Tietoturvallisuuden merkitys osana yritysten toimitusketjujen hallintaa

19. Turvallisuusjohdon koulutusohjelma

Lopputyöraportti

Kirill Filatov

Konecranes Global Oy

Helsinki 31.3.2026

Aalto University Executive Education and Professional Development

Tiivistelmä

Tässä työssä tarkastellaan toimitusketjuun liittyvien tietoturvallisuusriskien merkitystä ja hallintaa osana organisaation kokonaisvaltaista turvallisuuden johtamista. Työ lähtee liikkeelle toimintaympäristön muutoksesta, jossa ulkoisten toimijoiden rooli on kasvanut ja samalla organisaatioiden riippuvuudet toimitusketjuista ovat syventyneet. Tämä kehitys on näkynyt myös tietoturvallisuudessa, jonka varmistamisesta on tullut kriittistä myös toimitusketjun turvallisuuden osana.

Työssä analysoidaan keskeisiä toimitusketjuun liittyviä tietoturvallisuusriskejä sekä niiden hallintaa ohjaavaa kansainvälistä regulaatiota ja viitekehyksiä. Lisäksi tunnistetaan käytännön haasteita, kuten toimitusketjujen monimutkaisuus, näkyvyyden puute, vastuun hajautuminen sekä riskiperusteisuuden toteutumisen vaikeus organisaatioissa.

Työn keskeinen tavoite on käytännönläheinen malli toimitusketjun tietoturvallisuusriskien tehokkaaseen hallintaan. Malli kattaa toimittajien kategorisoinnin, riskiprofiloinnin, arvioinnin, sopimuksellisen ohjauksen, elinkaaren hallinnan sekä auditoinnin ja poikkeamien käsittelyn. Erityisesti korostetaan riskiperusteista lähestymistapaa, toimittajasuhteiden ymmärtämistä kokonaisuuksina sekä organisaation kykyä toimia epävarmuuden ja monimutkaisuuden keskellä.

Työ yhdistää teoreettisen tarkastelun ja käytännön näkökulman, tarjoten jäsennellyn kokonaisuuden, jota organisaatiot voivat hyödyntää kehittäessään toimitusketjuun liittyvää tietoturvallisuuden hallintaa.

Abstract

This work examines the role and management of information security risks within supply chains as part of an organization's overall security governance. It builds on the observation that modern organizations are increasingly dependent on external suppliers, technologies, and services, making supply chains a critical extension of their own security posture.

The work explores important information security risks arising from supply chain dependencies and reviews how these risks are addressed in international regulations and security frameworks. It also identifies practical challenges organizations face, including limited visibility beyond direct suppliers, fragmented ownership of supplier risks, and the difficulty of applying truly risk-based approaches in complex environments.

The main contribution of this work is a practical and structured model for managing supply chain information security risks. The model covers supplier segmentation, risk profiling, onboarding assessments, contractual controls, lifecycle management, auditing, and incident handling. Particular emphasis is placed on understanding supplier relationships as dynamic dependencies rather than static entities, and on aligning security practices with real-world constraints.

By combining theoretical insights with practical considerations, the thesis provides a structured approach that organizations can apply to strengthen the management of information security across their supply chains.

Sisältö

1 Johdanto

1.1 Työn tausta

Yritysten toimintaympäristö on viime vuosina muuttunut tavalla, joka on siirtänyt merkittävän osan organisaatioiden riskeistä niiden omien rajojen ulkopuolelle. Toimitusketjut eivät ole enää vain hankinnan tai logistiikan haasteita, vaan ne muodostavat keskeisen osan organisaatioiden teknologiasta, operatiivisesta tekemisestä ja tietoon liittyvästä kokonaisuudesta. Samalla tietoturvallisuus on yrityksissä kehittynyt yksittäisestä tukifunktiosta yhdeksi keskeisimmistä liiketoiminnan jatkuvuuden ja luottamuksen mahdollistajista.

Tämä työ on laadittu osana Aalto-yliopiston Turvallisuusjohdon koulutusohjelmaa (TJK), jossa tarkastellaan yritysturvallisuutta kokonaisvaltaisena johtamisen alueena. Ohjelman keskeinen ajatus on yhdistää eri turvallisuuden osa-alueet – kuten riskienhallinta, tietoturvallisuus, jatkuvuudenhallinta ja sidosryhmäyhteistyö – yhtenäiseksi johtamisen kokonaisuudeksi, jossa turvallisuus nähdään arvon, jatkuvuuden ja luottamuksen mahdollistajana. Tässä kontekstissa toimitusketjun tietoturvallisuus nousee erityisen merkittäväksi teemaksi. Se toimii rajapintana useiden turvallisuuden osa-alueiden välillä ja tuo näkyväksi sen, kuinka vahvasti organisaation turvallisuus riippuu sen ulkoisista kumppaneista. Toimitusketjun kautta syntyvät riskit eivät ole enää poikkeuksia, vaan osa normaalia toimintaympäristöä.

1.2 Työn tavoitteet

Tämän työn tavoitteena on tarkastella toimitusketjuun liittyvien tietoturvallisuusriskien hallintaa kokonaisuutena, joka yhdistää viitekehyksiä, regulatiivisia vaatimuksia sekä käytännön toimintamalleja. Työ pyrkii vastaamaan kysymykseen, miten organisaatiot voivat hallita toimitusketjuun liittyviä tietoturvallisuusriskejä tehokkaasti tilanteessa, jossa riippuvuudet ovat monimutkaisia, osittain näkymättömiä ja jatkuvasti muuttuvia.

Työssä ei keskitytä yksittäisiin teknisiin kontrolliratkaisuihin, vaan laajempaan johtamisen näkökulmaan: miten toimittajasuhteita tulisi ymmärtää, miten riskejä tulisi priorisoida ja millä tavoin organisaatio voi rakentaa toimintamallin, joka toimii myös käytännössä.

Työn keskeinen tavoite ei ole ainoastaan kuvata toimitusketjun tietoturvallisuuteen liittyviä ilmiöitä, vaan tuottaa jäsennelty ja käytännössä hyödynnettävä kokonaisuus, joka auttaa organisaatioita kehittämään omaa toimintaansa. Työ pyrkii tuomaan näkyväksi erityisesti ne kohdat, joissa teoria ja käytäntö eroavat toisistaan, sekä tarjoamaan näkökulmia siihen, miten tätä kuilua voidaan kaventaa. Samalla työ heijastaa Turvallisuusjohdon koulutusohjelma (TJK):n keskeistä ajatusta: turvallisuus ei ole yksittäinen toiminto, vaan johtamisen kokonaisuus, joka syntyy eri osa-alueiden yhteensovittamisesta. Toimitusketjun tietoturvallisuus toimii tässä kokonaisuudessa erityisenä mittarina organisaation kyvylle hallita monimutkaisuutta, epävarmuutta ja ulkoisia riippuvuuksia.

1.3 Lähestymistapa

Työ on luonteeltaan analyyttinen ja soveltava. Se ei pyri rakentamaan uutta teoriaa, vaan kokoamaan yhteen olemassa olevaa tietoa, jäsentämään sitä ja tarkastelemaan sitä kriittisesti käytännön kontekstissa. Lähestymistapa yhdistää ulkoisia kirjallisuuslähteitä, kansainvälisiä standardeja ja regulaatiota sekä kirjoittajan oman kokemuksen toimitusketjujen ja tietoturvallisuuden hallinnasta.

Kirjoitustapa on tarkoituksellisesti kaksitasoinen. Yhtäältä työ nojaa akateemiseen rakenteeseen ja käsitteelliseen selkeyteen, jossa ilmiötä tarkastellaan systemaattisesti eri näkökulmista. Toisaalta teksti pyrkii säilyttämään käytännönläheisyyden ja välttämään liiallista abstraktiota. Tavoitteena ei ole vain kuvata, miten toimitusketjun tietoturvallisuutta tulisi hallita teoriassa, vaan ennen kaikkea tarkastella, miten sitä todellisuudessa hallitaan – ja miksi siinä usein epäonnistutaan.

Keskeinen valinta kirjoitustavassa on ollut välttää liiallista yksinkertaistamista. Toimitusketjuun liittyvät tietoturvallisuusriskit eivät ole yksiselitteisiä

tai helposti rajattavia. Ne syntyvät usein useiden tekijöiden yhteisvaikutuksesta: teknisistä riippuvuuksista, organisatorisista rakenteista, sopimuksellisista ratkaisuista ja ihmisten tekemistä päätöksistä. Tästä syystä työ pyrkii käsittelemään aihetta tavalla, joka tunnistaa sen monimutkaisuuden, mutta tekee siitä samalla ymmärrettävän ja jäsennettävän.

1.4 Työn rajaukset

Tässä työssä keskitytään ensisijaisesti toimitusketjuun liittyviin tietoturvallisuusriskien hallintaan. Vaikka toimitusketjujen riskienhallinta kattaa myös esimerkiksi fyysisen turvallisuuden, geopoliittiset riskit ja vastuullisuuskysymykset, nämä teemat rajataan pääosin tarkastelun ulkopuolelle tai niitä käsitellään vain siltä osin kuin ne liittyvät tietoturvallisuuteen.

Lisäksi työ tarkastelee aihetta pääasiassa organisaation näkökulmasta, joka käyttää ja hallitsee monimutkaista, globaalia toimittajaverkostoa. Tämä tarkoittaa, että tarkastelun painopiste on erityisesti keskisuurissa ja suurissa organisaatioissa, joissa toimittajamäärät, teknologiset riippuvuudet ja regulaatiovaatimukset muodostavat monimutkaisen kokonaisuuden. Kirjoittaja on työn kirjoittamisen aikaan työskennellyt Konecranes Global Oy:ssa, mutta tämä työ ei heijasta kirjoittajan työnantajan näkemyksiä tai pidä sisällään yrityksen luottamuksellista tietoa. Kaikki tässä työssä esitetyt väitteet ovat kirjoittajan omia ja yhtäläisyydet työnantajaan ovat sattumaa.

1.5 Kirjoittajasta

Kirill Filatov on valmistunut vuonna 2010 Aalto Yliopiston Kauppakorkeakoulusta IT-johtamisen Maisteriksi ja haaveili IT-johtajan urasta. Tietoturvallisuus vei hänet osittain vahingossa mukaansa 2012 ja hän on siitä lähtien luonut uraa tietoturvallisuuskonsulttina ja erinäisissä tietoturvallisuuden johtotehtävissä. Kirill työskentelee tällä hetkellä toista vuotta Konecranes Global Oy:llä, jossa hän johtaa hallinnollisen tietoturvallisuuden tiimiä, joka vastaa tietoturvallisuuden hallintamallista, tietoturvallisuusriskeistä, tietoturvallisuusregulaation hallinnasta, sekä sovelluskehityksen ja toimittajien tietoturvallisuuden hallintamalleista. Ennen tätä Kirill työskenteli lähes viisi vuotta S-ryhmän CISO:na vastaten ryhmän kokonaisvaltaisesta tietoturvallisuudesta. Vapaa-ajallaan Kirill soveltaa hallintamalli-oppeja Köpsö-koiraansa – käytännön tulokset ovat edelleen tutkimusvaiheessa.

2 Toimitusketjun merkitys osana kokonaisvaltaista turvallisuuden hallintaa

2.1 Yritysten toimintaympäristön muutos

Yritysten toimintaympäristö on viime vuosikymmeninä muuttunut merkittävästi globalisaation, digitalisaation, lisääntyneen regulaation ja ulkoistamisen lisääntymisen seurauksena. Harva organisaatio tänä päivänä tuottaa tuotteensa ja palvelunsa itse, vaan liiketoiminta rakentuu laajojen toimittaja- ja kumppaniverkostojen varaan. Tämän vuoksi yrityksen toiminta ja siihen liittyvät riskit eivät ole enää pelkästään oman organisaation hallittavissa, vaan siihen vaikuttavat lukuisat ulkopuoliset toimijat, kuten alihankkijat, teknologiatoimittajat, palveluntarjoajat ja muut kumppanit. (Christopher & Peck, 2004) Näistä toimijoista muodostuvasta kokonaisuudesta puhutaan tässä työssä toimitusketjuna.

Perinteisesti toimitusketjun hallinta on keskittynyt logistiikan, hankinnan ja tuotannon tehokkuuden optimointiin. Tavoitteena on ollut kustannustehokkuuden, toimintavarmuuden ja tuotannon jatkuvuus. Viime vuosina toimitusketjujen merkitys on kuitenkin ymmärretty laajemmin myös turvallisuuden näkökulmasta. Organisaatiot ovat yhä riippuvaisempia ulkoisista kumppaneista, mikä tarkoittaa, että myös turvallisuusriskit syntyvät enenemissä määrin oman organisaation ulkopuolella. Tämän vuoksi toimitusketjujen turvallisuuden hallinta on monissa yrityksissä noussut keskeiseksi osaksi yritysten kokonaisvaltaista turvallisuuden hallintaa.

2.2 Toimitusketjun merkitys osana kokonaisvaltaista turvallisuuden hallintaa

Kokonaisvaltainen turvallisuuden hallinta tarkoittaa organisaation kykyä tunnistaa, arvioida ja hallita erilaisia turvallisuusriskejä systemaattisesti ja enna-

koivasti. Se kattaa useita osa-alueita, kuten fyysisen turvallisuuden, henkilöstöturvallisuuden, tietoturvallisuuden, tuotannon turvallisuuden sekä liiketoiminnan jatkuvuuden hallinnan. Kun ulkoisten toimijoiden käyttäminen yrityksessä lisääntyy, myös näihin liittyvät riskit lisääntyvät näillä kaikilla osa-alueilla.

Toimitusketjujen häiriöt voivat vaikuttaa suoraan yrityksen kykyyn toimittaa tuotteita asiakkaille, ylläpitää tuotantoa tai suojata luottamuksellista tietoa, minkä vuoksi toimitusketjuun liittyvä riskienhallinta toimii myös keskeisessä osassa liiketoiminnan jatkuvuuden varmistamista (Suresh, Sanders & Braunscheidel, 2020).

Toimitusketjujen merkitys korostuu erityisesti tilanteissa, joissa yritys on vahvasti riippuvainen tietyistä kriittisistä toimittajista tai teknologioista IT-palveluiden tuottamiseen liittyen. Monet yritykset käyttävät esimerkiksi ulkoisia IT-toimittajia, pilvipalveluja tai ohjelmistokomponentteja, joiden toiminta on keskeistä liiketoiminnan jatkuvuuden ja tiedon suojaamisen kannalta. Mikäli näissä palveluissa ilmenee häiriöitä tai turvallisuuspuutteita, seuraukset voivat heijastua laajasti koko toimitusketjuun ja edelleen yrityksen asiakkaisiin. Tämän vuoksi toimitusketjun turvallisuus ei ole ainoastaan yksittäisten organisaatioiden sisäinen kysymys, vaan se liittyy laajemmin eri toimijoiden väliseen riippuvuuteen.

2.3 Toimitusketjun hallinnan haasteet

Toimitusketjujen turvallisuutta tarkasteltaessa keskeisin haaste liittyy niiden monimutkaisuuteen ja laajuuteen. Suurilla organisaatioilla voi olla satoja tai jopa tuhansia toimittajia eri puolilla maailmaa. Näillä toimittajilla voi puolestaan olla omia alihankkijoitaan, jolloin syntyy useita toimitusketjun tasoja. Tämä lisää riskiä siitä, että turvallisuuspuutteet voivat jäädä huomaamatta ketjun alemmilla tasoilla. Lisäksi toimitusketjujen kansainvälisyys tuo mukanaan erilaisia toimintakulttuureja, regulaatioviitekehyksiä ja turvallisuuskäytäntöjä, mikä voi vaikeuttaa yhtenäisten turvallisuusvaatimusten toteuttamista.

Turvallisuuden näkökulmasta toimitusketjujen hallinnassa korostuu erityisesti riskienhallinnan merkitys. Organisaatioiden on kyettävä tunnistamaan, mitkä toimittajat ja palvelut ovat liiketoiminnan kannalta kriittisiä, ja millai-

sia riskejä näiden käyttöön liittyy. Riskit voivat liittyä esimerkiksi toimitusvarmuuteen, tietoturvaan, geopoliittisiin tekijöihin tai toimittajan taloudelliseen tilanteeseen.

Viime vuosien tapahtumat ovat osoittaneet, kuinka haavoittuvaisia toimitusketjut voivat olla erilaisille häiriöille. Esimerkiksi geopoliittiset jännitteet, pandemiat sekä kyberhyökkäykset ovat vaikuttaneet merkittävästi globaaleihin toimitusketjuihin. Tällaiset tapahtumat ovat korostaneet tarvetta kehittää toimitusketjujen resilienssiä eli kykyä kestää häiriöitä ja palautua niistä nopeasti. Resilienssi edellyttää paitsi teknisiä ratkaisuja myös strategista johtamista, jossa turvallisuus huomioidaan osana organisaation päätöksentekoa.

2.4 Toimitusketjun hallinta osana turvallisuusjohtamista

Yritysten turvallisuusjohtamisen näkökulmasta toimitusketjujen tehokas hallinta muodostaa keskeisen osa-alueen, joka vaatii sekä strategista että operatiivista ohjausta. Turvallisuus ei rajoitu pelkästään organisaation sisäisiin prosesseihin, vaan sen on ulotuttava myös yrityksen kumppaneihin ja toimittajiin. Tämä edellyttää selkeitä turvallisuusvaatimuksia, yhteistyötä eri toimijoiden välillä sekä jatkuvaa riskien arviointia muuttuvassa toimintaympäristössä.

Kokonaisuutena tarkasteltuna toimitusketjujen merkitys osana kokonaisvaltaista turvallisuuden hallintaa on kasvanut merkittävästi. Yritysten kyky hallita toimitusketjujaan turvallisesti vaikuttaa suoraan niiden liiketoiminnan jatkuvuuteen, maineeseen sekä asiakkaiden luottamukseen. Tämän vuoksi toimitusketjun turvallisuuden kehittäminen on noussut keskeiseksi teemaksi niin yritysten turvallisuusjohtamisessa kuin kansallisessa ja kansainvälisessä sääntelyssä.

3 Tietoturvallisuus osana toimitusketjun hallintaa

3.1 Toimitusketjun merkitys osana modernin organisaation tietoturvallisuuden hallintaa

Lisääntyneen digitalisaation myötä yritysten toimitusketjut ovat muuttuneet yhä tiiviimmin IT-järjestelmiin ja digitaalisiin palveluihin kytkeytyneiksi kokonaisuuksiksi. Toimitusketjujen sujuva toiminta perustuu laajasti tietojärjestelmien väliseen tiedonvaihtoon, automatisoituihin IT-prosesseihin sekä erilaisiin digitaalisiin alustoihin. Tämä kehitys on lisännyt toimitusketjujen tehokkuutta ja näiden läpinäkyvyyttä, mutta samalla lisääntynyt kompleksisuus on tuonut mukanaan uusia tietoturvallisuuteen liittyviä riskejä (Ivanov & Dolgui, 2020). Organisaatiot eivät nykyisin välttämättä tiedä missä heidän omistamansa tieto fyysisesti sijaitsee tai kuka siihen pääsee käsiksi, ja järjestelmien ylläpito on konkreettisesti siirtynyt pois organisaation käsistä. Kun järjestelmävalvoja ennen saattoi ennen istua fyysisesti samassa toimistossa ja tiesi tarkalleen, miten tietty palvelun on konfiguroitu, niin nyt tämä tieto saattaa olla monen ihmisen ja pitkän selvitysketjun takana ja tämän kompleksiuuden ymmärtäminen ja hallinta on haasteellista. Tämän vuoksi tietoturvallisuuden merkitys osana toimitusketjun hallintaa ja organisaatioiden kokonaisvaltaista turvallisuusjohtamista on noussut merkittävään rooliin, ja organisaatiot ovat jopa ryhtyneet kehittämään toimittajanhallinnan tietoturvallisuusstrategioita vähentääkseen näiden aiheuttamia poikkeamia yrityksen toiminnalle (Van‘t Schip, 2024).

Toimitusketjun hallinnalla tarkoitetaan organisaation kykyä suunnitella, ohjata ja valvoa toimitusketjun eri toimijoiden välistä yhteistyötä siten, että tuotteiden, palveluiden ja tiedon virta toimii tehokkaasti ja luotettavasti. Tietoturvallisuudella viitataan yksinkertaistettuna usein tietoturvallisuuden perusmalliin, joka varmistetaan tiedon suojaus kolmen pilarin varmistamisen kautta: luottamuksellisuus (vain valtuutetut tahot pääsevät käsiksi), eheys (tieto on

oikeanlaista ja muuttumatonta) sekä saatavuus (järjestelmät ovat käytettävissä, kun niitä tarvitaan). Tietoturvallisuuden varmistaminen osana toimitusketjun hallintaa on tullut yhä tärkeämmäksi, sillä toimitusketjujen eri toimijat käsittelevät usein yrityksen omistamia tietoja, käyttävät yhteisiä järjestelmiä yrityksen kanssa ja ovat usein jonkinlaisessa roolissa yrityksen liiketoiminnan jatkuvuuden osana. Tietoturvallisuudessa puhutaan usein heikoimman lenkin konseptista, viitaten siihen, että tietoturvallisuus on vain niin laadukasta kuin heikoin osa suojausta. Kun toimittajien rooli yrityksen toiminnassa kasvaa, toimitusketjun tietoturvallisuusasioiden pitää olla yhtä hyvässä kunnossa kuin muidenkin osa-alueiden.

Osana liiketoimintaa, yritykset jakavat toimitusketjuissaan usein toimittajille merkittäviä määriä luottamuksellista tietoa ja toimittajat saattavat olla kriittisessä roolissa osana jonkin palvelun tuottamista. Tietojen jakaminen on usein välttämätöntä yhteistyön mahdollistamiseksi, mutta samalla se lisää riskiä tietojen väärinkäytölle tai vuotamiselle kun tiedon hallinta ja suojakontrollit siirtyvät pois yritykseltä itseltään. Toimittajien ja muiden yhteistyökumppaneiden tietoturvakäytännöt voivat vaihdella merkittävästi, mikä tekee toimitusketjun kokonaisriskin hallinnasta äärimmäisen haastavaa. Toimittajien kiinnostus tietoturvallisuutta kohtaan voi myös vaihdella merkittävästi riippuen monista erinäisistä asioista. Tämän vuoksi yrityksen on kriittistä varmistaa, että myös toimitusketjussa noudatetaan riittäviä ja mielellään yrityksen omia kontrolleja vastaavia tietoturvakäytäntöjä.

3.2 Toimitusketjuun liittyvät tietoturvallisuusriskit

Toimitusketjun tietoturvariskit voivat ilmetä monella eri tavalla. Keskeinen riski liittyy tilanteisiin, joissa haitallinen taho pyrkii hyödyntämään toimitusketjua heikoimpana lenkkinä päästäkseen käsiksi kohdeorganisaation järjestelmiin tai tietoihin. Tällaisia hyökkäyksiä kutsutaan usein toimitusketjuhyökkäyksiksi. Niissä haitallinen taho ei välttämättä kohdista hyökkäystään suoraan kohdeyritykseen, vaan sen toimittajaan tai palveluntarjoajaan, jonka kautta pääsy yrityksen järjestelmiin on mahdollista. ENISA:n ja Verizon Data Breach Investigations-raportin mukaan toimitusketjuhyökkäykset ovat viime vuosina lisääntyneet merkittävästi, mikä korostaa toimitusketjujen turvallisuuden merkitystä osana organisaatioiden kyberturvallisuutta (ENISA, 2021, Verizon, 2025). On myös huomattava, että toimitusketjuhuijaukset eivät vält-

tämättä kohdistu suoraan yritykseen, vaan toimitusketjussa tapahtuvat tietoturvapoikkeamat saattavat aiheuttaa yritykselle merkittäviä haasteita ilman että juuri kyseiseen yritykseen olisi kohdistettu hyökkäystä kuten kävi logistiikkayritys Maerskille vuonna 2018 (Maersk, 2018)

Toimitusketjun tietoturvallisuuteen liittyvät riskit voivat syntyä myös tahattomien virheiden tai puutteellisten toimintatapojen seurauksena. Esimerkiksi puutteellisesti suojatut järjestelmät, heikot käyttöoikeuksien hallintakäytännöt tai riittämätön henkilöstön tietoturvaosaaminen toimitusketjun osana voivat altistaa kohdeyrityksen tietoturvapoikkeamille. Tämän vuoksi tietoturvallisuuden hallinta osana toimitusketjun hallintaa edellyttää systemaattista lähestymistapaa, jossa huomioidaan sekä tekniset ratkaisut että organisatoriset toimintamallit.

3.3 Toimitusketjun tietoturvallisuusriskien hallinta

Organisaatiot voivat hallita toimitusketjun tietoturvallisuusriskejä useilla eri keinoilla. Keskeisin ja yleisin keino on tietoturvavaatimusten sisällyttäminen toimittajasopimuksiin ja hankintaprosesseihin. Tällä varmistetaan juridisesti toimittajan noudattavan tiettyjen tietoturvakäytäntöjen noudattamista, säännöllisiä auditointeja tai tietoturvapoikkeamien raportointia.

Toinen tärkeä osa toimitusketjun tietoturvan hallintaa on toimittajien arviointi ja jatkuva seuranta. Organisaatioiden on tunnistettava, mitkä toimittajat ovat liiketoiminnan kannalta kriittisiä ja millaisia tietoturvariskejä niiden toimintaan liittyy. Tämän arvioinnin perusteella voidaan määrittää, millaisia valvonta- ja hallintatoimenpiteitä tarvitaan. Esimerkiksi kriittisten toimittajien osalta voidaan toteuttaa tarkempia turvallisuusarviointeja tai auditointeja, kun taas vähemmän kriittisten toimittajien osalta voidaan käyttää kevyempiä menettelyjä.

Tietoturvallisuuden integroiminen toimitusketjun hallintaan edellyttää myös organisaation sisäistä yhteistyötä. Toimitusketjujen tietoturvallisuuteen liittyvien riskien hallinta ei saisi olla yrityksen tietoturvallisuusyksikön vastuulla, vaan siihen tehokkaasti toteutettuna sen pitää perustua laajasta jalkautettuihin toimintamalleihin ja prosesseihin, johon osallistuvat myös hankinta-, riskienhallinta-, laki- ja ennen kaikkea eri liiketoimintayksiköt, jotka tosiasiassa vastaavan kunkin toimittajan tehokkaasta ja turvallisesta hallin-

nasta. Tehokas toimitusketjun tietoturvallisuuden hallinta edellyttää, että yrityksen eri toiminnot tekevät tiivistä yhteistyötä, jakavat tietoa riskeistä ja näihin liittyvistä hallintatoimenpiteistä.

Viime vuosina toimitusketjujen tietoturvallisuusasiat ovat nousseet kriittiseen rooliin myös eri maiden lainsäädäntöjen ja kansainvälisten standardien tasolla. Myös kaikki merkittävät turvallisuusstandardit ja viitekehykset kuten ISO27001 ja ”NIST Cybersecurity Framework” korostavat toimittajasuhteiden ja toimitusketjujen hallinnan merkitystä tietoturvallisuuden näkökulmasta.

4 Toimitusketjuun liittyvien tietoturvallisuusriskien hallinta globaalissa regulaatiokentässä

4.1 Regulatiivisten vaatimuksien lisääntyminen globaalisti

Viime vuosina toimitusketjun tietoturvallisuusasiat ovat nousseet merkittävään rooliin osana regulatiivisia vaatimuksia ympäri maailmaa, Euroopassa mm. NIS2-regulaation myötä (Van't Schip, 2024). Tietoturvallisuutta on pitkään käsitelty ensisijaisesti yksittäisen organisaation sisäisenä asiana, mutta yhä useammin lainsäätäjät ovat ryhtyneet tarkastelemaan tietoturvallisuutta ekosysteemisenä ilmiönä, jossa riskit syntyvät myös organisaation rajojen ulkopuolella (toimittajat, alihankkijat, ohjelmistokomponentit, pilvipalvelut, integraatiot ja hallintaketjut) ja jossa yritys toimii osana isompaa kokonaisuutta, esimerkiksi Euroopassa osana koko Euroopan yhteistä kyberpuolustusta. Tämän myötä toimitusketjun tietoturvallisuusasiat eivät ole enää taustaoletus, vaan ne on nostettu sääntelyssä eksplisiittiseksi vaatimukseksi: toimittajasuhteiden hallinnasta, hankinnoista, ohjelmistokehityksen käytännöistä ja haavoittuvuuksien elinkaaren hallinnasta on tullut sääntelyn kohteita, ei pelkästään parhaiden käytäntöjen suosituksia.

Viime vuosien merkittävät, julkisuudessakin nähdyt tietoturvallisuuspoikkeamat ovat osaltaan vauhdittaneet sääntelyn kehitystä, mutta tähän kehitykseen on vaikuttanut myös muut trendit. Toimitusketjujen digitalisoituminen on tehnyt riippuvuuksista syvempiä ja nopeammin skaalautuvia: yhden laajasti käytetyn ohjelmistokomponentin haavoittuvuus tai yhden palveluntarjoajan tietoturvallisuushaasteet voivat vaikuttaa lyhyessä ajassa laajaan joukkoon organisaatioita. Vakavin esimerkki tästä nähtiin vuonna 2020 SolarWinds-yrityksen tietoturvapoikkeaman myötä. Hakkerit onnistuivat asentamaan yrityksen tarjoamaan IT-valvontajärjestelmään haittaohjelman, joka onnistui leviämään globaalisti tuhansiin organisaatioihin, ml. Yhdysvaltojen hallintoon. Haitalliset toimijat onnistuivat pääsemään käsiksi asiakasyritysten

tietoihin kohdistamatta mitään haitallista toimintaa suoraan näiden tietoverkkoihin (Case SolarWinds, 2020).

Geopoliittinen toimintaympäristö on tuonut toimitusketjuun mukaan myös luottamusketjun ulottuvuuden: toimitusketjuun liittyvät riskit ajatellaan yhä useammin myös kansallisen turvallisuuden, strategisten riippuvuuksien ja kriittisen infrastruktuurin näkökulmasta.

4.2 Euroopan Unioni

EU:ssa toimitusketjuun liittyvä tietoturvallisuuden sääntely on vahvistunut kahdella eri tavalla. Organisaatiotason riskienhallintavelvoitteiden laajentaminen NIS2-regulaation kautta ja siinä esitetyt vaatimukset liittyen toimitusketjun tietoturvallisuuden hallintaa, sekä tuoteturvallisuuteen liittyvän CRA-regulaation kautta, jossa asetetaan merkittäviä vaatimuksia toimitusketjun tietoturvallisuudelle, kun yritys saattaa tuotteita EU:n markkinoille.

4.2.1 The Directive on security of network and information systems, eli Euroopan Unionin Kyberturvallisuusdirektiivi (NIS2)

Euroopan unionin kyberturvallisuussääntelyssä toimitusketjun tietoturvallisuus on noussut keskeiseen asemaan erityisesti NIS2-direktiivin myötä (NIS2, 2022). Direktiivi (EU) 2022/2555 korvaa vuonna 2016 annetun alkuperäisen NIS-direktiivin ja pyrkii vahvistamaan kyberturvallisuuden tasoa koko unionin alueella laajentamalla sekä sääntelyn soveltamisalaa että organisaatioille asetettuja riskienhallintavelvoitteita. Yksi keskeisistä muutoksista aiempaan sääntelyyn nähden on toimitusketjujen tietoturvallisuusriskien eksplisiittinen huomioiminen osana organisaatioiden kyberturvallisuuden riskienhallintaa. Tämän lisäksi regulaatio velvoittaa yrityksen huolehtimaan koko toimitusketjusta, joka pitää sisällään myös toimittajien alihankkijat, komponenttivalmistajat, pilvipalvelut ja ohjelmistokomponentit.

NIS2-direktiivi on laajentanut kyberturvallisuutta koskevan sääntelyn soveltamisalaa merkittävästi ja se kattaa aiempaa enemmän toimialoja ja organisaatioita. Direktiivi kehystää tietoturvallisuuden riskienhallinnan kokonaisuutena, jossa toimitusketjun tietoturvallisuus on yksi tärkeistä osa-alueista. Direktiivin artikla 21 vaatimus liittyy toimitusketjun tietoturvallisuustoimenpiteisiin, ja siinä tietoturvallisuusasioiden merkittävyyttä osana toimittajasuhteiden hallintaa. Direktiivi käytännössä muuttaa toimitusketjun tietoturvalli-

suusasioiden "hyvän hoitamisen" osaksi lakisääteistä riskienhallintaa ja valvottavaa johtamisvastuuta. Samalla se nostaa hankinnan ja toimittajahallinnan tietoturvallisuusasiat kriittiseksi osaksi kokonaisvaltaista tietoturvallisuuden hallintaa, jossa toimittajien arviointikriteerit ja toimitusketjun elinkaaren hallinta muuttuvat kriittisiksi prosesseiksi.

4.2.2 Cyber Resilience Act (CRA) eli Kyberkestävyyssäädös

Toinen merkittävä Euroopan unionin sääntelykokonaisuus on Cyber Resilience Act (CRA), eli Kyberkestävyyssäädös, joka kohdistuu digitaalisia elementtejä sisältäviin tuotteisiin, ja painottaa tietoturvallisuutta tuotteen koko elinkaaren ajan (“secure by design”, päivitykset, haavoittuvuuksien käsittely). CRA:n avulla pyritään varmistamaan tuotteiden suunnittelu, ylläpito ja päivitykset niin, että tuotteet on suojattu kyberuhkia vastaan. Vaikka CRA:n painopiste on tuoteturvallisuudessa, sen vaikutus toimitusketjuihin on merkittävä: jos yritys tuo markkinoille digitaalisen tuotteen, sen on hallittava myös tuotteeseen integroitujen komponenttien ja ohjelmistoriippuvuuksien turvallisuutta. Käytännön keskustelussa yksi keskeinen mekanismi on läpinäkyvyyden lisääminen (esim. SBOM-ajattelu), jotta organisaatiot voivat ymmärtää, mitä komponentteja tuote sisältää ja miten haavoittuvuuksiin reagoidaan koko ketjussa ja tuotteen koko elinkaaren ajan. Ilman tehokasta toimitusketjun hallintaa tämä on mahdotonta.

4.3 Yhdysvallat

Yhdysvalloissa tietoturvallisuuteen liittyvä regulaatio rakentuu liittovaltion ohjeistusten kautta ja mm. Presidentillisiin käskyihin. Tämän lisäksi tietynlaisten tietojen käsittely johtaa tiettyjen regulatiivisiin vaatimuksiin. Viime vuosina on nähty muutamia merkittäviä toimitusketjun tietoturvallisuuteen liittyviä vaatimuksia. "Executive Order 14028 (Improving the Nation’s Cybersecurity)" vuodelta 2021 sisältää merkittäviä vaatimuksia toimitusketjun turvallisuuden vahvistamiseen. NISTin koonti EO 14028:n toimeenpanosta (NIST, 2021) korostaa toimitusketjun tietoturvallisuusaspektien parantamista, ja NIST on julkaissut ohjeistuksia mm. kriittisen ohjelmiston turvallisuusmittareista ja toimittajien testauskäytännöistä. EO 14028:n viitekehykseen liittyy myös SBOM-käsite (Software Bill of Materials), joka on oleellisessa osassa myös EU:n CRA-regulaatiossa. SBOM:n ajatuksena on tehdä näkyväksi kaikki osat ja näihin liittyvät toimittajat, joista yrityksen kehittämät sovellukset rakentuvat.

Vuonna 2025 voimaan astunut CMMC 2.0-vaatimuskehikko koskettaa Yhdysvaltojen puolustusvoimille palveluita toimittavia ja näihin liittyviä tietoja käsitteleviä yrityksiä ja asettaa NIST SP 800-171-viitekehykseen pohjautuvia vaatimuksia yrityksen tietoturvallisuuden ja toimitusketjun hallinnalle.

4.4 Muut maat

Myös monissa muissa maissa, kuten Yhdistyneissä Kansakunnissa, Australiassa, Japanissa ja Kiinassa tietoturvallisuuteen liittyvä regulaatio on kehittynyt ja sisältää erinäisiä vaatimuksia yritysten toimitusketjun tietoturvallisuuden hallintaan. Mielenkiintoisena lisänä voidaan mainita tiettyjen maiden viime aikojen linjaukset, jotka ovat liittyneet tietyn maalaisten toimittajien ja palveluiden käyttämiseen. Kiinan viranomaiset linjasivat vuonna 2026, että Kiinassa toimivat yritykset eivät saa toiminnassaan käyttää Yhdysvaltalaisia tai Israelilaisia tietoturvatuotteita (Reuters, 2026). Menneiltä vuosilta on myös nähty merkittäviä kiistoja liittyen Kiinalaisten toimittajien käyttöön Yhdysvalloissa ja sen kautta myös erinäisten kumppanimaiden toimesta. Virallisten regulaatioiden ja viitekehysten lisäksi yritysten on seurattava ja ennakoitava geopoliittisten tilanteiden kehittymistä. Tätä kautta eskaloituvat toimitusketjuun liittyvät riskit voivat olla todella hankalia ennakoida ja varautua.

Kaiken kaikkiaan lisääntynyt ja lisääntyvä regulaatio tarkoittaa yrityksen näkökulmasta sitä, että toimitusketjun tietoturvallisuutta ei voi käsitellä erillisenä tai omana prosessinaan vaan se vaatii strategista ja operatiivista integraatiota: hankintastrategiaan, toimittajaohjaukseen, tuotekehityksen elinkaareen, haavoittuvuuksien hallintaan ja tietoturvapoikkeamien johtamiseen. Toimitusketjun tietoturvasta on tullut osa organisaation kykyä osoittaa sekä resilienssiä että vaatimustenmukaisuutta globaalissa ja pirstaloituvassa regulaatiokentässä.

5 Viitekehykset ja standardit

Tietoturvallisuuden hallinta toimitusketjuissa on noussut nykyisin myös keskeinen teema erinäisissä kansainvälisissä tietoturvallisuusstandardeissa ja -viitekehyksissä. Pilvipalvelut, ohjelmistokomponentit, ulkoistetut IT-palvelut sekä globaalit alihankintaketjut ovat muuttaneet tapaa, jolla tietoa käsitellään ja järjestelmiä ylläpidetään. Tietoturvallisuuden näkökulmasta tämä tarkoittaa, että merkittävä osa organisaation riskipinnasta sijaitsee sen omien rajojen ulkopuolella ja tämä heijastuu myös standardointiin.

Kansainväliset tietoturvallisuusstandardit ovat pyrkineet vastaamaan muutokseen tuomalla toimitusketjun merkittäväksi osaksi organisaation kokonaisvaltaista tietoturvallisuuden hallintaa. Sen sijaan että tietoturvallisuus nähtäisiin vain organisaation sisäisenä kontrollikokonaisuutena, standardit korostavat tarvetta hallita myös toimittajiin, palveluntarjoajiin ja muihin kumppaneihin liittyviä riskejä.

5.1 ISO/IEC 27001 ja ISO/IEC 27002

Yksi keskeisimmistä tietoturvallisuuden hallinnan standardeista on ISO/IEC 27001, joka määrittelee vaatimukset organisaation tietoturvallisuuden hallintajärjestelmälle (Information Security Management System, ISMS). Standardin lähtökohtana on riskiperusteinen lähestymistapa, jossa organisaatio tunnistaa tietoturvallisuuteen liittyvät riskit ja toteuttaa niihin suhteutettuja hallintatoimenpiteitä. Toimitusketjun näkökulmasta ISO/IEC 27001 tarkastelee toimittajien irrallisina alueina, mutta toimittajiin liittyvät kontrollit on hyvä implementoida osana organisaation kokonaisriskienhallintaa.

ISO/IEC 27001-standardin kontrollikokonaisuus on tarkemmin kuvattu ISO/IEC 27002 -standardissa, joka sisältää käytännön ohjeita tietoturvallisuuden hallinnan toteuttamiseen. ISO/IEC 27002:ssa toimitusketjuun liittyvä tietoturvallisuus on käsitelty erityisesti "supplier relationships"-kontrollien

kautta. Näiden kontrollien tavoitteena on varmistaa, että organisaation ja toimittajien väliset suhteet eivät heikennä organisaation muuta tietoturvallisuutta ja että toimittajiin liittyvät riskit tunnistetaan sekä hallitaan systemaattisesti.

ISO/IEC 27002 korostaa erityisesti kolmea keskeistä näkökulmaa toimitusketjun hallinnassa. Ensimmäinen on tietoturvallisuusvaatimusten sisällyttäminen toimittajasopimuksiin. Organisaation tulee varmistaa, että toimittajat sitoutuvat tietoturvallisuutta koskeviin velvoitteisiin, jotka ovat linjassa organisaation omien tietoturvallisuusvaatimusten kanssa. Tämä voi tarkoittaa esimerkiksi vaatimuksia pääsynhallinnasta, tietojen suojaamisesta, poikkeamien ilmoittamisesta tai auditointioikeuksista.

Toinen keskeinen näkökulma on toimittajiin liittyvien tietoturvallisuusriskien hallinta. Standardi korostaa, että toimittajiin liittyviä tietoturvallisuusriskejä tulisi arvioida suhteessa toimittajan rooliin ja palvelun kriittisyyteen. Esimerkiksi toimittaja, jolla on pääsy organisaation tietojärjestelmiin tai joka käsittelee luottamuksellista tietoa, edellyttää laajempaa tietoturvallisuuden hallintaa kuin toimittaja, joka toimittaa pelkästään fyysisiä tuotteita.

Kolmas keskeinen teema on toimittajasuhteiden jatkuva hallinta. ISO/IEC 27002 korostaa, että toimittajien tietoturvallisuutta ei tule arvioida pelkästään sopimuksen alussa, vaan organisaation tulisi seurata toimittajien toimintaa koko sopimussuhteen ajan. Tämä voi sisältää esimerkiksi säännöllisiä arviointeja, auditointeja tai turvallisuusraportointia.

Standardi määrittelee myös kontrollialueen 5.21 kautta yksityiskohtaisempia vaatimuksia liittyen IT-palveluiden ja kontrollialueen 5.23 kautta pilvipalveluiden tietoturvallisuuskontrolleihin. IT-palvelut ja eritysesti nykyisin hyvin laajasti käytetyt pilvipalvelut ovat monissa yrityksissä kriittisessä roolissa jatkuvuuden sekä tiedon suojaamisessa, ja tämän vuoksi myös standardi suosittelee kiinnittämään näihin erityistä huomiota.

5.2 NIST Cybersecurity Framework ja NIST SP 800-161

Yhdysvalloissa käytössä oleva keskeinen tietoturvallisuuden viitekehys on NIST Cybersecurity Framework (CSF), jota käytetään laajasti sekä julkisella että yksityisellä sektorilla. NIST CSF jäsentää tietoturvallisuuden hallinnan

viiteen päätoimintoon: Identify, Protect, Detect, Respond ja Recover. Toimitusketjuun liittyvät tietoturvallisuusriskit sijoittuvat erityisesti Identify- ja Protect -toimintojen alle.

NIST CSF:ssä toimitusketjuun liittyvä tietoturvallisuus on käsitelty Supply Chain Risk Management (SCRM) -teeman kautta. Viitekehys korostaa, että organisaatioiden tulee tunnistaa toimitusketjuun liittyvät riippuvuudet, arvioida niihin liittyvät riskit ja toteuttaa hallintatoimenpiteitä näiden riskien vähentämiseksi.

NIST on julkaissut toimitusketjun tietoturvallisuudesta myös erillisen standardin, NIST SP 800-161, joka käsittelee nimenomaan IT-toimitusketjun riskienhallintaa. Standardi korostaa erityisesti sitä, että tietoturvallisuusriskit voivat syntyä toimitusketjun kaikissa vaiheissa: suunnittelussa, kehityksessä, tuotannossa, toimituksessa sekä ylläpidossa. Tämä näkökulma laajentaa toimitusketjun tarkastelua pelkistä toimittajasopimuksista kohti laajempaa kokonaisuuden hallintaa toimittajien tietoturvallisuuden hallinnassa.

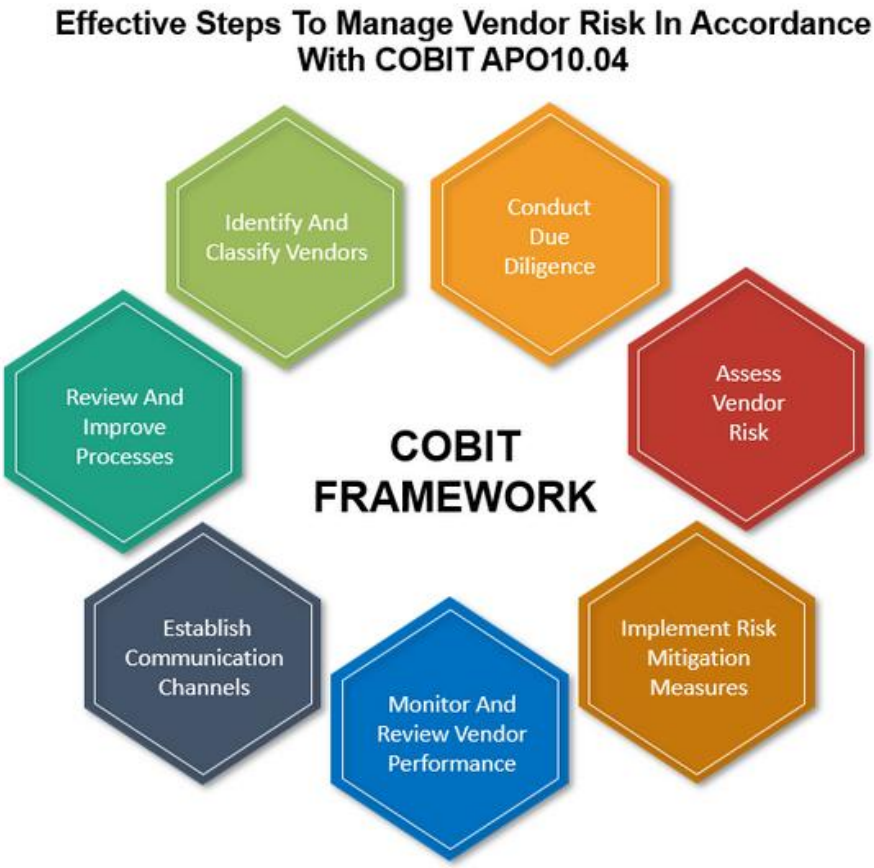
NIST:n lähestymistavassa keskeinen ajatus on, että toimitusketjuun liittyvät tietoturvallisuusriskit voivat liittyä esimerkiksi ohjelmistokomponentteihin, laitteistoihin, alihankkijoihin tai logistiikkaketjuihin. Tämän vuoksi organisaatioiden tulisi rakentaa prosesseja, jotka mahdollistavat toimitusketjun läpinäkyvyyden sekä komponenttien alkuperän ja luotettavuuden arvioinnin.

5.3 COBIT ja IT-hallintamallit

IT-hallinnan viitekehyksissä toimitusketjuun liittyvät tietoturvallisuusasiat käsitellään usein osana laajempaa palvelu- ja toimittajahallintaa. Yksi keskeinen viitekehys tässä kontekstissa on COBIT, joka keskittyy IT-hallinnan ja -ohjauksen periaatteisiin.

COBIT-viitekehys korostaa erityisesti toimittajahallinnan (vendor management) merkitystä osana IT-hallintaa. Viitekehys sisältää prosesseja, joiden avulla organisaatiot voivat arvioida toimittajien kyvykkyyttä, määrittää palvelutasot sekä valvoa sopimusten toteutumista. Tietoturvallisuuden näkökulmasta COBIT korostaa, että toimittajille asetettujen vaatimusten tulee olla linjassa organisaation oman tietoturvallisuuden hallintamallin kanssa.

COBIT:n näkökulma toimitusketjuun on erityisen kiinnostava siksi, että se tarkastelee tietoturvallisuutta osana laajempaa hallintamallia. Sen mukaan toimittajien tietoturvallisuuden hallinta ei ole pelkästään tietoturvaorganisaation vastuulla, vaan siihen osallistuvat myös hankinta, riskienhallinta ja liiketoimintajohto.



Kuva 1: COBIT-viitekehyksen toimittajariskien hallinnan vaiheet

5.4 ISO/IEC 28000 ja toimitusketjun turvallisuuden hallinta

Siinä missä ISO/IEC 27000 -sarja keskittyy erityisesti tietoturvallisuuden hallintaan, toimitusketjun turvallisuutta tarkastellaan myös muissa standardeissa. Yksi esimerkki tästä on ISO/IEC 28000, joka käsittelee toimitusketjun turvallisuuden hallintaa. Standardi keskittyy erityisesti logistiikkaan, mutta sen periaatteita voidaan soveltaa myös tietoturvallisuuteen.

ISO/IEC 28000-sarjan standardit korostavat toimitusketjun kokonaisvaltaista riskienhallintaa ja organisaatioiden välistä yhteistyötä turvallisuuskysymyksissä. Standardin keskeinen ajatus on, että toimitusketjun turvallisuus muo-

dostuu useiden eri toimijoiden yhteistoiminnasta. Tämä ajattelutapa on sovellettavissa myös tietoturvallisuuteen: yksittäisen organisaation turvallisuustoimenpiteet eivät riitä, jos muut toimitusketjun toimijat eivät noudata vastaavia käytäntöjä.

5.5 Standardien yhteiset periaatteet

Vaikka eri viitekehykset lähestyvät toimitusketjun tietoturvallisuutta hieman eri näkökulmista, niissä on tunnistettavissa useita yhteisiä periaatteita.

Ensimmäinen yhteinen periaate on riskiperusteinen lähestymistapa. Standardit korostavat, että toimittajiin liittyviä tietoturvallisuusriskejä tulee arvioida suhteessa toimittajan rooliin ja palvelun kriittisyyteen. Tämä mahdollistaa resurssien kohdentamisen niihin toimittajiin, joiden kautta syntyy merkittävimpiä riskejä.

Toinen yhteinen periaate on sopimuksellinen ohjaus. Standardit korostavat, että tietoturvallisuusvaatimukset tulee sisällyttää toimittajasopimuksiin ja että toimittajien tulee sitoutua organisaation tietoturvallisuusvaatimuksiin.

Kolmas periaate on jatkuva hallinta koko toimittajanhallinnan elinkaaren ajan. Toimitusketjun tietoturvallisuutta ei tulisi tarkastella kertaluonteisena arviointina, vaan jatkuvana prosessina, joka kattaa koko toimittajasuhteen elinkaaren.

Neljäs periaate on läpinäkyvyys ja yhteistyö. Standardit korostavat, että toimitusketjun tietoturvallisuus edellyttää tiedon jakamista ja yhteistyötä organisaatioiden välillä.

Vaikka toimitusketjun hallinta on aina korostunut erinäisissä viitekehyksissä ja standardeissa, nämä ovat laajentuneet näkökulmaa organisaation sisäisestä tietoturvallisuudesta kohti laajempaa toimitusketjun hallintaa. Tämä kehitys heijastaa toimintaympäristön muutosta, jossa organisaatiot ovat yhä riippuvaisempia ulkoisista palveluntarjoajista ja teknologiakumppaneista.

6 Toimitusketjuun liittyvien riskien hallinnan haasteet

6.1 Yritysten osto-organisaatiot ja toimittajien hallintaan liittyvät haasteet

Suurimmassa osassa globaaleja yrityksiä toimittajien hallintaan liittyvät vastuut ovat hajautuneet useiden eri organisaatioiden välille, vaikka osto-organisaatio toimii usein keskitettynä koordinoivana ja asetuksia määrittelevänä tahona. Osto-organisaatio asettaa perusvaatimukset toimittajien valinnalle, sopimiselle ja hallinnalle, mutta käytännössä toimittajasuhteiden toteutus ja niihin liittyvä riskienhallinta jakautuvat liiketoiminnan, tietoturvallisuuden, lakitoiminnon ja usein myös IT-organisaation kesken. Tämä johtaa tilanteeseen, jossa toimittajahallinta ei ole yhden funktion hallittavissa oleva kokonaisuus, vaan vaatii jatkuvaa yhteensovittamista eri tavoitteiden ja näkökulmien välillä.

Merkittävin haaste hajautukseen liittyen on se, että myös toimittajariskin hallinta hajaantuu. Yksittäisen toimittajan kokonaisriskin ymmärtäminen on vaikeaa, kun tieto ja vastuu jakautuvat useisiin paikkoihin. Samalla syntyy helposti päällekkäisiä, usein raskaita arviointiprosesseja tai toisaalta puutteita, kun kokonaisvaltaista hallintaa tai omistajuutta ei ole määritelty. Tämä korostuu erityisesti suurissa organisaatioissa, joissa toimittajamäärät ovat suuria ja toimintamallit vaihtelevat yksiköittäin.

Toinen keskeinen jännite syntyy kaupallisten tavoitteiden ja tietoturvallisuuden välillä. Osto-organisaatio pyrkii usein optimoimaan kustannuksia ja varmistamaan liiketoiminnan tarpeet, kun taas tietoturvallisuus pyrkii varmistamaan, että toimittajiin liittyvät riskit pysyvät hallinnassa. Toisaalta osto-organisaation vaatimukset saattavat olla hyvin raskaita, mutta ei-käytännönläheisiä, jolloin vaatimuksia toteuttavat organisaation osat ja ihmiset eivät ymmärrä näiden roolia ja merkitystä. Yleisin haaste tietoturvallisuusasioiden lä-

pikäymiseen osana hankintaprosessit tulee siitä, kun liiketoiminnalle kriittinen toimittaja ei täytä kaikkia tietoturvallisuusvaatimuksia. Kypsissä organisaatioissa tämän tilanteen ei pitäisi aiheuttaa merkittäviä haasteita, vaan tilanne ratkaistaan tietoisella päätöksenteolla, jossa riskit tehdään näkyviksi ja niitä punnitaan suhteessa liiketoimintahyötyihin.

Toimittajamäärien kasvu tuo mukanaan skaalautuvuuden haasteen. Kaikkia toimittajia ei voida hallita samalla tarkkuudella, eikä pelkkä sopimuksen arvo kerro toimittajan riskitasosta. Pieni tekninen komponentti voi muodostaa merkittävän tietoturvallisuusriskin, kun taas suuri toimittaja voi olla riskiltään rajattu. Tämä edellyttää siirtymistä kohti riskiperusteista ajattelua, jossa toimittajia tarkastellaan näiden aiheuttamien todellisen vaikutuksen kautta.

6.2 Toimitusketjujen monimutkaisuus ja näkyvyyden puute

Yksi toimitusketjuun liittyvien riskien hallinnan keskeisimmistä haasteista on toimitusketjujen rakenteellinen monimutkaisuus sekä siitä seuraava näkyvyyden puute. Vaikka organisaatio voi hallita omia sisäisiä prosessejaan verrattain hyvin ja asettaa toimittajilleen vaatimuksia, sen mahdollisuudet muodostaa kattava kuva toimittajaverkostonsa kokonaisuudesta ovat usein rajalliset. Tämä johtuu siitä, että moderni toimitusketju ei ole lineaarinen ketju, vaan moniulotteinen verkosto, jossa organisaation toimittajat käyttävät omia alihankkijoitaan, teknologiakumppaneitaan, pilvipalveluitaan ja ohjelmistokomponenttejaan. Tällaisessa rakenteessa riskit eivät synny ainoastaan suorissa toimittajasuhteissa, vaan myös näiden taustalla olevissa riippuvuuksissa, joihin organisaatiolla ei yleensä ole suoraa näkyvyyttä tai vaikutusmahdollisuutta.

Tietoturvallisuuden näkökulmasta tämä on erityisen merkittävä ongelma, koska digitaalinen toimitusketju on usein huomattavasti vaikeammin hahmotettava kuin fyysinen toimitusketju. Fyysisten tuotteiden ja materiaalivirtojen osalta organisaatiolla on usein suhteellisen hyvä käsitys siitä, mistä toimitukset tulevat ja millaisia vaihtoehtoja niille on. Digitaalisissa palveluissa, ohjelmistoissa ja ulkoistetuissa teknologiaratkaisuissa toimitusketju voi sen sijaan muodostua useista abstrakteista kerroksista. Organisaatio voi ostaa palvelun yhdeltä toimittajalta, joka hyödyntää sen tuottamiseen toista pilvipalvelutoimittajaa, kolmatta ohjelmistokomponenttien toimittajaa ja neljättä ulkoistettua tukipalvelua. Lopputuloksena organisaatio on riippuvainen useista toimijoista, vaikka se tunnistaa suoraksi sopimuskumppanikseen vain yhden.

Näkyvyyden puute aiheuttaa useita ongelmia. Ensinnäkin organisaatio ei välttämättä tiedä, missä sen dataa todellisuudessa käsitellään, millaisissa ympäristöissä sitä säilytetään tai keillä siihen on pääsy. Toiseksi organisaatio ei aina kykene tunnistamaan, milloin useat näennäisesti erilliset palvelut perustuvat samaan taustalla olevaan teknologiaan tai palveluntarjoajaan. Tällainen riippuvuuksien keskittyminen voi synnyttää riskejä, joissa toimittajan häiriö vaikuttaa samanaikaisesti useisiin liiketoiminnan kannalta kriittisiin palveluihin. Kolmanneksi näkyvyyden puute vaikeuttaa poikkeamatilanteiden hallintaa: jos organisaatio ei tiedä, mitä toimittajia ja alihankkijoita tiettyyn palveluun liittyy, myöskään vaikutusten arviointi ja korjaavien toimenpiteiden kohdentaminen eivät välttämättä onnistu nopeasti.

Toimitusketjun monimutkaisuus liittyy myös siihen, että riskit eivät ole pysyviä vaan muuttuvat ajan myötä. Toimittaja voi vaihtaa pilviympäristöä, ottaa käyttöön uuden alihankkijan, siirtää kehitystyötä toiseen maahan tai integroida palveluunsa uusia komponentteja ilman, että organisaation oma käsitys toimittajan aiheuttamasta riskistä muuttuu.

Monimutkaisuuden ja näkyvyyden puutteen ongelma korostuu erityisesti silloin, kun organisaatio pyrkii rakentamaan yhtenäistä hallintamallia globaalissa ympäristössä. Eri liiketoimintayksiköt voivat käyttää samoja toimittajia eri tarkoituksiin, hankkia paikallisesti omia palveluitaan tai tehdä teknologisia ratkaisuja ilman keskitettyä näkyvyyttä. Tällöin toimittajahallinta ei ole vain ulospäin suuntautuvaa toimitusketjun hallintaa, vaan myös sisäisen läpinäkyvyyden rakentamista. Organisaation on kyettävä ymmärtämään, mitä sen omissa yksiköissä ostetaan, miten niitä palveluja käytetään ja millaisia riippuvuuksia niistä syntyy.

Tämän vuoksi toimitusketjun monimutkaisuus ei ole pelkästään operatiivinen haaste, vaan myös johtamishaaste. Se pakottaa organisaation tunnistamaan, että kaikki riskit eivät ole näkyviä, kaikki riippuvuudet eivät ole suoraviivaisia eikä kaikkia ongelmia voida ratkaista lisäämällä yksittäisiä kontrollivaatimuksia. Olennaisempaa on rakentaa toimintamalli, jossa riskejä hallitaan riittävällä tasolla ja oikeiden tahojen toimesta.

6.3 Riskiperusteisuuden puute käytännössä

Toimitusketjuun liittyvä riskienhallinta kuvataan lähes poikkeuksetta riskiperusteiseksi, mutta käytännössä tämä periaate ei yleensä toteudu. Monissa organisaatioissa toimittajahallinnan prosessit rakentuvat yhdenmukaisiksi tarkistuslistoiksi, kyselyiksi ja hyväksyntävaiheiksi, joita sovelletaan laajasti ilman toimittajien erottelua todellisen riskitason perusteella. Tämä saattaa usein myös johtaa tilanteeseen, jossa merkittävää riskiä aiheuttavat toimittajat hyväksytään joidenkin prosessien ohi liiketoiminnan vaatimusten mukaan ja toisaalta pienet toimittajat pakotetaan liian raskaisiin hyväksyntäprosesseihin, jotka eivät korreloi näiden aiheuttaman riskin kanssa. Organisaatio voi käyttää merkittävästi aikaa ja resursseja hallinnollisten prosessien pyörittämiseen, vaikka varsinainen turvallisuushyöty jää rajalliseksi. Lopputuloksena syntyy illuusio hallinnasta: toimittajia on kyllä arvioitu, kyselyitä on lähetetty ja dokumentteja on kerätty, mutta riskien todellinen priorisointi ei ole toteutunut.

Riskiperusteisuuden puute johtuu usein osittain prosessien standardoinnin tarpeesta. Suurissa organisaatioissa halutaan ymmärrettävästi rakentaa yhdenmukaisia malleja, jotka ovat helposti toistettavia ja auditoitavia. Samalla kuitenkin menetetään herkkyyttä palvelun kontekstille. Toimittajan riski ei määräydy vain sen koon, sopimuksen arvon tai toimialan perusteella, vaan sen mukaan, mitä palvelulla tehdään, mihin se kytkeytyy ja millaista tietoa se käsittelee. Jos nämä erot jäävät huomioimatta, riskiperusteinen hallinta muuttuu muodolliseksi prosessiksi, joka kohtelee erilaisia toimittajia samalla tavalla.

Toinen merkittävä haaste liittyy siihen, että riskiperusteisuus ymmärretään liian kapeasti alkuvaiheen luokitteluna. Toimittaja saatetaan sijoittaa johonkin riskiluokkaan sopimuksen allekirjoittamisen yhteydessä, mutta luokittelu ei elä toimittajasuhteen mukana. Tällöin menetetään riskiperusteisen ajattelun tärkein ominaisuus: kyky kohdistaa huomiota sinne, missä riskit kulloinkin ovat suurimmat. Käytännössä toimittajan merkitys voi muuttua nopeasti, ja jos hallintamalli ei kykene reagoimaan tähän, alkuperäinen luokittelu menettää arvonsa.

Aidosti riskiperusteinen toimittajahallinta edellyttää kykyä hyväksyä myös se, että kaikkia toimittajia ei käsitellä samalla tavalla. Tämä voi tuntua hallinnollisesti epätasaiselta, mutta on käytännössä välttämätöntä. Ilman eriyttämistä organisaatio kuormittaa itseään turhilla prosesseilla ja samalla heikentää kykyään keskittyä toimittajiin, joilla on aidosti suuri vaikutus tietoturvallisuuteen ja liiketoiminnan jatkuvuuteen.

6.4 Toimittajien kyvykkyyksien ja vaatimusten epätasapaino

Yksi käytännön toimittajahallinnan haasteellisimmista kysymyksistä liittyy siihen, että organisaation turvallisuusvaatimukset ja toimittajien kyvykkyydet eivät aina kohtaa. Vaikka asiakasorganisaatio pyrkisi rakentamaan johdonmukaisen ja standardeihin perustuvan vaatimuskokonaisuuden, kaikki toimittajat eivät kykene vastaamaan siihen samalla tavalla. Erot voivat liittyä toimittajan kokoon, toimialaan, markkina-asemaan, teknologiseen kypsyyteen tai siihen, millaisia resursseja toimittajalla on käytettävissään tietoturvallisuuden hallintaan.

Tämä epätasapaino näkyy erityisen selvästi silloin, kun sama organisaatio käyttää hyvin erilaisia toimittajia. Toisessa päässä voivat olla suuret kansainväliset teknologiayhtiöt, joilla on sertifioituja hallintamalleja, auditointiraportteja ja kattavat tietoturvallisuusorganisaatiot. Toisessa päässä voivat olla pienet erikoistuneet toimijat, joiden palvelu voi olla liiketoiminnalle erittäin arvokas, mutta joiden kyky tuottaa laajaa dokumentaatiota, täyttää raskaita sopimusvaatimuksia tai osallistua monivaiheisiin arviointiprosesseihin on rajallinen. Jos kaikkia toimittajia lähestytään samalla tavalla, seurauksena voi olla merkittävä hallinnollinen kuormitus, joka hidastaa liiketoimintaa, tai tilanne, jossa kriittisiä, pienempiä toimittajia ei käytännössä pystytä ottamaan käyttöön lainkaan.

Ongelma ei kuitenkaan ole vain toimittajien heikommissa kyvykkyyksissä. Epätasapaino voi syntyä myös toiseen suuntaan. Suuret toimittajat, erityisesti globaalit pilvi- ja ohjelmistopalvelujen tarjoajat, eivät aina ole halukkaita mukautumaan yksittäisen asiakkaan yksityiskohtaisiin vaatimuksiin. Näiden palvelumallit perustuvat usein standardointiin ja oman aseman tietynlaiseen väärinkäyttöön omien käytäntöjen jalkauttamisessa. Tällöin organisaation haasteet liittyvät siihen, että toimittajalla on korkeat tietoturvallisuuskyvykkyydet, mutta organisaatiolla ei ole käytännössä mahdollisuutta vaatia tai varmistaa omien vaatimusten toteutumista.

Näissä tilanteissa organisaatio joutuu usein tekemään vaikeita päätöksiä. Jos turvallisuusvaatimuksia kevennetään liikaa toimittajan kyvykkyyksien mukaan, vaarana on, että organisaatio hyväksyy toimittajasuhteita, joiden riskit ylittävät sen oman hyväksyttävän tason. Jos taas vaatimuksista pidetään jäykästi kiinni kaikissa tilanteissa, seurauksena voi olla liiketoiminnan kannalta tärkeiden hankintojen estyminen, toimittajaehdokkaiden kaventuminen tai kustannusten merkittävä nousu. Toisin sanoen toimittajahallinta ei ole vain vaatimusten asettamista, vaan jatkuvaa tasapainoilua turvallisuuden, toteutettavuuden ja liiketoiminnan tavoitteiden välillä.

Tämä epätasapaino tuo näkyväksi myös yhden toimittajahallinnan syvällisemmän ongelman. Turvallisuusvaatimukset rakentuvat usein yrityksen omasta näkökulmasta ja tarpeista, jolloin toimittaja ja ostava organisaatio saattavat ajaa erilaisia etuja ja tarpeita. Asiakas voi pitää jotakin tietoturvallisuuskontrollia itsestään selvänä, mutta toimittajalle se voi olla vieras, kallis tai käytännössä vaikeasti toteutettava. Tämä voi aiheutua erityisesti tilanteessa, jossa organisaatio toimii regulaation alaisuudessa, joka ei kosketa toimittajaa.

Näistä syistä johtuen kypsä toimittajahallinta ei voi perustua pelkästään ajatukseen, että vaatimukset joko täyttyvät tai eivät täyty. Tarvitaan kykyä erottaa toisistaan ne vaatimukset, jotka ovat ehdottomia, ja ne, joissa voidaan hyväksyä vaihtoehtoisia toteutustapoja tai kompensoivia kontrollimekanismeja. Esimerkiksi pieneltä toimittajalta ei välttämättä voida edellyttää laajaa sertifiointikehystä, mutta siltä voidaan silti vaatia selkeitä pääsynhallinnan kontrolleja, perustason lokitusta tai poikkeamien ilmoitusvelvollisuutta. Vastaavasti suuren toimittajan standardisopimuksia ei ehkä voida muuttaa merkittävästi, mutta riskiä voidaan hallita muilla tavoin, kuten arkkitehtuurin rajaamisella, datan minimoinnilla tai lisävalvonnalla asiakkaan omassa ympäristössä.

Tästä näkökulmasta toimittajien kyvykkyyksien ja vaatimusten epätasapaino ei ole pelkästään haaste, vaan myös testi organisaation omalle kypsyydelle. Se paljastaa, kykeneekö organisaatio soveltamaan periaatteitaan käytäntöön vai nojaako se jäykkiin malleihin, jotka toimivat vain ideaalitilanteessa. Organisaatio, joka ymmärtää tämän epätasapainot, voi rakentaa modulaarisen ja riskiperusteisen toimittajien hallinnan mallin, jossa vaatimusten taso, näiden

varmistaminen ja sopimuksellinen sopiminen valitaan toimittajan ja palvelun todellisen riskin ja liiketoiminnan tarpeiden perusteella.

Tämä on myös yksi alue, jossa tietoturvallisuusorganisaation rooli muuttuu olennaisesti. Sen tehtävä ei ole vain määritellä kontrollit, vaan auttaa liiketoimintaa ja hankintaorganisaatiota löytämään ratkaisuja tilanteissa, joissa täydellinen vaatimustenmukaisuus ei ole realistista. Mikään yritys ei toimi tyhjiössä tai täydellisessä maailmassa, jossa toimittajien käytännöt ovat hyvin kehittyneitä, erittäin läpinäkyviä ja toimittajat ovat valmiita mukautumaan asiakkaan tarpeisiin. Yritykset toimivat markkinassa, jossa tarjolla olevat vaihtoehdot ovat epätäydellisiä ja jossa myös turvallisuusasiat on mietittävä tämän epätäydellisyyden ehdoilla.

7 Toimitusketjuun liittyvien tietoturvariskien tehokas hallinta

7.1 Toimittajien kategorisointi

Lähes kaikki modernit suuryritykset käyttävät toimitusketjussaan tänä päivänä toimittajia ja useimmissa näiden rooli on hyvin merkittävä yhdessä tai useammassa osassa yrityksen toimintaa. Toimittajien rooli ja määrä vaihtelee merkittävästi yrityksen toimialan ja sisäisistä toimintamalleista riippuen, mutta on selvää, että toimittajariskit ovat lisääntyneet merkittävästi samaan aikaan kun näiden merkittävyyttä liiketoiminnalle ja jatkuvuudelle ei ehkä vielä ymmärretä riittävästi. Kaikkia toimittajia ei kannata tai voi hallita samoilla tavoilla ja yrityksen toimintamalleista tai organisoinnista riippuen yrityksellä ei välttämättä ole edes nimettyä henkilöä vastaamaan toimitusketjun tietoturvariskeistä tai niiden hallinnasta. Tämän vuoksi tarvitaan priorisointia, jotta voimavarat voidaan keskittää kaikista merkittävimpiin riskeihin ja toimittajiin. Oikeaoppisella mallilla hallintaa voidaan myös tehokkaasti skaalata riippuen käytössä olevista resursseista toimittajahallintaan liittyen. Tässä osiossa kerron kokemukseeni peilaten parhaita käytäntöjä mitä yrityksessä voidaan ajatella soveltavan.

Tehokkaan toimitusketjuun liittyen riskienhallinnan mallin luomiseksi on tärkeää tunnistaa yrityksen käyttämät toimittajat, näiden merkityksellisyys liiketoiminnalle ja näihin liittyvät riskit tietoturvallisuuden näkökulmasta. Riippuen yrityksen toimialasta toimittajat kannattaa jakaa muutamaan eri kategoriaan hallinnan ja vaatimusten määrittelyn helpottamiseksi. Eri kategorioita voivat olla:

- Tietotekniikka (IT)
- Sovelluskehitys
- Automaatio (OT)
- Konsultit
- Fyysiset tuotteet

Edellä mainitun kategorisoinnin lisäksi toimittajat pitää pystyä priorisoimaan, johon tarvitaan määrittelyjä pohjautuen esimerkiksi toimittajan liiketoiminta-kriittisyyteen tai käsiteltävään tietoon. Tähän liittyviä kriteereitä voivat olla esimerkiksi:

- Toimittajalta ostettujen palveluiden arvo
- Toimittajan palveluiden liiketoimintakriittisyys
- Toimittajan käsittelemän tiedon kriittisyys yritykselle

Nämä kaksi yhdistämällä päästään seuraavaan vaiheeseen, jossa pystytään profiloimaan toimittajia riskiluokkiin ja käynnistämään näiden pohjalta toimenpiteitä ja prosesseja.

7.2 Toimittajien riskiprofilointi

Toimittajien kategorisointi muodostaa perustan toimitusketjun tietoturvallisuusriskien hallinnalle, mutta pelkkä kategorisointi ei vielä mahdollista riskien tehokasta priorisointia. Tämän vuoksi seuraavassa vaiheessa toimittajat profiloidaan näiden aiheuttaman tietoturvallisuusriskin näkökulmasta. Riskiprofiloinnin tavoitteena on tunnistaa ne toimittajat, joiden kautta organisaatio altistuu merkittävimmille tietoturvauhkille, sekä kohdentaa hallintatoimenpiteet suhteessa riskin tasoon.

Riskiprofilointi kannattaa perustaa useiden eri tekijöiden yhdistelmään. Yksi keskeinen tekijä on toimittajan liiketoimintakriittisyys, joka kuvaa sitä, kuinka merkittävää toimittajan palvelu tai tuote on organisaation operatiiviselle toiminnalle. Mitä suuremman vaikutuksen toimittajan toimittaman palvelun häiriö aiheuttaa organisaation toiminnalle, sitä kriittisempi toimittaja on kyseessä. Liiketoimintakriittisyyden arvioinnissa voidaan käyttää organisaation itsensä määrittelemiä toipumisaika- (RTO) ja toipumispistevaatimuksia (RPO). Toinen merkittävä kriteeri on tiedon kriittisyys, joka liittyy siihen, millaista tietoa toimittaja käsittelee tai mihin tietoihin toimittajalla on pääsy. Toimittaja, joka käsittelee luottamuksellista tai arkaluonteista tietoa, muodostaa tyypillisesti korkeamman tietoturvallisriskin kuin toimittaja, jolla ei ole pääsyä organisaation IT-järjestelmiin tai tietoihin.

Lisäksi riskiprofiloinnissa voidaan huomioida myös muita tekijöitä, kuten toimittajan pääsy organisaation järjestelmiin, integraatiot organisaation IT-ympäristöön, toimittajan toimittaman palvelun tekninen kompleksisuus ja

siitä aiheutuvat riippuvuudet sekä toimittajan oma tietoturvallisuuden kypsyystaso. Toimittajan palvelun kustannuksia voidaan myös käyttää yhtenä kriteerinä, mutta on otettava huomioon, että toimittajan palveluiden kustannus ei välttämättä korreloi toimittajan aiheuttaman riskin kanssa. Hyvänä esimerkkinä toimii internet-palveluiden sertifikaatteja ylläpitävät organisaatiot, joiden kustannukset ovat yleensä suhteellisen pieniä, mutta liiketoimintariski organisaation verkkosivujen kaatumisesta sertifikaattihaasteiden vuoksi on merkittävä. Näiden tekijöiden perusteella toimittajat voidaan jakaa esimerkiksi kahteen-neljään riskiluokkaan. Riskiluokitus toimii pohjana myöhemmille hallintatoimenpiteille, kuten sopimusvaatimuksille, auditoinneille, ja jatkuvalle seurannalle.

Tehokas riskiprofilointi edellyttää myös sitä, että arviointia päivitetään säännöllisesti. Toimittajan riskiprofiili voi muuttua esimerkiksi palvelun laajentuessa, uusien integraatioiden käyttöönoton myötä tai organisaation toimintaympäristön muuttuessa. Riskiprofilointi ei siten ole kertaluonteinen toimenpide, vaan jatkuva prosessi, joka tukee toimitusketjun kokonaisvaltaista tietoturvallisuuden hallintaa.

7.3 Uusien toimittajien ja näiden toimittamien palveluiden arviointi

Uusien toimittajien arvioinnin keskeinen tavoite ei ole ainoastaan varmistaa, että toimittaja täyttää tietyt tietoturvallisuusvaatimukset, vaan ennen kaikkea muodostaa perusteltu ja dokumentoitu päätös siitä, millä ehdoilla ja miten organisaatio voi ottaa uuden toimittajan osaksi omaa toimitusketjuaan. Jokainen toimittajasuhde luo organisaatioon uuden teknisen, operatiivisen tai tiedollisen riippuvuuden, ja avaa samalla uusia hyökkäysrajapintoja. Tämän vuoksi uusien toimittajien arviointi pitää nähdä osana laajempaa riskienhallinnan kokonaisuutta, jossa organisaatio päättää, millaisia riskejä se on valmis hyväksymään ja millaisilla kontrolleilla näitä riskejä hallitaan.

Toimittajien riskiprofilointi luo perustan sille, kuinka laaja ja syvällinen arviointi uusille toimittajille tulee tehdä. Kaikkien toimittajien arvioiminen samalla tasolla ei ole useimmille organisaatioille realistista eikä kustannustehokasta. Riskiprofiloinnin avulla organisaatio voi tunnistaa, mitkä toimittajat muodostavat merkittävimmän tietoturvariskin ja kohdistaa enemmän resursseja näihin toimittajiin. Käytännössä tämä tarkoittaa, että korkean riskiprofii-

lin toimittajille voidaan toteuttaa laajempia arviointeja ja teknisiä tarkasteluja, kun taas matalamman riskin toimittajien osalta voidaan käyttää kevyempiä arviointimenettelyjä.

Riskiprofilointiin perustuva arviointimalli mahdollistaa myös hallinnan skaalautuvuuden. Monet suuret organisaatiot voivat käyttää toimitusketjussaan satoja tai jopa tuhansia toimittajia, eikä kaikkien toimittajien syvällinen arviointi ole realistista tai järkevää. Toisaalta myös pienemmät organisaatiot voivat hyödyntää samaa mallia yksinkertaisemmassa muodossa. Olennaista ei ole arviointimenetelmän monimutkaisuus, vaan se, että organisaatio tekee tietoisia päätöksiä siitä, millä perusteella toimittajia arvioidaan ja kuinka paljon resursseja tähän prosessiin käytetään.

7.4 Toimittajasuhteen arviointi pelkän toimittaja-arvioinnin sijaan

Uusien toimittajien arvioinnissa keskeisin huomioon otettava asia on se, että tietoturvallisuusriskit ei synny pelkästään toimittajan ominaisuuksista, vaan ennen kaikkea siitä, miten toimittajan palvelu liittyy organisaation toimintaan, IT-järjestelmiin ja käsiteltävään tietoon. Tästä syystä arvioinnin tulisi kohdistua paitsi toimittajaan myös toimitettavaan palveluun sekä siihen liittyvään integraatiomalliin. Esimerkiksi hyviä tietoturvallisuuskäytäntöjä noudattava toimittaja voi muodostaa merkittävän riskin, mikäli sen palvelu vaatii laajat käyttöoikeudet organisaation kriittisiin järjestelmiin. Vastaavasti toimittaja, jolla ei ole todistetusti laadukkaista tietoturvallisuuskäytäntöjä, voi olla hyväksyttävä vaihtoehto, jos sen palvelu voidaan toteuttaa selkeästi rajatussa ympäristössä ilman pääsyä kriittisiin tietoihin.

Arvioinnin laajuutta määrittäessä keskeisiä kysymyksiä voivat olla esimerkiksi:

- Millaista pääsyä toimittajan palvelu vaatii organisaation järjestelmiin
- Mitä tietoa toimittaja käsittelee tai säilyttää
- Miten palvelu on teknisesti integroitu organisaation järjestelmiin
- Mikä on palvelun vaikutus liiketoiminnan jatkuvuuteen
- Miten palvelun muutoksia hallitaan ja viestitään

Näiden kysymysten avulla organisaatio voi muodostaa paremman kokonaiskuvan siitä, millainen riippuvuussuhde toimittajaan syntyy ja miten siihen liittyviä riskejä voidaan hallita.

7.5 Arviointimenetelmien valinta organisaation resurssien mukaan

Koska organisaatioiden toimintaympäristöt, riskinottokyvykkyys, tietoturvallisuusresurssit ja -kyvykkyydet vaihtelevat merkittävästi, ei ole olemassa yhtä, kaikille organisaatioille sopivaa mallia toimittajien arviointiin. Sen sijaan organisaatiot voivat rakentaa arviointiprosessin modulaarisesti siten, että siihen voidaan valita eri tasoisia menetelmiä käytettävissä olevien resurssien mukaan valittuun riskitasoon pohjautuen.

Yksinkertaisimmillaan toimittajan arviointi voi perustua sopimusten lisäksi rakenteelliseen tietoturvakyselyyn, jossa toimittajalta pyydetään tietoa sen tietoturvapolitiikoista, käytännöistä ja teknisistä kontrollimekanismeista. Tämä lähestymistapa on suhteellisen kevyt toteuttaa ja soveltuu erityisesti matalamman riskin toimittajille. Tietoturvakyselyt kannattaa mahdollisuuksien mukaan joko yhdistää toimittajasopimusten tietoturvavaatimusten kanssa tai vähintään pohjata kysymykset samoihin asioihin mitä sopimuksissa toimittajilta edellytetään.

Edellä mainitun lisäksi organisaatio voi arvioida toimittajia sertifikaatteihin ja standardeihin perustuen. Esimerkiksi ISO/IEC 27001 -sertifikaatti, SOC 2 -raportti tai vastaava kolmannen osapuolen arviointi voi tarjota lisävarmuutta toimittajan tietoturvallisuuskäytännöistä. Tällöin organisaation ei tarvitse itse suorittaa yksityiskohtaista auditointia, vaan se voi hyödyntää olemassa olevaa dokumentaatiota. Kolmansien osapuolten arvioinneissa on huomioitava tietyt haasteet:

- Sertifiointeja hakevat lähtökohtaisesti isommat ja IT-palveluita tuottavat organisaatiot, koska tietoturvallisuussertifiointi vaatii yleensä suhteellisen kypsää tietoturvallisuuden hallintaa ja kohtalaisen laajaa tietoturvallisuusorganisaatiota. Sertifioinnin puuttuminen ei automaattisesti korreloi huonojen tietoturvallisuuskäytäntöjen vuoksi
- Sertifiointeja arvioitaessa tarvitaan ammattitaitoa, koska näiden kohteet ja auditoidut asiat vaihtelevat merkittävästi ja jotta sertifioinnista olisi hyötyä organisaation omassa riskiarvioinnissa, näitä pitää pystyä

lukemaan kriittisesti, jotta muodostetaan kokonaisvaltainen ymmärrys näiden kattavuudesta ja riittävyydestä ostettavaan palveluun.
- Kannattaa myös ottaa huomioon, että sertifioinnit eivät poista organisaation vastuuta tai toimittajiin liittyviä riskejä, vaan organisaation on sertifikaatista huolimatta itse ymmärrettävä toimittajien tietoturvallisuuskäytännöt ja varmistettava sertifikaattien kattavuus riippuen toimittajan roolista.

Laajimmillaan toimittajan arviointi voi pitää sisällään myös palveluiden teknisiä tietoturvallisuusarviointeja tai toimittajan kuvaamien turvallisuusprosessien tarkempaa läpikäyntiä joko organisaation itsensä tai kolmannen osapuolen toimesta.

On kuitenkin tärkeää huomata, että tällaiset laajemmat arvioinnit edellyttävät usein merkittäviä resursseja sekä organisaation että toimittajan näkökulmasta. Tämän vuoksi niitä tulisi kohdistaa ensisijaisesti toimittajiin, joiden riskiprofiili on korkea.

7.5.1 Vähimmän luottamuksen periaate toimittajasuhteessa

Yksi tehokkaimmista tavoista vähentää toimitusketjuun liittyviä tietoturvallisuusriskejä on pyrkiä suunnittelemaan toimittajasuhteet siten, että toimittajaan luotetaan teknisesti mahdollisimman vähän. Tätä lähestymistapaa kutsutaan tietoturvallisuusviitekehyksissä vähimmän luottamuksen periaatteeksi. Sen sijaan tai sen lisäksi, että organisaatio yrittäisi varmistaa toimittajan tietoturvallisuuskäytäntöjen toimivuuden, organisaatio voi pyrkiä rajaamaan toimittajan vaikutusmahdollisuuksia järjestelmiin ja tietoihin sekä teknisesti, että operatiivisesti. Käytännössä tämä voi tarkoittaa esimerkiksi seuraavia toimenpiteitä:

- Toimittajan pääsy rajataan vain välttämättömiin järjestelmiin tai ympäristöihin
- Erillisten ympäristöjen tai testiympäristöjen käyttämistä toimittajan palveluille
- Käyttöoikeuksien aikarajaamista tai valvottuja hallintayhteyksiä
- Tietojen minimointia ja pseudonymisointia, erityisesti henkilötietoja käsitellessä
- Rajattuja ja hallittuja integraatiopisteitä organisaation järjestelmiin

Tällä lähestymistavalla voidaan merkittävästi vähentää toimitusketjuun liittyviä riskejä myös tilanteissa, joissa toimittajan tietoturvallisuuskäytännöt eivät ole täysin organisaation omien vaatimusten tasolla.

7.6 Toimittajasopimukset

Toimittajasopimukset muodostavat toimitusketjun tietoturvallisuusriskien hallinnassa yhden keskeisimmistä, mutta samalla myös usein väärinymmärretyistä hallintakeinoista. Sopimukset eivät itsessään estä tietomurtoa, poista haavoittuvuutta, varmista palvelun jatkuvuutta tai välttämättä kerro todellisuutta toimittajan tietoturvallisuuskäytännöistä, mutta sopimuksella on oleellinen rooli, koska sillä voidaan määrittää toimittajalle esitettävät tietoturvallisuusvaatimukset, vaatia edellisten todentamista, varmistaa miten poikkeamatilanteissa toimitaan ja kuka vastaa mistäkin asioita eri tilanteissa. Ilman riittäviä sopimuksellisia ehtoja organisaation käytännön mahdollisuudet ohjata, valvoa ja tarvittaessa pakottaa toimittaja korjaaviin toimenpiteisiin jäävät usein heikoiksi. Tästä näkökulmasta toimittajasopimus ei ole pelkkä juridinen asiakirja, vaan osa toimitusketjun tietoturvan hallintamallia ja riskienhallinnan infrastruktuuria. Samaan aikaan sopimukset ovat usein hyvin tulkinnanvaraisia ja eri osapuolet usein tulkitsevat niitä itselleen myönteisellä tavalla. Tämän vuoksi sopimuksiin kannattaa suhtautua hyvänä pohjana toimitusketjun tietoturvallisuuden varmistamisessa.

Edellisissä luvuissa käsitellyt toimittajien kategorisointi, riskiprofilointi sekä uusien toimittajien arviointi luovat perustan sille, millaisia tietoturvavaatimuksia sopimuksellisesti tulisi asettaa. Tämä linkki on keskeinen. Sopimuksellinen ohjaus ei voi olla tehokasta, jos vaatimukset ovat liian ylätasoisia, eivätkä määrittele vaatimuksia yksityiskohtaisesti. Vastaavasti liian raskaat ja yksityiskohtaiset sopimusvaatimukset voivat kuormittaa sekä organisaatiota että toimittajaa ilman, että tietoturvallisuusriskit oleellisesti pienenevät.

7.6.1 Sopimuspohjien modulaarisuus ja sitovuus

Myös toimittajasopimuksia ja näiden laajuutta olisi hyvä arvioida riskiperusteisesti, mutta erilaisten sopimuspohjien käyttö ja hallinta voi käytännössä osoittautua hankalaksi. Sen sijaan sopimusten tietoturvallisuusliitteet voidaan rakentaa modulaarisiksi niin, että kaikille toimittajille esitetään tietoturvallisuuden hallintaan ja yleisiin tietoturvallisuusasioihin liittyen samat vaatimuk-

set. Näiden lisäksi tietoturvallisuusvaatimuksiin voidaan yrityksen toimialasta ja käytettävistä toimittajista riippuen sisältää erinäisiä lisävaatimuksia mukaillen osion 7.1 toimittajien kategorisointia. Näissä lisävaatimuksissa on hyvä ottaa huomioon mahdolliset osiossa neljä kuvattujen regulaatioiden vaatimukset, mm. CRA:n vaatimukset ovat käytännössä joltain osin pakko sisällyttää toimittajien sopimusvaatimuksiin regulaation vaatimusten täyttämiseksi. Lisäosiot voidaan kuvata sitouttavan toimittajaa vain, jos toimittaja toimittaa tiettyyn kategoriaan liittyvää palvelua, jolloin toimittajat voivat jättää huomioimatta vaatimukset siltä osin, kun ne eivät tuotettavaan palveluun liittyviä.

Tietoturvallisuusliitteet ovat usein laadittu niin, että toimittajien odotetaan erikseen vahvistavan kunkin vaatimuksen esimerkiksi kuittaamalla kuhunkin kohtaan toimittajan sitoutuvat noudattamaan kyseistä vaatimusta. Tämä johtaa usein turhaan liitteiden käsittelyyn sekä organisaation, että toimittajan päässä ja mahdollistaa vaatimusten muokkaamisen jonka osana saatetaan hukata oleellisia vaatimusten kohtia. Tietoturvallisuusliite kannattaa laatia mahdollisimman yksiselitteisenä ja selkeänä niin, että toimittajalla ei ole mahdollisuutta kommentoida tai muokata yksittäisiä vaatimuksia. Liitteen loppuun voidaan erikseen mahdollistaa erityisehtoja joihinkin vaatimusten kohtiin, mutta tällöin on hyvä edellyttää toimittajalta kuvausta siitä miksi kyseistä vaatimusta ei implementoida ja kuvauksia mahdollisista kompensoivista kontrolleista.

7.6.2 Tietoturvallisuusvaatimusten pohja

Toimittajille asetettavien tietoturvallisuusvaatimusten yksi keskeisimmistä käytännön kysymyksistä on, mihin ne tulisi perustaa. Ilman selkeää viitekehystä toimittajavaatimukset jäävät helposti hajanaisiksi, päällekkäisiksi, liian yleisluontoisiksi tai päinvastoin monilta osin liian yksityiskohtaisiksi. Riskinä on se, että vaatimukset eivät ole riittäviä tai monimutkaisuudessa johtavan liian pitkiin tai hankaliin sopimusneuvotteluihin. Lisäksi vaarana on, että toimittajille asetetaan vaatimuksia, joita organisaatio ei itse noudata omassa toiminnassaan. Tällainen epäsymmetria heikentää vaatimusten uskottavuutta, vaikeuttaa niiden perustelemista ja voi johtaa tilanteeseen, jossa toimitusketjun hallinta rakentuu enemmän yksittäisten vaatimusten kuin yhtenäisen hallintamallin varaan.

Toimivana ajatuksena on pohjata tietoturvallisuusvaatimukset organisaation omassa käytössä olevaan tietoturvallisuuden hallintamalliin. Euroopassa yleisin käytössä oleva viitekehys ISO27001 toimii hyvänä pohjana, mutta myös muita viitekehyksiä voidaan käyttää. Tällaisen viitekehyksen käyttäminen tarjoaa kansainvälisesti tunnetun ja yleisesti käytetyn rakenteen tietoturvallisuuden hallinnalle. Se ei keskity vain yksittäisiin teknisiin kontrollitoimenpiteisiin, vaan tarkastelee tietoturvaa johtamisen, riskienhallinnan, vastuiden, jatkuvan parantamisen ja kontrolliympäristön kokonaisuutena. Juuri tämä tekee siitä erityisen käyttökelpoisen toimitusketjun tietoturvavaatimusten perustaksi. Toimittajilta ei tällöin vaadita irrallisia turvallisuustoimenpiteitä, vaan niitä pyydetään toimimaan osana sellaista mallia, jota organisaatio itsekin käyttää oman tietoturvallisuuden johtamiseen.

Yleisen viitekehyksen käyttämisen hyödyt korostuvat erityisesti siinä, että se mahdollistaa tietoturvallisuusasioista puhumisen yhteisellä kielellä toimittajan kanssa. Toimitusketjun tietoturvallisuuden haaste ei useinkaan ole vain kontrollien puute, vaan yhteisen ymmärryksen puute siitä, mitä “riittävä tietoturva” käytännössä tarkoittaa. Kun sekä organisaation että toimittajien vaatimuksia jäsennetään saman viitekehyksen kautta, syntyy läpi toimitusketjun yhdenmukaisempi tapa puhua esimerkiksi käyttöoikeuksien hallinnasta, poikkeamien hallinnasta, varautumisesta, toimittajavalvonnasta ja jatkuvasta kehittämisestä. Tämä vähentää tulkinnanvaraisuutta ja helpottaa myös käytännön yhteistyötä auditoinneissa, poikkeamien käsittelyssä ja toimittajasuhteiden elinkaaren aikaisessa hallinnassa.

Organisaatio omassa käytössä olevan viitekehyksen käyttäminen vaatimusten laadintaan luo toimitusketjuun peilimäisen hallintamallin: organisaatio ei vaadi toimittajilta mitään sellaista, mitä se ei itse pidä olennaisena tai mitä se ei ole itse kyennyt jalkauttamaan omassa toiminnassaan. Toimittajalle on myös huomattavasti helpompi perustella vaatimuksia, jos ne voidaan kytkeä organisaation omaan riskienhallinnan ja tietoturvallisuuden johtamismalliin eikä niitä esitetä irrallisena asiakaslistana. Samalla organisaatio voi välttää tilanteen, jossa toimittajavaatimukset ovat muodostuneet historian saatossa eri standardeista, auditoinneista ja yksittäisistä poikkeamista koostuvaksi kokoelmaksi, jota kukaan ei enää hallitse kokonaisuutena.

Saman viitekehyksen käyttämisen etu on myös siinä, että se auttaa rakentamaan johdonmukaisen linkityksen omasta toiminnastaan toimittajan toimintaa. Kun organisaatio on itse määritellyt erinäisiä tietoturvallisuuteen liittyviä prosesseja osaksi omaa tietoturvallisuuden hallintajärjestelmäänsä, voi se heijastaa näitä samoja periaatteita toimittajavaatimuksiin. Tällöin toimittajahallinta ei ole erillinen saareke, vaan jatke organisaation omalle tietoturvan hallintajärjestelmälle. Tämä on tärkeää erityisesti suuremmissa organisaatioissa, joissa toimittajahallinta helposti pirstaloituu hankinnan, tietoturvallisuuden, laki- ja liiketoimintayksiköiden välille.

On tärkeää huomioida, että esim. ISO/IEC 27001:een pohjaaminen ei tarkoita sitä, että toimittajilta vaadittaisiin ISO/IEC 27001 -sertifiointia tai identtistä kontrolliympäristöä. Tällainen vaatimus olisi monissa tilanteissa ylimitoitettu ja käytännössä epärealistinen. Olennaisempaa on, että vaatimukset johdetaan samasta viitekehyksestä ja sanoitetaan korkeammalle tasolle niin että jokaisen kontrollialueen perimmäiset tarkoitukset siirtyvät sopimuksellisesti sitovaksi. Toisaalta toimittajan mahdollinen sertifiointi auttaa varmentamaan sopimusten täyttymistä mahdollisten arviointien tai auditointien yhteydessä.

7.6.3 Sopimusten rooli tietoturvallisuuden hallinnassa

Tietoturvallisuuden näkökulmasta toimittajasopimuksella ja sen tietoturvallisuusliitteellä on vähintään neljä keskeistä tehtävää. Ensimmäinen niistä on odotusten konkretisointi. Vaikka toimittajalla olisi hyvät tekniset kyvykkyydet ja sertifioidut tietoturvallisuuskäytännöt, ei ole itsestään selvää, että toimittajan turvallisuuskäytännöt vastaavat organisaation omien toimintaympäristön vaatimuksia. Sopimus tekee näkyväksi sen, mitä toimittajalta odotetaan esimerkiksi pääsynhallinnan, haavoittuvuuksien hallinnan, lokittamiseen, poikkeamailmoitusten tai toimittajan oman toimitusketjun tietoturvallisuudelta. Asioiden juridinen sopiminen antaa paljon paremmat mahdollisuuden myös vaatia toimittajaa näyttämään asioita tarvittaessa toteen ja toisaalta painostaa toimittajaa suhtautumaan vaatimuksiin riittävän vakavasti.

Toinen tehtävä on vastuiden kohdentaminen. Toimitusketjuissa tietoturvallisuusriskit syntyvät usein epäselvistä vastuurajauksista. Käytännössä ongelmat eivät johdu siitä, ettei mitään olisi tehty, vaan siitä, että eri osapuolet olettavat toisen vastaavan tietystä osa-alueesta tai tekemisen tasosta. Sopi-

muksella voidaan täsmentää esimerkiksi, kumpi osapuoli vastaa käyttäjähallinnasta, lokien säilyttämisestä, varmuuskopioinnista, haavoittuvuuksien korjaamisesta, tietosuojavaatimuksista tai viranomaisilmoituksista.

Kolmas tehtävä on todennettavuuden mahdollistaminen. Ilman sopimuksessa määriteltyjä auditointioikeuksia organisaatiolla voi olla hyvin rajalliset mahdollisuudet varmistua siitä, että toimittaja todella noudattaa sovittuja käytäntöjä. Tällöin asiakas jää pitkälti toimittajan vakuuttelujen tai markkinointimateriaalin varaan.

Neljäs tehtävä on poikkeamatilanteiden hallinta. Tietoturvapoikkeaman hetkellä organisaatiolla on hyvin vähän aikaa neuvotella siitä, milloin toimittajan tulisi ilmoittaa tapahtuneesta, mitä tietoja sen tulee toimittaa, miten yhteistä tutkintaa tehdään tai mitä korjaavia toimia siltä odotetaan. Nämä asiat olisi hyvä olla sovittuna jo ennen poikkeamaa.

7.6.4 Tietoturvallisuusvaatimukset osana kaupallisia neuvotteluja

Yksi käytännön haasteista toimitusketjun tietoturvallisuusvaatimusten määrittelyssä on se, että niitä ei yleensä sovita irrallaan muista asioista, vaan päinvastoin osana laajempia kaupallisia neuvottelua. Sopimusneuvotteluissa käsitellään usein samanaikaisesti useista tavoitteista, joissa organisaatiolla ja toimittajalla voi olla erilaisia näkemyksiä: hinta, toimitusaikataulu, palvelun laajuus, vastuunrajoitukset, palvelutasot sekä toimittajan liiketoiminnalliset tavoitteet. Tässä kokonaisuudessa tietoturvallisuusvaatimukset voivat helposti näyttäytyä lisävaatimuksina, jotka hidastavat kaupallista prosessia tai lisäävät kustannuksia. Erityisesti tilanteissa, joissa organisaatio pyrkii nopeasti käynnistämään uuden projektin tai kun toimittajaa pidetään strategisesti merkittävänä, tietoturvallisuus saatetaan nähdä liiketoiminnan etenemistä jarruttavana tekijänä. Usein toimittajat myös käyttävät itse tietoturvallisuusvaatimuksia tahallaan väärin korostaakseen asioiden hankaluutta, samanaikaisesti tietäen, että hyvin toteutettu tietoturvallisuus ei välttämättä ole helppoa. Hyvin rakennetun tietoturvallisuusvaatimukset eivät pidä sisällään mitään sellaista mitä organisaatio ei itse toteuttaisi tai mikä ei olisi tietoturvallisuuden näkökulmasta järkevää.

Nämä haasteet eivät kuitenkaan tarkoita, että tietoturvallisuuden ja liiketoiminnannan tavoitteet olisivat lähtökohtaisesti ristiriidassa keskenään. Pikemminkin ne korostavat tietoturvallisuusorganisaation roolia liiketoiminnan

mahdollistajana. Tietoturvallisuusorganisaation tehtävänä ei ole ainoastaan tunnistaa riskejä ja asettaa vaatimuksia, vaan myös auttaa liiketoimintaa tekemään informoituja päätöksiä siitä, millaisia riskejä organisaatio on valmis hyväksymään ja millä ehdoilla yhteistyö toimittajan kanssa voidaan toteuttaa turvallisesti. Tämä edellyttää kykyä kääntää tietoturvallisuusvaatimukset liiketoiminnan kielelle ja osoittaa niiden yhteys konkreettisiin liiketoimintavaikutuksiin.

Pelkkä tekninen tai juridinen vaatimuslista itsessään ei yleensä riitä vakuuttamaan liiketoimintaa tai toimittajaa tietoturvallisuusvaatimusten merkityksestä. Sen sijaan olennaista on osoittaa, miksi tietyt vaatimukset ovat tarpeen juuri kyseisessä palvelussa ja mitä seurauksia niiden puuttumisella voi olla. Esimerkiksi vaatimus tietoturvallisuuspoikkeamien ilmoittamisesta tietyn ajan kuluessa ei ole vain hallinnollinen yksityiskohta, vaan se liittyy suoraan organisaation kykyyn täyttää omat viranomaisvelvoitteensa, rajoittaa mahdollisen tietomurron vaikutuksia ja viestiä asiakkailleen asianmukaisesti. Samoin vaatimus alihankkijoiden sitouttamisesta toimittajan tietoturvallisuusvaatimuksiin ei ole pelkkä muodollisuus, vaan sillä pyritään hallitsemaan toimitusketjuun syntyviä näkymättömiä ja hallitsemattomia riippuvuuksia. Kun tietoturvallisuusvaatimukset esitetään tällaisessa kontekstissa, ne eivät näyttäydy pelkkinä lisäehtoina, vaan osana palvelun laadun ja luotettavuuden varmistamista. Tämä muuttaa sopimusneuvottelujen luonnetta. Tietoturvallisuus ei enää ole este sopimukselle, vaan osa sen arvolupausta.

Tietoturvallisuusorganisaatio voi toimia myös liiketoiminnan ja myynnin tukena. Monilla toimialoilla asiakkaiden odotukset tietoturvasta ovat kasvaneet merkittävästi viime vuosina. Lisääntynyt regulaatio ja kyberturvallisuustietoisuus sekä julkisuudessa esillä olleet tietomurrot ovat lisänneet asiakkaiden kiinnostusta toimittajiensa turvallisuuskäytäntöihin. Tällaisessa ympäristössä vahvat tietoturvallisuuskäytännöt ja niiden osoittaminen ei ole pelkästään riskienhallinnan väline, vaan se voidaan kääntää myös kilpailueduksi.

Tietoturvallisuusvaatimuksista neuvottelu voi myös toimia arviointimekanismina toimittajille. Sopimusneuvottelujen aikana toimittajan suhtautuminen tietoturvallisuusvaatimuksiin paljastaa usein paljon sen tietoturvallisuuskäytänteiden ja johtamismallien kypsyydestä. Toimittaja, joka pystyy ja haluaa keskustella avoimesti tietoturvallisuuskäytännöistään, auditointioikeuksista,

poikkeamien raportoinnista tai toimittajiensa hallinnasta, osoittaa yleensä myös kyvykkyyttä hallita näitä asioita käytännössä.

Tästä näkökulmasta sopimusneuvotteluista voi tulla muutakin kuin pelkkä juridinen prosessi, se voi olla kriittinen osa toimittajan arviointia. Ne tarjoavat mahdollisuuden testata, miten toimittaja suhtautuu tietoturvallisuusasioihin käytännössä ja onko se sitoutunut pitkäjänteiseen yhteistyöhön näihin asioihin liittyen. Tämä voi auttaa organisaatiota tunnistamaan mahdollisia riskejä jo ennen sopimuksen allekirjoittamista.

On kuitenkin tärkeää huomata, että kaikkia tietoturvallisuusvaatimuksia ei voida aina saavuttaa täydellisesti ja joskus voidaan jopa joutua käyttämään toimittajan sopimuspohjia. Joissakin tilanteissa toimittajan markkina-asema, palvelun ainutlaatuisuus tai kaupalliset realiteetit voivat rajoittaa organisaation mahdollisuuksia vaikuttaa sopimusehtoihin. Tällöin tietoturvallisuusorganisaation rooli on auttaa liiketoimintaa ymmärtämään, mitä riskejä kompromissit tarkoittavat ja millä keinoilla näitä riskejä voidaan hallita. Tämä voi tarkoittaa esimerkiksi teknisiä rajoituksia integraatioihin, lisävalvontaa tai muita kontrolleja.

7.7 Toimittajien arviointi ja hallinta elinkaaren aikana

Vaikka toimittajien tietoturvallisuuden hallintaan liittyvistä toimenpiteistä monet tehdään ennen toimittajan palveluiden käyttöönottoa, ei toimittajien tietoturvallisuuden hallinta pääty sopimuksen allekirjoittamiseen tai palvelun käyttöönottoon. Toimittajasuhteen alkaessa toimittajan hallinnan osalta on siirryttävä jatkuvaan malliin, jossa pyritään hallitsemaan toimitusketjun tietoturvallisuusriskejä koko elinkaaren aikana. Muuttuvat teknologia, liiketoimintamallit ja organisaatiot aiheuttavat muutoksia myös toimittajasuhteen aikana. Palvelun laajuus voi kasvaa, integraatiot voivat syventyä, dataa voidaan alkaa käsitellä uudella tavalla tai toimittaja voi ottaa käyttöön uusia alihankkijoita. Tämän vuoksi toimittajien hallinta on nähtävä jatkuvana prosessina, joka kattaa koko toimittajasuhteen elinkaaren alkaen käyttöönotosta ja päättyen hallittuun irtautumiseen.

7.7.1 Määrämuotoinen riskienhallinta elinkaaren aikana

Yksi keskeinen havainto toimitusketjun tietoturvallisuuden näkökulmasta on se, että toimittajasuhteet ovat usein dynaamisia riippuvuuksia. Toisin kuin

monissa perinteisissä hankinnoissa, joissa toimittajan rooli pysyy suhteellisen muuttumattomana, digitaalisissa palveluissa toimittajan vaikutus organisaation toimintaympäristöön voi kasvaa merkittävästi ajan myötä. Esimerkiksi pilvipalvelu, joka alun perin tukee yhtä liiketoimintaprosessia, voi muutamassa vuodessa muodostua keskeiseksi osaksi organisaation IT-arkkitehtuuria. Samalla toimittajan käsittelemän datan määrä kasvaa ja tämän myötä palvelun kriittisyys lisääntyy. Jos toimittajan riskiprofiilia ei arvioida uudelleen elinkaaren aikana, organisaatio voi päätyä tilanteeseen, jossa merkittävä tekninen ja liiketoiminnallinen riippuvuus on syntynyt ilman tietoturvallisuuskontrollien uudelleenarviointia.

Tästä vuoksi toimittajia tulisi hallita systemaattisesti ja määrämuotoisesti koko elinkaaren ajan jatkuvan riskienarvioinnin kautta. Tämä ei tarkoita sitä, että kaikkia toimittajia tulisi arvioida tai kohdella samalla tavalla, vaan että organisaatiolla on mekanismeja havaita, milloin toimittajan riskiprofiili muuttuu. Muutoksia voivat olla esimerkiksi palvelun laajentuminen uusiin käyttötarkoituksiin, toimittajan yritysjärjestelyt, IT-infrastruktuurin muutokset tai uudet tai muuttuneet integraatiot organisaation järjestelmiin. Kun muutoksia tapahtuu, toimittajan aiheuttamaa riskiä tulisi arvioida uudelleen samoilla mekanismeilla, jota käytettiin alkuperäisessä toimittaja-arvioinnissa.

7.7.2 Elinkaaren hallinnan aikaiset tietoturvallisuuskontrollit

Käytännössä toimittajien elinkaaren aikainen hallinta voidaan rakentaa useista toisiaan täydentävistä mekanismeista. Ensimmäinen näistä on säännöllinen toimittaja-arviointi, joka toteutetaan ennalta määritellyin väliajoin. Tällaisen arvioinnin tavoitteena ei ole pelkästään tarkistaa, että toimittaja noudattaa sopimuksessa määriteltyjä velvoitteita, vaan myös arvioida, onko toimittajasuhteen riskiprofiili muuttunut. Arviointi voi sisältää esimerkiksi toimittajan turvallisuuskäytäntöjen päivittämistä koskevia kyselyitä, sertifikaattien tarkistamista tai keskusteluja toimittajan tietoturvallisuusorganisaation kanssa. Vaatimukset näille tulisi tulla keskitettynä tietoturvallisuusorganisaatiolta, mutta näiden toteuttamisesta tulisi lähtökohtaisesti vastata toimittajasta organisaatiossa vastaava taho.

Toinen tärkeä mekanismi on operatiivinen seuranta. Toimittajahallinta ei voi perustua pelkästään määräajoin tehtäviin arviointeihin, vaan organisaation tulisi seurata toimittajiin liittyviä turvallisuustapahtumia myös päivittäisessä

toiminnassa. Tämä voi tarkoittaa esimerkiksi tietoturvapoikkeamien raportointia, haavoittuvuuksiin liittyvää viestintää tai muutostenhallintaa koskevia käytäntöjä. Kun toimittaja raportoi merkittävästä tietoturvatapahtumasta tai teknisestä muutoksesta, organisaation arvioida, vaikuttaako tapahtuma sen omaan toimintaympäristöön. Lisäksi toimittajan tietoturvallisuustilannetta olisi hyvä valvoa ulkoisten lähteiden kautta mahdollisten puutteiden tai tietoturvallisuuspoikkeamien havaitsemiseksi. Valitettavasti edelleen on liian yleistä kuulla toimittajalla sattuneista tapahtumista julkisista lähteistä.

Kolmas näkökulma toimittajahallinnan elinkaarimallissa on yhteistyöhön perustuva kehittäminen. Toimittajasuhteet eivät ole pelkästään sopimuksia ja kontrollimekanismeja, vaan myös pitkäaikaisia kumppanuuksia. Tietoturvallisuuden näkökulmasta tämä tarkoittaa sitä, että organisaatiot voivat kehittää turvallisuuskäytäntöjään yhdessä toimittajiensa kanssa. Esimerkiksi säännölliset tapaamiset, yhteiset harjoitukset tai kokemusten vaihtaminen voivat parantaa molempien osapuolten kykyä hallita tietoturvallisuuteen liittyviä riskejä.

Toimittajahallinnan elinkaaren aikaista hallintaa voidaan katsoa myös organisaation digitaalisen ekosysteemin ylläpitona. Modernit organisaatiot eivät enää toimi yksin, vaan osana laajoja verkostoja, joissa palvelut, data ja teknologia liikkuvat useiden eri toimijoiden välillä. Tässä ekosysteemissä yksittäisen toimittajan turvallisuustaso ei riitä, vaan olennaista on, miten turvallisuus toteutuu koko verkoston tasolla ja että myös heikoin lenkki on riittävän vahva. Kun organisaatio seuraa toimittajiensa tietoturvallisuustilannetta systemaattisesti, se pystyy myös tunnistamaan laajempia riskejä, jotka liittyvät esimerkiksi yhteisiin teknologiariippuvuuksiin tai keskittyneisiin alihankintaketjuihin.

Elinkaaren aikainen hallinta liittyy myös organisaation kykyyn oppia uutta ja parantaa omaa toimintaansa. Jokainen toimittajasuhde tuottaa kokemuksia siitä, miten tietoturvallisuusvaatimukset toimivat käytännössä ja millaisia haasteita niiden toteuttamiseen liittyy. Tietoturvallisuuspoikkeamat, auditointien havainnot tai operatiivisessa yhteistyössä esiin nousevat ongelmat voivat tarjota arvokasta tietoa siitä, miten organisaation toimittajahallinnan mallia tulisi kehittää. Kun nämä kokemukset kerätään systemaattisesti, ne voivat auttaa parantamaan sekä tulevien toimittajien arviointia että sopimuksellisia vaatimuksia.

7.7.3 Toimittajasuhteen päättäminen

Toimittajasuhteen viimeinen vaihe on usein myös yksi kriittisimmästä tietoturvallisuuden näkökulmasta: sopimuksen päättyminen ja toimittajasta irtautuminen. Kun palvelu lopetetaan tai siirretään toiselle toimittajalle, organisaation tulee varmistaa, että kaikki käyttöoikeudet poistetaan, integraatiot puretaan hallitusti ja toimittajan hallussa oleva data palautetaan tai poistetaan asianmukaisesti. Nämä asiat on myös hyvä olla varmistettu jo sopimuksellisessa vaiheessa uutta toimittajaa käyttöönotettaessa, mutta toimittajasuhteen päättymisen yhteydessä on hyvä varmistaa, että vaatimukset ovat tiedossa ja että toimittaja ymmärtää vastuunsa. Ilman selkeää poistumisprosessia organisaatio voi jättää ympäristöönsä teknisiä tai organisatorisia “jälkiä”, jotka voivat muodostaa tietoturvallisuusriskejä myös sen jälkeen, kun toimittajan palveluita ei enää käytetä. Usein ongelmana on se, että toimittajasuhde ei pääty selkeästi tiettynä päivänä, vaan toimittajan palveluiden käyttämien hiipuu pikkuhiljaa. Tätä varten organisaation on hyvä asettaa määrityksiä minkä avulla voidaan tunnistaa, kun jonkun toimittajan palveluita ei enää aktiivisesti käytetä.

Elinkaaren aikainen toimittajahallinta ei saa muodostua liian raskaaksi prosessiksi, joka kuormittaa liikaa erilaisia sidosryhmiä. Kuten aiemmissa luvuissa on todettu, yritysten resurssit ja kyvykkyydet vaihtelevat merkittävästi ja tästä syystä toimittajahallinnan elinkaarimalli tulisi rakentaa riskiperusteisesti ja skaalautuvasti. Perustasolla organisaatio voi toteuttaa säännöllisiä tarkistuksia keskeisille toimittajilleen ja seurata tietoturvallisuuspoikkeamia. Seuraavalla tasolla voidaan lisätä säännöllisiä turvallisuuskatsauksia, riskiprofiilien päivittämistä ja tapaamisia toimittajan kanssa. Kehittyneemmässä mallissa toimittajien turvallisuustilannetta voidaan seurata jatkuvasti osana organisaation laajempaa tietoturvallisuuden tilannekuvaa.

Keskeistä on, että organisaatio ymmärtää toimittajasuhteiden muuttuvan luonteen ja rakentaa prosesseja, jotka mahdollistavat näiden muutosten hallinnan. Kun toimittajien arviointi ja hallinta nähdään elinkaaren aikaisena prosessina ja vastuut organisaatio sisällä tähän liittyen on selkeästi määritelty, organisaatio pystyy paremmin hallitsemaan toimitusketjun tietoturvallisuusriskien monimutkaisuutta ja vähentämään riskiä siitä, että tietoturvallisuus

heikkenee hiljalleen toimittajasuhteen kehittyessä. Samalla se vahvistaa toimitusketjun resilienssiä ja luo perustan pitkäjänteiselle ja turvalliselle yhteistyölle toimittajien kanssa.

7.8 Toimittajien auditointi

Toimittajien auditointi on yksi keskeisimmistä mekanismeista, joilla organisaatio voi varmistaa, että toimitusketjuun liittyvät tietoturvallisuusvaatimukset toteutuvat käytännössä. Toimittajien riskiprofilointi, sopimukselliset velvoitteet ja toimittajien hallinta elinkaaren aikana luovat hyvät lähtökohdat toimitusketjun tietoturvallisuuden hallinnalle ja yhteistyölle, mutta ilman edellä mainittujen varmentamista niiden käytännön toteutuminen jää helposti oletusten tai toimittajan lupausten varaan. Auditoinnit tarjoavat organisaatiolle mahdollisuuden siirtyä dokumentoiduista vaatimuksista todellisten riskien ja tilanteen parempaan hahmottamiseen ja arvioida sitä, miten toimittajan tietoturvallisuuden hallinta toimii käytännössä.

Toimittajien auditoinnin rooli korostuu erityisesti ympäristöissä, joissa organisaatio on riippuvainen toimittajan tarjoamasta ulkoisesta palvelusta, ohjelmistosta ja teknologiasta. Kun yrityksen liiketoimintakriittiset prosessit toteutetaan yhdessä toimittajan kanssa, organisaation oman tietoturvallisuuden taso on vahvasti riippuvainen toimittajan tietoturvallisuuskäytännöistä.

Samalla on hyvä ymmärtää, että auditointeja olisi hyvä käyttää muutenkin kuin valvonta- tai varmennusmekanismina. Parhaimmillaan ne toimivat yhteisenä oppimisen välineenä toimittajan kanssa, jonka avulla sekä organisaatio, että toimittaja voivat parantaa ja kehittää omia tietoturvallisuuskäytäntöjään ja syventää yhteisiä hyviä käytäntöjä. Auditointien avulla voivaan tuoda esiin myös parhaita käytäntöjä kummaltakin puolelta, tunnistaa kehityskohteita ja vahvistaa yhteistyötä.

Organisaatio voi toteuttaa auditoinnit itse, mutta usein voi olla järkevää ulkoistaa auditoinnit kolmannelle osapuolelle, yrityksille, joka on riippumaton sopimuksen osapuolista ja joilla on kokemusta sekä osaamista toteuttaa auditointeja. Tässä tapauksessa auditoinnin tavoitteista, auditointimalleista ja viitekehyksistä, aikatauluista ja rooleista sekä raportoinnista on hyvä sopia yhdessä mahdollisimman selkeästi, jotta auditoinneista saadaan mahdollisimman suuri hyöty mahdollisimman pienellä vaivalla auditoitavalle toimitta-

jalle. Lisäksi organisaation sisällä on hyvä yrittää sitouttaa myös muita sidosryhmiä, erityisesti toimittajan tuottavan palvelun omistajia osallistumaan auditoineihin, jotta vastuuta ja osallistumista saadaan jaettua mahdollisimman laajalle.

7.8.1 Auditointien rooli osana toimitusketjun tietoturvallisuusriskien hallintaa

Toimittaja-auditointien keskeisenä tarkoituksena on todentaa, että toimittaja noudattaa yhdessä sovittuja tietoturvallisuusvaatimuksia, ja että sen käytännöt ovat linjassa organisaation asettamien odotusten kanssa. Auditointien avulla organisaatio on myös arvioida toimittajan tietoturvallisuuskäytäntöjen ja tietoturvallisuuden hallintamallin kypsyyttä. Joissakin tapauksissa toimittaja saattaa täyttää yksittäisiä vaatimuksia hyvin tai täyttää vaatimukset muodollisesti, mutta käytännön kokonaisvaltainen tietoturvallisuuden hallinta voi olla puutteellista.

Tietoturvallisuusvaatimusten tulkinnassa voi olla myös merkittäviä eroja, jotka eivät välttämättä aiheudu puutteellisista kontrolleista, vaan niiden toteutustavasta. Viime vuosien suurimpia trendejä tietoturvallisuudessa on ollut ”Zero Trust”-periaate, jossa ideaalisti organisaation koko pääsynhallinta ja verkkoinfrastruktuuri rakennetaan tukemaan mallia, jossa käyttäjille annetaan vain ne oikeudet, joita hän juuri sillä hetkellä työssään tarvitsee. Tätä periaatetta voidaan tulkita hyvin monilla eri tavoilla ja tasoilla ja sen ympärille on syntynyt merkittävä määrä kaupallisia tuotteita. Tämän myötä eri organisaatiot saattavat tarkoittaa termistä puhuttaessa täysin eri asioita. Eri termistön ja kontrollien yhteinen läpikäynti osana auditointia tukee yhteisen näkemyksen ja yhteisen kielen muodostusta.

7.8.2 Auditointien haasteet

Vaikka toimittajien auditointi toimii tärkeässä roolissa toimitusketjun tietoturvallisuuden varmistamista, auditointiohjelma ja itse auditoinnit vaativat merkittävää suunnittelua ja resursseja ja siihen liittyy myös tiettyjä haasteita. Keskeisin haaste liittyy työn priorisointiin ja resurssien rajallisuuteen. Organisaatiolla voi olla satoja tai jopa tuhansia toimittajia ja näiden kaikkien tai edes suuren osan auditointi ei ole realistista eikä järkevää. Organisaation hyvä

käyttää aikaisemmin esiteltyä toimittajien riskiprofilointia yhdessä liiketoimintojen kanssa osana auditoitavien yritysten valintaa, jotta resurssin saadaan kohdistettua liiketoiminnan kannalta merkityksellisimpiin toimittajiin.

Toinen haaste liittyy toimittajien haluttomuuteen osallistua auditointeihin. Monet toimittajat kokevat haasteelliseksi avata omia toimintatapojaan, erityisesti kolmansille osapuolille ja lisäksi toimittajilla voi olla resurssihaasteita auditoineihin osallistumisessa. Monet suuremmat yritykset pyrkivät ensisijaisesti tarjoamaan standardoituja sertifikaatteja ja raportteja ja rajoittaa asiakkaiden erillisiä auditointeja. Aikaisemmin viitatussa sopimuksellisista liitteissä on hyvä sopia auditointioikeuksista etukäteen ja toimittajalle voidaan myös viestiä miltä osin auditointi eroaa heidän standardoiduista sertifikaateistaan.

Kolmas haaste on auditointien tehokkuus ja vaikuttavuus, sekä liiketoimintojen ja sidosryhmien kyky ymmärtää näiden merkittävyyttä. Auditoinnin voivat helposti muuttua muodolliseksi tarkistuslistaksi, jotka eivät tarjoa todellista ymmärrystä toimittajien tietoturvallisuuskäytännöistä. Tämä korostuu erityisesti silloin, jos auditoinnin keskittyvät pelkästään dokumentaation läpikäyntiin, eivätkä ne sisällä haastatteluja tai teknistä tarkastelua. Auditointien toteuttaminen ja tavoitteet on hyvä määritellä mahdollisimman tarkasti ja mallia parantaa auditointiohjelman edetessä.

Organisaation kannattaa rakentaa toimittaja-auditointiohjelmansa niin, että toimittajan riskiprofiilin ja toimittaman palvelun kautta auditoinnit kohdistetaan niihin asioihin, jotka juuri sen toimittajan osalta koetaan oleellisiksi. Lisäksi on hyvä huomioida toimittajan mahdolliset tietoturvallisuussertifikaatit ja vastaavat, joissa usein on käyty kattavasti läpi tietoturvallisuuden perusasiat kuten politiikat ja ohjeistukset. Profiloinnin perusteella auditoinnissa kannattaa keskittyä juuri niihin asioihin mitkä kyseisen toimittajan palvelussa muodostavat yritykselle suurimman riskin.

7.8.3 Auditointien tulevaisuus

Digitaalisen toimintaympäristön kehittyessä myös toimittajien auditointikäytännöt ovat muuttumassa. Perinteiset auditointimallit, jotka perustuvat määräajoin tehtäviin tarkastuksiin ja toimittajan haastatteluun, eivät aina vastaa nopeasti muuttuvan ympäristön tarpeisiin.

Jatkossa organisaatiot tulevat mahdollisesti siirtymään toimittajien osalta kohti jatkuvaa valvontaa ja keskinäiseen tiedonvaihtoon ja yhteistyöhön perustuvia malleja. Tämä voi tarkoittaa esimerkiksi automatisoituja raportointikäytäntöjä, jatkuvaa tilannekuvaa tai reaaliaikaista tietoa toimittajan turvallisuustapahtumista. Tällaiset lähestymistavat voivat täydentää tai jopa korvata perinteisiä auditointeja ja tarjota ajantasaisemman kuvan toimittajan tietoturvallisuuden tasosta. Lisäksi tekoälyn mukanaan tuomat mahdollisuudet auttavat muodostamaan parempaa tilannekuvaa myös toimittajien aiheuttamasta riskistä.

Samalla auditointien rooli voi laajentua pelkästä kontrollien tarkastamisesta kohti laajempaa toimitusketjun resilienssin arviointia. Organisaatiot voivat haastaa toimittajia vahvemmin siitä sitä, miten toimittajat varautuvat kyberhyökkäyksiin, miten ne palautuvat häiriötilanteista tai miten ne hallitsevat omia toimitusketjujaan.

7.9 Toimiminen sidosryhmien kanssa

Toimitusketjuun liittyvien tietoturvallisuusriskien hallinnan ei pitäisi olla yhden organisaation yksikön, prosessin tai työkalun varaan rakentuva kokonaisuus. Vaikka toimittajahallinta usein näyttäytyy ulospäin sopimuksina, arviointeina ja auditointeina, sen toimivuus riippuu ratkaisevasti siitä, kykeneekö organisaatio toimimaan johdonmukaisesti eri sisäisten ja ulkoisten sidosryhmiensä kanssa. Toimitusketjun tehokas hallinta on moninaisten sidosryhmien yhteistyötä. Siinä kohtaavat liiketoiminnot, hankinta-, tietoturvallisuus-, IT-, laki-, vastuullisuusyksikkö, viranomaiset sekä toimittajat itse. Vain näiden sidosryhmien yhteistyön myötä saadaan, tietoturvallisuusvaatimukset aidosti riskejä hallitsevaksi ja ohjaavaksi toiminnaksi.

Sisäisten sidosryhmien näkökulmasta yksi keskeinen haaste on se, että eri yksiköt tarkastelevat toimittajasuhteita eri logiikalla. Liiketoiminta näkee toimittajan keinona saavuttaa nopeutta tai tehokkuutta tekemiseen, osaamista tai markkinaetua. Hankinta tarkastelee toimittajaa kilpailutuksen, kaupallisten ehtojen ja toimittajamarkkinan kautta. IT arvioi yhteensopivuutta, teknistä toteutettavuutta ja operatiivista jatkuvuutta. Lakiyksikkö painottaa sopimuksellista hallittavuutta, vastuunrajauksia ja juridista turvaa. Tietoturvallisuusyksikkö tuo näkyviin riippuvuuksien, pääsyoikeuksien, datan käsittelyn ja poik-

keamien hallinnan riskit. Jos nämä näkökulmat kohtaavat toisensa liian myöhään, toimittajasuhteeseen liittyvät ongelmat tulevat näkyviin liian myöhään, usein vasta silloin kun toimittaja on jo valittu tai palvelu on jo käyttöönotettu.

Tästä syystä toimiminen sidosryhmien kanssa ei voi perustua vain siihen, että eri yksiköt pyydetään lausumaan oma kantansa hankinnan loppuvaiheessa tai hankinnan aikana. Kypsässä mallissa kyse on yhteisesti sovitusta mallista ja toimintarakenteesta, jossa olennaiset näkökulmat tulevat huomioiduiksi riittävän aikaisin ja tarkoituksenmukaisella tarkkuudella. Tämän ei pidä tarkoittaa raskasta hallinnollista mallia, vaan selkeää ymmärrystä siitä, missä vaiheessa mikäkin yksikkö tuo lisäarvoa ja missä kohtaa ja miten kaikkien yksiköiden tarpeet varmistetaan. Tietoturvallisuuden näkökulmasta tärkein muutos ei useinkaan ole lisätä kontrollipisteitä, vaan siirtää keskustelu oikeaan kohtaan prosessia. Mitä aikaisemmin toimittajasuhteen vaikutukset dataan, integraatioihin, jatkuvuuteen ja regulaatiovelvoitteisiin tehdään näkyviksi, sitä vähemmän syntyy myöhemmin vaikeita kompromisseja.

Ulkoisten sidosryhmien osalta toimittajahallinta ei tarkoita pelkästään vaatimusten esittämistä toimittajalle. Toimitusketjun tietoturvallisuus rakentuu käytännössä vuorovaikutuksesta, jossa toimittajat, mahdolliset alihankkijat, teknologiapartnerit, asiakkaat ja joissain tilanteissa myös viranomaiset vaikuttavat samaan kokonaisuuteen. Tällöin turvallisuutta ei voida johtaa yksisuuntaisesti. Organisaation on kyettävä paitsi asettamaan vaatimuksia, myös kuuntelemaan, tunnistamaan toimittajien todellisia kyvykkyyksiä ja ymmärtämään, millaiset turvallisuusratkaisut ovat käytännössä toteuttamiskelpoisia. Tämä korostuu erityisesti tilanteissa, joissa toimittaja on markkinassa vahvassa asemassa tai kun kyseessä on tiettyyn erityisosaamiseen perustuva palvelu, jolle ei ole helposti vaihtoehtoja.

Sidosryhmäyhteistyön kannalta yksi aliarvostettu näkökulma on yhteisen turvallisuuskielen rakentaminen. Toimitusketjun ongelmat eivät usein johdu siitä, etteikö joku olisi pitänyt turvallisuutta tärkeänä, vaan siitä, että eri osapuolet ymmärtävät riskit, velvoitteet ja käytännön hallintamekanismit eri tavalla. Kun organisaatio kykenee rakentamaan yhteisen kielen toimittajahallinnan ympärille esimerkiksi sopimuspohjien, vakioitujen vaatimusten, yhteisten käsitteiden ja hallintamallien avulla, vähenee myös epäselvyys siitä, mitä turvallisuus käytännössä tarkoittaa eri osapuolille.

Toimiminen sidosryhmien kanssa on siten toimitusketjun tietoturvallisuuden näkökulmasta ennen kaikkea yhteistyötä ja koordinointia. Se on organisaation kykyä varmistaa, että eri osapuolet eivät toimi irrallaan toisistaan, vaan ovat osana samaa hallittua kokonaisuutta. Ilman tätä kykyä parhaatkin kontrollit, sopimukset ja arviointimallit jäävät helposti sirpaleisiksi.

7.10 Toimittajapoikkeamien hallinta

Toimitusketjuun liittyvien tietoturvapoikkeamien hallinta on yksi niistä osa-alueista, jossa toimittajahallinnan todellinen kypsyys näkyy kaikkein konkreettisimmin. Arvioinnit, sopimukset, auditoinnit ja hallintamallit rakentuvat pitkälti oletukselle, että niiden avulla riskejä voidaan pienentää ja poikkeamien todennäköisyyttä vähentää. Ne eivät kuitenkaan poista sitä tosiasiaa, että toimitusketjuun liittyviä poikkeamia tulee väistämättä tapahtumaan. Tästä syystä toimittajapoikkeamien hallinta ei voi olla organisaatiossa erillinen asia, vaan kriittinen osa organisaation tietoturvapoikkeamien hallinnan ja toimittajahallinnan malleja.

Toimittajapoikkeama voidaan ymmärtää laajemmin kuin pelkästään tietomurtona tai teknisenä turvallisuustapahtumana. Se voi tarkoittaa toimittajan järjestelmään kohdistunutta hyökkäystä, poikkeamaa tietojen käsittelyssä, luvattomia käyttöoikeuksia, palvelun saatavuuteen vaikuttavaa kyberhäiriötä, haavoittuvuuden paljastumista kriittisessä komponentissa tai toimittajan alihankkijaketjussa tapahtunutta poikkeamaa, joka heijastuu asiakkaaseen samoilla edellä mainituilla syillä. Olennaista ei ole poikkeaman tekninen luokittelu, vaan se, että tapahtuma vaikuttaa tai voi vaikuttaa organisaation toimintaan.

Organisaation sisäiset poikkeamat ja toimittajapoikkeamat voivat sinänsä poikkeamana olla hyvin samankaltaisia, mutta toimitusketjun poikkeamat eroavat organisaation omista sisäisistä poikkeamista yhdellä oleellisella tavalla. Organisaatio ei yleensä hallitse poikkeamaa, kaikkia lokitietoja, teknistä tutkintaa tai edes tapahtumaan liittyvän tiedon ajallista saatavuutta itse. Käytännössä organisaatio on riippuvainen siitä, mitä toimittaja tietää, mitä se kertoo, kuinka nopeasti se reagoi ja kuinka avoimesti ja tehokkaasti se kykenee tekemään yhteistyötä. Tämän vuoksi toimittajapoikkeamien hallinnan keskeinen kysymys ei ole vain se, osaako organisaatio käsitellä poikkeamia, vaan myös se, miten se toimii tilanteessa, jossa sen oma kyky ymmärtää ja hallita tapahtumaa riippuu kolmannesta osapuolesta. On myös hyvä ottaa

huomioon, että toimittajalla sattunut poikkeama vaikuttaa todennäköisesti myös muihin asiakkaisiin, jolloin toimittaja saattaa priorisoida toimia tai viestintää sen pohjalta.

Tärkeimmät toimittajapoikkeaman periaatteet määritellään ja ennen poikkeamaa. Organisaatio ei voi rakentaa toimintamallia silloin, kun toimittaja ilmoittaa tietoturvallisuuspoikkeamasta. Poikkeamien hallinnan edellytykset syntyvät etukäteen määritellyistä ilmoitusvelvollisuuksista, yhteyspisteistä, vastuunjaosta, eskalaatiomalleista ja siitä, että toimittajan kanssa on ylipäätään yhteinen käsitys siitä, millaiset tapahtumat ovat olennaisia ja miten niistä viestitään. Tässä mielessä toimittajapoikkeamien hallinta on vahvasti riippuvainen aiemmissa luvuissa käsitellyistä sopimuksellisista, organisatorisista ja elinkaaren aikaisista toimenpiteistä. Toimittajapoikkeamien hallinta ei ole oma erillinen asiansa, vaan se on tilanne, jossa aiemmin rakennettu hallintamalli testataan käytännössä.

Toimiva toimittajapoikkeamien hallinta edellyttää yleensä ainakin neljää kyvykkyyttä. Ensimmäinen on varhainen tunnistaminen. Organisaation on saatava riittävän nopeasti tieto siitä, että toimittajalla on tapahtunut jotain sellaista, joka voi vaikuttaa omaan toimintaan. Tämä voi perustua toimittajan ilmoitukseen, jatkuvaan yhteistyöhön, mediaseurantaan, haavoittuvuustiedotteisiin tai organisaation omaan tilannekuvaan. Erityisesti kriittisten palveluiden ja komponenttien osalta on vaarallista nojata vain siihen, että toimittaja kertoo tapahtumasta riittävän ajoissa. Siksi kypsässä mallissa organisaatio rakentaa myös omaa kykyään tunnistaa toimitusketjuun liittyviä poikkeamasignaaleja muista lähteistä.

Toinen kyvykkyys on vaikutusten arviointi. Kun toimittajapoikkeamasta saadaan tieto, ensimmäinen kysymys ei ole vain mitä on tapahtunut, vaan mitä se merkitsee omalle organisaatiolle. Vaikutusten arvioinnissa on ymmärrettävä, mitä palveluita toimittaja tuottaa, mitä järjestelmiä poikkeama koskee, mitä tietoja on mahdollisesti vaarantunut, onko kyse jatkuvuuteen liittyvästä haasteesta vai luottamuksellisuusriskistä ja mitä regulaatio- tai sopimusvaikutuksia omille asiakkaille tilanteella voi olla. Tämä on usein vaikeampaa kuin sisäisten poikkeamien yhteydessä, koska lähtötieto on epätäydellistä ja muuttuu nopeasti. Siksi vaikutusten arviointia ei voida rakentaa improvisaa-

tion varaan. Organisaatiolla tulee olla jo valmiiksi käsitys siitä, missä palveluissa toimittajariippuvuudet ovat kriittisiä ja millaiset vaikutuspolut niihin liittyvät.

Kolmas kyvykkyys on yhteinen toiminnallinen johtaminen. Toimittajapoikkeaman hallinta ei ole puhtaasti tekninen asia eikä se kuulu pelkästään tietoturvallisuudelle. Poikkeaman vaikutuksesta riippuen mukana voivat olla liiketoiminta, IT, lakiyksikkö, viestintä, hankinta ja merkittävissä tapauksissa yleensä myös organisaation johto. Organisaation on kyettävä muodostamaan riittävän nopeasti yhteinen tilannekuva ja tekemään päätöksiä siitä, mitä toimia tarvitaan: rajoitetaanko integraatioita, katkaistaanko pääsyjä, käynnistetäänkö varajärjestelyt, tehdäänkö viranomaisilmoitus, tiedotetaanko asiakkaita, aktivoidaanko vakuutuksia tai tilataanko apua kolmannelta osapuolelta. Toimittajapoikkeamien erityispiirre on, että toiminnan johtaminen tapahtuu osin oman organisaation ulkopuolella syntyvän tiedon perusteella, mikä korostaa epävarmuuden sietämistä ja päätöksentekoa puutteellisella tiedolla. Usein voi myös olla epäselvää liittyykö poikkeama tietoturvallisuuteen, jolloin joukkoa joudutaan pitämään entistä suurempana varmuuden vuoksi.

Neljäs kyvykkyys on oppiminen ja rakenteellinen palautuminen. Toimittajapoikkeaman hallinta ei pääty siihen, että tekninen ongelma on ratkaistu tai palvelu on palautunut. Poikkeaman jälkeen organisaation on kyettävä arvioimaan, mitä tapahtuma paljasti sen toimittajahallinnan mallista. Oliko toimittajasta riittävä näkyvyys? Toimiko ilmoitusprosessi? Oliko vaikutusten arviointi mahdollista? Oliko sopimukselliset oikeudet riittävät? Oliko toimittajan riskiprofiili ymmärretty oikein? Juuri tällaiset kysymykset tekevät poikkeamasta arvokkaan oppimiskohdan. Ilman jälkiarviointia poikkeamasta tulee vain yksittäinen häiriö, vaikka se voisi toimia koko hallintamallin kehittämisen välineenä.

Toimittajapoikkeamien hallintaan liittyy kuitenkin myös useita rakenteellisia haasteita. Yksi niistä liittyy siihen, että toimittaja tietää usein enemmän omasta poikkeamastaan kuin organisaatio, mutta sillä voi olla samanaikaisesti kannustin rajata viestintäänsä, suojata mainettaan tai välttää keskeneräisen tiedon jakamista. Organisaation näkökulmasta tämä voi näyttäytyä hitaana, niukkana tai epäselvänä tiedonsaantina juuri silloin, kun nopeus ja tarkkuus olisivat kaikkein tärkeimpiä. Tämä ei aina johdu huonosta tahdosta,

vaan myös siitä, että toimittaja itse yrittää ymmärtää tapahtunutta. Silti seuraus on sama: poikkeamaa joudutaan hoitamaan ja päätöksiä tekemään epävarmalla tiedolla.

Toinen haaste liittyy poikkeaman rajapintoihin. Toimittajapoikkeamassa ei aina ole selvää, missä kohtaa toimittajan vastuu päättyy ja asiakkaan vastuu alkaa. Jos haavoittuvuus on toimittajan ohjelmistossa, mutta hyväksikäyttö edellyttää asiakkaan ympäristössä olevia puutteita, vastuunjako ei ole yksiselitteinen. Jos toimittaja ilmoittaa tapahtumasta teknisesti oikein mutta liian myöhään asiakkaan regulaatiovelvoitteisiin nähden, ongelma on yhtä aikaa toimittajan, asiakkaan ja hallintamallin ongelma. Tämän vuoksi toimittajapoikkeamien hallinta ei voi nojata vain jälkikäteiseen syyllisten etsimiseen, vaan sen on perustuttava etukäteen rakennettuun toimintatapaan, jossa myös epäselvät rajapinnat on mahdollisuuksien mukaan tunnistettu.

Kolmas haaste liittyy mittakaavan ja laajoihin vaikutuksiin. Yksittäinen toimittajapoikkeama voi olla hallittavissa, mutta modernissa ympäristössä sama tapahtuma voi vaikuttaa samanaikaisesti useisiin toimittajiin, palveluihin tai liiketoimintaprosesseihin. Esimerkiksi laajasti käytetyn ohjelmistokomponentin haavoittuvuus tai suuren pilvipalvelutoimittajan häiriö voi synnyttää tilanteen, jossa poikkeamien hallinta ei enää ole yksittäisen toimittajasuhteen operatiivinen tehtävä, vaan laaja toimitusketjun häiriö. Tällaisissa tilanteissa korostuu ennakolta rakennettu käsitys kriittisistä riippuvuuksista ja organisaation liiketoimintajatkuvuuden käytännöistä. Organisaatio, joka tietää etukäteen, mihin sen toiminta perustuu, pystyy poikkeamatilanteessa reagoimaan huomattavasti nopeammin kuin organisaatio, joka yrittää kriisin hetkellä kartoittaa, mihin kaikkeen poikkeama on vaikuttanut.

Toimittajapoikkeamien hallinnassa voidaan tunnistaa myös kypsyystasoja. Alkeellisimmassa mallissa organisaatio reagoi poikkeamiin tapauskohtaisesti ja pitkälti toimittajan antaman tiedon varassa. Kehittyneemmässä mallissa organisaatiolla on valmiit yhteyspisteet, vaikutusarviointimallit ja eskalaatiopolut keskeisille toimittajille. Kypsimmillään toimittajapoikkeamien hallinta on osa laajempaa toimitusketjun tilannekuvaa, jossa toimittajat eivät ole vain passiivisia ilmoitusvelvollisia, vaan osa organisaation jatkuvuutta ja resiliensiä tukevaa verkostoa. Tällöin poikkeamien hallinta muuttuu reagoinnista kyvyksi ennakoida, harjoitella ja rakentaa vaihtoehtoisia toimintamalleja etukäteen.

Näistä näkökulmista toimittajapoikkeamien hallinta voidaan nähdä toimitusketjun tietoturvallisuuden kypsyyden mittarina. Siinä paljastuu, onko aiemmin rakennettu hallintamalli aidosti toimiva vai ainoastaan muodollisesti olemassa. Jos toimittajan kriittinen tietoturvallisuusongelma johtaa viivästyneeseen tiedonkulkuun, epäselvään vaikutusarviointiin, sisäiseen sekavuuteen ja päätöksenteon halvaantumiseen, ongelma ei ole vain toimittajassa. Se on myös organisaation omassa kyvyssä johtaa toimitusketjuaan ja omia toimintojaan poikkeamatilanteessa.

Samalla toimittajapoikkeamien hallinta tarjoaa yhden tärkeimmistä mahdollisuuksista kehittää koko toimitusketjun hallintaa. Jokainen merkittävä poikkeama pakottaa organisaation tarkastelemaan uudelleen sitä, miten se valitsee toimittajansa, miten se rakentaa sopimuksensa, miten se määrittää kontrollinsa ja miten se ymmärtää omat riippuvuutensa toimittajiin. Se näyttää, mitkä osat toimitusketjun tietoturvallisuuden hallinnasta ovat aidosti kestäviä, ja mitkä ovat jääneet liian optimististen oletusten varaan.

Toimittajapoikkeamien hallinnan tavoite ei siten ole rakentaa mallia, jossa kaikki poikkeamat voidaan estää tai jossa kaikkiin tilanteisiin olisi täydellinen käsikirjoitus. Tavoitteena on rakentaa organisaatiolle kyky toimia järkevästi, nopeasti ja hallitusti tilanteissa, joissa merkittävä osa tapahtumasta on oman välittömän kontrollin ulkopuolella. Juuri tämä tekee siitä yhden toimitusketjun tietoturvallisuuden hallinnan vaativimmista mutta myös tärkeimmistä osa-alueista.

8 Yhteenveto

Tämän työn keskeisenä lähtökohtana on toiminut havainto siitä, että toimitusketjut eivät ole enää organisaation toiminnan taustarakenteita, vaan liittyvät olennaisesti organisaation turvallisuuteen, liiketoiminnan jatkuvuuteen ja organisaation kykyyn tuottaa arvoa. Toimitusketjun tietoturvallisuuden hallinnan merkitys on kasvanut samalla kun organisaatioiden riippuvuus ulkoisista palveluista, teknologiatoimittajista, ohjelmistokomponenteista ja kumppaneista on syventynyt. Samalla myös tietoturvallisuuden rooli on muuttunut. Sitä ei voida enää tarkastella vain organisaation sisäisten järjestelmien, käyttäjien ja kontrollien hallintana, vaan yhä enemmän sitä pitää tarkastella osana laajempaa kokonaisuutta, joka ulottuu toimitusketjun läpi.

Työn ensimmäinen keskeinen johtopäätös on, että toimitusketjun tietoturvallisuus ei ole irrallinen osa-alue, vaan sen pitää olla osa organisaation kokonaisvaltaista turvallisuuden hallintaa. Toimitusketjun kautta syntyvät riskit voivat samanaikaisesti vaikuttaa liiketoiminnan jatkuvuuteen, tietojen luottamuksellisuuteen, liiketoiminnan jatkuvuuteen, regulaatiovelvoitteiden täyttämiseen ja organisaation maineeseen. Juuri tästä syystä toimitusketjun tietoturvallisuuden hallintaa ei tulisi nähdä vain hankinnan, IT:n tai tietoturvallisuusyksikön tehtävänä, vaan korkeamman tason asiana. Sen tulisi olla kriittisessä osassa organisaation kykyä ymmärtää omia riippuvuuksiaan ja hallita niitä tietoisesti.

Toinen keskeinen havainto liittyy siihen, että toimintaympäristön muutos on tehnyt toimitusketjuista aiempaa vaikeammin hahmotettavia. Digitaaliset toimitusketjut rakentuvat useista toisiinsa kytkeytyvistä palveluista, rajapinnoista ja alihankintarakenteista, jotka eivät useinkaan näy suoraan organisaatiolle. Organisaatiolla voi olla hyvä näkyvyys omiin suoriin toimittajiinsa, mutta huomattavasti heikompi näkyvyys siihen, minkälaisiin teknologioihin, pilvipalveluihin, ohjelmistokomponentteihin tai muihin toimijoihin nämä nojaavat. Työssä on pyritty osoittamaan, että tämä näkyvyyden puute ei ole vain

operatiivinen ongelma, vaan yksi toimitusketjujen tietoturvallisuuden hallinnan rakenteellisista ydinhaasteista. Kaikkea ei voida tunnistaa eikä kaikkea voida hallita suoralla kontrolleilla. Siksi tehokas toimittajien tietoturvallisuuden hallinta ei perustu täydellisyyden tavoitteluun, vaan kykyyn tunnistaa ne riippuvuudet, joilla on eniten merkitystä organisaation toiminnalle ja ennakoida haasteita mahdollisimman tehokkaasti.

Työ tuo esiin myös sen, että toimitusketjun tietoturvallisuuden vaatimuksia ohjaa yhä vahvemmin erinäiset kansainväliset regulaatiot ja sen hallintaa erinäiset tietoturvallisuusstandardit. NIS2, CRA, CMMC 2.0 ja muut regulatiiviset mallit ohjaavat kaikki samaan suuntaan: organisaation ei enää katsota voivan rajata vastuutaan vain omiin sisäisiin prosesseihinsa, vaan sen on kyettävä hallitsemaan myös toimittajiin ja palveluketjuihin liittyviä tietoturvallisuusriskejä. Toimitusketjuvaatimusten ilmestymistä regulaatioon ei kannata tulkita vain velvoittava, raskaana asiana. Se kannattaa tulkita merkkinä siitä, että toimitusketjun tietoturvallisuus on siirtynyt parhaiden käytäntöjen alueelta kohti odotettua normaalia johtamiskäytäntöä.

Työssä tunnistettiin useita käytännön haasteita, jotka vaikeuttavat toimitusketjun tietoturvallisuuden hallintaa organisaatioissa. Toimittajahallinnan vastuut ovat usein hajautuneita, riskiperusteisuus jää käytännössä usein puutteelliseksi, toimittajien kyvykkyydet vaihtelevat merkittävästi ja sopimuksellisten vaatimusten sekä käytännön toteutuksen väliin jää usein selvä kuilu. Yksi työn läpi kulkeva ajatus onkin ollut, että toimitusketjun tietoturvallisuuden haasteet eivät johdu ensisijaisesti yksittäisten kontrollien puutteesta, vaan kyvystä rakentaa johdonmukainen, realistinen ja käytännössä toimiva hallintamalli. Ongelma ei useimmiten ole se, etteikö organisaatio tietäisi, mitä hyvät käytännöt teoriassa tarkoittavat, vaan se, että tämä tieto ei muutu saumattomasti päätöksenteoksi, sopimiseksi, arvioinniksi ja jatkuvaksi ohjaukseksi, jota organisaation eri osat toteuttavat ja johon kaikki osallistuvat.

Työn tärkein havainto on se, että toimitusketjun tietoturvallisuuden hallinta kannattaa rakentaa riskiperusteisesti, modulaarisesti ja organisaation omaan toimintaympäristöön suhteutettuna. Kaikkia toimittajia ei voida eikä kannata hallita samalla tavalla. Kaikilta ei voida vaatia samaa dokumentaatiota, samaa kypsyystasoa tai samoja sopimuksellisia vaatimuksia. Jotta modulaarisuus olisi mahdollista, organisaation on pakko rakentaa ja jalkauttaa prosessit,

jossa toimittajat voidaan kategorisoida, riskiprofiloida ja eri toimittajiin voidaan kohdistaa oikeanlaisia toimenpiteitä. Tämä mahdollistaa sen, että organisaatio voi kohdistaa rajalliset resurssinsa sinne, missä riskit ovat suurimmat, ja samalla säilyttää riittävän joustavuuden myös niissä tilanteissa, joissa toimittajavaihtoehdot ovat rajatumpia.

Työssä esitettyjen käytännön suositusten ytimessä on ajatus siitä, että toimittajaa ei tule arvioida vain toimittajana, vaan syntyvänä riippuvuussuhteena. Tämä on yksi työn keskeisimmistä näkökulmista. Toimittajasuhteen turvallisuus ei määräydy vain sen perusteella, millainen toimittaja on yleisellä tasolla, vaan ennen kaikkea sen perusteella, miten palvelu kytkeytyy organisaation ympäristöön, mitä tietoa palvelun osana käsitellään, minkälaisia käyttöoikeuksia se vaatii ja miten palvelun muutokset, poikkeamat ja päättyminen hallitaan. Tämä siirtää tarkastelun pois yksittäisistä kyselylomakkeista kohti laajempaa riippuvuuksien suunnittelua ja hallintaa.

Sopimusten osalta työn johtopäätös on, että sopimuksellinen ohjaus on välttämätön, mutta ei yksin riittävä väline. Sopimukset, tietoturvallisuusliitteet ja vaatimuspohjat ovat tärkeitä, koska ne tekevät näkyväksi odotukset, vastuut ja oikeudet. Niiden todellinen arvo syntyy kuitenkin vasta silloin, kun ne kytkeytyvät osaksi elinkaaren aikaista hallintaa, auditointia, sidosryhmäyhteistyötä ja poikkeamien hallintaa. Työssä on korostettu myös sitä, että tietoturvallisuusvaatimuksia ei tulisi rakentaa irrallisiksi, vaan ne on perusteltua pohjata samaan hallintamalliin, jota organisaatio itse noudattaa, esimerkiksi ISO/IEC 27001 -viitekehykseen. Tällöin toimittajilta ei vaadita satunnaisia tai historiallisesti kerrostuneita asioita, vaan läpi toimitusketjun yhteensopivia käytäntöjä.

Toimittajasuhteen elinkaaren tarkastelu tuo yhteen työn ehkä kaikkein käytännöllisimmän opetuksen: toimittajahallinta ei ole kertaluonteinen hyväksyntä tai hallinnollinen tarkistus, vaan jatkuva prosessi. Uuden toimittajan arviointi on tärkeä, mutta todelliset riskit muuttuvat usein vasta toimittajasuhteen aikana. Palvelut laajenevat, integraatiot syvenevät, alihankkijaketjut muuttuvat ja riippuvuudet kasvavat. Siksi toimittajien hallinnan on jatkuttava koko suhteen ajan aina toimittajan käyttöönotosta sopimuksen päättämiseen saakka. Tämä edellyttää sekä määrämuotoisia käytäntöjä että kykyä havaita muutoksia ja reagoida niihin oikealla tavalla ja oikeaan aikaan.

Työssä käsitellyt auditoinnit, sidosryhmäyhteistyö ja toimittajapoikkeamien hallinta muodostavat käytännössä testin hallintamallille. Auditointi osoittaa, onko vaatimuksia käytännössä olemassa ja jalkautettu. Sidosryhmäyhteistyö paljastaa, kykeneekö organisaatio toimimaan johdonmukaisesti yli organisatoristen rajojen. Toimittajapoikkeamien hallinta taas näyttää, onko etukäteen rakennettu malli aidosti toimintakykyinen silloin, kun toimitusketjussa tapahtuu jotakin odottamatonta. Näissä tilanteissa toimitusketjun tietoturvallisuus lakkaa olemasta papereiden läpikäymistä ja muuttuu operatiiviseksi todellisuudeksi.

Tämän työn tärkein johtopäätös on, että hyvä toimitusketjun tietoturvallisuuden hallinta ei synny täydellisistä prosesseista, vaan johdonmukaisista periaatteista. Organisaation ei tarvitse nähdä kaikkea, tarkistaa kaikkea tai vaatia kaikkea kaikilta. Sen on kuitenkin tiedettävä, mitä se pitää tärkeänä, miten se erottaa olennaisen epäolennaisesta ja millä tavoin se muuntaa tämän ymmärryksen toimittajavalinnoiksi, sopimuksiksi, arvioinneiksi, kontrollimekanismeiksi ja poikkeamatilanteiden toiminnaksi.

Lopuksi voidaan todeta, että on todennäköistä, että toimitusketjujen merkitys organisaatioiden turvallisuudelle tulee jatkossa edelleen kasvamaan. Teknologiset riippuvuudet syvenevät, regulaatio lisääntyy ja toimitusketjut muuttuvat yhä verkostomaisemmiksi. Tämä tarkoittaa, että toimitusketjun tietoturvallisuus ei ole ohimenevä teema, vaan pysyvä osa organisaatioiden toimintaympäristöä. Organisaatioiden kannalta ratkaisevaa ei ole se, kohtaavatko ne toimitusketjuun liittyviä tietoturvallisuushaasteita, vaan se, kuinka valmiita ne ovat ymmärtämään ne, johtamaan niitä ja oppimaan niistä. Tässä mielessä toimitusketjun tietoturvallisuuden hallinta on ennen kaikkea kokonaisvaltainen, organisaation läpileikkaava toimintatapa – ei yksittäinen kontrolli, prosessi tai dokumentti.

9 Lähteet

Christopher & Peck (2004) - *Building the Resilient Supply Chain*, International Journal of Logistics Management, Vol. 15, No. 2, pp1-13, 2004, haettu: https://www.researchgate.net/publication/228559011_Building_the_Resilient_Supply_Chain

Ivanov & Dolgui (2020) - *A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0,* Production Planning & Control, haettu: https://sce.carleton.ca/faculty/wainer/papers/A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4 0.pdf

Suresh, Sanders & Braunscheidel - *Business Continuity Management for Supply Chains Facing Catastrophic Events,* IEEE Engineering Management Review, Vol. 48, No. 3, 2020, haettu: https://par.nsf.gov/servlets/purl/10229443

Van't Schip (2024) – *The Regulation of Supply Chain Cybersecurity in the NIS2 Directive in the Context of the Internet of Things,* European Journal of Law and Technology, Vol. 15 No. 1, haettu: https://mail.ejlt.org/index.php/ejlt/article/download/989/1085?

NIS2 (2022) – *EU Direktiivi 2022/2555*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32022L2555

2025 Data Breach Investigations Report - https://www.verizon.com/business/resources/reports/dbir/

Threat Landscape for Supply Chain Attacks - https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Case Maers 2018 - https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

NIST 2021 - https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity

Reuters 2026 - https://www.reuters.com/world/china/beijing-tells-chinese-firms-stop-using-us-israeli-cybersecurity-software-sources-2026-01-14/

Case SolarWinds 2020 - https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

Kuva 1 - https://www.itsm-docs.com/blogs/cobit-framework/cobit-apo10-04-manage-vendor-risk

9.1