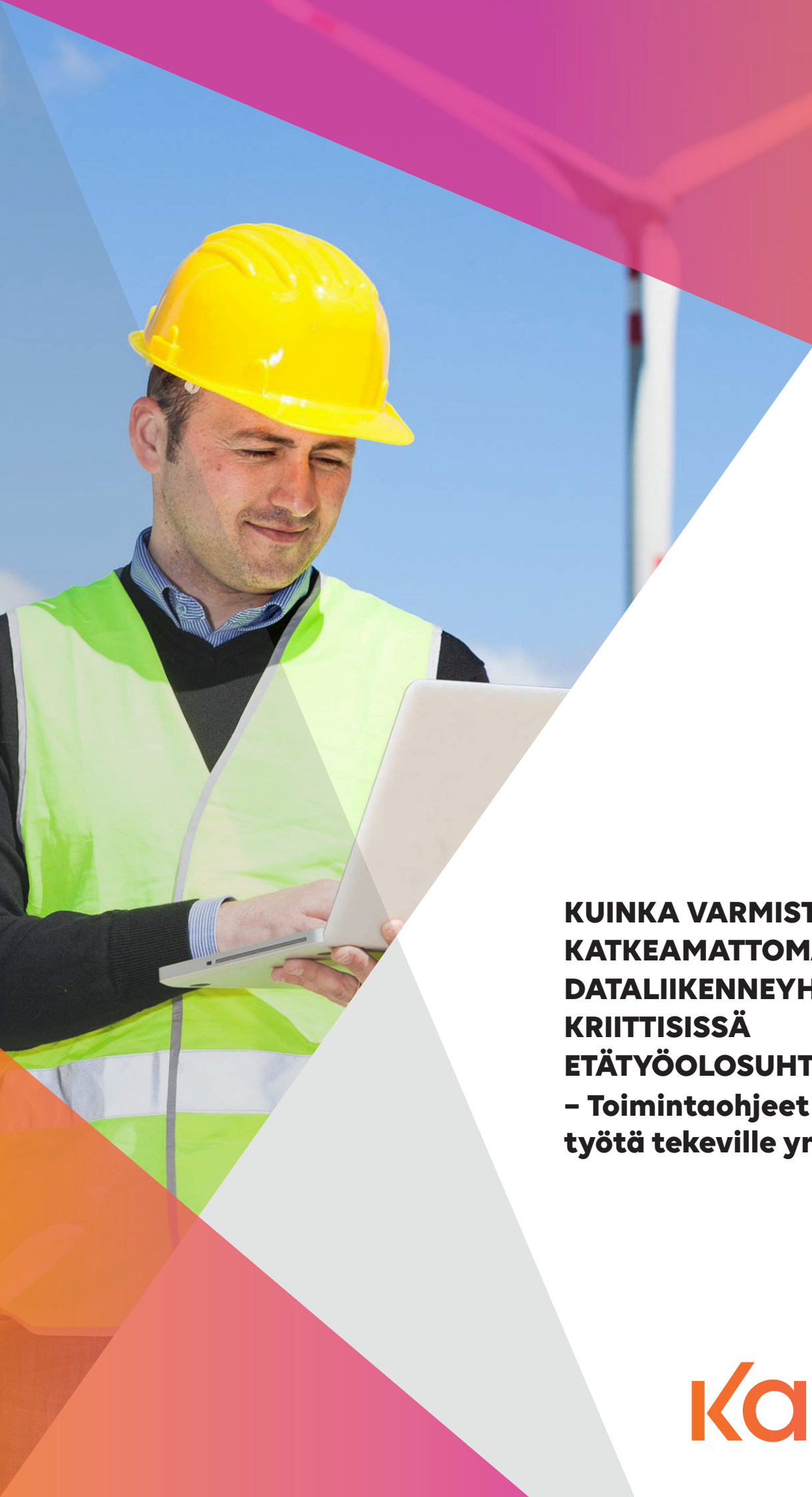
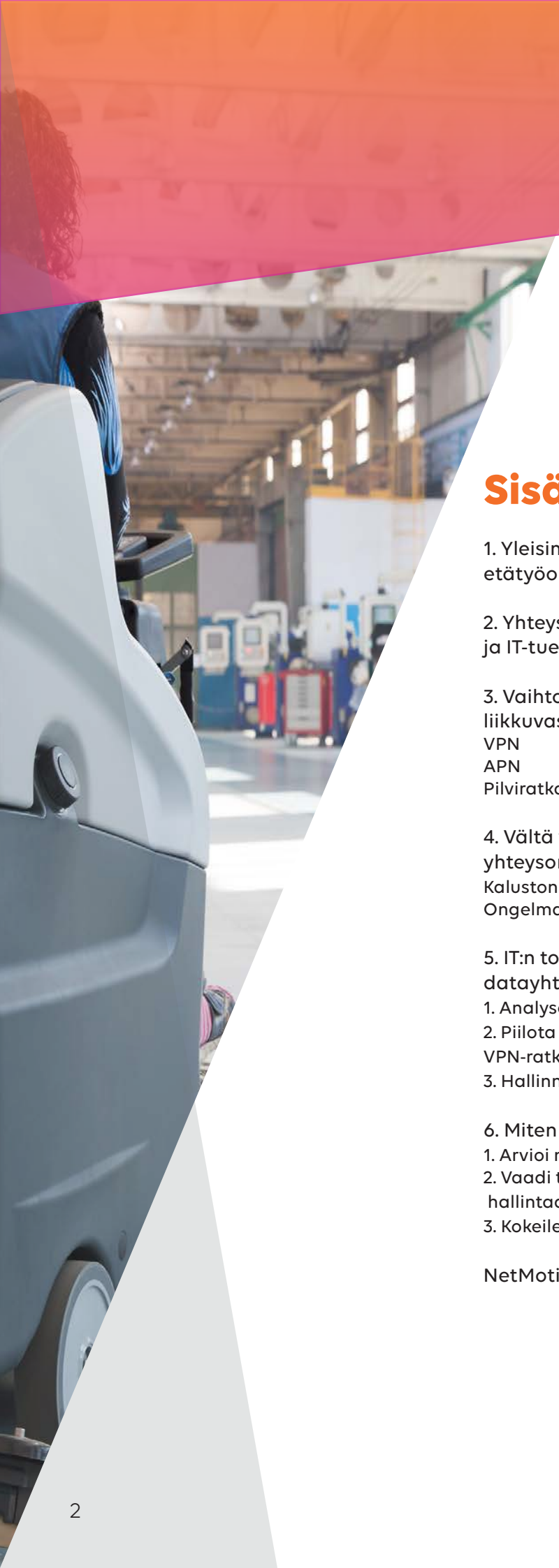
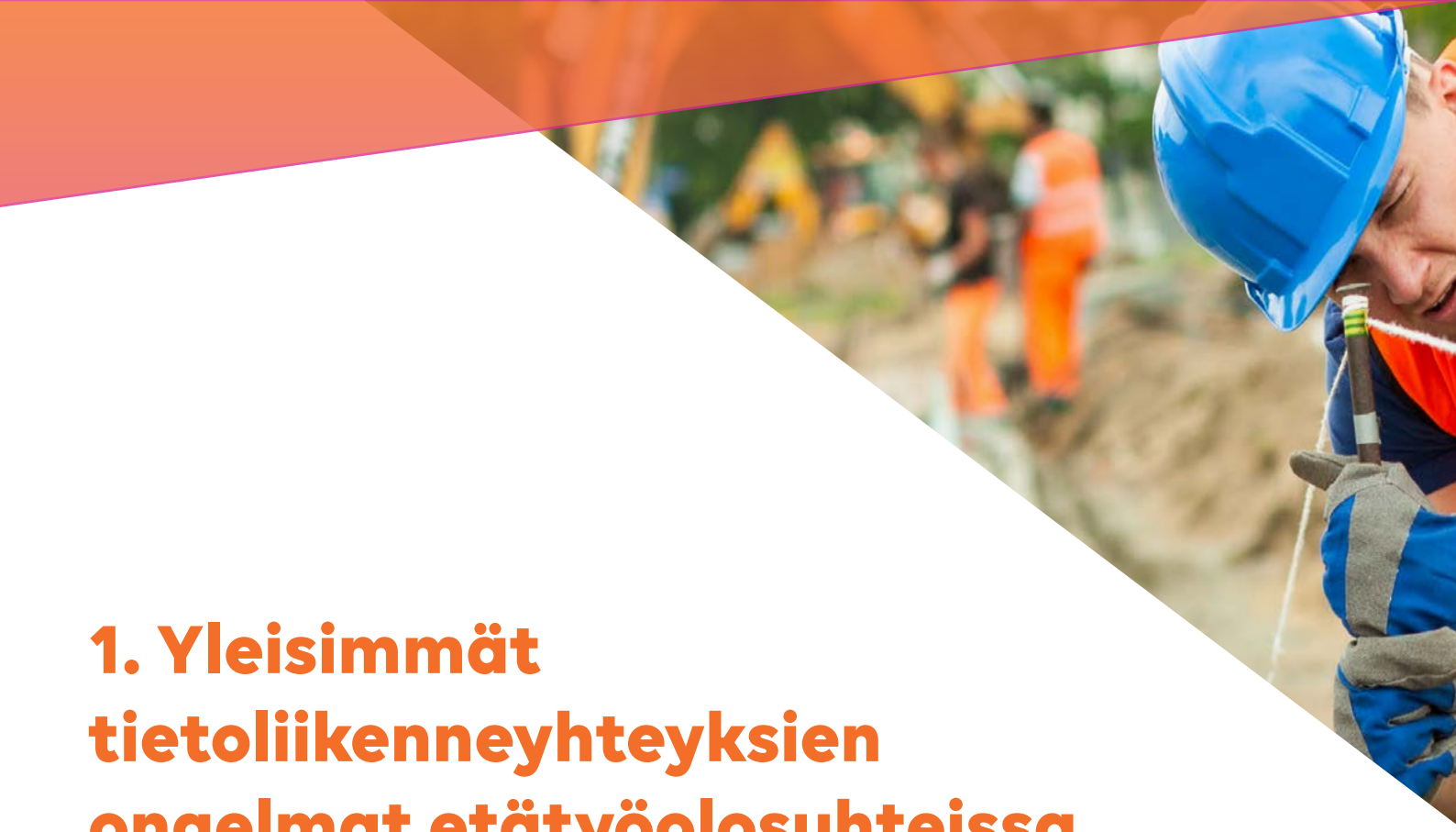


KUINKA VARMISTAT KATKEAMATTOMAT DATALIIKENNEYHTEYDET KRIITTISISSÄ ETÄTYÖOLOSUHTEISSA – Toimintaohjeet liikkuvaa työtä tekeville yrityksille

Kauko



Sisällys



1. Yleisimmät tietoliikenneyhteyksien ongelmat etätyöolosuhteissa

Etätyöskentely haastavissa olosuhteissa tai verkon katvealueilla näkyy niin, että tietoliikenneyhteyksissä esiintyy häiriöitä. Tällaisia katvealueita löytyy mm. maastosta, metsästä, mereltä ja suurilta työmailta. Myös varasto tai tuotantolaitos voi olla haasteellinen ympäristö verkon kannalta, sillä esimerkiksi varastotilassa säilytettävä suuri teräsmassa tai selluloosapaalit heikentävät yhteyksiä. Lisäksi rakennuksen rakenteet, kuten teräsbetonista rakennetut seinät tai kantavat tolpat, vaikuttavat tietoliikenneyhteyksiin.

Kun kenttätyöntekijä kohtaa yhteysongelmia käyttäessään langattomia verkkoja, koetaan usein, että päätelaitteessa on vikaa, tai että ongelma on operaattorin verkossa. Yhteysongelmien monimutkaisuuden ja niiden selvittelyn haasteellisuuden takia käyttäjä osaa harvoin suoraan syyttää pieniä katkoksia tietoliikenneyhteyksissä. Kun kenttätyöntekijä myöhemmin kertoo ongelmasta IT-tukeen, aletaan myös silloin ongelman syytä ja siten myös ratkaisua etsiä usein ensin käytettävästä laitteesta ja sen jälkeen operaattorin verkosta tai langattoman verkon ylläpitäjästä.

Haastavan työympäristön lisäksi nopeasti liikkuva työpiste saattaa aiheuttaa yhteysongelmia. Kun päätelaite liikkuu kohtalaista vauhtia, signaalin vahvuudet vaihtelevat merkittävästi yhteyden hyppiessä voimakkaamman signaalin perässä tukiasemalta toiselle. Verkkoa tarvit-seva päätelaite ei välttämättä pysykään vauhdissa mukana sen liikkuessa esimerkiksi trukin kyydissä WLAN-verkossa, tai jos työntekijä liikkuu päätelaitteen kanssa junassa 3G-verkossa. Tällainen tukiasemalta toiseen hyppiminen aiheuttaa pieniä yhteyskatkoksia ja yhteyden hetkellinen menettäminen herkimpien sovellusten kohdalla voi tarkoittaa, että ne eivät enää palaudu toimintakykyisiksi ilman laitteen uudelleen käynnistämistä.

Myös hyvän tietoturvan varmistaminen tuo omat haasteensa tietoliikenneyhteyksiin. Vaativa työ, jossa toimivat tietoliikenneyhteydet ovat kriittisessä osassa työn onnistumisen kannalta, edellyttää usein myös huipputason tietoturvaa. Tietoturvan varmistaminen saattaa kuitenkin hidastaa heikkoja datayhteyksiä entisestään. Pahimmillaan perinteiset ratkaisut, kuten kömpelöt VPN-sovellukset, laskevat käytettävyyden tasoa niin, että heikkoa yhteyttä ei voida hyödyntää enää ollenkaan.

Se, vaikuttavatko nämä pienet katkokset käyttäjän työskentelyyn, riippuu usein siitä, mikä käyttöjärjestelmä on käytössä ja kuinka herkästi käytössä olevat sovellukset reagoivat yhteyskatkoksiin. Esimerkiksi tietyt toiminnanohjausjärjestelmät (Enterprise Resource Planning, ERP) ovat herkkiä muutoksille verkossa. Niinpä ERP:n pätkiminen varastoympäristössä voikin olla monen yrityksen arkipäivää: katkoksen tapahtuessa näytölle tulee virheilmoitus, jolloin työntekijän täytyy pahimmillaan sulkea ja avata ohjelmat uudestaan, sekä kirjautua takaisin sisään järjestelmään.

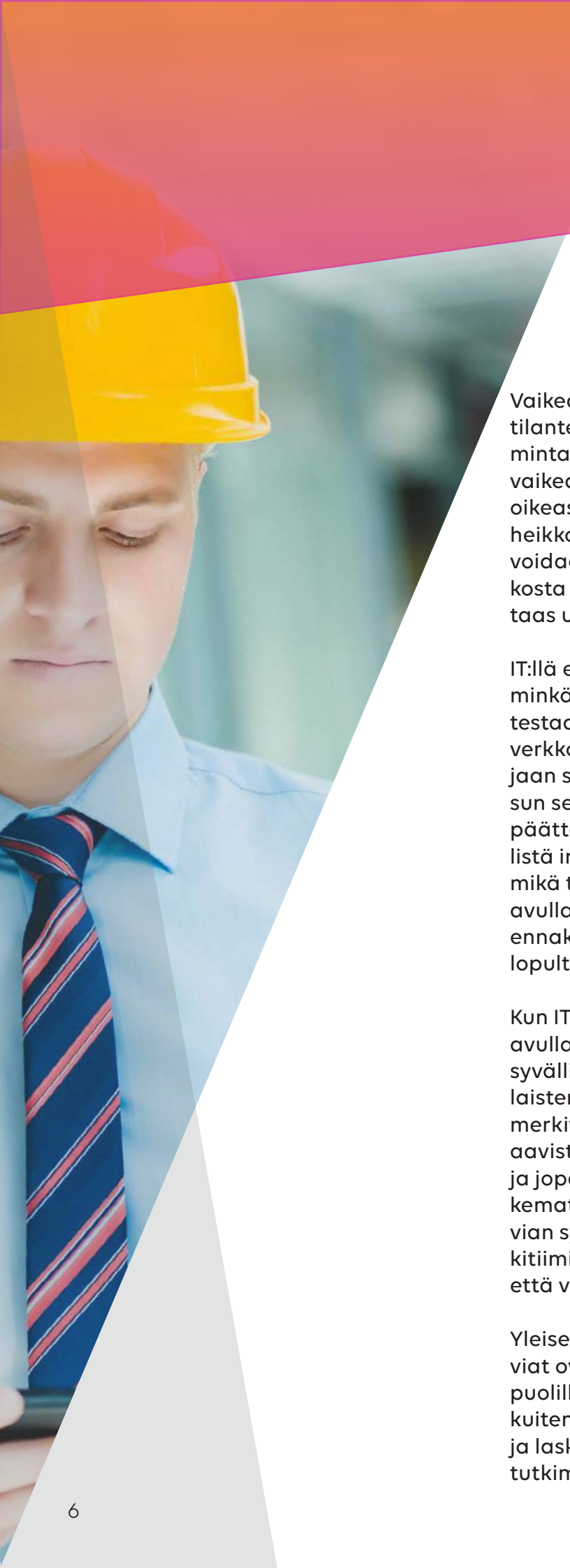
2. Yhteysongelmien vaikutus liiketoimintaan ja IT-tuen arkeen

Kun kyseessä on työtehtävä, jonka tekeminen vaatii yhteyden järjestelmään, kuten käytettävistä päätelaitteista yrityksen palvelimelle, ei työntekijä yhteyksien pätkiessä voi suorittaa tehtäviään tehokkaasti tai ollenkaan. Työntekijälle tämä tarkoittaa sitä, että hänen täytyy pahimmillaan sulkea käytössä oleva laite, avata se uudestaan ja mahdollisesti odottaa useita minuutteja järjestelmän turvallisuussääntöjen takia, ennen kuin voi kirjautua takaisin sisään.

Ongelmat ovat työntekijän kannalta turhauttavia, mutta kriittisessä työssä tämänkaltaiset katkokset ja ongelmat esimerkiksi VPN-yhteyksien kanssa voivat aiheuttaa mm. sairaaloissa ja lentokentillä vaikeita tilanteita. Jos työntekijä ei pääse tarkastelemaan kriittistä informaatiota, ei voi tehdä tarvittavia kirjauksia tai joutuu tekemään kirjaukset useaan otteeseen menetettyään katkoksen takia tallentamattoman työn, voi katkoksien aiheuttamat viivästykset käydä yritykselle kalliiksi.

Tämä haaste näkyykin myös työn raportoinnissa. Mikäli yrityksellä on palvelutasosopimus eli SLA (Service Level Agreement), jossa on määrätty, että asiakkaalle tehtävän työn täytyy olla valmis ja raportoitu tietyn ajan kuluessa, voi myöhästyminen tarkoittaa yritykselle sakon kaltaisia sanktioita. Tietoliikenneyhteyksissä ilmenneistä ongelmista huolimatta työntekijä onkin saattanut saada asiakkaalle tehtävän työn valmiiksi ajallaan, mutta ei pysty raportoimaan sitä verkon ongelmien takia.

Näillä ongelmilla on suora vaikutus liiketoimintaan, mutta ne aiheuttavat kustannuksia myös IT-tuessa, joka kuormittuu jokaisen pienen yhteyskatkoksen myötä tehdystä virheilmoituksesta ja korjauspyynnöstä. Tämänkaltaisten tikettien laatu on usein heikko, sillä itse ongelmasta, tapahtuman ajankohdasta ja muista muuttujista harvoin saadaan tarpeeksi täsmällistä tietoa. Lisäksi tikettien valtavan määrän vuoksi voi olla ylivoimaisen raskasta lähteä selvittämään, mistä yhteyden ongelmat tarkalleen johtuvat.

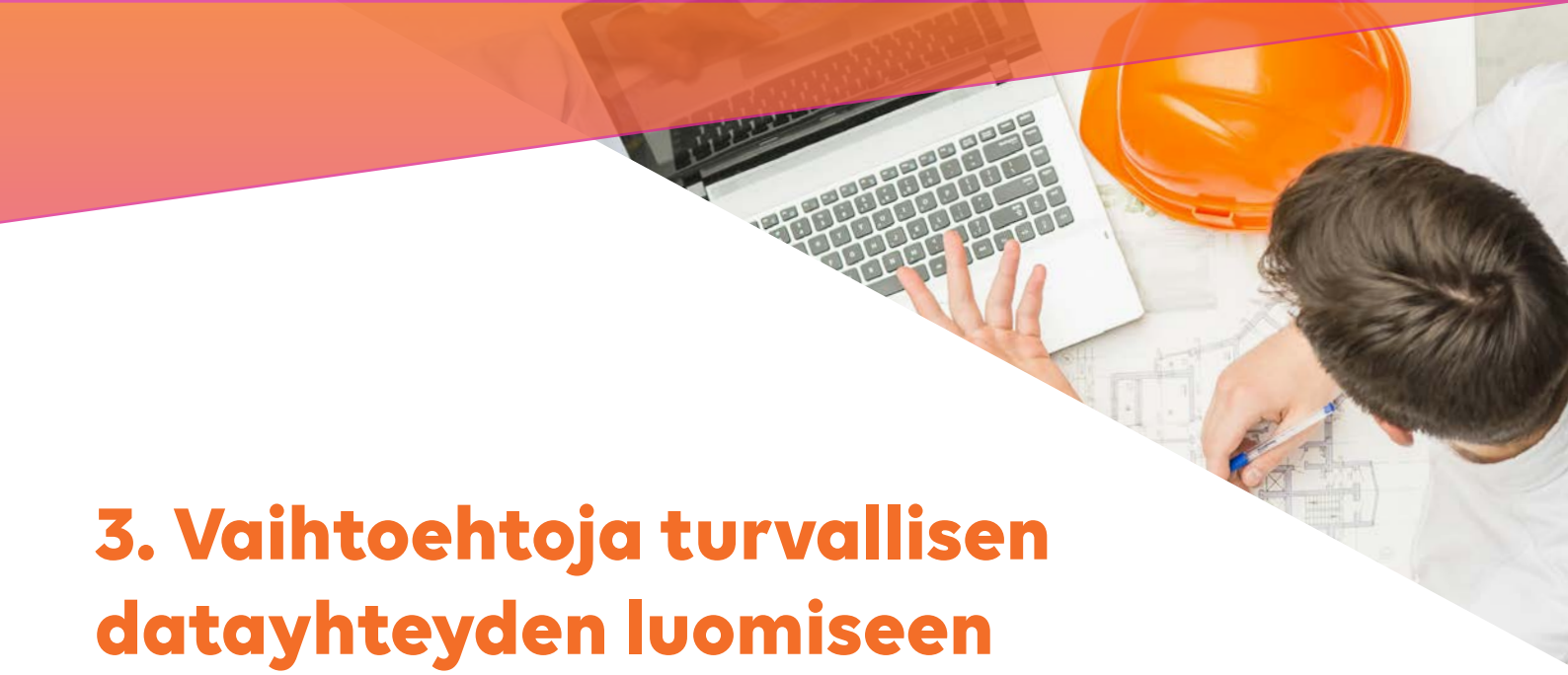


Vaikeasti selvitettäviä tikettejä ovat esimerkiksi tilanteet, joissa käyttäjä ilmoittaa, että ERP:n toiminta keskeytyy jatkuvasti kentällä. IT-tuen on hyvin vaikea lähteä selvittämään, mistä ongelmassa on oikeasti kyse: onko kyseessä ohjelmavika, laitevika, heikko signaali vai jokin muu häiriö. Jos kuitenkin voidaan osoittaa, että kyse on nimenomaan heikosta tietoliikenneyhteydestä, on taustasyitä siihen taas useita ja ongelman ratkaiseminen haastavaa.

IT:llä ei usein ole näkyvyyttä operaattorin verkkoihin, minkä takia ongelmaa joudutaan usein etsimään testaamalla kentällä eri laitteita ja operaattoreiden verkkoja. Myös verkon ylläpitäjään ja laitevalmistajaan saatetaan joutua olemaan yhteydessä. Ratkaisun selvittämiseen voikin mennä päiväkausia, jonka päätteeksi ei kuitenkaan välttämättä saada täsmällistä informaatiota vian aiheuttajasta tai siitä, että mikä täsmälleen oli lopulta se toimenpide, jonka avulla ongelma korjattiin. On siis lähes mahdotonta ennakoida kuinka kauan ongelman selvittäminen lopulta kestää ja voidaanko sen lähdettä selvittää.

Kun IT-tuella ei ole käytössään teknologiaa, jonka avulla tietoliikenneongelmiin voitaisiin pureutua syvällisesti ja täsmällisesti, korostuu IT-ammattilaisten henkilökohtaisen osaamisen ja kokemuksen merkitys. Kokenut IT-tuen työntekijä saattaa pystyä aavistamaan jo aikaisessa vaiheessa mistä on kyse ja jopa missä ketjun kohdassa on vika, kun taas kokemattomampi ei välttämättä osaa edes arvuutella vian syytä. Tämä asettaa omat vaatimuksensa IT-tukitiimin kokoamiselle ja voi vaikuttaa myös siihen, että voiko IT-tukea ulkoistaa.

Yleisesti epämääräisiin yhteysongelmiin liittyvät viat ovat aikaa vieviä ja vaivalloisia kaikille osapuolille. Verkon häiriöihin liittyvät haasteet ovat kuitenkin päivittäisiä ja jatkuvia ongelmia IT-tuelle ja laskevat tehokkuutta, kun heikkolaatuisen tiketin tutkimiseen hukkaantuu kallisarvoisia työtunteja.



3. Vaihtoehtoja turvallisen datayhteyden luomiseen liikkuvassa työssä

VPN

VPN-verkon (Virtual Private Network) avulla yrityksen verkkoja voidaan yhdistää kaksi tai useampia suojatusti julkisen verkon yli. Koska VPN hyödyntää julkista verkkoa, tiedonsiirtonopeus ei kärsi siksi, että kaista ei riittäisi. Esimerkiksi etätyössä tai kentällä työntekijät ottavat yleensä yhteyden työnantajan verkkoon VPN:n avulla.

Käyttäjä avaa VPN-yhteyden käynnistämällä sovelluksen, joka ottaa yhteyttä kohdeverkon palvelimeen ja suorittaa tunnistautumisen esimerkiksi käyttäjätunnuksella ja salasanalla. VPN-verkon yksityisyys ja tietoturva varmistetaan salauksella: tieto kryptataan salaiseksi paketiksi, joka kulkee suojattuna päätelaitteelta verkon läpi yrityksen sisäverkkoon asti, jossa paketti vasta voidaan purkaa.

Liikkuvassa työssä perinteinen VPN on ongelmallinen, sillä sitä ei olla suunniteltu mobiiliin ympäristöön. Ennen kuin VPN avaa tunnelin päätelaitteen ja kotipalvelimen välille, vaaditaan pisteiden välillä "kättely", joka voi tarkoittaa tunnistautumista, kuten salasanan antamista. Yhteyden avaaminen voi viedä aikaa ja jos verkko katkeaa, täytyy kättely tehdä aina uudestaan.

Tietoturvan takaamiseksi VPN saattaa katkaista yhteyden heti, kun verkossa tapahtuu katkoksia tai esiintyy ongelmia. VPN-yhteydelle staattisuus on tärkeää ja mobiilius asettaa sille yhä enemmän haasteita, sillä liikkuvassa työssä verkossa tapahtuu muutoksia jatkuvasti. Joten, vaikka yhteys voitaisiinkin avata ilman tunnistautumista, ilmoittaa VPN käytetyille ohjelmistoille yhteyskatkoksesta, mikä taas voi aiheuttaa lukemattomia ongelmia sovellusten käytettävyyteen. Pahimmillaan katkoksen yhteydessä esimerkiksi toiminnanohjausjärjestelmä voikin lakata toimimasta kokonaan.

APN

APN (Access Point Name) on operaattorin tarjoama yksityinen verkko. APN on varsin yleisesti käytetty ratkaisu esimerkiksi logistiikassa, terveydenhuollossa ja kotisairaanhoidossa. Operaattorin tarjoaman maksullisen yksityisen putken ideana on, ettei dataliikenne käy missään vaiheessa avoimen internetin puolella. Sitä käytettäessä ei siis tarvita erillistä suojausta, sillä operaattori on jo suojannut verkkoympäristön. APN:n avulla pysytäänkin koko ajan oman yrityksen sisäverkossa, vaikka liikuttaisiinkin fyysisesti muualla kuin työpaikan sisällä.

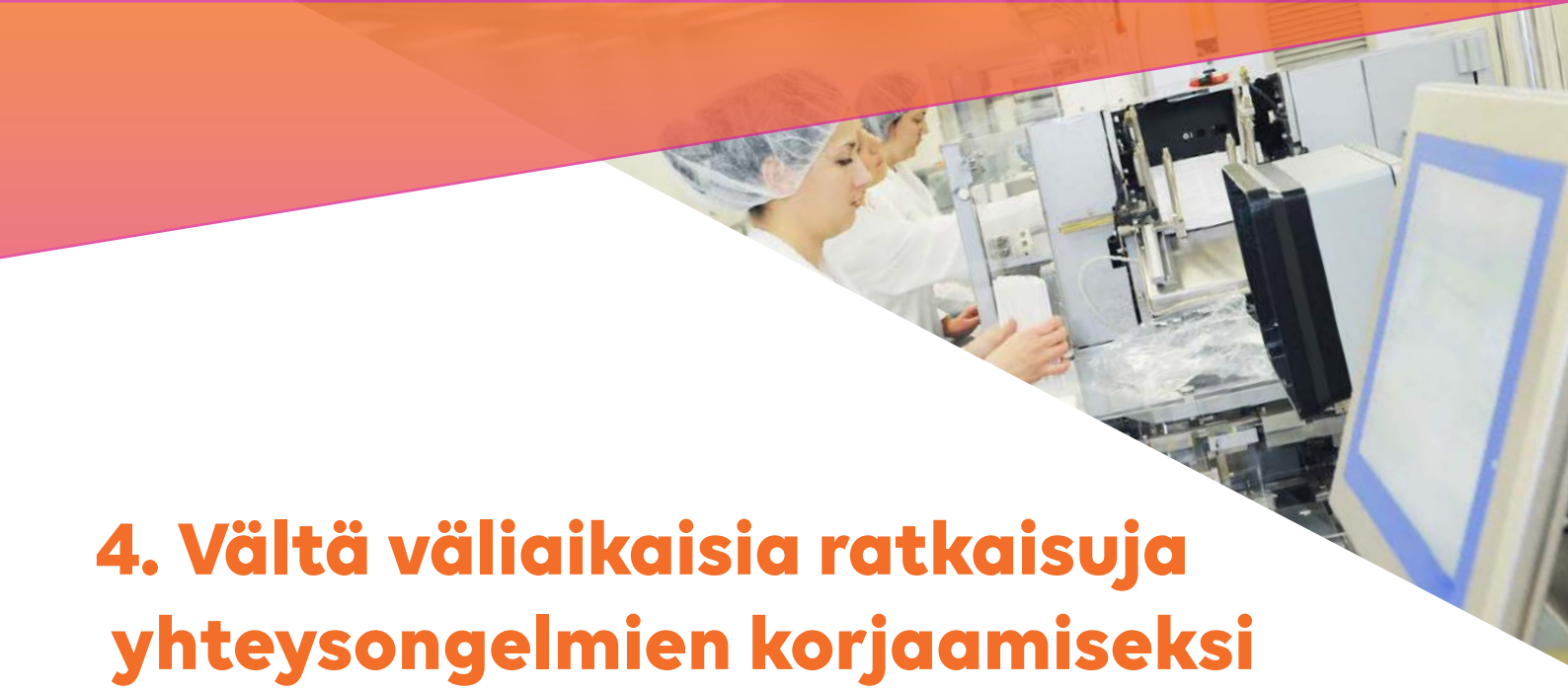
APN:n käytöstä syntyy paljon erilaisia kustannuksia. Sen käyttöä varten on hankittava tietynlaiset SIM-kortit sekä liittymät ja normaalien datayhteysmaksujen lisäksi on maksettava erillinen APN-maksu. Kannattaa myös huomioida, että APN-yhteyksissä on usein rajoitettu tiedonsiirtonopeus, kuten esimerkiksi 10 Mb/s, joka täytyy jakaa kaikkien käytettävien laitteiden kesken. APN:n ollessa käytössä ei voida myöskään hyödyntää WLAN-verkkoa ja yhteysongelmat voivat olla jopa yleisempiä kuin julkisessa verkossa. Lisäksi APN-yhteydet ovat usein maakohtaisia, joten globaalin yrityksen toimipisteille ei välttämättä ole saatavilla yhteistä APN-yhteyttä.

APN:n tietoturva ei ole aina yhtä korkeatasoinen kuin nykyaikaisempi VPN:n salaus. Tieto kulkee nykyisten kännykkästandardien mukaisissa salauksissa päätelaitteelta operaattorin konesaliin. Tiedonsiirtoväylä ei olekaan välttämättä täysin turvallinen jos ja kun tieto liikkuu 2G- tai 3G-verkoissa, joihin operaattori ei todennäköisesti ole kytkenyt kovin vahvoja salauksia.

PILVIRATKAISUT JA HYBRIDIMALLIT

Viime vuosina monet yritykset ovat siirtäneet toimintaansa pilvipalveluiden varaan. Esimerkiksi jatkuvasti yleistyvät Windows 10, Amazon Web Services ja Microsoft Office 365 ovat suosittuja alustoja. Pilveen siirryttäessä organisaatio ei tarvitse enää perinteistä APN:ää tai VPN:ää yhteyden luomiseen, mutta pilvessä on omat haasteensa: kun tieto ei sijaitse enää koneella, vaan pilvessä, on yritys vielä enemmän riippuvainen toimivista yhteyksistä.

Kun yritys ei voi siirtää kaikkia tietoja pilvipalveluihin, voi organisaatio toimia hybridiympäristössä, jossa osa yrityksen tiedoista tallentuu pilveen toisen osan jäädessä sisäverkkoon. Asia monimutkaistuu, kun perinteiset ratkaisut tuovat tiedon ensin sisäverkkoon, ennen kuin se voidaan siirtää pilveen. Oletusarvoisesti kaikki informaatio kiertää siis sisäverkon kautta ennen pilveen menoa, joka aiheuttaa turhaa kuormitusta. Tehokkuuden lisäämiseksi hybridiympäristössä käyttöön kannattaakin ottaa työkalu, jonka avulla on mahdollista määrittää mikä osa verkkoliikenteestä menee sisäverkkoon ja mikä osa suoraan pilveen.



4. Vältä väliaikaisia ratkaisuja yhteysongelmien korjaamiseksi

KALUSTON LISÄÄMINEN JA OPERAATTORIN VAIHTAMINEN

Yhteysongelmista pyritään usein eroon lisäämällä kalustoa. On mahdollista, että ns. raudan lisääminen parantaa tietoliikenneyhteyksiä väliaikaisesti paikallisesti: yhteyspisteiden ja tukiasemien määrän lisääminen esimerkiksi varastossa voi osin parantaa tilannetta. Kun organisaatio toimii monissa eri pisteissä ja työntekijät ovat jatkuvassa liikkeessä, ei tukiasemien, antennien tai reitittimien lisääminen ole kuitenkaan nopea eikä kustannustehokas ratkaisu: niiden tuomat lisäkustannukset voivat liikkua tuhansissa euroissa. Lisäksi IT-ympäristö muuttuu jatkuvasti, joten lisälaitteet eivät ole pysyvä ratkaisu.

Kenttätyöntekijöiden kokemia yhteysongelmia maastossa ei voida ratkaista samalla tavalla, jolloin usein pohditaan operaattorin vaihtamista. Operaattorin valinnalla on kuitenkin vain vähän merkitystä. Yritys saattaa toimia alueella, jossa jonkin tietyn operaattorin verkko on vahva ja vakaa, mutta mikäli yritys muuttaa tai laajentaa, voi uudella sijainnilla jollain toisella operaattorilla olla parempi verkko. Pahimmassa tapauksessa vanha operaattori ei edes toimi uudella alueella. Lisäksi yritys saattaa olla sitoutunut käyttämään valtakunnallisesti vain yhden operaattorin APN-yhteyttä.

Kun operaattorin vaihtaminen ei tule kysymykseen tai korjaa ongelmaa, voidaan verkon ylläpitäjälle tehdä pyyntö pystyttää uusia tukiasemamastoja tilanteen korjaamiseksi katvealueilla. Mutta myös tämä ratkaisee vain yhden ongelman ja vain yhdellä alueella. Lisäksi ylläpitäjä saattaa laskuttaa asiakasta tukiaseman pystyttämisestä, jos kukaan muu ei hyödynnä mastoa kyseisellä alueella.

ONGELMAN SIVUUTTAMINEN JA SOVELLUSKOHTAISET RATKAISUT

Ongelmia ei kannata yrittää sivuuttaa tai kiertää. Esimerkiksi erikoisten ohjeistusten antaminen, kuten käsky käyttää laitetta vain tietyssä paikassa tai sen uudelleenkäynnistäminen aina tietyssä vaiheessa, ei auta parantamaan työn tehokkuutta, vaan vaikuttaa negatiivisesti työntekijöiden motivaatioon.

Osa organisaatioista on lähtenyt rakentamaan ratkaisuja sen mukaan, missä laitteessa, operaattorissa tai WLAN-verkoissa ongelma piilee sekä minkä sovellusten kanssa ongelmia on esiintynyt useimmiten. Näiden palapelin palasten pohjalta yritys on voinut valita itselleen erillisiä ratkaisuja, joiden yhdistelmällä ongelmia esiintyy vähiten.

Muun muassa yksittäisten sovellusten toimivuutta on saatettu pyrkiä vahvistamaan esimerkiksi offline-toiminnoilla tai pienillä itse koodatuilla puskureilla itse sovelluksessa. Offline-toiminto voi olla täysin mahdollinen ja toimiva ratkaisu yhdelle sovellukselle, mutta usein käytössä olevia sovelluksia on satoja. Lisäksi eri sovellukset toimiessaan päällekkäin saattavat häiritä toistensa toimintaa. Omatekoisiin ratkaisuihin liittyy aina myös tietoturvariskejä, jonka vuoksi yksittäisten sovellusten muokkaaminen itse ei ole suositeltavaa.

Monisyisen rakennelman ongelmana onkin, että jokainen palapelin palanen on riippuvainen muista palasista. Voidaan huomata, että tiettyä päätelaitteita ei välttämättä enää olekaan saatavilla puolen vuoden kuluttua tai koko rakennelma rikkoutuu, kun hankitaan yksi uusi sovellus. Tällöin koko palapelin kokoaminen täytyy aloittaa alusta. Vanhanaikaisen ratkaisun kanssa siis jo yhden palan muuttuessa koko konsepti hajoaa käsiin, joten ratkaisu ei ole kauaskantoinen eikä taloudellisesti järkevä.

Pahimmillaan itse räätälöidyt ratkaisut voivat kaataa kokonaisia projekteja yrityksissä. Ensimmäisen version valmistuessa voidaan huomata, ettei ratkaisu olekaan toiminut käytännössä. Seuraavan version rakentamiseen voidaan joutua lähtemään eri ohjelmistoilla ja eri laitteilla, jolloin aikaa, rahaa ja työtunteja menee hukkaan koko ketjun mennessä uusiksi. Räätälöidyn rakentamisen sijaan yrityksen olisikin syytä etsiä ratkaisua, joka toimii stabiilina alustana kaikille sovelluksille ja yhteyksille, ja jolla vakaus ei ole väliaikaista, vaan pysyvää.

5. IT:n toimintaohjeet katkeamattomien datayhteyksien varmistamiseen

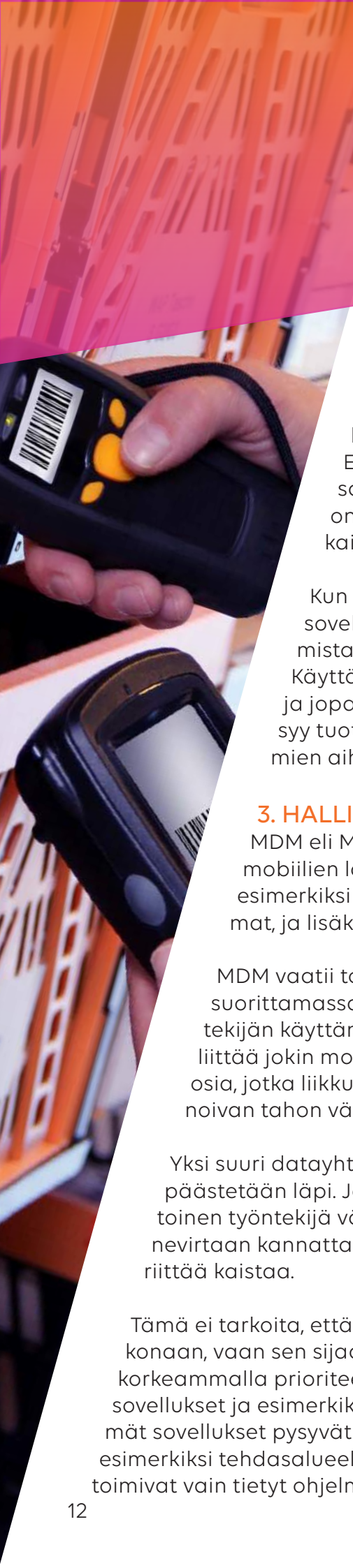
1. ANALYSOI JA LÖYDÄ TODELLINEN ONGELMAN LÄHDE

Perinteisesti IT:llä ei ole ollut tarvittavia työkaluja kenttätyön yhteysongelmien vianmääritykseen, vaan kenttätyöntekijöiltä tulleissa tiketeissä mainittujen ongelmien lähdettä on jouduttu arvailemaan. Verkko-ongelman aiheuttaja voi olla mitä tahansa päätelaitteen verkkokortista asiakasyrityksen runkoverkon kytkimeen. Ensimmäinen askel yhteyksien korjaamiseen onkin hankkia kunnon analytiikkatyökalut, joiden avulla IT saa näkyvyyden siihen, mitä yhteyksissä tapahtuu.

Verkon analytiikkatyökalun tulee mahdollistaa:

- Verkon suorituskyvyn valvonta ja analysointi
    - tietoliikenteen nopeus
    - huono signaalin laatu
    - palvelimien vastaanottoherkkyys
    - VPN:n yhdistymisen ongelmat
    - GPS:n toiminta ja yhteyskatkokset
- Käytettävien sovellusten kuormittavuuden seuranta
- Operaattorien verkkojen toiminta ja tehokkuus
- Vian paikantaminen
- Avoimet verkonhallintaominaisuudet
- Reaaliaikainen raportointi ja aikaleimalla varustetut virheraportit
- Hälytykset ongelmatilanteista

Oikeanlaisten työkalujen avulla tiedetään tarkalleen missä ongelma on ja IT:n on mahdollista rakentaa kestäviä ratkaisuja, jotka ehkäisevät samanlaisten ongelmien ilmaantumisen tulevaisuudessa.



2. PIILOTA PIENET YHTEYSONGELMAT MOBIILIN VPN-RATKAISUN AVULLA

Vaikka käytössä olisi monipuoliset raportoinnin ja analytiikan välineet, ei kaikkia pieniä yhteysongelmia voida ikinä korjata täysin. Eniten vaikeuksia tuottavat hetkelliset verkon katkeamiset, jotka saavat usein esimerkiksi ERP:n kaatumaan. Pienet yhteyskatkokset on kuitenkin mahdollista piilottaa käyttäjältä laadukkaaan VPN-ratkaisun avulla, joka on tarkoitettu mobiiliin työskentelyyn.

Kun käytössä on laadukas yhteyksienhallintatyökalu, herkätkään sovellukset, kuten ERP, eivät huomaa nopeaa verkkoyhteyden katkeamista, vaan käyttäjän näkökulmasta jatkavat toimintaansa normaalisti. Käyttäjän on siis mahdollista työskennellä ilman sovelluksen kaatumista ja jopa täysin tietämättömänä heikosta verkkoyhteydestä. Näin työ pysyy tuottavana, eikä IT-tuki kuormitu lukuisista väliaikaisten verkko-ongelmien aiheuttamista tiketeistä.

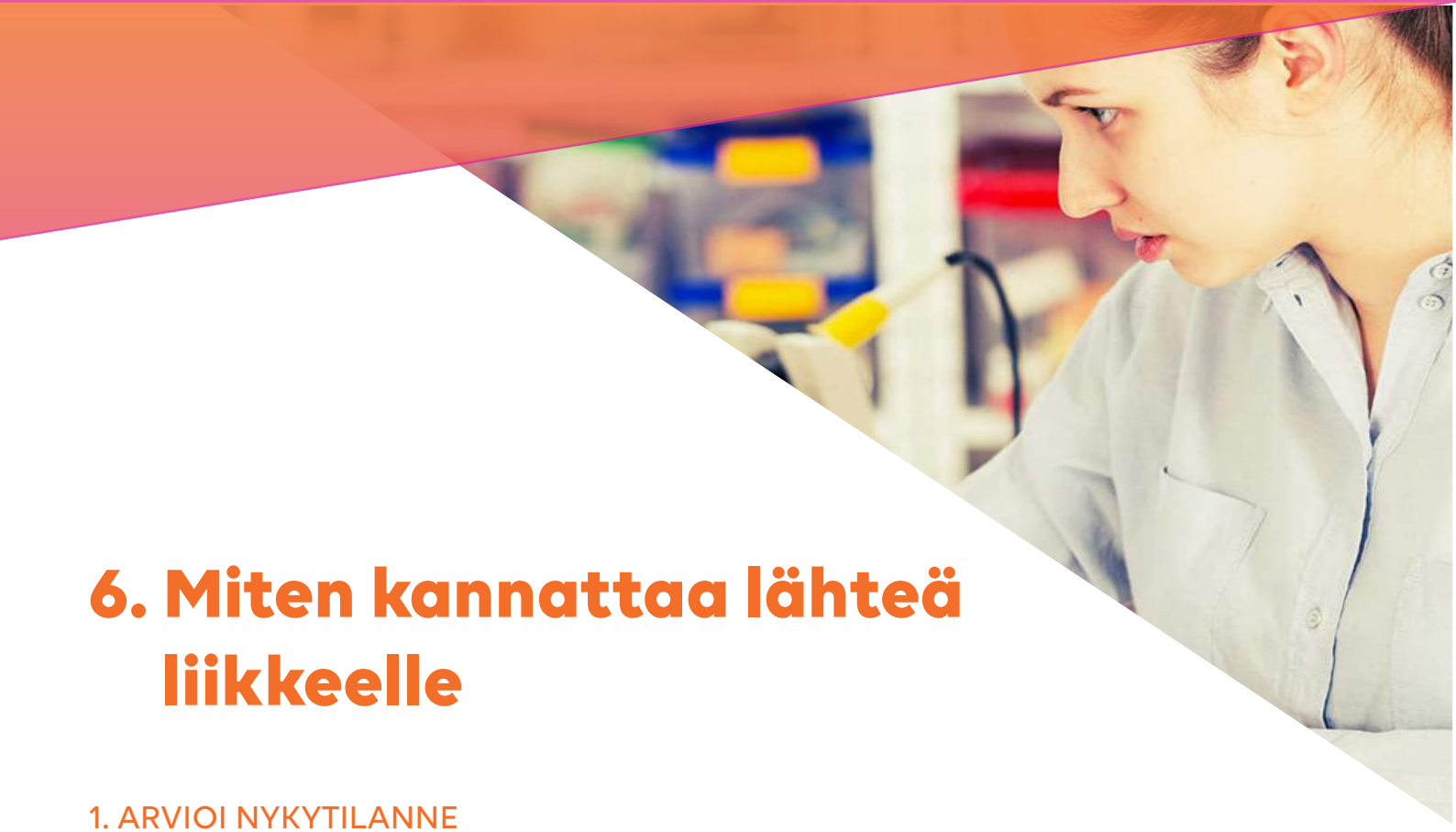
3. HALLINNOI TIETOLIIKENTEEN VIRTAA

MDM eli Mobile device management on yrityksissä koko ajan yleistyvä mobiilien laitteiden hallinnointityökalu. Työkalulla voidaan määrittää etänä esimerkiksi laitteiden turva-asetukset, laitteessa käytettävät ja sallitut ohjelmat, ja lisäksi laitteen päivityksiä voidaan mahdollisesti hallinnoida.

MDM vaatii toimiakseen kuitenkin hyvän verkkoyhteyden: jos työntekijä on suorittamassa työtehtävää katvealueella, ei MDM välttämättä toimi, eikä työntekijän käyttämää laitetta pystytä hallinnoimaan etänä. Työkaluun onkin syytä liittää jokin moderni, yhteyksiä hallitseva työkalu. Mitä enemmän yrityksillä on osia, jotka liikkuvat mobiilina, sitä tärkeämpää on, että putki laitteen ja sitä hallinnoivan tahon välillä pysyy avonaisena.

Yksi suuri datayhteyden toimivuuteen vaikuttava tekijä onkin se, millaista tietoa päästetään läpi. Jos kollega on tauolla ja katsoo Netflixiä vallaten koko liikenteen, ei toinen työntekijä välttämättä pysty siirtämään kriittistä tietoa verkon yli. Tietoliikennevirtaan kannattaakin määritellä bisnekselle kriittiset datapaketit, joille pitää aina riittää kaistaa.

Tämä ei tarkoita, että erillisten sovellusten käyttö päätelaitteella tarvitsisi estää kokonaan, vaan sen sijaan voidaan määritellä, mitkä operatiiviset sovellukset ovat aina korkeammalla prioriteetilla eli saavat ensin kaistaa. Yhteyksien heikentyessä turhat sovellukset ja esimerkiksi automaattiset päivitykset pudotetaan tällöin pois ja tärkeimmät sovellukset pysyvät toiminnassa vaikeissakin olosuhteissa. Samalla tavalla voidaan esimerkiksi tehdasalueella tai sairaalan pihapiirissä määrittää, että kyseisellä alueella toimivat vain tietyt ohjelmat, joita tarvitaan työntekoon.



6. Miten kannattaa lähteä liikkeelle

1. ARVIOI NYKYTILANNE

Ensimmäinen askel verkko-ongelmien korjaamisessa on arvioida organisaatiossa tällä hetkellä käytössä olevan VPN-, APN-, pilvi- tai hybridiratkaisun toimivuus. Vanhan ratkaisun tilalle tarvitaan kunnollinen yhteyttä hallinnoiva työkalu, jos organisaatiossa on mm. seuraavia ongelmia:

- IT:llä ei ole näkyvyyttä verkko-ongelmien syihin
- Operaattorin vaihtamista tai laitteiden lisäämistä joudutaan pohtimaan jatkuvasti
- Käytössä on herkkiä sovelluksia, kuten ERP, jotka tuottavat virhetilanteen pienimmistäkin yhteysongelmista
- IT joutuu tuottamaan sovelluskohtaisia ratkaisuja, kuten offline-toiminnallisuuksia

Tässä kohtaa voi olla hyödyllistä ottaa ilmainen konsultaatio palveluntarjoajalta. Palveluntarjoajalla on kokemuksia samanlaisista ongelmatilanteista ja heiltä on mahdollista saada arvokasta tietoa, jonka avulla voidaan selvittää suurimmat ongelmakohdat.

2. VAADI TOIMITTAJALTA LAADUKAS TYÖKALU YHTEYKSIEN HALLINTAAN JA VERKON ANALYTIIKKAAN

Valitettavasti halvalla ei useinkaan saa hyvää, ja nykyisen ratkaisun vaihtamista älykkääseen yhteyksienhallintatyökaluun ja laadukkaisiin analytiikkatyökaluihin kannattaa harkita, kun yhteysongelmat kentällä aiheuttavat kustannuksia liiketoiminnalle ja heikentävät työntekijöiden tyytyväisyyttä sekä tuottavuutta.

Vaihtoehtona APN- tai VPN-yhteydelle, joka saattaa taata hyvän tietoturvan, mutta samalla hidastaa yhteyksiä entisestään, toimii mobiili VPN, jonka avulla yleisimmät kentällä ja haastavissa olosuhteissa esiintyvät yhteysongelmat voidaan korjata tai kiertää. Laadukas yhteyksiä hallinnoiva työkalu mahdollistaa tiedon siirtämisen verkon yli sellaisissakin paikoissa, joissa heikkoa verkkoa ei tavallisilla työkaluilla voida edes havaita.

Vaadi toimittajalta seuraavat asiat:

- Ammattikäyttöön suunniteltu, langattomiin verkkoihin ja mobiililaitteisiin tukeutuva VPN
- Työkalut tietoliikennevirran hallintaan sekä syvälliseen verkon analysointiin
- Yhteysviiveiden piilottamisen mahdollisuus työkalun avulla, jotta ne eivät vaikuta sovellusten käytettävyyteen
- Skaalautuvuus yrityksen koon mukaan
- Helppo käyttöönotto ja ylläpito
- Yhteyden hallinnan kyky: yhteys mukautuu huonompiin verkkoihin ja verkon vaihtumisiin ja pystyy ottamaan kaiken irti kaikista yhteyksistä

3. KOKEILE RATKAISUA KÄYTÄNNÖSSÄ

Ennen kuin sitoudut uuteen ratkaisuun, pyri saamaan toimittajalta käyttöösi ilmainen kokeiluversio, sillä ratkaisua kannattaa aina testata käytännössä. Parhaat toimittajat järjestävät kokeilun nopeasti ja jos testikäytössä luotu ympäristö todetaan toimivaksi ratkaisuksi, on tärkeää, että se voidaan suoraan siirtää tuotantokäyttöön. Näin vältytään pitkiltä ja raskailta käyttöönottoprojekteilta sekä niiden aiheuttamilta ylimääräisiltä kustannuksilta.

Käyttöönoton jälkeen ratkaisun olemassaolon voi melkein unohtaa, vaikka sitä voi aina tarvittaessa viilata. IT-osastolla on ohjat käsissään ja se voi tarvittaessa säädellä yhteyksien ominaisuuksia sen mukaan mikä on toimivaa ja kustannustehokasta. Käyttäjälle ratkaisu on näkymätön: kenttätyöntekijä ei välttämättä edes tiedä mitä kautta data liikkuu, sillä tärkeintä on, että se liikkuu aina ilman ongelmia.

NetMotion – enemmän kuin tavanomainen VPN-yhteys

NetMotion on luotettava yhteysohjelmistoratkaisu, joka parantaa liikkuvien työntekijöiden tuottavuutta, turvallisuutta ja ohjausta. Se ei ole pelkästään VPN-yhteys, sillä sen avulla työntekijät pääsevät tehokkaasti käsiksi sovelluksiin vaihtelevista verkko-olosuhteista huolimatta. Netmotion on suunniteltu langattomiin verkkoihin ja mobiililaitteisiin tukeutuvaan ammattikäyttöön. Älykkäänä mobiili VPN-ratkaisuna se on mainio ratkaisu mobiiliyhteyksien tietoturvalliseen hallintaan, sekä antaa edellytykset tuottavampaan ja kannattavampaan mobiilityöskentelyyn.

Tutustu NetMotioniin

Kauko

www.kauko.com
puh. 095211