

AVAIN

UUTISET • 3.2026



Pääkirjoitus	
Tekoäly tuli työpaikoille, mutta tuliko harkinta mukana?	2
.....	
Puheenjohtajan palsta	
Uusia mahdollisuuksia rakentamassa	3
.....	
Turvallinen työ on laadukasta	4
.....	
Fyysinen murto vai kyberhyökkäys?	6
.....	
CRA: Kun lukko ei enää ole vain lukko	8
.....	
Teletilojen päivitetty lukitussuositus	11
.....	
Lakipalsta	
Urakan takuuajan vakuus ja takuu	12
.....	

Tekoäly tuli työpaikoille, mutta tuliko harkinta mukana?



Tekoälystä on tullut lyhyessä ajassa osa tavallista työpäivää. Sillä kirjoitetaan, käännetään, etsitään tietoa, tehdään yhteenvetoja ja haetaan ideoita. Moni meistä käyttää tekoälyä jo lähes huomaamatta ja uusia käyttötapoja löytyy jatkuvasti.

Kehitys on ollut niin nopeaa, etteivät työpaikkojen pelisäännöt ole aina pysyneet mukana. Uuden työkalun kohdalla ensimmäinen ajatus on helposti se, mitä kaikkea sillä voisi tehdä. Turvallisuusosalalla yhtä tärkeä kysymys on kuitenkin: **mitä sille voi kertoa?**

Lukkoseppämestarikilta on nostanut esiin tekoälyn käyttöön liittyvän tietoturvan, ja aihe on erittäin ajankohtainen koko alallemme.

Tekoälypohjaiset työkalut, kuten Copilot, Gemini ja ChatGPT, voivat parhaimmillaan tehostaa arkea ja helpottaa työntekoa. Niiden käytössä on kuitenkin muistettava, että kaikki työssä käsiteltävä tieto ei kuulu tekoälypalveluun.

Turvallisuusosalalla tämä korostuu erityisesti. Asiakastiedot, kohdetiedot, työtilaukset sekä lukitus-, kulunvalvonta- ja muihin turvajärjestelmiin liittyvät tiedot voivat olla erittäin arkaluonteisia. Sama koskee yrityksen sisäisiä ja luottamuksellisia tietoja.

Tekoälypalvelujen käyttöehdot ja tietojen käsittelytavat vaihtelevat. Siksi yrityksessä pitäisi olla selvää, mitä tekoälypalveluja työssä saa käyttää, mihin niitä saa käyttää ja ennen kaikkea millaista tietoa niihin saa syöttää. Luottamuksellista tai turvallisuuden kannalta arkaluonteista tietoa ei pidä syöttää tekoälypalveluun, ellei yritys ole hyväksynyt kyseistä palvelua ja sen käyttötapaa tällaisten tietojen käsittelyyn.

Ohjeistuksen pitäisi myös ulottua koko henkilöstöön. Tekoäly ei ole enää vain toi-

mistossa työskentelevien väline. Puhelimes- sa oleva tekoälysovellus kulkee mukana myös työmaalle, ja houkutus kysyä siltä neuvoa ongelmatilanteessa voi olla suuri. Silloin esimerkiksi valokuvan, työmääräimen tai järjestelmää koskevien tietojen mukana palveluun voi päätyä paljon enemmän tietoa kuin käyttäjä tulee ajatelleeksi.

Turvallisuusala perustuu luottamukseen. Olemme vuosikymmeniä kiinnittäneet huomiota siihen, kenellä on hallussaan avaimia, kuka saa nähdä piirustuksia ja järjestelmä-tietoja ja kenellä on pääsy asiakkaan tiloihin. Digitaalisessa maailmassa saman ajattelutavan pitää ulottua myös siihen, **kenelle, tai mille, tietoa annamme.**

Lukkoseppämestarikilta kannustaa hyödyntämään tekoälyä rohkeasti mutta harkiten. Tekoälystä tulee varmasti yhä tärkeämpi työväline myös turvallisuusosalalla, eikä sen käyttöä ole syytä tarpeettomasti rajoittaa. Olennaista on, että yrityksissä laaditaan tekoälyn käytölle selkeät pelisäännöt ja huolehditaan siitä, että ne tunnetaan niin toimistossa kuin kentälläkin.

Hyvä nyrkkisääntö on lopulta yksinkertainen: **jos et lähettäisi tietoa tuntematto-**

malle vastaanottajalle sähköpostilla, älä syötä sitä tekoälyllekään.

Uudet työkalut muuttavat tapaamme tehdä työtä, mutta yksi asia ei muutu. Turvallisuus syntyy edelleen harkinnasta, osaamisesta ja siitä, että luottamuksellista tietoa käsitellään luottamuksen arvoisesti.

Lukkoseppämestarikilta ry on vuonna 2002 perustettu erikoisammattitutkinnon suorittaneiden lukkoseppämestarien kilta.

Killan tarkoituksena on kehittää jäsentensä ammattitaitoa, edistää lukitus- ja turvasuojausalan osaamista sekä parantaa alan yleisiä toimintaedellytyksiä. Kilta haluaa myös osaltaan edistää oikeiden ja turvallisten lukitus- ja muiden turvallisuusratkaisujen käyttöä.

Killan jäsenenä on lukkoseppämestarien lisäksi henkilöitä, jotka ovat työuransa aikana merkittävästi edistäneet lukitusturvallisuutta ja alan koulutuksen kehittämistä.

Uusia mahdollisuuksia rakentamassa



Kesä on jälleen takana ja katse kääntyy kohti syksyä ja talvea. Vaikka viime vuodet eivät ole olleet rakennus- ja turvallisuusosalallaan aivan helpoimpia, ilmassa on nyt enemmän myönteisiä merkkejä. Toki myös edelleen epävarmuuksia. Talouden ennusteet ovat kuitenkin vähitellen parantuneet ja näkymät loppuvuodelle sekä ensi vuodelle antavat jo aihetta varovaiseen optimismiin.

Turvallisuuden tarve ei ole ainakaan vähentynyt. Päinvastoin toimintaympäristön muutokset, digitalisaatio, varautuminen ja kasvavat vaatimukset tuovat alallemme jatkuvasti uusia tarpeita ja samalla uusia liiketoimintamahdollisuuksia.

Turvaurakoitsijat ry:n hallituksessa olemme kuluvan vuoden aikana pohtineet paljon sitä, miten voimme entistä paremmin tukea jäsenyritystemme liiketoimintaa. Yhdistyksen tehtävä alan kehityksen seuraamisen ohella on pyrkiä olemaan siinä aktiivisesti mukana ja luomaan jäsenille uusia mahdollisuuksia. Työ jatkuu ja toivottavasti voimme kertoa uusista avauksista myöhemmin.

Yksi uusi askel on kuitenkin jo otettu. Turvaurakoitsijat ry lähtee mukaan **Turvallisuuden Superpäivän** ja **Finnish Security Awardsin** yhdistyskumppaniksi joulukuussa Helsingissä.

Turvallisuuden Superpäivästä rakennetaan koko turvallisuusalan yhteistä vuosittaista kohtaamispaikkaa, joka kokoaa saman katon alle turvallisuusalan yhdistyksiä, yrityksiä, asiantuntijoita, viranomaisia ja muita keskeisiä toimijoita. Päivässä ovat esillä niin turvallisuusteknologia, kyberturvallisuus, riskienhallinta, tekoäly, standardointi kuin varautuminen ja muuttuva turvallisuusympäristö.

Minusta on tärkeää, että Turvaurakoitsijat ry on mukana siellä, missä turvallisuusalan tulevaisuudesta keskustellaan. Meillä on vahva jäsenkunta, paljon käytännön osaamista ja näkemystä siitä, miten turvallisuus toteutetaan oikeassa elämässä. Fyysisen ja digitaalisen turvallisuuden rajat hämärtyvät koko ajan, ja juuri siinä kehityksessä turvaurakoitsijoiden osaamisen merkitys kasvaa.

Yhdistyskumppanuus joulukuun tapahtumassa tuo myös jäsenillemme konkreettista hyötyä. Käytössämme on muun muassa maksuttomia osallistumipaikkoja päivän seminaariin, joita jaamme ilmoittautumisjärjestyksessä. Yhdistyksellämme on myös mahdollisuus osallistua päivän sisältöön sekä olla näkyvästi mukana tapahtumassa ja Finnish Security Awards -gaalassa.

Samalla kumppanuus kertoo mielestäni jostakin laajemmasta. Turvaurakoitsijat ry on tänä päivänä aktiivinen, kehittyvä ja kokoaan suurempi toimija suomalaisella turvallisuusallalla. Meillä on osaava jäsenistö ja vahva verkosto ja haluamme olla rakentamassa yhteistyötä myös oman toimialamme rajojen yli.

Syksyyn on siis hyvä lähteä luottavaisena. Töitä riittää, uusia asioita on tulossa ja yhdistys tekee määrätietoisesti työtä sen eteen, että jäsenemme menestyvät myös tulevaisuudessa.

Hyvää ja menestyksekkästä syksyä kaikille!
Jyri Aho, puheenjohtaja

Turvallinen työ on laadukasta työtä



Turvallisuusalan puhuttaessa keskustelu keskittyy usein kyberturvallisuuteen, hybridi-uhkiin, tekoälyyn ja uusiin teknologioihin. Ne ovatkin tämän päivän turvallisuusalan keskeisiä teemoja. Samalla on kuitenkin hyvä pysähtyä pohtimaan yhtä perustavanlaatuaista asiaa, turvallisuus nimittäin syntyy edelleen ihmisistä.

Turvaurakointiyritysten asentajat, projekti-päälliköt ja huoltoteknikot työskentelevät päivittäin ympäristöissä, joissa turvallisuus on työn lähtökohta, ei sen lopputulos. Työtä tehdään rakennustyömailla, sairaaloissa, kouluissa, teollisuudessa, datakeskuksissa ja kriittisen infrastruktuurin kohteissa. Jokainen työpäivä edellyttää teknisen osaamisen lisäksi kykyä tunnistaa riskejä, arvioida niitä ja tehdä oikeita ratkaisuja myös muuttuvissa tilanteissa.

Turvaurakointiala on muuttunut valtavasti viimeisten vuosikymmenten aikana. Mekaanisten lukkojen rinnalle ovat tulleet sähköiset lukitusjärjestelmät, kulunvalvonta, kamera-valvonta, rikosilmoitinjärjestelmät, oviautomaatio ja verkottuneet turvallisuusratkaisut. Samalla myös asentajan työ on muuttunut vaativammaksi. Nykyinen turvallisuusjärjestelmä on usein osa asiakkaan tietoverkkoa ja toisinaan myös osa yhteiskunnan kriittistä infrastruktuuria.

Teknologian kehittyessä myös käsitys työturvallisuudesta on muuttunut. Vielä muutama vuosikymmen sitten työturvallisuus näh-

tiin pitkälti suojavarusteina, työmaaohjeina ja lakisääteisten velvoitteiden täyttämisenä. Ne ovat edelleen turvallisen työn perusta, mutta eivät enää yksin riitä.

Nykyään työturvallisuus on osa yrityksen johtamista, riskienhallintaa ja koko organisaation toimintakulttuuria. Se näkyy siinä, miten työ suunnitellaan, kuinka työntekijät perehdytetään, miten poikkeamista opitaan ja ennen kaikkea siinä, millaisia ratkaisuja tehdään kiireenkin keskellä. Mielestäni juuri tässä näkyy suomalaisen turvallisuusalan suurin kehityssaskel. Turvallisuudesta on tullut osa ammattilypeyttä.

Aikaisemmin hyvä asentaja oli usein se, joka sai työn valmiiksi nopeasti ja pysyi aikataulussa. Nykyään hyvä asentaja on ennen kaikkea ammattilainen, joka osaa arvioida riskit, käyttää oikeita työmenetelmiä ja tarvittaessa myös keskeyttää työn, jos turvallisuudesta jouduttaisiin tinkimään. Se ei ole hidastelua eikä varovaisuutta vaan korkeinta ammattitaitoa.

Tämä ajattelutavan muutos näkyy myös käytännön työssä.





Turvallinen työ on laadukasta työtä



Turvaurakointiliikkeen työntekijä on asentamassa kameravalvontajärjestelmää rakennuksen sisäänkäynnille. Viimeinen kamera pitäisi asentaa noin neljän metrin korkeuteen. Työmaan aikataulu on tiukka ja seuraa-va kohde odottaa jo. Lähistöllä on tikkaat, mutta oikean kokoinen henkilönostin on toisella puolella työmaata. Sen hakeminen veisi vartin. Kiireessä voisi syntyä houkutus "hoitaa tämä nopeasti" tikkaiden avulla. Ammattitaitoinen asentaja tekee kuitenkin toisen ratkaisun. Hän keskeyttää työn hetkeksi, hakee oikean työvälineen ja tekee asennuksen turvallisesti. Samalla kamera saadaan asennettua valmistajan ohjeiden mukaisesti oikeaan paikkaan ja oikeaan suuntaan.

Esimerkki kertoo paljon enemmän kuin yhdestä työvaiheesta. Se kertoo turvallisuuskulttuurista. Yrityksessä, jossa turvallisuus on aidosti osa toimintaa, työntekijällä on mahdollisuus sanoa: *"Tehdään tämä oikein."* Turvallisuudesta ei tingitä aikataulun vuoksi, eikä työntekijän tarvitse valita turvallisuuden ja tehokkuuden välillä. Tämä on myös asiakkaan etu. Turvallisesti tehty työ on lähes aina huolellisesti tehtyä työtä. Kun työvaiheita ei oikaista, järjestelmät asennetaan valmistajien ohjeiden mukaisesti, dokumentointi tehdään asianmukaisesti ja lopputuloksesta tulee laadukas. Työturvallisuus ja työn laatu eivät siis ole erillisiä asioita, vaan ne kulkevat käsi kädessä.

Turvallisuusajattelu ulottuu nykyisin paljon työmaan ulkopuolelle. Turvaurakoitsijan on hallittava sähköisten järjestelmien lisäksi tietoverkkojen perusteita, kyberturvallisuutta, asiakkaiden turvallisuusvaatimuksia ja yhä

monimutkaisempia kokonaisuuksia. Samalla työnantajan vastuu henkilöstön osaamisen ylläpitämisestä korostuu. Jatkuva kouluttaminen ei ole enää kilpailuetu, vaan välttämättömyys. Myös asiakkaiden odotukset ovat muuttuneet. Julkisissa hankinnoissa ja vaativissa turvallisuuskohteissa arvioidaan entistä tarkemmin toimittajien turvallisuusjohtamista, riskienhallintaa ja vastuullisuutta. Yhä useammin asiakkaat haluavat varmistua siitä, että yhteistyökumppani toimii järjestelmällisesti myös henkilöstön turvallisuuden näkökulmasta.

Turvaurakoitsijat ry jäsenyrityksiä yhdistää sitoutuminen tähän ajattelutapaan. Kaikilla jäsenyrityksillämme on ISO 45001 -työturvallisuus- ja työturvallisuusjärjestelmän sertifiointi. Sertifikaatti ei ole pelkkä kilpailutuksissa esitettävä todistus, vaan osoitus siitä, että turvallisuutta johdetaan suunnitelmallisesti, riskejä arvioidaan ennakoivasti ja toimintaa kehitetään jatkuvasti. Samalla se viestii asiakkaille, että turvallisuus on osa yrityksen laadun, ei erillinen prosessi.

Turvallisuusala rakentaa turvallisempaa yhteiskuntaa joka päivä. Siksi myös turvallisuuden tekijöiden on voitava tehdä työnsä turvallisesti. Hyvin johdettu työturvallisuus näkyy henkilöstön hyvinvointina, työn laaduna, toimitusvarmuutena, asiakaskokemuksena ja yrityksen maineena. Se on investointi, joka maksaa itsensä takaisin monella tavalla.

Tulevaisuudessa turvallisuusalan kilpailukyky rakentuu yhä enemmän luottamukselle. Asiakas ei osta pelkästään lukitus- tai turvallisuusjärjestelmää. Hän ostaa osaamista, vas-

tuallisuutta ja varmuutta siitä, että työ tehdään oikein myös silloin, kun kukaan ei ole katsomassa.

Siksi uskon, että työturvallisuudesta kannattaa puhua aiempaa enemmän. Ei vain siksi, että jokainen työntekijä ansaitsee palata terveenä kotiin työpäivän jälkeen, vaan myös siksi, että hyvin johdettu työturvallisuus on yksi suomalaisen turvallisuusalan tärkeimmistä laatutekijöistä ja kilpailueduista.

Lopulta turvallinen työ on aina myös laadukasta työtä.

Turvallinen työ on laadukasta työtä, muista nämä

- **Turvallisuus on ammattitaitoa.** Oikeat työmenetelmät ja riskien tunnistaminen kuuluvat hyvään ammattisuoritukseen.
- **Kiire ei ole syy oikaista.** Ammattilainen keskeyttää työn tarvittaessa ja tekee sen turvallisesti myös aikataulupaineessa.
- **Työturvallisuus ja laatu kulkevat käsi kädessä.** Turvallisesti tehty työ on yleensä myös huolellisesti tehty, oikein dokumentoitu ja laadukas.
- **Osaamista on ylläpidettävä jatkuvasti.** Teknologia, tietoverkot ja asiakkaiden turvallisuusvaatimukset muuttavat myös turvaurakoitsijan osaamistarpeita.
- **Hyvä turvallisuuskulttuuri näkyy asiakkaalle asti.** Se vahvistaa työn laatua, toimitusvarmuutta, luottamusta ja yrityksen mainetta.

Fyysinen murto vai kyberhyökkäys?

Asiakkaasi turvatekniikka voi mahdollistaa molemmat.

Kello on kaksi yöllä ja kohdeorganisaation toimisto on tyhjiään. Hyökkääjä ei lähesty rakennusta ovelta, vaan istuu kotisohvallaan kannettavan tietokoneen ääressä. Hän on jo sisällä.

Viikkoja aiemmin hän oli skannannut julkisesta internetistä näkyviä laitteita ja löytänyt useita osoitteita, joissa turvatekniikan hallintajärjestelmä oli suoraan saavutettavissa. Salasana murtui automaattisella työkalulla alle 20 sekunnissa. Kohdeorganisaation järjestelmän ohjelmistoversio oli kolme vuotta vanha ja tunnettu haavoittuvuus julkaistu jo vuosi sitten, mutta päivitystä ei ollut asennettu. Sisäänpääsy ei vaatinut erityistä osaamista, ainostaan kärsivällisyyttä ja oikeat työkalut.

Turvatekniikan tietoverkosta avautui näkyvä kameravalvontaan, kulunvalvontaan ja kiinteistöautomaatioon, mutta hyökkääjä ei jäänyt sinne. Hän huomasi, että turvatekniikan tietoverkko ja organisaation toimistoverkko olivat yhteydessä toisiinsa, sillä tietoverkon segmentointi oli tehty puutteellisesti vuosia sitten eikä sitä ollut koskaan tarkastettu. Siirtyminen toimistoverkkoon ja sieltä kiinnostaville palvelimille kävi nopeasti.

Seuraavien tuntien aikana hän kartoitti ympäristön ja asensi haittaohjelman, joka aktivoituisi myöhemmin. Ennen poistumistaan hän teki vielä yhden asian: kulunvalvontajärjestelmään lisättiin tuntematon käyttäjätunnus, jolle myönnettiin pääsyoikeus ra-



kennuksen kaikkiin tiloihin. Seuraavana yönä joku käveli sisään fyysisesti, kävi palvelinhuoneessa ja poistui jälkiä jättämättä.

Kun kryptolockeri aktivoitui kolme päivää myöhemmin ja palvelimet lakkasivat toimimasta, organisaatio ei aluksi ymmärtänyt mistä oli kyse. Turvatekniikka toimi normaalisti, kamerat tallensivat ja ovet avautuivat, eikä kukaan ollut seurannut turvatekniikan verkkoliikennettä tai vertaillut kulunvalvonnan käyttäjätietoja henkilöstöhallinnon rekisteriin. Poikkeama oli ollut käynnissä yli viikon ennen kuin se havaittiin.

Skenaario kuvaa hyökkäyslogiikkaa, joka hyödyntää nimenomaan turvatekniikan ja tietoverkon rajapintaa, aluetta, jota perinteinen IT-tietoturva ei valvo ja jota turvaurakoitsija

ei sopimuksensa perusteella hyvinään usein ylläpidä. Katvealue ei synny huolimattomuudesta vaan rakenteellisesti, eikä se ole harvinaisen. Kansainvälisesti arvostetun tietoturva-toimijan suomalaisille suurille ja keskisuurille organisaatioille teettämässä tutkimuksessa 90 prosenttia vastaajista nimesi suurimmaksi tietoturvan kehityskohteeksi juuri digitalisoituvien turvajärjestelmien aiheuttamien tietoturvariskien hallinnan. Samassa tutkimuksessa todettiin, että fyysisen ja digitaalisen turvallisuuden hallinta toisistaan erillään ei enää ole optimaalista, vaikka enemmistö organisaatioista toimii edelleen juuri näin.

Ratkaisu ei ole uusien järjestelmien hankkiminen vaan näkyvyyden rakentaminen niihin, joita jo on. Se edellyttää, että turvatek-

niikan verkkoliikennettä seurataan aktiivisesti, tietoverkkojen poikkeamat kytkeytyvät samaan valvontaan ja kulunvalvonnan tapahtumat voidaan verrata muuhun dataan reaaliajassa. Kun nämä toimivat yhdessä ympäri vuorokauden, aukot alkavat sulkeutua ja tilannekuva syntyy koko ympäristöstä eikä vain sen osista.

Mitä tämä tarkoittaa turvaurakoitsijalle käytännössä? Se tarkoittaa, että kyberturvallisuusosaaminen on nousemassa osaksi alan ammatillista perustaa. Osalle toimijoista se merkitsee oman osaamisen vahvistamista ja tietoturva-asiantuntijuuden tuomista osaksi palvelutarjoomaa. Osalle se tarkoittaa luotettavan kumppaniverkoston rakentamista, jotta asiakkaan kysymyksiin pystytään vastaamaan kokonaisuutena. Kumpikin tie on mahdollinen, mutta paikallaan jääminen ei enää ole. Asiakkaat, joiden toimintaan sääntely ja jatkuvuusvaatimukset yhä tiukemmin puuttuvat, alkavat esittää konkreettisia kysymyksiä: onko asennettu järjestelmä tietoturvallinen, kuka vastaa päivityksistä ja kenelle ylläpito kuuluu. Se turvaurakoitsija, joka on miettinyt vastauksensa valmiiksi, ei ainoastaan säilytä asiakkuuttaan vaan vahvistaa asemaansa kokonaisturvallisuuden luotettava kumppanina.

*Jarno Karvonen,
Loihde*

Taitotalo kouluttaa lukitusalan ammattilaisia

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 1.3.2027

**Lukkoseppämestari,
sähkö- ja automaatioalan erikoisammattitutkinto**
aloitus 1.2.2027

Tutustu myös näihin vakuutusyhtiöiden vaatimiin pätevyystentteihin:

**Rakenteellisen turvasuojauksen pätevyys,
uudet lukkosepät**

**Turvallisuusjärjestelmien suunnittelijan pätevyys,
pätevyyden uusijat**



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



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

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

TAITOTALO

Kun lukko ei enää ole vain lukko, CRA tuo kyberturvallisuus- vaatimukset turvallisuustuotteisiin



CRA:n ensimmäiset valmistajia koskevat ilmoitusvelvollisuudet tulivat voimaan 11. syyskuuta. Varsinaiset tuotevaatimukset seuraavat joulukuussa 2027, mutta turvallisuusalan yritysten kannattaa valmistautua muutokseen jo nyt.

Turvallisuusala on muuttunut nopeasti. Lukko ei välttämättä ole enää vain mekaaninen lukko, kamera ei ole vain kamera eikä kulunvalvontajärjestelmä toimi omassa suljetussa ympäristössään. Yhä useampi turvallisuustuote sisältää ohjelmistoja, verkkoyhteyksiä, pilvipalveluita ja etähallintaa.

EU:n *Cyber Resilience Act* eli CRA, suomeksi kyberkestävyyslainsäädös, tuo pakolliset kyberturvallisuusvaatimukset EU:n markkinoille tuotaville digitaalisia elementtejä sisältäville tuotteille. Turvallisuuslainsäädäntöön voivat kuulua esimerkiksi verkkoon liitettävät lukitus- ja kulunvalvontatuotteet, kamerat, hälytysjärjestelmien komponentit sekä erilaiset ohjelmistot ja pilvipalveluihin kytkeytyvät ratkaisut.

Kyberturvallisuudesta tulee siis entistä selvemmin myös tuoteturvallisuutta.

Ensimmäiset velvoitteet ovat jo voimassa

CRA:n varsinaisia tuotevaatimuksia sovelletaan pääosin 11.12.2027 alkaen, mutta ensimmäinen käytännössä merkittävä vaihe tuli voimaan jo 11.9.2026.

Siitä lähtien valmistajien on ilmoitettava tietoonsa tulleista aktiivisesti hyväksikäytetyistä haavoittuvuuksista ja tuotteen turvallisuuden vaikuttavista vakavista poikkeamista. Ensitieto on annettava 24 tunnin kuluessa ja varsinainen ilmoitus pääsääntöisesti 72 tunnin kuluessa.

Oleellista on, että raportointivelvollisuus koskee myös CRA:n soveltamisalaan kuuluvia tuotteita, jotka on saatettu markkinoille jo ennen joulukuuta 2027. Valmistajalla pitää siis olla toimintamalli haavoittuvuuksien vastaanottamiseen, käsittelyyn, raportointiin ja korjaamiseen.





Turvallisuus ulottuu koko tuotteen elinkaareen

CRA:n keskeinen periaate on, että kyberturvallisuus otetaan huomioon jo tuotteen suunnittelussa ja koko sen elinkaaren ajan.

Turvallisuusosalalla tällä on hyvin konkreettinen merkitys. Oven lukko voi olla mekaanisesti erittäin turvallinen, mutta jos sen sähköiseen hallintaan päästään verkon kautta luvatta käsiksi, kokonaisuus ei ole turvallinen.

Vastuu ei myöskään pääty tuotteen myyntiin. Valmistajan pitää määrittää tuotteelle tukijakso ja huolehtia sen aikana haavoittuvuuksien käsittelystä ja tietoturvapäivityksistä. Tukijakson on lähtökohtaisesti oltava vähintään viisi vuotta, mutta pitkäikäisissä tuotteissa sen tulee ottaa huomioon tuotteen odotettu käyttöikä.

Tämä on turvallisuusosalalla tärkeää, koska lukitus-, kulunvalvonta- ja kamerajärjestelmiä ei hankita muutamaksi vuodeksi. Tuotetta valittaessa onkin syytä kysyä: Kuinka pitkään tuotetta tuetaan? Miten päivitykset hoidetaan? Entä mitä tapahtuu, kun tuki päättyy?

Mitä CRA tarkoittaa turvaurakoitsijalle?

CRA:n raskaimmat velvoitteet kohdistuvat ennen kaikkea valmistajiin sekä tuotteen asemasta riippuen esimerkiksi maahantuojiin ja

jakelijoihin. Tavallinen turvallisuusjärjestelmän asentaja ei siis automaattisesti muutu CRA:n tarkoittamaksi valmistajaksi sillä perusteella, että hän asentaa tuotteen asiakkaalle.

Turvaurakoitsijan näkökulmasta sääntelyä ei silti voi sivuuttaa.

Turvaurakoitsija liittää tuotteita asiakkaan verkkoon, määrittää käyttäjiä ja käyttöoikeuksia, ottaa etäyhteyksiä käyttöön ja integroi eri järjestelmiä toisiinsa. Turvallinenkin tuote voidaan kuitenkin asentaa turvattomasti. Siksi turvaurakoitsijan ammattitaitoon kuuluu jatkossa yhä vahvemmin myös kyberturvallisuuden perusteiden ymmärtäminen. Oletus- salasanojen vaihtaminen, käyttöoikeuksien rajaaminen, etäyhteyksien suojaaminen, ohjelmistojen päivittäminen ja muutosten dokumentointi ovat osa turvallisesti toteutettua kokonaisuutta.

Huomiota kannattaa kiinnittää myös tuotteisiin tehtäviin muutoksiin. Jos tuotteeseen tehdään sen markkinoille saattamisen jälkeen olennainen muutos ja muutettu tuote saatetaan uudelleen markkinoille, muutoksen tekijälle voi syntyä CRA:n mukaisia valmistajan velvollisuuksia.

Kun varsinaisia tuotevaatimuksia aletaan soveltaa, kyberturvallisuus tulee myös osaksi tuotteen vaatimustenmukaisuuden arviointia ja CRA-vaatimusten täyttyminen osaksi CE-merkinnän kokonaisuutta.

Mitä kannattaa tehdä nyt?

Turvallisuusalan yritysten ei tarvitse ryhtyä CRA-juristeiksi. Nyt kannattaa kuitenkin selvittää, miten omat päämiehet ja tavaran-toimittajat ovat muutokseen valmistautuneet.

Tuotteita valittaessa kannattaa kiinnittää huomiota valmistajan päivityskäytäntöihin, tietoturvatuen kestoon sekä siihen, miten valmistaja käsittelee haavoittuvuuksia ja tiedottaa niistä myös jo käytössä olevien tuotteiden osalta.

Hieman halvempi tuote ei välttämättä ole edullisempi ratkaisu, jos sen tietoturvatuesta tai päivityksistä ei ole kunnollista tietoa.

Tässä on turvaurakoitsijalle myös mahdollisuus erottautua. Asiakkaalle ei myydä enää pelkästään lukitusta, kameraa tai kulunvalvontajärjestelmää, vaan **turvallisesti suunniteltu, asennettu ja ylläpidettävä kokonaisuus.**

Lopulta CRA:ssa on kyse varsin tutusta asiasta: **turvallisuustuotteen pitää olla turvallinen myös silloin, kun siihen päästään käsiksi verkon kautta.**

Turvallisuuden Superpäivä kokoaa alan yhteen joulukuussa

Turvaurakoitsijat ry on mukana yhdistyskumppanina uudessa Turvallisuuden Super päivässä, joka järjestetään perjantaina 4.12.2026 Scandic Park Helsingissä.

Tapahtumasta rakennetaan koko turvallisuusalan yhteistä vuosittaista kohtaamispaikkaa, joka tuo saman katon alle alan yhdistykset, yritykset, asiantuntijat ja viranomaiset. Päivän ohjelmassa käsitellään ajankohtaisia turvallisuuden teemoja kyberturvallisuudesta ja tekoälystä turvallisuusteknologiaan, varautumiseen ja muuttuvaan turvallisuusympäristöön.

Turvaurakoitsijat ry on mukana myös päivän seminaariohjelmassa omalla puheenvuorollaan. Seminaarin yhteydessä järjestetään TurvallisuusExpo, ja päivä huipentuu illalla Finnish Security Awards -gaalaan.

Yhdistyskumppanuuden myötä jäsenillemme on varattu 25 maksutonta osallistumispaikkaa päivän seminaariin, lounaalle, kahveille ja TurvallisuusExpoon. Kerromme ilmoittautumisesta ja tarkemmasta ohjelmasta myöhemmin.

Laita päivämäärä jo kalenteriin: 4.12.2026!

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 oviyksikkövalikoima 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 

Teletilojen päivitetty lukitussuositus

Kiinteistöjen talojakamoissa ja muissa laitetoiloissa kulkee yhteiskunnan arjen kannalta olennaista tietoliikennettä. Traficomin uusi suositus täsmentää laitetoilojen lukitusta, avainturvallisuutta ja kulunhallintaa – ja tuo uusia vaatimuksia erityisesti yli 10 huoneiston kiinteistöihin.

Talojakamo saattaa olla kiinteistön käyttäjälle lähes näkymätön tila, mutta turvallisuuden kannalta sen merkitys on suuri. Kiinteistön sisäverkkojen laitteet ja kytkennät sijaitsevat talojakamoissa, alijakamoissa, kerrosjakamoissa ja muissa laitetoiloissa. Lukituksella suojataan paitsi laitteita myös viestintäsalaisuutta ja muuta tietoturvallisuutta.

Traficom julkaisi vuonna 2026 päivitetyn suosituksen **Kiinteistöjen laitetoilojen lukitus 306/2026 S**. Se korvaa vuoden 2019 suosituksen ja huomioi uuden sisäverkkon ja teleurakointia koskevan määräyksen 65 F/2026 M.

Vastuu on kiinteistön omistajalla

Kiinteistön omistaja tai haltija vastaa yhteisten laitetoilojen lukituksesta ja niiden tieturvallisuudesta. Asiattomien pääsy tiloihin pitää estää, mutta samalla teleyritysten ja valtuutettujen teleurakoitsijoiden on päästävä tarvittaessa tekemään työtään.

Lukituksen suunnittelu onkin enemmän kuin lukon valinta. Huomioon on otettava muun muassa käyttöoikeudet, avainten säilytys ja luovutus, tilojen sijainti sekä tarvittavan avauspalvelun järjestäminen.

Yli 10 huoneiston kiinteistöihin uusi käytäntö

Yksi merkittävimmistä muutoksista koskee uusia ja sisäverkoltaan uudistettavia yli 10 huoneiston kiinteistöjä.

Teletilojen lukitus on pitänyt 1.5.2026 alkaen järjestää siten, että pääsy teletiloihin tapahtuu ulkoseinällä olevasta avainsäilöstä

saatavalla **reittiavaimella** sekä urakoitsijalle myönnetyllä varsinaiseen teletilan lukitukseen käyvällä avaimella.

Reittiavaimella päästään siis kulkemaan rakennuksessa talojakamolle, mutta sillä ei avata itse teletilaa. Avainsäilöä ja reittiavainta ei tarvita, jos teletilaan pääsee suoraan ulkoa. Erottelu on turvallisuuden kannalta tärkeä: rakennuksen kulkureittejä avaava avain ja varsinaiseen suojattuun laitetoilaan oikeuttava avain ovat eri asioita.

Talojakamo ei kuulu yleisavainjärjestelmään

Traficom suosittelee talojakamoon vähintään rakenteeltaan takalukkiutuvaa, Finanssiala ry:n luetteloimaa testattua käyttölukkoa. Lukituksessa käytettävien avainten kopioinnin pitää olla hallittua.

E erityisen tärkeää on, että **talokakamon ja muiden laitetoilojen lukkoja ei saa sarjoittaa samaan sarjaan kiinteistön muiden lukkojen kanssa**. Myös oven, kaapin ja muiden suojarakenteiden on oltava riittävän murtolujia.

KTL1E ja elektroninen lukitus tuovat hallittavuutta

Traficom nostaa suosituksessaan **KTL1E-lukitusjärjestelmän** esimerkiksi teleyritys-

ten yhteisestä lukitus- ja kulunhallintajärjestelmästä. Se myös suosittelee teleyrityskoh- taisten lukkojen korvaamista yhteisellä luki- tus- ja kulunhallintajärjestelmällä, esimerkik- si KTL1E:llä.

Elektronisesti hallittavassa lukituksessa käyttöoikeudet voidaan määritellä käyttäjä- kohtaisesti ja määrääjaksi, niitä voidaan hal- lita keskitetysti ja kulkutapahtumia jäljittää. Tämä parantaa avainturvallisuutta erityisesti laitetoiloissa, joissa käy useiden eri organisaa- tioiden henkilöstöä.

Käyttöoikeuksien koko elinkaari on kuiten- kin hallittava. Tarpeettomat oikeudet pitää

poistaa esimerkiksi tehtävän tai käyttötä- peen päättyessä tai avaimen kadotessa.

Lukitus on osa tietoturvallisuutta

Traficomin suosituksen keskeinen viesti on lopulta yksinkertainen: tietoturvallisuus ei ala vasta palomuurista tai verkkolaitteesta. Jos ulkopuolinen pääsee fyysisesti käsiksi kiin- teistön tietoliikenneverkon kytkentöihin ja laitteisiin, myös tietoturva voi vaarantua.

Turvaurakoitsijan näkökulmasta tämä ko- rostaa ammattimaisen lukitussuunnittelun merkitystä. Oikean lukon lisäksi tarvitaan toi- miva avain- ja kulkuoikeushallinta, hallitut avainten luovutusmenettelyt sekä tarkoituk- senmukainen rakenteellinen suojaus.

Lähde: Liikenne- ja viestintävirasto Traficom, Kiinteistöjen laitetoilojen lukitus, suositus 306/2026 S.



URAKAN takuuajan vakuus ja takuu

Asiakkaan ja lukkoliikkeen välisessä urakasopimuksessa voidaan lähtökohtaisesti sopia vapaasti urakan takuusta ja takuuajan vakuudesta. Vakiintuneesti sovelletut YSE 1998 ehdot eivät ole pakottavaa lainsäädäntöä, vaan sopimusehtoja, joita sovelletaan siltä osin kuin ne on otettu osaksi osapuolten välistä sopimusta eikä niistä ole erikseen poikettu.

Vakuuden ja takuun määrästä voidaan sopia

YSE:n mukaan urakoitsijan tulee antaa tilaajalle vakuus urakasopimuksen asianmukaisen täyttämisen turvaamiseksi. Mikäli urakasopimuksessa ei ole toisin määrätty, rakennusajan vakuus on 10 prosenttia ja takuuajan vakuus 2 prosenttia arvonlisäverottomasta urakkahinnasta. Säännös on kuitenkin nimenomaisesti tahdonvaltainen. Asiakas ja lukkoliike voivat siten sopia esimerkiksi pienemmästä vakuudesta tai siitä, ettei vakuutta aseteta lainkaan.

Sama periaate koskee YSE mukaista takuuta. Normaali takuu aika on kaksi vuotta, ellei urakasopimuksessa ole muuta määrätty.

Osapuolet voivat siten sopia pidemmästä tai lyhyemmästä takuusta taikka siitä, ettei takuuta sovelleta lainkaan. Esimerkiksi asunto osakeyhtiö asiakkaana on sopimusosapuolena toimiva oikeushenkilö, jolloin yritysten väliseen sopimussuhteeseen kuuluva sopimusvapaus on lähtökohtaisesti laaja.

Takuu ja takuuajan vakuus on kuitenkin erotettava toisistaan. Takuuajan vakuus on tilaajan saamisten turvaamiseksi asetettava vakuus. Takuu puolestaan määrittää urakoitsijan erityisen takuuajaisen virhevastuun. Takuuajan vakuudesta voidaan luopua ilman, että itse takuusta luovutaan. Vastaavasti takuusta voidaan sopia poikkeavasti riippumatta siitä, onko vakuutta asetettu. Vaikka takuusta luovuttaisiin sopimuksessa, vastaa lukkoliike joka tapauksessa suorituksensa laadusta normaalin virhevastuun perusteella.

Ehdoista voidaan sopia myös urakan aikana

Jos lukkoliike ja asiakas sopivat esimerkiksi urakan aikana, ettei lukkoliikkeeltä edellytetä vakuutta, tällainen sopimusmuutos on lähtö-

kohtaisesti pätevä. Samoin voidaan myöhemmin sopia alkuperäistä urakasopimusta muuttaen takuuajan lyhentämisestä tai takuun poistamisesta. Muutoksen tulee perustua molempien osapuolten suostumukseen. Erityisesti näyttökysymysten vuoksi tällaiset muutokset on syytä tehdä kirjallisesti.

Takuusta luopuminen ei kuitenkaan merkitse sitä, että lukkoliike vapautuisi kaikesta vastuusta. Urakkasuorituksen tulee vastaanottohetkellä vastata sovittua. Lisäksi YSE:ä sovelletaan takuuajan jälkeisestä vastuusta sellaisissa tilanteissa, joissa virhe johtuu esimerkiksi urakoitsijan laiminlyönnistä, täyttämättä jääneestä suorituksesta tai olennaisesta laadunvarmistuksen laiminlyönnistä. Tällaisen vastuun täydellinen poissulkeminen on oikeudellisesti huomattavasti ongelmallisempaa kuin tavallisesta takuusta luopuminen, eikä se ole muutenkaan tarpeellista.

Lukkoliikkeen kannalta keskeinen lähtökohta on siten, etteivät YSE:n kahden vuoden takuu aika tai kahden prosentin takuuajan vakuus ole asiakkaan hyväksi pakottavia vähimmäisehtoja. Niistä voidaan sopia toisin sekä

alkuperäisessä urakasopimuksessa että myöhemmin urakan aikana. Ratkaisevaa on, mitä osapuolet ovat tosiasiallisesti sopineet ja kuinka selvästi sopimusmuutos voidaan myöhemmin näyttää toteen.

Yhteenveto

Vaikka YSE:n soveltaminen onkin tavanomainen ja asialliseksi koettu tapa, voi pitkien ja luottamuksellisten asiakassuhteiden osalta voi olla perusteltua myös arvioida, onko vakuuden asettaminen, ja mihin määrään, kaikissa tilanteissa tarkoituksenmukaista. Vakuuden järjestäminen edellyttää työtä ja jonkin verran siitä kertyy myös kustannuksia. Harkitut muutokset YSE:n järjestelmään voivat koitua asiakkaan eduksi halvempaan hintaan.

Mahdolliset muutokset vakuuden tai takuunkaan osalta eivät merkitse sitä, etteikö lukkoliike vastaisi työnsä sopimuksen mukaisuudesta ja laadusta. Vakuuden tarpeellisuutta voidaan siten arvioida osana osapuolten välistä riskinjakoa, urakan laajuutta sekä aikaisempaan yhteistyöhön perustuvaa luottamusta.

ABLOY



ASSA ABLOY Access®

ASSA ABLOY Access on pilvipohjainen järjestelmä, joka on suunniteltu vastaamaan organisaatioiden muuttuviin tarpeisiin. Sen avulla voit hallinnoida helposti digitaalisia avaimia sekä kulku- ja mobiilitunnisteita.

abloy.fi/access