

AVAIN

UUTISET • 1.2025



Pääkirjoitus	
Turvaurakoitsijat ry 55 vuotta	2
.....	
Puheenjohtajan palsta	
Osallistu ja vaikuta	3
.....	
Sormisuojaus	
automaattioivissa	4
.....	
Turvallinen tulevaisuus	
NIS2-direktiivin myötä	5
.....	
Järjestäytynyt rikollisuus	7
.....	
Somehuijaukset	8
.....	
Verkkorikollisuus kasvussa	9
.....	
Tuoteuutuuksia	11
.....	
Lakipalsta:	
Hankintalain uudistus	12
.....	

Turvaurakoitsijat ry 55 vuotta

Kun järjestöme perustettiin 55 vuotta sitten, maailma oli täysin erilainen. Turvallisuusalan nojasi mekaanisiin järjestelmiin ja perinteisiin toimintamalleihin, joissa lukitus- ja valvontaratkaisut olivat pitkälti manuaalisia. Tänäpä seisoimme digitaalisen vallankumouksen keskellä, jossa kehittynyt teknologia, automaatio ja kyberturvallisuus ovat muodostuneet alan keskeisiksi kulmakiviksi.

Viisikymmentäviisi vuotta sitten turvallisuusalan ratkaisut perustuivat mekaanisiin lukitusjärjestelmiin ja analogiseen valvontaan. Teknologinen kehitys eteni asteittain, ja 1980-luvulla sähkömekaaniset lukitusratkaisut alkoivat yleistyä. 1990-luvulla digitaalinen murros toi mukanaan muun muassa elektroniset kulunvalvontajärjestelmät ja valvontakamerateknologian kehityksen.

2000-luvun alussa turvallisuusala koki merkittävän teknologisen loikan. Älylukot, biometrinen tunnistus, pilvipohjaiset valvontajärjestelmät ja IoT-ratkaisut nousivat turvallisuusratkaisujen keskiöön. Tänäpä turvallisuus ei enää tarkoita vain fyysisten rakenteiden suojaamista – se on kokonaisvaltainen

digitaalinen ekosysteemi, jossa kyberturvallisuus ja fyysinen turvallisuus kulkevat käsi kädessä.

Teknologian kehitys tuo mukanaan myös uusia haasteita. Kyberuhkien kasvu ja digitaalisten infrastruktuurien haavoittuvuus ovat tehneet turvallisuusalaista entistä monimutkaisemman. Tietosuojalainsäädäntö, kuten GDPR, ja kansalliset kyberturvallisuusohjelmat ovat määritelleet uusia standardeja alan toimijoille, mikä vaatii jatkuvaa sopeutumista ja ennakoivaa turvallisuusajattelua.

Järjestöme on ollut aktiivisesti mukana kehittämässä alan parhaita käytäntöjä ja tukemassa jäsenyrityksiämme muutoksessa. Olemme investoineet koulutukseen, tutkimukseen ja yhteistyöhön varmistaaksemme, että turvallisuusala pystyy vastaamaan digitalisaation tuomiin haasteisiin ja hyödyntämään sen tarjoamia mahdollisuuksia.

Tulevaisuus tuo mukanaan entistä älykkämpiä ja integroituneempia turvallisuusratkaisuja. Tekoäly ja koneoppiminen mahdollistavat uhkien ennakoivan tunnistamisen ja eh-

käisyn, automaatio parantaa järjestelmien toimintavarmuutta, ja hajautetut tietoverkkoratkaisut tekevät kyberturvasta entistä kestävämpää. Älykkäät turvajärjestelmät tulevat olemaan entistä enemmän osa päivittäistä elämääme ja jäsenyritystemme palveluvalikoimaa.

Järjestöme jatkaa työtään alan kehityksen eturintamassa. Tavoitteenamme on edistää turvallisuusratkaisuja, varmistaa alan korkeimmat turvallisuusstandardit ja tukea jäsenyrityksiämme jatkuvassa muutoksessa, joka muovaa turvallisuuden tulevaisuutta.

Tämä merkkivuosi ei ole vain katsaus menneeseen, vaan myös lupaus tulevasta. Yhdessä voimme rakentaa turvallisemman ja teknologisesti kehittyneemmän yhteiskunnan – seuraavat vuosikymmenet tulevat olemaan vähintään yhtä innovatiivisia kuin menneet.

Kiitos kaikille jäsenillemme ja yhteistyökumppaneillemme, jotka ovat olleet mukana tällä matkalla. Juhlistakaamme yhdessä turvallisuuden ja teknologian kehitystä!

Sigurd Wijkmanin 5.3.1970 lähettämässä perustettavan yhdistyksen kokouskutsussa päätettiin perustaa koko Suomen kattava liitto, jonka tarkoituksena oli valvoa ja suojella lukkoseppien yhteisiä etuja. Pienyrittäjinä he olivat yksinään voimattomia, mutta yhdessä he pystyivät vaikuttamaan ja kehittämään toimialaa.

Peruskivi on edelleen tallella, vaikka paljon on muuttunut noista päivistä. Millainen turvaurakoitsijoiden maailma onkaan tulevien vuosikymmenten kuluttua? Sen kertoo vain aika. Avataan ovi yhdessä tulevaisuuteen.



Ona Gardemeister, toimitusjohtaja

Osallistu ja vaikuta

– Turvaurakoitsijat ry:n vuosikokoustapahtuma 2025

Turvaurakoitsijat ry kutsuu jäsenensä vuoden tärkeimpään tapahtumaan, jossa turvallisuusala kohtaa, verkostoituu ja vaikuttaa! Nyt on aika juhlia yhdistyksemme 55-vuotista taivalta yhdessä alan huippuosaajien kanssa! Vuosikokoustapahtuma järjestetään 11.4.2025 Clarion Hotel Airport Helsingissä, jossa on luvassa hienoja asiantuntijapuheenvuoroja, inspiroivia keskusteluja sekä kollegoiden ja yhteistyökumppaneiden tapaamista.

Turvaurakoitsijat ry:n sääntömääräinen vuosikokous on paikka, jossa jäsenistöllä on mahdollisuus vaikuttaa ja tuoda oma näkemysensä esille mihin suuntaan ry:n toiminta tulisi viedä tulevaisuudessa. Vuosikokouksessa kerätään ideoita ja ajatuksia siitä, millaisena yhdistyksen toiminta haluttaisiin nähdä jatkossa. Nämä toiveet muodostavat hallitukselle suunnan ja tulevan kauden painopisteet ja kehityskohteet.

Sääntömääräinen kokous on vain osa vuosikokoustapahtumaa. Iso osa tapahtumasta

muodostuu verkostoitumisesta kollegoiden kanssa. Viime syksyn tapahtuman palautteissa monet teistä toivoi lisää aikaa keskusteluille ja yhdessäololle. Tämä otettiin huomioon, kun suunnittelimme 55-vuotisjuhlaa. Aikaa tapahtumalle on varattu enemmän ja ohjelma tehty hieman väljemmäksi.

Juhlakokouksen ohjelma on tuttuun tapaan osittain asiapitoinen ja osittain viihdepainotteinen. Asiaosuudesta vastaa kansanedustaja ja Aalto-yliopiston kyberturvallisuuden työelämäprofessori **Jarmo Linnell**, joka pitää meille katsauksen vallitsevaan turvallisuus tilanteeseen. Toisesta päivän luennoista vastaa Kesko Oyj:n Senior Manager, Security&Safety Grocery Trade Logistics **Vesa Manninen**, jonka esitys keskittyy yritysten muuttuviin turvallisuusvaatimuksiin. Molempien puhujien aiheet erittäin ajankohtaiset ja koskettavat varmasti jokaista jäsenliikettämme.

Edellisen kokouksen palautteissa esiin nousi myös toive saada enemmän aikaa yhteis-

toimintajäsenten tuote- ja palveluesittelyille. Perinteitä vaalien myös kevään juhlakokouksessa järjestetään suosittu yhteistoimintajäsenten tuote- ja palveluesittely, mutta aiemmasta poikkeavalla kaavalla. Nyt pidämme sen kahdessa osassa ja aikaa on varattu lähes tuplasti. Näin haluamme varmistaa kaikille mahdollisuuden tutustua tuotteisiin, palveluihin ja yrityksiin.

Vuosikokoustapahtuma huipentuu gaalailalliseen, jossa myös palkitaan vuoden turvaurakoitsija sekä vuoden yhteistoimintajäsen. Gaalan juontaa toimittaja **Tommy Fränti** ja viihdepuolesta vastaa House band. Tätä juttua kirjoittaessa tapahtumaan on ilmoittautunut todella paljon osallistujia, mutta mukaan mahtuu vielä. Tule tapahtumaan mukaan kuulemaan alaamme koskevista asioista sekä nauttimaan kollegoiden seurasta ja verkostoitumaan.

Osallistumalla voit vaikuttaa, nähdään Clarion Hotel Airportissa 11.4.2025!

Jyri Aho, puheenjohtaja

Sormisuojaus automaattioivissa

– EN 16005 -standardin keskeiset vaatimukset



Automaattiovet ovat olennainen osa julkisia ja kaupallisia tiloja, mutta niiden turvallisuus ei ole itsestäänselvyys. Yksi merkittävimmistä riskeistä liittyy sormien puristumis- ja leikkaantumisvaaroihin, joita voi esiintyä erityisesti oven liikkuvissa osissa. EN 16005 -standardi asettaa tarkat vaatimukset sormisuojaukselle, joiden avulla voidaan estää tapaturmia ja parantaa turvallisuutta.

Miksi sormisuojaus on tärkeää?

Automaattiovien suunnittelussa ja käytössä on tärkeää huomioida turvallisuusriskit, joista

sormivammat ovat yksi yleisimmistä. Erityisesti lapset, vanhukset ja liikuntarajoitteiset henkilöt ovat alttiita onnettomuuksille, ja heidän turvallisuutensa takaaminen edellyttää tehokkaita suojoitoimenpiteitä. EN 16005 -standardi määrittelee, miten automaattiovien sormisuojausten tulee toimia ja mitkä alueet tulee suojata mahdollisilta vaaratilanteilta.

Standardin mukaan automaattiovien vaaravyöhykkeet ulottuvat 2,5 metrin korkeudelle lattiasta tai muusta kulkutasosta mitattuna. Suojaus on suositeltavaa koko vaaravyöhykkeelle, mutta vähimmäisvaatimuksena pidetään 1,9 metrin korkeutta. Erityisen kriittisiä alueita ovat oven käyntisivu sekä saranapuolen rakoväli, joissa sormien jääminen puristuksiin on todennäköisintä.

Sormisuojausten toteuttamisessa voidaan hyödyntää useita eri ratkaisuja. Mekaaniset sormisuojaajat estävät fyysisesti sormien joutumisen vaaravyöhykkeelle, kun taas anturitekniikka havaitsee lähellä olevan esteen ja pysäyttää oven ennen kontaktia. Usein paras lopputulos saavutetaan näiden kahden menetelmän yhdistelmällä, jolloin turvallisuus on maksimaalinen ilman, että oven käyttömukavuus kärsii. Voidaankin todeta, että automaattiovien täydellinen sormisuojaus vaatii sensorin ja mekaanisen sormisuojaajan yhdistelmää.

Vaikka EN 16005 -standardi koskee ensisijaisesti uusia automaattiovia, myös vanhojen ovien turvallisuus on tärkeää. Konedirektiivin (MD 2006/42 EC) mukaan kaikkien käytössä olevien koneiden – mukaan lukien automaattiovet – on täytettävä ajankohtaiset turvallisuusvaatimukset. Tämä tarkoittaa, että myös vanhat ovet voidaan ja tulisi päivittää nykyaikaisilla sormisuojausratkaisuilla.

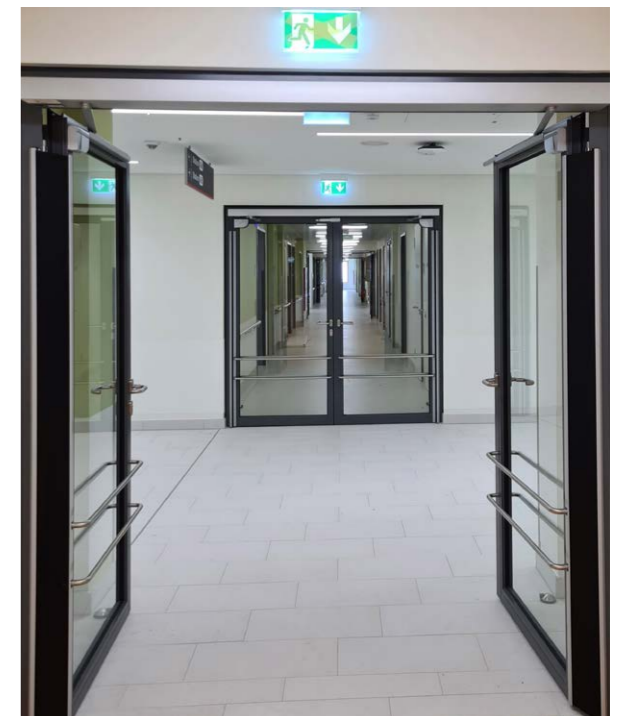
Huolto ja päivitykset ovat avainasemassa turvallisuuden ylläpitämisessä. Säännöllisillä tarkastuksilla voidaan varmistaa, että ovet toimivat turvallisesti ja että mahdolliset puutteet havaitaan ajoissa. Suositeltavaa on, että kaikki automaattiovet huolletaan vähintään kerran vuodessa, kun taas pelastusteiden automaattioville suositellaan kahden tarkastuskerran vuosittaista aikataulua.

Oikeanlainen sormisuojaus lisää turvallisuutta ja parantaa käyttäjäystävällisyyttä. Hyvin suunnitellut suojaratkaisut eivät häiritse oven toimintaa, vaan ne integroituvat saumattomasti kokonaisuuteen. Siksi on tärkeää valita laadukkaat ja testatut ratkaisut, jotka kestävät pitkään ja takaavat turvallisen käytön vuosiksi eteenpäin.

Raitatuote tarjoaa mekaanisia sormisuojaajia, jotka estävät fyysisen kosketuksen vaaravyöhykkeelle. Heidän maahantuomansa Athmer-

sormisuojaajat on testattu kestämaan yli miljoona käyttösykliä. Yritys tarjoaa myös nopeita toimitukset ja teknisen tuen, jolla varmistetaan sujuva käyttöönotto ja ylläpito.

Turvallisuus on investointi, joka maksaa itsensä takaisin vähentyneinä tapaturmina ja parempana käyttökokemuksena. Varmistamalla, että automaattiovet täyttävät EN 16005 -standardin vaatimukset, voidaan merkittävästi parantaa tilojen turvallisuutta ja käyttömukavuutta. Oikeilla ratkaisuilla jokainen ovi voi olla sekä turvallinen että toimiva.



Turvallinen tulevaisuus **NIS2**-direktiivin myötä

Digitaalisen maailman turvallisuus on noussut keskeiseksi huolenaiheeksi niin yrityksille kuin julkisille toimijoillekin. Kriittisen infrastruktuurin suojeleminen on entistä tärkeämpää, kun kyberuhkat ja operatiivisiin järjestelmiin kohdistuvat riskit monimutkaistuvat. Aluesuojaus ja videovalvonta ovat keskeisiä tekijöitä turvallisuuden varmistamisessa, ja niiden vaatimukset ovat kasvaneet merkittävästi.

NIS2-direktiivi ja Suomen kyberturvallisuuslaki

Euroopan unionin NIS2-direktiivi asettaa uudet vaatimukset kriittisen infrastruktuurin suojaamiselle. Direktiivin tavoitteena on vahvistaa kyberturvallisuutta ja yhtenäistää riskienhallintaa koko EU:n alueella. Suomi on edistynyt direktiivin käyttöönotossa, ja pian voimaan astuva kyberturvallisuuslaki velvoittaa yritykset eri sektoreilla, kuten energia-, terveydenhuolto- ja digitaalisen infrastruktuurin aloilla, noudattamaan uusia tietoturvastandardeja. Laki korostaa myös ylimmän johdon vastuuta kyberturvallisuustoimenpiteiden toteutuksessa.

Hikvisionin panos aluesuojaukseen ja videovalvontaan

Hikvision tarjoaa ratkaisuja, jotka vastaavat kasvaviin kyberturvallisuus- ja valvontavaatimuksiin. Korkean resoluution kamerat, tekoälypohjainen analytiikka ja kehittyneet aluesuojausratkaisut mahdollistavat entistä tehokkaamman valvonnan ja uhkien tunnistamisen.

Keskeisiä ominaisuuksia ovat:

- Korkean resoluution kuvantaminen
 - Tarkka kuva ja kehittynyt kuvankäsittely mahdollistavat luotettavan valvonnan erilaisissa olosuhteissa.
- Tekoälypohjainen analytiikka
 - Kehittyneet analysointityökalut tunnistavat poikkeavat tapahtumat ja parantavat reagointinopeutta.
- Aluesuojausratkaisut
 - Järjestelmät tunnistavat mahdolliset uhat ja estävät luvattoman pääsyn tehokkaasti.

Hikvisionin Secure by Design -lähestymistapa

Turvallisuuden huomioiminen jo suunnitteluvaiheessa on keskeistä kriittisten järjestelmien suojaamisessa. Hikvision noudattaa ”Secure by Design” -periaatetta, joka tarkoittaa, että tuotteet kehitetään alusta alkaen turvallisuus huomioiden.

Tämän lähestymistavan keskeisiä elementtejä ovat:

- Vahva tietoturva-arkkitehtuuri
 - Säännölliset päivitykset ja haavoittuvuuksien hallinta varmistavat järjestelmien turvallisuuden.
- End-to-end-salaus
 - Tiedonsiirron ja tallennuksen suojaaminen takaa tietojen luottamuksellisuuden.
- Säännölliset auditoinnit
 - Turvallisuuskatselmukset auttavat tunnistamaan ja korjaamaan mahdollisia riskejä ajoissa.

Kriittisen infrastruktuurin suojaaminen edellyttää kattavaa turvallisuusstrategiaa ja jatkuvaa valmiutta vastata uusiin uhkiin. NIS2-direktiivin myötä yritysten ja organisaatioiden on kiinnitettävä entistä enemmän huomiota tietoturvakäytäntöihinsä ja valvontaratkaisuihinsa varmistukseen toimintansa jatkuvuuden ja turvallisuuden.

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

Järjestäytynyt rikollisuus suomalaisessa yrityskentässä

Järjestäytynyt rikollisuus on viime vuosina noussut merkittäväksi huolenaiheeksi Suomen viranomaisten ja päättäjien keskuudessa. Harmaan talouden selvitysyksikön tuoreen raportin mukaan rikollisverkostot ovat laajentaneet vaikutusvaltaansa yritysmaailmaan, hyödyntäen yritysraakenteita rikollisen toiminnan peittelyyn ja rahanpesuun.

Selvityksen mukaan Suomessa on yli 2 400 yritystä, jotka ovat kytköksissä järjestäytyneeseen rikollisuuteen. Nämä yritykset toimivat erityisesti rakennusalalla, kiinteistöalalla ja autokaupassa, joissa esiintyy perinteisesti paljon harmaan talouden piirteitä. Rikollisorganisaatioihin sidoksissa olevien yritysten vastuuhenkilöillä on usein taustallaan rikoshistoria, ja monet näistä yrityksistä ovat taloudellisesti heikkoja, vakiintumattomia ja verovelkaisia.

Raportissa käytetty aineisto koostuu poliisin tiedustelutiedoista, joissa tunnistettiin 1 872 henkilöä, joilla oli sekä kytköksiä rikollisuuteen että vastuutehtäviä yrityksissä. Tämä henkilöryhmä jakautui kahteen kategoriaan: A-kategoria (269 henkilöä, 273 yritystä) ja B-kategoria (1 603 henkilöä, 2 134 yritystä), perustuen kytköksen varmuuteen ja vahvuuteen.

Järjestäytyneen rikollisuuden kytköksissä olevat yritykset aiheuttavat vuosittain merkittävän verovajeen yhteiskunnalle. Raportin ar-

vioiden mukaan menetettyjä verotuloja on noin 65 miljoonaa euroa vuosittain, josta noin 25 miljoonaa euroa on jo havaittu verotarkastuksissa ja noin 40 miljoonaa euroa on piilossa. Kokonaisuudessaan nämä yritykset raportoivat noin 1,5 miljardin euron liikevaihdon ja noin 350 miljoonan euron varallisuuden.

Velvoitteiden hoidon osalta rikollisverkostoihin liittyvissä yrityksissä havaittiin merkittäviä laiminlyöntejä. Yritykset olivat huomattavasti verovelkaisempia kuin verrokkiyritykset, ja niiden ilmoituskäytännöt olivat puutteellisia. Tämä viittaa systemaattiseen harmaan talouden hyödyntämiseen ja rikolliseen veronkiertoon.

Miten järjestäytynyttä rikollisuutta voidaan tunnistaa ja torjua?

Raportissa tarkasteltiin myös mahdollisuuksia tunnistaa järjestäytyneeseen rikollisuuteen kytkeytyneitä yrityksiä verotustietojen perusteella. Koneoppimismalleilla tehdyn analyysin perusteella tietyt talouden tunnusluvut, kuten verovelka, rekisteröitymättömyys ja ilmoituspuutteet, korreloivat vahvasti JR-kytköksen kanssa. Tämän tiedon avulla voidaan kehittää työkaluja, jotka auttavat viranomaisia tunnistamaan ja puuttumaan rikollisten yritysten toimintaan tehokkaammin.

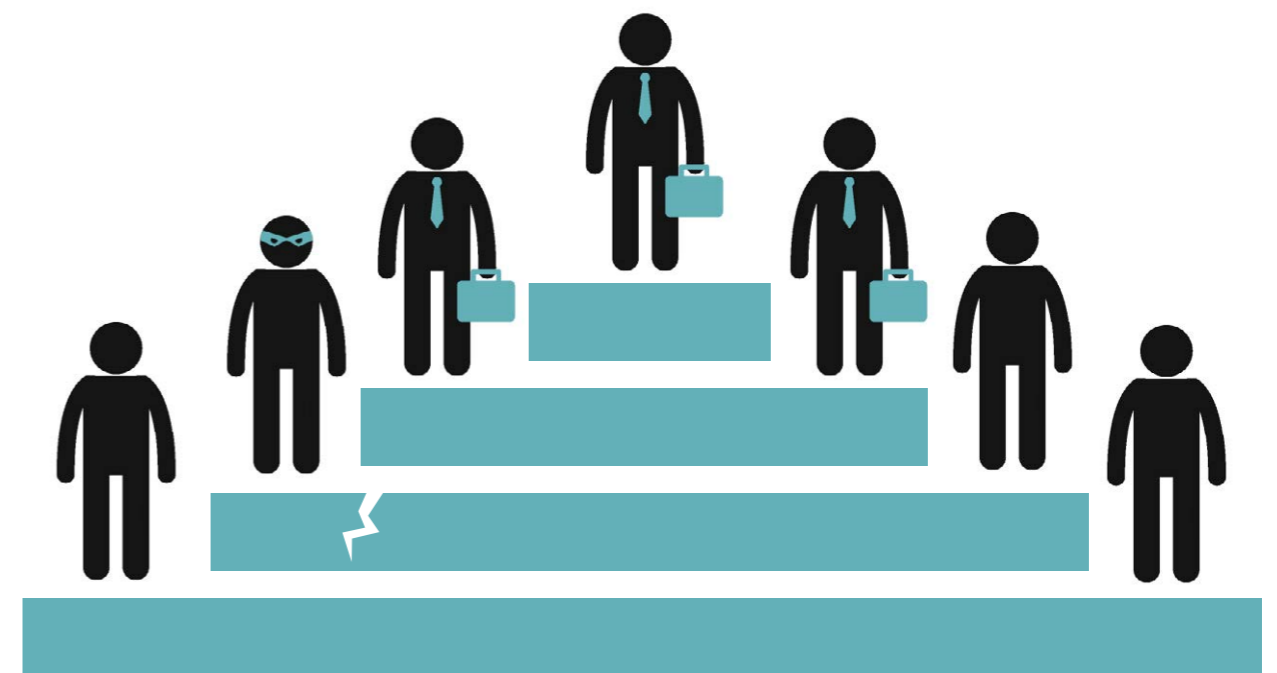
Hallinnollisella tasolla on käynnistetty useita hankkeita rikollisuuden torjumiseksi yritys-

kentässä. Esimerkiksi valtionavustuslakia on pyritty uudistamaan siten, että viranomaiset voisivat paremmin estää rikollisten toimijoiden pääsyn julkisiin tukiin ja avustuksiin. Myös kansainvälinen yhteistyö on keskeistä, sillä rikollisverkostot toimivat usein rajat ylittävästi.

Järjestäytynyt rikollisuus on vakiinnuttanut asemansa suomalaisessa yrityskentässä, erityisesti harmaan talouden riskialoilla. Rikollisten yritysten toiminta aiheuttaa merkittävää taloudellista haittaa yhteiskunnalle, heikentää rehellisten yritysten kilpailuasemaa ja vaarantaa yritystoiminnan luotettavuutta.

Tulevaisuudessa torjuntatoimien tehokkuutta voidaan parantaa kehittämällä viranomaisyhteistyötä, parantamalla tiedonvaihtoa ja ottamalla käyttöön uusia teknologioita rikollisen yritystoiminnan tunnistamiseksi. Lainsäädännön kehittäminen siten, että rikollisten mahdollisuuksia yritystoiminnan välityksellä rajataan tehokkaasti, on keskeinen askel kohti oikeudenmukaista ja turvallista yritysympäristöä.

Lähde: Verohallinto, harmaan talouden torjuntayksikön selvitys 14/2024



SOMEHUIJAUKSET

Sosiaalisen median käyttäjiä yritetään jallittaa monin tavoin. Likejacking on suuren yleisön kenties huonommin tuntema ilmiö.

Tietoturvyhtiö Panda Securityn mukaan kyse on piilotetuista Facebookin tykkäysnapista, joita käyttäjät tulevat painaneeksi tietämättään. Se voi johtaa suureen määrään ei-toivottua tai suorastaan haitallista sisältöä käyttäjän Facebook-syötteessä. Kyse on tavasta saada käyttäjä tykkäämään Facebook-päivityksestä tai -sivusta ilman hänen suostumustaan.

Temppu voi onnistua piilottamalla tykkäysnappi Facebookin ulkopuolisilla verkkosivuilla vaikkapa houkuttelevaan tarjoukseen tai videoon. Kun käyttäjä yrittää klikata tarjousta tai katsoa videota, hän tulee tietämättään painaneeksi tykkää-nappia, mikä voi nostaa haitallisen sisällön näkyvyyttä ja suosiota Facebookissa.

Likejacking on yksi kymmenestä somehuijauksesta, joista Panda varoittaa. Tässä ovat loput 9 IS:n muokkaamina:

1. Identiteettivarkaudet: Hyökkääjät voivat käyttää julkisia valokuvia ja tarkkoja tietoja luodakseen vääriä profileja sosiaaliseen mediaan. Rikolliset voivat toisen henkilön

nimissä houkutellessa ihmisiä esimerkiksi sijoittamaan rahaa.

2. Kyberkiusaaminen: Vahingolliset viestit tai päivitykset tai muu julkisesti tai yksityisesti jaettu sisältö voi tuottaa paljon tuskaa. Pidä tilisi yksityisinä ja ilmoita alustalle haitallisesta toiminnasta.

3. Väärät arvonnat: Huijarit matkivat usein oikeita brändejä ja mainostavat niiden nimissä arvontoja tai väittävät sinun voittaneen jotain. Palkinnon lunastaminen edellyttää henkilökohtaisten tietojen, kuten luottokortin numeron, luovuttamista. Oikeasti mitään palkintoa ei ole.

4. Tietojenkalastelu: Väärät viestit linkkeineen voivat näyttäytyä päällisin puolin esimerkiksi pankin lähettämiltä, mutta

niillä pyritään muun muassa varastamaan pankkitilillä olevat rahasi. Viestejä lähetetään suuria määriä perinteisinä tekstiviesteinä.

5. Tietomurrot: Jos somepalvelu murretaan ja sieltä onnistutaan varastamaan käyttäjien tietoja henkilötunnuksista luottokortin numeroon, uhrien tulee esimerkiksi kuolettaa korttinsa ja vaihtaa salasanansa. Murtojen lisäksi esiintyy julkisten tietojen keräämistä eli kaavintaa.

6. Haittaohjelmat: Haitallisia ohjelmia voidaan jakaa vaikkapa sovellustiedostoina puhelimeen. Vaarallisia linkkejä, tiedostoja tai päivityksiä voidaan upottaa somepäivityksiin tai videoihin, jotta hyökkääjät pääsisivät saastuttamaan puhelimia ja kaappaamaan tilejä.

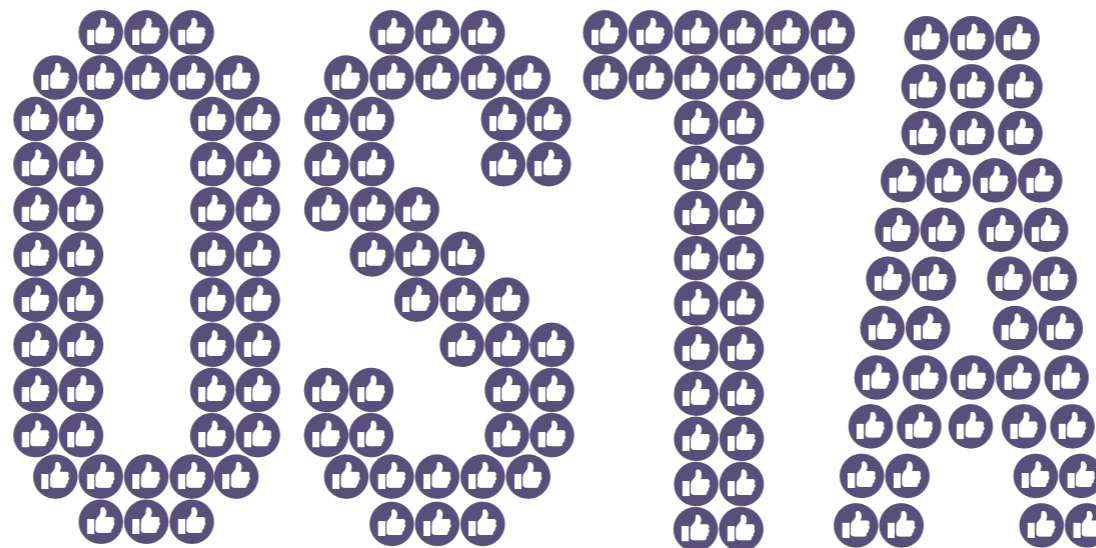
7. Brändien matkiminen: Huijarit luovat vääriä tilejä someen tunnettujen brändien nimissä johtaakseen asiakkaita harhaan ja kerätäkseen heidän tietojaan.

8. Kumppanuushuijaukset: Kumppanuusmarkkinointi (affiliate marketing) perustuu mainostajan ja sisällöntuottajan yhteistyöhön. Esimerkiksi videon katsojia voidaan kannustaa ostamaan tuotteita tällaisen yhteislinkin kautta. Huijarien väärät julkaisut lupaavat esimerkiksi lahjakortteja, mutta keräävätkin henkilökohtaisia tietoja tai levittävät haittaohjelmia.

9. Sosiaalinen manipulointi: Rikolliset voivat lähestyä aitojen tahojen nimissä luodakseen luottamusta. Sen onnistuttua uhri voi olla herkempi luovuttamaan esimerkiksi kirjautumistunnuksiaan tai muita henkilökohtaisia tietojaan.

Pandan mukaan hyökkääjät käyttävät armotta hyväkseen sitä valtavaa määrää henkilökohtaista tietoa, joka on jo valmiiksi saatavilla sosiaalisessa mediassa. Tilannetta pahentavat heikot salasanat ja kaksivaiheisen tunnistuksen käyttämättä jättäminen.

Lähde: Digitoday 1.3.2025



Verkkorikollisuus kasvussa



Suomalaiset menettivät verkkorikollisille yhteensä 62,9 miljoonaa euroa viime vuonna, Finanssiala ry laskee. Vuonna 2023 menetykset olivat yli 44 miljoonaa euroa.

Kaikkiaan rikolliset yrittivät huijata suomalaisia 107,2 miljoonan euron edestä viime vuonna verrattuna edeltävän vuoden 76,9 miljoonaan euroon. Pankit pystyivät pysäyttämään ja palauttamaan 44,3 miljoonaa euroa. Se on 35 prosenttia edellisvuotta enemmän.

Eniten rahaa, 31,9 miljoonaa euroa, menetti tietojenkalasteluhuijauksissa, joiden määrässä kasvu oli rajuinta, peräti 161 prosenttia. Sijoitushuijarit saivat salkkuunsa 20,1 miljoonaa euroa.

Huijarit käyttävät kalasteluun entistä monipuolisempia keinoja, kuten puhelinsoittoja, esiintyen esimerkiksi poliisina ja pankin työntekijänä. Huijarit luovat usein kiireen tuntua, mutta etenkin maksuja vahvistettaessa on syytä katsoa tarkkaan, mihin rahat ovat menossa.



Pankkien tilastot osoittivat merkittävää laskua rakkaushuijausten määrässä, mutta se johtuu kuitenkin siitä, että osaa rakkaushuijauksista on alettu luokitella tilastoissa sijoitushuijauksiksi. Rakkaushuijarit saattavat tarjota uhreilleen ”sijoitusmahdollisuuksia”, jotka osoittautuvat lopulta huijauksiksi.

Finanssiala ry:n petos- ja rikostorjunnasta vastaava johtaja **Niko Saxholm** korostaa, etteivät huijaukset lopu pelkällä torjunnalla.

– Tietojenvaihtoa sekä pankkien välillä että pankkien ja viranomaisten välillä olisi tehostettava huomattavasti. Nykyisen lainsäädännön vuoksi se on tällä hetkellä varsin rajattua, Saxholm arvioi tiedotteessa.

Saxholm haluaa saada sosiaalisen median jättiläiset ja internetin kauppapaikat poistamaan rikollisten mainokset alustoiltaan.

- Älä mene verkkopalveluun hakukoneen tai vaikkapa sähköpostiin tai tekstiviestinä tulleen verkkolinkin kautta.
- Etsi sähköposteista tai tekstiviesteistä epäilyttäviä yksityiskohtia, kuten väärin



kirjoitettuja verkkotunnuksia, kirjoitusvirheitä, vääriä päivämääriä ja muita virheellisiä tietoja. Hyvä suomi taikka oikeat tiedot eivät silti takaa viestin aitoutta.

- Kirjoita osoite itse selaimen osoiteriville ja huolehdi, että siinä ei ole kirjoitusvirheitä. Tallenna osoite selaimen kirjanmerkkeihin. Näin vältyt naputtelemasta sitä seuraavalla kerralla.
- Jos sijoitus- tai lainatarjous kuulostaa liian hyvältä ollakseen totta, on parasta olla tarttumatta siihen.
- Kiireen tuntua tarjouksissa kannattaa varoa ja jättää tarjous väliin.
- Jos mahdollista, käytä virallista mobiili-sovellusta selaimessa toimivan verkkopalvelun sijaan. Esimerkiksi pankeilla ja Suomi.fi-palvelulla on tällaiset.
- Käytä tunnistautumiseen mobiilivarmennetta verkkopankkitunnusten sijaan. Mobiilivarmenne on paikoin maksullinen palvelu.
- Käytä kirjautumiseen kaksivaiheista tunnistautumista pelkän salasanan sijaan. Tai harkitse avainkoodien käyttöä.
- Pidä tunnukset omana tietonasi, äläkä syötä niitä sivustolle, jonka aitoudesta et voi varmistua.
- Älä avaa pankin tai muun tahon nimissä



lähetettyjä liitteitä, vaan varmista niiden aitous soittamalla nimetyn tahon asiakaspalveluun.

- Jos jokin yllättävä taho pyytää sinua asentamaan laitteellesi ohjelman, älä tee niin. Käytä vain mobiililaitteesi virallista sovelluskauppaa.
- Älä vahvista tapahtumia, joita et tunnista ja tiedä tekeväsi juuri sillä hetkellä. Lue vahvistuspyynnöt aina huolella ja kiinnitä huomiota etenkin siirrettävään rahasummaan – jos jokin ei täsmää, älä vahvista mitään.
- Älä lähetä kuvia henkilöllisyysasiakirjoistasi tuntemattomalle.
- Jos olet myymässä jotain, varmista maksun saapuminen tilille ennen tuotteen luovutusta. Toinen tapa on käyttää perinteistä käteistä.
- Jos epäilet verkkopankkitunnustesi joutuneen väariin käsiin, sulje tunnukset viipymättä soittamalla pankkiin. Tee rikosilmoitus poliisille vasta sen jälkeen. Tällä tavalla maksimoit mahdollisuutesi saada rahasi takaisin.
- Petoksen uhriksi joutumista ei pidä hävetä ja salailla, vaan asiasta on tehtävä aina rikosilmoitus.
- Varoita tuttujasi huijauksesta, vaikka et itse olisi joutunut uhriksi. Jos olet, on nimissäsi saatettu lähettää huijausviestejä esimerkiksi sähköpostistasi löytyville kontakteille.



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

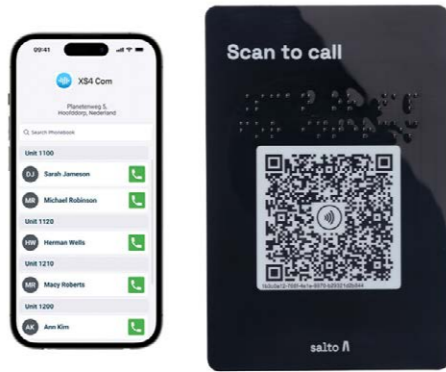
Älykäs, paikallinen kuluvalvontajärjestelmä, jonka laaja ovyksikkövalikoima sekä käytön helppous ja joustavuus vakuuttavat ominaisuuksillaan. Myös mekaaniset lukitusjärjestelmät ovat laajennettavissa kulunvalvonnaksi, joka voidaan integroida osaksi laajempaa on line -kulunvalvontajärjestelmää. dormakaba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

dormakaba 

salto Orion



salto XS4 Com



Salto lanseeraa kaksi uutta kulunvalvonta-innovaatiota

Salto aloittaa vuoden 2025 lanseeraamalla kaksi uutta innovaatiota täydentämään jo ennestään laajaa kulunvalvontavalikoimaa. Salto Orion tuo markkinoille edistyksellisen ja ennennäkemättömän kasvojentunnistusteknologian osana kulunvalvontaa ja Salto XS4 Com tarjoaa pilvipalvelupohjaisen oivpuhelinjärjestelmän helppokäyttöiseen vierailijoiden hallintaan.

”Molemmat innovaatiot keskittyvät kiinteistöjen turvallisuuden parantamiseen, helppokäyttöisyyteen ja järjestelmän helppoon käyttöönottoon ja ne sopivat eri tyyppisiin kokonaisuuksiin aina toimitilaratkaisuista asumiseen ja julkisiin tiloihin”, kommentoi **Katriina Forsback**, Salto Systems Oy:n maajohtaja.

ARQUE – pieni ja tyylikäs turvavalaisin

Arque on minimalistinen ja monipuolinen turvavalaisin, jota voidaan käyttää myös opastevalaisimena lisätarvikkeiden ansiosta. Se on erinomainen valinta useimpiin sisätiloihin, kuten toimistoihin, kauppoihin, hotelleihin, ravintoloihin jne. Perusmalli on tarkoitettu joko käytävien ja poistumisreittien, tai sitten avoimien alueiden valaisemiseen, linsistä riippuen. Valaisinta voidaan helposti täydentää pleksilaisella opasteella, joka napsautetaan pohjakehykseen. Arquessa on sisäänrakennettu turvavalaisusyksikkö ja LiFePO4-akku. IP44-kotelointiluokan ansiosta se soveltuu myös kosteisiin tiloihin. Arque on saatavilla valkoisena ja mustana ja sillä on viiden vuoden tuotetakuu.

Tutustu tarkemmin uutuuteen kamic.fi



CDVI lanseeraa ROBUSTAn: Uusi käsilähetin vaativiin ympäristöihin

Vuosikymmenten kokemuksella langattomista ohjausjärjestelmistä CDVI esittelee nyt ROBUSTAn, neljän painikkeen käsilähtetimen, joka on suunniteltu vastaamaan vaativien ympäristöjen tarpeisiin. ROBUSTA on ihanteellinen porttien, ovien, hissien ja kulunhallintajärjestelmien ohjaukseen, ja sen kestävä rakenne tekee siitä sekä kosteus- että iskunkestävän, mikä sopii erinomaisesti ulkokäyttöön ja teollisiin sovelluksiin.

Tärkeimmät ominaisuudet:

- Ergonominen muotoilu – Pyöristetty takaosa varmistaa, että lähetin pysyy kädessä.
- Selkeät kontrastivärit – Keltaiset ja mustat värit tekevät painikkeista helposti erottuvia ja käytettäviä.
- Äänivahvistus – Sisäänrakennettu summeri antaa selkeän äänisignaalin painikkeen yhteydessä, korvaten LED-ilmaisimen tarpeen.
- Korkea kestävyys – ROBUSTA kestää sekä pudotuksia että vettä, mikä takaa toimintavarmuuden eri ympäristöissä.
- Taktinen tuntopalaute – Uritettu painike helpottaa oikean toiminnon tunnistamista ilman, että tarvitsee katsoa.



ROBUSTA käyttää 64-bittistä KeeLoq® Hopping Code -salausmekanismia, joka varmistaa turvallisen signaalin siirron ja suojaa salakuuntelulta ja kopioinnilta. Sen kestävä kotelo ja käyttäjystävällinen muotoilu tekevät siitä luotettavan ratkaisun vaatimpiin sovelluksiin.

Käsilähetin on nyt saatavilla FSM:ltä ja valmis ostettavaksi!

Hankintalain uudistus

Hankintalain uudistushanke tuo toteutukseen merkittäviä muutoksia, joista yksi keskeisimpiä on sidosyksikköhankintoihin kohdistuva 10 prosentin vähimmäisomistusvaatimus. Tämä tarkoittaa, että hankintayksikön, kuten kunnan tai hyvinvointialueen, tulee omistaa vähintään 10 prosenttia sidosyksiköstä, jotta se voi tehdä hankintoja ilman kilpailutusta.

Tämä muutos voi lisätä turvallisuusalan kilpailutuksia, sillä nykyiset mahdolliset sidosyksiköt eivät välttämättä enää täytä uusia omistusvaatimuksia. Tämä voi tarkoittaa uusien tarjouskilpailujen avautumista, mutta samalla muutoksia nykyisiin hankintasuhteisiin.

Markkinakartoitus ja hankintojen jakaminen osiin

Uudistus korostaa markkinakartoitusten merkitystä ja tekee niistä pakollisia yli 10 miljoonan euron hankinnoissa. Tämä tarjoaa mahdollisuuden vaikuttaa hankintojen suunnitteluun jo ennen kilpailutusta.

Markkinakartoitus on hankintayksikön tekemä selvitys ennen varsinaista tarjouskilpailua. Sen avulla kartoitetaan markkinoilla olevia tuotteita, palveluita ja toimittajia sekä arvioidaan, millaisia vaihtoehtoja hankinnalle on saatavilla.

Sen tarkoituksena on varmistaa, että hankinta vastaa tarpeita ja on realistinen, saada tietoa markkinoiden kilpailutilanteesta ja uusista ratkaisuista sekä parantaa hankintaprosessin tehokkuutta ja laatua.

Markkinakartoitusta voidaan toteuttaa esimerkiksi keskusteluilla ja tapaamisilla potentiaalisten toimittajien kanssa, kyselyillä ja tietopyynnöillä yrityksille tai toimialajärjestöille, seminaareilla ja työpajoilla sekä julkaisemalla avoimia pyyntöjä hankintayksikön verkkosivuilla.

Hankintalain (1397/2016) 65 § sallii markkinakartoituksen, mutta edellyttää, että se tehdään avoimesti ja tasapuolisesti kaikille potentiaalisille toimittajille, se ei saa suosia tai syrjiä mitään yritystä tarjousvaiheessa eikä se saa rajoittaa kilpailua, esimerkiksi siten, että tarjouspyyntö suunnataan vain yhdelle yritykselle.

Uudessa hankintalain uudistuksessa esitetään, että markkinakartoitus olisi pakollinen yli 10 miljoonan euron hankinnoissa, mikä lisäisi sen käyttöä erityisesti suurissa rakennus- ja turvallisuushankinnoissa.

Yrityksille markkinakartoitus tarjoaa mahdollisuuden vaikuttaa hankinnan sisältöön ennen

kilpailutusta, parantaa niiden näkyvyyttä hankintayksikön suuntaan sekä auttaa varautumaan tulevaan tarjouskilpailuun ja räätälöimään tarjouksen paremmin. Sen vuoksi yritysten kannattaa seurata markkinakartoituksia ja osallistua aktiivisesti, jotta ne voivat paremmin kilpailuttaa tuotteitaan ja palveluitaan julkisissa hankinnoissa.

Lisäksi EU-hankintojen jakaminen osiin tulee pääsäännöksi, ellei tälle ole perusteltua syytä. Tämä voi avata pienille ja keskisuurille lukuille enemmän mahdollisuuksia, sillä suuret turvallisuus- ja lukitusjärjestelmähankinnat on jatkossa jaettava pienempiin osiin tai kilpailutettava erikseen.

Kilpailutuksen uusiminen ja poissulkemisperusteiden laajentaminen

Jatkossa tarjouskilpailu on uusittava, jos tarjouksia saadaan vain yksi, ellei hankintayksikkö ole tehnyt markkinakartoitusta tai jakanut hankintaa osiin. Tämä voi pidentää kilpailutusprosessia ja lisätä tarvetta panostaa tarjosten valmisteluun.

Poissulkemisperusteita laajennetaan koskemaan esimerkiksi korkean riskin toimittajia, mikä voi vaikuttaa erityisesti turvallisuustuotteita ja -palveluita tarjoaviin yrityksiin.

Miten kannattaa varautua?

Hankintalain muutokset lisäävät toteutukseen kilpailutuksia ja markkinoiden avoimuutta, mutta edellyttävät yrityksiltä aktiivista sopeutumista: Seuraa sidosyksikköhankintojen muutoksia ja varmista, vaikuttaako uusi omistusvaatimus nykyisiin sopimuksiin. Osallistu markkinakartoituksiin ja tuo yritys esille jo ennen kilpailutusta. Valmistaudu tarjouskilpailujen lisääntymiseen, sillä hankintojen jakaminen osiin avaa uusia mahdollisuuksia. Huolehdi yrityksen ja tuotteiden turvallisuusvaatimuksista ja varmista, ettei yrityksesi kuulu poissuljettaviin toimittajiin.

Hankintalain uudistus tuo sekä haasteita että mahdollisuuksia. Lukkoliikkeiden kannattaa pysyä aktiivisina ja hyödyntää muuttuva markkinatilanne parhaalla mahdollisella tavalla.

JUKKA RAHIKALA
Asianajotoimisto Rahikkala Oy



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