TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Ohje paikallisten matkaviestinverkkojen kyberturvallisuudesta ja riskienhallinnasta

Traficomin tutkimuksia ja selvityksiä

8/2023

Sisällysluettelo

1 Johdon tiivistelmä

Tämän ohjeen tarkoituksena on luoda yleiskuva paikallisista matkaviestinverkoista ja reunalaskennasta sekä niihin liittyvistä kyberturvallisuuden, riskienhallinnan ja toimintavarmuuden näkökulmista, jotta organisaatiot voivat paremmin suunnitella tällaisten verkkojen käyttöönottoa ja verkkojen hyödyntämistä omissa toiminnoissa. Ohje on suunnattu erityisesti yhteiskunnan kriittisiä toimintoja tuottaville organisaatioille, mutta on käyttökelpoinen myös muille organisaatioille, jotka haluavat hyödyntää paikallisia matkaviestinverkkoja. Ohjeen laatimisessa on hyödynnetty muuttuvan toimintaympäristön havainnollistamiseksi laadittuja erilaisia huoltovarmuusskenaarioita, jotka on esitelty tarkemmin luvussa 6.

Paikalliset matkaviestinverkot ja 5G-teknologia tarjoavat organisaatioille uudenlaisia digitalisaatioon ja tehokkuuden kasvattamiseen liittyviä mahdollisuuksia joustavien ja räätälöitävien langattomien tiedonsiirtomahdollisuuksien kautta.

Uudet matkaviestinverkkoteknologiat ovat ominaisuuksiltaan lähtökohtaisesti suorituskykyisempiä ja turvallisempia kuin esimerkiksi nykyisin usein käytössä olevat paikalliset WLAN-toteutukset. Kyberturvallisuuden ja toimintavarmuuden osalta on kuitenkin tärkeä ymmärtää matkaviestinverkkoteknologian tuomia erityispiirteitä, niihin liittyviä kyberturvallisuusnäkökulmia sekä suunnitella ja toteuttaa kokonaisuus tarkoituksenmukaisella tavalla pohtien toteutuksiin kohdistuvia riskejä ja uhkia. Tämän ohjeen tarkoituksena onkin tarjota organisaatioille tietoa paikallisisiin matkaviestinverkkoihin liittyvistä kyberuhkista, riskienhallinnasta sekä keinoista, joilla verkkojen toimintavarmuutta voidaan turvata.

Usein paikallinen matkaviestiverkkokokonaisuus hankitaan ulkopuolisten kumppanien avustuksella tai kokonaan niiden kautta. Järjestelmää hankittaessa organisaatioiden tulee varmistua, että sen turvallisuuden varmistamiseen ja ylläpitoon on varattu riittävästi omaa osaamista ja resursseja. Näin organisaation toimintaan ja kyberturvallisuuteen liittyvät tekniset tarpeet ja vaatimukset tulevat huomioiduksi suunnittelussa ja hankinnan aikana, järjestelmän teknisessä toteutuksessa, käyttöönotossa sekä organisaation päivittäisessä toiminnassa ja myöhemmin tapahtuvassa kehitystyössä.

Palveluissa joissa hyödynnetään esimerkiksi teleoperaattorien verkkoja, pilvipalveluja, integraattorikumppaneita tai muita palveluntarjoajia, tulee kunkin roolit ja vastuut määritellä selkeästi ja kirjata ne tarpeellisin osin sopimuksiin sekä lisäksi varmistaa sovittujen asioiden toteutuminen myös käytännössä. Ekosysteemiajattelun hyödyntäminen vastuiden tunnistamisessa, määrittelyssä ja sopimisessa auttaa osaltaan hallitsemaan monitoimittajaympäristön riskejä. Sopimusvelvoitteiden toteutuminen on kyettävä varmistamaan riittävän luotettavasti. Yhteistyökumppaneiden osalta on myös pyrittävä vakuuttumaan prosessien ja kyberturvallisuuden tasosta esimerkiksi testeillä tai auditoinneilla.

Kyberturvallisuus ja toimintavarmuus on huomioitava olennaisena osana koko palvelun ja ratkaisun elinkaarta aina suunnittelusta operointiin ja myöhemmin tehtäviin muutoksiin ja mahdollisiin laajennuksiin asti. Myös käytössä olevien ns. legacy-järjestelmien toimiminen paikalliseen matkaviestinverkkoon liitettynä osana tai sen rinnalla on arvioitava riskikartoituksessa. Lisäksi tulee kiinnittää

huomiota tulevaisuudessa tapahtuvaan käyttötapauksien mahdolliseen laajentumiseen ja ympäristön kehityksen tuomiin muutoksiin, sillä tällöin palvelun kriittisyys, riskitasot ja vaatimukset saattavat muuttua. Tässä ohjeessa on tarjottu linkkejä erilaisiin hyödynnettäviin lähteisiin sekä tarkistuslistoja käytettäväksi suunnittelutyön ja riskiarvioinnin tukena.

Palvelun käyttötapaus ja sen kriittisyys määrittävät soveltuvan toteutustavan valintaa sekä kyberturvallisuuden ja toimintavarmuuden tarpeita. Riittävä suunnittelu erilaisten poikkeustilanteiden varalta on tärkeää. Erityisesti kriittisten toimintojen ja järjestelmien osalta on esimerkiksi syytä varautua tilanteisiin, jossa yhteydet ulospäin menetetään kokonaan, mutta toiminnan tulee siitä huolimatta pystyä jatkumaan. Riittävät kahdennukset verkon eri osissa, osaamisen ja resursoinnin sekä toimittajan tuen varmistaminen tulee huomioida erilaisten häiriö- ja poikkeustilanteiden varalle. Varajärjestelyt tulee olla suunniteltuna etukäteen ja niiden mukainen toimintatapa tulee olla testattu myös käytännössä, jotta palvelun jatkuvuuteen voidaan luottaa. Ohjeessa luvussa 6 on esitelty erilaisia huoltovarmuusskenaarioita, joita voidaan hyödyntää suunnittelun ja riskien arvioinnin pohjana. Esitetyt skenaariot eivät kata kaikkia häiriö- ja poikkeustilanteita, mutta antavat pohjaa organisaation omille pohdinnoille.

Paikallisiin matkaviestinverkkototeutuksiin voi toteutustavasta riippuen liittyä erilaisia määräyksiä ja velvoitteita. Palvelun omistajalla on oltava kyvykkyys huolehtia toimimisesta ratkaisun toteutusmalliin liittyvien velvoitteiden ja määräysten mukaisesti. Tässä asiantuntevat kumppanit voivat auttaa. On kuitenkin muistettava, että juridista vastuuta ei voi sopimusten kautta ulkoistaa yhteistyökumppaneille. Ohjeessa luvussa 4 luodaan yleiskuva paikallisten matkaviestinverkkojen sääntelyyn. Sovellettava sääntely ja velvoitteet riippuvat verkon käyttö- ja toteutustavoista, yksityiskohtaisemmissa tulkinnoissa on tärkeä kääntyä Liikenne- ja viestintävirasto Traficomin puoleen. Kyberturvallisuuden velvoitteisiin ja määräyksiin liittyen Traficomiin voi olla yhteydessä sähköpostilla osoitteeseen kyberturvallisuuskeskus@traficom.fi. Radiotaajuuksiin liittyvissä kysymyksissä radiotaajuudet@traficom.fi.

Tämä ohje pohjautuu vuoden 2022 alkukesällä järjestettyihin työpajoihin, joihin osallistui toimialan yritysten, laitevalmistajien, akatemian ja loppukäyttäjien edustajia.

2 Johdanto

5G-teknologian mahdollistama suuri kapasiteetti, pienet yhteysviiveet ja luotettava kommunikaatio sekä ohjelmistopohjaisuus ja tarvittaessa verkon reunalla tapahtuva laskenta luovat monipuolisen työkalupakin, jonka avulla voidaan vastata eri sektoreilla toimivien organisaatioiden digitalisaatiokehityksen tarpeisiin. Digitalisaatiossa tavoitteina ovat toiminnan tehostaminen, automatisointi ja nykyisin myös parempi turvallisuustaso. Samalla toimintaa digitaalisesti kehittämällä sekä tehostamalla voidaan siirtyä kohti puhtaampia ilmastoa- ja ympäristöä vähemmän kuormittavia toimintatapoja, jonka merkitys tulee entisestään korostumaan tulevaisuudessa. Tämän ohjeen tarkoitus on auttaa organisaatioita kybertuvallisuuden ja riskienhallinnan toteuttamisessa siirryttäessä käyttämään paikallisia matkaviestinverkkoja.

Paikalliset matkaviestinverkot ja reunalaskenta

Ohjeessa esitellään yleisimmät paikalliset matkaviestinverkko- ja reunalaskentaratkaisut sekä kyberturvallisuuden varmistamiseen liittyvät näkökulmat läpi koko toteutuksen elinkaaren. Paikallisilla matkaviestinverkoilla tarkoitetaan tässä ohjeessa matkaviestinverkkoja, jotka eivät ole kaupallisten matkaviestinoperaattorien käytössä valtakunnalliseen teletoimintaan, vaan ne on toteutettu erikseen jonkun tietyn organisaation tarpeisiin käyttäen hyödyksi joko operaattorin olemassa olevaa verkkoa tai rakentamalla täysin erillinen yksityinen verkko tätä tarkoitusta varten. Tällaiset yksityiset verkot ovat tyypillisesti tietyn organisaation omassa käytössä, eikä niihin pysty liittymään kuin hallinnoitujen rajapintojen tai käyttöliittymien kautta sallitut käyttäjät. Paikallisille matkaviestinverkoille on erilaisia toteutusmalleja, jotka esitellään luvussa 3.1 Paikallisten verkkojen toteutusmallit sekä luvussa 3.2 Paikallisten verkkojen vastuut.

Reunalaskenta on toimintaa, jossa tietyt toiminnot kuten ~~tietty~~ tiedonkäsittely tai tietovarasto on sijoitettu muualle kuin palvelinkeskukseen, esimerkiksi palvelun käyttäjän omiin tiloihin sijoitettuun laitteistoon tai päätelaitteeseen, eli toisin sanoen verkon reunalle. Käytännössä reunalaskenta koostuu hajautetusta laskentakapasiteetista, jossa esimerkiksi tietoa keräävät laitteet kykenevät itse hyödyntämään laskentakapasiteettia tiedon analysointiin ilman, että data täytyy ensin siirtää keskitetyn laskentakapasiteetin piiriin. Reunalaskentaa käsitellään luvussa 3.3 Reunalaskenta sekä luvussa 3.4 Reunalaskentaratkaisujen vastuut.

Sääntely ja velvoitteet

Paikallisiin matkaviestinverkkototeutuksiin voi käyttötapauksesta ja toteutustavasta riippuen kohdistua myös sääntelyä ja velvoitteita. Teletoimintaa ja muita viestinnän välittäjiä säännellään tarkoin lainsäädännössä, ja Traficom on antanut useita, pääasiassa teleyrityksiä koskevia määräyksiä. Pilvipalvelun tarjoajan velvollisuudesta huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta säädetään myös laissa[1]. Tähän ohjeeseen on nostettu keskeisiä tietoturvaan ja toimintavarmuuteen liittyviä velvoitteita ja määräyksiä. Erikseen

[1] Katso luku 4.2.1.

on säädetty kiellosta käyttää viestintäverkon kriittisissä osissa kansallista turvallisuutta vaarantavia viestintäverkkolaitteita, mikä koskee yleisten viestintäverkkojen lisäksi ns. kriittisiä erillisverkkoja[2].

Toisinaan voi esiintyä tulkintakysymyksiä siitä, kuuluuko yrityksen tai yhteisön tarjoama palvelu tai jokin osa siitä Traficomin valvoman sääntelyn piiriin, joten aluksi onkin tärkeää tunnistaa, missä sääntelyn tunnistamissa eri rooleissa tietty toimija toimii. Kyberturvallisuuden velvoitteisiin ja määräyksiin liittyen Traficomiin voi olla yhteydessä esimerkiksi sähköpostilla osoitteeseen kyberturvallisuuskeskus@traficom.fi.

Oman organisaation käyttöön räätälöityjä paikallisia matkaviestinverkkoja voidaan toteuttaa joko hyödyntäen teleyritysten taajuuksia tai hakemalla Traficomilta omia taajuuksia toteutukselle. Vastuu radioluvan ehtojen noudattamisesta on aina radioluvan haltijalla. Jos organisaatiolle itselleen on myönnetty verkkototeutuksen radiolupa, vastuu radioluvan ehtojen noudattamisesta on organisaatiolla itsellään. Radiotaajuuksiin liittyvissä kysymyksissä lisätietoja saa Traficomilta esimerkiksi sähköpostitse osoitteesta radiotaajuudet@traficom.fi. Sääntelykokonaisuutta käsitellään tarkemmin luvussa 4 Sääntely ja valvonta.

Kyberturvallisuuden varmistaminen

Paikallisten matkaviestinverkkojen ja reunalaskennan ratkaisujen kyberturvallisuus rakentuu usein jaetuista vastuista. Ekosysteemitasolla vastuukysymykset ovat monimutkaiset, ja niihin on syytä kiinnittää erityistä huomiota käyttökohteen riskitason ja toimintavarmuusvaatimusten mukaan. Vastuukysymyksistä tarkemmin luvuissa 3.2 Paikallisten verkkototeutusten vastuunjako ja 3.4 Reunalaskentaratkaisujen vastuut. Vastuukysymysten ohella järjestelmien elinkaaren eri vaiheet vaativat erilaisia lähestymistapoja kyberturvallisuuteen. Ratkaisuiden kyberturvallisuutta, sen erityispiirteitä ja elinkaarenhallintaa käsitellään luvussa 5.

Suunnittelussa on tärkeää ymmärtää, miten liiketoimintatarpeet, järjestelmän käyttötapaukset ja -kohteet sekä riskit vaikuttavat verkon ja sen sovellusten suojaustarpeisiin sekä toimintavarmuuden rakentamiseen ja huoltovarmuuteen. Toteutusvaiheen kyberturvallisuuden varmistaminen poikkeaa toisistaan, mikäli järjestelmää rakennetaan itse, kumppanin kanssa tai ostetaan ns. avaimet käteen -ratkaisuna. Päivittäisessä toiminnassa sovelluskohteen toimintavarmuus ja jatkuvuus varmistetaan hyvillä toimintamalleilla ja operatiivisilla toimilla.

Uudet teknologiat tarjoavat hyötyjä ja mahdollisuuksia kyberturvallisuustason parantamiseen. Hajautetun reunalaskennan ominaisuuksia voidaan valjastaa esimerkiksi tietosuojan ja riskitason parantamiseen, kun laskenta tapahtuu paikallisesti tai lähellä datan lähdettä. Näin voidaan välttää esimerkiksi henkilötietojen tai liiketoiminnan kannalta kriittisen datan siirtymistä organisaation ulkopuolelle tai ulos EU-alueelta.

[2] Näitä ovat ydinvoimaloiden, satamien, lentokenttien ja vastaavien yhteiskunnan elintärkeiden toimintojen kannalta keskeisten toimijoiden yleiseen viestintäverkkoon liitetyt erillisverkot (SVPL 244 a §).

Toimintavarmuus ja huoltovarmuus

Toimintavarmuudella on tärkeä rooli yhteiskunnallisen huoltovarmuuden varmistamisessa. Toimintavarmuuden osalta on tärkeä tunnistaa palvelut ja toiminnot, joita paikallisilla matkaviestinverkoilla ja reunalaskennan ratkaisuilla tuotetaan. Kriittisen palvelun toiminta- ja huoltovarmuuden toteutus vaatii kattavaa ja eri riskitekijät huomioivaa suunnittelua, onnistuneen ja tarkoituksenmukaisen toteutuksen sekä jatkuvaa ylläpitoa ja testausta operoinnin aikana. Toimintavarmuuden näkökulmia avataan luvussa 3.7, riskienhallintaa käsitellään luvussa 5.3.1 ja jatkuvuudenhallintaa luvussa 5.6.

Luvussa 6 esitellään tämän oheen laatimisen taustalla olleet muutamat esimerkinomaiset huoltovarmuusskenaariot, joiden avulla lukija voi pyrkiä hahmottamaan erilaisia toimintaympäristöön liittyviä riskejä. Nämä esitetyt skenaariot eivät ole kaiken kattavia, mutta skenaarioita voi hyödyntää oman pohdinnan ja riskienhallintatyön tukena. On kuitenkin hyvä huomioida, että ne voivat muuttua ajan kuluessa tai olosuhteiden muuttuessa. Ohje tarjoaa myös listan kysymyksiä hyödynnettäväksi organisaation omassa kyberturvallisuus- ja riskienhallintatyössä Liite 1: Tarkistuslista ja itsearviointimalli.

3 Paikalliset matkaviestinverkot ja reunalaskenta

Paikallisten matkaviestinverkkojen ja reunalaskennan ratkaisujen hyödyntäminen osana palveluiden toteutusta vaatii omistajalta ja toteuttajalta ymmärrystä tarpeista ja erilaisista vaatimuksista, jotka palvelun osalta on täytettävä. Toteutusmallin valintaan liittyy kolme tärkeää kriteeriä: saavutettava palvelutaso, toimintavarmuus eri tilanteissa ja kyberturva. Paikallisen verkkojen toteutustapoja on useita ja näistä jokaiseen liittyy erilaisia velvollisuuksia ja vaikutuksia palvelun omistajalle, joita esitellään tässä luvussa.

3.1 Paikallisten verkkojen toteutusmallit

Paikallisten matkaviestinverkkojen toteutustapoihin liittyviä palveluntarjoajia on useita. Näitä ovat esimerkiksi teleoperaattorit, laitevalmistajat, pilvipalvelujen tarjoajat ja integraattorikumppanit. Tässä ohjeessa jokaisen erilaisen mahdollisen toteutustavan esittely ei ole mahdollista. Siksi toteutusmallit on yksinkertaistettuna jaettu viiteen erilaiseen pääryhmään niiden keskeisten ominaisuuksien mukaan. Toteutukset on jaettu alkaen puhtaasti yleiseen viestintäverkkoon pohjautuvasta toteutuksesta ja päätyen täysin itsenäiseen paikallisverkkototeutukseen, jossa verkolle käytetään myös ainoastaan siihen tarkoitukseen myönnettyjä omia taajuuksia.

Ohjeessa viitataan palveluun puhuttaessa palvelukokonaisuudesta, joka voi koostua itsenäisestä paikallisverkkototeutuksesta, reunalaskentatoteutuksesta tai näiden yhdistelmästä. Ratkaisulla viitataan palvelun osaan, joka tuottaa jonkin toiminnallisuuden tai palvelun asiakkaalle ja se voi koostua esimerkiksi verkkolaitetoteutuksesta, reunalaskennan sovelluksesta yms. Järjestelmä on suurempi kokonaisuus, johon voidaan lisätä uusia komponentteja tai muokata olemassa olevia komponentteja sen mukaan minkälaisia uusia ratkaisuja täytyy toteuttaa uusien palvelujen tuottamiseksi tai vanhojen palvelujen parantamiseksi. Kun ohjeessa

viitataan tietyn organisaation tarpeeseen tehtyyn paikalliseen verkkoon, puhutaan verkkoratkaisusta.

Seuraavaksi Taulukko 1 esittelee ylätasolla erilaiset toteutustavat, joilla organisaatio voi hyödyntää matkaviestinverkkoteknologiaa omassa toiminnassaan ja niiden ylätason erot.

	Yleinen viestintäverkko	**Yleisen viestintäverkon viipalointi (slicing)**	**Yleinen viestintäverkko paikallisella infrastruktuurilla**	**Paikallinen verkkototeutus käyttäen teleyrityksen taajuuksia**	**Paikallinen verkkototeutus käyttäen omia taajuuksia**
Yleiskuvaus	Yleisen viestintäverkon käyttö mahdollistaa palvelun, jonka ylläpidosta vastaa teleyritys.	Teleyrityksen tarjoama ratkaisu, jossa yleisessä viestintäverkossa voidaan tarjota käyttötarpeen mukaan räätälöityä laatutasoa erillisellä verkkoviipaleella.	Teleyrityksen tarjoama ratkaisu, joka antaa enemmän mahdollisuuksia verkon kontrollointiin ja datan eriyttämiseen paikallisesti.	Organisaation itsenäisesti tai kumppanin kanssa hankkima ja toteuttama verkkoratkaisu, jossa organisaatiolla on täysi kontrolli verkon suunnittelun, toteutuksen ja ylläpidon osalta.	Organisaation itsenäisesti tai kumppanin kanssa hankkima ja toteuttama verkkoratkaisu, jossa organisaatiolla on täysi kontrolli verkon suunnittelun, toteutuksen ja ylläpidon osalta. Käytössä organisaatiolle myönnetyt omat taajuudet.
Peittoalueen laajuus	Laaja peitto.	Laaja/paikallinen peitto.	Paikallinen peitto.	Paikallinen peitto.	Paikallinen peitto.
Palvelutaso	Oletuksena yleisen verkon normaali palvelutaso, mutta mahdollisuus sopia paremmasta palvelutasosta operaattorin kanssa verkkoneutraliteettia koskevien säännösten puitteissa[3].	Mahdollisuus sopia asiakaskohtaisesti parempi ja vakaampi palvelutaso verkkoneutraliteettia koskevien säännösten puitteissa[3].	Mahdollisuus toteuttaa asiakaskohtaisesti räätälöity ja moninaisempi palvelutaso. Voidaan hyödyntää paikallista reunalaskentaa.	Palvelutaso räätälöitävissä täysin tarpeiden mukaiseksi käytössä olevien resurssien puitteissa. Voidaan hyödyntää paikallista reunalaskentaa.	Palvelutaso räätälöitävissä täysin tarpeiden mukaiseksi käytössä olevien resurssien puitteissa. Voidaan hyödyntää paikallista reunalaskentaa.

[3] https://www.traficom.fi/sites/default/files/media/file/Muistilista-yrityksille-suuntaviivojen-edellyttamista-muutoksista.pdf.

Datan eriytettävyys paikallisesti	Data ei eriytettävissä paikallisesti, vaan kulkee teleyrityksen verkon kautta.	Data ei pääsääntöisesti eriytettävissä paikallisesti, vaan kulkee teleyrityksen verkon kautta.	Data mahdollista eriyttää paikallisesti ja pitää paikallisen verkon piirissä.	Data mahdollista eriyttää paikallisesti ja pitää paikallisen verkon piirissä.	Data mahdollista eriyttää paikallisesti ja pitää paikallisen verkon piirissä.
Taajuuksien käyttö	Toimitaan teleyrityksen julkisen verkon taajuuksilla. Vastuu on teleyrityksellä.	Toimitaan teleyrityksen julkisen verkon taajuuksilla. Vastuu on teleyrityksellä.	Toimitaan teleyrityksen julkisen verkon taajuuksilla. Vastuu on teleyrityksellä.	Toimitaan teleyrityksen taajuuksilla, mutta vastuu on radioluvan haltijalla, jos toteutukselle on haettu oma radiolupa.	Toimitaan omilla taajuuksilla. Vastuu on radioluvan haltijalla.
Vastuu kyberturvallisuuteen liittyvien lakisääteisten velvoitteiden toteutumisesta	Vastuut verkon osalta teleyrityksellä.	Vastuut verkon osalta teleyrityksellä.	Vastuut verkon osalta teleyrityksellä. Organisaation velvoitteiden laajuus riippuu sen roolista ja oman toiminnan luonteesta.[4] Organisaatio vastaa yleiseen viestintäverkkoon liittämisen turvallisuudesta osaltaan.	Vastuu verkon haltijalla. Organisaation velvoitteiden laajuus riippuu sen roolista, oman toiminnan luonteesta sekä siitä, liitetäänkö toteutus yleiseen viestintäverkkoon.	Vastuu verkon haltijalla. Organisaation velvoitteiden laajuus riippuu sen roolista, oman toiminnan luonteesta sekä siitä, liitetäänkö toteutus yleiseen viestintäverkkoon.

Taulukko 1. Matkaviestinverkon käytön eri toteutusmallien ylätason ominaisuuksia.

3.1.1 Yleinen viestintäverkko

Yleistä teleyritysten operoimaa matkaviestinverkkoa voidaan käyttää toteutettaessa palveluita. Tämä toteutusmalli voi tarjota hyvän verkon peiton ja kapasiteetin, sekä tietyissä tapauksissa kustannustehokkaan ratkaisun, silloin kun ei ole tarvetta eriyttää verkon hallintaa tai verkossa siirrettävää dataa pois yleisestä matkaviestinverkosta. Vaikka verkon peitto on pääosin hyvä, voi silti olla katvealueita, joissa haluttu datansiirtokapasiteetti ei ole riittävä. Yleisen verkon palvelutaso on oletuksena sama kaikille verkon käyttäjille, mutta palvelutasoon voidaan sopia tiukempia ehtoja teleyritysten kanssa. Tällöin on varmistettava, että

[4] https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/saantelyn-kohteet ja https://www.traficom.fi/fi/viestinta/viestintaverkot/mika-teletoimintaa.

mahdollinen priorisointi täyttää verkkoneutraliteettisääntelyn[5] asettamat kriteerit. Optimoitujen palveluiden osalta pitää myös pystyä osoittamaan, miksi sisältö, sovellus tai palvelu tarvitsee optimointia toimiakseen tietyllä laatutasolla. Tämä laatutaso on täsmennettävä ja on voitava osoittaa, ettei laatutasoa voida taata internetyhteyspalvelun avulla. Optimoitu palvelu ei voi korvata internetyhteyspalvelua. Palvelun laatua koskevien vaatimusten tulee olla objektiivisesti arvioituna tarpeen sisällön, sovelluksen tai jonkin keskeisen palvelua koskevan piirteen takaamiseksi. Traficom tarjoaa apua mahdollisessa tulkinnassa.

3.1.2 Yleisen viestintäverkon viipalointi

Yleisen viestintäverkon viipalointi mahdollistaa verkkoviipaleen käyttäjälle vakaamman palvelutason ja räätälöitävämmät verkon toiminnallisuudet. 5G-verkkoteknologia tarjoaa kaksi eri tapaa (standalone- ja non-standalone-ratkaisut) paikallisen matkaviestinverkon toteuttamiseksi.

Non-standalone 5G-verkkoratkaisussa käytetään teleyrityksen olemassa olevaa LTE EPC (LTE Evolved Packet Core) -ydinverkkoteknologiaa nopeampien ja luotettavampien palvelujen toteuttamiseen. Non-standalone toteutus edellyttää myös, että paikallinen matkaviestinverkko sisältää 4G (LTE) -radiorajapinnan ja taajuudet signalointia varten sekä erilliset taajuudet 5G-radiorajapinnalle varsinaisen datan siirtoon.

Standalone-ratkaisu puolestaan ei ole riippuvainen LTE-teknologiasta. Standalone ratkaisu on pilvinatiivi verkkototeutus, joka on täysin ohjelmallisesti konfiguroitava ja mahdollistaa verkkopalvelujen viipaloinnin (slicing) käyttötarpeen mukaan. Viipalointi voidaan käytännössä toteuttaa eri tavoilla. Se on mahdollista toteuttaa pelkästään radioverkossa tai kokonaisvaltaisemmin radioverkon ja ydinverkon kesken (end-to-end). Viipaloinnin toteutustavalla on vaikutusta turvallisuuteen.

Verkkoviipaloinnilla voidaan esimerkiksi tuotannon kriittisten palvelujen ohjaamiselle määritellä korkeampi prioriteetti ja palvelutaso verrattuna pienemmän prioriteetin tiedonsiirtotarpeeseen, kuten videokuvan lähettämiseen. Verkkoviipaloinnin avulla toteutettu verkkopalvelu mahdollistaa tarvittaessa laajan peiton ja se sopii erityisesti laajaa peittoaluetta tarvitseville käyttötapauksille, jotka edellyttävät tietyt ennalta määritellyt verkkopalvelun laatuvaatimukset.

3.1.3 Yleinen viestintäverkko paikallisella infrastruktuurilla

Kevyimmillään tässä toteutustavassa paikallinen radioverkko, eli tukiasemat, on sijoitettu asiakasorganisaation tiloihin asiakkaan tarpeiden mukaisesti, mutta ydinverkkoratkaisuna käytetään edelleen yleistä operaattoriverkkoa.

Tämän toteutuksen etuna on, että paikallisella radioverkolla voidaan toteuttaa tarvittava verkon peitto ja kapasiteetti juuri halutulle alueelle, sekä määritellä tarvittava palvelutaso radioverkkototeutukselle. Teleyritys on edelleen verkon ylläpitäjä, joten ratkaisun tilaajalla ei tarvitse olla osaamista verkon ylläpidosta.

Tarpeen vaatiessa on mahdollista tuoda myös ydinverkon elementtejä osaksi paikallista toteutusta. Näin voidaan toteuttaa ratkaisu, jossa data pysyy koko ajan

[5] https://www.traficom.fi/fi/viestinta/viestintaverkot/internetin-avoimuus-eli-verkkoneutraliteetti.

paikallisen verkon piirissä. Tämä on usein tärkeää palveluun investoivan asiakkaan oman toiminnan tarpeiden näkökulmasta.

3.1.4 Paikallinen verkko käyttäen teleyrityksen taajuuksia

Teleyrityksen taajuuksilla toteutettava itsenäinen paikallinen verkko voidaan toteuttaa siten, että teleyritys myös ylläpitää verkkoa tai niin, että asiakasorganisaatio itse tai kumppanin kanssa ylläpitää ja operoi verkkoa. Mikäli käytetään teleyrityksen taajuuksia ja toimitaan teleyrityksen radioluvan puitteissa, vastuu radioluvan ehtojen noudattamisesta on teleyrityksellä. Mikäli organisaatio tai tämän kumppani hakee radioluvan, vastuu radioluvan ehtojen noudattamisesta on luvan haltijalla. Tällöin taajuuksien käyttö edellyttää myös teleyrityksen suostumusta.

Paikallinen verkkoratkaisu voidaan toteuttaa täysin erillisenä suljettuna ratkaisuna, jossa data ei poistu paikallisen verkon piiristä missään vaiheessa. Näin voidaan varmistaa, että pääsy verkkoon ja dataan onnistuu vain paikallisesti. Verkkoon voidaan kuitenkin lisätä erikseen yhdysliikennerajapintoja tarpeen mukaan, kunhan huolehditaan sähköisen viestinnän palveluista annetun lain (917/2014 SVPL) mukaisista viestintäverkon ja -palvelun yleisistä laatuvaatimuksista (ml. tietoturva).[6] Tyypillisesti asiakasorganisaation omasta olemassa olevasta sisäisestä verkosta voi olla yhteys paikalliseen matkaviestinverkkoon, jolloin eri toimipisteistä on myös yhteys sinne. Mikäli kyseessä on yhteiskunnan elintärkeän toiminnon kannalta keskeisen toimijan yleiseen viestintäverkkoon liitetty erillisverkko, voi SVPL 244 a § tulla sovellettavaksi (katso luku 4.2.3).

Paikallisessa verkossa voidaan myös tapauksesta riippuen harjoittaa yleistä teletoimintaa,[7] jolloin organisaatiota pidetään teleyrityksenä, ja sitä koskevat lähtökohtaisesti kaikki SVPL:ssä säädetyt teleyrityksen velvollisuudet. Yleinen teletoiminta tarkoittaa sähköisten viestintäpalvelujen tarjontaa ennalta rajaamattomalle käyttäjäpiirille.[8]

Haasteena tässä ratkaisussa on oman radioverkon ja ydinverkon toteuttamistarpeen myötä korkeammat verkon rakentamiskustannukset sekä tarvittava osaaminen itsenäisen verkon ylläpitoon ja operointiin. Jos käyttöön tarvitaan perinteisten televerkon palveluita, kuten SMS tai verkkovierailuominaisuuden toteuttaminen, niidenkin tekeminen tai teettäminen on asiakkaan vastuulla. Verkkovierailun mahdollistamiseksi paikallinen verkko liitetään operaattorin yleiseen viestintäverkkoon, jolloin siihen kohdistuu myös kyberturvallisuuden sääntelyä[9]. Mikäli omalta organisaatiolta puuttuu osaamista verkon rakentamiseen, ylläpitoon ja operointiin, voidaan käyttää myös kolmatta osapuolta, jolla on tarvittava osaaminen.

[6] SVPL 243 § ja tapauksesta riippuen 247 § (ks. luku 4.2.1).
[7] Ks. SVPL 4 § velvollisuudesta tehdä teletoimintailmoitus ja sitä koskevista poikkeuksista. Ks. myös SVPL 6.4 §:ssä säädetty poikkeus toimiluvan vaatimukseen vähäisen paikallisen verkkopalvelun tarjoamisesta.
[8] Kyberturvallisuuden velvoitteisiin ja määräyksiin liittyen Traficomiin voi olla yhteydessä esimerkiksi sähköpostilla osoitteeseen kyberturvallisuuskeskus@traficom.fi.
[9] Katso luku 4.2

3.1.5 Paikallinen verkko käyttäen omia taajuuksia

Itsenäisin ratkaisu paikallisen verkon toteutuksessa on malli, jossa koko verkko on toteutettu paikallisesti ja siinä käytetään Traficomin verkolle myöntämiä omia taajuuksia[10]. Tämän ratkaisun voi toteuttaa yhteistyössä teleyrityksen, verkkolaitevalmistajan tai jonkun muun asiantuntevan toimittajan tai kumppanin kanssa. Verkon pystytys ja operointi on mahdollista myös asiakasyrityksen toimesta, mutta tähän vaaditaan syvää teknistä osaamista niin verkon suunnittelussa, rakentamisessa kuin operoinnissakin.

Etuna tässä ratkaisussa on, että verkko ja verkon käyttämät taajuudet ovat kokonaisuudessaan täysin omassa kontrollissa. Tämän seurauksena myös palvelutason ja tietoturvan toteuttaminen sekä mahdollisen sääntelyn mukaisuuden varmistaminen ovat toimijan omalla vastuulla. Verkkototeutukseen liittyvä sääntely on osattava tunnistaa ja toimittava sen mukaisesti esimerkiksi yhdysliikenteen rajapintojen liittämisen tai yleisen teletoiminnan harjoittamisen osalta.[11]

Omia taajuuksia käytettäessä on myös otettava huomioon Traficomin sille asettamat reunaehdot, kuten radioluvan voimassaoloaika sekä muut luvan tekniset parametrit. Omilla taajuuksilla toimiessa Traficom on ennen taajuuksien myöntämistä tehnyt taajuussuunnittelua, jolla on varmistettu häiriösuoja muita taajuuksien käyttäjiä kohtaan.

Mikäli teleyritysten taajuuksien käyttö tai omien taajuuksien hakeminen ei ole vaihtoehtona, on myös mahdollista hyödyntää luvasta vapaita taajuuksia oman paikallisen verkon toteuttamiseen. Tämä vastaa taajuusmielessä esimerkiksi WLAN-verkkojen toteuttamista. Tässä ratkaisussa tulee kuitenkin huomioida, että luvasta vapailla taajuusalueella on muitakin käyttäjiä yhtäläisin oikeuksin, eikä häiriösuojaa voida taata yksittäiselle toteutukselle. Alueella voi siis olla myös muuta käyttöä samoilla taajuuksilla, joka voi joissakin olosuhteissa häiritä paikallisen verkon toimintaa. Luvasta vapailla taajuuksilla käytettävissä olevat tehotasot ja muut tekniset reunaehdot on määritelty Traficomin määräyksellä 15 (Määräys luvasta vapaiden radiolähettimien yhteistaajuuksista ja käytöstä).[12] Suunnitellun käyttötapauksen toimintavarmuusvaatimukset tuleekin ottaa tarkasti huomioon valittaessa toteutusratkaisua.

3.2 Paikallisten verkkojen vastuut

Paikallisverkkoratkaisuja tarjoavia toimijoita on erilaisia. Tässä luvussa käytetään esimerkkinä teleyrityksiä, joilla on maan kattava, julkinen matkaviestinverkko, jonka asiakkaita voivat olla myös yksityiset ihmiset. Paikallisverkkoratkaisuja tar-

[10] Traficom Paikalliset 4G/5G-verkot: https://www.traficom.fi/fi/viestinta/viestintaverkot/paikalliset-4g5g-verkot
[11] Kyberturvallisuuden velvoitteisiin ja määräyksiin liittyen Traficomiin voi olla yhteydessä esimerkiksi sähköpostilla osoitteeseen kyberturvallisuuskeskus@traficom.fi.
[12] https://www.traficom.fi/fi/saadokset/maarays-15-luvasta-vapaiden-radiolahettimien-yhteistaajuuksista-ja-kaytosta.

joavat toimijat voivat hakea luvat tarvittavien taajuusalueiden käyttämiseen asiakkaan puolesta osana kokonaisratkaisua tai sitten verkko voi käyttää vapaita taajuusalueita, jos kysymyksessä ei ole kovin kriittinen järjestelmä.

Ylätasolla jaoteltuna paikallisten verkkototeutusten vastuunjako asiakasorganisaation ja teleyrityksen välillä menee siten, että mitä lähempänä ollaan yleisen viestintäverkon, eli operaattoriverkon ratkaisua, sitä enemmän vastuu on palvelua tarjoavan teleyrityksen puolella. Mitä lähemmäksi mennään paikallista itsenäistä verkkoratkaisua, sitä enemmän vastuu siirtyy asiakasorganisaation puolelle.

	Yleinen viestintäverkko	Yleisen viestintäverkon viipalointi	Yleinen viestintäverkko paikallisella infrastruktuurilla	Paikallinen verkko käyttäen teleyrityksen taajuuksia	Paikallinen verkko käyttäen omaa taajuusaluetta
Taajuudet	Teleyritys	Teleyritys	Teleyritys	Asiakasorganisaatio / Teleyritys	Asiakasorganisaatio
Verkon toteuttaminen	Teleyritys	Teleyritys	Teleyritys	Asiakasorganisaatio / Teleyritys	Asiakasorganisaatio / Teleyritys
Verkon operointi	Teleyritys	Teleyritys	Teleyritys	Asiakasorganisaatio / Teleyritys	Asiakasorganisaatio
Verkon tietoturva	Teleyritys	Teleyritys	Asiakasorganisaatio / Teleyritys	Asiakasorganisaatio / Teleyritys	Asiakasorganisaatio / Teleyritys
Yhdysliikennerajapinta julkiseen verkkoon	Teleyritys	Teleyritys	Teleyritys	Asiakasorganisaatio	Asiakasorganisaatio
Runkoverkko	Teleyritys	Teleyritys	Teleyritys	Asiakasorganisaatio	Asiakasorganisaatio
Radioverkko	Teleyritys	Teleyritys	Teleyritys	Asiakasorganisaatio	Asiakasorganisaatio
Päätelaitteet	Asiakasorganisaatio	Asiakasorganisaatio	Asiakasorganisaatio	Asiakasorganisaatio	Asiakasorganisaatio

Asiakasorganisaatio Teleyritys

Taulukko 2. Ylätasolla jaoteltu vastuujako asiakasorganisaation ja teleyrityksen välillä eri viestintäverkkoratkaisuissa.

Taulukossa asiakasorganisaation vastuu kattaa myös mahdollisten asiakasorganisaation käyttämien palveluntarjoajien vastuun. Tarkemmin vastuuasioita kyberturvallisuuden osalta käsitellään luvussa 5.

Vastuu päätelaitteista ja niiden tietoturvasta, samoin kun verkkototeutuksen päällä toimivista sovelluksista kuuluu aina asiakasorganisaatiolle. Siirryttäessä paikallisiin toteutuksiin, joissa verkon infrastruktuuria viedään paikan päälle, siirtyy näiden ympäristöjen ylläpitoon ja operointiin liittyvät vastuut asiakasorganisaation puolelle, ellei niitä ole sovittu teleyrityksen tai jonkun muun osapuolen vastuulle. Tässä tapauksessa myös yhdysliikennerajapintojen tietoturvasta huolehtiminen kuuluu oletuksena omalta osaltaan asiakasorganisaatiolle.

Paikallisen verkon verkkosuunnittelun vastuut verkon peitto- ja kapasiteettisuunnittelusta ovat lähtökohtaisesto asiakasorganisaation omalla vastuulla. Suunnittelussa voidaan hyödyntää myös osaavia kumppaneita. Verkkosuunnittelun osalta tulee huomioida myös suunnitelman jatkuva ylläpito mahdollisten uusien tarpeiden sekä muutosten ja päivitysten osalta. Muutostarpeiden seuranta on syytä vastuuttaa selkeästi ja tilanne tarkastaa säännöllisesti. Tarve päivittää suunnitelmaa tai tehdä laaja uudelleensuunnittelu voi myös nousta verkon tai palvelun uuden käyttötapauksen tai -tarpeen myötä. Lisäksi toimintavarmuuden kasvattamiseksi verkkosuunnittelussa voi olla tarpeen toteuttaa alueelle rinnakkaisia verkkoja eri teknologioilla ja taajuuskaistoilla. Vastuu ylläpidosta on syytä sopia tarkasti kaikissa tapauksissa, erityisesti jos käytetään suunnittelu- ja operointikumppania.

Lopuksi on kuitenkin syytä huomioida, että paikallisverkko- tai reunalaskennan palvelu koostuu useista komponenteista ja alustoista ja kokonaisuuden toteuttamiseen osallistuvat monet erilaiset toimijat. Näitä ovat erilaiset laitevalmistajat,

teleoperaattorit, pilvialustojen tarjoajat[13] sekä mahdolliset integraattorikumppanit ja niin edelleen. Jaettu vastuu palvelukokonaisuuden kyberturvallisuudesta muodostuu valitun toteutusmallin mukaan. Monitoimittajapalvelun hallinnassa palvelun omistajan kannalta kokonaishallinnan merkitys toteutuksesta kasvaa. Vastuukysymykset ovat monimutkaiset ja niihin on syytä kiinnittää erityistä huomiota käyttökohteen riskitason ja toimintavarmuusvaatimusten mukaan. On tärkeä ymmärtää tarkasti erilaiset vaikutukset, roolit, vastuut sekä määritellä ne ja varmistaa vastuiden jakautuminen myös sopimustasolla. On myös tärkeää huolehtia, että ne toteutuvat todennetusti eri toimijoiden välillä myös käytännön toiminnan tasolla.

Kokonaispalvelunhallintaan onkin hyvä käyttää ekosysteemiajattelua, jossa eri osapuolille määritellään rooli kokonaisuuden turvallisuuden toteutumisesta ja toimintavarmuudesta. Vastuista ja sopimuksista tarkemmin luvussa 5.2

Vinkki! Verkkosuunnittelu voi olla haastavaa, jolloin on suositeltavaa hyödyntää asiantuntevaa kumppania!

On nähtävissä, että tulevaisuudessa kentälle on tulossa uudentyyppisiä toimintamalleja. 5G-paikallisverkkojen toteutus voi olla hyvin yksinkertaisesta itse käyttöönotettavasta yhden solun verkosta monimutkaisiin kokonaisuuksiin, joissa hyödynnetään koneoppimista ja tekoälyä verkon suunnittelussa, käyttöönotossa ja operoinnissa. Suurten perinteisten toimijoiden lisäksi pienemmät erikoistuneemmat ratkaisujen tarjoajat voivat tehdä asiakkailleen räätälöidympiä ratkaisuja ja toimittaa ne avaimet käteen periaatteella suunnittelusta toteutukseen ja operointiin. O-RAN[14] allianssi omalla työllään mahdollistaa sen, että eri valmistajien radioverkkokomponentteja voidaan käyttää yhdessä verkossa. Tämä tyypillisesti alentaa rakennettavan järjestelmän kustannuksia ja varmistaa komponenttien saatavuutta.

3.3 Reunalaskenta

Reunalaskennan osalta tässä ohjeistuksessa keskitytään pilvipohjaiseen reunalaskentaan. Pilvipohjaisella reunalaskennalla tarkoitetaan ratkaisua, jota voidaan monitoroida ja konfiguroida keskitetysti pilvipalvelualustan tarjoamilla työkaluilla ja jossa voidaan käyttää pilvipalvelualustan palveluja. Ohjeistuksen ulkopuolelle jäävät esimerkiksi paikalliset IoT-toteutukset (Internet of Things), joissa dataa kerätään ja käsitellään erillisellä pilvipalveluihin integroimattomalla palvelimella.

Reunalaskenta voi olla mitä vain tietojenkäsittelyä koostuen samoista toiminnoista, joita tehdään pilvessä. Reunalaskenta voi olla yksinkertaisesta tiedon keräämisestä, varastoinnista ja tarjoamisesta monimutkaisiin toimintoihin, kuten koneoppimiseen.

Pilvipohjainen reunalaskenta laajentaa pilvipalveluja pilven reunalle. Reunalaskenta voi sijaita fyysisesti useassa eri paikassa. Tässä ohjeistuksessa reunalaskenta on jaettu sijainnin perusteella neljään eri kategoriaan seuraavasti:

[13] Pilvialustojen käyttöä käsitellään mm. Traficomin julkaisemassa 5G Security Architecture -ohjeessa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Traficom_5GSecurityArchitecture_A4.pdf
[14] https://www.o-ran.org/

Laitereuna (Device Edge):

Itse laitteeseen, kuten pilvipalvelualustaan kytkettyyn älykameraan toteutettu reunalaskentapalvelu tai -toiminnallisuus.

Paikallinen reunalaskenta (On-premise):

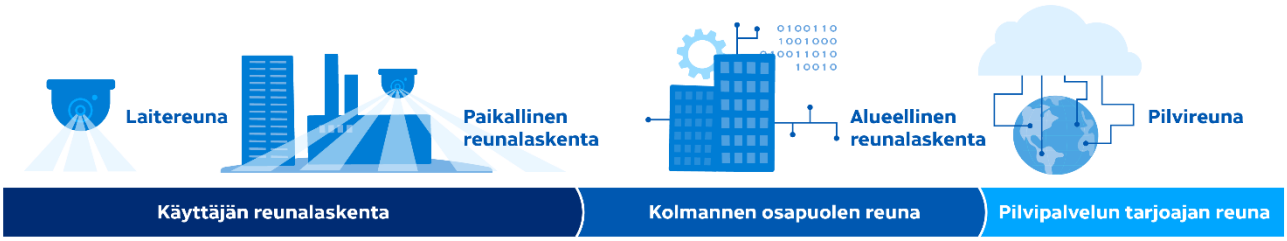
Tuotantolaitoksen, sataman tai vastaavan sijaintipaikan tiloihin tai alueelle toteutettu reunalaskentaratkaisu, johon voi olla kytkettynä lukuisia kameroita ja sensoreita, joiden keräämää dataa prosessoidaan paikallisesti. Ratkaisuja tarjoavilla toimijoilla on näihinkin valmista tarjontaa, joka voidaan asentaa ratkaisun tarjoajan tarjoamaan tai asiakkaan laitteistoon.

Alueellinen reunalaskenta (Regional):

Teleyrityksen, data center toimijan tai vastaavan muun kolmannen osapuolen toteuttama alueellinen, keskitetty reunalaskentaratkaisu, jossa voidaan prosessoida paikallisesti useiden asiakkaiden dataa.

Pilvireuna (Cloud Edge):

Pilvipalveluntarjoajan (mm. Microsoft, Google, Amazon) toteuttama maa- tai aluekohtainen reunalaskentapalveluratkaisu, jossa voidaan prosessoida useiden asiakkaiden dataa.



Kuva 1. Esimerkkikuva reunalaskennan sijaintimahdollisuuksista.

3.4 Reunalaskentaratkaisujen vastuut

Yleisesti voidaan sanoa, että reunalaskentapalvelun osalta asiakasorganisaation vastuut kasvavat, kun toteutus siirtyy lähemmäksi laitereunaa. Mitä lähemmäs pilvipalveluntarjoajan ratkaisua siirrytään, sitä suurempi vastuu on palveluntarjoajan puolella.

	Laitereuna	Paikallinen laskenta	Operaattori-reunalaskenta	Alueellinen reunalaskenta
Reunalaitteet				
Identiteetit ja hakemistoinfrastruktuuri				
Haavoittuvuuksienhallinta				
Verkkotietoturva				
Tietoaineistot				
Sovellukset				
Tilien ja identiteettien hallinta				

Asiakasorganisaatio Teleoperaattori Pilvitoimittaja

Taulukko 3. Reunalaskennan ratkaisujen ylätason vastuujako

Laitereuna- ja paikkakohtaisissa reunalaskentaratkaisuissa tulee ottaa erityisesti huomioon riskit ja uhat, joita liittyy laitteeseen sijoitetun sovelluskerroksen ja itse laitteen suojaukseen. Huomioon otettavia asioita ovat laitteen, esimerkiksi älykameran tai paikallisen reunalaskentapalvelimen osalta:

- Standardien mukainen ja lähtökohtaisesti turvallinen laite vaatii aina asetusten konfigurointia (mm. oletustunnusten ja salasanojen muuttaminen) ja ylläpitoa, muuten se voi olla erittäin haavoittuva osa koko palvelua. Puutteellinen laitteiden suojaus voi avata hyökkäyskanavan myös palvelussa käytettäviin pilviympäristöihin.
- Uusien laiteohjelmistopäivitysten turvaaminen. On määritettävä kuka päivityksiä saa tehdä, sallitaanko automaattiset päivitykset ja kuinka varmistetaan, että päivitysten mukana ei tule vihamielisiä toimintoja
- On määritettävä turvallinen sijoituspaikka ja fyysinen suojaus laitteille ja varmistettava, että laitteisiin pääsevät käsiksi vain henkilöt, joilla on oikeus siihen
- Kontrolli palveluun tallennetun tiedon pitämisestä paikallisena tai siirtämisestä julkipilveen on asiakasorganisaatiolla

Alueelliset reunalaskentaratkaisut ja pilvireunaratkaisut sijaitsevat teleyritysten, pilvipalvelutarjoajien tai vastaavien toimijoiden laitetiloissa, ja näin ratkaisujen fyysinen turvallisuus on palveluntarjoajan vastuulla. Näiden palvelujen tarjoajat ovat usein suurempia toimijoita, jotka tarjoavat usein myös työkaluja ratkaisun tietoturvan toteuttamiseen. Televerkkoihin rakennettavalle reunalaskentakomponentit voivat olla sijoitettuna tukiasemissa tai verkko-operaattorin tiloissa riippuen vaatimuksista. Tälle monikäyttöiselle reunalaskennalle (MEC, Multi-access

Edge Computing) on myös erillinen ryhmä standardointiin ETSI:ssa[15]. Huomioon otettavia erityispiirteitä ovat:

- Palveluntarjoajan luotettavuuden arviointi
- Palveluun tallennettavan ja siinä prosessoitavan tiedon sijainnin ymmärtäminen. Kaikki palveluntarjoajat eivät esimerkiksi takaa, että tieto pysyy Suomen rajojen sisäpuolella
- Turvallisuuden ja salauksen huomioiminen datanlähteiden integroinnissa reunalaskentaratkaisuun
- Tietoliikenneyhteyksien varmistaminen, koska yhteyden toimintahäiriö vaikuttaa palvelun saatavuuteen
- Mahdollinen yhteystarve Suomen rajojen ulkopuolelle, esimerkiksi globaalien pilvitoimittajien palveluissa yleisesti vaaditaan yhteys keskitettyyn palveluun, vaikka toteutus hyödyntäisi pilvireunaa
- MEC-standardointi on jatkuvasti kehittyvä, esimerkiksi nykyisessä ei ole määritelty kontrolleja eri asiakkaiden eriyttämiseksi, jolloin eriyttäminen täytyy toteuttaa muulla tavalla ja kompensoivilla kontrolleilla

3.5 Sopiminen ja sopimukset

Hankittavissa IT-ratkaisuissa ja palveluissa sopimus määrittää osapuolten välisen yhteistoiminnan pelisäännöt, kattaen myös kyberturvallisuuden. Sopimuksen tarkoitus ei ole vain kuvata hankinnan kohdetta, vaan ennen kaikkea taata, että osapuolet ymmärtävät oman vastuunsa, osaavat suunnitella ja toteuttaa toimintansa sen mukaisesti sekä saavuttavat tavoittelemansa hyödyt. Sopimisesta ja vastuista laajemmin luvussa 5.2 Vastuukysymykset ja sopimukset.

Apua sopimiseen saa esimerkiksi Huoltovarmuuskeskuksen ohjeesta Kyberturva ICT-sopimuksissa[16].

Huomioi sopimuksissa:

- Varmista vaatimusten, mukaan lukien kyberturvan, kattavuus tarpeeseen ja palvelun kriittisyyteen verrattuna
- Varmista hallinnointimalli
- Varmista yhteinen ymmärrys palvelun sisällöstä ja vastuista
- Tarkista, että palvelu vastaa tarpeistasi ja vaatimuksiasi
- Muista säännölliset läpikäynnit ja vaatimusten tarkastusoikeus
- Toteuta testaustarkastukset säännöllisesti
- Testaa vastuunjaon toimivuus

[15] ETSI - Multi-access Edge Computing - Standards for MEC.
[16] https://www.huoltovarmuuskeskus.fi/files/c9bab5825e7d15ba2062e5f47e485e5d02d63c45/kyberturva-ict-sopimuksissa.pdf.

Sopimisessa on tärkeä määrittää kontrollit, joiden avulla palveluntarjoajan ja tarjottavan palvelun turvallisuustaso voidaan todentaa. Erityisesti kriittisten palveluiden osalta ei tule vain luottaa toimittajan omaehtoiseen raportointiin, vaan varmistua turvallisuuden toteutumisesta. Tämä on mahdollista esimerkiksi standardinmukaisuus vaatimuksen ja/tai auditointi-/testausoikeuden avulla, jotka tulee huomioida osana sopimuksia. Käytettäessä kansainvälisiä palveluntarjoajia, erityisesti pilvipalveluntarjoajia, on varmistuttava, että huomioidaan paikalliset vaatimukset, saatavuus ja toteutettavien palvelujen kriittisyys. Näiden osalta eivät välttämättä vaatimukset täyty normaaleiden palveluehtojen alla.

Huom! Kolmansien osapuolten kautta on mahdollista saada osaamista mm. operoinnin tietoturvan varmistamiseen, sekä hankkia paikallisia matkaviestinverkkoja kokonaispalveluna, jossa toimittaja huolehtii tietoturvan toteutuksesta.

3.6 Kyberturvallisuuden näkökulmia

Moderni 5G-teknologia omaa lähtökohtaisesti paremmat ratkaisut kyberturvallisuuden varmistamiseen, kuin vanhemman sukupolven matkaviestinverkkoteknologiat. On kuitenkin hyvä muistaa, että teknologian hyödyntäminen uusilla tavoilla ja jatkuvasti kehittyvässä uhkaympäristössä aiheuttaa myös uusia riskejä. Siirtymäaikana ratkaisuja hyödynnetään rinnakkain, jolloin ne ovat vanhan ja uuden teknologian muodostamia hybridejä. Tällöin yhteistoiminnan ja integraatioiden kyberturvallisuus täytyy myös varmistaa.

Paikallisten matkaviestinverkkojen kyberturvallisuuden toteutukseen ja ylläpitoon on syytä varata suunnitteluvaiheesta alkaen riittävästi resursseja ja osaamista. Vaikka järjestelmä tai palvelukokonaisuus hankitaan kokonaispakettina kumppanilta, ostajalla täytyy olla kyvykkyyttä ja osaamista arvioida ja seurata kyberturvallisuuden toteutumista, asettaa vaatimuksia ja valvoa toiminnan onnistumista. Tässä em. työssä asiantuntijakumppaneiden hyödyntäminen on tarvittaessa hyvä ratkaisu.

Lisätietoa turvallisuuteen liittyvistä asioista matkaviestinverkoissa löytyy Euroopan telealan standardoimisjärjestö ETSI:n dokumentaatiosta[17]

Eri teknologioiden ja järjestelmien toimiminen yhdessä

Useimmiten paikallinen matkaviestinverkko joko korvaa kokonaan tai osittain aikaisemman verkkototeutuksen (esimerkiksi paikallisen WLAN-verkon) tai se tuodaan tarjoamaan liitettävyyskyvykkyyttä olemassa olevalle järjestelmälle (esimerkiksi teollisuusohjausjärjestelmä). Tällöin on huomioitava olemassa olevan järjestelmän erityispiirteet niin riskien-, jatkuvuuden- kuin kyberturvallisuuden hallinnan osalta. Osa organisaation vanhoista järjestelmistä (legacy) tulee toimimaan yhdessä paikallisen matkaviestinverkon kanssa. Uuden järjestelmän vaatimuksia määriteltäessä on hyvä huomioida, että vanhojen järjestelmien kyberturvallisuusratkaisut eivät välttämättä ole sellaisella tasolla, kuin nykyratkaisuihin ne olisi mahdollista toteuttaa. Vaikka kyberturvallisuuden osalta jouduttaisiin (perusturvaa vaarantamatta) tekemään kompromisseja, voi uuden järjestelmän turvallisuustaso olla parempi kuin vanhan. Myös toimintavarmuus voi olla uusilla järjestelmillä korkeammalla tasolla. Tällöin vanhan järjestelmän korvaaminen voi olla perusteltua myös kyberturvallisuuden näkökulmasta.

[17] ETSI - TC CYBER Roadmap

Huom! Kyberturvallisuuden näkökulmasta ns. legacy-ratkaisut ja 5G pitää pystyä turvallisesti yhdistämään keskenään. Tämä on syytä suunnitella ja toteuttaa huolellisesti.

Verkkojen ja palveluiden eriyttäminen

Verkkojen eriyttämisessä tulee myös huolehtia tietoturvatasoista ja toimintavarmuudesta. Mahdollisia eriyttämistapoja on useita, kuten täydellinen fyysinen eriyttäminen, erilaiset laiteratkaisut (mm. palomuurit) tai ohjelmistopohjainen, eli looginen eriyttäminen. Eriytyksen ylläpitäminen vaatii jatkuvaa verkon valvontaa sekä käyttövaltuus- ja pääsynhallinnan ylläpitämistä. Moderneissa tiedonkäsittelyympäristöissä voidaan hyödyntää myös erilaisia mikrosegmentointiratkaisuja. Kaikki eriyttämisratkaisut, niin laite- kuin ohjelmistopohjaiset, vaativat kattavan suunnittelun, toteutuksen sekä dokumentoinnin ja jatkuvan ylläpidon.

Huom! Mitä monimutkaisempi ympäristö on kyseessä, sitä vaativampaa ja virheherkempää on ylläpito.

Verkkojen eriyttämisessä tulee erityisesti huomioida asianmukaiset kontrollit eri turvatasojen palveluiden välillä. Esimerkiksi erilaiset testiympäristöt konfiguroidaan yleensä rajallisemmin tietoturvakontrollein, jotta mahdollistetaan tehokas kehitystyö. Mikäli matalan turvatason palvelusta on yhteyksiä korkeamman turvatason palveluihin, voidaan korkeamman tason tietoturvakontrollit pahimmassa tapauksessa kiertää. Omiksi turvatasoikseen on suositeltavaa eriyttää ainakin:

- Erillisverkot (Private network)
- Verkon viipaloinnista vastaavan kumppanin verkko
- Muut kumppanit
- Vanha infrastruktuuri (ns. legacy)
- Pilvipalvelut

Rajapinnat ja yhteydet muihin palveluihin

Mikäli paikallisesta matkaviestinverkosta on pääsy sekä yleiseen viestintäverkkoon, että esimerkiksi yritysverkkoon, yhdysliikennerajapintojen ja -kanavien tietoturvasta täytyy huolehtia tarkasti. Riskit on kartoitettava molemmin suuntaisesti, niin paikallisesta verkosta yleiseen/yritysverkkoon, kuin toisin päin. Lisäksi mm. käyttövaltuus- ja pääsynhallinnasta on varmistuttava sekä erilaiset hallintayhteydet/verkot on huomioitava riskien välttämiseksi. Verkkojen eriytys on tehtävä huolella.

Kyberturvallisuuden kannalta pienempi määrä rajapintoja ulkomaailmaan saattaa helpottaa turvallisen ratkaisun toteuttamista. Tämä puoltaa paikallisen verkkoratkaisun käyttöä, kun on tarve korkean tietoturvan ratkaisulle. On kuitenkin syytä ottaa huomioon, että paikallisessa ratkaisussa tietoturvan toteutus- ja operointivastuu on suurelta osin asiakasorganisaation harteilla.

Laki sähköisen viestinnän palveluista velvoittaa palveluntarjoajan (niin teleyrityksen kuin yleiseen viestintäverkkoon yhteen liitettävän verkon tai palvelun haltijan)

huolehtimaan yhdysliikennerajapinnan tietoturvallisuudesta. Turvattomasti toteutettu rajapinta on merkittävä hyökkäyskanava ja tuottaa potentiaalisesti riskejä sekä paikalliselle matkaviestinverkolle että yleisen verkon kyberturvallisuudelle.

3.7 Toimintavarmuus

Kriittisten organisaatioiden ja palveluiden toimintavarmuus on osa yhteiskunnan huoltovarmuutta. Toimintavarmuuden turvaaminen paikallisverkkoratkaisua toteutettaessa asettaa omat haasteensa ja vaatii osaamista. Siksi on tärkeää punnita huolella käytettävissä olevia resursseja ja osaamista sekä suhteuttaa ne asetettuihin tarpeisiin.

Palveluntoimittajan tai laitteiden valmistajan osalta on tärkeä varmistua tukijakson riittävyydestä ja saatavuudesta. Tämän osalta turvapäivitysten saatavuus on ehdoton edellytys palvelun toimintavarmuuden ylläpidolle. Valmistajan tuen ja sitoutumisen osalta jatkuvuuden varmistaminen on hyvä tunnistaa hankintavaiheessa. Myös osaamisen saatavuudesta on huolehdittava. Esimerkiksi muutos- tai poikkeustilanteissa vaaditaan erityistä osaamista, josta on huolehdittava suunnittelulla riittävässä määrin etukäteen.

Toimintavarmuutta voidaan kasvattaa hyvällä suunnittelulla, riskien hallinnalla ja vähentämällä paikallisen verkkototeutuksen riippuvuutta ulkopuolisista järjestelmistä ja verkoista. Ennen tietyn toteutusmallin valitsemista on kuitenkin syytä pohtia myös muita verkon toimintavarmuuteen liittyviä tekijöitä. Näitä ovat esimerkiksi:

- Kahdennettujen yhteyksien käyttäminen osana toteutusta
- Riittävän radioverkon peiton ja kapasiteetin varmistaminen tarvittavilla alueilla verkkosuunnittelun avulla varautuen myös erilaisiin häiriötilanteisiin
- Vararatkaisujen huomioiminen osana suunnittelua esim. mahdollisuudet hyödyntää nopeasti toista radioverkkoa paikallisen 5G-verkon häiriintyessä
- Varalaitteiden hankkiminen ja niiden toimintakyvystä huolehtiminen tai niiden saatavuuden turvaaminen
- Sähkönsyötön ja riittävän varavoiman saatavuuden turvaaminen
- Erilaisiin häiriö- ja vikatilanteisiin varautuminen ennalta
- Poikkeustilanne ja toipumissuunnittelu (ks. luku 5.6 Jatkuvuudenhallinta)
- Hyökkäyspinta-alan minimointi (ks. luku 5.3.3 Turvallisen suunnittelun periaatteet)

Toimitusketjujen hallinta on huomioitava niin toimittajien, komponenttien kuin osaamisen osalta. Toimintavarmuutta voidaan turvata varalaitteiden hankinnalla, mutta varastoitavien varalaitteiden elinkaaresta on syytä huolehtia ja varmistua säännöllisesti niiden toimintakyvystä. Varalaitteiden ja komponenttien saatavuus on varmistettava suunnittelussa ja operatiivisen ylläpidon aikana. Komponenttien saatavuus, varastointi ja testaus/kierrättäminen on kriittistä, jotta voidaan varmistaa varastoitavien komponenttien toimivuus.

Järjestelmän tuottamiin palveluihin voi tulla katkoksia tai ne voivat estyä kokonaan erilaisten vikojen vuoksi. Laitteisto voi vikaantua, ohjelmistossa tai laitteistossa voi olla suunnittelu- tai toteutusvirheitä, järjestelmän operaattori voi tehdä käyttövirheitä tai ulkoinen tapahtuma voi aiheuttaa vian. Vikaantuminen voi olla lyhytkestoista, pitkäkestoista tai lopullista. Vikasietoisen järjestelmän tarjoamat palvelut eivät keskeydy vikatilanteessa tai palveluihin tulee rajoituksia vain ajallisesti tai vain osaan palveluista riippuen vian suuruudesta ja järjestelmän vikasietoisuudesta.

Erityisesti kriittisten palveluiden osalta tulee varautua myös tilanteeseen, jossa ulkoiset yhteydet menetetään. Kriittisimpien palveluiden toiminta tulee varmistaa myös tällaisessa tilanteessa.

Reunalaskennassa laskenta tehdään lähempänä datan tuottajaa/käyttäjää, jolloin tietoliikenneyhteyden katkeaminen pilvipalveluun ei välttämättä aiheuta välitöntä katkosta palveluun. Jos esimerkiksi tuotantoon liittyvä automaatio on toteutettu toisessa maassa sijaitsevaan julkipilvipalveluun ja näiden palveluiden väliseen yhteyteen tulee häiriöitä tai pahimmassa tapauksessa menetetään koko yhteys, vaarannetaan tuotannon jatkuminen. Tuomalla laskenta lähelle datan lähdettä, voidaan tätä riskiä pienentää merkittävästi.

Laitteiston vikasietoisuuden osalta riski puolestaan kasvaa, mikäli laskenta on keskitetty yhteen paikkaan, jossa laiterikko tai onnettomuus voi vaarantaa koko järjestelmän. Tätä riskiä voidaan pienentää hajauttamalla, esimerkiksi toteuttamalla palvelun kahdennus, elpymistoiminnallisuus (disaster recovery) ja varmuuskopiot toisaalla sijaitsevaan paikkaan. Pilvipohjainen reunalaskenta mahdollistaa toteutuksen, jossa voidaan vapaasti valita, mikä osa tiedosta halutaan pitää paikallisesti ja mikä osa halutaan kopioida pilveen. Tarvittaessa koko järjestelmästä voidaan ottaa varmuuskopiot pilviympäristöön.

Vinkki! Kokeneen asiantuntijatahon hyödyntäminen suunnittelukumppanina luo vakaan pohjan verkkoratkaisuille. Kokenut asiantuntijataho kykenee suunnittelemaan järjestelmän tarpeiden pohjalta ja huomioimaan siinä niin kyberturvallisuuteen, tietoturvaan, kuin toimintavarmuuteenkin liittyvät näkökulmat. Asiantuntijatahoa voidaan hyödyntää myös poikkeustilanteiden harjoittelussa, perustuen erilaisiin skenaarioihin.

Palvelua pyörittävän alustan täydellinen kahdentaminen ja redundanssi voi ratkaista osan toimintavarmuuteen liittyvistä riskeistä, mutta lisää toteutus- ja ylläpitokuluja. Mikäli palvelu ei ole kriittinen, voi palvelujen kriittisten komponenttien kahdentaminen olla riittävä toimenpide. Myös tietoliikenneverkon suunnittelulla voidaan vahvistaa toimintavarmuutta. Verkkorakenne, jossa pyritään tietoliikennereittien kahdennukseen tai rengasrakenteeseen, tukee luonnostaan toimintavarmuutta.

HUOM! Toimintavarmuuden takaamiseksi onkin suositeltavaa pyrkiä kahdentamaan palvelun osia, erityisesti kriittisiä, niin laajasti kuin se on toimintavarmuuden, liiketoimintatarpeen ja budjetin osalta perusteltua.

Yleisen teletoiminnan osalta toimintavarmuutta koskevia tarkempia vaatimuksia on annettu Traficomin määräyksessä viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista (ks. luku 4.2.1).

Toimintavarmuutta on suositeltavaa testata säännöllisesti, tarkemmin testaamisesta luvussa 5.3.3 Turvallisuuden varmistaminen.

3.8 Paikallisen matkaviestinverkon toteutusmallin valinta

Paikalliset matkaviestinverkot kykenevät tuomaan erilaisia digitalisaation hyötyjä toteuttajalleen. Esimerkiksi tuotantolaitoksen eri toimintojen ja prosessien ohjausta voidaan jatkossa hoitaa paikallista matkaviestinverkkoa, reaaliaikaista dataa ja tehokasta laskentaa hyödyntämällä.

Toteuttaessa palveluita toteutusmallin valintaan liittyy hinnan lisäksi muita kriteerejä:

- Toteutettavien käyttötapausten tarpeet
- Vaatimukset verkon suorituskyvylle ja ominaisuuksille
- Verkolta vaadittava peitto/palvelualue
- Organisaation kriittisen datan pysyminen organisaation hallussa
- Toteutuksen kyberturvallisuustaso
    - Huomioiden myös vanhat järjestelmät ja niiden integraatiot
- Rajapinnat muihin palveluihin
- Toimintavarmuuden ja jatkuvuudenhallinnan näkökulma

Onkin tärkeä arvioida kaikki näkökulmat läpi, jotta kyetään varmistamaan palveluiden tarkoituksenmukaisuus, turvallisuus ja toiminnan jatkuvuus. Korvaamalla esimerkiksi olemassa oleviin WLAN-tukiasemiin pohjautunut verkkoratkaisu suorituskykyisellä ja joustavuutta lisäävällä 4G/5G-verkolla saavutetaan välittömästi sovelluskohteen toimintavarmuuteen ja jatkuvuuteen liittyviä hyötyjä. Samalla kuitenkin kyberturvallisuuden varmistaminen uuteen teknologiaympäristöön siirryttäessä vaatii oman työnsä, jotta teknologian päivityksellä ei vaaranneta toiminnan tietoturvaa.

Tärkeä näkökulma on palveluissa käsiteltävän datan hallinta. Datan kriittisyys ja suojaustarve on merkittävä ajuri koko palvelun kriittisyyden määrittelyssä. Tämän lisäksi on ratkaisevaa huomioida missä dataa käsitellään ja tallennetaan, erityisesti mikäli palveluntarjoajia on useampia tai hyödynnetään globaaleita pilvipalveluita. Toimintavarmuuden ja jatkuvuuden näkökulmasta kriittisten palveluiden tiedon täytyy olla omistajan hallussa kaikissa olosuhteissa. Myös riskien ja vaatimustenmukaisuuden varmistamiseksi on hyödyllistä määritellä datan eriyttäminen ja hyödyntää erilaisia kontrolleja datan käsittelyn minimointiin, kuten salaus, anonymisointi tai pseudonymisointi.

Lisäksi tulee muistaa, että mahdollisia sääntelyyn liittyviä juridisia vastuita määräysten ja velvoitteiden noudattamisesta, joita käsitellään tarkemmin luvussa 4, ei voi ulkoistaa yhteistyökumppaneille.

Ekosysteemitasolla eri ratkaisujen vastuukysymykset ovat moninaisia ja vaikutukset eri toteutustavoista palvelun toteuttajalle erilaisia. Vastuukysymyksiin on syytä kiinnittää erityistä huomiota palveluita ja niiden hankintaa suunniteltaessa.

Erityisesti käyttökohteen riskitason ja toimintavarmuusvaatimusten huomioon ottaminen on tärkeää. Toimintavarmuuden kannalta kriittisimpien ratkaisujen osalta on hyvä varautua tilanteisiin, joissa toiminta täytyy kyetä pitämään käynnissä, vaikka yhteydet ulospäin menetetään. Valintojen mukanaan tuomat hyödyt sekä riskit ja uhkat on syytä ymmärtää.

Kaikki käyttötapaukset eivät toki vaadi matkaviestinverkkoteknologian käyttöönottoa. Paikallisten matkaviestinverkkojen lisäksi yritykset voivat käyttää omiin viestintäyhteyksiinsä, kuten kauko-ohjaukseen ja puheyhteyksiin myös muihin teknologioihin perustuvia omia yksityisiä luvanvaraisia radioverkkoja. Lisätietoa näistä löytyy Traficomin verkkosivuilta.[18]

4 Sääntely ja valvonta

Paikallisen matkaviestinverkon toteuttamiseen voi myös liittyä sääntelyä ja velvoitteita. Näiden laajuus riippuu paikallisen verkon toteutustavasta, sen mahdollisesta yhteenliittämisestä yleiseen viestintäverkkoon ja käyttökohteesta itsestään. Tässä luvussa on kuvattu sääntelyyn ja velvoitteisiin liittyviä asioita, jotka voivat tapauksesta riippuen koskea myös paikallisia toteutuksia.

4.1 Sääntelyn ja valvonnan kohteet

Traficomin Kyberturvallisuuskeskus valvoo toimialaansa kuuluvia tietoturvallisuutta, häiriöttömyyttä ja luottamuksellisen viestinnän suojaa koskevia säännöksiä ja määräyksiä sekä ohjaa toimivaltaansa kuuluvia toimijoita niiden noudattamisessa.

EU:n verkko- ja tietoturvadirektiivissä (ns. NIS-direktiivi[19]) säädetään tietoturvavelvollisuuksista ja häiriöraportoinnista useilla eri sektoreilla. Suomessa velvoitteet asetetaan sektorikohtaisessa lainsäädännössä ja niitä valvovat sektoreiden omat valvontaviranomaiset. Sääntelyn soveltamisalan piiriin kuuluvien toimijoiden on huolehdittava palvelujensa ja ICT-infrastruktuurinsa riskienhallinnasta ja tietoturvasta sekä raportoitava havaitsemansa tietoturvauhat ja -loukkaukset toimialansa valvontaviranomaiselle.[20] NIS-direktiivin tulee jatkossa korvaamaan entistä laajempi NIS2-direktiivi, joka pannaan kansallisesti täytäntöön lähivuosina (ks. luku 4.3.1).

Yleisten sähköisten viestintäverkkojen ja yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajien (teleyritysten) velvollisuudesta huolehtia tietoturvasta säädetään EU-tasolla ns. teledirektiivissä[21].

Usein voi esiintyä tulkintakysymyksiä siitä, kuuluuko yrityksen tai yhteisön tarjoama palvelu tai jokin osa siitä Traficomin valvoman sääntelyn piiriin. Keskeistä

[18] https://www.traficom.fi/fi/viestinta/viestintaverkot/taajuuksia-monipuolisesti-yritysten-tarpeisiin
[19] Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa, https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016L1148&from=FI
[20] https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/nis-koordinointi-ja-viranomaisyhteistyo
[21] Euroopan parlamentin ja neuvoston direktiivi (EU) 2018/1972 eurooppalaisesta sähköisen viestinnän säännöstöstä (uudelleenlaadittu), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L1972

on tunnistaa, missä sääntelyn tunnistamissa eri rooleissa tietty toimija toimii. Rooleja voi olla useita, mutta kutakin toimintaa arvioidaan erikseen. Muutama esimerkki sääntelyn, eli ohjauksen ja valvonnan kohteista[22]:

- Erilaiset viestinnän välittäjät:
    - Teleyritykset: esimerkiksi yleisen matkaviestinverkon operaattorit; yleistä teletoimintaa ovat verkkopalvelu ja ennalta rajaamattomalle käyttäjäpiirille tarjotut viestintäpalvelut, jotka muodostuvat kokonaan tai pääosin viestien siirtämisestä viestintäverkossa, sekä ns. henkilöiden välisen viestinnän palvelut
    - Yhteisötilaajat: esimerkiksi yritys, oppilaitos tai virasto, joka on hankkinut teleyritykseltä viestintäpalvelun ja käsittelee omassa viestintäverkossaan käyttäjien viestejä, välitystietoja tai sijaintitietoja
    - Muut viestinnän välittäjät kuin edellä mainitut, jotka välittävät sähköistä viestintää viestinnän osapuoliin nähden kolmantena osapuolena
- Digitaalisen palvelun tarjoajat (DSP): pilvipalvelu, hakukonepalvelu, verkossa toimiva markkinapaikka
- Kriittiset erillisverkot: ydinvoimalan, sataman, lentokentän tai muiden vastaavien yhteiskunnan elintärkeiden toimintojen kannalta keskeisten toimijoiden toimintaa palveleva verkko, joka on liitetty yleiseen viestintäverkkoon.

Kyberturvallisuuden velvoitteisiin ja määräyksiin liittyen Traficomiin voi olla yhteydessä esimerkiksi sähköpostilla osoitteeseen kyberturvallisuuskeskus@traficom.fi.

4.2 Viestinnän välittäjiä koskevia velvoitteita ja määräyksiä

4.2.1 Keskeisiä tietoturvaan ja toimintavarmuuteen liittyviä velvoitteita ja määräyksiä

Sähköisen viestinnän palveluista annetun lain (917/2014, SVPL)[23] 243 §:ssä säädetään viestintäverkon ja -palvelun yleisistä laatuvaatimuksista. Niihin kuuluu velvollisuus suunnitella, rakentaa ja ylläpitää yleiset viestintäverkot ja -palvelut sekä niihin liitettävät viestintäverkot ja -palvelut muun ohella siten, että:

> 1) sähköinen viestintä on tekniseltä laadultaan hyvää ja tietoturvallista;
> 2) ne kestävät normaalit odotettavissa olevat ilmastolliset, mekaaniset, sähkömagneettiset ja muut ulkoiset häiriöt sekä tietoturvauhat;
> 3) niiden suorituskykyä, käytettävyyttä, laatua ja toimintavarmuutta voidaan seurata;
> 4) niihin kohdistuvat merkittävät tietoturvaloukkaukset ja -uhat sekä niiden toimivuutta merkittävästi häiritsevät viat ja häiriöt voidaan havaita; ––
> 7) kenenkään tietosuoja, tietoturva tai muut oikeudet eivät vaarannu; ––
> 9) ne eivät aiheuta kohtuuttomia sähkömagneettisia tai muita häiriöitä taikka tietoturvauhkia;
> 10) ne toimivat yhdessä ja viestintäverkot voidaan tarvittaessa liittää toiseen viestintäverkkoon;

[22] https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/saantelyn-kohteet
[23] https://www.finlex.fi/fi/laki/ajantasa/2014/20140917

> 11) niihin tehtävistä muutoksista ei aiheudu ennakoimatonta häiriötä muille viestintäverkoille ja viestintäpalveluille; ––
> 14) ne toimivat mahdollisimman luotettavasti myös valmiuslaissa (1552/2011) tarkoitetuissa poikkeusoloissa ja normaaliolojen häiriötilanteissa ––.

SVPL 247 ja 247 a §:ssä säädetään erikseen teleyrityksen, viestinnän välittäjän sekä digitaalisen palvelun tarjoajien- velvollisuudesta huolehtia tietoturvasta ja riskienhallinnasta. NIS-direktiivin mukaiset pilvipalveluntarjoajia koskevat velvoitteet, joista säädetään SVPL 247 a §:ssä, voivat soveltua myös virtualisoinnissa käytettävän infrastruktuurin/alustan tarjoajaan, mikäli palvelun katsotaan täyttävän pilvipalvelun määritelmän ja palvelun tarjoaja on vähintään keskisuuri yritys[24].

SVPL 244 §:ssä säädetään Liikenne- ja viestintäviraston valtuudesta antaa SVPL 243 §:ssä tarkoitettuja viestintäverkkojen ja -palvelujen laatua, tietoturvallisuutta ja yhteensopivuutta koskevia määräyksiä. Lisäksi Traficom voi SVPL 247 §:n nojalla antaa määräyksiä tietoturvasta. Alla keskeisiä tietoturvaan ja toimintavarmuuteen liittyviä velvoitteita ja määräyksiä, jotka joitakin poikkeuksia lukuun ottamatta koskevat vain yleistä teletoimintaa:

- Määräys teletoiminnan tietoturvasta (määräys 67)[25]: Tietoturvan toteuttamista koskevat vähimmäisvaatimukset teleyrityksille. Määräyksellä pyritään varmistamaan, että tietoturvatekijät huomioidaan rutiininomaisesti osana verkkojen toteutusta.

- Määräys viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista (määräys 54)[26]: Minimivelvoitteet laitteiden tehonsyötön varmistukselle, laitteiden ja yhteyksien varmistamiselle sekä laitteiden fyysiselle suojaamiselle.

- Määräys viestintäverkkojen ja -palvelujen laadusta ja yleispalvelusta (määräys 58)[27]: Viestintäverkkojen ja -palvelujen toimintavarmuuden, suorituskyvyn, luotettavuuden ja laadun mittaaminen ja varmistaminen.

- Määräys hätäliikenteen teknisestä toteutuksesta ja varmistamisesta (määräys 33)[28]: Varmistetaan hätäpuhelujen normaaleja puheluja paremmat onnistumismahdollisuudet erilaisissa viestintäverkon ruuhka- ja häiriötilanteissa sekä hätäpuheluiden ja hätätekstiviestien sekä niihin liittyvän hätäpalvelun kannalta olennaisen informaation siirtyminen viestintäverkoista hätäkeskuksiin.

- Määräys viestintäverkon sähköisestä suojaamisesta (määräys 43)[29]: Yleisten viestintäverkkojen ja niihin liitettyjen laitteiden ja viestintäverkkojen

[24] Riskienhallintavelvoite ei tällä hetkellä koske NIS-direktiivissä tarkoitettuja mikroyrityksiä tai pieniä yrityksiä.
[25] https://www.finlex.fi/fi/viranomaiset/normi/480001/44046
[26] https://www.traficom.fi/sites/default/files/media/regulation/M%C3%A4%C3%A4r%C3%A4ys_viestint%C3%A4verkkojen_ja_-palvelujen_varmistamisesta_sek%C3%A4_viestint%C3%A4verkkojen_synkronoinnista.pdf
[27] https://www.finlex.fi/data/normit/42162/M58B2014.pdf
[28] https://www.finlex.fi/fi/viranomaiset/normi/480001/27699
[29] https://www.finlex.fi/fi/viranomaiset/normi/480001/5203

suojaamista ilmastollista alkuperää olevilta ja sähkölaitteistojen aiheuttamilta ylijännitteiltä ja ylivirroilta.

SVPL 275:ssä säädetään eräille toimijoille velvollisuus ilmoittaa palveluaan koskevasta häiriöstä Traficomille.

- Teleyritykset: ilmoitettava viipymättä, jos sen palveluun kohdistuu tai sitä uhkaa merkittävä tietoturvaloukkaus taikka muu tapahtuma, joka estää viestintäpalvelun toimivuuden tai häiritsee sitä olennaisesti. Teleyrityksen on ilmoitettava myös ilman aiheetonta viivästystä häiriön tai sen uhan arvioitu kesto ja vaikutukset, korjaustoimenpiteet sekä ne toimenpiteet, joilla häiriön toistuminen pyritään estämään. Teleyrityksen tulee ilmoittaa myös henkilötietojen tietoturvaloukkauksesta (komission asetus (EU) N:o 611/2013).

- DSP-toimijat: ilmoitettava viipymättä sen palveluun kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä.

- Määräys teletoiminnan häiriötilanteista (määräys 66)[30]: Velvoitteet teleyrityksille tietoturva- ja toimivuushäiriöiden havaitsemista ja hallintaa kuin niistä ilmoittamista ja tilastointia varten.

4.2.2 Varautuminen

SVPL:n luvussa 35 (281–284 §:t) säädetään varautumisesta normaaliolojen ja poikkeusoloihin. Varautumisvelvoitteet koskevat pääosin teleyrityksiä.

- Muun muassa kyky palauttaa viestintäverkon kriittinen järjestelmä ja sen hallinta Suomeen käytettäessä valmiuslain mukaisia toimivaltuuksia.

- Suositus teletoiminnan varautumisesta (suositus 311) antaa teleyrityksille neuvoja lain varautumisvelvoitteiden täyttämiseen: suosituksessa on nostettu esiin asiakokonaisuuksia, joita Liikenne- ja viestintävirasto suosittelee teleyrityksiä ottamaan huomioon osana varautumisvelvollisuutta ja olemassa olevia varautumiskäytäntöjä. Suositus on osin salassa pidettävä.

4.2.3 Viestintäverkon kriittisissä osissa käytettävät laitteet

SVPL 244 a §:ssä säädetään kiellosta käyttää viestintäverkon kriittisissä osissa verkkolaitetta, jos on painavia perusteita epäillä, että laitteen käyttäminen vaarantaisi kansallista turvallisuutta tai maanpuolustusta (käyttökielto). Tällä tarkoitetaan sitä, että käytöllä mahdollistettaisiin ulkomainen tiedustelutoiminta tai toiminta, jolla häirittäisiin, lamautettaisiin tai muuten vahingollisella tavalla vaikutettaisiin Suomen tärkeisiin etuihin, yhteiskunnan perustoimintoihin tai kansanvaltaiseen yhteiskuntajärjestykseen. Traficom voi edellytysten täyttyessä velvoittaa viestintäverkon omistajan tai muun haltijan poistamaan viestintäverkkolaitteen verkosta.

Viestintäverkon kriittisillä osilla tarkoitetaan lain mukaan verkon keskeisiä toimintoja ja toimenpiteitä, joilla kontrolloidaan tai ohjataan olennaisella tavalla verkkoon pääsyä ja verkossa kulkevaa liikennettä. Traficomin määräyksessä viestintäverkon

[30] https://www.finlex.fi/fi/viranomaiset/normi/480001/42167

kriittisistä osista[31] määrätään viestintäverkon kriittisten osien tunnistamisesta ja dokumentoinnista ja määritellään viestintäverkon kriittiset osat.

Käyttökielto koskee paitsi yleisiä viestintäverkkoja myös ns. kriittisiä erillisverkkoja, joilla tarkoitetaan ydinvoimaloiden, satamien, lentokenttien ja vastaavien yhteiskunnan elintärkeiden toimintojen kannalta keskeisten toimijoiden yleiseen viestintäverkkoon liitettyjä erillisverkkoja.

4.2.4 Välitystietojen ja viestinnän käsittely

SVPL 17 luvussa säädetään viestinnän luottamuksellisuudesta. Viestinnän osapuoliin nähden sivullinen viestinnän välittäjä voi käsitellä välitystietoja ja viestejä ainoastaan laissa säädettyihin tarkoituksiin. Niillä on lisäksi vaitiolovelvollisuus. Tämä sähköisen viestinnän tietosuojasääntely tulee ottaa huomioon yleisen tietosuojasääntelyn, kuten yleisen tietosuoja-asetuksen (GDPR) ohella.

Alla olevasta taulukosta 4 voi tarkastella sovellettavat keskeiset tietoturvaan ja toimintavarmuuteen liittyvät velvoitteet, verkon tyypistä riippuen. Yleisellä viestintäverkolla tarkoitetaan viestintäverkkoa, jota käytetään viestintäpalvelujen tarjontaan ennalta rajaamattomalle käyttäjäpiirille. Muulla viestintäverkolla tarkoitetaan sellaista rajatun käyttäjäpiirin käytössä olevaa verkkoa, jota ei pidetä yleisenä viestintäverkkona. Viestinnän välittäjällä tarkoitetaan teleyritystä, yhteisötilaajaa ja sellaista muuta tahoa, joka välittää sähköistä viestintää muutoin kuin henkilökohtaisiin tai niihin verrattaviin tavanomaisiin yksityisiin tarkoituksiin. Yhteen liittämisellä tarkoitetaan esimerkiksi sitä, että matkaviestinverkon tekniikalla toteutetusta erillisverkosta on yhteys internetiin kiinteän verkon yhteen liittämisen kautta tai mahdollisuus soittaa puheluita erillisverkon ulkopuolelle.

[31] https://www.finlex.fi/fi/viranomaiset/normi/480001/47015

Taulukko 4 Keskeiset tietoturvaan ja toimintavarmuuteen liittyvät velvoitteet.

	Yleinen viestintäverkko	Muu viestintäverkko, joka liitetty yleiseen viestintäverkkoon	Muu viestintäverkko, jota ei ole liitetty yleiseen viestintäverkkoon
Viestintäverkon ja -palvelun yleiset laatuvaatimukset (SVPL 243 §)	kyllä	kyllä, yhteenliittämisen osalta	ei
Viestinnän välittäjän velvollisuus huolehtia tietoturvasta (SVPL 247 §)	kyllä	vain jos välitetään viestintää	vain jos välitetään viestintää
Määräys teletoiminnan tietoturvasta (määräys 67)	kyllä	ei	ei
Määräys viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista (määräys 54)	kyllä	ei	ei
Määräys viestintäverkkojen ja -palvelujen laadusta ja yleispalvelusta (määräys 58)	kyllä	ei	ei
Määräys hätäilmoitteen teknisestä toteutuksesta ja varmistamisesta (määräys 33)	kyllä	ei	ei
Määräys viestintäverkon sähköisestä suojaamisesta (määräys 43)	kyllä	kyllä	ei
Määräys teletoiminnan häiriötilanteista (määräys 66)	kyllä	ei	ei
Erityinen velvollisuus ilmoittaa häiriöstä ja tietoturvaloukkauksista (SVPL 275 §; määräys 66; komission asetus (EU) N:o 611/2013)	kyllä	ei	ei
Velvollisuus varautua normaaliolojen häiriötilanteisiin ja poikkeusoloihin (SVPL 281 §)	kyllä	vain varautumisvelvolliset*	vain varautumisvelvolliset*
Varautumissuunnittelu (SVPL 282 §)	kyllä	vain varautumisvelvolliset*	vain varautumisvelvolliset*
Kyky palauttaa viestintäverkon kriittinen järjestelmä Suomeen (SVPL 283 §)	kyllä	ei	ei
Kielto käyttää viestintäverkon kriittisissä osissa kansallista turvallisuutta vaarantavia laitteita (SVPL 244 a §) sekä määräys viestintäverkon kriittisistä osista	kyllä	vain jos ns. kriittinen erillisverkko	ei

* Varautumisvelvollisia ovat huoltovarmuuden turvaamisen kannalta keskeisten radiotaajuuksien käyttäjät ja käyttäjäryhmät, joista Liikenne- ja viestintäministeriö päättää Huoltovarmuuskeskuksen esityksestä.

HUOM! Velvoitteiden täyttämisen juridista vastuuta ei voi ulkoistaa yhteistyökumppaneille.

Vinkki! Lisätietoja kyberturvallisuuden velvoitteisiin ja määräyksiin liittyen voi tiedustella esimerkiksi sähköpostilla osoitteesta kyberturvallisuuskeskus@traficom.fi.

4.3 Sääntely kehittyy

4.3.1 NIS-direktiivin uudistaminen (NIS2-direktiivi)

Yhteiskunnan toiminnan kannalta keskeisten toimialojen verkko- ja tietojärjestelmien tietoturvan ja toimintavarmuuden varmistamista koskevan NIS-direktiivin uudistamisella luodaan aiempaa laajemmat puitteet EU:n yhteiselle kyberturvallisuussääntelylle. Niin kutsutussa NIS2-direktiivissä[32] säädetään muun muassa soveltamisalan piiriin kuuluville toimijoille kohdistuvista varautumis- ja riskienhallintavelvoitteista sekä velvoitteesta ilmoittaa toimialan valvovalle viranomaiselle toimintaan kohdistuvista merkittävistä häiriötilanteista. Toimijoita kannustetaan ilmoittamaan vapaaehtoisesti myös kyberturvallisuuteen liittyvistä uhkatilanteista ja läheltä piti -tilanteista. Direktiivissä säädetään myös valvovan viranomaisen valvontatoimivaltuuksista ja siitä, millaisia toimenpiteitä viranomaisen tulee kyetä toteuttamaan osana valvontatehtäväänsä. Direktiivin julkaisun ja voimaantulon jälkeen Euroopan unionin jäsenvaltioilla on vajaat 2 vuotta aikaa saattaa se osaksi kansallista lainsäädäntöään. NIS2-direktiivi on julkaistu 14.12.2022 ja se on saatettava osaksi kansallista lainsäädäntöä 17.10.2024 mennessä. Direktiivin mukaista sääntelyä on sovellettava kaikissa Euroopan unionin jäsenvaltioissa 18.10.2024 alkaen. Tätä ohjetta päivitetään tämän osalta tarpeen mukaan.

4.3.2 Kriittisten toimijoiden häiriösietokykyä koskeva direktiivi (ns. CER-direktiivi)

CER-direktiivillä[33] on tarkoitus kehittää yhteiskunnan kannalta kriittisten toimijoiden varautumista ja resilienssiä asettamalla kansallisesti kriittiseksi arvioiduille toimijoille erityisiä varautumisvelvoitteita häiriönsietokyvyn vahvistamiseksi. Häiriönsietokyky kattaa toimijan kaiken toiminnan, mukaan lukien fyysisen omaisuuden ja infrastruktuurin. Direktiivissä säädetään kriittisten toimijoiden velvoitteesta ilmoittaa niiden toimintaan kohdistuvista häiriötilanteista ja poikkeamista toimialansa valvovalle viranomaiselle sekä valvovan viranomaisen toimivallasta suorittaa tarkastuksia ja saada kaikki tarvittavat tiedot valvontatehtävänsä toteuttamiseksi. CER-direktiivi korvaa vanhan kriittisen infrastruktuurin suojaamista koskevan ECI-direktiivin[34].

[32] Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS 2 -direktiivi), saatavilla osoitteessa: https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32022L2555&from=EN

[33] Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2557, annettu 14 päivänä joulukuuta 2022, kriittisten toimijoiden häiriönsietokyvystä ja direktiivin 2008/114/EY kumoamisesta, saatavilla osoitteessa: https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32022L2557&from=EN

[34] https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32008L0114&from=en

Direktiivi koskee kansallisesti kriittiseksi arvioituja toimijoita seuraavilta sektoreilta: Liikenne, energia, pankit, finanssimarkkinat, terveydenhoito, vesi- ja jätevesihuolto, digitaalinen infrastruktuuri, julkishallinto, avaruus ja elintarvikeala.

CER-direktiivi on julkaistu 14.12.2022 ja se on saatettava osaksi kansallista lainsäädäntöä 17.10.2024 mennessä. Direktiivin mukaista sääntelyä on sovellettava kaikissa Euroopan unionin jäsenvaltioissa 18.10.2024 alkaen. Tätä ohjetta päivitetään tämän osalta tarpeen mukaan.

4.4 Taajuuksien käyttö

Seuraavissa alaluvuissa on lyhyesti kuvattu taajuuksien käytön mahdollisuuksia toimittaessa teleyritysten taajuuksilla tai haettaessa omaa taajuusaluetta paikallisen verkon toteuttamiseen. Radiotaajuuksiin ja taajuuksien käyttöön liittyvissä kysymyksissä Traficomia voi lähestyä esimerkiksi sähköpostilla osoitteeseen radiotaajuudet@traficom.fi.

4.4.1 Teleyrityksen taajuuksilla toimiminen

Yleisimmin teleyrityksen taajuuksilla toimitaan siten, että teleyritys osallistuu tiiviisti paikallisen matkaviestinverkon toteuttamiseen ja tällöin toimitaan teleyrityksen oman radioluvan puitteissa teleyrityksen omilla taajuuksilla. Mikäli teleyritys ei ole kiinnostunut olemaan mukana toteutuksessa, Traficom voi hakemuksesta myöntää radioluvan paikalliselle toteutukselle teleyrityksen taajuuksilla teleyrityksen suostumuksella. Tällöin vastuu radioluvan ehtojen noudattamisesta on luvan haltijalla eli toteuttajalla itsellään.

4.4.2 Omilla taajuuksilla toimiminen

Traficom voi hakemuksen perusteella myöntää taajuudet paikallisille toteutuksille ”First-Come-First-Served”-periaatteella, mikäli hakemus täyttää SVPL 41 § määritellyt radioluvan myöntämisen edellytykset. Jos samalle alueelle tulee samanaikaisesti useampia hakemuksia, ne ratkaistaan yhdessä. Jos taajuuksia ei riitä kaikille, lupa myönnetään hakijoille, joiden toiminta parhaiten vastaa sähköisen viestinnän palveluista annetun lain tavoitteita (mm. viestintäpalvelujen tarjonnan edistämistä, taajuuksien tehokasta käyttöä sekä kilpailua)[35].

Ennen radioluvan hakemista järjestelmän käyttöön tarvittaviin radiotaajuuksiin, suositellaan hakemaan taajuusvarausta radiojärjestelmän suunnittelua varten. Taajuusvaraus on hyödyllinen myös, jos radiolähettimen hankkiminen edellyttää ennakkotietoa käytettävissä olevista radiotaajuuksista.

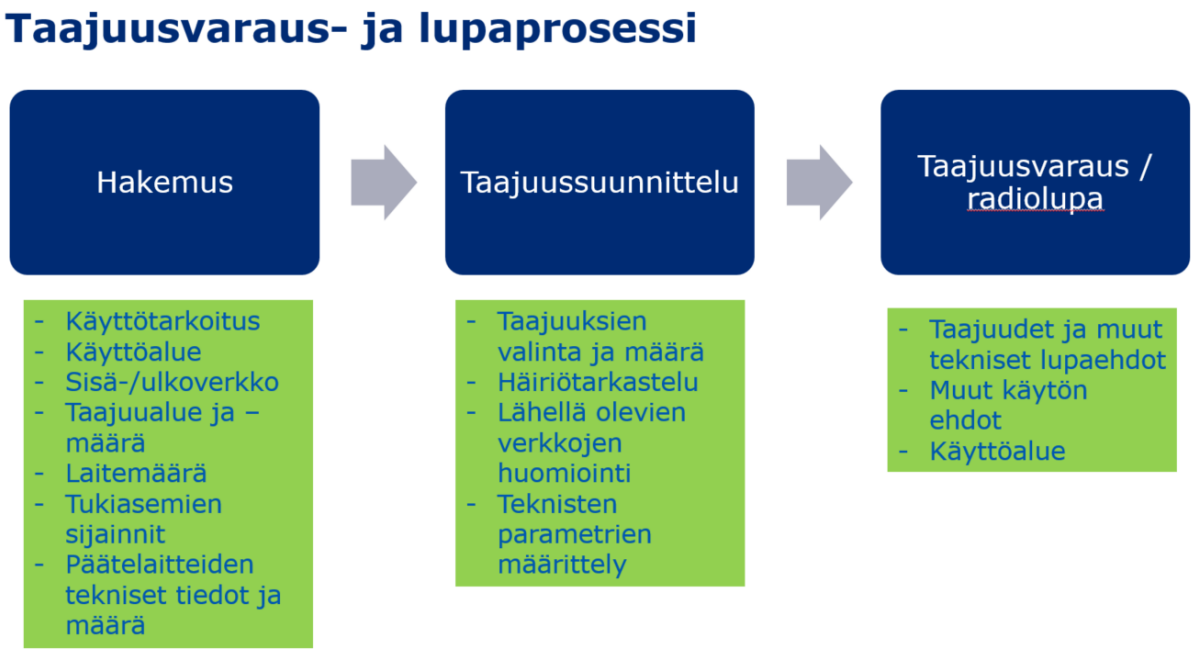
Näin hakija voi jo aikaisessa vaiheessa varmistua, että suunnitellun radioverkon käyttöön on saatavissa tarkoituksenmukaiset taajuudet. Taajuusvaraus myönnetään vain, jos sen myöntämisen edellytykset täyttyvät. Jotta hakijalle voidaan varata teknisesti tarkoituksenmukaisia taajuuksia, tulee hakemukseen liitettävän radioverkkosuunnitelman perustua todelliseen ja toteutettavissa olevaan radiojärjestelmähankkeeseen.

[35] https://www.traficom.fi/fi/viestinta/viestintaverkot/paikalliset-4g5g-verkot

Taajuusvarauksen sijasta voidaan radioverkolle hakea myös suoraan radiolupaa. Radiolupa voidaan myöntää ilman taajuusvarausta, jos lupahakemus radioverkkosuunnitelmineen on riittävän tarkka ja toteuttamiskelpoinen radioluvan myöntämiseksi ja luvan myöntämisen edellytykset myös muilta osin täyttyvät.

Hakemuksessa on esitettävä vapaamuotoinen radioverkkosuunnitelma. Hakemuksessa tulee ilmoittaa haettava taajuusmäärä perusteluineen. Radioluvat myönnetään perustuen taajuustarpeeseen ja paikallisesti käytettävissä olevaan taajuusmäärään.

Radioluvassa määritellään verkon tekniset lupaehdot ja muut käytön ehdot. Ilma-alus käytön (esim. dronet) salliminen päätetään tapauskohtaisesti hakemuksen perusteella. Taajuuksien käytön teknisistä lupaehdoista löytyy lisää tietoa Traficomin paikallisten matkaviestinverkkojen nettisivuilta.[35] Alla olevassa kuvassa on kuvattuna omien taajuuksien hakemisen taajuusvaraus- ja lupaprosessia ja siinä tarvittavia tietoja.



Kuva 2. Omien taajuuksien hakemisen lupa- ja taajuusvarausprosessi.

Radiolupa on voimassa tyypillisesti enintään kuusi vuotta. Radiolupa voidaan yleensä myöntää uudelleen hakemuksesta. Lupaa on suositeltavaa hakea riittävän ajoissa ennen edellisen luvan voimassaoloajan päättymistä.

Taajuusvarauksesta ja radioluvasta peritään taajuusmaksu, joka perustuu taajuusmäärään sekä muihin liikenne- ja viestintäministeriön taajuusmaksuasetuksessa määrättyihin maksuperusteisiin[36].

Vinkki! Lisätietoja taajuuksien käyttöön ja radiolupiin liittyen voi tiedustella osoitteesta radiotaajuudet@traficom.fi.

[36] https://www.finlex.fi/fi/laki/alkup/2019/20191454

4.4.3 Uudet radiolaitteiden tietoturvavaatimukset RED art. 3(3)(d/e/f)

Kaikkien EU-alueella markkinoille saatettavien radiolaitteiden tulee täyttää EU:n radiolaitedirektiivin RED 2014/53/EU[37] vaatimukset. RED on Suomessa saatettu voimaan muun muassa lailla sähköisen viestinnän palveluista (917/2014). RED:n nojalla on annettu uusi asetus 2022/30[38] koskien RED:n artikloja 3(3)(d/e/f). Asetuksessa tietyille RED:n soveltamisalaan kuuluville laitteille, kuten internetiin liitettäville laitteille, leluille, lastenhoitoon liittyville laitteille ja päälle puettaville laitteille, asetetaan tietoturvallisuusvaatimuksia. Uusilla vaatimuksilla suojataan verkkoja, parannetaan käyttäjien yksityisyyden suojaa ja pienennetään sellaisten taloudellisten petosten riskiä, joissa hyödynnetään verkkoon liitettyjä laitteita. Asetuksessa on annettu siirtymäaika laitevalmistajille. EU-markkinoille saatettavien laitteiden pitää olla uusien vaatimusten mukaisia 1.8.2024 lähtien.

5 Kyberturvallisuus elinkaaren eri vaiheissa

Kyberturvallisuus ja toimintavarmuus ovat laaja kokonaisuus ja niitä voidaan parantaa eri tavoin verkon elinkaaren eri vaiheissa. Elinkaaren vaiheilla on omat painopisteensä, joihin on syytä kiinnittää huomiota. Tässä luvussa esitellä asioita, jotka on tarpeen huomioida paikallisia matkaviestinverkkoja ja reunalaskentaa toteutettaessa.

Kyberturvallisuuden erilaisia viitekehyksiä ja työkaluja

Seuraavana on koottuna muutamia hyödyllisiä viitekehyksiä ja työkaluja kyberturvallisuustyöhön.

Tietoturvallisen 5G-arkkitehtuurin osalta Traficom on julkaissut ohjeen:

- 5G Security Architecture | Kyberturvallisuuskeskus[39]

Tietoturvan ylläpitämisen ja kehittämisen tueksi on saatavilla erilaisia työkaluja. Organisaatiolla kyberturvallisuuden kypsyyttä voi arvioida esimerkiksi seuraavien mallien avulla. Malleja voidaan hyödyntää oman organisaation tai palveluntarjoajien yleisen kyberturvallisuuskypsyyden arviointiin:

- NIST – Cybersecurity Framework[40]
- Kybermittari[41]

Kyberturvallisuuden hallintajärjestelmän toteutukseen soveltuvia malleja ovat esimerkiksi:

- ISO27001[42]
- Katakri[43]

[37] https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32014L0053&from=FI
[38] https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32022R0030&from=EN
[39] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Traficom_5GSecurityArchitecture_A4.pdf
[40] Cybersecurity Framework | NIST
[41] https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostot/kybermittari
[42] https://www.iso.org/isoiec-27001-information-security.html
[43] https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille

Palveluidenkontrollien määrittelyn ja arvioinnin tueksi voidaan hyödyntää seuraavia:

- Katakri, PiTuKri[44]
- ISO27002[45]
- CIS Controls[46]

Yllä mainittujen ohjeiden avulla on myös mahdollista arvioida palveluiden kyberturvallisuutta, riippuen työkalusta hieman eri näkökulmista. Arvioinnin voi toteuttaa itse tai hyödyntää ulkopuolista asiantuntijakumppania.

Palvelukehityksessä hyödynnettäviä ohjeita ja malleja ovat esimerkiksi:

- Traficomin ohje: Turvallinen tuotekehitys – kohti hyväksyntää[47]
- OWASP Project Security Knowledge Framework[48]

Yllä mainittu lista ei ole kaiken kattava, vaan muitakin malleja ja työkaluja (maksullisia ja maksuttomia) löytyy. On tärkeä tunnistaa omaan toimintaansa parhaiten soveltuvat työkalut.

5.1 Kyberturvallisuuden erityispiirteitä

Paikallisten matkaviestinverkkojen kyberturvallisuuden erityispiirteitä voidaan jaotella eri tasoihin:

Laiteturvallisuus

- Laitetason tietoturvan toteutus ja varmistaminen kuuluvat yleensä laitetoimittajan vastuulle. Tämän varmistamiseen voidaan hyödyntää valmistajan tietoturvan standardoimista, laitteiden tietoturvaa määrittäviä standardeja tai sopimuksessa määriteltyjä vaatimuksia.

- Erilaiset standardit voivat ohjata laiteturvallisuutta, mutta niiden rajat on hyvä ymmärtää. Esimerkiksi 5G-verkkojen laitteiden radiorajapinnan tietoturvallisuutta määrittää standardisointijärjestöjen yhteistyöelimen 3GPP[49] (3rd Generation Partnership Project) tuottama ohjeistus. Standardien osalta tulee huomioida viive, jolla ne otetaan käyttöön laitteiden osalta. Esimerkiksi 3GPP julkaisee erilaisia standardikokonaisuuksia, joiden osalta saattaa kestää jopa kaksi vuotta, ennen kuin ne on otettu käyttöön laitteissa.

- Standardoitujen laitteiden käyttäminen voi varmistaa tietynlaisen perustason tietoturvallisuuden, mutta turvallisuustoiminnallisuuksien käyttöönottoon ja oikeanlaiseen hyödyntämiseen on syytä perehtyä tarkasti ja arvioida niiden tarkoituksenmukaista hyödyntämistä huomioiden sovelluskohteen riskit. Palvelun omistajan tulee varmistaa myös muulla tavalla, kuten sopimuksilla, laitetason tietoturvan toteutuminen ja sen ylläpito koko palvelun elinkaaren ajan. Tämä pitää sisällään esimerkiksi päivitysten ja tarvittavan tuen saannin

[44] https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/pilvipalveluiden-turvallisuuden-arviointi-kriteeristo-pitukri
[45] https://www.iso.org/standard/75652.html
[46] https://www.cisecurity.org/controls
[47] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Turvallinen_tuotekehitys_Suomi_J003_2018.pdf
[48] https://owasp.org/www-project-security-knowledge-framework/
[49] https://www.3gpp.org/

koko käytön ajalle. Standardoitujen laitteiden osalta on varmistuttava minkä sukupolven standardeja ne noudattavat ja millaisia vaikutuksia näillä on laitteiden tietoturvallisuudelle.

- Laiteturvallisuuden osalta tulee huolehtia myös fyysisestä turvallisuudesta ja laitesuojauksesta.

- Laitetason kyberturvallisuus käsittää niin verkko-, palvelin-, reunalaskenta- kuin päätelaitteiden kyberturvallisuuden ja toimintavarmuuden.

Verkkotason turvallisuus

- Verkkotason tietoturvan toteutus riippuu palvelun toteutusmallista ja siihen liittyvistä vastuista. Yleensä verkkotason tietoturva on operaattorin ja infrastruktuuritoimittajan vastuulla, mutta mikäli paikallinen ratkaisu toteutetaan palvelun omistajan toimesta, tulee verkkotason tietoturvakontrollit huomioida

- Verkkotason tietoturvallisuudessa täytyy ratkaisusta riippuen huomioida:

    - Verkon ja reitityksen tietoturva, verkkoliikenteen suodatus
    - Viestiverkon ja yhteyskäytäntöjen tietoturva (Signalling security)
    - Viestinnän tietoturva ja salausratkaisut
    - Virtualisoinnin tietoturva
    - Infrastruktuurin tietoturva

- Mikäli verkkotasonratkaisut hankitaan palveluna, tulevat niihin liittyvät tietoturvaratkaisut mahdollisesti valmiiksi määritettynä. Sopimustasolla tulee huolehtia, että turvallisuus tarvittaessa kyetään todentamaan, joko kolmannen osapuolen standardoinnin tai auditointi/testausoikeuden kautta.

- Tietoturvallisuus erityisesti verkon rajoilla: varmista reunalaskennan verkkoon turvallinen pääsy hyödyntämällä yhteyden salausta, tarkoituksenmukaista suodatusta, luotettavaa todennusta ja pääsynhallintaa.

Sovellustason turvallisuus

- Sovellustason turvallisuus viittaa paikallisten matkaviestinverkkojen päällä toteutettavien palvelujen ja ratkaisujen tietoturvaan sekä reunalaskennan ratkaisujen tietoturvaan.

- Sovellustason tietoturva kattaa myös asiakkaan vastuulla olevat osiot pilvialustojen tietoturvakonfiguraatioista.

- Sovellustietoturva koostuu useasta osa-alueesta. Osa-alueet ovat toteutusvaiheen riskienhallinta ja uhkamallinnus, toteutuksen aikaisen kontrollien toteutus sekä operatiivisen vaiheen kontrollien suunnittelu ja dokumentointi.

- Sovellustason kyberturvallisuuden vastuu riippuu toteutusmallista:

    - mikäli palvelu ostetaan kokonaisratkaisuna, vastaa palvelun toimittaja valtaosasta teknisistä kyberturvakontrolleista,

- mikäli sovellus toteutetaan itse palvelun omistajan toimesta, tulee heillä olla myös kyvykkyys määrittää, toteuttaa ja varmistaa kyberturvallisuus kaikissa sovelluksen elinkaaren vaiheissa.

Käyttäjien- ja käyttöoikeuksien hallinta

- Käyttäjien- ja käyttöoikeuksien hallinta on perusta kyberturvallisuudelle. Riittävät ja käyttötarpeeseen rajatut käyttöoikeudet mahdollistavat palvelun tehokkaan käytön, mutta rajaavat riskejä, joita tarpeettoman laajat käyttöoikeudet toisivat. Samalla täytyy varmistua käyttäjien asianmukaisesta todentamisesta. Monivaiheista (MFA) tunnistamista on suositeltavaa käyttää aina, kun se vain on mahdollista. Käyttäjien ja käyttöoikeuksien hallinta koskettaa kaikkia toimijoita palvelun osalta.

- Erityisen tärkeää on huolehtia korotetuista käyttäjätunnuksista (esim. pääkäyttäjät), joita voidaan tarvita niin pilvipalveluiden ylläpitoon, operaattorien toimintaan tai muiden järjestelmien ylläpitoon.

- Vastuu käyttöoikeuksien hallinnasta täytyy tunnistaa palvelun kussakin komponentissa. Vastuu tulee myös huomioida sopimuksissa.

- Palveluiden ja ratkaisujen käyttäjien oikeudet käyttää kutakin palvelun toiminnallisuutta on myös kyettävä todentamaan.

Käyttöönoton ja operoinnin turvallisuus

- Paikallisten matkaviestinverkkojen ja reunalaskennan palvelujen käyttöönoton ja operoinnin turvallisuus koostuu kyberturvallisuuden ja toimintavarmuuden vaatimusten tunnistamisesta, koko palvelujen kattavasta riskienhallinnasta, sekä käyttöönoton ja operoinnin aikaisesta kyberturvallisuuden kontrollista.

- Avainhenkilöihin liittyvät riskit ja niiden hallinta on huomioitava toteutettaessa paikallisia matkaviestinverkkoja ja reunalaskennan ratkaisuja huoltovarmuuskriittisissä palveluissa. Kriittisissä rooleissa toimivien henkilöiden taustat tulee varmistaa turvallisuusselvityksillä. Lisäksi avainhenkilöiden osalta on suunniteltava mahdolliset sijaisuudet. Sijaisuuksien määrittely voi tiettyjen osaamisprofiilien osalta olla haastavaa, jos osaamista ei ole organisaatiossa riittävän laaja-alaisesti.

- Palveluntarjoajien osalta avainhenkilöihin liittyvät riskit on huomioitava osana vastuiden määrittelyä ja sopimuksia, jotta esimerkiksi poikkeustilanteissa osaavan työvoiman saatavuus on varmistettu. Myös esimerkiksi kriittisiin tehtäviin liittyvät mahdolliset henkilövaraukset tulee toteuttaa Puolustusvoimien suuntaan (ns. VAP-varaukset[50]). Päivittäiseen toimintaan liittyvän operoinnin kyberturvallisuuden tarpeita ovat mm. tietoturvavalvonnan ja poikkeamiin vastaamisen toteutus, haavoittuvuuksien- ja päivitystenhallinta sekä muutoshallinnan toteutus.

- Tietoturvavalvonta täytyy olla järjestetty siten/niin, että poikkeustilanteet kyetään jälkeenpäin selvittämään. Tämä korostuu erityisesti palveluissa, joissa hyödynnetään yleistä viestiverkkoa tai huoltovarmuuskriittisissä palveluissa.

[50] https://puolustusvoimat.fi/asiointi/henkilovaraukset

Osapuolten täytyy huomioida myös ilmoitusvelvollisuus erilaisista kyberturvallisuustapahtumista osana palvelusopimuksia.

- Kyky tunnistaa uhkia aikaisin on tärkeää. Varmista, että valvonta, uhkien tunnistaminen ja vastaaminen on mahdollista koko reunalaskentaratkaisun osalta. Reunalaskentaratkaisu on lähtökohtaisesti hajautettu, joten proaktiivinen kyky tunnistaa ja reagoida uhkiin on tärkeää niin ympäristöjen, tietoliikenteen kuin laitteiden osalta.

- Verkkotason ratkaisujen tulee täyttää myös erilaisia vaatimuksia, joihin kuuluvat niin EU-tason sääntely, Suomen kansallinen sääntely sekä mahdolliset muut viitekehykset (esim. GDPR).

Vinkki! Palvelujen hankintaan ja toteutukseen voi olla hyödyllistä käyttää kumppania, jolta löytyy asiantuntemusta tarpeellisista kyberturvallisuuteen- ja toimintavarmuuteen liittyvistä asioista.

Konvergenssi perinteisten IT-ympäristöjen (Information Technology) ja erillisverkkoratkaisujen välillä sekä pilvialustojen kasvava hyödyntäminen laajentavat hyökkäyspinta-alaa, avaavat uusia mahdollisuuksia hyökkääjille sekä aiheuttavat riskejä toimittajaketjuun. Hyökkäyspinta-alan minimointi on laajemmin esitetty luvussa 5.3.3 Turvallisen suunnittelun periaatteet. Hybridiratkaisujen riskienhallinnassa täytyy ymmärtää, miten eri sukupolvien teknologioiden integrointi toteutetaan tietoturvallisesti.

Virtualisointi

Virtualisointi ja ohjelmisto-ohjatut verkot (Software Defined Networking, SDN) laajentavat hyökkäyspinta-alaa muun muassa ohjelmistohaavoittuvuuksien sekä rajapintojen laajan hyödyntämisen kautta. Ohjelmallisesti ohjattavat ja konfiguroitavat laitteet ja verkot ovat alttiita niin haavoittuvuuksille kuin inhimillisille virheille. Virtualisoinnin toteutus tietoturvallisesti vaatii asiantuntemusta ja ylläpitoa, kuten muidenkin järjestelmien. Tällöin tulee kyberturvallisuudenhallinnan olla kattavaa ja jatkuvaa myös niiden osalta.

Eri virtualisointitekniikoiden ja toteutustapojen välillä on suuria eroja riskeissä ja kompleksisuudessa. Myös vastuut vaihtelevat riippuen siitä, miten virtualisointia toteutetaan tai hankintaan. Riskit ja uhat sekä vastuut on syytä tunnistaa. Virtualisoinnin tietoturvahaasteita voivat olla ainakin:

- Virtuaalikoneiden puutteellinen elinkaarenhallinta, jolloin vanhoja virtuaalikoneita jää ylläpidon ulkopuolelle sisältäen pahimmillaan sensitiivistä tietoaineistoa

- Virtualisointi-levykuvien tietoturva, ransomware ja muita haittaohjelmia sisältävien levykuvien jakaminen

- Verkkotietoturva, esimerkiksi virtuaalikoneiden välisten yhteyksien hallinta ja sen puutteet sekä puutteellinen eriyttäminen

- Eri luottamustasojen välisten rajoitusten puutteet

- Hypervisor-alustan tietoturvakontrollien puutteet

- Integraatioiden tietoturva, erityisesti pilvipalveluihin

5.2 Vastuukysymykset ja sopimukset

Kyberturvallisuuden huomioimisessa osana ratkaisujen elinkaarta on tärkeä tunnistaa toteutus- tai palvelumallin vastuut eri toimijoiden välillä. Kokonaisratkaisuna hankittu paikallinen matkaviestinverkko asettaa omistajalleen kyberturvallisuuden varmistamiseksi erilaisia haasteita kuin tuotantolaitokseen itse toteutettu paikallinen verkko.

Kumppanienhallintaan voidaan hyödyntää ITIL-viitekehyksen Toimittajahallinta-osiota[51], joka kattaa näkymän niin kumppaneiden tunnistamiseen kuin palvelun aikaiseen hallintaan.

Järjestelmän omistajan vastuu

Järjestelmän omistajalla on vastuu kokonaisuudesta, eikä vastuuta voi täysin ulkoistaa. Eri kyberturvallisuuskontrollien toteutusvastuun voi sopimuksellisesti hankkia kumppanilta, mutta kokonaisvastuu riskienhallinnasta, kyberturvallisuudesta sekä toimintavarmuudesta on aina viimekädessä omistajalla. Hankinta- ja sopimusosaamisen kautta kyetään varmistumaan, että tunnistetut kyberturvallisuustarpeet toteutuvat palvelukumppanin toiminnassa. Tapauksissa, joissa järjestelmän omistaja hoitaa myös toteutuksen kokonaisuudessaan, kaikki vastuu kyberturvallisuuden ja toimintavarmuuden osalta on omistajalla.

Jaettu vastuu

Riippuen toteutusmallista yleensä vastuut kyberturvallisuuden ja toimintavarmuuden osalta on jaettu. Vastuutahoja on ainakin palvelun/järjestelmän omistaja, operaattori, pilvipalvelun toimittaja sekä mahdolliset muut palveluntarjoajat.

Kumppaneita voidaan hyödyntää monessa roolissa:

- Suunnittelukumppani – asiantuntijakumppani vastaa järjestelmän tai palvelun suunnittelusta. Omistajan vastuulla edelleen määritellä liiketoimintatarpeet ja -vaatimukset sekä kyberturvallisuusvaatimukset

- Radioverkkosuunnittelu – erityisen tärkeä osa-alue paikallisten matkaviestinverkkojen suunnittelussa on radioverkkosuunnittelu. Verkon kattavuus, kapasiteetti, katvealueiden hallinta ja mahdolliset varayhteydet on tärkeä suunnitella huolella. Lisäksi suunnitelmat mm. laiterikkojen varalta on tärkeä huomioida.

- Integraattorikumppani – palveluntarjoaja, joka vastaa palvelun toteutuksesta tietylle alustalle. Alustana on esimerkiksi operaattorin verkkosiivu tai pilviympäristö. Integraattorilla voi sopimuksesta riippuen olla kokonaisvastuu kyberturvallisuuden ja toimintavarmuuden suunnittelusta, toteutuksesta ja varmistamisesta.

- Pilvipalveluntoimittaja – pilvipalveluntarjoaja vastaa ympäristönsä ja alustansa kyberturvallisuudesta ja jatkuvuudesta. Tämä tarkoittaa pääasiassa verkko- ja infrastruktuurin kyberturvallisuutta. Sovelluskerros ja soveltuvin osin integraatioiden ja rajapintojen kyberturva ei kuulu palveluntarjoajan vastuulle.

[51] https://wiki.en.it-processmaps.com/index.php/Supplier_Management

- Pilvipalveluiden osalta vastuunjakoon vaikuttaa myös pilven toimitusmalli: julkipilvi, hybridipilvi sekä yksityiset pilvipalvelut.

- Operaattori – Operaattori tarjoaa tietoliikenneverkon ja sen palvelut asiakkaidensa käyttöön. Verkon tietoturvan toteutuksesta ja operoinnista vastaa operaattori.

Huom! Verkko-operaattorin palveluiden osalta on useita mahdollisuuksia hyödyntää heitä myös kyberturvallisuutta parantavissa rooleissa: Esimerkiksi verkon operoinnin ja tietoturvan varmistajana, kun kyse on WLAN- ja toimistoverkkoympäristöjen kokonaispalveluista. Verkko-operaattori kykenee auttamaan palvelunestohyökkäyksien torjunnasta, mutta tämän osalta sopiminen on suositeltavaa tehdä ennen hyökkäyksen kohteeksi joutumista.

Jaetun vastuun osalta on tärkeä tunnistaa erilaisia kyberturvallisuuteen liittyviä ilmoitusvelvollisuuksia. Tällä tarkoitetaan esimerkiksi vaatimusta tiedottaa asiakkaita tai valvojaa erilaisista tietoturvatapahtumista määräaikojen puitteissa. Vaatimukset täytyy tunnistaa ja siirtää eteenpäin palveluntarjoajille osana palvelusopimuksia.

Ratkaisun toteutus kokonaisuudessa palveluntarjoajan vastuulla

Ratkaisun tekninen toteutus on kokonaisuutena palveluntarjoajan vastuulla. Kuitenkin kokonaisvastuu kyberturvallisuudesta ja jatkuvuudesta on palvelun omistajalla, vaikka teknisten kontrollien toteutus on palveluntarjoajan vastuulla. Palvelun omistaja vastaa myös henkilöstönsä koulutuksesta ja tietoturvatietoisuudesta.

Toimittajien osalta on syytä huomioida, että esimerkiksi suurten pilvipalveluntarjoajien palvelut voivat poiketa toisistaan. On syytä selvittää tarkasti, mitä hankittavaan palveluun kuuluu, millaiset palvelun ehdot ovat ja miten vastuut on määritelty. Palvelun hankinnassa on syytä tunnistaa myös muuttuvat sopimusehdot, palveluntarjoajat voivat päivittää ehtojaan. Tällöin palvelun asiakkaan vastuulla on seurata muutoksia, tunnistaa niiden vaikutukset ja arvioida palvelun jatkaminen tai tarve teknisiin muutoksiin palvelun toteuttamisessa.

Lisäksi on tärkeää muistaa, että mahdollisia sääntelyyn liittyviä juridisia vastuita määräysten ja velvoitteiden noudattamisesta, joita käsitellään tarkemmin luvussa 4, ei voi ulkoistaa yhteistyökumppaneille.

Sopimusten merkitys

Sopimisen merkitys vastuiden määrittelyssä on tärkeää. Sopimuskumppanuus varmistaa selvät vastuut ja roolit sen lisäksi, että sopimuksessa kuvataan hankittava palvelu tai järjestelmä. Sopimuksilla varmistetaan myös tuen saatavuus, erityisesti poikkeustilanteissa. Sopimuksessa tulee huomioida matkaviestinverkon toteutusmallin ja palvelumallin vaikutukset kyberturvallisuuden elinkaareen sekä tunnistaa ja sopia kyberturvallisuuteen liittyvistä vastuista

Osana sopimuksia on tärkeä huomioida tarpeet varmistaa palveluntarjoajan tietoturva. Erityisesti kriittisten palveluiden osalta ei tule luottaa vain palveluntarjoajan raportoimaan kyberturvallisuuden tasoon, vaan sopimukseen tulee rakentaa tapoja varmistua todellisesta kyberturvallisuuden tasosta. Näitä voivat olla esimerkiksi vaatimus standardin mukaisuudesta sekä auditointi/testausoikeus joko asiakkaan tai kolmannen osapuolen toimesta.

Sopimuksissa tulee myös huomioida erilaisten ulkoisten vaatimusten täyttyminen ja siirtäminen eteenpäin palveluntarjoajille. Vaatimusten vyöryttämisellä palveluntarjoajalle hallinnoidaan osaltaan omia riskejä. Toki on huomioitava, että juridista riskiä ei voida täysimääräisesti siirtää sopimuksilla.

Traficomin Kyberturvallisuuskeskus on julkaissut sosiaali- ja terveydenhuollon hankintoihin tietoturva- ja tietosuojavaatimukset, joita voi soveltuvin osin hyödyntää myös muissa hankinnoissa.[52]

Vinkki! Sopimusasiantuntijan hyödyntäminen esimerkiksi ulkopuolisena resurssina isompien järjestelmähankkeiden osalta voi olla järkevää, jos organisaatiolla ei ole sopimusasiantuntemusta omasta takaa.

Palvelutasosopimus

Palvelutasosopimus (SLA, Service Level Agreement) on asiakkaan ja palveluntarjoajan välinen sopimus, jossa määritellään palvelulle tietyt vaatimustasot. Sitä mitataan erityyppisillä mittareilla ja palvelutason alittamisesta seuraa yhteisesti sovittu sanktio. Palvelutaso täytyy valita sellaiseksi, että se takaa riittävän palvelun saatavuuden ja laadun ottaen huomioon kustannukset. Palvelutaso määrittelee mm. miten suuren osan ajasta palveluntarjoaja lupaa palvelun toimivan, miten nopeasti palvelun tarjoaja reagoi palvelun häiriöihin ja miten nopeasti palvelu palautetaan toimivaksi häiriötilanteen sattuessa.

Yleisissä viestintäverkoissa on käytössä palveluntarjoajan oletuspalvelutaso, jota voi olla mahdollista parantaa erillisellä sopimuksella. Paikallisen verkkototeutuksen palvelutaso ja saatavuus voidaan toteuttaa yksilöllisemmin. Tasoa voidaan nostaa esim. toteuttamalla varaverkko, verkon kahdennus ja varavoima verkolle. Yleensä palvelutasoa ja saatavuutta nostavat ratkaisut nostavat myös palvelun hintaa ja tekevät verkon ylläpidosta ja hallinnasta monimutkaisempaa.

Korkean palvelutason ratkaisuissa on myös huomioitava, että pelkkä paikallinen ratkaisu ei aina riitä, vaikka paikallisen ratkaisun palvelutaso olisikin korkea. Riskinä voi olla myös paikallisen ratkaisun menettäminen onnettomuuden tai muun tapahtuman seurauksena. Tätä riskiä voidaan pienentää kahdentamalla data ja toiminnallisuus pilveen tai muuhun toisaalla sijaitsevaan ympäristöön, jos se on käyttötapauksen osalta mahdollista. Tietyissä tapauksissa teleyrityksen tulee kyetä palauttamaan kriittinen järjestelmä sekä sen ohjaus, ylläpito ja hallinta Suomeen (ks. luku 4.2.2). Tällainen sääntely tulee tunnistaa ja huomioida suunnittelussa.

[52] KTK: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/sosiaali-ja-terveydenhuollon-hankintojen-tietoturva-ja

5.3 Suunnittelu

Ratkaisun suunnitteluvaihe on tietoturvan osalta ja erityisesti vaatimusten tunnistamisen näkökulmasta erittäin tärkeä. Tietoturvan toteutuksessa myöhemmin elinkaaren aikana tunnistetut tarpeet ovat yleisesti kalliimpia ja hankalampia toteuttaa, kuin jos ne olisi tunnistettu ennen varsinaisen kehitystyön ja toteutuksen aloittamista.

Suunnitteluvaiheen vastuu on pääasiassa kokonaisuutena ratkaisun omistajalla, erityisesti kun määritetään liiketoiminta-, tietoturva- ja jatkuvuusvaatimuksia.

5.3.1 Riskienhallinta

Riskienhallinnan lähtökohtana on ymmärtää, mitkä asiat järjestelmässä tai palvelussa ovat toiminnan näkökulmasta kriittisiä. Tämä onnistuu esimerkiksi mallintamalla toimintaprosesseja ja tunnistamalla liitoskohdat paikallisen matkaviestinverkon tai reunalaskennan järjestelmän sekä ulkopuolisten palveluiden ja verkkojen välillä. Liitoskohtien tunnistaminen auttaa tunnistamaan kriittiset pisteet, joissa toimintaprosessi tukeutuu järjestelmään. Näin kyetään tunnistamaan kriittisiä järjestelmätoimintoja ja toteuttamaan niiden riskienhallintaa.

Ennen kuin kyetään toteuttamaan tehokasta riskienhallintaa, täytyy tunnistaa palvelun eri osa-alueiden vastuut.

Riskienhallinnanprosessi tulee integroida osaksi ratkaisujen elinkaarta sekä esimerkiksi jatkuvuudenhallinnan prosessia. Näin ne tukevat toisiaan ja jatkuvuudenhallinnassa voidaan keskittyä esimerkiksi merkittävimpiin tunnistettuihin riskeihin osana uhkaskenaarioita.

Riskienhallinnan erityispiirteitä

Verkon muuttuminen 5G-teknologioiden avulla yhä enemmän pelkästä siirtoputkesta jaetuksi tiedon tuottamisen ja käsittelyn alustaksi laajentaa riskienhallinnan perspektiiviä. On huomioitava teknologian tuomat riskit, monitoimittajaympäristöön liittyvät riskit sekä ymmärtää paikallisten matkaviestinverkkojen ja reunalaskennan järjestelmien kompleksisuus. Kokonaisjärjestelmien osalta verkon rajat hämärtyvät, niissä hyödynnetään uusia toiminnallisuuksia samalla kun kokonaisuudet laajenevat niin verkkoympäristön, toimijoiden määrän kuin kyberturvallisuusvaatimusten osalta.

Kybervakuuttaminen

Useat vakuutusyhtiöt tarjoavat kybervakuuttamista osaksi organisaation tietoturvan- ja riskienhallintaa. Kybervakuutusten kattavuus vaihtelee toimijoittain suuresta ja täten onkin tärkeää tiedostaa, mitä vakuutuksen alle kuuluu ja millaisia tapahtumia se korvaa. On kuitenkin hyvin tärkeää huomioida, että mahdollinen vakuutus ei itsessään suojaa epätoivotuilta tapahtumilta. Joillain vakuutusyhtiöillä kybervakuutus tuo myös ottajalleen velvoitteita kyber- ja tietoturvan osalta, joten myös näistä on hyvä varmistua, mikäli vakuutusta ollaan ottamassa.

Kannattaa myös huomioida, että iso osa poikkeustilanteista, varsinkin suuremmista kriiseistä, on ns. force majeure -tilanteita, jotka vakuutuksista on yleensä

rajattu pois. Vakuutusten kohdalla on huomioitava, että toimintavarmuuden varmistamista ja varautumista ei voida vakuutuksilla ulkoistaa.

5.3.2 Turvallisuusvaatimusten tunnistaminen ja määrittely

Kriittinen vaihe ratkaisujen suunnittelussa on vaatimusten tunnistaminen. Vaatimusten puutteellisuus voi johtaa merkittäviin viivästyksiin ja ylimääräisiin kustannuksiin myöhemmissä vaiheissa, kun jo toteutettuja osia pyritään saattamaan myöhemmin tunnistettujen vaatimusten mukaisiksi.

Vaatimuksia voidaan tunnistaa useasta lähtökohdasta:

- Liiketoimintavaatimukset: liiketoiminnalle merkittäviä vaatimuksia, joiden täyttyminen edistää liiketoiminnan menestystä. Esimerkiksi palvelun saatavuus omille toiminnoille tai asiakkaille.

- Turvallisuusvaatimukset: organisaation toimintaperiaatteisiin kuuluvien turvallisuusvaatimusten toteutuminen myös paikallisten matkaviestinverkkojen kohdalla. Esimerkiksi turvallisen sovelluskehitysten vaatimusten toteutuminen.

- Vaatimustenmukaisuus (Compliance): organisaatiolle kohdistettuja, ulkoisia vaatimuksia, joiden toteutuminen vaikuttaa esimerkiksi toimiluvan kautta. Yleensä laista, toimialan sääntelystä tai kansallisista tai kansainvälisistä standardeista kumpuavia vaatimuksia. Esimerkiksi henkilötiedon luottamuksellisuuteen liittyvät vaatimukset.

Vaatimusten tunnistaminen täytyy tehdä ratkaisun omistajan toimesta, erityisesti liiketoimintavaatimusten tunnistaminen on mahdotonta tehdä ulkopuolisen toimesta.

5.3.3 Turvallisen suunnittelun periaatteet

Tietoturvallisen suunnittelun periaatteet liittyvät sekä vaatimusten tunnistamiseen että tietoturvallisen arkkitehtuurin määrittämiseen. Tässä luvussa esitetään muutamia periaatteita, joita on suositeltavaa hyödyntää osana ratkaisujen suunnittelua.

Hyökkäyspinta-alan minimoiminen

Hyökkäyspinta-alan minimoiminen viittaa suunnitteluperiaatteisiin, joiden osana palvelun ulospäin näkyvät rajapinnat ja käyttöliittymät pyritään rajoittamaan vain ehdottoman tarpeellisiin. Tämä varmistaa sen, että ratkaisuun päästään ulkopuolelta käsiksi vain tarpeenmukaisin menettelyin ja ylläpitäjän täysin hallussa olevin ratkaisujen kautta. Ulkoisten yhteyksien ja rajapintojen dokumentointi osana suunnittelua on myös tärkeää.

Ulkoverkkoon näkyvät palvelut altistavat erityisesti kyberhyökkäyksille, alla 0 esittää näkökulmia uhka-arvion pohjaksi.

Hyökkäysvektori	Syy	Ratkaisu
Ohjelmointiraja-pinnat (API)	Ohjelmistorajapintojen puutteellinen suojaaminen tai tarpeeton näkyminen ulkoverkkoon.	Tarpeettomien rajapintojen sulkeminen tai piilottaminen.
Käyttöliittymät	Käyttöliittymien puutteellinen suojaaminen tai niissä olevat haavoittuvuudet voivat altistaa erilaisille hyökkäyksille.	Käyttöliittymien tietoturvallinen suunnittelu ja toteutus. Haavoittuvuuksienhallinnan toteutus ja säännöllinen tietoturvatestaus. Tarpeettomien käyttöliittymien ja niiden toiminnallisuuksien poistaminen käytöstä.
Tietoliikenne-verkko	Tietoliikenneverkon haavoittuvuuksien ja konfigurointivirheiden hyödyntäminen erilaisissa hyökkäyksissä, mm.: - Laitteiden ja käyttäjien seuranta - Tiedon salakuuntelu	Tietoverkkoturvallisuuden määrittely ja toteutus, IP-tason tietoturva. Liikenteen seuranta, valvonta ja suodatus. Tiedon salaus ja muu suojaus.
Salasanat	Salasanojen murtaminen tai hyödyntäminen esimerkiksi phishing-hyökkäysten kautta.	Pelkän salasanatunnistautumisen rajaaminen, MFA-ratkaisuiden käyttöönotto. Henkilöstön tietoisuuden kehittäminen phishingin osalta.
Henkilöstö	Henkilöstön kautta realisoituvat tietoturvauhat: - Phishing-hyökkäykset - Kiristäminen - Sisäpiirin rikokset	Henkilöstön tietoturvatietoisuuden kehittäminen. Vaarallisten työyhdistelmien tunnistaminen ja rajoittaminen. Pääkäyttäjäoikeuksien rajaaminen, ns. break-the-glass tunnisteiden hyödyntäminen.
Palvelut	Ulkoverkkoon näkyvien palveluiden kautta realisoituvat uhat mm. haavoittuvuuksien kautta.	Palveluiden alasajo, haavoittuvuuksien- ja päivitystenhallinta.

Taulukko 5. Huomioitavia hyökkäysvektoreita.

Hyökkäyspinta-alan tunnistaminen, minimointi ja dokumentointi on tärkeä tehdä ratkaisun omistajan toimesta tai vähintäänkin omistajan tulee osallistua toteutukseen. Näin kyetään haastamaan esimerkiksi erilaisten ylläpitoyhteyksien tarve, jotka palveluntarjoajan mielestä voivat olla tarpeellisia, mutta kokonaistietoturvan näkökulmasta ovat merkittäviä riskejä.

Hyökkäyspinta-alan minimoinnissa paikallisten matkaviestinverkkojen osalta tulee huomioida ainakin:

- Vähimmän käyttöoikeuden periaate – erityisesti ylläpitäjätunnusten hallinta
- Ylläpitoyhteyksien suojaaminen ja ohjaus esimerkiksi suojattujen VPN-yhteyksien kautta

- Verkkoliitosten määrän rajoitus ja suojaaminen
- Verkkorakenteen ja segmentoinnin toteuttaminen tukemaan eri turvatason verkkoalueita
- Integraatioiden suojaaminen
- Yhdysliikennerajapintojen minimointi ja suojaaminen – erityisesti yleisiin verkkoihin
- Yleiseen viestintäverkkoon näkyvien komponenttien rajoittaminen ja suojaaminen

Oletusasetusten turvallinen konfigurointi (Secure-by-Default)

Oletusasetusten turvallinen konfigurointi viittaa suunnitteluperiaatteeseen, jossa ratkaisun komponenttien (mm. laiteohjelmistot (firmware), käyttöjärjestelmät, sovellukset) oletuskonfiguroinnit määritetään tietoturvallisiksi sekä konfiguroidaan ylimääräiset toiminnallisuudet pois päältä muuttamalla esimerkiksi oletuskonfiguraatiot ja -käyttäjätunnukset. Käyttäjätunnukset yksilöidään ja niiden tarvitsemat oikeustasot minimoidaan. Periaatteen mukaisesti nämä tarvittavat muutokset tehdään aina osana komponenttien käyttöönottoa.

Syvyysajattelu tietoturvakontrollien toteutuksessa (Defence-in-depth)

Suunnittelussa syvyysajattelu tarkoittaa sitä, että ratkaisuun suunnitellaan useita suojaustasoja. Syvyysajattelusta käytetäänkin usein termiä monitasoinen suojaus tai turvallisuus. Tällöin mikäli kontrollit yhdellä tasolla eivät toimi tai ovat kierrettävissä, koko ratkaisun tietoturva ei vaarannu.

Esimerkiksi ratkaisun arkkitehtuurin suunnittelussa ei tule luottaa siihen, että kerros palomuureja verkon rajalla tuottaa kattavan tietoturvan. Yksittäiset kontrollit ovat aina kierrettävissä, joko teknisesti tai inhimillisiä heikkouksia hyödyntäen, kuten phishing-hyökkäyksissä.

Paikallisten matkaviestinverkkojen kerroksellinen tietoturva onkin suunniteltava palveluiden tasot huomioiden, ainakin:

- Fyysinen turvallisuus ja laitesuojaus
- Palvelintietoturva
- Virtualisointikerroksen tietoturva
- Verkkotietoturva
- Laitetietoturva ja fyysinen suojaus
- Käyttäjätietoturva ja -tietoisuus

Oletusarvoinen tietoturva (Secure-by-Design)

Oletusarvioinen tietoturva tarkoittaa suunnitteluperiaatetta, jossa tietoturva huomioidaan kaikissa vaiheissa ja komponenttien osalta. Paikallisten matkaviestinverkkojen ja reunalaskennan ratkaisuiden oletusarvioisen tietoturvan suunnittelussa on huomioita erityisesti seuraavat näkökulmat:

- Kattavan autentikoinnin käyttö – sekä lähettävän- että vastaanottavan pään autentikointi luotettavuuden varmistamiseksi ja end-to-end yhteyden suojaamiseksi
- Oletus avoimesta verkosta – suunnittelussa ei tule luottaa laitteiden tai prosessien oletusturvaan, vaan toteuttaa suojaus osana palvelun tai järjestelmän suunnittelua, esimerkiksi varmistamalla syvyyssuojauksen toteutumisen
- Ymmärrys siitä, että jokainen yhteyspiste ja integraatio voidaan murtaa – vaaditaan salausta koko viestintäketjun yli siten, että mahdollisesti salakuunneltu liikenne on hyödytöntä hyökkääjälle

Turvallisuus vikatilanteissa (Fail safe)

Kun tietotekninen maailma tukee ja jopa ohjaa fyysisen maailman toimintoja, on erityisen tärkeä varautua vikatilanteisiin. Tällöin esimerkiksi itseohjautuvan ajoneuvon ohjaus matkaviestinverkon yli ja ohjausyhteyden vikaantuminen on tilanne, jossa fyysisen maailman tarpeet ohjaavat suunnittelua. Itseohjautuvan ajoneuvon ohjausyhteyden katkeaminen asettaa fyysisen turvallisuuden ja työturvallisuuden riskin alle. Onkin suositeltavaa konfiguroida tällainen ratkaisu automaattisesti pysäyttämään itseohjautuvan ajoneuvon turvallisesti, jos ohjausyhteys katkeaa.

Paikallisten matkaviestinverkkojen vikatilanteita voivat olla esimerkiksi yhteyskatkot, laitteiden vikaantuminen tai ohjelmistojen kaatuminen. Ratkaisujen suunnittelussa tulee ymmärtää erilaisten vikaantumisten vaikutus ja huomioida ne suunnittelussa.

5.3.4 Uhkamallinnus

Uhkamallinnuksella tarkoitetaan turvallisuusanalyysin tekemistä ratkaisulle. Analyysissä pyritään tunnistamaan mahdollisia riskejä, uhkia sekä heikkoja kohtia. Uhkamallinnuksessa on hyödyllistä kyetä ajattelemaan kuten mahdollinen hyökkääjä; tunnistamaan kohtia, joita ulkopuolinen voi kyetä hyödyntämään tai joiden toimintaa ulkopuolinen kykenee häiritsemään.

OWASP[53] suosittelee uhkamallinnukseen strukturoitua toteutustapaa, jossa tunnistetaan:

- Mitä olemme toteuttamassa? Ratkaisun toteutussuunnitelma, arkkitehtuuri, määrittelyt ym.
- Mikä voi mennä pieleen? Mitä osia ratkaisussa voidaan käyttää väärin, mikä voi rikkoutua, miten käyttöoikeuksia voidaan hyödyntää vääriin tarkoituksiin jne.
- Miten tunnistettujen väärinkäyttöskenaarioiden vaikutusta voidaan pienentää? Kuinka estää ratkaisun osakomponenttien väärinkäyttö, kuinka suojataan käyttöoikeuksia ja kirjautumisia ym.
- Arvio uhkamallinnuksen ja hallintakeinojen kattavuudesta.

[53] https://owasp.org/www-community/Threat_Modeling

Uhkamallinnuksen avulla on mahdollista tunnistaa ratkaisun väärinkäyttöä, uhkatoimijoita, hyökkäysvektoreita ja -malleja sekä kehittää suunnittelumalleja ja kompensoivia kontrolleja tunnistettuihin uhkatekijöihin. Uhkamallinnuksessa on tärkeä huomioida palvelun kriittisyys.

Uhkamallinnuksen tuloksia voidaan hyödyntää myös jatkuvuudenhallinnassa sekä varautumisessa erilaisiin poikkeustilanteisiin (esimerkiksi löytämällä erilaisia uhkaskenaarioita).

Eri toimintakerrosten huomioiminen osana uhkamallinnusta on tärkeää. Ohessa esimerkinomainen lista paikallisten matkaviestinverkkojen ja reunalaskennan palveluiden ja järjestelmien osalta:

Palvelukerros	Ydinverkko	Reunaverkko ja -laitteet	Radioverkko	Laitekerros
• Pilvipalvelu-haavoittuvuudet • Sovellushaavoittuvuudet • API-ohjelmistorajapinta-haavoittuvuudet	• Ohjelmisto-haavoittuvuudet • Palvelunesto-hyökkäykset (DoS ja DDoS) • Haasteet ja virheet virtualisoinnissa • Jaettujen alustojen uhat (mm. sivukanavahyökkäykset)	• MEC (Multi-access Edge Computing) komponenttien konfigurointivirheet ja haavoittuvuudet • Laajassa MEC-ekosysteemissä huomioitava myös mahdolliset kumppanit ja heidän tietoturva • Kontrolloimattomat noodit (rogue nodes) • Haasteet autentikaation kanssa • Erilaiset hyökkäystekniikat	• Yhteyksien häirintä (jamming) • Väliintulo-hyökkäykset (Man-in-the-middle) • Liikenteen kuuntelu • Signalointi hyökkäykset (radioverkon palveluesto)	• Kaapatut laitteet • Hajautetut palvelunesto-hyökkäykset • Väliintulo-hyökkäykset • Haittaohjelmat

Taulukko 5. Matkaviestinverkkojen ja reunalaskennan uhkia

Huomiota paikallisten matkaviestinverkkojen uhkamallinnuksessa kannattaa erityisesti kiinnittää palvelujen ja verkon rajoille, rajapinnoille, käyttöliittymiin sekä eri tahojen vastuun rajoille. Varsinkin vanhemman, ns. legacy-infrastruktuurin liittäminen paikalliseen verkkoon tai avaamaan sen kautta yhteyden muuhun IT-infrastruktuuriin saattaa aiheuttaa uusia uhkia.

Myös GSMA on tuottanut osana 5G Security Knowledgebase[54] uhkamallinnustyökaluja sekä -skenaarioita. ENISA:n raportista luvusta ”3.12.1 SECURITY CONSIDERATIONS, Risks related to legacy technologies” löytyy laajemmin perinteisten televerkkoteknologidoiden riskeistä [55]

Teknologian tuomista riskeistä yksi tärkeä huomioonotettava asia on televerkoissa käytössä oleva vanha SS7 (Signalling System 7) -protokolla, jota luotaessa ei olla huomioitu tietoturvan merkitystä. Myös uudemmassa Diameter-protokollassa on turvallisuuspuutteita. Jos televerkkoon avataan yhteys, jossa käytetään vanhoja protokollia, pitää turvallisuudessa ottaa huomioon protokollien turvallisuuspuutteet, esim. yhteys pitää olla salattu, verkkoon saa päästä käsiksi vain luotettu henkilökunta jne. Lisätietoa SS7- ja Diameter-protokollien haavoittuvuuksista ja niiden huomioonottamisesta turvallisuudessa löytyy muun muassa ENISA:n raportista Signalling Security in Telecom SS7/Diameter/5G[56].

Vinkki! Uhkamallinnuksen tukena on suositeltavaa käyttää myös ulkopuolista asiantuntija-apua. Ulkopuolinen näkökulma on erityisen tärkeää tunnistettaessa palveluun liittyviä uhkia ja haavoittuvuuksia. Useat tietoturvatoimijat ylläpitävät sovellustietoturvaan ja uhkamallinnukseen erikoistuneita yksiköitä.

5.3.5 Tietoturvallinen arkkitehtuuri

Tietoturvallisen arkkitehtuurin suunnittelussa huomioidaan ratkaisun erityispiirteet ja tunnistetut vaatimukset (liiketoiminta-, turvallisuus-, jatkuvuusvaatimukset ym.) Traficomin julkaisema 5G Tietoturva-arkkitehtuuri[57] tarjoaa ylätason ohjeita ja tarkistuslistoja tukemaan 5G-teknologiaan pohjautuvien palveluiden rakentamista ja operointia

3GPP tuottaa ohjeistusta 5G-ratkaisujen tietoturva-arkkitehtuurin määrittelemisen tueksi[58]. Turvallisen arkkitehtuurin pääkohdat ovat:

- Autentikaatio- ja auktorisointimekanismien toteutus verkko- ja laitetasolla tietoturvallisesti
- Verkkoliikenteen suodatus ja salaus
- Radioverkon identiteettien suojaaminen väliaikaisten tunnisteiden avulla
- Verkkolaitteiden fyysinen suojaus, jotta kyetään varmistumaan turvallisesta käynnistämisestä ja suojaamaan sensitiivistä dataa

Paikallisten verkkojen ja reunalaskennan osalta tietoturvallisen arkkitehtuurin suunnittelussa datan ja laskennan sijainnit on hyvin tärkeä tunnistaa ja suojata. Houkuttelevat kohteet kyberrikollisille täytyy tunnista suunnittelussa ja suojaamisessa.

[54] https://www.gsma.com/security/5g-cybersecurity-knowledge-base/
[55] ENISA Threat Landscape for 5G Networks Report — ENISA (europa.eu)
[56] https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g
[57] https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/5g-security-architecture
[58] https://www.3gpp.org/news-events/3gpp-news/sec-5g

5.3.6 Tietosuoja

Tietosuojaan liittyvät asiat on hyvä ottaa huomioon jokaisen ratkaisun kohdalla. Suoria henkilötietoja käsitellään mm. osana käyttöoikeuksia, jolloin tietoturvan vuoksi välttämättömät loki- ja IP-tiedot muuttuvat helposti henkilötietoja sisältäviksi. Lisäksi tietosuoja- ja viestintälainsäädännön tietosuojavaatimusten lisäksi on syytä huomioida muu vaikuttava lainsäädäntö, kuten esimerkiksi laki yksityisyyden suojasta työelämässä. Henkilötietojen osalta toteutettavassa vaikutustenarvioinnin metodologiana voi hyödyntää esimerkiksi Tietosuojavaltuutetun toimiston tuottamaa ohjetta[59]

Kun viestintäpalveluratkaisuun liittyy viestinnän välittäjän roolissa toimimista, tulee viestintäpalvelun tarjoamisen aikana syntyvien välitystietojen käsittely suunnitella ja toteuttaa sähköisen viestinnän palveluista annetun lain (SVPL) edellyttämällä tavalla. Viestintäpalveluiden yksityisyydensuojaa valvoo Suomessa Traficom.

Osana tietosuoja-arviointia tulee huomioida mahdollinen henkilötietojen siirto tai käsittely EU/ETA:n ulkopuolelle. Tässä eri palveluissa ja ratkaisuissa hyödynnettävät pilvialustat ovat mahdollinen riski. Suuret pilvipalvelutoimittajat tarjoavat mahdollisuuden rajoittaa tietojen sijainti ja käsittely EU/ETA:an, mutta näin ei välttämättä ole kaikkien toimijoiden ja palveluiden kanssa. Henkilötietojen käsittely, kuten esimerkiksi varmuuskopiointi tai välitystiedon uhka-analyysin suorittaminen, EU/ETA:n ulkopuolella edellyttää aina tapauskohtaista laillisuuden arviointia ja siihen liittyvien sopimuksellisten, teknisten ja organisatoristen suojatoimien suunnittelua ja toteutusta.

5.3.7 Alusta ja ohjelmistokomponentit

Alustoilla on omat turvallisuusominaisuutensa, jolloin on hyvä ymmärtää alustan tuomat riskit ja kontrollit. Alustojen kyberturvallisuuden osalta on tärkeä huomioida ohjelmistopäivitykset sekä poikkeamahavainnointiin liittyvä valvonta, esimerkiksi ns. EDR (End-point-Detection/Reponse) tuotteen avulla.

Alustana paikallisten matkaviestinverkkojen ja reunalaskennan järjestelmissä voi toimia operaattorin verkko tai pilvipalvelu. Tällöin alustan tietoturva on palveluntarjoajan vastuulla, mutta sen turvallisuuden varmistaminen on hyödyllistä varmentaa säännöllisesti. Palveluntarjoajalta voidaan vaatia säännöllistä tietoturvatestausta mahdollisesti riippumattoman kolmannen osapuolen toimesta tai esimerkiksi tietoturvasertifioinnin ylläpitoa alustanhallinnassa.

Alustatietoturvallisuus rakentuu pitkälti alustakomponenttien ja niiden palveluntarjoajien toteuttamalle tietoturvalle. Näiden osalta on tärkeä varmistua, että alustakomponentit, verkkolaitteet ja tietoverkon toteutus on tehty tietoturvallisesti. 3GPP:n ja GSMA:n yhteistyönä syntynyt NESAS[60] (Network Equipment Security Assurance Scheme) voi auttaa arvioimaan alueen ratkaisuja. Yleisesti alustojen ja verkkojen tietoturvan osalta on hyvä luottaa standardoituihin järjestelmiin ja tietoturvasertifioituihin toimijoihin.

Pilviympäristöjen osalta on muistettava, että tietoturvan toteutuksessa on jaettu vastuu palveluntarjoajan ja käyttäjän välillä. Palveluntarjoajat, erityisesti globaalit

[59] Vaikutustenarviointi | Tietosuojavaltuutetun toimisto
[60] https://www.gsma.com/security/network-equipment-security-assurance-scheme/

toimittajat, tarjoavat yleisesti korkean tietoturvan ratkaisuja, mutta vain alustan osalta. Alustojen päällä toteutettavien ympäristöjen tietoturvallisuuden hallinta ja operointi jää asiakasorganisaation vastuulle.

Avoimen lähdekoodin ohjelmistokomponentit

Kaupallinen ohjelmisto	Avoimen lähdekoodin ohjelmisto
Kaupallisen toimijan tuottama ohjelmisto, yleensä maksullinen	Ohjelmisto, joka on vapaasti saatavilla internetistä, kattaen lähdekoodin. Suosittuja ohjelmistoja ylläpidetään sen ympärille syntyneen yhteisön toimesta.
Toimittaja vastaa kehitysestä ja testaamisesta, maksuun liittyy yleisesti vastuu toiminnasta ja turvallisuudesta	Kehitys ja testaus toimii avoimen kehityksen ja yhteistyön kautta. Ei vastuuta virhe- tai haavoittuvuuskorjauksista (tai muistakaan toiminnallisuuskista)
Lähdekoodi on toimittajan omaisuutta	Lähdekoodi on hyödynnettävissä lisenssiehtojen puitteissa
Käyttöön liittyy maksun tai lisenssin mukana tulevat oikeudet, jotka vaihtelevat (esim. käytön laajuus)	Maksutta käytettävissä lisenssiehtojen puitteissa
Toimittaja vastaa turvallisuudesta, hintaan sisältyy mm. haavoittuvuuksien ja virheiden korjaukset	Haavoittuvuuksia ja virheitä korjataan yhteisön toimesta, riippuen yhteisön aktiivisuudesta toiminta voi olla nopeaa, hidasta tai olematonta
Kaupallisella toimijalla on insentiivi varmistaa ohjelmistonsa turvallisuus suojatakseen omaa liiketoimintaa, mutta täydellistä turvallisuutta ei voida taata. Esimerkiksi ns. nollapäivähaavoittuvuuksia voi esiintyä ohjelmistossa kuin ohjelmistossa	Avoimen lähdekoodin ohjelmistojen turvallisuus riippuu paljolti käytön laajuudesta ja sen ympärille rakentuneen yhteisön aktiivisuudesta. Laaja käyttö ja aktiivinen yhteisö kykenee tunnistamaan ja korjaamaan haavoittuvuuksia nopeastikin, mutta vähemmän käytettyjen ohjelmistojen sykli voi olla hidas.

Taulukko 5. Kaupallisten ja avoimen lähdekoodin ohjelmistojen ominaisuudet

Huom! Sekä kaupallisten että avoimen lähdekoodin ohjelmistojen käyttöön sisältyy paljon huomioitavaa. Molemmissa tapauksissa on käyttäjän ymmärrettävä mitä hän käyttää, millaisilla ehdoilla ja mitä seurauksia näillä voi toiminnalle olla. Älä oleta minkään valmisohjelmiston olevan täysin turvallinen, vaan varmistu siitä omin toimenpitein. Myös palveluntarjoajan järjestelmien osana voidaan hyödyntää avoimen lähdekoodin ohjelmistoja.

5.3.8 Toimitusketjujen hallinta

Järjestelmien osalta on tärkeä kartoittaa toimitusketjut ja tunnistaa kriittiset palveluntarjoajat. Usein palvelukumppanien taustalla voi vaikuttaa muita toimittajia, joihin järjestelmän omistajalla itsellään ei ole välttämättä suoraa sopimussuhdetta. Esimerkiksi pilvipalveluiden käyttö tai avoimen lähdekoodin ohjelmistojen hyödyntäminen voivat aiheuttaa riskejä osana palveluketjuja. Tällöin esimerkiksi kyberturvallisuuden varmistaminen voi olla haastavaa.

Toimitusketjujen tunnistamisen osana on huolehdittava:

- Riskienhallinnasta – mitä riskejä eri toimittajista ja heidän välisistään riippuvuuksista voi palvelun / järjestelmän osalta syntyä?

- Jatkuvuudenhallinta – kuinka toimitusketjut vaikuttavat jatkuvuudenhallintaan. Voiko esimerkiksi yhden toimittajan taloudellinen konkurssi vaikuttaa? Kuinka onnistuu jatkuvuus- ja toipumissuunnitelmien tekeminen toimittajaverkostossa?

- Kyberturvallisuuden operointi – kuinka toimittajien osalta huolehditaan kyberturvallisuuden valvonnasta ja poikkeamiin reagoinnista? Riittääkö esimerkiksi kuukausiraportointi poikkeustilanteista?

Kumppaneiden osalta on hyvä tunnistaa myös sopimusvaatimusten lisäksi esimerkiksi resursointiasiat. Riittääkö kumppanilla työvoimaa poikkeustilanteissa ja kuinka työvoiman saatavuus on varmistettu? Erityisesti kehittyneiden teknologioiden osaajapoolit ovat yleensä rajallisia, jolloin työvoiman saatavuuteen ja kouluttamiseen on tärkeä varautua.

Huoltovarmuuskriittisiin järjestelmiin liittyvien toimittajien osalta on tärkeä huomioida seuraavat:

- Voidaanko varmistua, että toimittajan toimitusketjuun ei kohdistu vaikuttamista ulkopuolisten tahojen osalta.

- Toimittajan kyky huolehtia saatavuudesta niin työntekijöiden ja osaamisen kuin komponenttien osalta.

- Toimittajan yleinen kyvykkyys huolehtia tarjottujen laitteiden ja ratkaisujen kyber- ja tietoturvasta. Mikä on toimittajan historia toteutuneissa kyberhyökkäyksissä ja tietoturvaongelmissa, miten ne hoidettiin ja mitä muutoksia niiden perusteella tehtiin? Onko toimittajalla uskottavat tietoturvan varmistavat prosessit ja ohjelmat?

Vinkki! Omaksu myös kumppaneiden osalta Zero-trust-lähestymistapa. Oleta, että jokainen kumppani voi olla kyberhyökkäyksen kohteena. Mitoita toimenpiteet tämän mukaisesti ja määritä omat hallintamenettelyt siten, että varmistutaan kokonaistietoturvan toteutumisesta. Vaadi kumppaneilta todisteita kyberturvallisuusvaatimusten täyttymisestä tai auditoi/testaa itse tai kolmannen osapuolen avulla heidän kyberturvallisuus säännöllisesti.

5.4 Toteutus

Toteutusvaiheessa voidaan hankkia erilaisia kokonaisuuksia valmiina tai kehittää niitä alusta saakka, sovelluskehityksestä lähtien. Erilaiset tavat nostavat esille erilaisia riskejä ja painopistealueita, jolloin turvallisuuden toteutuksen täytyy myös mukautua. Turvallisuusratkaisuiden dokumentointi on usein laiminlyöty, mutta tärkeä osa toteutusta.

5.4.1 Turvallisuuden varmistaminen

Turvallista ratkaisua hankittaessa täytyy varmistaa, että huolehditaan ratkaisun turvallisuuden koventamisesta ja testaamisesta sekä haavoittuvuuksien hallinasta.

Turvallisuuden koventaminen

Konfiguroidaan ratkaisu uhkamallinnuksen ja hyökkäyspinta-alan minimoinnin suunnitelmien mukaisesti. Uhkamallinnus ja hyökkäyspinta-alan minimointi esitetty luvussa 5.3.3 Turvallisen suunnittelun periaatteet.

Turvallisuuden testaaminen

Turvallisuuden testaamisella on tarkoitus varmistaa, että koventaminen on tehty oikein, eikä toteutukseen ole jäänyt turvallisuusaukkoja, esim. tiedettyjä haavoittuvuuksia avoimen lähdekoodin komponentteihin. Testausta voidaan tehdä erilaisilla työkaluilla täysin tai osittain automaattisesti tai manuaalisesti. Esim. Web-sovelluksille löytyy OWASP:n toteuttamana lista uhkista, jotka on syytä testata. [61]

Testaus pitää tehdä aina ennen kuin uusi versio julkaisusta otetaan käyttöön. Testauksia pitää myös tehdä käytön aikana säännöllisesti, jotta uudet havaitut uhkat tai tahattomat konfiguraatiomuutokset löydetään.

Paikallisten matkaviestinverkkojen sekä reunalaskennan tietoturvatestauksen kattavuudesta on hyvä varmistua seuraavin toimenpitein:

- Kontrollitarkastukset – testataan eri komponenttien konfiguraatioiden ja kontrollien tila.
- Haavoittuvuuksienhallinta sekä haavoittuvuusskannaukset – toteutetaan eri komponenttien haavoittuvuuksien kartoitukset, testaus ja hallinta.
- Automatisoitu ja dynaaminen tietoturvatestaus – toteutetaan syvällisempi tietoturvatestaus, sekä automatisoiduin työkaluin että asiantuntijan toteuttamana.
- Hyökkäyssimulaatiot – Erilaisia kyberhyökkäyksiä simuloivat harjoitukset kuten Red teaming.
- Bug bounty – organisaation ulkopuolisen testausosaamisen hyödyntäminen, jossa havaittujen haavoittuvuuksien raportoinnista maksetaan palkkio. Bug bounty on hyvä malli täydentää ja tukea muuta tietoturvatestausta, mutta ainoana mallina sen kattavuus on usein puutteellinen.

Vinkki! Tietoturvatestaus vaatii syvällistä asiantuntemusta ja varsinkin laajat ja yksityiskohtaiset testaukset on suositeltavaa toteuttaa asiantuntijakumppanin toimesta.

5.4.2 Turvallinen ohjelmointi

Turvallinen ohjelmisto toteutetaan noudattamalla hyväksi todettuja ohjelmistokehityksen periaatteita. Lisäksi ohjelmiston turvallisuus otetaan huomioon kaikissa käytön vaiheissa lähtien vaatimusten määrittelystä, suunnittelusta ja käyttöönotosta sekä ylläpidosta ja kehitystyöstä aina käytön lopettamiseen. Tästä aiheesta

[61] https://owasp.org/www-project-top-ten

löytyy paljon yleistä materiaalia ja ohjeistusta. Hyviä käytäntöjä turvallisen ohjelmiston kehittämiseen löytyy esimerkiksi OWASP:n[62] tai SEI CERT[63]:n tuottamana.

Kaikki turvallisen ohjelmistokehityksen käytännöt pätevät myös paikallisiin matkaviestinverkkoihin ja reunalaskentaympäristöihin tehtäville ohjelmistoille. Osa käytännöistä on kuitenkin reunalaskentaympäristöissä erityisen tärkeitä, joten ympäristön erityispiirteet on otettava huomioon suunnittelussa ja toteutuksessa.

Reunalaskentaympäristö on tyypillisesti turvattomampi kuin perinteinen konesaliympäristö, koska siinä laitteisiin tai verkkokomponentteihin voi ulkopuolinen päästä helpommin käsiksi. Lisäksi verkkoon voi olla kytkettynä paljon erilaisia laitteita, jotka laajentavat hyökkäyspinta-alaa.

Materiaalia tietoturvan huomioonottamisesta ohjelmistokehityksessä:

- OWASP Project Security Knowledge[64]
- CISQ – Consortium for Information & Software Quality[65]

Huom! Turvallinen ohjelmointi ja sen menettelyt tulee linkittää palvelun tai järjestelmän riskienhallintaan ja uhkamallinnukseen, jotta voidaan huomioida erityispiirteet ja niiden vaatimat kontrollit koko elinkaaren ajan.

5.5 Käyttö ja operointi

Käyttöönoton jälkeen järjestelmä siirtyy ylläpito- ja operointivaiheeseen, jossa sen kyberturvallisuuden ylläpito on tärkeä huomioida osana päivittäistä toimintaa. Tämä vaihe vaatii ylläpidon määrittelyä ja toteutusta, kyberturvallisuuden valvontaa ja poikkeamiin vastaamista sekä haavoittuvuuksien- ja päivitystenhallintaa. Operoinnissa on huomattava myös jatkuva toimittajahallinta ja sopimuksiin liittyvä valvonta ja tarkastukset.

5.5.1 Ylläpito ja päivitykset

Laitteissa ja ohjelmistoissa voi olla vikoja ja haavoittuvuuksia ja niihin halutaan myös tuoda uusia ominaisuuksia. Tämän vuoksi laitteita ja ohjelmistoja päivitetään. Päivitykset täytyy aina tehdä suunnitellusti varmistaen, että turvallisuus ei vaarannu päivityksen aikana eikä sen seurauksena.

Haavoittuvuuksienhallinta

Haavoittuvuuksia voi olla laitteissa, niiden ohjelmistoissa tai muissa ohjelmistokomponenteissa. Laitteiden ja niiden ohjelmistoista vastaa yleensä laitteen valmistaja, joka tarjoaa korjaukset laitteen käyttäjille. Haavoittuvuuksien hallinta on jatkuva prosessi, jossa haavoittuvuuksia pyritään tunnistamaan useiden toimenpiteiden avulla:

[62] GitHub - OWASP/CheatSheetSeries https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/migrated_content
[63] https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards
[64] OWASP Security Knowledge Framework | OWASP Foundation
[65] CISQ Home | Consortium for Information & Software Quality (it-cisq.org)

- Komponenttitoimittajien haavoittuvuusviestintä – komponenttitoimittajat tiedottavat niitä koskevista haavoittuvuuksista, päivityksistä sekä mitigointikeinoista.

- Tietoturvaviranomaisten tiedotus – esimerkiksi Traficomin Kyberturvallisuuskeskus tuottaa haavoittuvuustietoa[66] säännöllisesti verkkosivujensa kautta. Yleensä viranomaisilta voi tilata myös tiedotteet suoraan sähköpostiin.

- Haavoittuvuusskannaukset – Työkaluilla automaattisesti tai manuaalisesti toteutettavat haavoittuvuusskannaukset tunnistavat järjestelmässä ja sen osissa mahdollisesti piilevät haavoittuvuudet.

Haavoittuvuuksienhallinnan määrittelyssä voi hyödyntää OWASP Vulnerability Management Guide -ohjetta[67]

Jos avoimen lähdekoodin komponentista löytyy haavoittuvuus, mutta siihen ei ole tulossa korjausta, on vaihtoehtoina tehdä korjaus itse tai teettää se kumppanilla. Jos mahdollista, korjaus kannattaa toimittaa myös komponentin alkuperäiseen koodikantaan, jotta se on automaattisesti komponentin seuraavassa versiossa käytettävissä itselle ja muille. Näin vältytään muutosten yhdistämiseltä, kun uusi versio komponentista julkaistaan. Isommissa komponenteissa haavoittuvuus voi myös sijaita koodissa, jota ei omassa ohjelmistossa tarvita. Tällöin komponentin ominaisuus voidaan konfiguroida pois käytöstä. Jos em. ei ole mahdollista, poistaa tarpeeton koodi väliaikaisesti, kunnes komponentista julkaistaan uusi korjattu versio.

Jatkuva tietoturvatestaus

Käytössä olevalle järjestelmää täytyy olla suunnitelma säännöllisestä ja järjestelmällisestä testaamisesta. Testaamisella varmistetaan, että järjestelmässä ei ole uusia löydettyjä haavoittuvuuksia, uudet tunnetut hyökkäystavat eivät vaaranna järjestelmää eikä järjestelmään ole tehty turvallisuutta heikentäviä konfiguraatiomuutoksia. Automaattinen testaus tehdään useammin ja manuaalinen testaus yleensä harvemmin. Käytössä olevan järjestelmän osalta on suositeltavaa jatkaa tietoturvatestausta, säännöllisesti sopivin välein sekä merkittävine muutosten/päivitysten yhteydessä. Näin voidaan proaktiivisesti varmistua haavoittuvuuksien tunnistamisesta sekä tietoturvaongelmien havainnoinnista.

[66] https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet
[67] Owasp: https://owasp.org/www-project-vulnerability-management-guide/

5.5.2 Valvonta ja poikkeustilanteet

Operoinnin aikana korostuvat palvelun ja järjestelmän toiminnan ja tietoturvan valvonta. Toiminnan valvonta liittyy toimintavarmuuden ja jatkuvuuden turvaamiseen, jotta kyetään tunnistamaan tapahtumat, jotka vaikuttavat epäsuotuisasti palvelun toimintaan. Operatiivinen valvonta seuraa mm. järjestelmän palvelutasoja tavoitteena varmistaa palveluiden saatavuus tavoitteiden mukaisesti.

Tietoturvavalvonta pyrkii tunnistamaan palvelun tietoturvaan kohdistuvat tapahtumat ja hyökkäykset sekä mahdollistamaan tapahtumiin vastaamiseen ja torjumiseen suunniteltujen toimenpiteiden aloittamisen mahdollisimman nopeasti. Tietoturvavalvonta pyrkii varmistamaan palvelun tietoturvan kaikissa elinkaaren vaiheissa, tunnistaen tapahtumia ja käynnistämällä toimenpiteitä.

Osana valvontaa on suositeltavaa hyödyntää uhkatietoa, joko avoimista tai kaupallisista lähteistä. Lisäksi useilla eri aloilla toimii erilaisia yhteistyöryhmiä, joiden puitteissa toimijat voivat vaihtaa luottamuksellisesti uhka- ja hyökkäystietoa. Traficom fasilitoi ISAC-ryhmien tiedonvaihtoa[68].

OT-ympäristöjen (Operational Technology) valvonta eroaa perinteisestä IT-ympäristön (Information Technology) tietoturvavalvonnasta merkittävästi. Yleiset teknologiat ja valvontatyökalut eivät välttämättä sovi yhteen tuotannon tietojärjestelmien kanssa, vaan niiden valvonnassa voidaan joutua tukeutumaan omiin, erikoistuneisiin valvontateknologioihin. Esimerkiksi agenttipohjainen valvonta ei välttämättä onnistu, koska operatiivisen teknologian laitteisiin sellaisen asentaminen on mahdotonta saatavuusvaatimusten vuoksi. Tällöin hyödynnetään erilaisia valvontakeinoja, esimerkiksi tietoliikenteen analysointia tai pakettien syvätutkimusta.

Vinkki! On suositeltavaa integroida tietoturvavalvonnan ja poikkeamiin vastaamisen prosessit yleisiin häiriöhallinnan prosesseihin. Häiriöiden selvittämisessä on paljon samankaltaisuuksia ja usein tarvitaan myös samoja osaamisprofiileja työhön. Tietoturvavastaamiseen vaaditaan kuitenkin usein myös erityisosaamista, joka täytyy huomioida suunnittelussa.

Valvonnan suunnitteluun, toteutukseen ja operointiin voi olla suositeltavaa hyödyntää asiantuntijakumppania, jolta löytyy asiantuntemusta yhteen tai useampiin valvonnan vaiheeseen. Myös vakavien tietoturvahäiriöiden tutkintaan ja palautumiseen on tarjolla osaavia asiantuntijakumppaneita.

[68] https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostot/isac-tiedonvaihtoryhmat

5.6 Jatkuvuudenhallinta

Jatkuvuudenhallinta mahdollistaa toiminnan jatkumisen myös epäsuotuisissa olosuhteissa. Jatkuvuudenhallinnan yhteydessä voidaan puhua myös liiketoiminnan kestävyydestä. Aiheesta enemmän esimerkiksi Huoltovarmuuskeskuksen sivuilla[69]

Jatkuvuussuunnittelun tavoitteena on liiketoiminnan ja sen keskeisten prosessien jatkuvuuden varmistaminen ja toiminnan turvaaminen. Osana suunnittelua tunnistetaan organisaatiota uhkaavia tekijöitä ja niiden seurauksia sekä suunnitellaan toimenpiteitä toipumiskyvyn turvaamiseksi. Jatkuvuussuunnittelun tavoitteena on:

- Ylläpitää organisaation toimintaa ja tarjota palveluja/tuotteita keskeytyksettä
- Kyvykkyys palautua ja jatkaa erityisesti kriittisiä toimintoja mahdollisimman nopeasti häiriön jälkeen
- Minimoida taloudelliset vaikutukset

Paikallisten matkaviestinverkkojen ja reunalaskennan osalta jatkuvuussuunnittelussa on katettava ainakin:

- Verkkoyhteyksien katkeaminen - erityisesti kriittisten palveluiden on kyettävä toimimaan, vaikka yhteydet olisivat poikki
- Varakomponenttien saatavuus, uusinta ja varastoinnin suunnittelu, jotta komponentit säilyvät käyttöönottokunnossa
- Radioverkkosuunnittelu ja varayhteyksien huomioiminen
- Henkilöstön ja osaamisen varmistaminen poikkeustilanteissa
- Toimittajaketjun jatkuvuudenhallinta, varajärjestelyt esimerkiksi pilvialustojen mahdollisissa vaihtamisissa
- Palveluiden siirtäminen pilvialustalta toiselle. Ongelmaksi saattaa nousta eri palveluiden natiivikomponenttien hyödyntäminen, joka sitoo tiettyyn alustaan. Tällaiset riippuvuudet on tärkeä tunnistaa ja dokumentoida.
- Palveluiden siirtäminen joko kotimaahan tai kotimaan ulkopuolelle riippuen poikkeustilanteesta

Jatkuvuudenhallinnan tulee olla jatkuvaa tekemistä, jossa suunnitelmia päivitetään säännöllisesti ja merkittävien muutosten jälkeen sekä testataan soveltuvin osin suunnitelmia erilaisia skenaarioita hyödyntäen.

[69] https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/jatkuvuudenhallinta

5.7 Tulevaisuudessa tapahtuva kehitys

Ratkaisujen kyberturvallisuuden hallinta ei pääty operointivaiheeseen ja sen aikaiseen valvontaan ja ylläpitoon. On erityisen tärkeä huomioida jatkokehityksen tuomat muutokset ja niiden riskit. Usein toteutuksissa lähdetään ensin liikkeelle pienimuotoisemmin rajatuilla ja yksinkertaisemmilla käyttötapauksilla ja näitä laajennetaan vähitellen kohti organisaation kannalta kriittisempiä toimintoja. Verkkoympäristön kehittäminen ja käyttötapausten laajentaminen voi helposti muuttaa riskitasoja ja vaatia uudenlaista lähestymistä kyberturvallisuuden sekä riskien- ja jatkuvuudenhallinnan näkökulmasta.

5.7.1 Muutoshallinta

On tärkeää, että järjestelmän kaikki komponentit kuten laitteet, niiden ohjelmistot, muut ohjelmistokomponentit ja työkalut on luetteloitu. Komponenttien käytössä olevat versiot ja niiden tiedetyt haavoittuvuudet ovat tiedossa. Järjestelmän ja kaikkien komponenttien testitulokset on dokumentoitu ja kaikki tiedetyt haavoittuvuudet ja poikkeamat on raportoitu työkaluun. Näiden tietojen perusteella tiedetään, mikä on järjestelmän tilanne ja voidaan suunnitella uusien versioiden käyttöönotto tarpeen mukaan.

Muutoshallinta on erityisen tärkeää huomioida tilanteissa, joissa järjestelmän käyttö laajenee merkittävästi. Järjestelmään tuodaan esimerkiksi uusia käyttötapauksia, joiden riskiprofiili eroaa olemassa olevista tai suljettuja tai rajoitettuja verkkoja liitetään avoimeen verkkoon. Tällöin on tärkeää päivittää riskienhallinta, uhkamallinnus sekä muut suunnittelun pohjana toimineet arviot ja uudelleen kalibroida tietoturvatarpeet.

5.7.2 Riippuvuuksienhallinta

Järjestelmien riippuvuuksien tulee olla dokumentoitu projektin alusta saakka. Näin erilaisissa muutostilanteissa tiedetään, millaisia riippuvuuksia täytyy hallita ja mitä vaikutuksia niillä voi olla eri tilanteissa. Riippuvuudet voivat olla sekä teknisiä että esimerkiksi kumppaneihin tai lainsäädännön vaatimusten muutoksiin liittyviä. Nämä kaikki tulee dokumentoida. Visualisoimalla saadaan helposti tilannekuva erilaisista riippuvuuksista.

Jaettujen resurssien käyttö voi johtaa haasteisiin, erityisesti poikkeustilanteissa. Esimerkkejä voivat olla jaettujen resurssien tietosuojahaasteet tai suurten pilvitoimittajien resurssien saatavuus erilaisissa muuttuneissa tilanteissa. Riippuvuuksienhallinnan kautta kyetään tunnistamaan ja varautumaan tällaisiin haasteisiin.

Päivitystilanteissa erilaiset yhteensopivuushaasteet voivat vaikuttaa järjestelmän toimintaan, mikäli komponentit eivät tue toisiaan päivitysten jälkeen.

5.8 Järjestelmän lopettaminen

Elinkaaren lopussa järjestelmä tai sen osia ajetaan alas ja mahdollisesti korvataan uudella järjestelmällä tuotannon jatkuessa. Järjestelmän, sen osan tai yksittäisen laitteen käytöstä poistossa pitää huolehtia myös turvallisuudesta. Järjestelmään talletetut tiedot pitää siirtää uuteen järjestelmään ja poistaa vanhasta niin, että tietoa ei pysty jälkeenpäin palauttamaan. Laitteiden muistit pitää tyhjätä tai ne pitää tuhota niin, että tietoa ei pysty palauttamaan.

Integraatioiden ja yhteysliikennerajapinnat tulee purkaa huolellisesti, jotta varmistutaan yhteyksien katkaisemisesta, palomuurien ja porttien sulkemisesta sekä käyttöoikeuksien poistamisesta.

6 Huoltovarmuusskenaariot

Tässä luvussa esitellään tämän oheen laatimisen taustalla olleet muutamat erilaiset yleiset esimerkkiskenaariot, joiden avulla lukija voi pyrkiä hahmottamaan muuttuvaa toimintaympäristöä ja siihen liittyviä riskejä. Toteutuessaan tämän luvun skenaariot voisivat vaarantaa toteutettujen ratkaisujen toiminnan jatkuvuutta ja kyberturvallisuutta. Skenaarioissa esitetyt vaikutukset ovat esimerkinomaisia ja ne eivät ole kaiken kattavia. On kuitenkin tärkeää pysähtyä pohtimaan skenaarioiden mahdollisia erilaisia vaikutuksia oman toiminnan näkökulmasta.

Enisa tuottaa myös uhkaraportointia 5G-verkkoihin[70] liittyen, jota voi hyödyntää riskeihin varautumisessa. Uhkien pohjalta on hyödyllistä tehdä erilaisia skenaarioita ja riski/uhka-arvioita oman verkkoympäristön ja käyttötapausten näkökulmasta.

Tässä tunnistetut esimerkkiskenaariot ovat olleet ohjeen koostamisen tukena, mutta ratkaisujen toimintavarmuuden ja jatkuvuuden arviointien ei tule rajoittua pelkästään näihin skenaarioihin. On suositeltavaa tunnistaa kullekin ratkaisulle omat riski/uhkaskenaariot ja niille tarkoituksenmukaiset hallintakeinot. Traficom tuottaa myös erilaisia harjoitusskenaarioita organisaatioiden hyödynnettäväksi.[71]

Toimitusketjuongelmat

Skenaario

Häiriö globaaleissa teknologian toimitusketjuissa esimerkiksi valmistuksessa tai logistiikassa, mikä vaarantaa komponenttien saatavuuden joko verkkoja toteuttavalla organisaatiolla tai heidän laitetoimittajillaan. Skenaariossa haasteita voi olla kansainvälisissä alihankintaketjuissa, tarvittavien komponenttien saatavuudessa tai logistiikassa.

Mahdollisia vaikutuksia

Globaaleissa toimitusketjuissa pienikin häiriö voi vaikuttaa komponenttien tai laitteiden saatavuuteen. Yhdenkin komponentin saatavuusongelma voi aiheuttaa sen, että tiettyjä laitteita ei pystytä valmistamaan eikä toimittamaan rakenteilla oleviin tai käytössä oleviin paikallisiin matkaviestinverkkoihin. Tällöin verkkoa ei saada rakennettua suunnitellun mukaiseksi tai käytössä olevan verkon komponentin vikaantuessa, verkkoa ei saada korjattua alkuperäisen kaltaiseksi. Tämä voi vaarantaa verkon toimintakykyä ja verkon tarjoamaa palvelutasoa ja vaikuttaa siten käyttötapausten toimintavarmuuteen.

Pohdittavaa

- Miten varaudutaan laiterikkoihin ja äkillisiin kapasiteettitarpeen muutoksiin?

[70] ENISA Threat Landscape for 5G Networks Report — ENISA (europa.eu)
[71] https://www.kyberturvallisuuskeskus.fi/fi/s/kyberharjoitusskenaariot/skenaariot

- Miten mahdollistetaan tekninen yhteensopivuus, mikäli joudutaan hyödyntämään eri valmistajien laitteita tai varaosia osana varautumista tai poikkeustilannetta? Onko yhteensopivuus suunniteltu tai huomioitu etukäteen?

- Missä määrin on mahdollista huomioida laiteiden saatavuus eri tilanteissa eri toimittajien kanssa tehdyissä sopimuksissa ja kolmansien osapuolien kanssa?

- Miten verkon ja järjestelmän suunnittelussa on huomioitu myös mahdolliset laiterikot ja ongelmat korvaavien laitteiden saatavuudessa? Miten esimerkiksi radioverkkosuunnitelmassa on huomioitu päällekkäinen verkkopeitto ja varayhteydet, jos osa käytetyistä tukiasemalaitteista vikaantuu?

- Jos verkkoa suunniteltaessa saatavuusongelmista johtuen todetaan toteutusmallin olevan mahdoton, mitä mahdollisuuksia on toteuttaa verkko toisella toteutusmallilla? Mitä vaikutuksia toimitusmallin muutoksella on?

Pandemia

Skenaario

Globaali pandemia jonka laaja-alaiset vaikutukset koskettavat mm. osaavan työvoiman saatavuutta, toimitusketjuja (Ks. luku 5.3.8) sekä vaikuttavat organisaatioiden uhkakenttään. Pandemia vaikuttaa työvoiman saatavuuteen akuutin sairastamisen ja poissaolojen tai pidemmän työkyvyttömyyden kautta, mutta myös etätyöskentelyn tuomien erilaisten muutosten kautta. Samalla toimitusketjut kohtaavat häiriöitä ja mm. viranomaistoiminta ruuhkautuu. Pandemia vaikutuksia voidaan hyödyntää myös kyberrikollisten toimesta ja etätyöskentely avaa uusia uhkavektoreita (Ks. kyberhyökkäys).

Mahdollisia vaikutuksia

Oman osaavan henkilöstön saatavuus verkkoympäristön ylläpitoon ja operointiin heikkenee. Samanaikaisesti voi tulla esiin mahdollisia tarpeita tehdä muutoksia verkkoon ja järjestelmiin, jos henkilöstö siirtyy laajemmin etätyöskentelyyn, joka kasvattaa ylläpidon työkuormaa. Yrityksen ulkopuolisen osaamisen ja avun saatavuus ja mahdollisuudet matkustaa ja liikkua kohteisiin voi heiketä merkittävästi. Viranomaistoiminta voi ruuhkautua pandemian moniulotteisten vaikutusten vuoksi, joka viivästyttää mm. turvallisuusselvityksiä. Laitetilojen tai valvomoiden käytettävyyteen voi äkillisesti kohdistua rajoituksia karanteenitoimenpiteiden vuoksi esim. siten, että altistustilanteissa tilojen käyttö ei ole mahdollista ennen niiden tarkoituksen mukaista puhdistamista.

Pohdittavaa

- Kuinka varmistetaan osaavan henkilöstön saatavuus eri tilanteissa, jotka voivat myös muuttua nopeasti? Miten huolehditaan resurssien varaukset? Varahenkilöjärjestelyihin ja osaamispohjan leventämiseen on kiinnitettävä huomioita riittävän ajoissa.

- Miten mahdollistetaan toiminnan jatkuminen ja toiminnan riittävä maantieteellinen kattavuus, jos oman henkilöstön ja kumppanien matkustaminen vaikeutuu?

- Millä tavalla toimintojen, järjestelmien sekä henkilöstön osalta huolehditaan priorisoinnista?

- Miten varmistetaan laitetilojen ja valvomoiden turvalliset työskentelyolosuhteet, puhtaus ja käytettävyys erilaisissa nopeastikin muuttuvissa tilanteissa? Miten suoritetaan tarkoituksen mukaiset puhdistustoimenpiteet nopeasti, mikäli se on tarpeen?

- Miten varmistetaan riittävän tuen saatavuus kumppaneiden ja kolmansien osapuolten suunnalta poikkeustilanteessa? Miten merkittävä rooli omalla organisaatiolla on, jotta kumppanit ja toimittajat priorisoivat palvelua/tukea/huoltoa tilanteessa, jossa myös heidän toimintaansa kohdistuu rajoitteita?

- Mitkä ovat vaihtoehtoiset toimittajat palveluille, laitteille tai tuelle?

Pilvipalvelujen saatavuus

Skenaario

Tilanteessa pilvipalveluihin sijoitettujen ohjelmistojen ja alustojen saatavuudessa esiintyy katkoksia tai niiden kapasiteetti on merkittävästi rajoittunut. Tämän lisäksi kansainvälisissä tietoliikenneyhteyksissä voi esiintyä häiriöitä. Tilanteessa pilvipalveluihin sijoitettujen hyötykuormien suorittaminen on rajoitettua tai ne eivät toimi ajoittain ollenkaan. Tämä aiheuttaa mahdollisia vaikutuksia paikallisen verkon ja reunalaskennan palvelutasoon sekä niiden varassa toimivien käyttötapausten ja sovellusten toimintavarmuuteen.

Mahdollisia vaikutuksia

Globaalit pilvipalvelut voivat olla heikosti käytettävissä. Ongelmat voivat johtaa pilvipalvelujen hyödynnettävyyden merkittävään laskuun. Erityisesti kriittisten palvelujen osalta ei tällöin välttämättä voida luottaa pilvipalvelujen saatavuuteen. Vaikka verkon hyötykuormat olisi sijoitettu alueelliseen tai paikalliseen pilviratkaisuun, voi niissäkin esiintyä ongelmia tai katkoksia, mikäli niiden yhteydet ylemmäs pilvipalveluntarjoajien ympäristöihin vaarantuvat. Useimmat pilvipalvelutarjoajien reunalaskentaratkaisut toimivat myös paikallisina ratkaisuina, ilman yhteyttä julkipilveen, mutta toiminnoissa saattaa olla rajoituksia. Mikäli halutaan toteuttaa valmius myös täysin paikalliseen toimintaan, on se otettava huomioon jo palvelun suunnitteluvaiheessa. Myös kansainvälisiä tietoliikenneyhteyksiä tarvitsevat toiminnot kuten laajat yritysverkot tai laitevalmistajien tarjoama ylläpito sekä päivitysten toimittaminen voivat häiriintyä. Tilanteessa teknologiatoimittajien ja logistiikkatoimijoiden toimita saattaa myös häiriintyä.

Pohdittavaa

- Missä määrin paikalliset matkaviestinverkot ja reunalaskennan ratkaisut ovat riippuvaisia ulkoisista alustoista ja palveluista?

- Mikäli pilvipalvelut eivät ole käytössä, mikä on minimi palvelutaso, joka voidaan saavuttaa paikallisilla alustoilla? Onko tämä taso riittävä?

- Mikäli tilanteessa esiintyy kansainvälisten tietoliikenneyhteyksien katkoksia, löytyykö tarvittavia palveluja kotimaasta ja voidaanko ne sijoittaa kotimaahan? Millä tavoin ja miten nopeasti palvelut ovat palautettavissa Suomeen?

- Miten varaudutaan etukäteen palveluiden palauttamiseen Suomeen tai niiden siirtämiseen ulkomaille? Onko toteutettu verkkoratkaisu sellainen, että siihen kohdistuu velvoitteita tai sääntelyä toimintojen palauttamisesta?

Satelliittipohjaisten aika- ja paikkatietojen saatavuuden heikentyminen

Skenaario

Jos 5G-verkossa noudatetaan aikajakoista dupleksointia, tarvitsee se toimiakseen tarkan kellosignaalin, jotta radiolähetys- sekä vastaanottoajankohta sekä lähetys- ja vastaanottotaajuus saadaan pidettyä tarkkoina verkon häiriöttömän toiminnan varmistamiseksi. Lisäksi satelliittipaikannus tarvitsee toimiakseen erittäin tarkan kellosignaalin, jolla satelliitit ja vastaanottimet pidetään tahdistettuna. Koska satelliittipaikannus on käytettävissä ympäri maailman, sitä käytetään yleisesti myös matkaviestinverkkojen yhtenä tarkkana kellolähteenä. Satelliittipaikannuksessa käytettävän radiosignaalin teho on äärimmäisen pieni, joten sen häiritseminen paikallisesti on suhteellisen helppoa.

Skenaariossa yksittäisen organisaation tai laajemmin yhteiskunnan toimintaan vaikuttamiseen pyrkivät taho voi tehdä tällaista häirintää. Myös aurinkomyrsky voi haitata satelliittipaikannuksen toimintaa ja tehdä osan jonkin satelliittipaikannusjärjestelmän satelliiteista toimintakyvyttömiksi. Lopputuloksena tarkan kellosignaalin saatavuus häiriintyy, jolla on vaikutuksia satelliittipohjaisiin aika- ja paikkatiedon järjestelmiin.

Mahdollisia vaikutuksia

Aikajakoista dupleksointia noudattavissa matkaviestinverkoissa on oltava varmistetut kellolähteet. Jos tarkka kellolähde ei ole saatavilla, datan siirtäminen verkossa voi ajan kuluessa heikentyä merkittävästikin. Samalla synkronoimaton aikajakoista dupleksointia noudattava paikallinen verkko voi häiritä muita samalla maantieteellisellä ja taajuusalueella toimivia matkaviestinverkkoja, joista osassa voi olla myös kriittisempiä palveluja. Näin ollen, vaikka organisaatio itse sietäisi toiminnassaan paikallisen verkkonsa ja siihen liitettyjen käyttötapausten toimintavarmuuden laskua, voi synkronoimaton verkko aiheuttaa häiriötä lähialueen muille verkoille.

Pohdittavaa

- Miten hoidetaan aikajakoista dupleksointia noudattavien matkaviestinverkkojen synkronointi, jos satelliittipaikannussignaalia ei ole saatavilla?
- Kriittisissä kohteissa on tärkeää olla varajärjestelmiä synkronointisignaalin saatavuudelle. Miten synkronointi on varmistettu varajärjestelmillä, joita voidaan hyödyntää satelliittipohjaisen aika- ja paikkatietojen häiriintyessä?

Kyberhyökkäys

Skenaario

Skenaariossa organisaatio voi joutua tietojen tuhoajalla (wiper) tai kiristyshaittaohjelmalla (ransomware) toteutetun kyberhyökkäyksen kohteeksi. Tiedon tuhoaja pyrkii pyyhkimään kohteeksi joutuneen organisaation tietojärjestelmien tiedot. Kiristyshaittaohjelma pyrkii estämään tietojärjestelmien käytön salaamalla tiedostoja lunnaita vastaan.

Mahdollisia vaikutuksia

Kyberhyökkäys voi vaarantaa toimijan oman IT-toiminnan tai palvelutoimittajan tai -verkoston toiminnan. Onnistuessaan hyökkäys aiheuttaa merkittäviä vaikutuksia IT-infran, -laitteiden ja järjestelmien toimivuudessa. Onnistuneesta hyökkäyksestä toipuminen, verkkojen ja laitteiden puhdistus ja toiminnan uudelleen käynnistäminen on työlästä ja aiheuttaa pahimmillaan merkittäviä viiveitä. Organisaatio joutuu hyökkäyksen johdosta ns. palautumispisteeseen omassa toiminnassaan. Organisaation tulee määritellä palautumispiste, joka voidaan olettaa turvalliseksi.

Pohdittavaa

- Miten paikalliset matkaviestinverkot ja reunalaskennan ratkaisut on suojattu kyberhyökkäyksiltä?
- Miten tunnistetaan ja hallitaan paikallisten matkaviestinverkkojen ja niiden palvelujen ulkoinen hyökkäyspinta-ala?
- Miten verkkojen tietoturvavalvonta kykenee havaitsemaan ja vastaamaan mahdollisiin hyökkäyksiin riittävän ripeästi?
- Miten onnistuneen kyberhyökkäyksen vaikutukset voidaan rajata? Onko tähän varauduttu ennalta tehdyllä suunnittelulla? Traficomin Kyberturvallisuuskeskus on julkaisut ohjeita kyberhyökkäystilanteista toipumiseen.[72]
- Miten toimittaja- ja kumppaniverkoston riskien- ja jatkuvuudenhallinta on varautunut tällaisiin tapahtumiin heidän organisaatiossaan ja toiminnoissaan?

Pitkät sähkökatkokset

Skenaario

Skenaariossa energian saatavuustilanne heikkenee ja sähköntuotannossa sekä siirrossa voi esiintyä häiriöitä. Syynä voi olla esimerkiksi yleiset energian saatavuusongelmat tai energiantuotannon tai siirtoinfrastruktuurin häiriöt.

Mahdollisia vaikutuksia

Energiansaanti paikalliseen palvelutuotantoon voi häiriintyä. Tilanteessa voi esiintyä katkoksia palvelutoimittajaketjussa tai katkokset voivat kohdistua järjestelmäomistajan omiin palveluihin. Katkojen pidentyessä myös varavoimalla varmennetut kriittiset laitteet voivat uhata sammua ja prosessit tai tuotanto voi pysähtyä, jos energiansaantia ei kyetä varmistamaan riittävän pitkäksi aikaa.

Pohdittavaa

- Millä tavalla energiankäyttöä voidaan priorisoida pitämällä kriittisimmät toiminnot käynnissä?

- Minkälaisia kytköksiä ja riippuvuuksia paikallisella verkolla ja järjestelmillä on kriittisiin toimintoihin?
- Millaiset varavoimaratkaisut esimerkiksi akkuvarmennus tai muu vastaava on tarpeellista toteuttaa paikalliselle verkolle ja järjestelmille?
- Miten hyvin järjestelmän ylläpitoon ja operointiin osallistuvat mahdolliset kolmannet osapuolet tai palvelun tarjoajat pystyvät tilanteessa tarjoamaan omat palvelunsa riittävällä palvelutasolla?
- Mitä muita vaikutuksia sähkönsaannin mahdolliset häiriöt voivat saada aikaan verkkopalvelun ylläpidon ja operoimisen osalta?
- Millaisia vaikutuksia mahdollisilla toteutuvilla sähkökatkoilla on eri järjestelmille? Mitä tapahtuu esimerkiksi kulunvalvonnalle? Järjestelmien uudelleenkäynnistystä voi olla tarkoituksenmukaista testata etukäteen.

Liite 1: Tarkistuslista ja itsearviointimalli

- **Miten kyseiseen (verkko-)järjestelmään sovellettavat velvoitteet ja määräykset on tunnistettu?**

- Miten kyseiseen järjestelmään sovellettavien velvoitteiden ja määräyksien toteutuminen ja noudattaminen on varmistettu ja miten toteutuminen on dokumentoitu?

- **Millä tavoin ja missä määrin järjestelmä on suunnitellussa käyttökohteessaan kytköksissä yhteiskunnan huoltovarmuuden ylläpitämiseen?**

- Millä tavoin järjestelmän mahdolliset häiriöt, vikatilanteet tai kyberturvallisuuden puutteet voivat vaikuttaa huoltovarmuuteen?

- Mihin yhteiskunnan huoltovarmuuden kannalta kriittisiin toiminteisiin ja palveluihin järjestelmä voi vaikuttaa?

- Millä tavoin toteutettava järjestelmä voi vaikuttaa yhteiskunnan huoltovarmuuden kannalta kriittiseen toiseen järjestelmään?

- Miten näiden yhteiskunnan huoltovarmuuden kannalta kriittisten toiminteiden ja palveluiden jatkuvuuden varmistaminen on huomioitu järjestelmän suunnitelmassa?

    - Miten kriittisten toiminteiden ja palveluiden jatkuvuus on huomioitu suunnitelmassa?

    - Miten vikasietoinen ja kriittisten toiminteiden palveluiden jatkuvuuden näkökulmasta riittävä suunniteltu verkkototeutus on?

    - Miltä osin ja millä tavoin kriittisten toiminteiden ja palveluiden jatkuvuus on varmistettu kahdentamisella?

    - Miten järjestelmän ja sen komponenttien elpyminen on varmistettu?

    - Miten järjestelmän palauttamiseen tarvittavan datan saatavuus on varmistettu eri tilanteissa?

- Missä määrin toteutettu verkkototeutus vastaa suunniteltua ja mitä suunnitelmasta poikkeavia muutoksia verkkototeutukseen on tehty?

- Miten verkkototeutuksen toimintavarmuus todennettu (esim. testaamalla)?

- Miten turvallisuusvaatimukset on huomioitu järjestelmän ja sen komponenttien hankinnassa?

    - Määritelläänkö turvallisuusvaatimukset erillisessä hankinnan vaatimusliitteenä?

- **Miten järjestelmän osakokonaisuuksien turvallisuudesta vastaavat osapuolet on määritelty ja miten vastuut on kirjattu sopimuksiin?**

- Miten järjestelmän jokaisen osan turvallisuudesta vastaava osapuoli sovittu ja kirjattu sopimukseen?

- Miten varmistutaan, että turvallisuudesta vastaavilla osapuolilla on riittävä osaaminen turvallisuuden hoitamiseen vaatimusten mukaisesti?
- Miten palveluntarjoajan luotettavuus on arvioitu eri näkökulmista?
- Miten verkkotason turvallisuuteen liittyvät vastuut on tunnistettu ja sovittu?
- Miten kaikkien laitteiden turvallisuuteen liittyvät asiat on sovittu?
- Miten sovellusten turvallisuuteen liittyvät asiat on sovittu?
- Millä tavoin on sovittu, että asiakasorganisaatiolla on oikeudet varmistaa tai auditoida toimittajan kyberturvallisuus tarvittaessa?
- Mikäli on tarvetta pitää kriittinen data Suomen rajojen sisäpuolella, miten palvelun tarjoaja takaa tämän?
- **Miten riskianalyysi on tehty?**
- Millä tavoin reunalaskennan erityispiirteet on otettu huomioon riskianalyysissä?
- Miten paikallisen matkaviestinverkon erityispiirteet on otettu huomioon riskianalyysissä?
    - Onko verkko toteutettu itse?
        - Miten yhdysliikennerajapintojen ja -kanavien turvallisuus on varmistettu?
        - Millä tasolla mahdolliset riippuvuudet yleisien televerkkojen laitteisiin on tunnistettu?
- **Onko järjestelmän kyberturvallisuudelle tehty vaatimusmäärittely?**
- Miten kaikki kyberturvallisuuteen liittyvät kontrollit, vastuut, vastuulliset tahot ja riskit on huomioitu?
- Miten tietoturvallisuus verkon rajoilla on varmistettu?
    - Salatut tunneloinnit, palomuurit, pääsyn hallinta
- Miten alusta, ympäristöt ja ohjelmistokomponentit on konfiguroitu tietoturvallisiksi?
    - Palveluntarjoaja on yleensä vastuussa omien järjestelmiensä tietoturvasta ja asiakasorganisaatio omien järjestelmiensä tietoturvasta.
- Millä tavoin sovellustason tietoturvasta on huolehdittu?
- Miten valvonta kyberhyökkäyksiä vastaan on toteutettu ja miten niitä voidaan tunnistaa? Millä tavoin kyberhyökkäyksiin vastaaminen on suunniteltu ja testattu?
- Millä tavoin järjestelmää on peilattu erilaisia huoltovarmuusskenaarioita vastaan relevanttien toimenpiteiden tunnistamiseksi? Onko tunnistetuille skenaarioille tehty toimintasuunnitelmat?

- Skannataanko tunnetut haavoittuvuudet koko järjestelmästä säännöllisesti?
- Miten varmistetaan haavoittuvuuksia sisältävien komponenttien päivitykset tarvittaessa?
- **Miten uhkamallinnus on tehty?**
- Onko mietitty, mitä eri asioita voi mennä pieleen?
    - Mitä osia ratkaisussa voidaan käyttää väärin, mikä voi rikkoutua, miten käyttöoikeuksia voidaan hyödyntää vääriin tarkoituksiin jne.?
    - Miten tunnistettujen väärinkäyttöskenaarioiden vaikutusta voidaan pienentää?
    - Kuinka estää ratkaisun osakomponenttien väärinkäyttö, kuinka suojataan käyttöoikeuksia ja kirjautumisia ym.?
- Miten on arvioitu tehdyn uhkamallinnuksen ja hallintakeinojen laajuutta ja riittävyyttä?
- Miten on varauduttu kyberhyökkäysten torjumiseen?
- **Miten järjestelmän ja sen laitteiden ja komponenttien turvallisuus on varmistettu?**
    - Miten turvallisuuspuutteet voidaan tunnistaa? Erilaisten heikkouksien, haavoittuvuuksien ja virheiden hyödyntäminen verkkojen operatiivisessa ylläpidossa, esimerkiksi inhimillisten konfiguraatiovirheiden, korjaamattomien haavoittuvuuksien hyödyntäminen.
- Onko kaikki järjestelmän komponentit luetteloitu?
    - Ylläpidetäänkö luetteloa ja kaikkien komponenttien todellinen tila on tiedossa (myös virtuaalikoneet)?
- Miten laitteiden turvallisuudesta on huolehdittu (verkko-, reunalaskenta- ja päätelaitteet)?
    - Onko käytössä muita kuin standardoituja laitteita?
    - Onko laitteet sijoitettu turvallisiin tiloihin mahdollisuuksien mukaan?
    - Onko laitteiden oletuskonfiguraatiot muutettu niin, että laitteet ovat turvallisia?
    - Pidetäänkö laitteiden ohjelmistot ajan tasalla?
    - Sallitaanko laitteiden päivitykset vain luotetuista lähteistä?
- Miten verkkokomponenttien turvallisuudesta on huolehdittu?
    - Miten verkkoelementit on konfiguroitu varmistamaan verkon turvallisuuden?
    - Miten verkkosuunnittelussa ja -toteutuksessa on tehty toimenpiteitä rajoittamaan hyökkääjän etenemistä verkossa?

    - Onko liikenne salattu kaikkien komponenttien välillä?

- Miten sovellusten turvallisuus on varmistettu?

    - Onko sovelluksille ja ohjelmistokomponenteille tehty tarkoituksenmukainen konfigurointi mm. oletustunnukset on poistettu ja/tai salasanat muutettu?

    - Tehdäänkö sovelluksille ja niiden ohjelmistokomponenteille haavoittuvuusskannaukset säännöllisesti?

    - Päivitetäänkö haavoittuvuuksia sisältävät sovellukset ja ohjelmistokomponentit suunnitellusti?

    - Onko pelkästään välttämättömät rajapinnat julkaistu käytettäväksi? Miten rajapintojen turvallisuudesta on huolehdittu?

- Onko data turvassa?

    - Miten kriittisen datan salauksesta on huolehdittu?

    - Missä data sijaitsee? Onko sijaintia määritelty ja onko sijainti eri tilanteissa hallinnassa?

        - Sijaintivaatimus voi olla esim. Suomen tai EU:n rajojen sisällä.

- **Miten verkkoympäristön operoinnin tuvallisuudesta on huolehdittu?**

    - Kuinka laajasti järjestelmä on monitoroinnin piirissä?

    - Miten virtualisointi-levykuvien tietoturvasta on huolehdittu?

    - Miten kiristysohjelmia ja muita haittaohjelmia sisältävien levykuvien jakaminen ja käyttäminen on estetty?

    - Miten verkkotietoturva, esimerkiksi virtuaalikoneiden välisten yhteyksien hallinta ja sen mahdolliset puutteet voidaan tunnistaa?

    - Miten riittävän tasoinen eriyttäminen on toteutettu?

    - Miten eri luottamustasojen välisten rajoitusten mahdolliset puutteet voidaan tunnistaa?

    - Missä määrin hypervisor-alustan tietoturvakontrollit ovat riittävän kattavat ja hallinnassa?

    - Miten integraatioiden tietoturva, erityisesti pilvipalveluihin, on varmistettu?

- Miten turvallisuus on otettu huomioon kaikissa järjestelmän rakentamisen vaiheissa ja kaikissa komponenteissa?

    - Miten autentikoiti on toteutettu? Autentikoidaanko sekä lähettäjä, että vastaanottaja?

    - Ovatko kaikki järjestelmän komponentit turvallisia?

    - Jos ulkopuolinen pääsee järjestelmään sisään, saadaanko vahingot minimoitua tekemällä kaikista komponenteista riittävän turvallisia?
  - Onko tietoliikenne salattua päästä päähän?

- **Miten jatkuvuudenhallintaa on suunniteltu?**
- Miten erilaiset vikatilanteet on otettu huomioon?
- Millä tasolla ratkaisulle on tunnistettu erilaiset uhkaskenaariot ja niille tarkoituksenmukaiset hallintakeinot?
- Missä määrin laitteiden varakomponenttien saatavuutta ja varastointia on suunniteltu? Miten varastoidut komponentit säilyvät jatkuvasti käyttöönottokunnossa?
- Miten radioverkon häiriö- tai vikatilanteiden vaikutukset toimintavarmuuteen on huomioitu? Mikä on toimintasuunnitelma erilaisissa radioverkon vikatilanteissa?
- Millä tavoin radioverkkosuunnittelussa ja toteutuksessa on huomioitu radioverkon kapasiteetin äkillinen aleneminen tai peittoalueen kutistuminen häiriöiden tai vikatilanteiden vuoksi?
- Millä tavoin toteutukselle on varmistettu tarvittavat varayhteydet?
- Miten henkilöstön riittävä saatavuus ja myös varahenkilöstön osaaminen on varmistettu erilaisia poikkeustilanteita varten?
- Miten kumppaneilta saatava verkkoympäristön operointiin liittyvä kriittinen tuki voidaan varmistaa myös erilaisia poikkeustilanteita varten?
- Miten toimittajaketjun jatkuvuudenhallinta on varmistettu ja varajärjestelyt suunniteltu esimerkiksi vaihdettaessa pilvialustaa?
    - Palveluiden siirtäminen pilvialustalta toiselle. Ongelmaksi saattaa nousta eri palveluiden natiivikomponenttien hyödyntäminen, joka sitoo tiettyyn alustaan. Tällaiset riippuvuudet on tärkeä tunnistaa ja dokumentoida.
- Miten palveluiden siirtäminen poikkeustilanteessa joko kotimaahan, tai kotimaan ulkopuolelle on suunniteltu?
    - Kansainvälisten verkkoyhteyksien katketessa palveluiden sijainti kotimaassa voi olla parempi ratkaisu.
    - Paikallisen katastrofin sattuessa, palveluiden sijainti ulkomailla voi olla parempi ratkaisu, jos tietoliikenneyhteydet toimivat.
- Miten hyökkäyspinta-ala on tunnistettu, minimoitu ja dokumentoitu?
  - Onko käyttöoikeudet minimoitu ja oikeudet vain niillä jotka niitä oikeasti tarvitsevat? Erityisesti ylläpitäjätunnusten hallintaan pitää kiinnittää huomiota.
  - Miten hallinnointiyhteydet on suojattu?

- Miten yhdysliikennerajapinnat on suojattu?
- Millä tavalla yleiseen viestintäverkkoon näkyvien komponenttien määrää on rajoitettu ja komponentit suojattu?

Käsitteet ja lyhenteet

Käsite	Määritelmä	Lisätietoa
3GPP	3rd Generation Partnership Project	Usean standardointijärjestön yhteistyöorganisaatio, joka pyrkii luomaan matkaviestinjärjestelmille maailmanlaajuisia teknisiä määrittelyjä
4G	Nejännen sukupolven matkaviestinjärjestelmä	
5G	Viidennen sukupolven matkaviestinjärjestelmä	
6G	Kuudennen sukupolven matkaviestinjärjestelmä, jonka määrittelytyö on vielä kesken.	White Papers - 6G Flagship
CERT	Kyberturvallisuuskeskuksen CERT-toiminnon tehtävänä on ennaltaehkäistä tietoturvaloukkauksia ja tiedottaa tietoturva-asioista.	
Core network	Ydinverkko	
EDR	End-point-Detection/Reponse	
ENISA	European Network Information Security Agency	
EPC	Evolved Packet Core	Viimeisin versio 3GPP ydinverkkoarkkitehtuurista
ETSI	European Telecommunications Standards Institute	Eurooppalainen telealan standardisoimisjärjestö
GDPR	General Data Protection Regulation	
GSMA	Global System for Mobile Communications	
IoT	Internet of Things	
IP	Internet Protocol	
IT	Information Technology	
Kyber-	tietoverkkoihin liittyvä	
Kyberhyökkäys	verkkohyökkäys	https://www.kielitoimistonsanakirja.fi/#/kyberhy%C3%B6kk%C3%A4ys
Kyberturvallisuus	yhteiskunnan ja sen kriittisten järjestelmien toimintavarmuus kyberhyökkäysten varalta	https://www.kielitoimiston-sanakirja.fi/#/kyberturvallisuus
LTE	Long Term Evolution	
LTE EPC	LTE Evolved Packet Core	
MEC	Multi-access Edge Computing	
MFA	Multi Factor Authentication	
NESAS	Network Equipment Security Assurance Scheme	
NIST	National Institute of Standards and Technology	
Open RAN	O-RAN alliance is working for transforming Radio Access Networks Towards Open, Intelligent, Virtualized and Fully Interoperable RAN	https://www.o-ran.org/
OT	Operational Technology	
OWASP	Open Web Application Security Project®	OWASP Foundation | Open Source Foundation for Application Security

PMO	Paikallisen matkaviestinverkon Operoija (Operaattori?)	Taho joka operoi paikallista matkaviestinverkkoa
Ransomware	kiristysohjelma	
RAN	Radioliityntäverkko (Radio Access Network)	
RED	Radio Equipment Directive	
SDLC	Software Development LifeCycle	
SVPL	Laki sähköisen viestinnän palveluista	
SDN	Software Defined Networking	
SEI	Software Engineering Institute	
SMS	Short Message Service	
TCP	Transmission Control Protocol	
Teleyritys	Lain määritelmän mukaan teleyrityksellä tarkoitetaan sitä, joka tarjoaa verkkopalvelua tai viestintäpalvelua ennalta rajaamattomalle käyttäjäpiirille eli harjoittaa yleistä teletoimintaa.	
TLS	Transport Layer Security	
TPM	Trusted Platform Module	
Viestinnän välittäjä	teleyritys, yhteisötilaaja tai muu sellainen taho, joka välittää sähköistä viestintää muutoin kuin henkilökohtaisiin tai niihin verrattaviin tavanomaisiin yksityisiin tarkoituksiin	
Wiper	tietojen tuhoaja	

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus
PL 320, 00059 TRAFICOM
p. 029 534 5000

kyberturvallisuuskeskus.fi

ISBN 978-952-311-848-5
ISSN 2669-8757 (Verkkojulkaisu)

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus