SÄÄNTELYSTÄ JATKUVAAN KOKONAIS-TURVALLISUUTEEN

LOIHDE

Sisällysluettelo:

LOIHDE

Johdanto

Eurooppalainen sääntely on viime vuosina muuttanut turvallisuustyön vaatimustasoa merkittävästi. Kyse ei ole yksittäisestä säädöksestä, vaan laajemmasta kehikosta, joka koskee sekä fyysistä että digitaalista toimintaympäristöä.

Organisaatioilta edellytetään järjestelmällistä riskienhallintaa, kykyä havaita ja käsitellä poikkeamia sekä dokumentoitua näyttöä siitä, että turvallisuus on osa normaalia päivittäistä toimintaa.

NIS2, CER, DORA ja CRA kohdistuvat eri toimialoihin ja eri näkökulmiin, mutta niiden vaikutus organisaatioiden arkeen on samansuuntainen. Turvallisuus on liitettävä johtamiseen, riskienhallintaan ja jatkuvuuden varmistamiseen. Vastuu ei rajoitu yksittäisiin järjestelmiin tai teknisiin ratkaisuihin, vaan ulottuu toimitusketjuihin, palveluntarjoajiin ja hallintamalleihin.

Monessa organisaatiossa turvallisuutta on jo kehitetty pitkäjänteisesti. Uusi sääntely ei edellytä kaiken aloittamista alusta, mutta se edellyttää kokonaisuuden tarkastelua uudesta näkökulmasta. On ymmärrettävä, missä vaatimukset jo täyttyvät, missä on kehittämistarpeita ja miten kokonaisturvallisuutta johdetaan jatkossa.

Tämän oppaan tarkoituksena on jäsentää sääntelyn kokonaiskuva ja tuoda esiin, mitä vaatimukset käytännössä tarkoittavat. Ensimmäisessä osassa kuvataan keskeiset säädökset ja niiden velvoitteet. Toisessa osassa tarkastellaan, miten organisaatio voi rakentaa jatkuvan kyvykkyyden vastata näihin vaatimuksiin. Kolmannessa osassa käsitellään toteutusmallia ja kumppanivalintaa sekä sitä, miten kokonaisturvallisuus varmistetaan pitkällä aikavälillä.

Opas on suunnattu organisaatioille, jotka haluavat ymmärtää sääntelyn vaikutukset omaan toimintaansa ja rakentaa hallitun, osoitettavan toimintamallin. Tavoitteena on tarjota selkeä rakenne ja käytännön näkökulma, jonka avulla turvallisuutta voidaan kehittää suunnitelmallisesti ja johdetusti.

OSA 1 | SÄÄNTELYN KOKONAISKUVA

1.1 NIS2

Kyberturvallisuuden vahvistaminen

Mikä se on?

NIS2 on Euroopan unionin kyberturvallisuus-direktiivi, jonka tavoitteena on varmistaa korkea ja yhtenäinen verkko- ja tieto-järjestelmien turvallisuustaso jäsenvaltioissa. Suomessa direktiivi on toimeenpantu kyber-turvallisuuslailla (124/2025).

Direktiivi perustuu riskiperusteiseen lähestymistapaan. Toimijoiden on tunnistet-tava, arvioitava ja hallittava toiminnassaan käytettäviin verkko- ja tietojärjestelmiin kohdistuvia riskejä.

Mitä se vaatii?

NIS2 edellyttää, että organisaatio toteuttaa asianmukaiset ja oikeasuhtaiset kyber-turvallisuuden riskienhallintatoimenpiteet.

Kyberturvallisuus ei rajoitu erilliseen IT-ympä-ristöön, vaan kattaa kaikki verkkoon kytketyt järjestelmät, mukaan lukien modernin turvatek-niikkan ja kriittisten tilojen valvontaratkaisut.

Ketä se koskee?

NIS2 koskee keskeisiä ja tärkeitä toimijoita yhteiskunnan kannalta merkittävillä toimialoilla.

Näitä ovat muun muassa:

- **Energia**
- **Liikenne**
- **Terveys**
- **Juomavesi ja jätevesi**
- **Digitaalinen infrastruktuuri**
- **Julkishallinto**
- **Finanssiala**
- **Avaruustoiminta**
- **Tietyt teollisuuden ja valmistuksen alat**
- **Digitaaliset palveluntarjoajat**

- Velvoitteet kohdistuvat pääsääntöisesti keskisuuriin ja suuriin organisaatioihin.
- Soveltamisala määräytyy toimialan ja organi-saation koon perusteella.
- Myös toimitusketjun kautta vaikutukset voivat ulottua pienempiin toimijoihin.

Vaatimukset kohdistuvat erityisesti seuraaviin osa-alueisiin:

Riskienhallinta:

- riskien tunnistaminen ja arviointi
- suojatoimenpiteiden määrittely ja toteutus
- riskienhallinnan säännöllinen päivittäminen

Poikkeamien hallinta ja ilmoittaminen:

- kyky havaita merkittävät tietoturva-poikkeamat
- selkeä menettely poikkeamien käsittelyyn

Velvollisuus ilmoittaa merkittävistä poikkeamista viranomaiselle:

- ennakkovaroitus 24 tunnin kuluessa
- poikkeamaraportti 72 tunnin kuluessa
- loppuraportti viimeistään kuukauden kuluessa

Toiminnan jatkuvuus:

- häiriötilanteisiin varautuminen
- palautumissuunnitelmat
- kriittisten toimintojen suojaaminen

Toimitusketjun turvallisuus:

- keskeisten palveluntarjoajien riskien arviointi
- ulkoistusten hallinta

Johtamisvastuu:

- johto vastaa kyberturvallisuuden järjestämisestä
- vaatimusten noudattamista valvo-taan viranomaisvalvonnalla

— Keskeinen velvoite —

Organisaation on varmistettava, että kyberturvallisuuden riskienhallinta, poikkeamien havaitseminen ja raportointi ovat järjestelmällisesti toteutettuja ja todennettavissa.

1.2 CER

Kriittisten toimijoiden häiriönsietokyky

Mikä se on?

CER-direktiivi (EU 2022/2557) vahvistaa kriittisten toimijoiden häiriönsietokykyä Euroopan unionissa. Suomessa direktiivi on toimeenpantu lailla yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta (310/2025).

Sääntelyn tavoitteena on varmistaa, että yhteiskunnan kannalta välttämättömät palvelut ja infrastruktuurit kestävät erilaisia häiriöitä ja pystyvät jatkamaan toimintaansa myös poikkeustilanteissa.

CER painottaa erityisesti kriittisen infrastruktuurin suojaamista ja toiminnan jatkuvuutta. Se kattaa fyysiset uhat, mutta huomioi myös digitaaliset riippuvuudet ja toimitusketjut osana kokonaisuutta.

Mitä se vaatii?

CER edellyttää, että nimetty kriittinen toimija toteuttaa asianmukaiset ja oikeasuhtaiset toimenpiteet häiriönsietokyvyn varmistamiseksi.

Ketä se koskee?

Laki koskee niin sanottuja kriittisiä toimijoita, eli organisaatioita, joiden toiminnan keskeytymisellä olisi merkittävä vaikutus yhteiskunnan toimivuuteen.

Näitä ovat muun muassa:

- **energia- ja sähköverkkojen toimijat**
- **vesihuollon ja jätehuollon toimijat**
- **terveydenhuollon palveluntuottajat**
- **liikenteen ja logistiikan toimijat**
- **digitaalisen infrastruktuurin ylläpitäjät**
- **elintarvikehuollon keskeiset toimijat**

- Kriittiset toimijat tunnistetaan ja nimetään kansallisesti toimivaltaisen viranomaisen toimesta.
- Nimetyn toimijan on tehtävä yhteistyötä valvovan viranomaisen kanssa ja täytettävä sille asetetut velvoitteet.

Velvoitteet kohdistuvat erityisesti seuraaviin osa-alueisiin:

Riskien arviointi:

- Toimintaan kohdistuvien riskien tunnistaminen ja arviointi
- Fyysisten, teknisten ja muiden uhkien huomiointi
- Riippuvuuksien ja keskinäisvaikutusten arviointi

Häiriönsietokykyä koskevat toimenpiteet:

- Turva- ja suojaustoimenpiteiden toteuttaminen
- Häiriöiden ehkäisy- ja lieventämistoimet
- Organisaation sisäisten valmiuksien varmistaminen

Toiminnan jatkuvuus ja palautuminen:

- Jatkuvuussuunnitelmien laatiminen
- Palautumiskyvyn varmistaminen häiriötilanteissa
- Häiriötilanteiden hallintamenettelyt

Viranomaisyhteistyö ja raportointi:

- Merkittävien häiriöiden ilmoittaminen valvovalle viranomaiselle
- Yhteistyö ja tiedonvaihto viranomaisten kanssa
- Velvoitteiden noudattamisen osoittaminen

— Keskeinen velvoite —

Nimetyn kriittisen toimijan on arvioitava toimintaansa kohdistuvat riskit ja toteutettava asianmukaiset ja oikeasuhtaiset toimenpiteet häiriönsietokyvyn varmistamiseksi.

1.3 DORA

Digitaalinen toimintakyky finanssialalla

Mikä se on?

DORA (Digital Operational Resilience Act, EU 2022/2554) on EU-asetus, jonka tavoitteena on vahvistaa finanssialan digitaalista toimintakykyä ja varmistaa, että rahoitussektorin toimijat kestävät ja hallitsevat tieto- ja viestintäteknologiaan liittyviä häiriöitä.

Toisin kuin direktiivit, DORA on suoraan sovellettava asetus. Se ei edellytä kansallista täytäntöönpanoa samalla tavalla kuin NIS2 tai CER, vaan sitä sovelletaan yhtenäisesti koko EU:n finanssisektoriin. Kansalliset viranomaiset vastaavat kuitenkin valvonnasta ja seuraamuksista.

Mitä se vaatii?

DORA edellyttää, että finanssialan toimijalla on kattava ja dokumentoitu digitaalisen toimintakyvyn hallintakehikko. Hallintamallin on katettava koko ICT-ympäristö ja oltava osa organisaation johtamisrakennetta.

Ketä se koskee?

DORA koskee laajasti finanssialan toimijoita, kuten:

- **Luottolaitoksia ja pankkeja**
- **Maksulaitoksia ja sähköisen rahan liikkeeseenlaskijoita**
- **Sijoituspalveluyrityksiä**
- **Vakuutus- ja jälleenvakuutusyhtiöitä**
- **Rahastoyhtiöitä ja varainhoitajia**
- **Kryptovaratoimijoita**

- Lisäksi DORA:ssa säädetään kriittisten ICT-palveluntarjoajien valvonnasta.
- Tietyt merkittävät ICT-palveluntarjoajat voidaan nimetä kriittisiksi, jolloin niihin kohdistuu erityinen EU-tason valvontakehikko.

Vaatimukset kohdistuvat erityisesti seuraaviin osa-alueisiin:

ICT-riskien hallinta:

- ICT-riskien tunnistaminen ja arviointi
- Riskienhallintapolitiikat ja menettelyt
- Jatkuva seuranta ja hallintakehikon ylläpito

ICT-häiriöiden hallinta ja raportointi:

- Merkittävien ICT-tapahtumien tunnistaminen ja luokittelu
- Dokumentoidut käsittely- ja eskalointimenettelyt
- Raportointivelvoitteet toimivaltaiselle valvontaviranomaiselle

Digitaalisen toimintakyvyn testaus:

- Säännöllinen testaus toimintakyvyn varmistamiseksi
- Kriittisten järjestelmien testaus
- Merkittävimmille toimijoille myös kehittyneet uhkasimulaatiot ja tunkeutumistestaukset

ICT-kolmansien osapuolten riskien hallinta

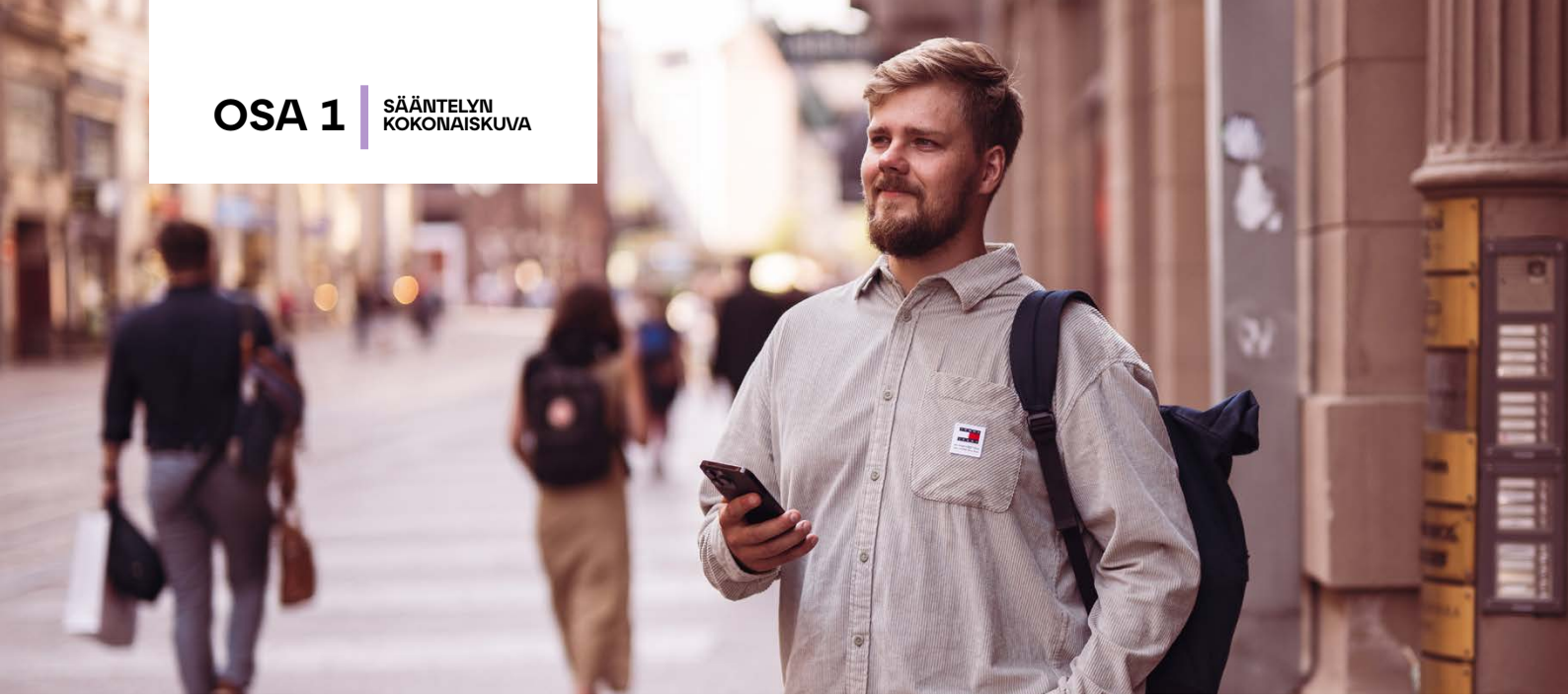
- Kriittisten ICT-toimittajien tunnistaminen
- Sopimusvaatimusten ja valvonnan järjestäminen
- Ulkoisiin riippuvuuksiin liittyvien riskien jatkuva arviointi

Johdon vastuu

- Johto vastaa digitaalisen toiminta-kyvyn järjestämisestä
- Hallintamallin tulee olla osa organisaation johtamista ja valvontaa

— Keskeinen velvoite —

Finanssialan toimijan on ylläpidettävä kattavaa ja dokumentoitua ICT-riskien hallintakehikkoa sekä varmistettava, että merkittävät ICT-häiriöt havaitaan, hallitaan ja raportoidaan säädetyllä tavalla.



1.4 CRA

Kyberturvallisuus digitaalisissa tuotteissa

Mikä se on?

CRA (Cyber Resilience Act) on EU-asetus, jonka tavoitteena on varmistaa, että markkinoille saatettavat tuotteet, joissa on digitaalisia elementtejä, täyttävät kyber-turvallisuusvaatimukset.

Asetus koskee tuotteita, joissa on ohjelmisto- tai laitekomponentteja ja jotka ovat yhteydessä verkkoon tai muulla tavoin digitaalisesti ohjattuja. Sen tarkoituksena on parantaa tuotteiden turvallisuustasoa jo suunnittelu- ja kehitysvaiheessa sekä varmistaa haavoittuvuuksien hallinta ja tieto-turvapäivitykset tuotteen tukijakson aikana.

CRA on suoraan sovellettavaa lainsäädäntöä EU:ssa.

Mitä se vaatii?

CRA edellyttää, että tuotteiden kyber-turvallisuus huomioidaan suunnittelu- ja kehitysvaiheesta lähtien sekä tuotteen tukijakson ajan.

Ketä se koskee?

CRA koskee ensisijaisesti:

- **Valmistajia, jotka saattavat EU-markkinoille tuotteita, joissa on digitaalisia elementtejä**
- **Maahantuojia**
- **Jakelijoita**

- Valmistajalla tarkoitetaan toimijaa, joka suunnittelee tai valmistaa tuotteen ja saattaa sen markkinoille omalla nimellään tai tavara-merkillään.
- Sääntely kattaa tuotteet, joissa on ohjelmisto- tai laitekomponentteja ja jotka sisältävät digitaalisia toimintoja. Se voi koskea esimerkiksi teollisia laitteita, älylaitteita ja muita verkottuneita tuotteita, jotka saatetaan EU-markkinoille.

Vaatimukset kohdistuvat erityisesti seuraaviin osa-alueisiin:

Turvallinen suunnittelu ja kehitys:

- Tuotteiden suunnittelu siten, että kyberturvariskit minimoidaan
- Oletusarvoisesti turvalliset asetukset
- Asianmukainen tekninen dokumentaatio

Haavoittuvuuksien hallinta:

- Haavoittuvuuksien tunnistaminen ja käsittely
- Turvallisuuspäivitysten ja korjausten toimittaminen tuotteen tukijakson aikana
- Prosessi ilmoitettujen haavoittuvuuksien vastaanottamiseen ja käsittelyyn

Markkinoille saattamisen vaatimukset:

- Vaatimustenmukaisuuden arviointi
- Teknisen dokumentaation laatiminen
- CE-merkinnän kiinnittäminen ja vaadittujen tietojen toimittaminen

Ilmoitusvelvollisuudet:

- Aktiivisesti hyväksikäytettyjen haavoittuvuuksien ja merkittävien tietoturvapoikkeamien ilmoittaminen säädetyllä tavalla
- Yhteistyö toimivaltaisten viranomaisten kanssa

— Keskeinen velvoite —

Valmistajan on varmistettava, että markkinoille saatettava tuote on suunniteltu ja toteutettu kyberturvallisesti sekä että haavoittuvuuksia hallitaan ja korjataan tuotteen tukijakson ajan.

1.5 Mitä yhteistä?

Sääntelyn yhteinen rakenne

NIS2, CER, DORA ja CRA kohdistuvat eri toimialoihin ja eri näkökulmiin. Osa painottaa operatiivista kyberturvallisuutta, osa kriittisen infrastruktuurin häiriönsietokykyä ja osa digitaalisten tuotteiden turvallisuutta. Tarkemmin katsottuna niiden perusrakenne on kuitenkin samankaltainen.

Kaikki säädökset perustuvat riskiperusteiseen ajatteluun. Organisaation on tunnistettava omaan toimintaansa kohdistuvat uhat, arvioitava niiden vaikutus ja toteutettava oikeasuhtaiset toimenpiteet. Velvoitteet eivät ole kaikille samanlaisia, vaan ne suhteutetaan toiminnan laajuuteen, merkitykseen ja riskitasoon.

Toinen yhteinen nimittäjä on jatkuvuus. Sääntely ei keskity ainoastaan ennaltaehkäisyyn, vaan korostaa kykyä hallita häiriötilanteita ja palauttaa toiminta hallitusti. Riskienhallinta, valvonta ja palautumissuunnittelu muodostavat kokonaisuuden, joka on osa normaalia toimintaa – ei erillinen kehityshanke.

Säädöksissä toistuu myös vaatimus osoitettavuudesta. Organisaation on pystyttävä näyttämään, että riskienhallinta, poikkeamien käsittely ja jatkuvuustoimenpiteet ovat käytännössä toiminnassa. Dokumentointi, raportointi ja johdon vastuu eivät ole muodollisuuksia, vaan keskeinen osa velvoitetta.

Lisäksi kaikissa sääntelykokonaisuuksissa korostuu toimitusketjun merkitys. Turvallisuus ei rajoitu organisaation omiin järjestelmiin ja tiloihin, vaan ulkoiset palveluntarjoajat, turvallisuustekniikan toimittajat, ICT-toimittajat ja muut riippuvuudet on huomioitava osana kokonaisuutta.

— Keskeinen havainto —

Vaikka säädökset eroavat soveltamisalaltaan, niiden ydinkysymys on sama: onko organisaatiolla järjestelmällinen ja jatkuva toimintamalli, joka kattaa riskienhallinnan, valvonnan, raportoinnin ja toiminnan jatkuvuuden muuttuvassa toimintaympäristössä?

OSA 2 | JATKUVAN KYVYKKYYDEN RAKENTAMINEN

2.1 Nykytilan arviointi

Riskienhallinta on lähtökohta

Sääntelyn vaatimuksia ei täytetä aloittamalla uusista investoinneista. Työ alkaa nykytilan ymmärtämisestä. Useimmilla organisaatioilla on jo käytössä turvajärjestelmiä, valvontaa ja toimintamalleja, mutta kokonaiskuva usein puuttuu. Ilman Ilman kokonaiskuvaa on vaikea arvioida, on vaikea arvioida, vastaavatko nykyiset ratkaisut uusiin vaatimuksiin ja missä todelliset riskit sijaitsevat.

Riskienhallinta ei ole yksittäinen dokumentti tai auditointia varten laadittu raportti. Se on tapa jäsentää organisaation toimintaa, tunnistaa kriittiset kohteet ja suhteuttaa riskit niiden merkitykseen.

Kriittiset toiminnot ja riippuvuudet

Nykytilan arviointi alkaa kriittisten toimintojen tunnistamisesta. Mitkä järjestelmät, tilat ja palvelut ovat liiketoiminnan kannalta välttämättömiä? Mitä tapahtuisi, jos ne eivät olisi käytettävissä?

Tarkastelu ei rajoitu vain omiin järjestelmiin. Toimitusketjut, ulkoistetut palvelut ja ICT-riippuvuudet ovat usein keskeisiä riskitekijöitä. Sääntely korostaa, että myös nämä riippuvuudet on huomioitava osana kokonaisuutta.

Loihteen Turvaratkaisut-palveluissa fyysisen turvallisuuden kokonaisuus arvioidaan suhteessa kriittisiin toimintoihin. Kameravalvonnan, kulunvalvonnan ja muun turvatekniikan rooli tarkastellaan osana liiketoiminnan jatkuvuutta, ei irrallisina järjestelminä.

Näkyvyys turvallisuusympäristöön

Riskienhallinta edellyttää näkyvyyttä. Organisaation on tiedettävä, miten sen kriittiset järjestelmät toimivat ja missä riskit todellisuudessa sijaitsevat.

Fyysisessä ympäristössä tämä tarkoittaa turvajärjestelmien toiminnan, kattavuuden ja suojaustason seurantaa. Loihteen tekninen valvontapalvelu tuottaa jatkuvaa näkyvyyttä turvatekniikan tilaan ja häiriöihin. Turvatekniikan analytiikkapalvelu syventää näkymää yhdistämällä eri järjestelmien tuottamaa tietoa ja hyödyntämällä analytiikkaa poikkeamien tunnistamisessa.

Digitaalisessa ympäristössä näkyvyys syntyy rakenteisesta arvioinnista ja teknisestä testauksesta. Loihteen Tietoturvan ja suojan arviointi tuottaa kokonaiskuvan kyberturvakyvykkyydestä, haavoittuvuuksista ja suojaustasosta. Tulokset suhteutetaan liiketoimintariskeihin ja sääntelyn vaatimuksiin, jolloin tarvittavat kehitystoimet voidaan kohdistaa oikein.

Näkyvyys muuttaa riskienhallinnan oletuksista johdetuksi ja osoitettavaksi toiminnaksi.

Dokumentointi ja kehityspolku

Nykytilan arvioinnin tulos ei ole pelkkä havaintolista. Sen tulee muodostaa dokumentoitu kokonaiskuva, jonka perusteella kehittämistä voidaan priorisoida ja mitata.

Kun fyysinen ja digitaalinen turvallisuus tarkastellaan yhtenä kokonaisuutena, syntyy selkeä kokonaisturvallisuuden kehityspolku. Kaikkea ei tarvitse muuttaa kerralla, mutta riskit ja toimenpiteet on pystyttävä perustelemaan ja osoittamaan.

— Keskeinen periaate —

Ilman realistista nykytilan arviointia turvallisuustyö perustuu oletuksiin. Kokonaisturvallisuuden kattava ja dokumentoitu kartoitus, jossa tarkastellaan sekä fyysistä että digitaalista toimintaympäristöä, luo perustan hallitulle kehittämiselle ja vaatimustenmukaisuuden osoittamiselle.

2.2 Jatkuva valvonta ja tilannekuva

Kokonaisturvallisuuden näkyvyys ratkaisee reagointikyvyn

Sääntely edellyttää, että organisaatio kykenee havaitsemaan poikkeamat, reagoimaan niihin ja osoittamaan, että näin tapahtuu. Tämä ei toteudu pelkästään suunnitelmilla tai yksittäisillä tarkastuksilla. Tarvitaan jatkuvaa näkyvyyttä kriittisiin toimintoihin ja järjestelmiin.

Tilannekuva kuvaa organisaation turvallisuusympäristön tämänhetkistä tilaa. Se perustuu jatkuvaan seurantaan siitä, mitä fyysisessä ja digitaalisessa ympäristössä tapahtuu, ei yksittäisiin määräajoin laadittaviin raportteihin.

Mistä tilannekuva muodostuu?

Tilannekuva syntyy useista havainnoista, jotka liittyvät toisiinsa. Fyysisessä ympäristössä tieto syntyy kulkemisesta, liikkeestä ja hälytyksistä. Digitaalisessa ympäristössä vastaavaa tietoa syntyy kirjautumisista, konfiguraatiomuutoksista ja järjestelmätapahtumista.

Yksittäinen tapahtuma ei vielä kerro paljoa. Kun tapahtumat yhdistetään, muodostuu kokonaisuus, jonka perusteella voidaan arvioida riskin vakavuutta ja vaikutusta liiketoimintaan.

Jos esimerkiksi kriittiseen tilaan kuljetaan poikkeukselliseen aikaan ja samanaikaisesti järjestelmässä tehdään hallinnollinen muutos, kokonaiskuva muuttuu. Kyse ei ole enää irrallisista havainnoista, vaan tilanteesta, joka vaatii arviointia.

Miksi fyysinen ja digitaalinen eivät ole erillisiä?

Digitaalinen infrastruktuuri sijaitsee fyysisissä tiloissa. Verkkolaitteet, tallentimet, palvelimet ja valvontajärjestelmät ovat konkreettisia kohteita, joiden suojaus perustuu sekä fyysisiin että digitaalisiin kontrollimekanismeihin.

Jos fyysinen pääsy kriittisiin kohteisiin ei ole riittävän hallittu, digitaalinen suojaus voi menettää merkityksensä. Samaan tapaan

digitaalinen haavoittuvuus voi altistaa fyysisen turvallisuusjärjestelmän väärinkäytölle.

Siksi valvonta ei voi olla jaettu kahteen siiloon. Tilannekuva on uskottava vain, jos se kattaa molemmat näkökulmat.

Kuka seuraa ja analysoi tapahtumia?

Järjestelmät tuottavat jatkuvasti dataa. Ilman aktiivista seurantaa ja analysointia tieto jää kuitenkin hyödyntämättä.

Fyysisen turvallisuuden osalta tämä tarkoittaa, että tapahtumia ei ainoastaan tallenneta, vaan niitä tarkastellaan osana laajempaa kokonaisuutta. Loihteen valvomopalvelut tukevat hälytysten käsittelyä ja tilanteiden arviointia. Turvatekniikan analytiikkapalvelu auttaa yhdistämään eri järjestelmien tuottamaa tietoa ja tunnistamaan poikkeavia tapahtumaketjuja.

Digitaalisessa ympäristössä Loihteen CSOC-kyberturvakeskus tuottaa jatkuvaa näkyvyyttä asiakasympäristöihin. Lokitietoa analysoidaan, uhkia priorisoidaan ja toimenpiteet käynnistetään hallitusti. Näin poikkeamat eivät jää yksittäisiksi hälytyksiksi, vaan niistä muodostuu ymmärrettävä tilannekuva.

Miten käyttöoikeudet ja ajantasaisuus liittyvät valvontaan?

Tilannekuva ei rajoitu siihen, mitä tapahtuu. Se sisältää myös tiedon siitä, kuka saa toimia ja millä valtuuksilla.

Jos käyttöoikeuksia ei hallita systemaattisesti, lokitieto menettää osan merkityksestään. On eri asia havaita poikkeava toiminto kuin ymmärtää, oliko tekijällä siihen oikeus. Identiteetin- ja pääsynhallinta varmistaa, että käyttöoikeudet vastaavat rooleja ja että muutokset ovat hallittuja ja dokumentoituja.

Ylläpitäjien pääsynhallinta tuo näkyvyyttä kaikkein kriittisimpiin oikeuksiin. Kun laajimmat valtuudet ovat valvottuja, myös poikkeamien analysointi perustuu luotettavaan tietoon.

Ajantasaisuus on osa samaa kokonaisuutta. Verkkoon kytketyt laitteet ja järjestelmät sisältävät ohjelmistoja, joiden turvallisuustaso vaikuttaa suoraan riskitasoon. Päivitysten tilanne ja mahdolliset haavoittuvuudet ovat osa tilannekuvaa, koska ne kertovat, missä riskipisteet voivat syntyä ennen varsinaista häiriötä.

Mitä jatkuva valvonta mahdollistaa?

Kun fyysinen ja digitaalinen tieto yhdistetään ja sitä seurataan aktiivisesti, organisaatio pystyy:

- havaitsemaan poikkeamat ajoissa
- arvioimaan niiden vaikutukset
- käynnistämään hallitun reagoinnin
- dokumentoimaan toimenpiteet

Tämä ei ole vain operatiivinen etu. Se on myös edellytys sille, että organisaatio voi osoittaa täyttävänsä sääntelyn vaatimukset.

— Keskeinen periaate —

Jatkuva valvonta muuttaa riskienhallinnan käytännön toiminnaksi. Tilannekuva syntyy vasta, kun fyysinen ja digitaalinen ympäristö nähdään yhtenä kokonaisuutena ja sitä seurataan systemaattisesti.

2.3 Elinkaaren hallinta

Turvallisuus ei ole kertahanke

Turvallisuusratkaisut hankitaan usein projektina. Järjestelmä suunnitellaan, asennetaan ja otetaan käyttöön. Sen jälkeen arki alkaa. Tässä vaiheessa moni organisaatio ajattelee työn olevan valmis. Sääntelyn näkökulmasta työ on vasta alkanut.

Sekä fyysiset että digitaaliset ratkaisut vanhenevat. Laitteiden elinkaari päättyy, ohjelmistot päivittyvät ja uusia haavoittuvuuksia löydetään jatkuvasti. Ilman systemaattista ylläpitoa turvallisuustaso ei romahda yhdessä hetkessä, vaan heikkenee vähitellen. Usein puute havaitaan vasta häiriötilanteessa.

Mitä elinkaaren hallinta tarkoittaa käytännössä?

Elinkaaren hallinta tarkoittaa, että turvallisuusratkaisujen toimivuutta, ajantasaisuutta ja kattavuutta seurataan suunnitelmallisesti. Järjestelmät eivät saa jäädä oman onnensa varaan, vaan niiden kunto, päivitykset ja tukikelpoisuus ovat tiedossa.

Fyysisessä ympäristössä tämä tarkoittaa sitä, että valvontajärjestelmät, kulunhallinta ja muut turvatekniikan ratkaisut pidetään toimintakunnossa ja ajantasaisina. Huollot, ohjelmistopäivitykset ja pääkäyttäjähallinta eivät ole erillisiä toimenpiteitä, vaan osa jatkuvaa turvallisuuden ylläpitoa. Loihteen Turvaratkaisut-palveluissa huolto- ja ylläpitopalvelut sekä pääkäyttöpal-

velut tukevat tätä kokonaisuutta ja varmistavat, että järjestelmät vastaavat muuttuvaa toimintaympäristöä.

Digitaalisessa ympäristössä elinkaaren hallinta näkyy haavoittuvuuksien tunnistamisena, korjaustoimenpiteiden koordinointina ja turvallisuuskyvykkyyden jatkuvana kehittämisenä. Kyberturvapalvelut ja CSOC-kyberturvakeskus tuottavat näkyvyyttä ympäristön riskitasoon ja tukevat korjaavien toimenpiteiden toteutusta, jotta suojaustaso ei jää staattiseksi.

Kuka vastaa jatkuvuudesta?

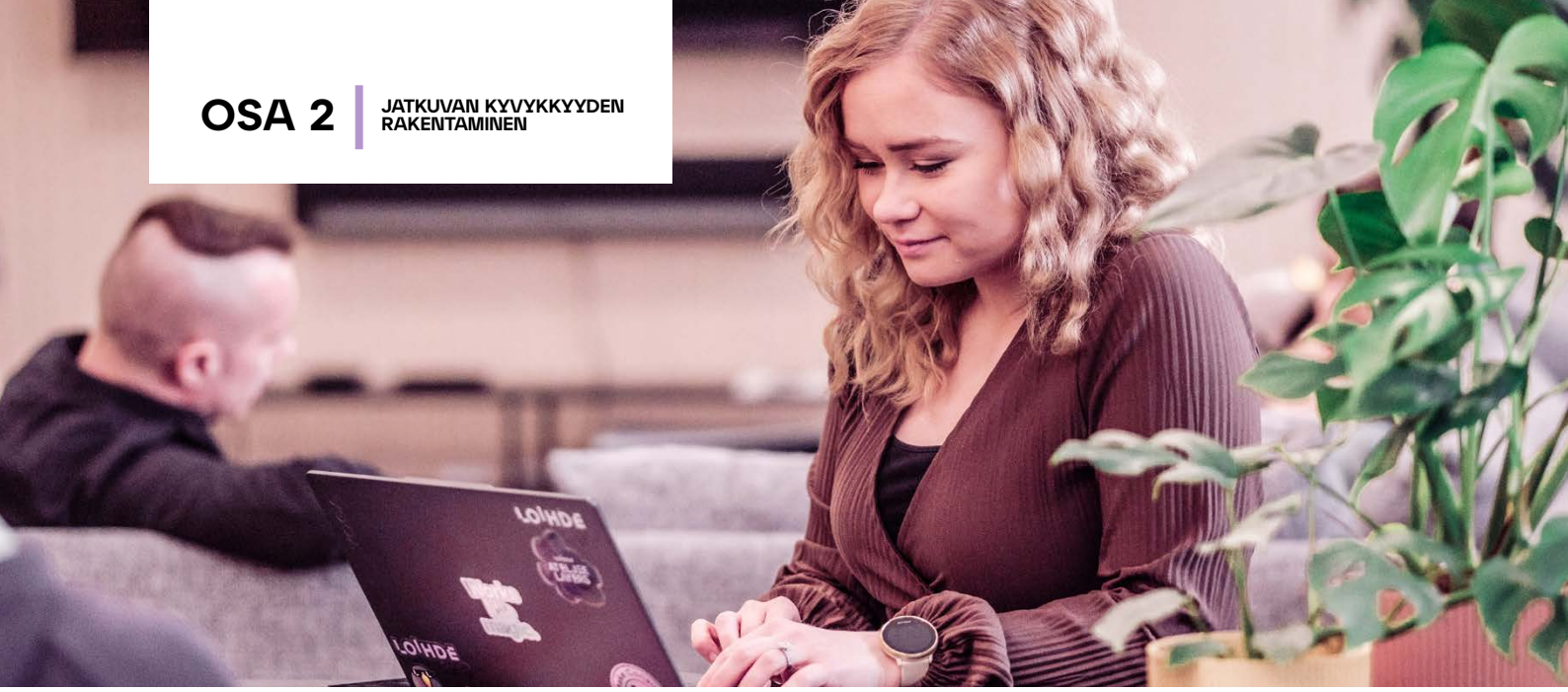
Elinkaaren hallinta ei ole vain tekninen kysymys. Se liittyy vastuisiin ja toimintamalleihin.

- Kuka seuraa, että kriittiset järjestelmät ovat tuettuja?
- Kuka varmistaa, että päivitykset toteutuvat ajallaan?
- Kuka arvioi, milloin ratkaisu ei enää vastaa riskiympäristöä?

Kun elinkaaren hallinta on osa johdettua palvelumallia, turvallisuus ei jää yksittäisten henkilöiden varaan. Se muuttuu ennakoivaksi toiminnaksi, jossa järjestelmien kunto ja riskitaso ovat tiedossa ennen kuin ongelma realisoituu.

— Keskeinen periaate —

Turvallisuus ei heikkene yhdessä yössä. Se heikkenee vähitellen, jos sitä ei ylläpidetä. Siksi elinkaaren hallinta on keskeinen osa sääntelyn edellyttämää jatkuvaa kyvykkyyttä ja osoitettavaa riskienhallintaa.



2.4 Yksi turvallisuus®

Kun kokonaisuus ratkaisee

Turvallisuutta tarkastellaan usein kahdesta näkökulmasta: fyysisenä ja digitaalisena. Käytännössä nämä eivät kuitenkaan ole erillisiä maailmoja.

Verkkoyhteydet, valvontajärjestelmät, palvelimet ja tuotantolaitteet sijaitsevat fyysisissä tiloissa. Fyysinen pääsy voi mahdollistaa digitaalisen väärinkäytön. Digitaalinen haavoittuvuus voi vaikuttaa puolestaan fyysisiin järjestelmiin. Vaikutukset ovat yhteisiä, vaikka välttämättä hallintamallit eivät aina ole.

Sääntely ei keskity siihen, mistä häiriö alkaa. Se keskittyy siihen, miten organisaatio hallitsee riskiä, reagoi poikkeamiin ja varmistaa toiminnan jatkuvuuden. Kun turvallisuutta johdetaan erillisissä siiloissa, kokonaiskuva muodostuu vasta jälkikäteen. Valvonta tapahtuu eri järjestelmissä, raportointi eri kanavissa ja vastuunrajat voivat hämärtyä.

Yksi turvallisuus® tarkoittaa sitä, että fyysiset turvaratkaisut ja kyberturvapalvelut kytkeytyvät samaan johtamismalliin. Tilannekuva muodostuu yhdestä kokonaisuudesta, ei useista erillisistä näkymistä. Riskienhallinta, valvonta, reagointi ja jatkuvuus rakentuvat yhteisen rakenteen varaan.

Tämä ei tarkoita kaikkien järjestelmien uusimista tai sitoutumista yhteen teknologiaan. Kyse on arkkitehtuurista ja toimintamallista. Olemassa olevat ratkaisut voivat toimia osana hallittua kokonaisuutta, kun ne liitetään selkeään riskienhallintaan, yhtenäiseen valvontaan ja johdettuun raportointiin.

Kun turvallisuutta johdetaan yhtenä kokonaisuutena, sääntelyn vaatimukset eivät jakaudu erillisiksi projekteiksi. Ne kytkeytyvät samaan rakenteeseen, jossa riskit tunnistetaan, poikkeamat havaitaan ja vaikutukset hallitaan systemaattisesti. Kokonaisturvallisuuden kehittäminen helpottuu merkittävästi, kun eri osa-alueet nähdään yhteisenä ja toisiaan vahvistavana kokonaisuutena.

Lopulta kysymys ei ole siitä, onko organisaatiolla riittävästi järjestelmiä. Kysymys on siitä, muodostavatko ne hallitun kokonaisuuden.

OSA 3 | KUKA TÄMÄN TEKEE?

3.1 Tehdäänkö itse vai kumppanin kanssa?

Turvallisuuden kehittäminen voidaan toteuttaa omilla resursseilla, kumppanin tuella tai yhdistelmämallilla.

Oikea ratkaisu riippuu organisaation koosta, toimintaympäristöstä ja riskiprofiilista. Keskeistä on arvioida realistisesti oma kyvykkyys ja sen jatkuvuus.

Monessa organisaatiossa turvallisuuden perustaso on jo valmiiksi hyvä. Fyysinen suojaus on rakennettu huolellisesti ja kyberturvaan on tehty investointeja. Haaste kuitenkin syntyy usein siitä, että kokonaisuus laajenee ja vaatimukset koskettavat useita osa-alueita samanaikaisesti. Turvallisuus ei ole enää yksittäinen projekti, vaan jatkuva toimintamalli.

Ennen kuin toteutusmallista päätetään, on syytä pysähtyä muutaman perustavan kysymyksen äärelle.

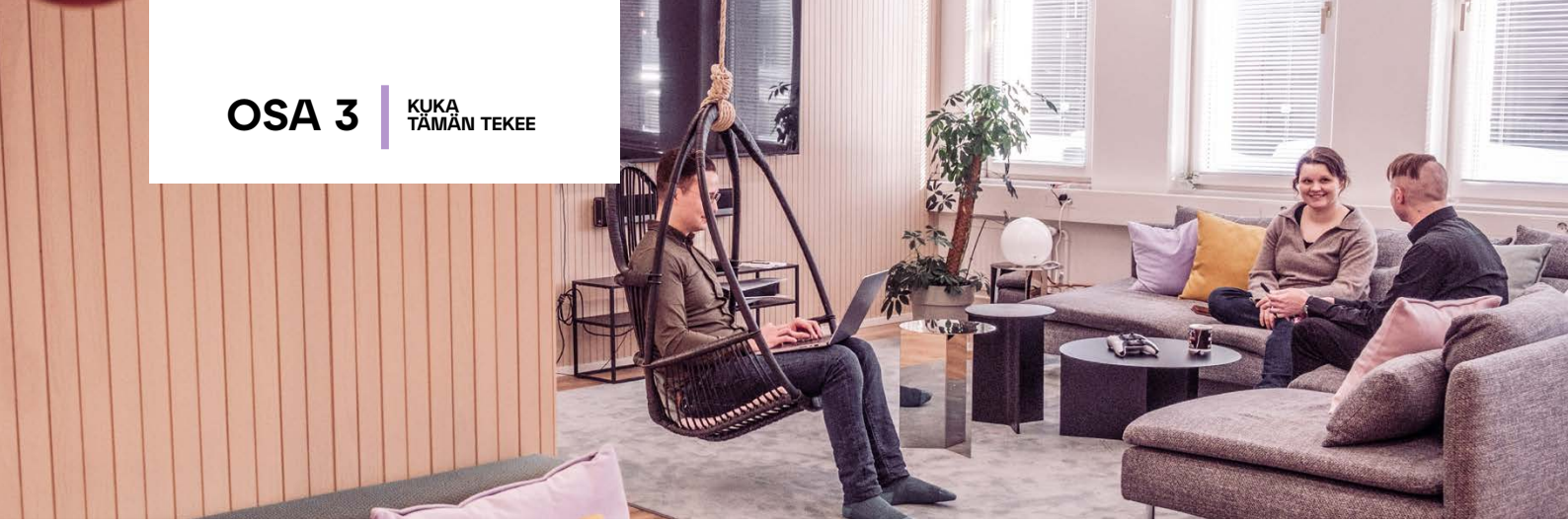
Pohdittavaa organisaatiolle

- **Onko osaaminen riittävää sekä fyysisessä että digitaalisessa turvallisuudessa?**
- **Onko valvonta ja reagointi järjestetty ympärivuorokautisesti?**
- **Onko riskienhallinta jatkuvaa vai projektiluonteista?**
- **Onko fyysisen ja digitaalisen turvallisuuden kehittäminen johdettu yhtenä kokonaisuutena?**

Usein vastaus ei ole yksiselitteinen. Osaamista on, mutta resurssit ovat rajalliset. Valvontaa on, mutta se ei kata kaikkia kriittisiä toimintoja. Prosesseja on kuvattu, mutta niiden toteutumista ei seurata systemaattisesti.

Sääntely ei edellytä, että kaikki tehdään omin voimin. Se edellyttää, että vastuut ovat selkeät ja toimintakyky säilyy myös häiriötilanteessa. Organisaation johdon vastuu ei siirry, vaikka osa toteutuksesta tehdään kumppanin kanssa.

Turvallisuudessa ratkaisevaa ei ole se, kuka tekee eniten. Ratkaisevaa on se, että kokonaisuus toimii myös silloin, kun sitä todella tarvitaan.



3.2 Millainen kumppani tukee vaatimuksia?

Kaikki turvallisuuspalvelut eivät tue sääntelyn kokonaisvaatimuksia samalla tavalla. Kumppanin valinnassa ei ole kyse yksittäisestä järjestelmästä tai hinnasta, vaan siitä, miten hyvin kokonaisuus toimii pitkällä aikavälillä.

Sääntely korostaa riskienhallintaa, jatkuvaa valvontaa, dokumentointia ja elinkaaren hallintaa. Jos kumppani keskittyy vain yhden osa-alueen toimittamiseen, vastuu kokonaisuuden yhteensovittamisesta jää organisaatiolle. Tämä voi johtaa siiloihin, päällekkäisiin ratkaisuihin ja epäselviin vastuurajoihin.

Hyvä kumppani toimii teknologianeutraalisti ja valitsee ratkaisut asiakkaan toimintaympäristön mukaan. Tavoitteena ei ole sitoa asiakasta yhteen teknologiaan tai valmistajaan, vaan rakentaa hallittu ja joustava kokonaisuus.

Keskeistä on myös kyky yhdistää fyysinen ja digitaalinen turvallisuus samaan tilannenäkymään. Kun turvajärjestelmät, valvonta ja kyberturvatoiminnot tukevat toisiaan, syntyy yhtenäinen tilannekuva. Ilman tätä kokonaisuus jää helposti hajanaiseksi.

Toinen ratkaiseva tekijä on palvelumalli. Projektitoimitus voi ratkaista yksittäisen tarpeen, mutta sääntelyn näkökulmasta turvallisuuden on pysyttävä ajan tasalla. Kumppanin on kyettävä tarjoamaan jatkuvaa ylläpitoa, kehittämistä ja reagointikykyä, ei pelkkää käyttöönottoa.

Kumppanin rooli ei rajoitu tekniseen toteutukseen. Sen tulee kyetä tuottamaan selkeää raportointia, tukemaan päätöksentekoa ja osallistumaan turvallisuuden kehittämiseen osana organisaation johtamisrakennetta. Kun turvallisuutta johdetaan tiedolla, kehittäminen muuttuu suunnitelmalliseksi.

— Keskeinen periaate —

Sääntelyn vaatimukset eivät kohdistu yksittäisiin järjestelmiin, vaan organisaation kykyyn hallita turvallisuutta kokonaisuutena. Kumppanin on pystyttävä tukemaan riskienhallintaa, valvontaa, reagointia ja jatkuvaa kehittämistä sekä fyysisessä että digitaalisessa ympäristössä.

Turvallisuuden muistilista organisaatioille

Dokumentoitu riskienarviointi

Organisaatiolla on ajantasainen ja dokumentoitu arvio kriittisistä toiminnoista, keskeisistä riippuvuuksista ja merkittävimmistä riskeistä.

Selkeä vastuunjako

Turvallisuuden omistajuus, päätöksenteko ja raportointi ovat määritelty. Johdolla on näkyvyys kokonaisuuteen.

Jatkuva valvonta

Kriittiset tilat, järjestelmät ja verkot ovat aktiivisen seurannan piirissä. Poikkeamien havaitsemiseen ja käsittelyyn on määritelty prosessi.

Toimitusketjun hallinta

Keskeiset palveluntarjoajat ja tekniset riippuvuudet on tunnistettu, ja niiden riskit arvioidaan säännöllisesti.

Päivitysten ja haavoittuvuuksien hallinta

Sekä turvatekniikan että tietojärjestelmien päivityksistä ja korjauksista huolehditaan suunnitelmallisesti.

Harjoiteltu toimintamalli

Poikkeamatilanteiden käsittelyä on testattu. Organisaatio tietää, miten toimitaan ja miten raportointi hoidetaan.

Säännöllinen raportointi johdolle

Turvallisuustilanne esitetään liiketoimintariskin näkökulmasta, ei pelkästään teknisinä mittareina.