aina ammattilaisille.

Turva-urakoitsijoiden näkökulmasta tärkeää on pysyä ajan tasalla kehityksestä ja arvioida, milloin tekoälyratkaisusta on todellista hyötyä asiakkaalle – ja milloin kyse on vielä enemmän markkinapuheesta.

Mitä seuraavaksi?

Kameravalvonta on tällä hetkellä tekoälyn näkyvin käyttökohde, koska kuvamateriaalin analysointi sopii hyvin koneoppimismalleille. Silti suurin potentiaali pitkällä aikavälillä voi olla **integroinnissa**: kun tekoäly yhdistää kameratiedon, kulkutapahtumat, lukituslogit ja hälytykset yhdeksi tilannekuvaksi, syntyy aivan uudenlainen työkalu riskienhallintaan.

Toisin sanoen kameravalvonta on nyt kehityksen kärki, mutta tulevaisuudessa tekoälystä voi tulla koko turvajärjestelmän ”aivot”.

Pk-yrityksen varautuminen

– kilpailukykyä kriiseissäkin

Yritysten toimintaympäristö on muuttunut entistä arvaamattommaksi. Pandemiat, geopoliittiset kriisit, kyberuhat ja toimitusketjujen häiriöt ovat osoittaneet, että myös pienimmät yritykset voivat joutua vakavien tilanteiden keskelle. Suomen Yrittäjät on laatinut *Pk-yrityksen varautumisopas*, joka korostaa, että varautuminen ei ole ylimääräinen velvollisuus, vaan olennainen osa kilpailukykyä ja yrityksen jatkuvuuden turvaamista.

Miksi varautuminen on tärkeää?

Pk-yritykset muodostavat merkittävän osan Suomen elinkeinoelämästä ja huoltovarmuudesta. Kun sähkö katkeaa, tietoliikenneyhteydet häiriintyvät tai avainhenkilö sairastuu, yrityksen toiminta voi pysähtyä kokonaan. Varautuminen vahvistaa yrityksen iskunkestävyyttä ja vähentää riskiä, että ongelmat kaatavat koko liiketoiminnan.

Elintärkeät toiminnot keskiöön

Varautuminen alkaa oman yrityksen kriittisten toimintojen tunnistamisesta: mitä prosesseja ilman yritys ei selviä? Näitä voivat olla esimerkiksi sähkösaanti, tietojärjestelmät,

polttoainehuolto tai keskeiset alihankkijat. Kun riskit on tunnistettu, voidaan rakentaa suunnitelma niiden hallintaan. Oppaassa kehoitetaan myös ottamaan käyttöön vähintään 72 tunnin varautumissuunnitelma, joka takaa toiminnan jatkuvuuden lyhytaikaisissa häiriöissä.

Konkreettisia toimia pk-yrityksille

Opas suosittelee käytännön toimia, kuten:

- **Varavoimaratkaisut ja polttoainetarastot**, jotta perustoiminnot eivät pysähdy.
- **Tietoliikenneyhteyksien ja tietoturvan varmistaminen**, esimerkiksi varayhteyksillä ja pilvipalveluiden hyödyntämisellä.
- **Alihankkijoiden ja kumppaneiden arviointi**, sillä verkoston heikkoudet heijastuvat suoraan yritykseen.
- **Harjoittelu ja ohjeistus**, jotta henkilöstö osaa toimia myös kriisitilanteissa.
- **Avoin viestintä**, joka lisää luottamusta asiakkaisiin ja sidosryhmiin.

Pk-yrityksen varautuminen on osa jokapäiväistä johtamista



Yhteistyö ja vastuullisuus

Varautuminen ei koske vain yksittäistä yritystä. Jokainen toimija on osa laajempaa verkostoa, joka ylläpitää yhteiskunnan kokonaisturvallisuutta. Yrittäjäjärjestöjen, toimialajärjestöjen ja alueorganisaatioiden tarjoamat työkalut ja koulutus ovat arvokas tuki. Samalla vastuullinen varautuminen voi kääntyä kilpailueduksi – asiakas luottaa toimittajaan, joka huolehtii myös poikkeustilanteista.

Varautuminen ei pk-yrityksessä ole byrokraatia, vaan luonnollinen osa arjen johtamista. Kun riskit tunnistetaan, vastuut selkeytetään ja perusvalmiudet pidetään kunnossa, yritys on valmis kohtaamaan tulevaisuuden haasteet. Kuten oppaassa todetaan: viranomaiset eivät turvaa yrityksen jatkuvuutta – vastuu on aina yrittäjällä. Mutta valmistautumalla ajoissa kriisit voidaan kohdata hallitusti ja jopa kääntää vahvuudeksi.

Uusi palkka-avoimuusdirektiivi ja sen vaikutukset turvallisuusalan yrityksiin

Euroopan unioni on hyväksynyt palkka-avoimuusdirektiivin, joka tuo merkittäviä muutoksia yritysten toimintaan myös Suomessa. Direktiivin tavoitteena on kaventaa sukupuolten välistä palkkaeroa ja lisätä läpinäkyvyyttä palkitsemisessa ja se astuu voimaan keväällä 2026. Suomen hallitus on tehnyt lakiesityksen toukokuussa 2025 ja lain olisi tarkoitus astua voimaan toukokuussa 2026. Mitä tämä tarkoittaa yrityksille?

Mitä direktiivi velvoittaa?

Direktiivi edellyttää, että työntekijöillä on oikeus saada tietoa oman palkkansa perusteista sekä siitä, miten palkat määräytyvät yrityksessä. Lisäksi tietyt työnantajat joutuvat raportoimaan palkkaeroista säännöllisesti. Suurimpia velvoitteita tulee niille työnantajille, joilla on vähintään 100 työntekijää, mutta vaikutukset ulottuvat pienempiinkin yrityksiin.

Vaikutukset turvallisuusalan yrityksissä

Suuri osa alamme yrityksistä ovat pk-yrityksiä, joissa työntekijämäärä jää alle sadan henkilön. Tämä ei kuitenkaan tarkoita, ettei direktiivi koskettaisi niitä. Työntekijöiden oikeus palkkatietojen läpinäkyvyyteen koskee kaikkia työnantajia. Käytännössä tämä merkitsee sitä, että yritysten on pystyttävä perustelemaan palkkausjärjestelmänsä selkeästi ja dokumentoidusti.

Mahdollisuudet ja haasteet

Positiivisena puolena palkka-avoimuus voi lisätä luottamusta työnantajan ja henkilöstön välillä. Selkeä palkkausjärjestelmä tekee yrityksestä houkuttelevamman työnantajan ja helpottaa uusien osaajien rekrytointia. Toisaalta direktiivi voi lisätä hallinnollista taakkaa ja vaatia uusia järjestelmiä palkkatietojen seurantaan ja raportointiin.

Miten direktiiviin tulisi varautua?

Ennen voimaan astumista seuraavat asiat olisi hyvä hoitaa kuntoon:

- Käydä läpi palkkausjärjestelmänsä ja dokumentoida sen perusteet.
- Varmistaa, että palkkaeroille on asialliset ja syrjimättömät syyt ja aloittaa sisäiset palkkavertailut ja korjata epäselvyydet hyvissä ajoin ennen 2026.
- Seurata kansallista lainsäädäntöä, jolla direktiivi saatetaan voimaan Suomessa.

Direktiivi astuu voimaan vaiheittain, mutta sen vaikutukset ovat pitkäkestoisia. Tämä tarjoaa parhaimmillaan yrityksille myös mahdollisuuden profiloitua vastuullisina työnantajina – kunhan valmistautuminen tehdään ajoissa. Huom! Lakiesitykseen voi tulla vielä muutoksia, mutta tämä on ehdotuksen sisältö.

Muistilista: Palkka-avoimuusdirektiivin velvoitteet eri kokoisille yrityksille:

1. Velvoitteet kaikille työnantajille (yrityksen koosta riippumatta)

- Työnhakijalle annettava tieto palkasta tai palkkahaarukasta ennen rekrytointineuvottelua.
- Ei saa kysyä hakijan aiempaa palkkahistoriaa.
- Työntekijällä oikeus pyytää tietoa oman palkan perusteista sekä samankaltaisia tehtäviä tekevien palkoista.
- Pyyntöön vastattava kahden kuukauden kuluessa.
- Palkkausjärjestelmän tulee perustua selkeisiin ja syrjimättömiin kriteereihin.

2. Velvoitteet yrityksille, joissa vähintään 50 työntekijää

- Palkkakehityksen ja uralla etenemisen kriteerit oltava läpinäkyvästi saatavilla henkilöstölle.
- Työnantajan on kyettävä osoittamaan, että palkkaerot perustuvat objektiivisiin syihin.

3. Velvoitteet yrityksille, joissa vähintään 100 työntekijää

- Pakollinen palkkaraportointi (gender pay gap):
 - Miesten ja naisten keski- ja mediaanipalkat
 - Bonukset ja muuttuvat palkanosat
 - Palkkojen jakaumat (kvartiilijaot)
- Raportti toimitettava henkilöstölle ja viranomaisille.
- Mikäli palkkaeroja ei pystytä perustelemaan, työnantajan velvollisuus on korjata tilanne.



Työlainsäädäntö elää

– irtisanomiskynnyksen madaltamisen rajankäyntiä

Työoikeuden sääntely on jatkuvasti poliittisen keskustelun ja lainsäädäntöhankkeiden kohteena. Työsopimuslain ja siihen liitännäisten lakien uudistamistyössä yksi keskeisimmistä teemoista on ollut työntekijän irtisanomissuojan taso. Hallituksen linjauksissa on nähty pyrkimys madaltaa työnantajan kynnystä päättää työsuhde tilanteissa, joissa työntekijän toiminta tai suoriutuminen ei vastaa odotuksia.

Hallitus on lähettänyt syyskuun alkupuolella lainsäädännön arviointineuvoston käsiteltäväksi esitysluonnoksen, jossa irtisanomissuojan madaltamisaikeista ollaan tultu takaisin voimassa olevien säännösten suuntaan.

Asiallinen ja painava syy vai pelkkä asiallinen syy?

Nykyinen työsopimuslaki edellyttää työntekijän irtisanomiselle ”asiallista ja painavaa syytä”. Tämä kaksiosainen vaatimus on tulkinnallisesti merkinnyt sitä, että pelkkä vähäinen laiminlyönti tai lievä rikkomus ei voi oikeuttaa irtisanomiseen. Painavuusvaatimus on luonut rajan, joka suojaa työntekijää perusteettomilta työsuhteen päättämisiltä.

Uudistushankkeen yhteydessä on kuitenkin esitetty, että irtisanomisperusteena riittäisi jatkossa pelkkä ”asiallinen syy”. Tulkinnallisesti muutos voisi alentaa irtisanomiskynnystä merkittävästi, koska ”painavuuden” vaatimus on ollut keskeinen suojatekijä. Mikäli laki-

tekstiin jäisi vain asiallisuusvaatimus, oikeuskäytännön varaan jäisi määrittely siitä, kuinka vähäiset rikkomukset tai laiminlyönnit voisivat tulla kysymykseen irtisanomisperusteena.

Varoitusmenettelyn rooli

Toinen keskeinen keskustelunaihe on ollut varoitusmenettelyn muuttaminen. Nykyisen käytännön mukaan työntekijän irtisanominen on mahdollista, jos hän syyllistyy samaan tai olennaisesti samanlaiseen rikkomukseen, josta hänelle on aikaisemmin annettu varoitus. Tämä varoitusmenettely on nähty työntekijän oikeusturvaa vahvistavana, sillä sen avulla työntekijälle annetaan mahdollisuus korjata toimintansa ennen työsuhteen päättämistä.

Uudistuksen valmistelun aikana on kuitenkin esitetty mallia, jossa aikaisempi varoitus voisi toimia irtisanomisperusteiden pohjana myös silloin, kun uusi rikkomus ei olisi täysin samankaltainen. Tämä merkitsisi käytännössä sitä, että työntekijä, joka on saanut varoituksen esimerkiksi myöhästelyistä, voisi helpommin tulla irtisanotuksi myöhemmin myös muunlaisen laiminlyönnin perusteella. Näin varoituksen merkitys yleisenä työsuhteen päättämistä helpottavana välineenä kasvaisi.

Alisuoriutuminen oikeuskäytännössä

Alisuoriutumisen sisällyttäminen nimenomaisesti irtisanomisperusteena työsopimuslakiin

on ollut myös valmistelun aikana esillä. Viimeisimpien tietojen mukaan hallituksen luonnoksessa tästä on kuitenkin luovuttu. On huomattava, että korkeimman oikeuden ja työtuomioistuimen oikeuskäytännössä työntekijän jatkuva ja olennaisesti työvelvoitteita rikkova alisuoriutuminen on jo nykyisellään voinut muodostaa irtisanomisperusteen.

Käytännössä työnantajan on kuitenkin pitänyt osoittaa, että alisuoriutuminen ei johdu työnantajasta johtuvista seikoista, kuten puutteellisesta perehdytyksestä, epärealistisista tavoitteista tai työolosuhteiden puutteista. Lisäksi työntekijälle on tullut antaa varoitus ja mahdollisuus parantaa suoritustaan. Oikeuskäytännön vakiintunut linja on siis jo nykyisellään tarjonnut työnantajille mahdollisuuden vedota alisuoriutumiseen, mutta asettanut sen käyttämiselle tiukat reunaehdot.

Talous- ja työllisyyspoliittiset perusteet

Uudistusehdotusten taustalla on ollut erityisesti elinkeinoelämän edustajien tavoite lisätä yritysten halukkuutta rekrytoida uusia työntekijöitä. Ajatuksena on, että jos työsuhteen päättäminen on helpompaa, työnantajat uskaltavat helpommin ottaa henkilöstöriskejä. Tätä perustelua on kuitenkin työntekijäjärjestöjen taholta kritisoitu siitä, että liian väljät irtisanomisperusteet voivat lisätä työntekijöiden epävarmuutta ja heikentää sitoutumista työ-

hön. Erityisesti pienten ja keskisuurten yritysten näkökulmasta helpompi irtisanomismahdollisuus nähdään positiivisena asiana.

Tulevan oikeuskäytännön merkitys

Vaikka lakimuutokset hyväksyttäisiin, niiden käytännön merkitys konkretisoituu vasta tuomioistuinten tulevassa ratkaisukäytännössä. On selvää, että muutos ”asiallisesta ja painavasta syytä” pelkkään ”asialliseen syyhyyn” antaisi tuomioistuimille laajemman harkintavallan määritellä, mitkä tilanteet oikeuttavat työsuhteen päättämisen. Samoin varoitusmenettelyn muutoksen seurauksena voidaan odottaa uusia rajankäyntejä siitä, kuinka erilaiset rikkomukset tai laiminlyönnit voidaan rinnastaa toisiinsa.

Näin ollen työnantajat ja työntekijät joutuvat joka tapauksessa odottamaan, millaisia linjauksia käräjäoikeudet, hovioikeudet ja viime kädessä korkein oikeus tulevat tekemään. Vasta nämä linjaukset antavat todellisen kuvan siitä, missä irtisanomiskynnyksen uusi raja kulkee. Mikäli lakimuutokset hyväksytään, voidaan perustellusti odottaa, että irtisanomissuoja heikkenee ainakin jossain määrin.

JUKKA RAHIKALA
Asianajotoimisto Rahikkala Oy
044 0400 004



Kokonaisratkaisu turvallisuuden ja kulkemisen hallintaan

Vie organisaatiosi tehokkuus, kulkemisen hallinta ja turvallisuus uudelle tasolle ja hyödynnä koko potentiaalisi **ABLOY OS** -kulunvalvonta- ja **PROTEC² 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



ABLOY