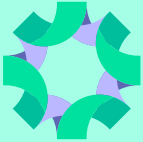




5G-privaattiverkkojen riskienhallinnan ohjeistus



Huoltovarmuusorganisaatio



Huoltovarmuusorganisaatio

www.huoltovarmuuskeskus.fi

Huoltovarmuudella tarkoitetaan kykyä sellaisten yhteiskunnan taloudellisten perustoimintojen ylläpitämiseen, jotka ovat välttämättömiä väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen materiaalistien edellytysten turvaamiseksi vakavissa häiriöissä ja poikkeusoloissa.

Huoltovarmuuskeskus (HVK) on työ- ja elinkeinoministeriön hallinnonalan laitos, jonka tehtävänä on maan huoltovarmuuden ylläpitämiseen liittyvä suunnittelu ja operatiivinen toiminta.

Huoltovarmuusorganisaatio (HVO) on verkosto, joka työskentelee yhdessä Suomen toimintakyvyn ja sen edellyttämän huoltovarmuuden hyväksi. Siihen kuuluvat Huoltovarmuuskeskus ja sen hallitus, huoltovarmuusneuvosto sekä eri toimialojen sektorit ja poolit. Lisäksi yhteistyötä tehdään alueellisten toimijoiden, kuten aluehallintovirastojen, kuntien ja kaupunkien sekä alueellisten toimikuntien kanssa.

Julkaisija: Huoltovarmuuskeskus

Laatinut: PricewaterhouseCoopers Oy

Kuvat: Gettyimages

Taitto: LM Someco Oy

Julkaisuvuosi: 2025

ISBN: 978-952-7470-39-8

This work is licensed under CC BY 4.0.
To view a copy of this license, visit
<https://creativecommons.org/licenses/by/4.0/>

Sisältö

1 Johdanto	5
1.1 Tämän ohjeistuksen tausta, tarkoitus ja kohderyhmät	5
1.2 Riskien hallinta on varautumisen perusta	6
1.3 Miksi privaattiverkkoihin investoidaan	6
1.4 Verkkoteknologiset vaihtoehdot	7
2 Riskienhallinta ja kyberturvallisuuden toimintamalli	8
2.1 Riskienhallinnan toimintaperiaatteet	8
2.2 Riskienhallinnan tehokkuus	8
2.3 Kyberturvallisuuden toimintaperiaatteet	8
3 Verkon hankinnan riskienhallinta	9
3.1 Verkon hankinta	9
3.1.1 Kasvava riski toimitusketjuissa	9
3.1.2 Toimitusketjut ja keskinäiset yhteydet	9
3.1.3 Sääntelyyn ja vaatimustenmukaisuuteen liittyvät haasteet toimitusketjuissa	9
3.1.4 Lisätietoa ja linkejä toimittajiin kohdistuvista riskeistä	10
3.2 Tuoteturvallisuuteen liittyvät vaatimukset toimittajille	10
3.2.1 Kriittiset verkkolaitteet	10
3.2.2 Laitteisiin liittyviä erityisvaatimuksia	10
3.3 Pilvipalveluihin liittyvät vaatimukset toimittajille	11
3.3.1 Pilvipalvelujen tarjoajien palveluiden soveltaminen erillisverkossa	11
3.3.2 Vaatimukset pilvipalvelujen toimittajalle	11
3.3.3 Lisätietoa ja linkejä pilvipalveluihin liittyvästä turvallisuusvaatimuksista 5G verkkoihin liittyen	13
4 Verkon suojaaminen	15
4.1 Käytössä olevan verkon turvallisuus	15
4.2 Ohjelmistokehityksen turvallisuus	15
4.2.1 Lisätietoa ja linkejä turvallisista ohjelmistokehitysvaatimuksista	16
5 Verkon ylläpito ja valvonta	18
5.1 Verkon ylläpidon elinkaarimalli	18
5.1.1 Tuotteen arviointi, testaus ja elinkaaren tuki	18
5.1.2 Tuotteen arviointia, testausta ja elinkaaritukea koskevat vaatimukset	18
5.1.3 Lisätietoa ja linkejä tuotetestausvaatimuksista	20
5.2 Verkon hallinta, valvonta sekä turvallisuuden kehittäminen	21
5.2.1 IT infrastruktuurin valvonta tietoliikenneverkon rakenteissa	22
5.2.2 Viipaloinnin valvonta	24
5.2.3 Virtualisoinnin hallinta	25

5.2.4	Verkkovierailuyhteyksien ja kansallisen yhteyden seuranta	25
5.2.5	Puhelupalvelujen, erillisverkkojen ja reunalaskennan valvonta	26
5.2.6	Euroopan telealan standardointilaitos (ETSI) Multi-Access Edge Computing (MEC)	27
5.2.7	Network Exposure Function (NEF)	27
5.2.8	Reunalaskenta	28
5.2.9	Yksityisten verkkojen rajapintojen valvonta	28
5.2.10	Ydinverkon yleinen ohjaustason valvonta	29
5.2.11	Ydinverkon valvonta (käyttäjätaso)	30
5.2.12	SIM-kortin etävalmisteluinfrastruktuurin valvonta	31
5.2.13	Radioliityntäverkon (RAN) ja runkoliityntäyhteyksien valvonta	31
6	Haavoittuvuuksien ja poikkeamien hallinta	32
6.1	Haavoittuvuustietojen raportointi	32
6.1.1	Haavoittuvuustiedot	32
6.1.2	Haavoittuvuustietojen raportointia ja korjauspäivitysten hallintaa koskevat vaatimukset	32
6.1.3	Lisätietoa ja linkkejä haavoittuvuustietojen hallinnasta ja raportoinnista	33
6.2	Häiriötietojen raportointi	33
6.2.1	Häiriötietojen raportointia koskevat vaatimukset	33
6.2.2	Lisätietoa ja linkkejä häiriötietojen raportoinnista	34
7	Kontrollit	35
7.1	Verkon hankinnan kontrollit	36
7.2	Verkon valvonnan kontrollit	57
7.3	Varautumisen ja kriisistä palautumisen kontrollit	69

1 Johdanto

Digitalisoituminen on yksi yhteiskunnan tärkeimmistä turvallisuus- ja kilpailutekijöistä. Mitä tehokkaammin ja nopeammin, mutta samalla turvallisemmin voimme hyödyntää digitalisaation tarjoamia mahdollisuuksia, sitä paremmin tulemme yhteiskuntana pärjäämään globaalissa kilpailussa.

Olemme edenneet digitalisoinnissa siihen vaiheeseen, että lähes kaikki yhteiskunnan palvelurakenteet tarvitsevat tiedon välittämiseen vaadittavaa turvallista tietoliikenneinfrastruktuuria, joka on näin ollen myös keskeinen osa kansallista kriittistä infrastruktuuria. Tietoliikenneverkkojen ympärillä on havaittu enenevässä määrin pyrkimyksiä anastaa, häiritä tai lamauttaa tietoliikennettä. Näitä pyrkimyksiä vastaan on puolustauduttava jatkuvasti. Otettaessa uusia teknologioita käyttöön, on oltava erityisen varovainen, koska yleensä kehityspanostukset kohdistetaan aluksi teknologian toimivuuteen riskienhallintanäkökulmien jäädessä vähemmälle huomiolle.

Tätä taustaa vasten Huoltovarmuuskeskus on nähnyt tarpeelliseksi, että 5G-teknologian käyttäjien riskienhallintaan laaditaan ohjeistus. Tämä ohjeistus on suunnattu erityisesti Suomen kriittisen infrastruktuurin organisaatioille.

5G teknologian mahdollistamat uudet tietoliikennearkkitehtuurimallit lisäävät tietoliikenneverkkojen monikäyttöisyyttä. Yhteiskunnassa ja eri organisaatioissa tullaan ottamaan käyttöön 5G teknologialla toteutettuja privaattiverkkoja. Näissä yritysverkoissa voi olla aiempaa enemmän verkon hallintaan liittyviä toimijoita, joiden vastuut tulee ottaa hankinnan yhteydessä tehtävissä sopimuskokonaisuuksissa huomioon. On hyvä tiedostaa, että lopulta verkon haltija on vastuussa verkosta. Tästä syystä tämä ohjeistus alkaa 5G-privaattiverkon riskienhallinnassa jo hankintavaiheesta.

5G teknologiaan liittyvät standardit ovat vielä osin kesken, ja osa uusista ominaisuuksista on julkaistu samoihin aikoihin, kun tätä ohjeistusta on laadittu. Näin ollen, kaikki toiminnallisuudet joihin ohjeessa viitataan, eivät välttämättä ole vielä käytännössä teknologisesti saatavilla. Ne ovat merkittäviä riskienhallintaan vaikuttavina toiminnallisuuksina, jotka on tiedostettava tulevan varautumisen kannalta. Ohjetta luettaessa on siis huomioitava aikajänne, joka voi vaikuttaa kontrollien soveltamiseen. Kun kyseessä on vielä nopeasti muuttuva teknologinen soveltamisala, ohjeistukseen tulee päivityksiä säännöllisesti.

On todennäköistä, etteivät nykyiset verkkolaitteet ja ohjelmistot pysty vielä lähtökohtaisesti täyttämään

kaikkia tässä ohjeistuksessa esitettyjä kattavan riskienhallinnan teknisiä ja ohjelmallisia vaatimuksia. Ohjeistus onkin tarkoitettu helpottamaan myös toimittajia huomiomaan riskienhallinnan tarpeet heti suunnitteluvaiheessa myös tulevaisuuden vaatimukset huomioiden.

Ohjeistuksen alkuosassa on kuvattu tietoliikenneverkkojen riskienhallinnan osa-alueita ja loppuosassa on luettelo kontrolleista, joiden avulla riskejä voidaan hallita käytännössä. Kunkin verkkoympäristön kokonaisuutta tulee kuitenkin arvioida tietoliikennearkkitehtuurin, käyttöönottan organisaation sekä sen toimialan erityispiirteet huomioiden. Tässä ohjeistuksessa olevat kontrollit eivät siis välttämättä sovellu sellaisenaan implementoitaviksi, vaan ne on räätälöitävä tapauskohtaisesti eri ympäristöihin ja toimialoihin soveltuviksi.

1.1 Tämän ohjeistuksen tausta, tarkoitus ja kohderyhmät

Tämä ohjeistus on tarkoitettu erityisesti niille organisaatioille, jotka ovat osa Suomen kriittistä infrastruktuuria ja jotka käyttävät tai tulevat käyttämään 5G-privaattiverkkoa toiminnassaan. Ohjeistus on muidenkin organisaatioiden hyödynnettävissä. Riskit, joita ohjeistuksen kontrolleilla pyritään hallitsemaan, voivat olla minkä tahansa 5G-privaattiverkkoja käyttävän organisaation uhkana.

Kehittyvä 5G-viestintäteknologia avaa organisaatioiden viestiverkkoihin uusia hyökkäysrajapintoja. Niiden systemaattinen ja kattava kontrollointi on syytä implementoida toimintaympäristöön samassa aikataulussa uuden teknologian käyttöönoton kanssa.

Organisaatioilla itsellään on harvoin uusien teknologioiden riskienhallintaan riittäviä resursseja, tai osaamista. Siksi erityisasiantuntijoiden laatima ja yleiseen käyttöön tuleva ohjeistus vaadittavista toimenpiteistä tehostaa ja nopeuttaa siirtymistä uuteen teknologiaan. Se helpottaa riskejä torjuvien kontrollien käyttöönottoa ja näin koko yhteiskunnan kilpailukyky ja riskienhallinta paranee.

Ohjeistuksella tuetaan konkreettisesti huoltovarmuus-kriittisten organisaatioiden turvallisten 5G-verkkojen suunnittelua ja rakentamista. Ohjeistuksen avulla viedään konkreettisesti eteenpäin EU:n ja Suomen valtion tasolla aloitettua 5G-riskienhallinnan kehitystyötä ja siinä hyväksikäytetään tähän mennessä EU:n ja Traficomien työryhmissä valmisteltua ja julkaistua aineistoa. Tämä on jatkumoa HVK:n rahoittamille ja Traficomien toteuttamille 5G kyberturvallisuutta koskeville hankkeille.

Ohjeistuksessa loppuosassa esitetyt kontrollit perustuvat alan standardeihin ja viitekehyksiin, organisaatioiden kanssa käytyihin keskusteluihin, soveltuviin käytäntöihin, EU:n ja Traficom:n työryhmissä valmisteluihin ja julkaistuihin aineistoihin, lainsäädäntöön sekä alan erityisohjeistuksiin.

Ohjeistus ja kontrollit ovat kuvattu yleistasolla, ja niihin ei ole huomioitu erityistoimialojen poikkeavia vaatimuksia. Kunkin toimijan tulee varmistaa osaltaan viimeisin lainsäädännöllinen ohjeistus sekä sovitettava tämän ohjeistuksen mukaiset suositukset soveltuvin osin omaan ympäristöönsä sopivaksi.

Ohjeistuksessa on myös viitteitä lähteisiin, joista löytyy lisätietoa ohjeistuksen soveltamisen tueksi.

1.2 Riskien hallinta on varautumisen perusta

Kasvaviin ughiin tulisi varautua systemaattisella riskien hallinnalla. Ensin on tunnettava organisaation toiminta, olemassa olevat rakenteet, organisaatio, roolit organisaatiossa, suojattavat kohteet, käytössä olevat teknologiat, vallitseva lainsäädäntö sekä tunnettava organisaation tavoitteet.

Riskit, jotka voivat estää tavoitteiden saavuttamisen, on tunnistettava. Tämän jälkeen voidaan suunnitella sekä implementoida riskien hallitsemisen kontrollit. Varautumisen tueksi on harjoitettava, miten erilaisissa riskitilanteissa tulee toimia sekä suunniteltava tarkoin, kuinka riskien realisoituessa, palaudutaan.

Tietoliikenneverkon muuttuminen 5G-teknologian myötä laajentaa riskienhallinnan kokonaisuutta monimutkaisemmaksi ja vaikeammin hallittavaksi. Muun muassa teknologian tuomat riskit, monitoimittajaympäristö, verkkoon liitettävän laitekannan lisääntyminen, paikallisten matkaviestinverkkojen sekä siihen liittyvän reunalaskennan kompleksisuus vaativat riskienhallintatoimien päivittämistä.

Aiemmat puhelinverkkosukupolvet perustuivat puhelinoperaattoreiden toteuttamiin verkkoratkaisuihin. Teknologioista tai niiden varaan rakennetuista palveluista vastasivat puhelinoperaattorit. Liiketoimintamallit perustuivat joko liittymä- tai kapasiteettipohjaiselle mallille, jolla yritykset ja organisaatiot ostivat palvelua puhelinoperaattoreilta.

Näiden palveluiden hankintaan ei vaadittu ostajalta syvempää ymmärrystä tietoliikenne- tai puhelinverkkojen rakenteesta, vaan lähtökohtaisesti toiminta perustui luottamukseen osapuolten välillä. Toisaalta langaton tietoliikenne on pääosin ollut vain datan ja puheen välittämistä päätelaitteelta tukiasemalle ja tuki-

asemalta eteenpäin tietoliikenneinfrastruktuuria hyödyntäen vastaanottajalle. Olennaisia kriteereitä palvelumalleissa, oli tietoliikenteen nopeus sekä kapasiteetti. Saatavuuden turvaamiseksi käytettiin palvelurakenteiden kahdentamista, eli useampia reititysyttejä sekä mahdollisesti palvelutuottajiksi valittiin kaksi toimittajaa verkkoliikennöinnin ylläpidon turvaamiseksi. Kapasiteettipohjaisissa sopimusmalleissa palvelun ostaja oli vastuussa oman kapasiteettitarpeen arvioinnista ja liittymäpohjaisessa mallissa tarjottiin tavoitteellisia saatavuustekijöitä, joiden osalta saattoi verkon kuormituksesta johtuen olla hetkellistä vaihtelua.

Näihin toimintamalleihin tulee muutoksia 5G-teknologian käyttöönoton yhteydessä, jolloin organisaatioiden on syytä päivittää myös riskienhallinnan kokonaisuus kontrolleineen koko arvoketju huomioimalla alusta loppuun. Uudentyyppisiä riskejä voi ilmetä hankintavaiheessa, käyttöönotossa, ylläpidossa, järjestelmien kehittämisessä, laitteiden hankinnassa, integraatioissa, liikenteen ja datan käytön suunnittelussa, verkon kattavuuden varmistamisessa, paikallisen pilvipalvelun kehittämisessä, yksityisverkon ja julkiverkon välisessä rajapinnassa, mahdollisissa roaming tarpeissa, laskutuksessa, kustannuksien hallinnassa, jatkoinvestoinneissa, turvallisuudessa sekä jatkuvasta koulutuksessa. Tämä ohjeistus on laadittu edellä lueteltujen aiheiden riskienhallinnan tueksi.

1.3 Miksi privaattiverkkoihin investoidaan

Digitalisaatiossa hyödynnetään langattomia verkkoja sitä enemmän, mitä paremmiksi ne saadaan kehitettyä erityisesti siirtonopeuden, latenssin, kapasiteetin, energiakulutuksen ja häiriöttömyyden osalta. Myös se, miten monia laitteita verkkoon voidaan kytkeä samanaikaisesti, on tärkeää hyödynnettävyyden näkökulmasta. Kun edellä mainitut kyvykkyydet saadaan riittäväälle tasolle langattomissa verkoissa, niiden avulla on mahdollista toteuttaa entistä dynaamisempia ja tehokkaampia liiketoimintaprosesseja.

Esimerkiksi liikkuva satamanosturi tarvitsee laadullisesti tarkkaa sijaintietoa nopeasti. Tällöin siihen liittyvää dataa ei voida siirtää pilvipalvelukeskuksiin satojen tai tuhansien kilometrien päähän käsiteltäväksi, vaan sen on oltava pienemmän verkkoviiveen takia lähempänä nosturia. Siksi on rakennettava lähipilvipalveluratkaisu, jonka ansiosta pienen latenssin vaativa data on lähellä ja se voidaan prosessoida nopeasti. Muu vähemmän aikakriittinen data voidaan siirtää perinteisempää dataväylää pitkin.

Erillisverkoista jaetaan tietoa useille toimijoille ja niissä on huomioitava mm. verkkovierailut, laitteiden yhteensopivuudet, erityyppisten toimittajaketjujen hallinta ja

näiden takia myös uudentyyppiset turvallisuusuhat. Toisaalta 5G-teknologia tarjoaa huomattavasti kehittyneempää turvallisuutta langattomaan datan siirtämiseen kuin aiempien sukupolvien dataverkot, mutta samalla myös hallintamallit muuttuvat. Muutoksen mukana syntyy samalla uuden tyyppisiä riskejä tietoliikenneverkoille ja niitä hyödyntäville palveluille.

1.4 Verkkoteknologiset vaihtoehdot

Organisaatio voi hankkia privaattiverkon ja hallita sitä itse ilman ulkopuolista toimijaa, tai sen voi toteuttaa hankkimalla oman erillisen verkkosegmentin teleoperaattorilta tai verkkoihin erikoistuneelta palvelutuottajalta.

Oman taajuuden hankkimalla organisaatio voi saada täyden kontrollin omaan erillisverkkoon ilman operaattoria tai kolmansien osapuolten mukanaoloa. Organisaatio toimii tällöin itse operaattorina. Organisaation vastuulle tulee tukiasemat, antennit, verkon taustajärjestelmät, kaikki verkkoon tuotettavat palvelut sekä siihen liitettävät laitteet. Lisäksi tässä vaihtoehdossa tulee erikseen suunniteltavaksi verkkovierailut ja niihin liittyvät yhdysliikennesopimukset.

Toinen tapa toteuttaa erillisverkko on ns. viipaleteknologia. Tällöin olemassa olevasta 5G puhelinoperaattorin verkosta viipaloidaan erillinen virtuaalinen osa, josta valitaan eritasoisia toteutuksia, asiakkaan tarpeitten mukaan. Tyypillisesti tähän vaihtoehtoon operaattori tarjoaa verkon ylläpitoon, laitteiden tai liittymien hallintaan, mahdollisesti laskutukseen sekä muihin tietoliikenneverkkoon liittyvien palveluiden tuottamiseen palvelumalleja.

Näitä kahta vaihtoehtoista toteutuskokonaisuutta voi myös hyödyntää erityyppisinä yhdistelminä ja niihin liittyviä palveluita voivat toteuttaa erityyppiset palveluja järjestelmätoimittajat.

2 Riskienhallinta ja kyberturvallisuuden toimintamalli

2.1 Riskienhallinnan toimintaperiaatteet

Riskienhallinnan tulee olla keskeinen osa yrityksen strategista ja operatiivista suunnittelua. Periaatteena tulisi noudattaa ennakoivaa ja kattavaa merkittävien riskien arviointia ja tunnistamista. Lähtökohtaisesti riskienhallinnan pohjan voidaan soveltaa esimerkiksi ISO31xxx – standardia. On tärkeää tarkastella riskejä niin liiketoiminnallisen kuin muun operatiivisen toiminnan näkökulmista. Olennaisia osa-alueita ovat toimitusketjuihin, henkilöstöön, teknologiaan sekä viestintäverkkoa käyttävien tahojen näkökulmat. Riskienhallinnan toimeenpanon on oltava järjestelmällistä ja luotettavaa sekä riskienhallinnan periaatteet ja vastuut on määriteltävä riittävän selkeästi ja yrityskohtaisesti ja dokumentoituna kirjallisesti. Riskien hallintaan tulee sitouttaa koko organisaation henkilökunta.

Varsinaisesti riskienhallinnan toimintaperiaatteisiin ei erillisverkkojen osalta ole erityistä lisättävää, vaan siihen soveltuu riittävän kattavasti ”Liikenne- ja viestintävirasto Traficomien suositus NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä”-dokumentaatio sekä yleisesti suositeltavat laajasti käytettävät riskien hallintastandardit.

Tämä lisäksi riskienhallinnallisesti Kyberturvallisuuskeskus on julkaisut erillisen määräyksen viestintäverkon kriittisistä osista. Mikäli erillisverkko on kytkettynä tai sen kautta on olemassa yhteys julkiseen viestintäverkkoon, on kiinnitettävä listattujen kriittisen osien osalta erityistä huomiota varautumiseen sekä niihin osiin kohdistuvaan riskienhallintaan.

2.2 Riskienhallinnan tehokkuus

Riskienhallinnan tehokkuus perustuu hyvään kontrolliseen suunnitteluun ja suunniteltujen kontrollien noudattamiseen. Kriittisiin erillisverkkoihin liittyvät kontrollien toimivuus on suositeltavaa todentaa auditoinnilla, johon on olemassa myös siihen hyvin soveltuva kansainvälinen ja laajasti käytetty standardi (ISAE3000). Auditoinnin laajuus voi vaihdella verkon ja käyttökohteen laajuuden ja kriittisyyden perusteella. Koska viestintäverkkoihin liittyy poikkeuksellisen paljon uudentyypisiä riskejä, mm. toimittaja riippuvuudet, toimittajien omistuksien vaihdokset, jatkuva lainsäädännön uudistuminen sekä valtioiden välinen kilpailu, auditointeja tulisi toteuttaa säännöllisin väliajoin.

2.3 Kyberturvallisuuden toimintaperiaatteet

Riskienhallinnan yleisiin toimintaperiaatteisiin ei erillisverkkojen osalta ole erityistä lisättävää. Siihen soveltuu kattavasti Liikenne- ja viestintävirasto Traficomien suositus NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä.

3 Verkon hankinnan riskienhallinta

3.1 Verkon hankinta

3.1.1 Kasvava riski toimitusketjuissa

5G-privaattiverkkoa hankkiessa on tärkeää tiedostaa, että tietoliikenneinfrastruktuurin toimitusketjussa on paljon toimijoita. Riskienhallinnan näkökulmasta tämä tarkoittaa, että privaattiverkkokin on altis toimitusketjuhyökkäyksille monimutkaisten ja toisiinsa kytkeytyneiden teknisten kokonaisuuksien takia. Hankintasopimuksia laadittaessa tämä on tärkeää huomioida.

Toimitusketjuihin liittyvät riskit tulevat esille ENISA:n uhkakuvaraportissa (lokakuu 2023), missä todetaan toimitusketjuhyökkäyksistä seuraavaa:

”Toimitusketjuhyökkäyksistä kohdistuivat julkishallintoon (21 %), digitaalisen palvelun tarjoajiin (16 %), digitaaliseen infrastruktuuriin (10 %) ja energiasektoriin (9 %).

Haavoittuvuuksien hyödyntäminen kohdistuivat digitaalisen palvelun tarjoajiin (25 %), digitaalisiin infrastruktuureihin (23 %) ja julkishallintoon (15 %), laajasti kaikkiin sektoreihin (8 %) sekä yksittäisiin henkilöihin (8 %).”

ENISAn raportissa esitetyt lähitulevaisuuden näkymät osoittavat, että toimitusketjun organisaatioiden riskienhallintaa on syytä valvoa sen lisäksi, että huolehditaan oman organisaation riskienhallinnasta.

”Hämmästyttävää on että, 61 prosenttia yrityksistä on joutunut ohjelmistojen toimitusketjuhyökkäyksen kohteeksi viimeisen kahdentoista kuukauden aikana, ja näiden yrityksiin kohdistuvien hyökkäysten kokonaiskustannuksien arvioidaan kasvavan 76 prosenttia vuonna 2026, vuoteen 2023 verrattuna.”

ENISA:n tekemän kartoituksen perusteella voi todeta, että hyökkääjät näkevät toimitusketjuhyökkäykset yhtenä keskeisenä keinona päästä käsiksi yritysten toimintaan. Tämän ne tekevät kohdistamalla hyökkäykset toimittajiin varsinaisen kohdeyrityksen sijaan. Hyökkääjien varsinaiset hyökkäyskohteet ovat usein hyvin turvattu ja siksi hyökkäyksen kohdistaminen heikommin varautuneeseen toimittajaan on hyökkääjän kannalta tehokkaampi lähestymistapa. Vaikka toimitusketjuihin kohdistunut hyökkäys ei ole vielä yleisin hyökkäystyyppi, sitä ei pidä jättää varautumisen ulkopuolelle. ENISA uskoo raportissaan toimitusketjuhyökkäysten nelinkertaistuvan lähitulevaisuudessa, minkä perusteella on syytä panostaa aiempaa enemmän toimittajien hyökkäyksiin varautumisen valvontaa. Tämä

on tärkeää huomioida myös 5G-privaattiverkkojen toimittajien osalta hankintasopimuksia tehtäessä.

3.1.2 Toimitusketjut ja keskinäiset yhteydet

Toimitusketjujen valvontaan aiheuttaa haasteita se, että tietoliikenneinfrastruktuurin toimitusketjussa on paljon toimijoita: laitevalmistajia, ohjelmistokehittäjiä, palveluntarjoajia ja logistiikkayrityksiä. Rakenteen monimutkaisuus laajentaa hyökkäyspintaa ja mahdollistaa lukuisia sisään tulopisteitä hyökkääjille. Toimitusketjun keskinäiset kytkökset johtavat siihen, että kompromissit turvallisuuskontrolleissa missä tahansa toimitusketjun osassa voivat johtaa vakaviin tietomurtoihin, jotka vaikuttavat moniin organisaatioihin ja niiden asiakkaisiin.

Advanced Persistent Threat (APT) -organisaatiot ovat vastuussa huomattavasta määrästä toimitusketjuhyökkäyksiä. Nämä organisaatiot suorittavat kehittyneitä, kohdennettuja hyökkäyksiä, joiden tavoitteena on saada pitkäaikainen pääsy arkaluonteisiin tietoihin. Esimerkiksi APT29:n aiheuttama SolarWinds-hyökkäys oli esimerkki menetelmistä, joilla hyökkääjät voivat soluttautua toimitusketjuun ja pysyä siinä piilossa johtaen laajoihin yritysten verkkojen vaarantumisiin. APT-hyökkäykset käyttävät usein kehittyneitä sosiaalisen suunnittelun tekniikoita sekä nollapäivän haavoittuvuuksia tunkeutuakseen alkuperäisiin kyberpuolustuksiin. Näin tekemällä ne voivat ylläpitää jatkuvaa järjestelmän hallintaa ja liikua järjestelmien sisällä. Tämä voi johtaa pitkäaikaiseen arkaluontoisten tietojen vuotamiseen ja laajoihin vahinkoihin.

3.1.3 Sääntelyyn ja vaatimustenmukaisuuteen liittyvät haasteet toimitusketjuissa

Kyberturvallisuutta koskevat vaatimukset tiukentuvat. Tietoliikenneyritykset toimivat monimutkaisissa vaatimustenmukaisuusympäristöissä. Vaatimustenmukaisuuden varmistaminen kaikkien toimitusketjun kumppanien osalta on haastavaa mutta tärkeää jo sopimusvaiheessa, koska noudattamatta jättäminen voi johtaa merkittäviin taloudellisiin seuraamuksiin ja oikeudellisiin seurauksiin. Tämän vuoksi tietoliikenneyritysten on syytä asettaa sopimuksellisesti tiukat vaatimustenmukaisuuskehykset toimittajilleen ja valvottava systemaattisesti niiden noudattamista.

3.1.4 Lisätietoa ja linkkejä toimittajiin kohdistuvista riskeistä

EU ENISA, "Threat Landscape", October 2023, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>

EU ENISA, "Threat landscape for supply chain attacks", July 2021, <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>

SANS Institute, "What You Need To Know About the SolarWinds Supply-Chain Attack", <https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/>

Great Britain, Department for Digital, C., "UK Telecoms Supply Chain Review Report", <https://www.gov.uk/government/publications/telecoms-supply-chain-review-terms-of-reference>

NBC10 Philadelphia, "Ransomware Hits Hundreds of US Companies, Security Firm Says", <https://www.nbcphiladelphia.com/news/national-international/new-ransomware-attack-paralyzes-hundreds-of-u-s-companies/2868462/>

MOVEit Hack, "The Ransomware Attacks Explained", <https://www.kolide.com/blog/moveit-hack-the-ransomware-attacks-explained>

GitHub Security Lab, "The Octopus Scanner Malware: Attacking the open source supply chain", <https://securitylab.github.com/research/octopus-scanner-malware-open-source-supply-chain/>

Threatpost, "Mimecast Certificate Hacked in Supply-Chain Attack", <https://threatpost.com/mimecast-certificate-microsoft-supply-chain-attack/162965/>

Verkada Mass Hack, <https://ipvm.com/reports/verkada-hack>

Darkreading, "Okta Data Compromised Through Third-Party Vendor", <https://www.darkreading.com/endpoint-security/okta-employee-data-exposed-third-party-vendor>

Nasdaq, "Inside The Scam: Victims Of Ledger Hack Are Receiving Fake Hardware Wallets", <https://www.nasdaq.com/articles/inside-the-scam%3A-victims-of-ledger-hack-are-receiving-fake-hardware-wallets-2021-06-17>

3.2 Tuoteturvallisuuteen liittyvät vaatimukset toimittajille

3.2.1 Kriittiset verkkolaitteet

Privaattiverkon hankinnan vaatimusten suunnittelussa olisi hyvä pyytää Traficomilta tiedot, mitä verkon solmu-kohtia sekä verkossa olevia laitteita pidetään kansallisesti kriittisinä. Tämä kriittisten verkkolaitteiden luettelo on hyvä lähde, kun hankintaa tehdessä harkitaan, mitä turvallisuus sertifiointeja toimittajalta on syytä pyytää hankinnan yhteydessä. Operaattorin tai erillisverkon hankkijan ei pitäisi tyytyä kommentteihin, että "verkko on turvallinen, koska se on eristetty" tai "verkko on suojattu.

3.2.2 Laitteisiin liittyviä erityisvaatimuksia

Laitteet tai verkkotoiminnot eivät saisi aiheuttaa riskiä matkaviestinoperaattorille tai kansallisesti huoltovarmuus-kriittiselle erillisverkolle. ENISA korostaa, että 5G verkkolaitteiden turvallisuuteen on kiinnitettävä huomiota kaikissa toimenpiteissä (5G Toolbox vaatimus, TM02). Riittävä perustason tietoturva voidaan saavuttaa luotettavan palveluntarjoajan suorittamalla testauksella sekä auditoinnilla. Sertifioidut laitteet varmistavat turvallisuuden peruslaadun, mutta erillisen testauksen ja auditoinnin avulla saadaan varmempi kuva luotettavuudesta sekä turvallisuudesta. Ohessa on esitetty esimerkki, millaisia varmuksia voidaan hankkia verkon eri osiin suunnitelmallisesti.

5G-verkkolaitteiden turvallisuussuunnitelman luominen

Yksilöidään EU:n ENISA 5G Toolboxin TM09 ja TM10 teknisten toimenpiteiden sisältö laitteilta vaadittujen sertifiointikaavioiden perusteella.

Esimerkki:

1. Reitittimet ja kytkimet: yhteiset turvallisuus-kriteerit, EU:n yhteisten kriteerien perusteella sertifiointi (EUCC), liittovaltion tietojenkäsittelystandardi (FIPS) 140-3
2. Verkkotoiminnot: 3rd Generation Partnership Project (3GPP) Security Assurance Specification (SCAS) ja GSMA Network Equipment Security Assurance Scheme (NESAS), EU 5G Certification
3. Upotettu UICC (eUICC): GSMA NESAS -tietoturvan mukainen eUICC vaatimustenmukaisuus toimittajalta
4. Mahdolliset alueelliset sertifiointit
5. Lopuksi verkkokohtaiset kontrollitestaukset (esim. ISAE3000 standardin mukaisesti) kokonaisturvallisuusvaatimusten varmentamiseksi.

Alla olevassa kaaviossa kuvataan GSMA suosittelemia turvallisuusohjeistuksia liittyen 5G verkon eri osa-alueihin kontrollien soveltamiseen.



Kuva 1: Esittää GSMA suosittelemia turvallisuusohjeistuksia liittyen 5G verkon eri osa-alueihin kontrollien taustoiksi.

3.3 Pilvipalveluihin liittyvät vaatimukset toimittajille

3.3.1 Pilvipalvelujen tarjoajien palveluiden soveltaminen erillisverkossa

Pilvipalveluiden käyttö on 5G:n perusteknologista arkkitehtuuria. Ilman pilviratkaisuja 5G tietoliikenneverkko on vaikea saada täyttämään liiketoiminnallisia hyötyjä tai soveltumaan suunniteltujen käyttötapauksien toteuttamiseen.

Pilvipalvelujen tarjoajien on kuitenkin noudatettava EU:n säännöksiä. Käytännössä se vaatii samaa laatu- ja palvelutasoa erillisverkoissa kuin julkisissa tietoliikenneverkoissakin. Verkkoa hankkivan organisaation on syytä varmistua hankintasopimuksen tekemisen yhteydessä pilvipalvelutoimittajan tietoturvan, IT-tekniikan sekä tietoliikenteen asiantuntemuksesta.

3.3.2 Vaatimukset pilvipalvelujen toimittajalle

Hankinnoissa on varmistuttava kokonaisturvallisuudesta, jossa erityistä huomioita tulee kiinnittää seuraaviin osa-alueisiin:

- 1. Saatavuus:** Pilvipalveluntarjoajat tarjoavat erilaisia palvelumalleja. Valitun palvelusopimuksen tulisi sisältää operaattorin / huoltovarmuuskriittisten yksityisverkkoja käyttävien organisaatioiden vaatimia saatavuus- ja käytettävyyssvaatimuksia.
- 2. Raportointi:** EU:n NIS2-vaaratilanteiden raportoinnin aikatauluvaatimukset:
 1. 24 tuntia – ensimmäinen raportti (alustava kuvaus tapahtumista),
 2. 72 tuntia – toinen yksityiskohtainen raportti,
 3. 30 päivää – koko raportti.

Koska nämä määräajat koskevat kaikkea huoltovarmuus kriittistä infrastruktuuria EU:ssa, pilvipalvelujen tarjoajien on myös niitä noudatettava ja tämä on syytä varmistaa sopimuksellisesti.

On suositeltavaa, että sääntelyviranomaisen kanssa sovitaan erikseen yhteisestä käsityksestä, miten vaaratilanteiden osalta pilvipalveluntarjoajan kanssa toimitaan.

- 3. Yhteyspisteet ja välineet:** Sovitaan pilvipalvelutoimittajan kanssa selkeät yhteyspisteet ja käytettävät tiedonvaihtovälineet haavoittuvuutta ja poikkeamia koskevien tietojen saamiseksi ja vaihtamiseksi.
- 4. Haavoittuvuustietojen vaihto:** Sovitaan pilvipalvelutoimittajan kanssa haavoittuvuustietojen vaihtotapa, mukaan lukien korjaustiedoston arvioitu haittavaikutus ja arvio korjauspaketin saatavuudesta. Tämä tulisi tehdä automatisoidusti käyttämällä teollisia standardeja, jotta vältetään integraatiot ja tiedon välitys sähköpostiviestintäpostilaatikoihin, joita ei valvota 24/7.
- 5. Asiakasprosessit:** Pilvipalveluja käyttävän toimijan omat asiakkaat ovat myös veloitettuja raportimaan tietoturva uhista ja loukkauksista ja näiden vaatimukset on otettava huomioon. Pilvipalveluja käyttävien tai niitä tuottavien operaattorien, jotka toimivat huoltokriittisen yrityksen toimitusketjussa, on tuettava yritysten raportointivaatimuksia valvoville viranomaiselle
- 6. Tekniset asiakirjat:** Pilvipalvelujen tarjoajan on annettava riittävän yksityiskohtaiset tiedot käytetyistä protokollista ja työkaluista, kuten API-yksityiskohdat, MIP (Key Management Interoperability Protocol) tai julkisen avaimen salausstandardit (PKCS)#11. Hankintasopimukseen on kuvattava vaatimukset näiden käytöstä sekä laadusta.
- 7. Vaatimustenmukaisuus:** EU:ssa pilvipalvelujen tarjoajien, jotka haluavat hallinnoida julkisen operaattorin matkaviestinverkkoa, on täytettävä vaatimukset EU:n ENISA 5G Toolbox:in vaatimista toimenpiteistä, jotka liittyvät pilvipalveluihin.
- 8. Asiakkaan eristäminen:** Pilviasiakkaat on eroteltava riittävästi pilvipalvelun tuotantoinfrastruktuurissa riskiprofiilien mukaisesti. Tämä voidaan tehdä esimerkiksi ottamalla käyttöön YK:n, NCSC:n tai CISA:n ohjeet asiakkaiden erottamiseen ja eristämiseen.
- 9. Pilvipalvelun fyysinen sijainti:** On olemassa rajoituksia verkkotoiminnoilla, joita saa käyttää vain kyseisessä maassa. On suositeltavaa määrittää sopimuksellisesti, mitkä toiminnot edellyttävät sijaintiin liittyviä vaatimuksia ja yksilöidä kyseiset vaatimukset sopimuksessa.
- 10. Salausavainten hallinta:** Operaattorin pilven suojauksen salausavainten hallinta riippuu valitusta pilvipalvelumallista. Toiminnanharjoittajan on tarkistettava ja määriteltävä:
 1. Pilvipalveluntarjoajan keskeiset hallintakäytännöt (mukaan lukien tiedot säilytettävien avainten turvallisuudesta, avaintenkäytöstä, siirrettävistä avaimista, suojattujen kanavien käytöstä jne.),
 2. Käytettävissä olevat avainpituudet ja rakenne (symmetrinen/epäsymmetrinen) käyttötarkoitus (salaus/allekirjoitus), (algoritmit) missä protokollissa avaimia käytetään,
 3. Sisäiset ja API-pohjaiset aktivoinnit, joihin liittyy avainmateriaalia, mukaan lukien tekniset yksityiset kohdat, jotka vaikuttavat keskeisen materiaalin näkyvyyteen (esim. avainmateriaalin luominen, master-key-hallinta, avainten muuttaminen, päivittäminen, tallentaminen, käytöstä poistaminen, hakeminen ja tuhoaminen).

Suosittelujen asiakasavainten hallintamenettelyjen vastaanottaminen vastuunjaon mukaisesti. Operaattori on vastuussa joistakin salausavaimista, joten pilvipalveluntarjoajan olisi ilmoitettava operaattorille turvallisuuskäytännöistä (esim. tehtävien erottaminen, vähimmäisoikeudet, tallennus jne.) ja kuinka turvallisuuden osalta toteutetaan seuraavat asiat:

- Miten luvaton pääsy avainaineistoon estetään,
- Avainten elinkaaren hallinta,
- Luodaanko avaimet turvallisesti esimerkiksi NIS 800-90A:n mukaisesti,
- KMS:n fyysinen ja elektroninen suojaus,
- Miten haavoittuvuudet havaitaan ja poistetaan,
- Ovatko poistetut avaimet palautettavissa ja kuinka kauan,
- Mitä prosesseja ja vastatoimia on käytössä pahantahtoisten järjestelmänvalvojien tai muiden sisäisten uhkien havaitsemiseksi,
- Onko asiakasavaimia käsittelevät salausprosessit turvallisesti erotettu muista prosesseista,
- Onko olemassa etenemissuunnitelmaa siirtymiseksi kvanttiresistenttiin salaukseen,
- Onko pilvipalveluntarjoajan KMS-ratkaisu oma vai kolmannen osapuolen,
- Miten varmistetaan, että kolmannen osapuolen KMS on riittävän turvallinen.

11. Laitteiston suojausmoduulit: Laitteiston suojausmoduulien (HSM) käyttö erittäin arkaluonteisiin salaustoimintoihin ja huoltovarmuus kriittisten verkkotoimintojen, kuten pilviavaimenhallintajärjestelmän (KMS), tukemiseen. HSM:n on oltava FIPS 140-3 -yhteensopiva.

12. Identiteetin- ja pääsynhallinta: Pilvipalveluntarjoajan tulee noudattaa tunnettuja identiteetin- ja pääsynhallintastandardeja ja määriteltyjä turvallisuuskäytäntöjä, kuten CISA Use Secure Cloud Identity and Access Management Practices, C5, CCM tai NIST 800-192. Tämä sisältää politiikat, tehtävien erottamisen ja hallinta (admin) tai muita etukäyttöoikeuksia.

13. Turvallinen tietojen tallennus: Pilvipalveluntarjoajan tulisi noudattaa tunnettuja standardeja ja käytäntöjä tietojen tallennuksen suhteen, kuten CISA, C5 tai CCM. Riippumattomien luotettujen tahojen olisi validoitava vaatimustenmukaisuus hyödyntäen esimerkiksi ISAE3000 raportointi-standardia.

14. Katastrofipalautus: Tulee hankkia "prioriteetti" katastrofipalautukselle, eli avaintoiminnot UDM, AMF, SMF jne.

Pilvipalveluiden riskienhallinnassa voidaan hyväksikäyttää viitekehyksenä BSI:tä (Bundesamt für Sicherheit in der Informationstechnik Cloud Computing Compliance Controls Catalog (C5)), jota pilvipalvelujen tarjoajat käyttävät nykyään laajasti. C5 sisältää myös kartoitukset ISO/IEC 27017:ään, ISO/IEC 27001:een ja CSA Cloud Control Matrixiin.

Näiden lisäksi on mahdollista hyödyntää Suomessa kehitettyä ja tunnettua PiTuKria (Criteria to Assessment the Information Security of Cloud Services), jonka versio 1.1.2020 perustuu malleihin C5, ISO/IEC 27017 ja ISO/IEC 27001.

3.3.3 Lisätietoa ja linkkejä pilvipalveluihin liittyvästä turvallisuusvaatimuksista 5G verkkoihin liittyen

EU NIS2 Directive, [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2021\)689333](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333)
Cloud Security Alliance (CSA), Cloud Controls Matrix (CCM), <https://cloudsecurityalliance.org/research/cloud-controls-matrix>

EU European Union Agency for Cybersecurity (ENISA), 5G Toolbox, <https://www.enisa.europa.eu/news/enisa-news/5g>

Bundesamt fuer Sicherheit in der Informationstechnik (BSI) C5, https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html

UK National Cybersecurity Centre (NCSC), Customer separation, <https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-3-separation-between-customers>

National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), Implement Network Segmentation and Encryption in Cloud Environments, <https://media.defense.gov/2024/Mar/07/2003407861/-1/-1/0/CSI-CloudTop10-Network-Segmentation.PDF>

National Institute of Standards and Technology (NIST), Recommendation for Random Number Generation Using Deterministic Random Bit Generators, <https://csrc.nist.gov/pubs/sp/800/90/a/r1/final>

National Institute of Standards and Technology (NIST), Federal Information Processing Standard (FIPS) 140-3, <https://csrc.nist.gov/pubs/fips/140-3/final>

National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), Use Secure Cloud Identity and Access Management Practices, <https://media.defense.gov/2024/Mar/07/2003407866/-1/-1/0/CSI-Cloud-Top10-Identity-Access-Management.PDF>

National Institute of Standards and Technology (NIST), Verification and Test Methods for Access Control Policies/Models (NIST 800-192), <https://csrc.nist.gov/pubs/sp/800/192/final>

National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), Use Secure Cloud Key Management Practices <https://media.defense.gov/2024/Mar/07/2003407858/-1/-1/0/CSI-CloudTop10-Key-Management.PDF>

National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), Secure Data in the Cloud, <https://media.defense.gov/2024/Mar/07/2003407862/-1/-1/0/CSI-CloudTop10-Secure-Data.PDF>

National Security Agency (NSA), Uphold the Cloud Shared Security Model, <https://media.defense.gov/2024/Mar/07/2003407863/-1/-1/0/CSI-CLOUDTOP10-SHARED-RESPONSIBILITY-MODEL.PDF>

National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), Mitigate Risks from Managed Service Providers in Cloud Environments, <https://media.defense.gov/2024/Mar/07/2003407859/-1/-1/0/CSI-CloudTop10-Managed-Service-Providers.PDF>

EU European Union Agency for Cybersecurity (ENISA), Cloud Services Scheme EUCS, <https://certification.enisa.europa.eu/>

4 Verkon suojaaminen

4.1 Käytössä olevan verkon turvallisuus

Käytössä olevan erillisverkon turvallisuudessa on huomioitava erityisesti kontrolloitu ohjelmistokehitys sekä palvelujen kehittämisen ja tuotetestauksen laatu.

Edellä mainittujen alueiden riskienhallinnassa on huomioitava toimitusketjussa olevat toimijat, jotka voivat kehittää ohjelmistoja ja joilla on avoin pääsy testijärjestelmiin tai verkon ylläpito oikeus etäyhteyksien avulla. Edelleen riskienhallinnassa on huomioitava esimerkiksi se, että toimitusketjun toimijoilla voi olla oletusarvoiset kovakoodatut salasanat tuotteissaan tai alihankkijat eivät käytä suojausprotokollia. Tämän tyyppiset alihankkijat ovat korkean riskin toimittajia, joiden kautta voi mahdollistua onnistuneet tietoturvahyökkäykset tietoliikenneverkkoihin.

4.2 Ohjelmistokehityksen turvallisuus

Monet haavoittuvuudet johtuvat laiminlyönneistä, aikapaineesta, ohjelmiston heikosta laadusta ja riittämättömästä tietoturvaosaamisesta.

Tietoliikenteessä tyypillinen syy katkoksille johtuu ohjelmistojen epätodellisten päivitys- ja korjaustiedostoista. Vaikka tätä riskiä ei voida koskaan täysin poistaa, hyvät ohjelmistokehityskäytännöt ja ohjelmistotestaus voivat parantaa tilannetta huomattavasti. Ne tekevät tietoliikenneinfrastruktuurista kestävämmän.

Jos noudatetaan olemassa olevia kontrolliviitekehyksiä, joihin tämän ohjeistuksen kontrollisuositukset perustuvat, kehittyneitä tietoturva kokonaisarkkitehtuurissa sekä riittävää tuotetestausta, vältetään heikkolaatuisilta ja heikosti suojatuilta ohjelmistoilta sekä riskialttiilta takaporteilta. Siten ei jouduta myöskään tilanteeseen, missä testaus toteutetaan loppukäyttäjien toimesta tuotantoverkossa.

Avoimen lähdekoodin ja kolmannen osapuolen ohjelmistoriskeihin on suunniteltava kontrollit, koska toimitusketjuihin kohdistuvat hyökkäykset ovat lisääntyneet. Riskienhallinnassa on huomioitava alihankkijat, jotka voivat kehittää ohjelmistoja ja joilla on avoin pääsy testijärjestelmiin tai verkon ylläpito oikeus etäyhteyksien avulla. Edelleen riskienhallinnassa on huomioitava esimerkiksi se, että alihankkijoilla voi olla oletusarvoiset kovakoodatut salasanat tuotteissaan tai alihankkijat eivät käytä suojausprotokollia. Tämän tyyppiset alihankkijat ovat korkean riskin toimittajia, ja niiden kautta mahdollistuu onnistuneet tietoturvahyökkäykset tietoliikenneverkkoihin.

Hankintasopimuksessa ja verkon ylläpidon aikana on huolehdittava että:

1. Arkkitehtuuri- ja suunnitteluasiakirjat ovat ajantasaisia ja ne ovat saatavilla. Tähän tulisi sisältyä ajantasainen API, rajapintojen kuvaukset, protokollat sekä käytetyt algoritmit. Operaattorin ja erillisverkon asiakkaan on huolehdittava, että se saa ajantasaisesti päivitykset näistä asiakirjoista (esim. rajapintojen laajennukset).
2. Ohjelmistokehitys noudattaa tunnettuja standardeja. Jos toimittaja poikkeaa yhteisistä tunnetuista standardeista, on annettava täydelliset tiedot ja vertailu joihinkin tunnettuihin standardeihin.

Ohjelmistokehityksen turvallisuus on myös osa 5G Toolbox TM01 ja TM08 (Technical Measure).

Arkkitehtuuri-, suunnittelu- ja ohjelmistokehitysdokumenttien olisi katettava seuraavat vaatimukset:

1. Ohjelmistoprojektien turvallisuuden hallinta, joka sisältää turvallisuusasiantuntijalausunnot, palomuurisen ja pullokaulapisteiden turvallisuussuunnitelmat, turvallisuuskatsaukset ja tehtävien erottelut (tietoturvatestaus vs. kehitys)
2. Turvalliset koodauskäytännöt, kuten Carnegie Mellon, OWASP, Synopsis, OpenSSF
3. Tietoturvatestaussuunnitelmat, sisältäen koodin kattavuus, testin kattavuus, staattinen sovellusten tietoturvatestaus (SAST), dynaaminen sovellusten tietoturvatestaus (DAST), ohjelmistokomponenttien analyysi (SCA), protokolla fuzzing, kooditarkistukset, mahdollisesti riippumaton laboratoriotestaus, uusimmat tietoturvalöydöt, kuten GTPDOOR tai GSMA Roaming and Interconnect Fraud and Security (RIFS) (TEID-satunnaisuus, asiakirjanumero RIFS109_04). Testaussuunnitelmien avulla voidaan myös arvioida, onko toimittaja ajan tasalla tietoturvaasteista
4. Ohjelmiston laadunvarmistussuunnitelma ja -prosessi, mukaan lukien julkaisukriteerit
5. Turvallinen kehitysympäristö (kehitysympäristön kovettaminen)
6. Suojattu rakennusprosessi ja määrittäminen
7. Haavoittuvuusarviointi ja vahvistus kriittisten virheiden puuttumisesta testisuunnitelman kattavuuden perusteella
8. Avoimen lähdekoodin ja kolmannen osapuolen tietoturvatarkastusprosessi
9. Osallistujien tehtäväkohtainen koulutussuunnitelma

Ohjelmiston materiaaliluettelo (SBOM)

Ohjelmiston mukana tulee toimittaa yksityiskohtainen ohjelmistoluettelo (SBOM), joka sisältää ohjelmiston yksityiskohtaisen koostumuksen, jotta SBOM voidaan yhdistää CVE-rekisteriin mahdollisten piilotettujen haavoittuvuuksien tunnistamiseksi nopeasti. SBOM-muodon olisi oltava yhteisten standardien mukainen (National Telecommunications and Information Agency (NTIA) tai Telecommunication Industry Associations (TIA)) ja vaihdon olisi käytettävä standardeja, kuten CycloneDX tai Software Package Data Exchange (SPDX).

4.2.1 Lisätietoa ja linkkejä turvallisista ohjelmistokehitysvaatimuksista

National Institute of Standards and Technology (NIST), Secure Software Development Framework SSDF (NIST 800-218), <https://csrc.nist.gov/pubs/sp/800/218/final>

EU ENISA, "Cybersecurity of 5G networks EU Toolbox of risk mitigating measures - 5G Toolbox", <https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>

Cybersecurity and Infrastructure Security Agency (CISA), Securing the Software Supply Chain – Recommended Practices Guide for Developers, <https://www.cisa.gov/resources-tools/resources/securing-software-supply-chain-recommended-practices-developers>

Carnegie Mellon, University Secure Software Development Lifecycle Processes, https://insights.sei.cmu.edu/documents/430/2013_019_001_297287.pdf

OWASP, Secure Software Development Lifecycle" (SSDLC), https://owasp.org/www-project-developer-guide/draft/foundations/secure_development/

Synopsys, Secure Software Development Lifecycle Phases, <https://www.synopsys.com/blogs/software-security/secure-software-development-life-cycle-journey.html>

OpenSSF, <https://openssf.org/> (go to Technical Initiatives -> For Developers)

National Telecommunications and Information Agency (NTIA), Software Bill of Material (SBOM), <https://www.ntia.gov/page/software-bill-materials>

Telecommunication Industry Associations (TIA) Supply Chain Security Standard SCS 9001, <https://tiaonline.org/what-we-do/scs-9001-supply-chain-security-standard/>

CycloneDX, <https://cyclonedx.org/> and <https://github.com/CycloneDX> Software Package Data Exchange (SPDX), <https://spdx.dev/>

5 Verkon ylläpito ja valvonta

5.1 Verkon ylläpidon elinkaarimalli

5.1.1 Tuotteen arviointi, testaus ja elinkaaren tuki

Vaikka ohjelmistokehitysprosessi olisi turvallinen ja toimittaja testaisi ohjelmistot perusteellisesti, jokainen verkko on ainutlaatuinen arkkitehtuuriltaan ja koostumukseltaan. Tämän takia on suositeltavaa, että operaattori tai erillisverkon omistaja testaa myös itse vastaanotetut tuotteet sekä toiminnallisesti että turvallisuuden näkökulmasta.

5.1.2 Tuotteen arviointia, testausta ja elinkaaritukea koskevat vaatimukset

EU ENISA painottaa verkkolaitteiden turvallisuuden perustasoa 5G Toolbox vaatimuksessa TM02. Tähän perustason tietoturvaan saadaan varmuutta luotettavan palveluntarjoajan suorittamilla testauksilla, auditoinneilla sekä sertifiointeilla. Yleensä toimittaja antaa ohjeita toimitetun tuotteen tai korjaustiedoston toiminnan testaamisesta sen asianmukaisen toiminnan varmistamisesta verkossa. Tuotetestaus keskittyy usein toiminnalliseen osaan mutta ei tietoturvaan.

Mikäli toimittaja antaa turvallisuuden varmistamisesta tietoja, kuten 3GPP SCAS:n ja SBOM:n kuvaamasta hyvästä ohjelmistoturvallisuuden testauksesta ja kehityksestä, voidaan tuloksia arvioida helpommin. Koska testausten kattavuus voi vaihdella paljon, ne eivät välttämättä anna tarkkaa ja täydellistä kuvaa haavoittuvuudesta ja toimitetun ohjelmiston laadusta.

Hankintasopimukseen tulee sisällyttää riittävät vaatimukset, joiden laatimisessa on suositeltavaa hyödyntää tätä ohjeistusta, Traficomien ohjeistuksia sekä oman organisaation riskienhallintaa.

Toimittajien tulisi antaa tiedot suoritetuista tietoturvatesteistä ja niiden tuloksista aiemmin sovittujen testisuunnitelmien mukaisesti. Kolmannen osapuolen tekemien testien tuloksista olisi myös suositeltavaa saada tieto.

Vaadittavia tietoja ovat verkkolaitteiden ja tukiasemien, kuten valvontakameroiden, ovien lukitusten, aitojen ja turvakaappien fyysiseen turvallisuuteen liittyvät seikat, joita kuvataan EU:n ENISAn 5G Toolboxin osiossa Technical Measure TM06. Fyysiseen turvallisuuteen tulisi kiinnittää erityistä huomiota tukiasemien ja muiden fyysiselle uhalle alttiina olevien laitteiden osalta. Tällaisia ovat esimerkiksi monikäyttöiset reunalaskentakoneet (MEC).

Tuotteen testaussuunnitelman tulisi täyttää EU:n ENISAn teknisestä toimenpiteestä TM07 esitetyt vaatimukset. Niiden mukaan on varmistettava ohjelmistojen eheys siten, että ohjelmistomuutokset ja korjaustiedostojen tila tunnistetaan luotettavasti ohjelmistopäivityksiä asennettaessa ja tietoturvakorjauksia päivitettäessä 5G-privativerkkoihin.

Hankintasopimukseen tulisi sisällyttää tiedonvaihtovaatimukset. Sopimuksessa tulisi olla kuvattu suorituskäytännöt ja kuinka toimittajan tulee ylläpitää tietoturvaluokitustaan. Vaatimuksissa on oltava kuvaukset SIEM/NOC/SOC integroinneista verkkojärjestelmään, jotta eri yhteyspisteiden kautta tulevat uhat olisivat selkeämpää havaita. Näin verkon uhakuva voidaan visualisoida helpommin EU:n ENISA 5G Toolbox Technical Measure TM05:n mukaisesti.

Seuraavassa listassa on esitelty mahdollisia kohteita sisällytettäväksi tietoturvatestauksen testisuunnitelmaan:

- 1. Ohjelmistokomponenttien analyysi (SCA)** ja tulosten vertaaminen annettuun SBOMiin sen varmistamiseksi.
- 2. Vaatimustenmukaisuustestin näytteenotto:** Otetaan näytejoukko tuotteen sertifiointitesteistä (esim. 3GPP SCAS TS 33.117) ja validoidaan se ohjelmistoa vastaan sekä tehdään tarvittavia lisäauditointeja/testauksia tarpeen mukaan.

3. Yleinen tietoturvatilasto: Testin kattavuus voi sisältää:

- a) Syötteen validointi (erityisesti tunnisteiden testaus ja erikoismerkkien sisällyttäminen).
- b) Ohjelmointirajapintatila "brutal force" voimakeinot/pakotus (esim. sen testaaminen, kuinka usein ohjelmointirajapintaa voidaan kutsua erilaisilla virheellisillä IMSI-tunnuksilla)
- c) Kovakoodatut salasanat, käyttäjätunnukset, API-avaimet (käytön eliminointi).
- d) Injektiovirheiden hallinta.
- e) Tiukkojen pääsynvalvontamekanismien validointi ja niiden täytäntöönpano (EU ENISA 5G Toolbox TM03:n mukaisesti)
- f) Kommentisarjahyökkäysten hallinta.
- g) Kiistämättömyyden valvonta.
- h) Huijauksen hallinta.
- i) Virheiden käsittely ja poikkeusten hallinta (viketestaus).
- j) Käyttöoikeuksien mahdolliset korotukset ja niiden hallinta.
- k) Asetusten ohittaminen (esim. kahden lähettäjäisännän (master) lisääminen signaalintilastin suodattimien konfigurointi sekä moniosaisen MAP-tilastin välttäminen (vaatimukset, GSMA FS.19/FS.11).
- l) Lisäykset SCAS- tai vaatimustenmukaisuusmäärittäisiin sen varmistamiseksi, että toimittajan testaus toimii ajantasaisilla vaatimuksilla.
- m) Stressitila.

4. Turvallisuuden koventamisohjeistuksen saatavuus: Verkkolaitetoimittajan tulisi antaa vahvistavia tietoja operaattorille ja erillisverkon asiakkaille, miten poistetaan käytöstä tietoliikenneliitännät, joita ei käytetä tai kuinka ohjelmointirajapintoja rajoitetaan/suojataan. Tämä koskee myös IMS:ää, VoLTE:tä, ydinverkkoa ja RAN-verkkoa eikä pelkästään taustalla olevaa tietotekniikkainfrastruktuuria. Tämä on tärkeää sen estämiseksi, että hyökkääjän hallintamahdollisuudet leviävät järjestelmän sisällä tietoliikennesovellusprotokollien avulla. Verkkolaitetoimittajan on joko toimitettava todisteet mukautetusta tietoturvakovettamisesta tai annettava asiakkaalle opas niiden toteuttamiselle.

5. Tarpeettomien ominaisuuksien poistaminen: Mikäli tietoliikenneverkko perustuu segmentointiin, tulisi solmupisteiden kommunikointi toisten segmenttien elementtien kanssa sekä sovellusliittymät ja integraatorajapinnat rajoittaa vain ehdottomasti tarpeelliseen viestintään. Tämä rajoitus tulisi validoida. Näin varmistetaan, ettei IT-infrassa ole avoimia portteja ja käyttämättömiä sovelluksia. Tämä koskee enimmäkseen erillisverkkoa, joka ei hyödynnä erillisverkon täyttä toiminnallista laajuutta. Sama voi koskea myös matkapuhelinoperaattoria, joka ei halua käyttää kaikkia verkkotoimintoja.

6. Käyttöturvallisuuden validointi: Vastaanotettujen tuotteiden ja ohjelmistojen taustalla olevat tietoturvaongelmat ilmenevät tyypillisesti vasta tuotteen käyttövaiheessa. Hankintasopimukseen tulisi sisällyttää vaatimus saada toimittajalta tarvittavat pikakorjauspaketit ilmenneisiin tietoturva tai laatuongelmiin. Tuotteille, kuten signaalintalomuureille, suositellaan erillistä Pen-testingin suorittamista säännöllisesti. Tämä antaa varmuutta sekä alkuperäisen tuotetoimituksen että käyttöön otetun toiminnallisen tuotteen turvallisuudesta.

Sertifiointien, auditointien ja testauksen lisäksi hankintasopimuksessa on tärkeää varmistaa laitetilastin tuki koko elinkaaren ajan.

7. Suojauskonfigurointi: Verkosta tulee saada riittävän yksityisy dokumentaatio erityisesti suojauskonfiguraatioista ja konfiguraation vaikutuksista (esim. Kubernetes-säilöt). Jos turvatoimia ei oteta käyttöön tai testejä ei suoriteta, tämä on dokumentoitava selkeästi siten, että valintoihin johtaneet syyt ja perustelut on todettavissa dokumentaatiosta.

8. Viimeisimmät tietoturvatilat: Tietoliikennesolmujen, joita käytetään segmentointiin, kuten signaalintalomuurit, kuormituksen tasaajat ja SDN (Software Defined Network) -ohjaimet ovat kohteita, joiden turvallisuuden tilasta toimittajan tulisi raportoida säännöllisesti.

9. Pitkäaikainen tuki: Haavoittuvuustiedot ja niiden korjaukset tulisi olla saatavilla tuotteen koko käyttöajan versio päivitystenkin osalta. Toimittajan tulisi huolehtia myös sertifiointipäivityksistä. Nämä vaatimukset tulisi sisällyttää hankintasopimukseen.

10. Tulevat hyökkäykset: Tuotteesta tulisi olla kuvaus siitä, mitkä algoritmit ovat käytössä, jotta voidaan tunnistaa, käytetäänkö vanhentunutta ja heikoksi muuttunutta algoritmia. Tuotteessa tulisi olla mahdollisuus korvata heikot algoritmit vahvemmilla (mahdollisesti pidemmällä avaimilla), jotta voidaan varmistaa, että tuote on turvallinen myös odotetun elinkaarensa lopussa kvanttisalaus-hyökkäyksiä vastaan.

5.1.3 Lisätietoa ja linkkejä tuotetestausvaatimuksista

Traficom, list of critical network equipment, https://www.finlex.fi/data/normit/47015/Regulation_on_critical_parts_of_a_communications_network.pdf

EU ENISA, "Cybersecurity of 5G networks EU Toolbox of risk mitigating measures - 5G Toolbox", <https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>

National Telecommunications and Information Agency (NTIA), Software Bill of Material (SBOM), <https://www.ntia.gov/page/software-bill-materials>

Telecommunication Industry Associations (TIA) Supply Chain Security Standard SCS 9001, <https://tiaonline.org/what-we-do/scs-9001-supply-chain-security-standard/>

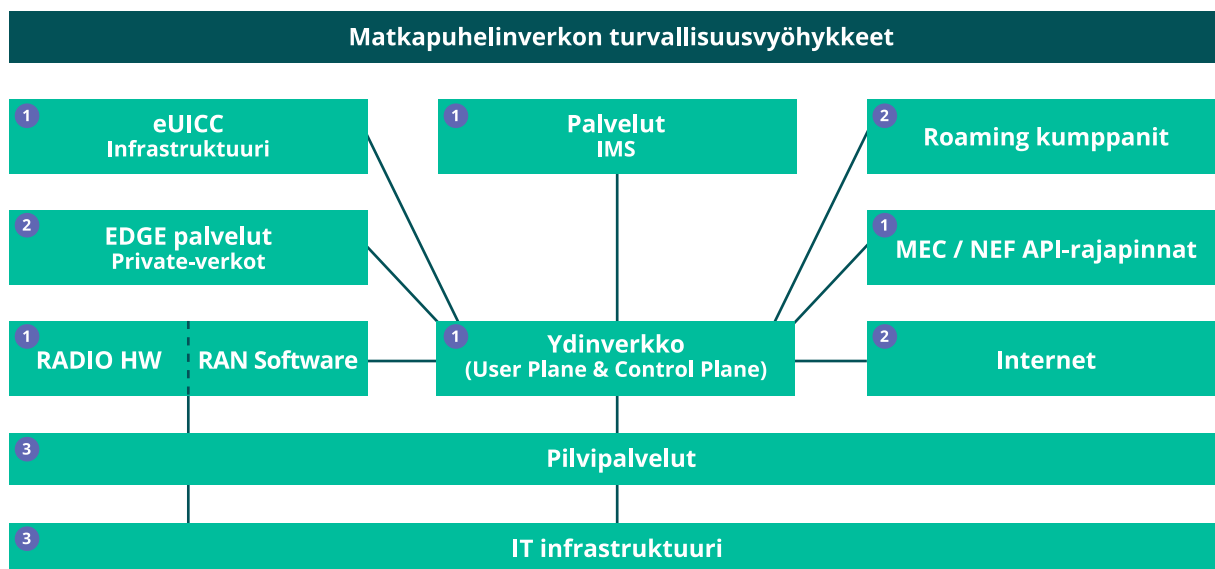
UK National Cybersecurity Centre (NCSC), Vendor assessment, <https://www.ncsc.gov.uk/report/vendor-security-assessment>

UK National Cybersecurity Centre (NCSC), Pentesting, <https://www.ncsc.gov.uk/guidance/penetration-testing>

5.2 Verkon hallinta, valvonta sekä turvallisuuden kehittäminen

Mobiiliverkko voidaan jakaa turvavyöhykkeiden, uhkaprofiilileiden sekä verkossa käytettyjen tekniikoiden perusteella. Poikkeamien seuranta tapahtuu kyseisen profiilivyöhykkeen reunoilla. Vaikka Yhdysvaltain valtiollisen standardointilaitoksen NIST SP 800-207:n määrittelemä Zero Trust -arkkitehtuuri (ZTA) olisi hyödyllinen mobiiliverkon pitkäaikaiselle kehitykselle, sen soveltaminen matkaverkkoihin tulee viemään aikaa. Parhailtaan näemme seuraavien teknisten osien kehittyvän. Jatkossa ne voivat olla turvavyöhykkeiden perusta. Joitakin näiden alueiden profiilirajoja valvotaan huolellisesti, toisia ei useinkaan valvota lainkaan.

1. IT-infrastruktuuri on yleisesti operaattorin omistuksessa.
2. Pilvi-infrastruktuuri perustuu usein yksityiseen pilveen, mutta on olemassa myös hybridipilviä.
3. Verkkovierailuyhteys ja kansainvälisen tietoliikenteen solmupisteet muodostavat yhteyden kolmansiin osapuoliin.
4. Palvelut, kuten IMS, voivat muodostaa yhteyden internetiin ja verkkovierailuverkkoon.
5. Privaattiverkot ja reunalaskentapalvelimet, esimerkiksi paikallista sisältöä tai tekoälyä varten voivat olla operaattorin tai asiakkaan hallinnoimia.
6. Network Exposure Functions (NEF)- ja Multi-Access Edge Computing (MEC) -rajapinnat tarjoavat kolmansille osapuolille pääsyn esimerkiksi sijaintitietoihin.
7. Ydinverkon ohjaus- ja käyttäjätaso ovat yleensä operaattorin hallinnassa.
8. eUICC-infrastruktuuri - SIM-kortin etävalmisteluinfrastruktuuria voi hallinnoida operaattori itse tai se voidaan hankkia palveluna.
9. Radioliityntäverkot (RAN) ja runkoliityntäyhteydet RAN-verkosta ydinverkkoon ovat yleensä operaattorin valvonnassa. RAN:illa on oma erityinen laitteistonsa, mutta myös ohjelmistokomponentti, joka voidaan laittaa pilveen esimerkiksi O-RAN standardin tarjoaman integraation rajapinnan avulla.



Kuva 2: Matkapuhelinverkon turvallisuusvyöhykkeet

Edellä kuvattua karkeaa jakoa voidaan pitää hyvänä teknisenä lähestymistapana. [1] tarkoittaa infrastruktuuria, joka on yleensä operaattorin hallinnassa. [2] tarkoittaa ulkoisia osapuolia tai ulkoista verkon osaa, joka on ulkoisten osapuolten hallinnassa. [3] tarkoittaa IT-infrastruktuuria, joka on myös yleisesti operaattorin hallinnassa.

5.2.1 IT infrastruktuurin valvonta tietoliikenneverkon rakenteissa

Jokaisessa mobiiliverkossa on olemassa sen rakenteisiin liittyvä IT-infrastruktuuri. Tämä infrastruktuuri sisältää erilaisia toimintoja sekä komponentteja, kuten palvelimia, reitittäjiä, kytkimiä ja muita verkkolaitteita. Se sisältää myös ohjelmistojärjestelmiä verkkotoimintojen, asiakaslaskutuksen ja muiden tarvittavien palvelutoimintojen hallintaan. Tämän IT-infrastruktuurin avulla operaattorit voivat tarjota luotettavia ja tehokkaita televiestintäpalveluja asiakkaille. Erityisesti 5G-verkkojen osalta on tärkeää tiedostaa, että niihin liittyvä IT-infrastruktuuri ei välttämättä eroa paljoakaan normaalista yrityksen IT-infrastruktuurista ja se sisältää samoja riskejä kuin normaali IT-ympäristö.

IT infrastruktuurin ja tietoliikenneverkkoihin kohdistuvat uhat

Hyökkääjä voi tyypillisesti hyödyntää operaattorin IT-infrastruktuuria vahingon aiheuttamiseen tai tietojen anastamiseen. Vaihtoehtoisesti hyökkääjät voivat käyttää sitä siirtymäpisteinä kohti ydinverkkoa ja suuremman hyökkäyksen valmistelua. On havaittu hyökkäyksiä, jotka yhdistävät IT-tyypiset hyökkäykset tietoliikenneinfrastruktuurin protokollisiin, kuten GTPDOOR (Linux/GTP) tai MessageTap (Linux/SMS).

Tämän uhkan takia on arvioitava, tulisiko IT ja operatiivinen tietoliikenneinfrastruktuuri yhdistää tai sijoittaa rinnakkain. Ratkaisua voi perustella sillä, että 5G käyttää monia IT-protokollia ja se on riippuvainen pilvipalveluista ja palvelinten virtualisoinneista. Jotkut operaattorit ovat jo ryhtyneet osittain yhdistämään näitä kahta kokonaisuutta tai sijoittamaan ne fyysisesti lähelle toisiaan. Osa operaattoreista pyrkii siihen, että IT-yksikkö ja operatiivinen tuotanto käyttävät mahdollisuuksien mukaan samoja työkaluja esimerkiksi monitorointiin (SIEM) ja verkkoon tunkeutumisen havaitsemisjärjestelmään (IDS) verkon solmukohdissa.

IT-infrastruktuurin poikkeamien valvontakohteet

Operaattorit valvovat usein alla listattuja tapahtumia ja IT-infrastruktuurin osia. Näitä valvontatoimia tulisi soveltuvin osin käyttää myös 5G-privaativerkkojen kontrollointiin.

Epätavalliset verkkoliikennemallit: Operaattorit voivat seurata epänormaaleja kuormapiikkejä tai pudotuksia verkkoliikenteessä sekä odottamattomia tapahtumailmiöitä, jotka poikkeavat normaaleista käyttäytymismalleista. Tämä voi olla merkki hajautetusta palvelunestohyökkäyksestä (DDoS) tai epätavallisesta verkkotoiminnasta esimerkiksi TCP Sync -hyökkäyksessä.

Luvattomat käyttöyritykset: Valvomalla epätavallisia kirjautumisyrittäjiä, kuten epäonnistuneita kirjautumisyrittäjiä tai useita kirjautumisyrittäjiä eri sijainneista, voi tunnistaa mahdolliset luvattomat käyttöyritykset tai verkkoinfrastruktuuriin kohdistuvat "brute force" raan voiman hyökkäykset.

Epätavallinen järjestelmätoiminta: Matkapuhelinoperaattorit valvovat järjestelmän epänormaalia toimintaa, kuten odottamatonta resurssien käyttöä tai palvelimilla käynnissä olevia epätavallisia prosesseja. Tämä voi auttaa havaitsemaan haittaohjelmatartunnat, luvattomat ohjelmistoasennukset tai järjestelmän vaarantumisen. Tällainen seuranta on hyödyllistä myös sen välttämiseksi, että 5G käyttää enemmän (kalliita) pilviresursseja kuin se todella tarvitsee.

Kokoonpanomuutokset: Verkkolaitetekoonpanojen odottamattomien tai luvattomien muutosten valvonta voi auttaa tunnistamaan mahdolliset tietoturvaloukkaukset tai yritykset manipuloida infrastruktuuria.

Poikkeava IT-verkon käyttäjien käyttäytyminen: Operaattorit voivat seurata epänormaalia IT-verkon käyttäjien käytöstä, kuten epätavallisen suurta datan käyttöä, liiallisia yhteyksiä tai epätavallisia tietojen käyttötapoja, epätavallisia sijaintimalleja tai käyttöaikoja. Tämä voi auttaa tunnistamaan kiristysohjelmien tai vaarantuneiden laitteiden aiheuttamat mahdolliset uhat.

Järjestelmälokien analysointi: Järjestelmälokien analysointi epätavallisten tai epäilyttävien toimintojen varalta voi auttaa havaitsemaan poikkeavuuksia ja mahdollisia tietoturvaloukkauksia. Tämä sisältää virheiden, kirjautumisia epätavallisista paikoista tai muiden epänormaalien lokimerkintöjen seurannan.

Dynaaminen sisällön seuranta: Virtuaalikoneiden ja -säilöjen, latausten ja lokitiedostojen luomista on valvottava mahdollisten palvelunestohyökkäysten tai resurssien loppumistilanteiden tunnistamiseksi.

Ohjelmistopäivitysten valvonta: IT-infrastruktuuriin kohdistuu jatkuvasti päivityksiä, joiden asennusajan kotien ympärille, sekä ennen että jälkeen on kohdistettava erityistä valvontaa. Niiden yhteydessä voi jäädä turvallisuus aukkoja tai muita virheitä järjestelmään lisäten riskitasoja.

Valvottavat poikkeamat riippuvat aina kuitenkin yksittäisen verkon infrastruktuurista, arkkitehtuurista, toimintatavoista, riskienhallinnasta, lainsäädännöstä sekä turvallisuusvaatimuksista.

SIEM, IPS sekä IDS järjestelmät osana valvontaa

Operaattorin on oltava tietoinen verkkonsa turvallisuustilanteesta. SOC (Security Operations Center) integroidaan tai muuten yhdistetään Security Information and Event Management System (SIEM) -järjestelmään. Järjestelmä suorittaa keskitetyn kirjaamisen ja tapahtumien reaaliaikaisen analyysin. SIEM syötetään yleensä tunkeutumisen havaitsemisjärjestelmien (IDS) ja tunkeutumisenestojärjestelmien Intrusion Preventing System (IPS) tiedoilla. SIEM korreloi eri lähteistä peräisin olevat tapahtumatiedot ja muuntaa tiedot hyödyllisiksi analyysitiedoiksi. Useimmat operaattorit integroivat SIEM-järjestelmään mahdollisimman monta lähdejärjestelmää, koska sen avulla voidaan ymmärtää poikkeamatilanteet suoraan ilman erillisiä analyysityökaluja. Tällainen integraatio helpottaa myös viestintää häiriötilanteissa.

SIEM:iä käytetään myös lähdevalidointiin eli tarkistamalla esimerkiksi järjestelmien nimet, IP-osoitteet, käyttöjärjestelmät, asennetut korjaustiedostot, päivitykset ja asennetut ohjelmistot.

NOC:lla (Network Operations Center) on näkymä verkon kuormitustilanteesta. Ohjelmistojen valvonta tarkkailee hyväksymättömien ohjelmistojen asennusyrityksiä tai onnistuneita, luvattomien ohjelmistojen käyttöä tai hyväksytyjen ohjelmistojen luvattonta käyttöä.

SIEM vastaa tapahtumien asianmukaisesta kirjaamisesta rikosteknistä tutkimusta ja tarkastuksia varten. Yleisiä lokitietoja, jotka tuotetaan operaattorin IT-infrastruktuurissa, ovat:

- Suojauslokit
- Järjestelmälokit
- Sovelluslokit (katso myöhempi ohjaus ja käyttäjätaso)
- Palomuurin lokit
- Välityspalvelimen lokit
- Lokien muutokset

Lokit tallennetaan keskitetysti, aikaleimataan ja allekirjoitetaan. SIEM-järjestelmään tallennetaan usein kopio lokista sen varmistamiseksi, että lokien muutokset sekä eheys voidaan todentaa. SIEM tarvitsee myös korrelaatiomoottorin tiedot. Operaattorit voivat käyttää tietojen menetyksen estämistyökaluja (DLP) arkaluonteisten tietojen mahdollisen poiminnan havaitsemiseksi.

Fyysisten riskien hallinta

Loogisten riskien lisäksi on olemassa fyysiseen turvallisuuteen liittyviä riskejä, jotka voivat aiheuttaa riskin televiestintäinfrastruktuurille. Näiden hallitsemiseksi tulisi toteuttaa ainakin seuraavia toimenpiteitä:

- Pääsynvalvonta tulisi sijoittaa alueille, missä sijaitsee verkon fyysistä infrastruktuuria. Näiden alueiden vierailijat tulisi rekisteröidä ja heidän toimintaansa valvoa mm. valvontakameroiden tai vartijoiden avulla. Myös niiden työntekijöiden, joiden työtehtäviin verkon ylläpito ei kuulu, pääsyä esimerkiksi konesaliin tulisi kontrolloida avainten ja kulunvalvonnan avulla. Vartioimattomissa tiloissa (esim. tukiasemilla) tulisi olla murtohälyttimet ja valvontakamerat. Verkkolaitteiden fyysiseen valvonnan piiriin tulisi sisällyttää myös kolmannet osapuolet, jotka hoitavat esim. logistiikkaa, huoltoa ja siivousta.
- Verkkolaitetiloissa tulisi olla palovaroittimet, lämpöanturit ja CO₂-anturit.
- Verkkolaitetilojen veden ja kosteuden valvonta tulisi toteuttaa kosteusantureiden, lämmitys-, ilmanvaihto- ja ilmastointijärjestelmän (LVI) antureiden avulla.
- Verkkolaitetilojen fyysinen avainhallinta tulisi järjestää samoilla periaatteilla kuin looginen pääsynhallinta.
- Fyysisten yhteyksien valvonta tulisi järjestää siten, että esimerkiksi valokuitukatkokset tai uudelleenreititykset havaitaan mahdollisimman nopeasti.

Tietoturvallisuuden valvonta eri pilvipalvelumallien hyödyntämismalleissa

Tietoturvalvonnin vastuunjako pilvipalveluntarjoajan ja matkapuhelinoperaattorin välillä riippuu käytettävästä palvelumallista. Kaikissa, niin Infrastruktuuri Palveluna (IaaS), Alusta Palveluna (PaaS) tai Ohjelmisto Palveluna (SaaS) palvelumalleissa operaattorin on itse huolehdittava tietoturvasta ja valvottava sen toteutumista. Yksityiskohdat valvontatavoista riippuvat yksittäisestä palveluiden hankintasopimuksesta ja niissä sovitusta palvelusisällöistä sekä tasoista (SLA).

Tyypillisesti vastuujakomallit ovat rakenteeltaan seuraavia:

IaaS-mallissa pilvipalveluntarjoaja on vastuussa taustalla olevan infrastruktuurin turvallisuudesta, mukaan lukien datakeskusten, verkkoinfrastruktuurin ja isäntäjärjestelmien fyysinen turvallisuus. Teleoperaattori on kuitenkin vastuussa omien virtuaalikoneidensa (VM), konttinsa (= container) ja pilvi-infrastruktuurissa toimivien sovellustensa suojaamisesta. Teleoperaattori tai yksityisverkkoa operoiva yritys on vastuussa omien konttisovellustensa turvaamisesta ja konttien orkestrointialustan konfiguroinnista. Tämä kattaa järjestelmälokin valvonnan, muutosten valvonnan määrittämisen,

virtuaalikoneen / säilön elinkaaren hallinnan valvonnan ja palomuurien, konttilokien valvonnan ja muutossäilöjen kuvien valvonnan ja asianmukaisten turvatoimien toteuttamisen (muutosten valvonta) säilöissä.

PaaS-mallissa pilvipalveluntarjoaja huolehtii taustalla olevan infrastruktuurin turvallisuudesta, kuten IaaS-mallissa. Lisäksi pilvipalveluntarjoaja vastaa myös palvelualustan ja ajonaikaisen ympäristön turvallisuudesta. PaaS-mallissa, joka tarjoaa konttialustoja, kuten pilvipohjaisia konttipalveluita, kuten AWS Elastic Container Service (ECS) tai Google Kubernetes Engine (GKE), pilvipalveluntarjoaja vastaa taustalla olevan infrastruktuurin sekä konttialustan turvallisuudesta. Teleoperaattori on asiakkaana, käyttäjänä vastuussa konttialustalla käyttöön otettujen sovellustensa turvaamisesta, mukaan lukien konttilokien valvonnasta, kulunvalvonnan toteuttamisesta ja muusta valvonnasta sekä konttikuvien ja virtualisoidujen verkkotoimintojen turvallisuuden varmistamisesta. Operaattorin tulee seurata sovelluksiinsa liittyviä lokeja ja tietoturvatapahtumia, kuten ydinverkkotoiminnot, API-käyttöoikeudet jne. Vastaavasti pilvipalveluntarjoajan vastuulla on alustatason suojaus ja tietoturvan valvonta.

SaaS-mallissa pilvipalveluntarjoaja on vastuussa useimmista tietoturvakokonaisuuksista, mukaan lukien taustalla oleva infrastruktuuri, palvelualusta, säilöt ja itse sovellukset. Teleoperaattori tai yksityistä verkkoa käyttävä yritys SaaS-kuluttajana joutuu tyypillisesti luottamaan SaaS-palveluntarjoajan tarjoamiin tietoturvatoinenpiteisiin. Heillä voi kuitenkin olla esimerkiksi käyttäjien käyttöoikeuksien hallintaan ja tietosuojaan liittyviä vastuita SaaS-palvelusopimuksen sisällön mukaan.

Yksi suuri riski pilviympäristöissä on se, että sovellus voi "murtautua" ulos ympäristöstään (virtuaalikone tai kontti) vaarantaen toisen samassa infrastruktuurissa toimivan sovelluksen. Vastuu tämän tilanteen turvallisuusvalvonnasta riippuu sovellettavasta palvelumallista, ja käyttöönottotyypistä. Jopa siinä tapauksessa, että käyttöönotto tapahtuu yksityisessä pilvessä, jossa on käytössä vain tietoliikennesovelluksia, tietoturvalvonta tulee olla käytössä. Sillä vältetään yleistyvien tietoturvariskien leviämistä esimerkiksi kiristysohjelmien "hyppääminen" säilöstä toiseen aiheuttaen koko televiestintäjärjestelmän vaarantaminen.

Tyypillisiä kohteita, joita on seurattava virtuaaliomaisuuden "purkautumisen" varalta, ovat:

- **Pilvipalvelun konttioikeuksien valvonta:** Konttien valvonta sen varmistamiseksi, että säilöt eivät toimi oletusarvoisesti pääkäyttäjänä eivätkä käytä tarpeettomia käyttöoikeuksia tai asennettuja ohjelmistokomponentteja. Harkitse Kubernetes-ympäristöissä "Pod Security Policy" suojauskäytännön

määrittämistä, joka estää pod:eja suorittamasta etuoikeutettuja säilöjä.

- **Käyttöoikeuksien valvonta:** Käyttöoikeuksien valvonta vain lukusäilöjen, vain lukutiedostojärjestelmien ja minimaalisten kuvien varmistamiseksi komentojen suorittamisen estämiseksi.
 - **Tietojen ja tapahtumien seuranta:** Valvo klusteritason (Kubernetes) tietoja ja tapahtumia, jotka liittyvät konttien taltiomääritysten muuttamiseen.
 - **Prosessitoimintojen seuranta:** Valvo prosessitoimintaa (kuten odottamattomia prosesseja, jotka kutevat säilön ulkopuolella ja/tai "isännässä"), jotka saattavat viitata yritykseen paeta etuoikeutetusta säilöstä isäntään.
 - **Valvo Syscall:eja:** Valvo järjestelmäkutsujen, kuten liitoksen, odottamatonta käyttöä, joka saattaa olla merkki yrityksestä paeta etuoikeutetusta säilöstä isäntään.
 - **Valvo säilökuvien käyttöönottoa:** Valvo epäilyttävien tai tuntemattomien säilökuvien ja -toimintojen, erityisesti pääkäyttäjänä toimivien säilöjen, käyttöönottoa.
 - **Ydinmoduulien asennuksen valvonta:** Valvo sellaisten ydinmoduulien asennusta, joita voidaan käyttää väärin pakenemaan säilöjä isäntään.
- Pilviympäristössä olisi noudatettava kyberhygienian perusturvatoimia. Niiden käyttöä tulisi seurata:

- **Valvo pääkäyttäjän käyttäytymistä ja käyttöoikeuksien käyttöä:** Valvo juuritilien oikeaa käyttöä. Root-käyttäjää ei käytetä virtuaalikoneessa tai säilöissä paitsi alustuksen (sovellusasennusten) aikana, ja käyttöoikeudet poistuvat suorituksen aikaisen suorituksen päätyttyä. Säilöille tai virtuaalikoneille ei voida myöntää lisäoikeuksia niiden suorituksen aikana (esimerkiksi "ei uusia-oikeuksia" -merkintä säilössä).

- **Valvo säilöjä ja virtuaalikoneita tunnistetietojen artefaktien varalta:** Arkaluonteisia tietoja (esim. yksityisiä avaimia, kriittisiä määrittystiedostoja, tunnistetietoja) ei saa koskaan julkaista tuotanto-VM/Container-näköistiedostossa.

5.2.2 Viipaloinnin valvonta

Verkkoviipalointi on yksi teknologinen keino toteuttaa 5G-privaaattiverkkoja. Se ei kuitenkaan ole vielä laajasti käytössä Suomessa. Viipalointia käytettäessä, operaattorin on varmistettava joko itse valvomalla (IaaS ja PaaS)

tai sopivalla palvelutasosopimuksella pilvipalveluntarjoajan kanssa, että viipaleet on eristetty oikein ja niiden valvonta toimii operaattorin asettamien vaatimusten mukaisesti. Tämä estää konttien mahdollisen puhkeamisen tai vastaavat väärinkäytöstapahtumat. Viipaleiden eristämistä ei ole vielä täysin määritelty standardeissa.

Yhdysvaltain valtion virastolla CISA:lla on ohjeistus 5G-verkon viipalointiin ja GSM Associationilla (GSMA) on julkaissut spesifikaatio NR.116, jossa viipalokohdan vaatimukset on määritelty yhden verkon sisällä ja NR.113 5G-verkkovierailutapaukselle. Näissä standardeissa ei ole tällä hetkellä tarpeeksi yksityiskohtaisia ohjeita siitä, miten viipaleita tulisi seurata.

Operaattorin tulee valvoa toimittajien ja pilvipalveluntarjoajien kanssa tehtyjä palvelutasosopimuksia, siinä olevia (SLA) vaatimuksia ja varmistaa, että määritellyt asiat, kuten saatavuus, toimitetaan sopimuksessa määritetyllä tavalla. Viipalointia käyttävien kriittisten yksityisten yritysten tulisi määrittää tarvittavat eristys- ja käytettävyytiedot palvelutasosopimuksessaan.

5.2.3 Virtualisoinnin hallinta

Verkkotoimintojen virtualisointi ratkaisussa (NFV), virtualisoitu toiminnallisuus asetetaan sopivaan infrastruktuuriin, jota kutsutaan NFVI:ksi (NFV Infrastructure). Koko virtualisointia ohjaa ja hallinnoi Management and Orchestration (MANO). Mobiiliverkkotoimittajat tarjoavat MANO-järjestelmiään, ja vastaavasti pilvipalveluntarjoajilla on tarjolla laaja valikoima omia työkaluja virtualisoinnin hallintaan.

MANO:n seurannassa operaattorit voivat luottaa omiin pilvivalvontatyökaluihinsa tai hyödyntää pilvipalveluntarjoajan työkaluja valitun palvelumallin mukaan. Jokaisella suurella pilvipalveluntarjoajalla on laaja valikoima maksullisia työkaluja sekä lisäpalveluita, jotka liittyvät pilvipalvelun hallintaan ja seurantaan, esim. API:t.

ETSI:n NFV-tietoturvastandardi ei sisällä selkeitä turvallisuus määrittelyjä eikä rajoitteita pilvipalvelujen tarjoajien tarjoamien työkalujen ja palvelujen soveltamiselle. Siihen liittyvät rajaukset ja määrittelyt on tehtävä tilaajan toimesta itse.

5.2.4 Verkkovierailuyhteyksien ja kansallisen yhteyden seuranta

Televerkot eivät ole erillisiä vaan ne ovat vuorovaikutuksessa kansallisten ja kansainvälisten kumppaneidensa kanssa globaalissa verkossa. Tämä tapahtuu solmupisteiden kautta. Koska tällaiseen vuorovaikutukseen käytetyt verkot eivät tällä hetkellä tue standardinomaisia luotettavia todennusmenetelmiä ja turvallisuusvaatimuksia, operaattorit käyttävät erilaisia sovelluskerroksen

palomuuereja ja suodattimia solmupisteiden suojaamiseen. Suurin osa matkapuhelinoperaattoreiden suodattuksesta tehdään seuraavasti:

- SS7 (Signaling System No. 7) -yhteenliityntäpisteitä hyödyntävät nykyään kansallisvaltioiden valvontaorganisaatiot, kuten NSO. Valvonta tehdään yleensä GSMA FS.07:n ja FS.11:n uusimpien versioiden mukaisesti erillisessä SS7-palomuurissa tai "soveltamalla" STP-yhteyksiliikennekytkimessä. Käytännössä modifioitu STP (Signaling Transfer Point) -kytkinmenetelmä on edullinen mutta vaatimustenmukainen. Sen suodatus- ja havaitsemisnopeutta pidetään alhaisena. Nämä "muokatut" STP-kytkimet havaitsevat yleensä heikosti hyökkäyksiä.
- "Diameter interconnection"-yhteen liittämistä valvotaan 4G-yhteenliittämisen osalta GSMA FS.19:n mukaisesti ja se suoritetaan signaloivalla palomuurilla. Käyttäjä voi säätää "Diameter interconnection" rajaavaa reuna-ainetta (DEA), tätä tarkoitusta varten, mutta tietoturvalvonnan laatu yleensä kärsii ja turvaongelmat ovat samat kuin "muokatussa" STP:ssä.
- Tekstiviestiliikennettä valvotaan GSMA FS.42:n ja PRD SG.22:n mukaisesti SMS-palomuuereilla.
- GTP-U-liikennettä (GPRS Transport Protocol – user plane) valvotaan GSMA FS.37:n vaatimuksia soveltaen (ohjeistuksessa on erillinen kappale käyttäjätason valvonnasta) sekä suurten turvallisuustoimittajien kaupallisen sovellustarjonnan mukaisesti.

Operaattorit valvovat saapuvaa ja jotkut myös lähtevää liikennettä. Lähtevää liikennettä valvotaan sen havaitsemiseksi, onko hyökkääjä onnistunut ohittamaan valvonnan ja suodatuksen, mikä on valitettavan yleistä. Lisäksi valvontaa tapahtuu verkkovierailuyhteydellä (kansainvälinen) ja kansallisella yhteydellä, koska hyökkääjät hyödyntävät joskus heikommin suojattua kansallisen yhteyden rajapintaa sekä siihen kohdistuvaa heikompaa valvontaa.

Syy, miksi 5G-signalointipalomuuereja ei ole käytössä johtuu siitä, että kaupallisia 5G-verkkovierailuyhteyksiä ei ole vielä paljon toteutettuna. Kun GSMA FS.36:ta käytetään laajalti, tulee GSMA FS.36:n käytettävän palomuurisääntöihin ja liikenteen valvontaan 3GPP-yhteensovivassa Security Edge Protection Proxy (SEPP) -välityspalvelimessa uusia vaatimuksia ja toiminnallisuuksia.

Edellä mainittujen protokollien lisäksi on olemassa verkkoliikenne seurantaa ja suodatusta seuraavasti:

- GSMA FS.38:n mukainen SIP-protokolla (Session Initiation Protocol), joka liittyy IP Multimedia Subsystem (IMS) -verkkovierailuun.
- GTP-C-liikennettä (GPRS Transport Protocol – ohjaustaso) valvotaan GSMA FS.20:n mukaisesti istuntokaappausten ja siihen liittyvien tietojen anastushyökkäysten estämiseksi.

Vaikka näiden kahden protokollan suodattimia ei käytetä kovin yleisesti, niitä ei pidä unohtaa. Yleensä, kun hyökkääjät epäonnistuvat helpommassa kohteessa lisääntyneen turvallisuuden vuoksi, he kääntyvät muihin protokolliin ja lähestymistapoihin yrityksissään. Siksi nämä protokollat olisi pidettävä myös aktiivisesti mukana riskienhallinnan suunnitellussa.

Televiestinnässä monet hyökkäykset tulevat liikekumppaneiden kautta (esim. tekstiviestipalvelujen tarjoajat, tukkuasiakkaat), jotka vuokraavat pääsystä epäluotettaville osapuolille. Roamingin merkinantopalomuurien lisäksi jotkut operaattorit harkitsevat nyt palvelusopimuksiin sisällytettäviä uusien vaatimuksia koskien verkkovierailuja, joita kumppaneiden on noudatettava. GSMA:n FS.52 GT (Global Title) Leasing Guide -opasta suositellaan kumppaneiden parempaan turvallisuusvalvontaan. Teknisestä näkökulmasta SLA-sopimuslausekkeen turvallisuusvaatimusten noudattamista tulisi valvoa rajapinnassa, jossa sijaitsee yhteysliikenteen signalointipalomuuri.

5.2.5 Puhelupalvelujen, erillisverkkojen ja reunalaskennan valvonta

Matkapuhelinoperaattorit, laitetoimittajat tai niiden kumppanit tarjoavat puhelu-, data- ja multimedialpalveluja kriittisillä sektoreilla toimiville yrityksille. Markkinoille on tullut myös toimijoita, jotka ylläpitävät erillisverkkoja palveluna sekä tarjoavat verkon sisäisiä tietotai reunalaskennan palveluita. Nämä ovat yleensä ei-julkisia, hyvin erityisiä B2B-järjestelyjä ja niistä on saatavilla rajoitetusti tietoa, kuinka niissä esimerkiksi suoritetaan reunalaskenta. Tässä luvussa on yleiskatsaus siitä, mitä teknisiä lähestymistapoja näihin toteutuksiin voitaisiin valvonnan osalta soveltaa.

PBX (Private Branch Exchange) on puhelinjärjestelmä, jota käytetään organisaatiossa sisäisten ja ulkoisten puheluiden hallintaan. Sitä käytetään tyypillisesti ääniviestintään yksityisessä verkossa, jolloin käyttäjät voivat soittaa ja vastaanottaa puheluita organisaation sisällä. PBX-järjestelmät perustuivat perinteisesti "circuit-switch" tekniikoihin, ja niitä käytettiin pääasiassa puheviestintään.

IMS-järjestelmä (IP Multimedia Subsystem) puolestaan on arkkitehtoninen kehys, joka mahdollistaa multimedialpalvelujen tarjoamisen IP-verkkojen kautta. Se on suunniteltu tarjoamaan alustana joustavia ja skaalautuvia multimedialpalveluita, kuten äänen, videon, multimedialviestien välittämiseen. IMS perustuu IP-pohjaisiin protokolliin ja se tukee erilaisten viestintäteknologioiden ja -palvelujen integrointia. Jotkut yritykset käyttävät IMS:ää ja yksityisiä verkkoja korvaamaan kiinteän puhelininfrastruktuurinsa.

Perinteiset PBX-järjestelmät toimivat itsenäisesti organisaation sisällä, hallitsivat sisäisiä äänipuheluita ja muodostivat yhteyden yleiseen puhelinverkkoon (PSTN) ulkoisia puheluita varten. IP-pohjaisen viestinnän mukana PBX-järjestelmät mahdollistavat laajemmat järjestelmäintegraatiot IP-tekniikkaa hyödyntäen. Nämä IP-PBX-järjestelmät voisivat hyödyntää IMS-arkkitehtuuria parantaakseen palveluominaisuuksiaan ja tarjotakseen äänen lisäksi muita multimedialpalveluja.

PBX:lle ei ole olemassa standardia, jossa olisi valvonta huomioituna. PBX:n valvontaan tulisi hyödyntää seuraavia menetelmiä:

CDR (Call Detail Record) -analyysi: PBX-järjestelmän luomien puhelutietotietueiden valvonta ja analysointi voi auttaa tunnistamaan epäilyttäviä tai luvottomat puhelutoiminnot. Tähän sisältyy epätavallisten puheluiden käytösmallien, odottamattomien puheluiden kohteiden tai liian pitkien puheluiden kestojen valvonta, jotka voivat viitata vilpilliseen tai haitalliseen toimintaan. Lisäksi voidaan saada selville riskiksi luokiteltuihin maihin kohdistuvia määrältään poikkeavia puhelumääriä.

Tunkeutumisen havaitsemis- ja estojärjestelmät (IDS/IPS): IDS/IPS-ratkaisujen käyttöönotto voi auttaa havaitsemaan ja estämään PBX-järjestelmään kohdistuvat luvottomat käyttöyritykset tai muut haitalliset toimet. Nämä järjestelmät valvovat verkkoliikennettä, analysoivat malleja ja antavat hälytyksiä tai aktivoituvat, kun mahdollisia uhkia tai poikkeamia havaitaan.

Petosten havaitseminen: Epätavallisten tai vilpillisten puhelutoimintojen, kuten lisämaksullisen palvelunumeron väärinkäytön, tietullipetosten tai luvottoman puhelujen reitityksen, valvonta voi auttaa havaitsemaan ja ehkäisemään petollisesta toiminnasta johtuvia taloudellisia menetyksiä. Tämä voidaan saavuttaa reaaliaikaisella seurannalla, kuvioanalyysillä ja sääntöihin perustuvilla havaitsemismekanismeilla.

Kulunvalvonta ja todennus: Tehokkaiden pääsynhallintatoimenpiteiden, kuten suojatun käyttäjän todennuksen ja salasanaikäytäntöjen, käyttöönotto voi auttaa estämään luvottoman pääsyn PBX-järjestelmään.

Käyttölokien seuranta ja käyttäjien toiminnan valvonta voivat myös auttaa tunnistamaan ja tutkimaan epäilyttäviä kirjautumisyrittäjiä tai luvattonta käyttöä.

Järjestelmälokianalyysi: Jotkin PBX-järjestelmät tarjoavat automaattisia ja helppoja tapoja luoda järjestelmälokeja. PBX-järjestelmän luomien järjestelmälokien seuranta ja analysointi voi antaa tietoa mahdollisista tietoturvahäiriöistä tai poikkeamista. Tähän sisältyy epätavallisten järjestelmätapahutumien, virheiden, epäonnistuneiden kirjautumisyrittysten tai luvattomien kokoonpanomuutosten valvonta. Mainittujen tapahtumien valvonta on suositeltavaa, koska ne voivat viitata tietoturvaloukkauksiin tai PBX-järjestelmän manipulointiryhtymisiin.

IMS:n ja SIP:n valvonnassa vertailukohdaksi voidaan ottaa GSMA FS.38 (ei-julkinen) – standardi. SIP-seuranta perustuu käytännössä usein petosten estämiseen, koska joissakin petosskenaarioissa käytetään IMS/SIP:tä.

5.2.6 Euroopan telealan standardointilaitos (ETSI) Multi-Access Edge Computing (MEC)

Euroopan telealan standardointilaitos (ETSI) Multi-Access Edge Computing (MEC) keskittyy laskenta- ja tallennusresurssien mahdollistamiseen verkon reunalla, lähempänä loppukäyttäjiä ja laitteita. Tuomalla nämä resurssit lähemmäs verkon reunaan, vähenee verkkoviive ja paranee sovellusten ja palveluiden yleinen suorituskyky. ETSI MEC pyrkii integroimaan reunalaskenta-ominaisuudet saumattomasti olemassa oleviin tietoliikenneverkkoihin, sisältäen 4G-, 5G-, Wi-Fi- ja kiinteät verkot. Se hyödyntää verkkotoimintojen virtualisointia (NFV) ja ohjelmisto-ohjattua verkkoa (SDN) luodakseen joustavan ja skaalautuvan reunalaskentaympäristön. Seurannan kannalta on tärkeää huomata, että ETSI MEC määrittelee joukon avoimia sovellusrajapintoja ja standardeja, jotka mahdollistavat sovellusten yhteen toimivuuden ja saumattoman integroinnin reunalaskenta-infrastruktuuriin. Näiden ohjelmointirajapintojen avulla sovellukset voivat hyödyntää reunalaskentaresursseja, käyttää reaaliaikaisia verkkotietoja sekä hyödyntää kontekstittietoisia ominaisuuksia.

Nämä rajapinnat on todennettava ja niiden käyttö on erikseen sallittava. Yleensä OAuth:ia käytetään näiden toimintojen valtuutukseen. Näitä MEC-sovellusliittymiä ei vielä käytetä laajalti, mutta standardoitujen sovellusrajapintojen käytössä on kasvua yritysasiakkaiden osalta. Valvottavat kohteet ovat samat molemmissa MEC- ja NEF-tapauksissa (katso lisätietoja seuraavasta osasta).

MEC API -rajapintavalvonta: Kun nämä sovellusliittymät otetaan käyttöön ja asetetaan ulkoisten osapuolten saataville, valvonta perustuu tunnettuihin alan standardeihin perustuviin tapoihin, kuten OWASP API -suojausohjeisiin yhdistettynä sovelluskohtaisiin

suodattimiin (esim. sallitut IMSI-alueet jne.). API:n käyttöoikeuksien myöntäminen on valvottava tarkasti, koska nykyiset ETSIn MEC-spesifikaatiot eivät ole kovin yksityiskohtaisia soveltuville valtuutustunnuksille ja tässä yhteydessä on olemassa riskejä.

5.2.7 Network Exposure Function (NEF)

NEF on varsin tehokas joukko sovellusrajapintoja matkaviestinverkkotietojen välittämiseksi kolmansille osapuolille. Sen avulla valtuutetut kolmannen osapuolen sovellukset ja palvelut voivat hyödyntää saatavia tietoja, järjestää verkkopalveluja, hallita tilaajatietoja ja mahdollistaa turvallisen vuorovaikutuksen mobiiliverkkoinfrastruktuurin kanssa. Jos sitä ei valvota tarkasti, se voi johtaa vakavaan asiakastietojen (esim. paikkatietojen) anastukseen, liikenteen uudelleenohjaukseen tai muihin hyökkäyksiin.

NEF API -seuranta

NEF-sovellusrajapinnan ominaisuuksia:

Pääsy verkkotietoihin: NEF tarjoaa valtuutetuille kolmannen osapuolen sovelluksille ja palveluille pääsyn tiettyihin verkkotietoihin. Tämä voi sisältää tietoja tilaajista, laitteista, verkon kattavuudesta, palvelun laadusta (QoS), verkkotoiminnoista ja muista asiaankuuluvista tiedoista.

Palvelun orkestrointi: NEF helpottaa palvelun orkestrointia sallimalla valtuutettujen sovellusten pyyntä ja hallita verkkopalveluja loppukäyttäjien puolesta. Tämä sisältää ominaisuuksia, kuten istunnon luomisen, käytäntöjen täytäntöönpanon, kaistanleveyden jakamisen ja muut verkkoon liittyvät toiminnot.

Tilaajatietojen hallinta: NEF tarjoaa tilaajatietojen hallintaominaisuuksia, joiden avulla valtuutetut sovellukset voivat käyttää ja hallita tilaajiin liittyviä tietoja. Tämä sisältää palvelut, kuten tilaajan todennuksen, valtuutuksen ja identiteetin hallinnan. Tarjoamalla valvotun pääsyn tilaajatietoihin NEF mahdollistaa henkilökohtaiset ja kontekstittieoiset palvelut, kuten vaikka tilausvideot urheilustadionilla.

NEF on vastuussa sen varmistamisesta, että vain valtuutetut sovellukset ja palvelut voivat käyttää verkko-resursseja ja tietoja. Se valvoo todennus- ja valtuutusmekanismeja ulkoisten yksiköiden identiteetti- ja käyttöoikeuksien tarkistamiseksi. NEF käyttää OAuth-pohjaista Common API Framework for 3rd Generation Partnership Project (3GPP) northbound APIs (CAPIF) -mallia. Tässä yhteydessä NEF vastaa myös seurannasta, mutta ETSI tai 3GPP eivät määrittele tarkkoja yksityiskohtia. Vaikka NEF:n julkisia käyttöönottoja ei ole vielä paljon, on suositeltavaa, että valvonnassa noudatetaan OWASP API Security -ohjeita.

Tärkeimmät seurattavat asiat:

Rikkinäinen/huonosti suojattu objektitason

valtuutus: Tämä tapahtuu, kun hyökkääjä pystyy käyttämään objekteja, joita hänen ei pitäisi pystyä käyttämään. Tämä voi johtua heikosta käyttöoikeuksien hallinnasta tai liian hienojakoisista valtuutustunnuksista.

Rikkinäinen/huonosti toteutettu todennus: Tämä aiheutuu todennusmekanismien puutteista, joiden avulla hyökkääjät voivat arvata käyttäjätunnustietoja sekä jaettuja tunnistetietoja API-käyttöä varten.

Liiallinen tietojen jakaminen: API:t paljastavat usein enemmän tietoja kuin on tarpeen, luottaen siihen, että niitä hyödyntävät asiakkaat suodattavat niistä pois tarpeettomat tiedot. Tämä voi johtaa arkaluonteisten tietojen paljastumiseen. Jos NEF API ei esimerkiksi ole räätälöity asiakkaalle, se antaa liikaa pääsyoikeuksia tietoihin. Vaikka EU:n puhelinoperaattorit suorittavat IT-järjestelmäkovennuksia, eli sulkevat tarpeettomia portteja ja poistavat käyttämättömiä ominaisuuksia, sitä ei ole vielä sovellettu televiestintäprotokollien ja -liitännöiden osalle.

Resurssien puute ja nopeuden rajoittuminen: Tämä viittaa API-kutsujen määrän rajoitusten puuttumiseen, mikä voi johtaa palvelunestohyökkäyksiin ja resurssien ehtymiseen. Hyökkääjä voi esimerkiksi pakottaa IMSI-alueet NEF API:ssa ylikuormitukseen, koska ei ole olemassa nopeus- ja kuormitusrajoitusta.

Rikkinäinen/huonosti toteutettu toimintotason

valtuutus: Näin tapahtuu, kun hyökkääjät voivat käyttää sovellusrajapintoja tai suorittaa rajoituksetta toimintoja virheellisten valtuutustarkistusten vuoksi. Tästä yksi esimerkki on IMSI-spesifisen valtuutuksen puuttuminen NEF:ssä.

Joukkomääritys: Tämä haavoittuvuus ilmenee, kun asiakkaiden (kuten JSON:n) antamat tiedot on sidottu suoraan malliin, jolloin hyökkääjät voivat mahdollisesti muokata objektin ominaisuuksia, joihin heillä ei pitäisi olla valtuuksia.

Suojausmääritys: Tämä sisältää laajan valikoiman ongelmia, jotka johtuvat suojaamattomista [default] oletusmäärityksistä, puutteellisista määrityksistä ja väärin määritetyistä HTTP-otsikoista.

Injektio: Tämä kattaa erilaiset injektiohyökkäykset, joissa tulkkille lähetetään epäluotettavia tietoja. Koska NEF-ohjelmointirajapintaa voi käyttää useampi kuin yksi yritysasiakas, yksi asiakas voi mahdollisesti pyrkiä käyttämään toisen asiakkaan tietoja.

Resurssien hallinta: Tähän liittyy API-versioiden asianmukaisen dokumentoinnin ja hallinnan puute, mikä

johtaa vanhojen, vanhentuneiden tai korjaamattomien API-päätepidesteiden paljastumiseen. Vaikka ohjelmointirajapinnat ovat standardoituja, on vielä monia asioita, joissa toimittaja voi toteuttaa oman soveltamistavan ja laajennuksensa vapaasti rajapinnassa. Toimittajan tulisi dokumentoida, kaikki laajennukset asianmukaisesti ja asetetta ne operaattorin saataville. Joissakin kyberhyökkäyksissä näitä toimittajakohtaisia kenttiä on käytetty hyökkääjän tietojen välittämiseen.

Kirjaaminen ja valvonta: Tietoturvahäiriöiden havaitsemiseen ja niistä palautumiseen on oltava riittävät lokitus ja valvontamekanismit. Lokit ja valvontamekanismit tarvitaan häiriöiden korjaamiseen ja niistä palautumiseen. NEF on ensisijaisesti API-toiminto, ei tietoturvan valvontasolmu. Siksi on otettava huomioon, että siihen liittyviä tapahtumia valvotaan ja logi-tiedot integroidaan SIEM:iin.

5.2.8 Reunalaskenta

Reunalaskenta tarjoaa sisältöä tai palveluita lähellä verkon reunaa. Vaikka ETSI MEC on joukko standardoituja sovellusrajapintoja, jotka mahdollistavat laskennan verkonreunalla, reunalaskenta itsessään on tyypillisesti paikallinen sisältöpalvelin (esim. tuotantolaitoksella) tai paikallinen laskentapalvelu, kuten tekoälyn data-analytiikkaratkaisu. Datan ja laskentatehon tulisi sijaita lähellä todellista käyttökohdetta, jotta sitä voidaan hyödyntää pienellä verkkoviiveellä hyödyntäen paikallista tietojen tallennusta. Termiä reunalaskenta käytetään yleisesti kuvaamaan käyttäjätason liikenteen uudelleenreititystä paikalliselle palvelimelle jatkokäsittelyä varten tai paikallinen palvelin toimittaa tietoja esimerkiksi tietokantapalvelua paikallisella tehdasalueella. Tämä toteutetaan verkkoliikenne ohjauksessa, eli liikennepyyntö siepataan, tarkastetaan tarvittavan uudelleenohjauksen varalta ja liikenne ohjataan paikalliselle palvelimelle ennalta määritettyjen kriteerien perusteella.

Valvonnan näkökulmasta on varmistettava, että uudelleenohjauksen ja uudelleenohjauksen palvelimen osoitteen kriteerien eheys suojataan, jotta vältetään käyttäjien haitallinen uudelleenohjaus haittaohjelmalvelimille tai sieppaustarkoituksiin. Todentaminen ja luottamuksellisuus on varmistettava kaikkien reunalaskenta-arkkitehtuurin liittyvien kokonaisuuksien välillä.

5.2.9 Yksityisten verkkojen rajapintojen valvonta

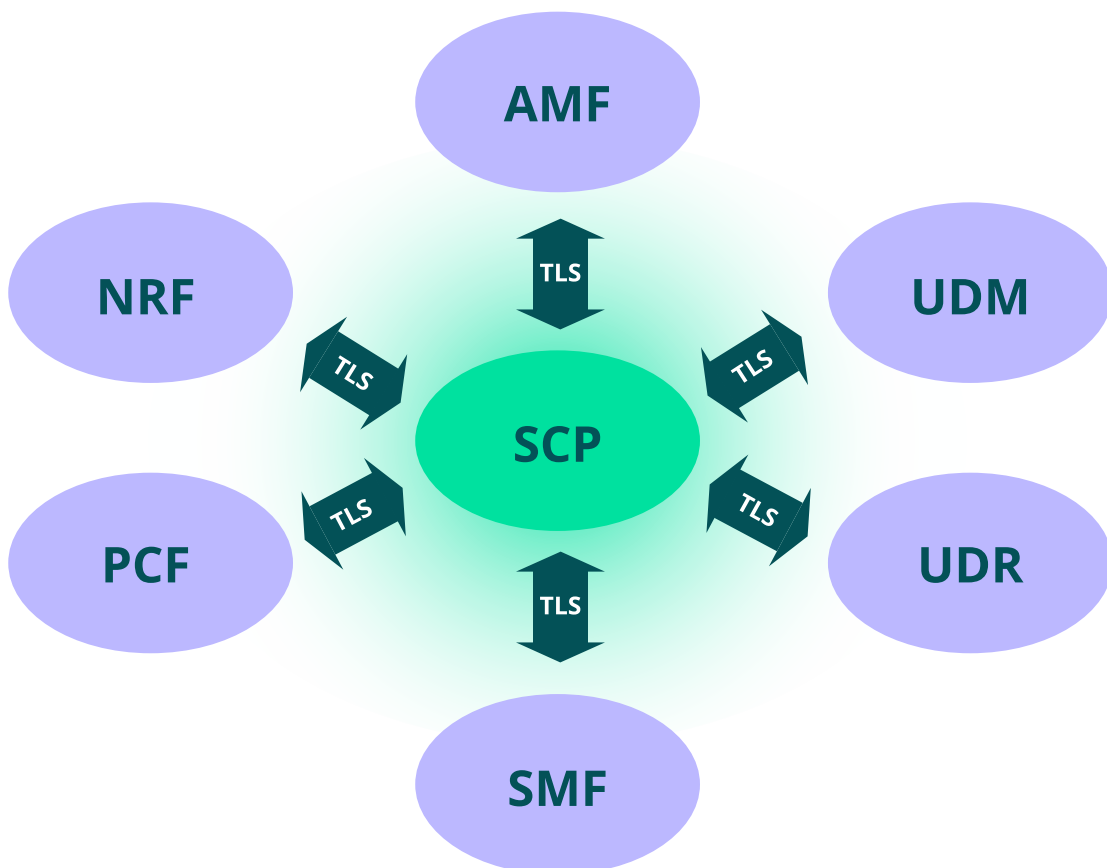
Yksityisiä verkkotyyppejä ja käyttöönottovalintoja on laaja valikoima. Useimmat yksityiset verkot ovat nykyään eristettyjä ja niillä on vain rajapinta Internetiin User Plane Function (UPF) -toiminnosta.

Netmaniasin julkaisussa esitetään seitsemän erilaista käyttöönottovaihtoehtoa yksityisille verkoille. Koska käyttöönottojen yksityiskohdat eivät yleensä ole julkisia, on oletettava, että ainakin osa niistä esiintyy markkinoilla. Valvonnan osalta ensimmäinen askel on tunnistaa rajapinnat, joissa tieto ylittää organisaatio-rajat, ja silloin sitä rajapintaa on valvottava. Yleensä voidaan käyttää uudelleen suodatusmenetelmiä ja ohjelmallisia ratkaisuja, joita käytetään NEF- ja MEC-sovellusliittymiin ja verkkovierailuun, mutta tapauksen sääntöjä on mukautettava. Jos käytetään IMS-järjestelmiä, voidaan ottaa käyttöön IMS/SIP-valvonta.

5.2.10 Ydinverkon yleinen ohjaustason valvonta

Ohjaustason valvonta on tyypillistä roaming-rajapinnoille ja niille, joissa verkkoliikenteessä organisaation rajat ylitetään (esim. privaattiverkko, NEF, MEC). Operaattorin runkoverkossa on kasvava tarve seurata kuormitusta. Tällä on suuri merkitys 5G-verkossa. 4G:ssä jokainen rajapinta piti "kytkä päälle" erikseen. 5G:ssä kaikki palvelupohjaiseen arkkitehtuuriin (SBA, service based architecture) kuuluvat verkkotoiminnot voivat kommunikoida kaikkien muiden SBA:n verkkotoimintojen kanssa. Vaarantunut tai huonosti toimiva verkkotoiminto voi siten estää koko verkon toiminnan, ylikuormittamalla kriittisiä rajapintoja.

Tätä tarkoitusta varten on olemassa Service Communication Proxy (SCP), joka määriteltiin 3rd Generation Partnership Project (3GPP) -hankkeessa. Se on SBA:n keskeinen yksikkö, eikä se voi vain suorittaa todentamiseen ja valtuutukseen liittyviä toimia, vaan SCP voi myös seurata verkon kuormitusta. Matkapuhelinoperaattorit voivat käyttää SCP:tä, sekä rinnakkain myös omaa kuormituksen valvonta- ja / tai turvallisuusratkaisuaan.



Kuva 3: Palveluviestinnän (SCP) toiminnallinen arkkitehtuuri sisältää ylläkuvatut toiminnallisuudet

Palveluviestinnän lokitietojen seurantaan tulisi sisällyttää dynaamisten toimintojen osalta ainakin tapahtumalokitiedostot ja latausten luontitiedot.

Kutsuvan linjan identiteetin (CLI) väärentämisen valvonta

Monet hyökkäykset käyttävät CLI (Calling Line Identity) -tunnistetietojen väärentämistä. Tässä hyökkäysmallissa kuluttajia huijataan paljastamaan pankkitunnuksensa, tai heidät johdetaan paljastamaan muita arkaluonteisia tietoja. CLI-huijausta käyttävät myös kansallisvaltioiden hyökkääjät. Väärennetyt viestit eivät ole vain yleinen petosriski tavallisille kuluttajille, vaan ne voivat myös tarjota onnistuneen sosiaalisen manipuloinnin polun kansallisvaltiollisille toimijoille, jotka osaavat piilottaa hyökkäyksen alkuperän, ja näiden osoittamisen syyllisiksi voi osoittautua vaikeaksi. Koska käytettävissä on laaja valikoima menetelmiä ja kansallisvaltiot käyttävät erilaisia lähestymistapoja hyökkäyksissään, niitä on haastavaa torjua.

Tällä hetkellä operaattorit Suomessa pystyvät estämään miljoonia roskapostiviestejä ja haitallisia puheluita, mutta hyökkääjät kokeilevat aina uusia tapoja ohittaa olemassa olevat suojakontrollit.

GSMA on tehnyt tutkimuksen onnistuneista teknisistä toimenpiteistä, joita eri puolilla maailmaa on käytetty (katso GSMA CLI Validiteetin parantaminen – ratkaisut ja sääntelyn arviointi).

Liikenne- ja viestintävirasto Traficom hyväksyi 16.5.2022 päivitetyn version määräyksestään 28. Se asettaa teleyrityksille uusia veloitteita estää soittajan tunnuksen väärentäminen ja huijauspuhelujen välittäminen vastaanottajille. Päivitetyn sääntelyn tavoitteena on estää suomalaisten puhelinnumeroiden käyttö kansainvälisessä kyberrikollisuudessa ja vähentää ulkomailta tulevien huijauspuheluiden määrää.

Käytössä on kaksi menetelmää CLI: n validointiin saapuvissa kansainvälisissä puheluisissa, joita suositellaan operaattoreiden käyttöön ja joita voidaan käyttää merkittävänä perustana puhelujen estämiselle:

- 1. Teleyritysten välisten puhelujen validointi**
- 2. Saapuvien puhelujen validointi välityspalvelimen avulla**

Nämä toimenpiteet ovat tällä hetkellä tehokkaita, mutta kuten aina, näidenkin kiertämiseen löydetään uusia tapoja. Siksi CLI-huijaussuojauksen tehokkuutta on seurattava. GSMA CLI: n voimassaoloasiakirjasta on suositeltavaa seurata päivitettäviä suojaustapoja, jotka on todettu tehokkaiksi.

5.2.11 Ydinverkon valvonta (käyttäjätaso)

5G-käyttäjätason liikenteen seuranta tapahtuu yleensä User Plane -toiminnolla (User Plane Function, UPF).

Liikenteen seuranta

UPF:n liikenteen seuranta sisältää läpikulkevan verkkoliikenteen (GTP-U-liikenteen) analysoinnin poikkeamien havaitsemiseksi. Tämä sisältää pakettivirtojen, kaistanleveyden käytön ja verkon suorituskykymittareiden seurannan. Seuraamalla liikennemalleja ja -määriä voidaan tunnistaa poikkeavuuksia, kuten äkillisiä liikennepiikkejä, epätavallisia tietomalleja, protokolliatyyppiä tai muuta odottamatonta käyttäytymistä. Tämä mahdollistaa turvallisuusuhkien tai epänormaalien verkkotoimintojen, kuten haittaohjelmien saastuttamien IoT-laitteiden, SIM-boksien jne., havaitsemisen.

Liikenteen seurantatyökalut ja -tekniikat voivat sisältää liikennevirtauspohjaisen analyysin, pakettien sieppauksen ja analyysin, tilastollisen analyysin ja reaaliaikaiset seurantapaneelit. Nämä työkalut tarjoavat näkyvyyden verkkoliikenteeseen ja auttavat tunnistamaan poikkeamat normaalista käyttäytymisestä, esimerkiksi havaitsemaan DDoS:n (hajautettu palvelunesto). Automaattisia DDoS-lieventämisyjärjestelmiä voidaan käyttää DDoS-hyökkäysten havaitsemiseen ja niihin vastaamiseen reaaliajassa ja ne voivat automaattisesti estää tai ohjata epäilyttävät liikennevirrat.

Kattava pakettitarkastus (DPI)

DPI (Deep Packet Inspection) -toimintoa käytetään UPF:ssä verkkopakettien sisällön tarkastamiseen karkealla tasolla. DPI:n käytännön käyttö riippuu suuresti yksittäisestä odotetusta suorituskyvystä, vaikutuksesta ja uhkatilanteesta. Liikenteen seuranta DPI:n avulla voidaan käyttää eri tasoilla ja siten suorituskykyvaikutuksia voidaan hallita. DPI mahdollistaa pakettien otsikoiden ja hyötykuorman sisällön tutkimisen, jotta saadaan tietoa verkkoliikenteestä ja havaitaan mahdolliset tietoturva-uhat. DPI mahdollistaa haitallisen liikenteen tunnistamisen ja estämisen, verkon tunkeutumisyriyten havaitsemisen sekä luvattomien protokollien tai sovellusten tunnistamisen.

DPI:tä voidaan käyttää myös liikenteen optimointiin, liikenteen muokkaukseen, sisällön suodattamiseen tai palvelun laadun (QoS) hallintaan käytettävän sovelluksen tai protokollan perusteella. DPI sisältää erikoistuneiden DPI-moottoreiden tai -laitteiden käytön. Niillä voidaan analysoida ja käsitellä paketteja reaaliajassa. Nämä moottorit voivat käyttää sääntöpohjaista vastaavuutta, allekirjoituspohjaista analyysiä tai jopa edistyneitä koneoppimisalgoritmeja pakettien hyötykuorman mallien tai poikkeavuuksien tunnistamiseen.

Näiden valvontatekniikoiden käyttöönotto UPF:ssä auttaa varmentamaan tietoliikenneverkon käyttäjätason turvallisuutta ja eheyttä. Se mahdollistaa turvallisuusuhkien havaitsemisen ja varautumisen, varmistaa verkon optimaalisen suorituskyvyn ja parantaa tarjottujen verkkopalvelujen yleistä luotettavuutta.

Aikaisempien verkkosukupolvien tietoliikennevalvonta on hyvin samankaltaista, koska ne käyttävät myös GTP-U-protokollaa. Jotkut operaattorit suunnittelevat käyttäjätason valvonnan käyttöä lähempänä RAN-verkkoja N3-liitännän pisteessä 5G:ssä. Tällainen suodatus tehtäisiin käyttäjätasoon, käyttäjältä tai tukiasemalta tuleviin ughiin varautumiseksi.

Operaattorit käyttävät myös käyttäjän viipalointimallia, eristäen käyttäjäsegmenttejä verkossa. Tämä ei vastaa varsinaisesti verkkoteknologista todellista viipalointia. Viipalointimallia käytettäessä erotetaan käyttäjätason liikenne eri asiakkaista verkkotasolla kytkentätalun liitin pisteissä. Tällaista erottelua tulisi valvoa IT-infrastruktuurin tasolla.

5.2.12 SIM-kortin etävalmisteluinfrastruktuurin valvonta

Esineiden internet (IoT) -laitteissa, kuten autoissa, on sulautettu UICC (eUICC), jota kutsutaan yleisesti virtuaaliseksi SIM-kortiksi eli eSIMiksi. eUICC on määritettävä käytettäväksi valittujen matkapuhelinoperaattorin tietojen kanssa. Tämä soveltaminen ja määrittäminen tapahtuu SIM-kortin etähallintainfrastruktuurin kautta. SIM-kortin etähallintainfrastruktuuri lisää tietoliikennesovelluksen (USIM-profiilin) eUICC-siruun.

Jos matkapuhelinoperaattori ottaa käyttöön SIM-kortin etävalmisteluinfrastruktuurin tai käyttää SIM-korttitoimittajan palvelua, infrastruktuuria on valvottava ainakin seuraavilla osa-alueilla:

- SIM-kortin etähallintainfrastruktuurin elementtien väliset liitännät, haitallisen koodin tai tietojen lisäämisen estämiseksi,
- Etähallinnan kautta lähetettävien tietojen eheys eUICC:lle ja
- SIM-kortin etävalmistelun suojaavien tunnistetietojen suojaus.

GSMA määrittelee tietoturvastandardit SIM-kortin etäkäsitelyinfrastruktuurin sertifiointiin. Näiden sertifiointistandardien avulla voidaan määrittää luotettava kumppani, joka noudattaa GSMA Security Accreditation Scheme (SAS) for Subscription Management (SM) -järjestelmää ja tämä olisi suositeltavaa myös sisällyttää osaksi hankintasopimusta.

5.2.13 Radioliityntäverkon (RAN) ja runkoliityntäyhteyksien valvonta

Häirinnän ja väärän tukiaseman tunnistuksen valvonta voidaan toteuttaa kehittyneillä false base -asemilla. Tällaisen hyökkäyksen riskiprofiili riippuu tukiaseman maantieteellisestä sijainnista ja siksi myös valvonta toteutetaan paikallisesti.

Valvontaa toteutetaan kohdennetuilla maantieteellisillä alueilla, esimerkiksi suurlähetystöjen, sotilaskohteiden ja hallituksen keskeisten kohteiden läheisyydessä niihin kohdistuvien hyökkäysten havaitsemiseksi. Myös kriittisten privaattiverkkojen osalta vastaava valvonta on suositeltavaa.

Jos satelliittiviestintää on tarkoitus käyttää rinnakkain matkaviestinnän kanssa, GPS-tietojen häirintää tulee seurata vastaavasti, koska se voi vaikuttaa satelliittiviestinnän käyttöön. Tässä tapauksessa olisi otettava huomioon GPS:n eri vaihtoehdot.

Mobiili-runkoliityntäyhteyden (N1, N2, N3 liitännät 5G:ssä ja S1 4G:ssä) valvonta voidaan tehdä IT-infrastruktuurin tasolla eli IPSec-tunnelin ja siihen liittyvien parametrien valvonta tukiaseman, ja ydinverkon solmukohdan (AMF tai UPF) välillä. Tukiaseman ja ydinverkon välisen ohjauskoneliikenteen valvontaan ei ole saatavilla kaupallisia palomuureja, jotka olisivat tietoliikennekohtaisia. Mutta yksinkertainen PCAP-valvonta voi paljastaa, onko suojaus päällä. Tätä sovelletaan myös sen valvontaan, onko käyttäjäliikenne suojattu ilmarajapinnassa vai ei. Ilmarajapinnassa on se riski, että turva-algoritmeja ei käytetä esimerkiksi suorituskykyisistä tai väärin tukiasemien asetusten vuoksi.

6 Haavoittuvuuksien ja poikkeamien hallinta

Haavoittuvuuksien käsittely ja poikkeamien hallinta on keskeinen osa verkon toimintaa. Teleoperaattoreita ja kriittisen infrastruktuurin yrityksiä kannustetaan lisäämään laitetoimittajien ja pilvipalvelujen tarjoajien kanssa tekemiinsä hankintasopimuksiin ehtoja, jotka liittyvät haavoittuvuuksien käsittelyyn, haavoittuvuuksiin liittyviin tietoihin ja poikkeamien raportointiin. Häiriönhallintasuunnitelmassa olisi otettava huomioon mobiiliverkkoinfrastruktuuri ja toimitusketjun / toimitajan riippuvuudet.

Seuraavat kaksi standardia ovat suositeltavia haavoittuvuuksien käsittelyssä ja paljastamisessa:

- ISO/IEC 29147:2018 Tietotekniikka — Suojaustekniikat — Haavoittuvuuksien paljastaminen
- ISO/IEC 30111:2019 Tietotekniikka — Suojaustekniikat — Haavoittuvuuksien käsittelyprosessit.

Lakisäätöiden raportointivelvoitteidensa täyttämiseksi operaattorit ja yksityisten verkkojen käyttäjät voivat tarvita tietoja ja tukea toimittajilta. Tällaisen tuen olisi oltava osa toimittajien kanssa tehtäviä hankintasopimuksia, jotta varmistetaan, että ne saavat toimittajalta riittävästi tietoa ja tukevat haavoittuvuutta esimerkiksi CVSS:n kautta tehtävässä pisteytyksessä.

Automatisoituja keinoja, kuten Vulnerability Exploitability eXchange (VEX), voidaan käyttää tiedonvaihdon automatisointiin.

Jotkut tilanteet saattavat vaatia toimittajan tukea ongelman ratkaisemiseksi. Hankintasopimuksessa tulisi varmistaa toimittajan tuki häiriötilanteessa (esim. hätäkorjaukset ja asiantuntijaresurssit).

Häiriönhallintasuunnitelman testauksessa tulisi olla mukana toimittaja, joka varmentaa oikea-aikaiset toimenpiteet ja niiden tuen.

Toimenpiteet, joilla parannetaan laitteisto- ja ohjelmistovikojen sietokykyä

EU:n sääntelyviranomaiset vaativat, että verkot ovat ylikuormitusuojattuja ja että kuormitustilannetta seurataan. Operaattorit käyttävät kuormituksen tasapainotusta, jota tukee 5G:n natiivi tuki virtualisointiin. Software Designed Network (SDN) -ohjauskerros ohjaa liikennevirtoja. SDN-ohjauskerrosta voidaan käyttää tukemaan laitteistohallintaa laitteistovian havaitsemi-

seksi automaattisesti ja palauttamiseksi. Ydinverkossa Service Communication Proxy (SCP) voi auttaa kuormituksen seurannassa ja hallinnassa.

Jotkut operaattorit käyttävät omaisuudenhallintatyökalujaan tunnistaakseen laitteiston vaihtotarpeen odotetun tyypillisen käyttöiän perusteella. Hätätilanteita koskevat nopeat toimitussopimukset ovat toimenpide, jolla viallinen laitteisto voidaan korvata nopeasti.

Mobiiliverkkojen kriittisimpien resurssien vikasietopalvelimia voidaan käyttää varmistamaan saatavuus katastrofin aiheuttaman palvelimen vikaantuessa. Koska tuho voi koskea kokonaista palvelinkeskusta, pilvipalvelimien tai hajautettujen palvelimien käyttöä tulisi harkita yksilöllisen riskin mukaan. Laitevikojen osalta yhteistyö pilvipalveluntarjoajien kanssa voi olla hyvä tapa varmistaa saatavuus.

6.1 Haavoittuvuustietojen raportointi

6.1.1 Haavoittuvuustiedot

Haavoittuvuudet ovat osa ohjelmistoa. Huoltovarmuuskriittisen infrastruktuurin tarjoajalle, kuten teleoperaattorille tai kriittiselle erillisverkolle, on tärkeää saada ajan tasasta haavoittuvuusuhkatietoa pystyäkseen korjaamaan haavoittuvuuden.

6.1.2 Haavoittuvuustietojen raportointia ja korjauspäivitysten hallintaa koskevat vaatimukset

Matkapuhelinoperaattorin ja huoltovarmuuskriittisen infrastruktuuriyritysten on tärkeää pysyä ajan tasalla uusimmista haavoittuvuuksista ja niiden mahdollisesti aiheuttamista riskeistä. Nämä haavoittuvuudet voivat sisältyä:

- Standardeihin (arkkitehtuuri ja protokollat),
- Tuotteen toteutukseen (software tai laitteisto) ja
- Käytettävyyteen tai muihin toiminnallisiin (konfigurointi ja käyttöönotto).

Jos haavoittuvuus on pelkästään standardeissa, eikä implementoituna käytäntöön, se ei ole uhka. Mikäli tuotteessa on haavoittuvuus, sen korjaamisesta on toimittaja vastuussa.

Standardien haavoittuvuus: Standardien haavoittuvuuden vuoksi on suositeltavaa, että toimittaja ilmoittaa asiakkaille/käyttäjälle ongelmasta, koska toimittajat yleensä edistävät standardointia. Toimittajan on myös ilmoitettava, aikooko hän korjata ongelman standardointielimen kautta tai jollain muulla tavalla.

Tuotteiden haavoittuvuus: Toimittajan on annettava ennakoivasti tietoja käyttämiensä tuotteiden, protokollien ja työkalujen haavoittuvuuksista. Nämä tiedot olisi annettava oikea-aikaisesti määriteltyjen informointikanavien kautta. Hankintasopimuksessa on kuvattava, raportoinnin aikataulusta; raportoinnin ajoituksen on täytettävä valvojan viranomaisten vaatimukset sekä noudatettava NIS2-aikajanaa.

Haavoittuvuuden pisteytystiedot: Toimittajan toimittamiin haavoittuvuustietoihin on liitettävä CVSS:n mukainen pisteytys ja vaikutusanalyysi. Hankintasopimuksessa on määriteltävä, edellytetäänkö korkean CVSS-pistemäärän haavoittuvuudelta välitöntä ”häätäkorjausta” vai riittävät esimerkiksi 3 kuukauden korjausväli. Häätäkorjausmenettelyt on sovitettava yhteen oman organisaation toiminnan kanssa. On tiedostettava, ettei toimittajalta ole välttämättä aina kaikkia haavoittuvuustietoja heti saatavilla. Osin on myös huomioitava, ettei oma organisaatio myöskään voi tehdä joitakin päivityksiä välittömästi.

Kanava ja työkalut: Toimittajan suositellaan käyttämään standarditapoja, kuten VEX (Vulnerability Exploitability eXchange), jotta saumaton integrointi SBOM:n kanssa olisi mahdollista. VEXin käyttö mahdollistaa useiden toimittajien tietojen helpomman yhdistämisen kokonaisvaltaiseksi uhkakuvaksi sekä hallinnan korjaus-aikatauluksi.

Odotettu vaikutus ja lieventäminen: Toimittajan on annettava tietoja mahdollisen korjaustiedoston saataavuudesta ja/tai aikatauluarviosta kyseisessä kontekstissa. Jos toimittaja antaa viivästyneitä tietoja vain nimenomaisesti vasta pyydettyä, tai ei toiminta niitä lainkaan, vaikuttaa se toimittajan turvaluokitukseen sekä riskiluokitukseen jatkossa. Toimittajien tulee antaa arvio odotetusta haittavaikutuksesta, mutta oman organisaation on itse lopulta arvioitava haittavaikutuksen laajuus ja riskit toiminnalle.

Haavoittuvuustietoja ei aina kyetä tai tarvitse antaa kerralla. Ne voidaan toimittaa progressiivisesti, kun toimittaja tutkii ongelmaa ja löytää tarkemmat yksityiskohdat VEX-päivitysten avulla.

Jos matkapuhelinoperaattori tarjoaa hallittuja erillisverkkoja tai toimittaa niitä huoltovarmuuskriittisille asiakkaille, on operaattorin ilmoitettava haavoittuvuuksista kyseiselle huoltovarmuuskriittiselle asiakkaalle mahdollisimman pian.

6.1.3 Lisätietoa ja linkkejä haavoittuvuustietojen hallinnasta ja raportoinnista

Cybersecurity and Infrastructure Security Agency (CISA), Vulnerability Exploitability eXchange (VEX) – Use Cases, https://www.cisa.gov/sites/default/files/2023-01/VEX_Use_Cases_Aprill2022.pdf

Cybersecurity and Infrastructure Security Agency (CISA), Minimum Requirements for Vulnerability Exploitability eXchange (VEX), <https://www.cisa.gov/resources-tools/resources/minimum-requirements-vulnerability-exploitability-exchange-vex>

CycloneDX, <https://cyclonedx.org/>

OASIS Common Security Advisory Framework (CSAF), <https://www.oasis-open.org/committees/csaf/>

CycloneDX and VEX, <https://cyclonedx.org/capabilities/vex/>
Vaaratilanteita koskevien tietojen vaihto

6.2 Häiriötietojen raportointi

6.2.1 Häiriötietojen raportointia koskevat vaatimukset

Häiriöiden raportointi tehdään Suomessa kyberturvallisuuskeskukseen sekä mahdollisesti huoltovarmuuskriittisillä yrityksillä sekä NIS2-toimijoilla erikseen määritetyille valvovalle viranomaisille.

Toimitusketjun häiriöt voivat johtaa arvokkaiden tietojen menetykseen sekä vakaviksi häiriöiksi omassa infrastruktuurissa. Hankintasopimuksessa tulisi edellyttää poikkeamien raportointia.

Raportoinnissa tulee olla vähintään seuraavat tiedot:

1. Kehitysympäristö
2. Allekirjoitusinfrastruktuuri ja avainhallintainfrastruktuuri
3. Kolmannen osapuolen toimittajat, esim. käyttöjärjestelmät tai olennaiset avoimen lähdekoodin kirjastot
4. Todennus- ja valtuutusinfrastruktuuri
5. Loki- ja seuraintainfrastruktuuri

6. Testaus ja SBOM-infrastruktuuri
7. Muoto ja sisältökuvaus, esim. MITRE ATT&CK Enterprise Framework yhdistettynä MITRE ATT&AK 5G FiGHT- ja GSMA FS.57 MoTIF -järjestelmiin
8. Raportin kielet mm. paikallinen kieli ja englanti
9. Käytettävät työkalut, kuten STIX:n ja TAXII:n käyttö automaattiseen tapahtumatietojen vaihtoon

Raportoinnin lähestymistapa ja muoto olisi yhdenmukaistettava paikallisen CSIRT-toimijan sekä toimialaa valvovan viranomaisen kanssa.

6.2.2 Lisätietoa ja linkkejä häiriötietojen raportoinnista

Technical Guideline on Incident Reporting under the EECC, <https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc>

EU European Union Agency for Cybersecurity (ENISA), Telecom Security Incidents 2022, <https://www.enisa.europa.eu/publications/telecom-security-incident-2022> (published 2024)

EU European Union Agency for Cybersecurity (ENISA), CyClone, <https://www.enisa.europa.eu/topics/eu-cyber-crisis-and-incident-management/eu-cyclone>

EU European Union Agency for Cybersecurity (ENISA), Cybersecurity Incident Reporting and Analysis System (CIRAS), <https://ciras.enisa.europa.eu/>

MITRE ATT&CK FiGHT (for 5G), <https://fight.mitre.org/>

GSMA FS.54 Mobile Threat Intelligence Framework (MoTIF) Principles (April 2024), https://www.gsma.com/security/?post_type=resource&p=7738

MITRE ATT&CK Framework Enterprise Matrix, <https://attack.mitre.org/matrices/enterprise/>
Structured Threat Information Expression (STIX), <https://oasis-open.github.io/cti-documentation/stix/intro.html>

Trusted Automated Exchange of Intelligence Information (TAXII), <https://oasis-open.github.io/cti-documentation/taxii/intro.html>

7 Kontrollit

5G erillisverkkojen suojaaminen vaatii laajasti erityyppisiä kontrollitoimenpiteitä. Tässä luvussa on kansainvälisten ja suomalaisten vaatimusviitekehysten perusteella listattu 5G-verkkoihin liittyvät riskit (riskikuvaus) ja kuvattu niihin sopivat hallintatoimenpiteet eli kontrollit (kontrollikuvaus).

Koska eri organisaatioilla ja toimialoilla on erilaisia toimintaympäristöjä ja prosesseja, tämän ohjeistuksen kontrollikuvaukset on kirjoitettu yleisellä tasolla. Kunkin huoltovarmuuskriittisen organisaation sekä 5G-erillisverkon hankkivan yrityksen tuleekin soveltaa näitä suosituksia ja ohjeistuksia omaa riskiarvioita hyödyntäen. Riskiarvion perusteella tulee tarvittaessa lisätä myös sellaisia kontrolleja, joita tässä ohjeistuksessa ei ole. Kaikkien riskien huomioiminen ja hallinta ei ole koskaan yleisellä tasolla mahdollista ja tästäkin ohjeistuksesta voi puuttua sellaisia kontrolleja, jotka ovat jossakin tietyssä ympäristössä välttämättömiä.

5G-erillisverkon ja siihen liittyvien kontrollien käyttöön otossa on suositeltavaa käyttää riittävästi asiantuntija apua, jotta erillisverkosta saa mahdollisimman suuren liiketoiminnallisen hyödyn, halliten samalla 5G-erillisverkoille ominaiset riskit.

7.1 Verkon hankinnan kontrollit

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuulinen taho
Hankintatoimi – Turvallisuuden hallinta					
P-SM-1	Tietoturvan hallinta	Riippuvuudet toimittajista	Toimittajan tietoturva voi heikentyä ja mahdollistaa hyökkääjän pääsyn järjestelmiin	Toimittajan riippuvuuksien arviointi ja vaihtoehtoisten toimittajien listaus.	Hankintatoimi
P-SM-2	Tietoturvan hallinta	Toimittajariippuvuuden arvioinnin päivittäminen	Toimittajariippuvuudet saattavat muuttua ja mahdollistaa hyökkääjän pääsyn järjestelmiin	Kriittisiksi katsottujen palvelujen tai laitteiden hankinnat johtavat turvallisuusarvioinnin päivittämiseen. Pitkäaikaiset sopimukset on tarkistettava ja päivitettävä säännöllisesti.	Hankintatoimi
P-SM-3	Tietoturvan hallinta	Toimittajien turvallisuuspolitiikat	Heikkolaatuiset tuotteet voivat altistaa hyökkäysriskin kasvamiseen	Televiestinnän turvallisuuden tavoitemittareiden luominen hankintasopimukselle. Televiestintätuotteen tai -palvelun turvallisuuslaatua koskevan erillisprosessin luominen operatiivisten prosessien ja hankintojen välillä, sen varmistamiseksi, että televiestinnän turvallisuuden liittyviä suorituskykyindikaattoreita voidaan valvoa.	Hankinta, operatiivinen tiimi
P-SM-4	Tietoturvan hallinta	Toimittajan ja toimitusketjujen perusturvallisuuspolitiikojen validointi	Toimittajalta puuttuvat perussuojausprosessit, ja sitä voidaan käyttää sisääntulovektorina operaattoriin/erillisverkkoon kohdistuvaan hyökkäykseen	Tunnettujen tietoturvasertifikaattien ohjeistuksen noudattaminen, erityisesti ISO 27000, ISO 27011 (tietoliikenne), ISO 27017 (pilvi).	Hankintatoimi
P-SM-5	Tietoturvan hallinta	Toimittajien toimitusketjun turvallisuuden hallinta	Toimittajien alihankkijoiden turvallisuuspuutteet voivat vaarantaa kokonaisturvallisuuden mahdollistaa hyökkäykset järjestelmiin	Varmistetaan, että toimittajalla on käytössä toimitusketjun riskienhallintaprosessit ja että ne vastaavat operaattoreiden / erillisverkkosiakkaiden riskienhallintavaatimuksia.	Hankintatoimi sekä riskienhallinta

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuullinen taho
P-SM-6	Tietoturvan hallinta	Korkean riskitason toimittajan määrittelmä	Korkean riskin toimittajan epäselvä määrittelmä voi johtaa korkeampiin laitekustannuksiin tai heikosti suojattujen ohjelmistojen käyttöön	Otetaan käyttöön suojautumiselle mittareihin perustuva määrittelmä, mikä on korkean riskin toimittaja ja miten turvallisiksi luokitellut toimittajat määritellään. Tässä on otettava huomioon NIS2- tai yhteiskuntakriittiseen toimialaan/organisaatioon kohdistuvat vaatimukset, vallitseva uhkaympäristö, korkean riskin toimittajien turvavalvontakustannukset, korkean riskin toimittajien turvavalvonnan tehokkuus ja mahdollisten vaikutusten ennakointi.	Hankinnat, riskienhallinta, operatiivinen johto
P-SM-7	Tietoturvan hallinta	NIS2- tai yhteiskuntakriittisen toimialan/organisaation tunnistaminen	Organisaation vastuut NIS2:n toimialojenasiakkaille, jos tietomurto toteutuu riittämättömästi suojatun verkon kautta	Riittävän korkean turvallisuusvalvonnan varmistaminen NIS2:n yhteiskuntakriittisille/huoltovarmuuskriittisille asiakasorganisaatioille luomalla luettelo kriittisistä asiakkaista, jotka voivat käyttää laitetta tai palvelua.	Hankinta, riskienhallinta, operatiivinen palvelutuotanto, Asiakaspalvelutiimi
P-SM-8	Tietoturvan hallinta	Altistumis-ympäristö	Vastuu omille NIS2 kohderyhmä asiakkaille, jos tietomurto tapahtuu puutteellisesti suojatun verkon kautta	Mobiiliverkon riskien arviointi ottaen huomioon palveluarkkitehtuuri, huoltovarmuuskriittiset yksityisasiakkaat, esineiden internet/pilvipalvelut sekä palveluun kytketyt tuotantolaitosprosessit.	Hankinta, riskienhallinta, Palvelutuotannon operatiivinen tiimi
P-SM-9	Tietoturvan hallinta	Uhka maisema	Käytössä ei ole riittäviä turvatoimia, koska uhkaympäristöä ei tunneta	Ei teknisten riskien arviointi keräämällä tietoja Suojelupoliisilta, Traficomilta, CISA:lta, EU:sta ENISA:lta ja alaa valvovalta viranomaiselta sekä muista toimialaan liittyvistä lähteistä.	Hankinta-toimi Riskienhallinta
P-SM-10	Tietoturvan hallinta	Korkean riskin toimittajien turvallisuusvalvontakustannukset	Korkeat turvallisuus-kustannukset tehottomista turvallisuustoimista	Arvio kustannuksista, jotka aiheutuvat suuririskisen toimittajan käytön valvonnan/varautumisen korvaamisesta verrattuna muihin toimittajiin tai muihin vaihtoehtoihin.	Hankinnat, riskienhallinta

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuullinen taho
P-SM-11	Tietoturvan hallinta	Korkean riskin toimittajien turva- valvonnan tehokkuus	Korkeat turvallisuus- kustannukset tehottomista turvatoimista	Arvio korkean riskin toimit- tajan käytön valvonnan/ varautumisen kompensoinnin tehokkuudesta verrattuna muihin toimittajiin tai muihin vaihtoehtoihin.	Hankinta, riskien- hallinta, palvelu- tuotannon tiimi
P-SM-12	Tietoturvan hallinta	Korvausten valvonta- suunnitelma korkean riskin toimittajillen	Suuririskistä toimit- tajaa saatetaan käyttää ilman asianmukaisia korvaavia toimen- piteitä, mikä voi johtaa mahdolli- seen riskialtistumi- seen tietoliikenne- verkolle ja datalle	Kompensoivien kontrollien valikoiman valitseminen korkean riskitason toimitta- jalle. Tämä on tehtävä toimit- tajakohtaisesti, koska riskit vaihtelevat tarjottavien lait- teiden ja palvelujen tyyppin mukaan sekä mahdollisen käyttökohteen mukaan.	Hankinta, riskien- hallinta, palvelu- tuotannon tiimi
P-SM-13	Tietoturvan hallinta	Luettelo kriittisistä verkkolaitteista ja -elementeistä	Riittävien turvalli- suusvalvontatoimien puuttuminen kriittiseen verkkoelementtiin voi johtaa havaitse- mattomiin haavoit- tuvuuksiin tai tiuk- kojen turvallisuus- valvontatoimien soveltaminen kaik- kiin verkkoelement- teihin voi aiheuttaa tarpeettomia kustannuksia	Luettelon luominen kriitti- sistä verkkolaitteista, palve- luista ja verkkoelementeistä. Tähän olisi sisällyttävä 5G, olemassa oleva IT-infrastruk- tuuri, pilvipalvelut, verkkolait- teet ja muut palvelut (esim. Lähtökohdaksi olisi otettava Traficomin luettelo. (https:// www.finlex.fi/data/ normit/47015/Regulation_on_ critical_parts_of_a_communi- cations_network.pdf). Perus- telut laitteiden lisäämiselle tai poistamiselle kriittisten lait- teiden luetteloon/luettelosta olisi dokumentoitava esim. poistettu käytöstä, kriittisten- tietojen tallennus, vaihdettu uuteen laitteeseen jne.	Hankinta, riskien- hallinta, palvelu- tuotannon tiimi
Hankintatoimi – Laite sertifiointit/testausvaatimukset					
P-EC-1	Laitteiden sertifiointi	5G-verkko- laitteiden sertifiointi- suunnitelman laatiminen	Tietoturvan heikko suorituskyky voi johtaa laite haavoit- tuvuuksiin ja kasva- viin hyökkäyksiin	Toiminnallisten vaatimusten mukaisuuden lisäksi verkko- laitteilta vaadittujen tieto- turvasertifikaattien luominen. Tässä luettelossa olisi otettava huomioon 5G-laitteiden kriittisyys toiminnan kannalta. EU on julkaissut luettelon kriittisistä 5G-laitteista, joita voidaan pitää perustasona määritte- lylle. Kaikissa hankintatoimen vaatimuksissa (RFQ/RFP) tulee esittää laitteiden sertifiointivaatimukset.	Hankinta, operatiiv- inen palvelu- tuotanto- tiimi Alihank- kijat

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuulinen taho
P-EC-2	Laitteiden sertifiointi	Korvausperusteet sertifiointipuutteellisista verkkotoiminnoista sekä mahdollisesti päivittämättömistä ohjelmisto/laitteversioista	Tietoturvan puutteellisuus voi heikentää suorituskkyä tai johtaa haavoittuviin laitteisiin ja sitä kautta kasvattaa hyökkäysriskiä	Luettelon laatiminen hyväksyttävistä vaihtoehtoista vaatimuksista poikkeamisille, jotka johtuvat puutteellisesta sertifiointijärjestelmästä, esim. tunnetun tahon testaustulokset, vaihtoehtoinen skeema. Toimittajan tulee esittää testitulokset operaattorille / erillisverkkosiakkaalle. Tarjouspyynnössä tulee esittää, kuinka vaatimusten täyttäminen todennetaan riippumattomien toimijoiden toimesta (esim. ISAE3000 raportilla) Suunnitelma, kuinka toimitaan, mikäli käytöstä löytyy sertifioiduttomia, palvelukuvauksesta puuttuvia tai testaamattomia laitteita/ palveluita.	Hankinta, operatiivinen palvelu tuotantotiimi
P-EC-3	Laitteiden sertifiointi	Myöhästynyt sertifiointi	Operaattori ei saa käyttää sertifioidussa hyväksymättömiä/poikkeavia toimenpiteitä, tai käyttää turvallisuustasolla heikompia verkko-elementtejä jotka voivat johtaa kasvaviin tietoturvariskeihin.	Tähän liittyvien vaatimusekkeiden sisällyttäminen hankintasopimukseen, joka varmistaa, että toimittaja alihankkijoineen toimittaa sertifikaatin ajoissa. Jos tästä poiketaan, verkkoon liitettyjen laitteiden testaus/turvallisuusarviointi voidaan suorittaa toimittajan kustannuksella.	Hankinta-toimi
P-EC-4	Laitteiden sertifiointi	Palomuurin signaalointivaatimustenmukaisuus	Verkon vaarantuminen vajavaisesti toimivan signaalointipalomuurin vuoksi	Merkinantopalomuurin olisi oltava riittävän laadukas ja perustuttava GSMA-merkinantopalomuurin suositusten uusimman versioon eli (tällä hetkellä viimeisin versio) GSMA FS.07 (SS7), FS.11 (SS7), FS.19 (halkaisija), FS.20 (GTP), FS.21 (yhteyshäiriön suojaus), FS.36 (5G), FS.38 (SIP) ja FS.42 (binääriteksti- viestit). Vaatimustenmukaisuuden olisi oltava vaatimukseksi tarjouspyynnössä.	Hankinta-toimi

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuul- linen taho
P-EC-5	Laitteiden sertifiointi	eUICC- valmistelu- arkki- tehtuurin sertifiointi	SIM-kortin etäohjatun SIM sisällönhallinnan infrastruktuurin vaarantuminen voi johtaa loppukäyt- täjän päätelaitteen täydelliseen vaarantumiseen avaamalla mahdol- lisuuden asentaa haittaohjelmia pätelaitteisiin/ SIM-kortteihin.	Hankintaprosessi tulee edellyttää tarjouspyynnössä toimittajien olevan sertifioitu GSMA-SIM-etäprovisioinnin SCAS-sertifiointien mukaisesti.	Hankinta- toimi
Hankintatoimi – Pilvipalvelut					
P-C-1	Pilvi- palvelut	Saatavuus	Tietoliikenteen saatavuus/ käytettävyys ei täytä lakisääteisiä tai liiketoiminnal- lisia vaatimuksia	Hankintasopimuksen tulee sisältää tarvittava saatavuus- luokitteluvaatimuksia, joita pilvipalvelun tarjoaja tarjo- ajan tulee täyttää. Vaatimus- luokkien on mitattava operaattorin / huoltovar- muuskriittisen NIS2-erillis- verkon verkkoasiakkaan lakisääteisiä saatavuus/ laatuvaatimuksia.	Hankinta- toimi
P-C-2	Pilvi- palvelut	Poikkeama raportointi pilvi- palveluille	Kyvyttömyys noudattaa lakisääteisiä poikkeamien raportointi- velvoitteita, josta voi aiheutua sanktioita tai muita seuraamuksia.	Hankintasopimuksen olisi tuettava EU:n NIS2-turvalli- suuspoikkeamien rapor- toinnin vaatimuksia: 24 tuntia ensimmäinen raportti (ilmoitusvelvollisuus) 72 tuntia – toinen yksityiskoh- tainen raportti, 30 päivää – täydellinen raportti, jotta raportointivelvoitteet voidaan täyttää tapauksissa, joissa pilvipalvelussa on tapahtunut häiriö, jolla on vaikutuksia matkaviestinverkkoon.	Hankinta- toimi
P-C-3	Pilvi- palvelut	Yhteys- pisteet	Kyvyttömyys noudattaa lakisääteisiä poikkeamien raportointi- velvoitteita, josta voi aiheutua sanktioita tai muista seuraamuksia.	Palvelusopimuksessa on ilmoitettava selkeät yhteys- pisteet turvallisuuspoik- keamia koskevien tietojen vaihtoa varten. Sopimuksessa on mainittava kontaktien yhteistiedot sekä saatavuus (palvelumallin mukaisina aikoina sekä mahdollisesti palveluaikojen ulkopuolella).	Hankinta- toimi

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuulinen taho
P-C-4	Pilvi- palvelut	Yhteystietojen saatavuus	Kyvyyttömyys noudattaa lakisää- teisiä poikkeamien raportointivelvoiteita, josta voi aiheutua sanktioita tai muita seuraamuksia.	Palvelusopimuksessa on mainittava erikseen yhteys- henkilö häiriötietojen vaih- toon, joka voi vaikuttaa 5G-verkon toimintaan sekä yhteyshenkilön saatavuus palveluaikoina, ja niiden ulko- puolella oleva päivystys.	Hankinta- toimi
P-C-5	Pilvi- palvelut	Haavoittu- vuuksia koskevien tietojen vaihdossa käytettävät työkalut	Tietämättömyys haavoittuvuuksista voi johtaa viivästy- neeseen (rajoi- tetun) palvelun liitoksiin ja järjestelmän vaarantumiseen	Palvelusopimuksessa on kuvattava kumppanien väliseen pilvipalveluhaavoit- tuvuuksia koskevien tietojen vaihtoon käytetyt välineet ja niiden yksityiskohdat (esim. formaatit). Lisäksi jos palveluketjussa on alihankki- joita, joita tarvitaan myös niistä vastaavat tiedot.	Hankinta- toimi
P-C-6	Pilvi- palvelut	Pilvipalvelun haavoittu- vuustietojen saatavuuden ajoitus	Tietämättömyys haavoittuvuuksista voi johtaa viivästy- neeseen palvelun liitoksiin ja järjestelmän vaarantumiseen	Palvelusopimuksessa on määriteltävä tavoiteajat, jolloin pilvipalvelutarjoaja asettaa saataville pilvipal- velun haavoittuvuuksia koskevat tiedot ja kuvaukset.	Hankinta- toimi
P-C-7	Pilvi- palvelut	Pilven haavoittu- vuustietojen muoto ja korjausten tiedostojen toimituksen ajoitus	Tehoton lieventä- missuunnitelma voi johtaa järjestelmän vaarantumiseen (esim. rajoitetun tai osittain korjatun palveluliitoksen suunnitelma- toteuttaminen riippuu korjaus- tiedoston saatavuudesta, jos korjausta ei ole tulossa tai se on pahasti myöhässä)	Hankintasopimukseen on sisällytettävä kuvaus tiedoista, joita haavoittu- vuuksien osalta vaihdetaan kuvaus vaikutusten laajuus- desta sekä arvio korjaus- tiedon saatavuudesta (milloin ensimmäinen korjauserä on saatavilla). Tähän olisi oltava ensisijaisesti automatisoidut toteutustavat noudattaen alan teollisia suosituksia ja standardeja, jotta vältetään laajamittaiset korkeakustan- nukselliset järjestelmä inte- graatiot, tai epävarma sähkö- postiviestintä paikkoihin, joita ei valvota 24/7.	Hankinta- toimi Palvelu- tuotanto- tiimi
P-C-8	Pilvi- palvelut	Pilvihaavoit- tuvuudesta ja -tapahtumista tiedottaminen	Mikäli huoltovar- muuskriittiselle asiakkaalle ei viestitä ajoissa haavoittuvuuksista tai aiheutuneista tietoturvapoikkeaa- mista, aiheutuu sopimussakkoja tai yhteiskunnallisia sanktioita.	Hankintasopimuksessa on otettava huomioon tarvit- tavat asiakirjat, joita mahdol- lisesti riippuvaiset NIS2- huoltovarmuuskriittiset toimijoiden erillisverkot tarvitsevat raportoidakseen haavoittuvuuksista ja poik- keamista valvovalle viranomaisilleen.	Hankinta- toimi, viestintä, lakiasasto- asiat, Palvelu- myynti

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuullinen taho
P-C-9	Pilvipalvelut	Teknisen dokumentaation saatavuus	Teknisen tiedon puute voi johtaa väärään turvallisuuden tunteeseen ja lisätä järjestelmän turvallisuusriskeille altistumista.	Palvelusopimuksella olisi varmistettava, että pilvipalvelujen tarjoaja antaa riittävän yksityiskohtaiset tiedot käytetyistä protokollista ja välineistä. Operatiivisen ryhmän olisi annettava hankinnalle palautetta työkalujen ja protokollien turvallisuuden laadusta ja kyseisten asiakirjojen kattavuudesta, jotta riskiosasto voi arvioida asianmukaisesti tähän tuotteeseen liittyvät riskit.	Hankinta, palvelutuotantotiimi, riskiosasto
P-C-10	Pilvipalvelut	Pilvipalveluiden (5G) -yhteensopivuus	Pilvipalvelutarjoaja 5G verkoteknologiaa tukevan infrastruktuurin tietoturvan puutteellisuus voi aiheuttaa verkon käytettävyyden heikentymistä Mikäli verkko ei täytä EU:n 5G Toolbox vaatimuksia, ja näistä havaitut muutokset voivat johtaa sanktioihin.	Hankintasopimuksessa on määriteltävä pilvipalvelutarjoajan velvollisuudesta noudattaa EU:n, ENISA 5G Toolbox:in ja sen täydennyksen sekä siinä kuvattuja pilvipalveluvaatimuksia. EU ENISA 5G Toolbox ei ota kantaa liiketoiminnan jakautumiseen eli siihen, onko pilvipalvelutuotettu hybridimallilla, erillistaajuuksiverkkona vai julkisen verkon osana – se koskee kaikkia näitä vaihtoehtoja.	Hankintatoimi
P-C-11	Pilvipalvelut	Asiakasverkon eristäminen	Asiakkaan puutteellinen eristäminen pilvipalvelusta voi johtaa tietojen joutumisen ulkopuolisten käsiin sekä järjestelmän käytön vaarantumiseen.	Palvelusopimuksessa on kuvattava, kuinka pilvipalvelutarjoaja antaa tietoja siitä, miten se eristää asiakkaansa riittävästi. Tarvittavia yksityiskohtia vaatimuksesta riittävydestä sopimukseen on syytä konsultoida IT sekä lakiasioista vastaavien tahojen kanssa organisaatiossa.	Hankintatoimi, IT osasto, Riskien hallinta

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuullinen taho
P-C-12	Pilvipalvelut	Fyysinen pilvipalvelun sijainti	Väärin lakisääteisten perusteiden tulkittamisesta voi aiheutua sanktioita tai sakkoja.	On tunnistettava lakisääteiset veloitteet (B2B-asiakasliiketoiminnan palvelukuvausten ja sopimussisältöjen osalta) mahdollinen tarve (riskienhallinta vastuiden/palvelutuotantotiimin toimintamallien vaatimusten mukaisuus), jotta erillisverkko tai osa julkisesta operaattoriverkosta toimii "maassa" tai "EU:ssa". Mikäli joitakin maa rajoitteita tai palvelutuotantovaatimuksia asetettu sijainnille. Jos tällainen erityistarve on olemassa, on se huomioitava palvelusopimuksessa ja mahdollisesti eriteltävä ne palvelurakenteet tai toiminnallisuudet 5G-verkosta, joihin kohdistuu palvelutuotannon sijaintiin erityisvaatimuksia.	Hankinta-toimi Riskien hallinta, Lakiosasto Palvelu tuotantotiimi
P-C-13	Pilvipalvelut	Pilvipalveluiden salausavainten hallinta	Suojaamattomien pilvipalveluavainten hallinta voi johtaa tietojen paljastumiseen, tietojen anastamiseen sekä järjestelmän käytön vaarantumiseen	Hankintatoimen sekä palvelun tuotantotiimin on tunnistettava vastuulliset tahot, jotka huolehtivat pilvipalvelun salausavaimista. Jos pilvipalveluntarjoaja vastaa, pilvipalvelun salausavaimista, on nämä hallintavaatimukset sisällytettävä palvelusopimukseen. Jos yksityinen yritys/elinkeino-toiminnanharjoittaja vastaa avaintenhallinnasta, on sopimukseen liitettävä, että seuraavat toimenpiteet täytetään: <ul style="list-style-type: none"> - Keskeiset johtamispoliittikat määritelty - Käytettävissä olevat avainhallintapolitiikat/ avainvaatimukset - Sisäisen avainmateriaalin kuvaustenhallinta sekä API-pohjainen hallinnan aktivointisuojauksen toteutuskuvaus 	Hankinta-toimi Palvelu-tuotantotiimi

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuul- linen taho
P-C-14	Pilvi- palvelut	Laitteiden/ laitteisiin liittyvien rajapintojen suojaus- moduulien käyttö	Palvelinjuuren turvallisuuteen, eheyteen ja luotta- muksellisuuteen liittyvien riskien tunnistaminen, mikä voi johtaa koko järjestelmän käytön vaarantu- misen sekä luoda mahdollisuuden toisena henkilönä esiintymiseen, tietojen anasta- misen, tietojen menetykseen tai mahdollisen tietojen väärännöksen.	Vastuunjaon mukaan hankin- tatoimen on varmistettava sopimuksellisesti, että pilvi- palveluntarjoaja käyttää turvallisia laitteiston suojaus- moduuleja tärkeimpiin tieto- turvatoimintoihin ja tallennuk- seen. Mikäli asia on operatii- visen palvelutuotantotiimin vastuulla, on oltava käytössä todisteet HSM-moduulin käytöstä arkaluonteisissa turvallisuustoiminnoissa avaintenhallintakäytäntöjen mukaisesti. Operaattori/erillis- verkkoyhtiö saattaa yrittää rajoittaa pilvipalveluntarjo- ajan HSM-moduulin käytön vain itselleen. Mikäli HSM- moduuli ei ole saatavilla, on pilvipalveluntarjoajan annet- tava tiedot siitä, miten HSM-moduulissa asiointi on suojattu (esim. miten erillinen järjestelmänvalvojan pääsy, oma dataosio, käyttöoikeuk- sien on turvattu ja valvonta/ lokitus toteutettu ja mitä tietoturvakäytäntöjä noudate- taan). HSM-ratkaisun tulee olla FIPS 140-3 -yhteensopiva.	Hankinta- toimi
P-C-15	Pilvi- palvelut	Pilvipalve- luiden identiteetin- ja pääsyn- hallinta	Epävirallisen suojausmene- telmän käyttö henkilöllisyyden ja käyttöoikeuksien hallinnassa voi johtaa järjestelmän vaarantumiseen	Hankintatoimessa on varmis- tettava, että pilvipalvelutar- joaja noudattaa tunnettuja identiteetin- ja pääsynhal- linnan standardeja ja hyviä käytäntöjä, kuten CISA käyttö pilvipalveluiden IAMissa, C5 suositukset, CMM tai NIST 800-192 suositukset. Mikäli käytetään paikallisia pilvipalve- luita, on tärkeä käydä organi- saation erityisvaatimukset läpi IT ja palvelutuotanto organi- saatioiden kanssa. Lisäksi on esitettävä tavat, kuinka vaati- musten mukaisuus todetaan.	Hankinta- toimi, Palvelu- tuotanto- tiimi, IT osasto
P-C-16	Pilvi- palvelut	Pilvipalve- luiden data tallennuksen data turvallisuus	Epävirallisten suojausmenetel- mien käyttö pilvi- palvelutallennuk- sessa voi johtaa tietojen menetyk- seen tai sisällön vääräntämisen	Hankintatoimessa on varmis- tettava, että pilvipalvelutar- joaja noudattaa tunnettuja identiteetin- ja pääsynhal- linnan standardeja ja hyviä käytäntöjä, kuten CISA käyttö pilvipalveluiden IAMissa, C5 suositukset, CMM tai NIST 800-192 suositukset. Mikäli käytetään paikallisia pilvipalve- luita, on tärkeä käydä organi- saation erityisvaatimukset läpi IT ja palvelutuotanto organi- saatioiden kanssa. Lisäksi on esitettävä tavat, kuinka vaati- musten mukaisuus todetaan.	Hankinta- toimi, Palvelu- tuotanto- tiimi, IT osasto

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuulinen taho
P-C-17	Pilvi- palvelut	Vastuukartta sekä roolitukset	Epäselvät vastuut ja roolimääritykset voivat johtaa suojaamattomaan toimintaan virheisiin tai järjestelmään kyvyttömyyteen toipua hyökkäyksestä tai tietoturvarikkomuksesta	Hankintatiimin tulee varmistaa, että palvelusopimuksissa on hyvin yksityiskohtainen vastuukartta. Vastuukartan on sisällettävä seuraavat tiedot: 1: Ylläpito (fyysinen ja looginen), korjaus, kirjaaminen (pinojen ja sovelluksen eri osat), palomuurit (erityyppiset palomuurit), 2. Haavoittuvuus- ja tapah-tumaraportointi, tiedon-hallinta, API-turvallisuus ja pääsynhallinta, tunnistetietojen hallinta ja avainten-hallintajärjestelmät (KMS), 3. Varmuuskopiointit ja toipumissuunnitelma	Hankinta-toimi, Palvelu-tuotanto-tiimi, IT Osasto, Lakiosasto
P-C-18	Pilvi- palvelut	Uhkatilanteesta palautumisen priorisoinnit	Jos pilvi tai osa verkosta katkeaa, kriittisen verkon palauttamisen ensisijaisuuden puuttuminen voi johtaa viivästyneeseen palautumiseen	Riskienhallinta-, IT-osasto ja palvelutuotanto tiimi on laadittava katastrofientilanteiden palautussuunnitelma. Suunnitelmassa olisi oltava ennallistamista koskevat painopisteet, joissa otetaan huomioon järjestelmäkriittisyys, organisaationtoimivuus ja palvelusta riippuvaiset asiakkaat. Hankintatoimen tulisi ottaa edellä kuvatut osa-alueet huomioon pilvipalveluntarjoajan kanssa tehtävässä palvelusopimuksessa varmistaa, että palvelukriittiset verkkotoiminnot ovat etusijalla palautustoinnassa sekä korjausten toteutustyössä.	Hankinta-toimi Palvelu-tuotanto-tiimi, IT Osasto, Riskien hallinta, Lakiosasto
Hankinta – Turvallinen ohjelmistokehitys					
P-SDLC-1	Turvallinen ohjelmistokehitys	Arkkitehtuurin ja suunnitteluasiakirjojen saatavuus	Vanhentuneet tai puuttuvat arkkitehtuuridokumentit voivat johtaa suojaamattomiin rajapintoihin, päivittämättömiin kriittisiin järjestelmiin/laitteisiin aiheuttaen kokonaisjärjestelmän vaarantumiseen	Hankintasopimukseen olisi sisällytettävä velvoite toimittaa ajantasaiset arkkitehtuuri- ja suunnitteluasiakirjat. Palvelutuotannon tulee antaa palautetta hankintatoimelle vaatimuksista, ja asiakirjojen on oltava riittävän yksityiskohtaisia, ajantasaisia ja niitä ylläpidettävä säännöllisesti (esim. korjausten vuoksi).	Hankinta-toimi, Palvelu-tuotanto-tiimi

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuulinen taho
P-SDLC-2	Turvallinen ohjelmisto-kehitys	Ohjelmisto-projektien ja ohjelmisto-kehityksen tietoturvan hallinta	Huonosti hoidettu tietoturva ohjelmisto-projekteissa ja ohjelmistokehityksessä johtaa haavoittuvuuksiin, aiheuttaen järjestelmän toiminnan vaarantumiseen tai verkon käytettävyyden heikkenemisen.	Hankintasopimukseen on sisällytettävä vaatimus, jonka mukaan toimittajan on annettava tiedot siitä, miten se varmistaa ohjelmistotuotteen tietoturvan hallinnan ja siihen tarvittavan ylläpidon. Erityisesti on huomioitava: 1. Turvallisuusasiantuntijoiden ottaminen mukaan hankkeeseen, 2. Turvatarkastukset, turvallisuusarvioinnit ja tehtävien erottaminen (turvallisuustestaus vs. kehittäminen)	Hankinta-toimi
P-SDLC-3	Turvallinen ohjelmisto-kehitys	Turvalliset ohjelmointikäytännöt	Heikosti turvallisuuden huomiointi ohjelmointikäytännöissä voi johtaa haavoittuvuuksiin, jotka johtavat järjestelmän toiminnan vaarantumiseen	Hankinnassa olisi varmistettava, että sopimus sisältää veloitteet toimittajille (ja niiden alihankkijoille) sekä ohjeistukset kuinka tietoturva on huomioitava ohjelmiston kehitystyössä ja mitä turvallisen ohjelmointiin vakiokäytäntöinä vaaditaan ja mitä toimittajat noudattavat, esim. Carnegie Mellon, OWASP, Synopsis, OpenSSF.	Hankinta-toimi
P-SDLC-4	Turvallinen ohjelmisto-kehitys	Toimittajan tietoturva-testaus-suunnitelma	Puutteellinen tietoturvatestaus tai puutteellinen testauksen kattavuus johtaa yleensä ylläpidollisiin ongelmiin, käyttökatkoksiin ja tietovuotoihin.	Hankintasopimuksessa on vaadittava, että toimittaja tarjoaa tuotteen testauksen laajuudesta tiedot sekä testisuunnitelman. Suunnitelman tulisi sisältää: ohjelmisto sisällön testauslaajuuden, testin kattavuuden, staattinen sovellusten tietoturvatestauksen (SAST), dynaaminen sovellusten tietoturvatestauksen (DAST), ohjelmistokomponenttien analyysit (SCA), "fuzzaus-vaikutukset", koodin sisältö tarkistukset, tarvittaessa riippumattoman laboratoriotestauksen, viimeisimmät tietoturvalöydöt. IT osaston ja palvelutuotannon tulee tarkentaa näitä vaatimuksia vastaamaan palvelutuotannon sisältöä, jotta varmistutaan toimittajavaatimusten täyttyminen (toimittaja turvallisuus).	Hankinta-toimi, Palvelutuotantotiimi, IT osasto

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuullinen taho
P-SDLC-5	Turvallinen ohjelmistokehitys	Ohjelmistojen laadunvarmistus	Heikkolaatuiset ohjelmistot voivat johtaa palvelukatkoksiin ja tietovuotoihin.	Hankintasopimuksessa on oltava vaatimus, että toimittajan on annettava tietoja siitä, miten he varmistavat ohjelmiston laadun (sisältäen: pullonkaulat, rajapinnat, koulutus/palvelutuen, osaamisen ylläpidon sekä tulosten arvioinnin.)	Hankinta-toimio
P-SDLC-6	Turvallinen ohjelmistokehitys	Turvallinen ohjelmistokehitysympäristö	Saastunut ohjelmistokehitysympäristö voi johtaa saastuneisiin tuotteisiin, joissa on takaportteja tai muita haavoittuvuuksia.	Hankintasopimuksessa on oltava vaatimus, jonka mukaan toimittajan on annettava tietoja siitä, miten he varmistavat ohjelmistokehitysympäristönsä eheyden. Organisaation oman IT-osaston arvioinnit tulee sisällyttää prosessiin.	Hankinta-toimi, IT osasto
P-SDLC-7	Turvallinen ohjelmistokehitys	Turvallinen ohjelmistojen tuotantoprosessi (koodikäännökset jne.)	Huonosti toteutettu ohjelmiston koontiversio voi johtaa haavoittuviin ohjelmistotuotteisiin. Tämä voi johtaa järjestelmän käytön vaarantumiseen	Hankintasopimukseen on otettava vaatimus, jonka mukaan toimittajan on annettava tietoja siitä, miten he varmistavat ohjelmiston turvallisen rakenteen, käännösten ja kehitysprosessin turvallisuuden sekä kokoonpanon. Organisaation oma IT-osaston arvioinnit tulee sisällyttää prosessiin.	Hankinta-toimi, IT osasto
P-SDLC-8	Turvallinen ohjelmistokehitys	Haavoittuvuus arviointi	Kriittisten virheiden riskin minimoimatta jättäminen voi johtaa järjestelmän käytön vaarantumiseen.	Hankintasopimuksessa on kuvattava, kuinka toimittaja suorittaa ohjelmistonsa haavoittuvuusarviointia. Toimittajan tulee kuvata miten he minimoivat kriittisten virheiden riskiä. IT-osasto ja operatiivinen tiimi voivat auttaa toimittajien vastauksen arvioinnissa. Organisaation oman IT-osaston arvioinnit tulee sisällyttää prosessiin.	Hankinta-toimi, IT-osasto, Palvelutuotanto tiimi

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuulinen taho
P-SDLC-9	Turvallinen ohjelmisto-kehitys	Avoimen lähdekoodin ja kolmannen osapuolen tietoturvakatselmointi	Kolmansien osapuolten ja avoimen lähdekoodin tietoturvariskien minimoimatta jättäminen voi johtaa tietoturva-aukkoihin, joita voidaan hyödyntää ulkopuolisten tahojen toimesta.	Hankintasopimukseen tulee sisällyttää vaatimus, että toimittajalla on oltava tehokas prosessi tietoturvallisuuden varmistamiseksi, kun se integroi avoimen lähdekoodin komponentteja tai kolmannen osapuolen ohjelmistoja tuotteisiinsa. Prosessi voi sisältää lähdekoodin tarkistukseen (kuinka toteutetaan), tai tehdään testauksessa, kuinka, varmistetaan testaamalla tietoturvallisuus/eheys. Organisaation oman IT-osaston arvioinnit tulee sisällyttää prosessiin.	Hankinta-toimi, IT-osasto, Palvelutuotanto tiimi
P-SDLC-10	Turvallinen ohjelmisto-kehitys	Ohjelmistokehittäjien tietoturvakoulutus	Ohjelmistokehittäjät, joita ei ole koulutettu tietoturva-vaatimusten mukaiseen ohjelmointiin, tuottavat ohjelmistoja, jotka ovat alltiita muistin ylivuodoille ja muille turvallisuusriskeille sekä haavoittuvuuksille, jotka voivat johtaa järjestelmän käytön vaarantumiseen.	Hankintasopimuksen tulee sisältää toimittajille vaatimuksen, jossa kuvataan ohjelmistokehittäjien tietoturvan osaamiskoulutus sekä osaamisen ylläpidon suunnitelma.	Hankinta-toimi, IT-osasto, Palvelutuotanto tiimi
P-SDLC-11	Turvallinen ohjelmisto-kehitys	Ohjelmiston sisällön materiaali-luettelo (SBOM)	Ohjelmiston koostumuksen vajaa tuntemus voi johtaa piileviin haavoittuvuuksiin (esim. Log4j), joita voidaan hyödyntää ulkopuolelta toteutettaviin hyökkäyksiin ja voivat johtaa järjestelmän käytön vaarantumiseen.	Hankintasopimukseen tulisi sisällyttää toimittajalle vaatimus, kuinka toimittaja on listannut ohjelmistosta yksityiskohtaisen ohjelmistokomponenttiluettelon (Software Bill of Material, SBOM). Mitä osia ja palasia ohjelmisto yksityiskohtaisesti sisältää ja kuinka se on rakennettu ja miten SBOM voidaan yhdistää CVE-rekisteriin (haavoittuvuuksien tunnistamiseksi).	Hankinta-toimi, IT-osasto, Palvelutuotanto tiimi
P-SDLC-12	Turvallinen ohjelmisto-kehitys	Materiaalilistauksen muoto SBOM-muoto	Yhteisen SBOM-muodon puuttuminen voi johtaa haavoittuvuuksien havaitsemisen ja järjestelmän vaarantumiseen.	Hankintasopimuksessa on oltava toimittajalle vaatimus standardisoidusta listautavasta ohjelmistolistauksesta (SBOM:lle sisältäen allekirjoitusmuodot). Organisaation oman IT-osaston arvioinnit tulee sisällyttää prosessiin. SBOM voidaan validoida mm. ohjelmistokomponenttien analysointityökaluilla (SCA).	Hankinta-toimi, IT-osasto, Palvelutuotanto tiimi

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuul- linen taho
Hankinta - Tuotteen arviointi, testaus ja elinkaaren hallinta					
P-PETL-1	Tuotteen arviointi, testaus ja elinkaaren hallinta	Testisuunnitelman tulokset	Puutteellisesti testatut ohjelmistot ovat alttiita haavoituvuuksille, jotka voivat johtaa järjestelmän käytön vaarantumiseen.	Hankintasopimuksessa on oltava vaatimus toimittajalle testisuunnitelman tulosten vaatimien toimenpiteiden toteuttamisesta. Organisaation oma IT-osaston arvioinnit tulee sisällyttää prosessiin. Mikäli toimittaja ei toimita tuloksia ja tai riittäviä selvitystä testauksesta, on lisättävä oikeus testauttaa ohjelmistot toimittajan kustannuksella. Testaukseen on sisällytettävä myös mahdolliset kolmannet osapuolet ja niiden komponentit.	Hankinta-toimi, Palvelu- tuotanto- tiimi, IT osasto
P-PETL-2	Tuotteen arviointi, testaus ja elinkaaren hallinta	Fyysistä turvallisuutta koskevat vaatimukset	Looginen suojaus on mahdollista ohittaa fyysisen suojauksen puutteen vuoksi	Operatiivinen palvelutiimi toteuttaa yhdessä riskienhallinnan kanssa luettelon vaadituista fyysisistä tarkastuksista tuotteen/palvelun hyväksyntäprosessiin. Vaatimukset on sisällytettävä palvelun hankintasopimukseen.	Hankinta- toimi, Palvelu- tuotanto- tiimi, IT osasto, Riskien- hallinta
P-PETL-3	Tuotteen arviointi, testaus ja elinkaaren hallinta	Testisuunnitelman tulosten validointi	Puutteellisesti testatut ohjelmistot ovat alttiita haavoituvuuksille, jotka voivat johtaa järjestelmän käytön vaarantumiseen.	Jos toimittaja toimittaa vain omat testituloksensa tai ne ovat puutteellisia, on asiasta annettava vastine, ja mikäli toimittaja ei korjaa testatuloksiaan, voidaan testaus toteuttaa toimittajan kustannuksella (vaatimus tulee sisällyttää hankintasopimukseen). Testauksen tulee perustua validointitestisuunnitelmaan, joka on suoritettu onnistuneesti. Tämän testauksen sisällön olisi mahdollistettava hankintatoimelle perusteet toimittajien kyberturvallisuuden pisteyttämiseen.	Hankinta- toimi, Palvelu- tuotanto- tiimi, IT osasto

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuulinen taho
P-PETL-4	Tuotteen arviointi, testaus ja elinkaaren hallinta	Toimittajan suojauksen suorituskykyprosessi	<p>Palvelutuotannosta vastaavilla yksiköillä tulee olla riittävästi asiantuntemusta ja ymmärrystä arvioida toimittajan turvallisuusperiaatteista/toimintatavoista, sekä kyky valvoa sopimukseen liittyvien turvallisuusvaatimusten noudattamista.</p> <p>Mikäli tässä on puutteita, turvallisuusvaatimuksista johtuvia korjauksia ei osata vaatia eikä toimittajalla ole sopimuksellisia riskejä parantaa tietoturvakäytänteitään, mikä voi johtaa kyberturvapuutteellisesti toteutettuja ohjelmistoja, jotka voivat johtaa järjestelmän käytön vaarantumiseen.</p>	Hankintasopimukseen sisällytettyjen vaatimusten toteutumisen valvonta koko sopimuksen elinkaaren ajan.	Hankinta-toimi, Palvelutuotantotiimi, IT osasto
P-PETL-5	Tuotteen arviointi, testaus ja elinkaaren hallinta	SIEM/NOC/SOC-integrointi	<p>Puutteellinen ymmärrys järjestelmäkoneistuksesta ja huonosti suunniteltujen valvonta sensoreiden asennus tai lokitietojen keruu laitteista, järjestelmistä, tietokannoista, ohjelmistoista, verkkoliikenteestä, sekä puutteellisesti toteutettu SOC/SIEM integraation toteuttaminen johtaa hyökkäysten havaitsemisen viiveisiin, johtaan viiveisiin uhkien torjunnassa ja hyökkäyksestä toipumisessa.</p>	Hankintasopimukseen tulee sisällyttää yksityiskohtaisesti tieto, mitä toimintoja tulee valvoa, kuinka pitää valvoa, mistä tietoa kerätään, SOC/SIEM integraatiot ja maksimi-viiveet hyökkäysten raportointiin.	Hankinta-toimi Palvelutuotantotiimi, IT osasto

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuullinen taho
P-PETL-6	Tuotteen arviointi, testaus ja elinkaaren hallinta	Tietoturvan koventamis-dokumentointi/tulokset	Puutteellisesti tietoturva koventaminen tietoliikenne-infrastruktuuri-kokonaisuudessa voi johtaa haavoit-tuviin järjestelmä pisteisiin, mahdollistaen hyökkääjien mahdollisuudet löytää tapoja käyttää teleinfra-struktuuria hyväkseen kanavana hyökkäyksissä kolmansiin järjestelmiin.	Hankintasopimukseen tulee sisällyttää vaatimus tieto-liikenneinfrastruktuurin turvallisuuden koventamisesta.	Hankinta-toimi, Palvelu-tuotanto-tiimi, IT osasto
P-PETL-7	Tuotteen arviointi, testaus ja elinkaaren hallinta	Tarpeettomien ominai-suuksien poistaminen	Tarpeettomat tai käyttämättömät toiminnallisuudet voivat aiheuttaa tietoturva riskejä ja mahdollistaa hyökkääjien Tietoliikenne-infrastruktuurin hyödyntämisen omissa hyökkäyk-sissä tai mahdolli-suuden ottaa koko infrastruktuuri osin tai kokonaan hallintaansa.	Hankintasopimuksen tulee sisältää vaatimus, että toimit-taja poistaa kaikki tarpeet-tomat/käyttämättömät toiminnallisuudet käytöstä. Tämä koskee ohjelmisto-toimintoja, rajapintoja, tietokantojen rajapintoja sekä palveluita. Näistä on oltava käytössä ajantasainen dokumentaatio toimittajalta ja se tulee audi-toida säännöllisesti.	Hankinta-toimi Palvelu-tuotanto-tiimi, IT osasto
P-PETL-8	Tuotteen arviointi, testaus ja elinkaaren hallinta	Käyttövarmuuden validointi	Turvallisuuson-gelmat voivat johtua ohjelmiston turvallisuuspuut-teista, huonosta tuoterakenteesta sekä ohjelmiston laadullisista puut-teista. Nämä voivat johtaa järjestelmän käytön vaarantumiseen.	Hankintasopimukseen tulee sisällyttää riittävä laaduntar-kastusaika omalle organisaatiolle. Laatu tulee auditoida, jotta toimittajaa voidaan vaatia korjaamaan mahdol-liset puuteet tai virheet. Näiden toteamiseen on organisaatiossa oltava riittävä osaaminen ja välineet. Todentamisaika on oltava riittävä, jotta tarvittavat puutteet voidaan havaita ja reklamoida toimittajalle sovitun aikaraamin puitteissa.	Hankinta-toimi, Palvelu-tuotanto-tiimi, IT osasto

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuullinen taho
P-PETL-9	Tuotteen arviointi, testaus ja elinkaaren hallinta	Tietoturvan dokumentointi integrointien osalta, rajapintaturvallisuus kuvaukset	Suojaamaton järjestelmähallinnan integraatio, suojaamattomat/salaa-mattomat rajapinnat voivat johtaa tietojen menetykseen tai järjestelmän käytön vaarantumiseen.	Hankintasopimuksessa on oltava lausekkeet, joiden mukaan toimittajan on toimitettava riittävän kattava ja ajantasainen dokumentaatio asianmukaisten suojausmekanismien käytöstä ja määräyksistä sekä tietoturvaan liittyvän konfiguraation mahdolliset vaikutukset (esim. Kubernetes-kontit). Dokumentaatiossa olisi myös perusteltava tapaukset, jossa turvatoimia ei oteta käyttöön tai testejä ei suoriteta, ja nämä on oltava yhteisesti ymmärrettyjä ja hyväksytyjä sopimuksellisesti.	Hankinta-toimi, Palvelu-tuotanto-tiimi, IT osasto
P-PETL-10	Tuotteen arviointi, testaus ja elinkaaren hallinta	Uhkatie-dustelutietokirjasto- tojen hallinta	Ilman uhkatie-dustelutietoja/kirjasto- turvallisuustoimet niiden eliminoimi- seksi vanhenevat mahdollistaen hyökkääjien pääsyn järjestelmiin ja ne voivat vaarantaa järjestelmän käytön.	Hankintasopimukseen on sisällytettävä vaatimus toimittajalta uhkatie-dustelutietokirjasto- tojen/kirjastojen ajantasai- sesta ja niiden perusteella torjuntatoimien toteuttamisesta. Tämä koskee verkon solmu- pisteitä, joita käytetään segmentointiin, kuten signa- lointipalomureja, kuormi- tuksen tasaajia, ohjelmisto- pohjaista verkkoa (SDN). Mikäli toimittaja ei pysty näitä tietoja toimittamaan, on huolehdittava, että tarvittava tieto saadaan muista lähteistä kuten valtion viran- omaisilta, palvelua tuotta- valta yritykseltä, GSMA:lta tai muilta operaattoreilta.	Hankinta- toimi
P-PETL-11	Tuotteen arviointi, testaus ja elinkaaren hallinta	Jatkuva palvelu/ tuotetuki ja päivitykset, päivitys- paketit	Ilman pitkäaikaista jatkuvaa tuotetukea ja tuotepäivityksiä, laitteesta, järjestel- mästä sekä ohjel- mistosta tulee haavoittuva.	Hankintasopimuksen tulee sisältää laitteiden, ohjelmis- tojen sekä järjestelmän elin- kaaren aikainen tuki ja yllä- pito, jossa mukana tietoturvapäivitykset. Päivityksen tulee sisältää tarvittavat sertifikaattien ajantasaiset versiot, päivi- tetyt ja korjatut tekniset tiedot (ei välttämättä uusia versioita, joissa on uusia ominaisuuksia). Tarkat ajoitusvaatimukset olisi määritettävä sopimuk- sessa oman organisaation tavoitteiden mukaisiksi.	Hankinta- toimi, Palvelu- tuotanto- tiimi, IT osasto

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuulinen taho
P-PETL-12	Tuotteen arviointi, testaus ja elinkaaren hallinta	Tulevaisuuden varautuminen hyökkäysvalmius	Riittämätön varautuminen tulevia tietoturvahyökkäyksiä vastaan voi johtaa hyökkäjän kasvaviin mahdollisuuksiin hyödyntää olemassa olevia haavoittuvuuksia tulevaisuudessa. Viiveet voivat johtaa korvausvaatimuksiin asiakailta ja taloudellisiin menetyksiin.	Hankintasopimukseen tulee sisällyttää vaatimus toimittajan sekä sen alihankkijoiden tuki jatkuvasta tuotepäivityksien saatavuudesta sekä riittävän nopeasta toiminnasta niiden tuottamiseksi sekä mallit, miten mahdolliset myös väliaikaiset korjausratkaisut saadaan käyttöön. Päivityksissä on myös otettava huomioon tietoturva-algoritmien tarve (mahdolliset kvanttiteknologian vaikutukset näihin), satunnaislukugeneraattoreihin liittyvät vaatimukset sekä tekoälyn vaikutukset.	Hankinta-toimi
P-PETL-13	Tuotteen arviointi, testaus ja elinkaaren hallinta	Tietoja käytetyistä suojausalgoritmeista ja -ominaisuuksista	Tietämättömyys heikkojen tietoturva-algoritmien käytöstä voi johtaa järjestelmän vaarantumiseen.	Hankintasopimuksessa olisi edellytettävä, että toimittaja ilmoittaa, mitä algoritmeja ja satunnaislukugeneraattoreita on sen käytössä järjestelmän turvallisuuden varmistamiseksi. Nämä on säännöllisesti arvioitava turvallisuuden kannalta niin ettei vanhentuneita ratkaisuja ole käytössä.	Hankinta-toimi, Palvelutuotantotiimi, IT osasto
Hankinta – Haavoittuvuuksia koskevien tietojen vaihto					
P-VE-1	Haavoittuvuuksia koskevien tietojen vaihto	IT- ja tietoliikenne-tuotteiden haavoittuvuustietojen vaihdossa käytettävät työkalut ja protokollat	Tietämättömyys haavoittuvuuksista voi johtaa viivästyneeseen varautumiseen ja järjestelmäsuojautumistoimiin vaarantaen järjestelmän käytön.	Hankintasopimuksessa olisi määriteltävä käytettävät työkalut ja protokollat, joita käytetään kumppaneiden välisessä tieto- ja tietoliikennetuotteiden haavoittuvuutta koskevien tietojen vaihdossa. Vaatimuksiin on huomioitava oman organisaation tarpeet.	Hankinta-toimi, Palvelutuotantotiimi, IT osasto
P-VE-2	Haavoittuvuuksia koskevien tietojen vaihto	IT- ja tietoliikenne-tuotteiden haavoittuvuutta koskevien tietojen saatavuuden ajoitus	Tietämättömyys haavoittuvuuksista voi johtaa viivästyneeseen varautumiseen ja järjestelmäsuojautumistoimiin vaarantaen järjestelmän käytön.	Hankintasopimuksessa olisi määriteltävä tavoiteaika-aulut, jolloin toimittaja asettaa saataville tietoteknisten ja tietoliikennetuotteiden haavoittuvuutta koskevat tiedot. Aikataulujen on vastattava NIS2-toimialalle määritellyjä minimivaatimuksia.	Hankinta-toimi

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuulinen taho
P-VE-3	Haavoittuvuuksia koskevien tietojen vaihto	IT- ja tietoliikenne-tuotteiden haavoittuvuutta koskevien tietojen muoto ja korjausten ajoitus	Tehoton tietoturvapoikkeamien torjunta tai huonosti tehty toteutus suunnitelma voi johtaa järjestelmän käytön vaarantumiseen. Ongelmia voi olla korjauspakettien hidas toimitus tai sisältö, joka ei ole soveltuva. Tai korjausta ei ole lainkaan saatavilla.	Hankintasopimukseen olisi sisällytettävä vaatimukset tietoliikennetuotteiden haavoittuvuutta koskevien tietojen raportoinnista, raporttien sisältövaatimuksesta ja korjausten aikarajoista.	Hankintatoimi, Palvelutuotantotiimi, IT osasto
P-VE-4	Haavoittuvuuksia koskevien tietojen vaihto	Tuotteen haavoittuvuuden vakavuusvai- kutustiedot	Haavoittuvuuden vakavuus voi johtaa viivästyneeseen tietoturvakorjaukseen tai aiheuttaa järjestelmän käytön vaarantumiseen.	Hankintasopimuksessa on oltava vaatimus toimittajalle antaa mahdollisimman laajasti tietoa haavoittuvuuden vakavuudesta ja vaikutuksista. Tässä on suositeltavaa hyödyntää standardoidun pisteytyksen mukaisesta tapaa prioriteeteista ja on myös huomioitava oman organisaation toimintaan liittyvät tarpeet. Oma organisaatio on velvollinen viestimään asioista myös asiakkaille sekä viranomaisille.	Hankintatoimi, Palvelutuotantotiimi, IT osasto
P-VE-5	Haavoittuvuuksia koskevien tietojen vaihto	Poikkeustilanteen haavoittuvuuteen liittyvät yhteystiedot	Korkean turvallisuusriskin haavoittuvuuden vaikutuksia ei ole voitu rajoittaa ja tämä johtaa tietojen vuotamiseen tai järjestelmän käytön vaarantumiseen	Hankintasopimuksessa on oltava yhteystiedot kriisitilanteiden varalle, kaikille vuorokauden ajoille, mikäli sopimuksessa ylläpito on sovittu kattamaan ympärivuorokautisen toiminnan. Yhteystietojen saatavuus ja yhteydenpito tavat on oltava tarkasti kuvattuna sekä mitkä ovat kriisitilanteisiin reagoimisen vasteajat. Nämä on oltava synergiasa oman organisaation toimintakyvyn ja asiakaspalvelun kanssa.	Hankintatoimi, Palvelutuotantotiimi, IT osasto

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuulinen taho
P-VE-6	Haavoittuvuuksia koskevien tietojen vaihto	Haavoittuvuustietojen vaihdon elinkaarituki	Tietämättömyys olemassa olevasta tietoturva-vaavoittuvuudesta, joka johtuu siitä, ettei toimittaja ylläpidä ja välitä haavoittuvuustietoja vanhentuneelle käytössä olevalle tuotteelle tai järjestelmälle (tai jostakin muusta syystä) esimerkiksi määräajan umpeuttua. Tämä voi johtaa järjestelmän käytön vaarantumiseen.	Hankintasopimukseen on sisällytettävä pitkän aikavälin tuki haavoittuvuustietojen vaihtoa varten tuotteen odotetun käyttöiän perustuen. Tarkat ajoitusvaatimukset on määritettävä yhdessä oman organisaation toimintakyvyn ja asiakasvelvoitteiden mukaisesti.	Hankinta-toimi, Palvelutuotantotiimi, IT osasto
Hankinta – Uhkatilanteita koskevien tietojen vaihto					
P-IE-1	Uhkatilanteita koskevien tietojen vaihto	Sääntelevän viranomaisten tietojenvaihdon muoto/sisältörakenne	Puutteelliset tiedot poikkeamista ja tietoturva-uhkista voivat johtaa väärin suojaus/varautumistointenpiteisiin ja väärin lähestymistapoihin ja aiheuttaen taloudellisiin seuraamuksia kuten sanktioita ja tuotannon keskeytyskorvauksia.	Hankintasopimuksessa ja toimintamalleissa on varmistettava, että vaatimukset vastaavat sääntelyviranomaiselle ilmoitettavaa laajuutta ja sisältöä ja että se vastaa omille asiakkaille ja sidosryhmille tehtäviä velvollisuuksia.	Hankinta-toimi, Palvelutuotantotiimi, Lakiosasto
P-IE-2	Uhkatilanteita koskevien tietojen vaihto	Sääntelevän viranomaisten tietojenvaihdon muoto/sisältörakenne	Yhteensopimattomista tiedonvaihdyökaluista ja käytetyistä manuaalisista prosesseista aiheutuva viivästynyt tilannekuvatietoisuus tapahtumista voi johtaa myöhästyneisiin torjuntatoimenpiteisiin ja aiheuttaa vahinkoa asiakkaille, yhteistyökumppaneille, yhteiskunnalle sekä omalle liiketoiminnalle sekä taloudellisia seuraamuksia.	Hankintasopimuksen ja toimittajan suorituskyvyn varmistamiseksi on määriteltävä mitä tietojenvaihtotapoja, työkaluja sekä sisältöä käytetään, ja samalla on varmistettava, että ne soveltuvat toimialaa valvovalle viranomaiselle sekä mahdollisesti tukevat asiakassitoumuksia.	Hankinta-toimi, Palvelutuotantotiimi, IT osasto

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuul- linen taho
P-IE-3	Uhka- tilanteita koskevien tietojen vaihto	Kriittisten- toimialojen/ yritysten yritystietojen vaihdon muoto/ sisältö- rakenne	Puuteelliset/ epäyhtenäiset uhkatiliedot poikkeamista ja uhkista voivat johtaa väärin torjuntatoimen- piteisiin ja korjauk- siin, tarpeettomiin viiveisiin sekä mahdollisiin taloudellisiin seuraamuksiin	Hankintasopimuksessa on toiminnan jatkuvuuden varmentamiseksi määritel- tävä yhteiskuntakriittisen toimialan yrityksen viran- omaisraportoinnin laajuus, millä aikataululla tai tavoilla raportointi toteutetaan, raportoinnin sisältö ja miten yhteyttä ylläpidetään toimit- tajan toimesta.	Hankinta- toimi, Palvelu- tuotanto- tiimi, IT osasto, Lakiosasto
P-IE-4	Uhka- tilanteita koskevien tietojen vaihto	Kriittisten- toimialojen/ yritysten yritystietojen vaihdon muoto/ sisältö- rakenne	Puuteelliset/ epäyhtenäiset uhkatiliedot poikkeamista ja uhkista voivat johtaa väärin torjuntatoimen- piteisiin ja korjauk- siin, tarpeettomiin viiveisiin sekä mahdollisiin taloudellisiin seuraamuksiin	Hankintasopimukseen on toiminnan jatkuvuuden turvaamiseksi määriteltävä yhteiskuntakriittisen toimijan veloitteiden mukaiset tiedonvaihdon työkalut, aikataulut, sisällöt ja toimintamallit.	Hankinta- toimi Palvelutu- otantotiimi, IT osasto

7.2 Verkon valvonnan kontrollit

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuulinen taho
NM-ITI-1	IT-infrastruktuurin seuranta	Poikkeavat verkko-liikennemallit	Hyökkääjää ei välttämättä havaita, kun hän anastaa tietoja tai liikkuu järjestelmässä	Liikenteen seuranta IT-tasolla poikkeavien verkkoliikennemallien havaitsemiseksi	Tekninen Palvelutuotanto / IT osasto
NM-ITI-2	IT-infrastruktuurin seuranta	Luvattomat käyttö-yritykset	Hyökkääjä voi murtautua järjestelmään sulkemalla tilejä ja käyttöliittymiä	Liikenteen seuranta IT-tasolla luvattoman käytön, poikkeavien kirjautumisten havaitsemiseksi. Valvontaominaisuuksilla varustettujen kulunvalvontajärjestelmien käyttö	Tekninen Palvelutuotanto / IT osasto
NM-ITI-3	IT-infrastruktuurin seuranta	Poikkeava järjestelmän käyttäytyminen	Järjestelmä saattaa olla vaarantunut	Järjestelmän käyttäytymisen seuranta	Tekninen Palvelutuotanto / IT osasto
NM-ITI-4	IT-infrastruktuurin seuranta	Konfiguraatio ja toiminnalliset muutokset	Suojausrakennetta muutettu suojaamattomaksi hyökkääjän toimien sallimiseksi	Konfiguraatiomuutosten valvonta hälytysraporttien ja lokituksen avulla (esim. suojausasetukset)	Tekninen Palvelutuotanto / IT osasto
NM-ITI-5	IT-infrastruktuurin seuranta	Poikkeava IT-verkon käyttäjän käyttäytyminen	Vaarantunut IT-verkon käyttäjä, esimerkiksi palvelutili, voi aiheuttaa DoS:n tai tietovuodon	IT-verkon käyttäjien seuranta poikkeavia käyttäytymismalleja havaitsevien analyysityökalujen ja niistä generoituvien hälytysten avulla	Tekninen Palvelutuotanto / IT osasto
NM-ITI-6	IT-infrastruktuurin seuranta	Järjestelmälokin analyysi	Järjestelmän havaitsematon vaarantuminen	Seurattujen tapahtumien kirjaaminen ja lokien analysointi (automaattinen + asiantuntija), SOC ja SIEM liitokset	Tekninen Palvelutuotanto / IT osasto

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuullinen taho
NM-ITI-7	IT-infrastruktuurin seuranta	Dynaaminen sisällön valvonta	Resurssien ehtyminen ja mahdolliset korkeat varastointikustannukset	Dynaamisen sisällöntuotannon toimintojen valvonta	Tekninen Palvelutuotanto / IT osasto
NM-ITI-8	IT-infrastruktuurin seuranta	Tilannekohtainen turvallisuustietoisuus	Ei näkyvä järjestelmän vaarantuminen	SOC/SIEM:n (ja NOC:n lataus) käyttö, keskitetyn näkymän saamiseksi verkon suojaus- ja turvallisuustilasta	Tekninen Palvelutuotanto / IT osasto
NM-ITI-9	IT-infrastruktuurin seuranta	Keskitetty tietojen kerääminen ja korrelaatio	Hyökkäyksen puutteellinen ymmärtäminen voi johtaa siihen, että hyökkäystä ei havaita tai hyökkääjää ei voida poistaa verkosta	IDS/IPS:n käyttö, joka syöttää SIEM:ään, joka korreloi ja analysoi tietoja.	Tekninen Palvelutuotanto / IT osasto
NM-ITI-10	IT-infrastruktuurin seuranta	Lokit	Hyökkäyksiä ei voida tunnistaa tai niiden laajuutta arvioida	Lokien tuottaminen ja seuranta valituin kriteerein. - Suojauslokit - Järjestelmän lokit - Sovellusten lokit - Palomuurin lokit - Välityspalvelimen lokit - Vaihda lokit	Tekninen Palvelutuotanto / IT osasto
NM-ITI-11	IT-infrastruktuurin seuranta	Lokien tietojen säilytys	Hyökkääjää ei voida yksilöidä tai hyökkäyksen laajuutta ei voida määrittää	Keskitetty tallennus, esim. SIEM (mahdollinen varmuuskopio toissijaisesti). Lokit ovat eheyssuojattuja ja sisältävät aikaleiman. Lokien lukemista seurataan ja muutokset estetään.	Tekninen Palvelutuotanto / IT osasto
NM-ITI-12	IT-infrastruktuurin seuranta	Omaisuusluettelon tukeminen seuraamalla	Hyökkääjä voi tuoda verkkoon haitallisen tahon	Seurantaratkaisu, joka tukee omaisuusmuutosten havaitsemista. Muutokset on validoitava omaisuusluettelon kanssa.	Tekninen Palvelutuotanto / IT osasto

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuul- linen taho
NM-ITI-13	IT-infra- struktuurin seuranta	Ohjelmistojen valvonta	Hyökkääjä voi asentaa verkkoon haittaohjelmia tai kirstystohjelmia	Valvontaratkaisun tulisi myös valvoa ohjelmistoja ja havaita uudet ohjelmistot verkossa. Tämän tulisi olla linjassa muutoksenhallintaprosessin ja omaisuusluettelon (sw-osa) kanssa.	Tekninen Palvelu- tuotanto / IT osasto
NM-ITI-14	IT-infra- struktuurin seuranta	Lähtevän liikenteen seuranta	Hyökkääjä anastaa arkaluonteisia tietoja	Lähtevän liikenteen seuranta, esim. DLP-työkalun avulla.	Tekninen Palvelu- tuotanto / IT osasto
NM-ITI-15	IT-infra- struktuurin seuranta	Fyysinen turvallisuus - kulun- valvonta	Fyysinen pääsy palvelimiin ja tiloihin voi johtaa järjestelmän vaarantumiseen.	Kriittisiä laitteita sijaitseville alueille fyysisen pääsynval- vonnan toteuttaminen. Valvontakameroiden tai kulunvalvontasuojusten käyttö. Kohdistettu kulun- valvonta jaetuille alueille (esim. jaettu tukiasema). Kolmansien osapuolten fyysisen pääsyn valvonta, erityishuomio palvelutuotan- toon ja niiden toteuttajiin esim. siivous, laitehuolto/ kunnossapito.	Fyysisestä turvalli- suudesta vastaava organi- saatio
NM-ITI-16	IT-infra- struktuurin seuranta	Fyysinen turvallisuus - paloturvalli- suusvalvonta	Henkilöriskit	Palohälyttimet, lämpöilmai- simet, CO2-ilmaisimet, jotka on kytketty hälytysjärjestelmään	Fyysisestä turvalli- suudesta vastaava organi- saatio
NM-ITI-17	IT-infra- struktuurin seuranta	Fyysinen turvallisuus - kosteuden valvonta	Henkilöriskit	Hälytysjärjestelmään kytketyt vesi- ja kosteusanturit	Fyysisestä turvalli- suudesta vastaava organi- saatio
NM-ITI-18	IT-infra- struktuurin seuranta	Fyysinen turvallisuus - yhteyksien valvonta	Fyysiset Infrastruktuririskit	Yhteyksien valvonta, esimer- kiksi katkenneiden kaape- leiden, keskeytysten, uudel- leenreityksen, jakajan aset- tamisen havaitseminen	Tekninen Palvelu- tuotanto / IT osasto

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuulinen taho
NM-CM-1	Pilvipalveluiden seuranta	Turvallisuuden valvontavastuut	Epäselvät vastuut voivat johtaa siihen, että järjestelmän vaarantumista ei havaita	Palvelutasosopimus (SLA) sisältää tietoja tietoturvan valvontavastuun jakautumisesta ja lokien käytöstä (esim. tapahtumien tutkintaa varten)	Pilvipalveluntarjoaja, hankintatoimi, Operatiivinen palvelutuotanto
NM-CM-2	Pilvipalveluiden seuranta	Tietoturvan valvonta	Arkaluonteisten tietojen menetykset	Riippumaton valvontapalveluja käyttöönottomalleissa tietoturvan valvonta osana (esim. asiakastiedot) ja tietojen menetyksen tai kiristysohjelman havaitseminen	Operatiivinen palvelutuotanto
NM-CM-3	Pilvipalveluiden seuranta	Fyysisen infrastruktuurin ja datakeskusten valvonta	Data-keskuksen fyysisen pääsyn tai fyysisten yhteyksien aiheuttama järjestelmän rikkoutuminen	Datakeskuksen fyysinen turvallisuus osana palveluhankintatasosopimusta.	Pilvipalveluntarjoaja, hankintatoimi
NM-CM-4	Pilvipalveluiden seuranta	Master-järjestelmän infrastruktuurin valvonta	Järjestelmän haavoittuminen Master-järjestelmään pääsyn kautta	Suojauksen valvontatyökalut, jotka havaitsevat tietoturvan vaarantumisen pilvipalvelun (IaaS, PaaS, SaaS) Master-järjestelmissä osana SLA:ta. Esimerkiksi Syslogeja tai muita lokeja valvotaan.	Pilvipalveluntarjoaja, hankintatoimi
NM-CM-5	Pilvipalveluiden seuranta	Standardien noudattaminen	Valvonnan suojauskontrollien näkyvyyden puute voi johtaa heikosti suojatun pilvipalveluntarjoajan valitsemiseen	SLA sisältää vaatimuksen noudattaa teollisia turvallisuusstandardeja, jotka sisältävät turvallisuuden valvonnan perusvaatimuksia	Pilvipalveluntarjoaja, hankintatoimi
NM-CM-6	Pilvipalveluiden seuranta	Pääsynhallinta pilvipalvelujen hallintaan	Riittämätön pääsynhallinta pilvipalveluissa voi johtaa DoS:ään ja tietojen menetykseen	Vahva IAM, jossa MFA mahdollisuuksien mukaan ja roolipohjainen pääsynhallinta, jota valvotaan poikkeavuuksien, kuten sijainnin, käytetyn resurssin, roolin jne. varalta.	Pilvipalveluntarjoaja, operatiivinen palvelutuotanto

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuullinen taho
NM-CM-7	Pilvipalveluiden seuranta	Virtuaaliomaisuuteen pääsyn kirjaaminen	Seurantalokien viive voi johtaa siihen, että vaaratilanteita ei pystytä havaitsemaan ajoissa	Virtuaalikoneisiin, säilöihin, pilvihallintaan, valtuutuspalvelimiin jne. pääsyn kirjaaminen (esim. osana IAM:ää)	Pilvipalveluntarjoaja, operatiivinen palvelutuotanto
NM-CM-8	Pilvipalveluiden seuranta	Virtuaaliomaisuuden elinkaaren seuranta	Virtuaalikoneiden riittämätön elinkaaren hallinta, jolloin vanhat ohjelmistot jäävät ylläpidon ulkopuolelle ja niihin liittyvät virtuaalikoneet voivat johtaa arkaluonteisten tietojen menetykseen	Virtuaalikoneiden / konttien elinkaaren tilan seuranta.	Pilvipalveluntarjoaja, operatiivinen palvelutuotanto
NM-CM-9	Pilvipalveluiden seuranta	Kontin (container) valvonta ja oikeudet (eristäminen)	Rikkoutuneen säilön rajoitus voi johtaa tietojen menetykseen	Konttien valvonta sen varmistamiseksi, että kontit eivät toimi oletusarvoisesti pääkäyttäjänä, eivätkä käytä tarpeettomia oikeuksia tai asennettuja komponentteja. On suositeltavaa soveltaa Kubernetes-ympäristöissä podin suojauskäytännön määrittämistä, joka estää podeja suorittamasta etuoikeutettuja säilöjä.	Pilvipalveluntarjoaja, operatiivinen palvelutuotanto
NM-CM-10	Pilvipalveluiden seuranta	Käyttöoikeuksien valvonta	Rikkoutuneen säilön rajoitus voi johtaa tietojen menetykseen	Käyttöoikeuksien valvonta vain luku -säilöjen, vain luku -tiedostojärjestelmien ja komentojen suorittamisen estämiseksi tarvittavien kuvien minimoimiseksi.	Pilvipalveluntarjoaja, operatiivinen palvelutuotanto
NM-CM-11	Pilvipalveluiden seuranta	Tietojen ja tapahtumien seuranta	Rikkoutuneen säilön rajoitus voi johtaa tietojen menetykseen	Valvotaan klusteritason (Kubernetes) tietoja ja tapahtumia, jotka liittyvät säilöjen asemamääritysten muuttamiseen.	Pilvipalveluntarjoaja, operatiivinen palvelutuotanto
NM-CM-12	Pilvipalveluiden seuranta	Prosessitoimintojen seuranta	Rikkoutuneen säilön rajoitus voi johtaa tietojen menetykseen	Valvotaan prosessitoimintaa (kuten odottamattomia prosesseja, jotka syntyvät säilön ulkopuolella ja/tai Master-tasolla), jotka saattavat viitata yritykseen paeta etuoikeutetusta säilöstä Master-tasolle.	Pilvipalveluntarjoaja, operatiivinen palvelutuotanto

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuulinen taho
NM-CM-13	Pilvipalveluiden seuranta	Syscallien valvonta	Rikkoutuneen säilön rajoitus voi johtaa tietojen menetykseen	Valvotaan järjestelmäkutsujen, kuten asennuksen, odottamatonta käyttöä, joka saattaa olla merkki yrityksestä paeta etuoikeutetusta säilöstä Master-tasolle.	Pilvipalveluntarjoaja, operatiivinen palvelutuotanto
NM-CM-14	Pilvipalveluiden seuranta	Konttikuvien käyttöönoton seuranta	Rikkoutuneen säilön rajoitus voi johtaa tietojen menetykseen	Valvotaan epäilyttävien tai tuntemattomien säilökuvien ja -podien, erityisesti pääkäyttäjänä toimivien säilöjen, käyttöönottoa.	Pilvipalveluntarjoaja, operatiivinen palvelutuotanto
NM-CM-15	Pilvipalveluiden seuranta	Ytimen moduulien asennuksen valvonta	Rikkoutuneen säilön rajoitus voi johtaa tietojen menetykseen	Valvotaan sellaisten ydinmoduulien asennusta, joita voidaan käyttää väärin säilöistä pakenemiseen Master-tasolle.	Pilvipalveluntarjoaja, operatiivinen palvelutuotanto
NM-CM-16	Pilvipalveluiden seuranta	Ohjelmistomuutosten seuranta	Luvaton tai testaamaton ohjelmisto voi johtaa järjestelmän vaarantumiseen	Valvotaan ohjelmiston asennusta ja validoidaan ohjelmistomuutokset muutoksenhallintaprosessissa ja omaisuudenhallintajärjestelmässä	Pilvipalveluntarjoaja, operatiivinen palvelutuotanto
NM-CM-17	Pilvipalveluiden seuranta	Pilvipalveluiden valvonta palomuurien avulla	Suojaamattomat pilven sisääntulokohdat voivat johtaa järjestelmän vaarantumiseen	Palomuurien käyttöönotto pilvipalveluiden valvonnassa	Pilvipalveluntarjoaja, operatiivinen palvelutuotanto
NM-CM-18	Pilvipalveluiden seuranta	API-rajapinta-valvonta	Riittämätön API-rajapinta-valvonta ja suodatus voi johtaa tietojen menetykseen ja järjestelmän vaarantumiseen	API-kutsujen valvonta mukautetuilla palomuuereilla ja suodattimilla, jotka suodattavat sovellustasolla (esim. käyttämällä OWASP API-suojasta oppaana)	Pilvipalveluntarjoaja, operatiivinen palvelutuotanto

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuul- linen taho
NM-CM-19	Pilvi- palveluiden seuranta	Seuraa (juuritason) Root-käyttöä	Laaja Root-tilin käyttö voi johtaa järjestelmän vaarantumiseen	Valvotaan juuritilien oikeaa käyttöä. Root-käyttäjää ei käytetä virtuaalikoneessa tai säilöissä paitsi alustuksen/ asennuksen aikana, ja käyttö- oikeudet tulee poistaa asen- nuksen päätyttyä. Säilöille tai virtuaalikoneille ei voida myöntää lisäoikeuksia niiden suorituksen aikana (esimer- kiksi "ei uusia-oikeuksia" -merkintä säilössä).	Pilvipalve- luntarjoaja, opera- tiivinen palvelu- tuotanto
NM-CM-20	Pilvi- palveluiden seuranta	Tunniste- tietojen artefaktien valvonta	Hyökkääjät saattavat käyttää "säilöön" unohtu- neita tunniste- tietoja järjestelmän käyttöön	Valvotaan säilöjä ja virtuaali- koneita tunnistetietojen artefaktien varalta. Estetään, että arkaluonteisia tietoja (esim. yksityisiä avaimia, kriittisiä määrittystiedostoja, tunnistetietoja) ei voi julkaista tuotanto-VM/ Container-näköistiedostossa.	Pilvipalve- luntarjoaja, opera- tiivinen palvelu- tuotanto
Verkon valvonta – verkkovierailu ja reunat					
NM-RE-1	Roaming- ja reuna- valvonta	SS7 Yhteen- liittämisen valvonta	Arkaluonteisten tietojen hallinta	Saapuvan ja lähtevän liiken- teen kansainvälisen ja kansal- lisen yhteyden seuranta GSMA FS.07:n ja FS.11:n viimeisimmän version mukaisesti	Opera- tiivinen palvelu- tuotanto
NM-RE-2	Roaming- ja reuna- valvonta	Rajapinta yhteen- liittämisen valvonta	Arkaluonteisten tietojen hallinta	Saapuvan ja lähtevän liiken- teen kansainvälisen ja kansal- lisen yhteyden seuranta GSMA FS:n uusimman version mukaisesti.	Opera- tiivinen palvelu- tuotanto
NM-RE-3	Roaming- ja reuna- valvonta	5G-yhteen- liittämisen valvonta	Arkaluonteisten tietojen hallinta	Saapuvan ja lähtevän liiken- teen kansainvälisen ja kansal- lisen yhteyden seuranta GSMA FS:n uusimman version mukaisesti.	Opera- tiivinen palvelu- tuotanto
NM-RE-4	Roaming- ja reuna- valvonta	SEPP:n käyttöönotto (5G)	Arkaluonteisten tietojen hallinta	3GPP-yhteensopivan SEPP:n käyttö, joka tukee GSMA FS.36 -valvontaa, suodatusta ja uhkatiedustelua	Opera- tiivinen palvelu- tuotanto sekä hankinta- toimi

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuullinen taho
NM-RE-5	Roaming- ja reuna- valvonta	SIP-seuranta	Arkaluonteisten tietojen hallinta	Saapuvan ja lähtevän liikenteen valvonta GSMA FS.38:n uusimman version mukaisesti. SIP-valvonta voi tapahtua lisäksi Sh-rajapinnalla (IMS-järjestelmän ja ydinverkon välillä)	Operaatiivinen palvelutuotanto
NM-RE-6	Roaming- ja reuna- valvonta	GTP-C- valvonta	Arkaluonteisten tietojen hallinta	Saapuvan ja lähtevän liikenteen valvonta GSMA FS:n uusimman version mukaisesti.	Operaatiivinen palvelutuotanto
NM-RE-7	Roaming- ja reuna- valvonta	GTP-U- valvonta	Arkaluonteisten tietojen hallinta	Saapuvan ja lähtevän liikenteen valvonta GSMA FS:n uusimman version mukaisesti.	Operaatiivinen palvelutuotanto
NM-RE-8	Roaming- ja reuna- valvonta	SMS-seuranta	Laitetartunta, bottiverkot, kiristysohjelmahyökkäykset	Saapuvan ja lähtevän liikenteen valvonta GSMA FS.42:n ja SG.22:n uusimpien versioiden mukaisesti	Operaatiivinen palvelutuotanto
NM-RE-9	Roaming- ja reuna- valvonta	Kumppani- liittymän suojaus	Epäluotettavat kumppanit voivat suorittaa haitallisia toimia viestintä- ja tietoliikenneverkoille	SLA-sopimuslausekkeiden (esim. GSMA FS.52) turvallisuusvaatimusten noudattamista olisi valvottava rajapinnassa asianmukaisen merkinantopalomuurin avulla. Valvotaan pääsyä verkko- ja tietojärjestelmiin. Luodaan prosessi poikkeusten hyväksymiseksi ja käyttöoikeusrikkomusten rekisteröimiseksi.	Operaatiivinen palvelutuotanto
NM-RE-10	Roaming- ja reuna- valvonta	MEC API- valvonta	Arkaluonteisten tietojen hallinta	Otetaan käyttöön API-kohdattaiset valvontasuodattimet, jotka ottavat huomioon API:n erityispiirteet (esim. IMSI-tason valtuutus) ja noudattavat OWASP:tä. Seurannan olisi katettava <ul style="list-style-type: none"> - Rikkinäisen objektitason valtuutus - Rikkinäinen todennus - Liiallinen tietojen jako - Resurssien puute ja käytön rajoittaminen - Oikeudet - Massatietojen luovutus - Suojauksen virheellinen määritys - Injektio - Virheellinen omaisuudenhallinta - Riittämätön kirjaaminen ja seuranta sekä integrointi SIEM:iin 	Operaatiivinen palvelutuotanto

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuul- linen taho
NM-RE-11	Roaming- ja reuna- valvonta	NEF API -seuranta	Arkaluonteisten tietojen hallinta	Otetaan käyttöön API-koh- taiset valvontasuodattimet, jotka ottavat huomioon API: n erityispiirteet (esim. IMSI-tason valtuutus) ja noudattavat OWASP:a. Seurannan olisi katettava - Rikkinäisen objektitason valtuutus - Rikkinäinen todennus - Liiallinen tietojen luovutus - Resurssien puute ja käytön rajoittaminen - Oikeudet - Massantietojen luovutus - Suojauksen virheellinen määrittäminen - Injektio - Virheellinen omaisuudenhallinta - Riittämätön kirjaaminen ja seuranta sekä integrointi SIEM:iin	Opera- tiivinen palvelu- tuotanto
NM-RE-12	Roaming- ja reuna- valvonta	CDR-seuranta ja analysointi	Luvattomat tai vilpilliset puhelut	PBX-järjestelmän luomien puhelutietojen seuranta ja analysointi	Opera- tiivinen palvelu- tuotanto
NM-RE-13	Roaming- ja reuna- valvonta	PBX- aktiivisuuden valvonta	PBX-järjestelmään kohdistuvat luvattomat käyttöyritykset tai haitalliset toimet.	Tunkeutumisen havaitsemis- ja ehkäisyjärjestelmät (IDS/ IPS) Näillä järjestelmät valvo- taan verkkoliikennettä, analy- soidaan malleja ja annetaan hälytyksiä ja niiden avulla suojaudutaan, kun mahdol- lisia uhkia tai poikkeamia havaitaan.	Opera- tiivinen palvelu- tuotanto
NM-RE-14	Roaming- ja reuna- valvonta	Petosten havaitse- minen ja seuranta	Luvattomat tai vilpilliset puhelut	Epätavallisten tai vilpillisten puhelutoimintojen, kuten lisämaksullisen numeron väärinkäytön, tietullipetosten tai luvattoman puhelujen reitityksen, valvonta. Tämä tulisi toteuttaa reaaliaikaisella seurannalla, kuvioanalyysillä ja sääntöihin perustuvilla havaitsemismekanismilla.	Opera- tiivinen palvelu- tuotanto

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuul- linen taho
NM-RE-15	Roaming- ja reuna- valvonta	PBX-käyttö- oikeuksien ja todennuksen hallinnan valvonta	PBX-järjestelmään kohdistuvat luvat- tomat käyttö- yritykset tai haitalliset toimet.	Tehokkaiden kulunvalvonta- toimenpiteiden, kuten suojatun käyttäjän todennuksen ja sala- sanakäytäntöjen, käyttöön- otto, jolla pyritään estämään luvatonta pääsyä PBX-järjestel- mään. Käyttölokien seuranta ja käyttäjien toiminnan valvonnalla tunnistetaan ja tutkitaan epäilyttäviä kirjautu- misyrittäjiä tai luvatonta käyttöä.	Opera- tiivinen palvelu- tuotanto
NM-RE-16	Roaming- ja reuna- valvonta	PBX-järjestel- mälokien valvonta	PBX-järjestelmään kohdistuvat luvat- tomat käyttö- yritykset tai haitalliset toimet.	PBX-järjestelmän luomien järjestelmälokien seuranta ja analysointi voi antaa tietoa mahdollisista tietoturva- häiriöistä tai poikkeamista. Tähän sisältyy epätavallisten järjestelmätapahtumien, virheiden, epäonnistuneiden kirjautumisyrittysten tai luvat- tomien kokoonpanomuut- osten valvonta, jotka voivat viitata tietoturvaloukkauksiin tai PBX-järjestelmän manipulointiyrittäjiin.	Opera- tiivinen palvelu- tuotanto
NM-RE-17	Roaming- ja reuna- valvonta	Verkkoyhteys valvonta	Käyttäjän uudelle- nohjaus haitalli- selle palvelimelle	Uudelleenohjauksen estäminen/suojaus. Hälytys laukeaa, mikäli yritetään uudelleenohjausta.	Opera- tiivinen palvelu- tuotanto
NM-RE-18	Roaming- ja reuna- valvonta	Organisaatio- rajojen valvonta	Luvatonta käyttöä valvomattomien rajapintojen kautta	Julkisen operaattorin ja privaattiverkon välisten organisaatorajat ylittävien rajapintojen valvonta.	Opera- tiivinen palvelu- tuotanto
Network Monitoring – Core Network (control plane)					
NM-CNC-1	Ydinverkon (CP) valvonta	Palvelupoh- jaisen arkkitehtuurin kuormituksen valvonta	Saavuttamattomat verkkotoiminnot voivat aiheuttaa verkkokatkoksen	SBA-väylän verkon kuormi- tuksen seuranta, mahdollisesti SDN:n tuella ruuhkien välttämiseksi.	Opera- tiivinen palvelu- tuotanto
NM-CNC-2	Ydinverkon (CP) valvonta	Dynaaminen sisällön valvonta	Resurssien loppuminen ja järjestelmän käyttökatkos	Suojaus kasvavalta tai dynaamiselta sisällöltä (e.g. log tiedostot, lataukset) vasta- toimilla, kuten järjestelmän päätoiminnoista, kiintiöistä tai järjestelmän valvontatyö- kaluista erotetun erityisen tiedostojärjestelmän käytöllä sen varmistamiseksi, että vältetään skenaario, jossa tiedostojärjestelmä saavuttaa maksimikapasiteettinsa	Opera- tiivinen palvelu- tuotanto

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuul- linen taho
NM-CNC-3	Ydinverkon (CP) valvonta	CLI-huijaus- suojaus – teleyritysten välillä	Luottamus verk- koon murenee, loppukäyttäjiä huijataan.	Teleyritysten välillä soittavien puhelujen seuranta ja validointi	Opera- tiivinen palvelu- tuotanto
NM-CNC-4	Ydinverkon (CP) valvonta	CLI-huijaus- suojaus - välitys- palvelin	Luottamus verk- koon murenee, loppukäyttäjiä huijataan.	Saapuvien puhelujen valvonta ja validointi välityspalvelimen avulla	Opera- tiivinen palvelu- tuotanto
NM-CNC-5	Ydinverkon (CP) valvonta	CLI-huijaus- suojaus – hyökkäyksen kehityksen seuranta	Luottamus verk- koon murenee, loppukäyttäjiä huijataan.	CLI:tä koskevien asiakkaiden valitusten seuranta	Opera- tiivinen palvelu- tuotanto Asiakas- palvelut sekä laadun- valvonta
NM-CNU-1	Ydinverkon (UP) valvonta	Pakettivirran valvonta	Bottiverkot voivat suorittaa haitallisia toimia matkapuhe- linverkon avulla ja johtaa resurssien loppumiseen	Pakettivirtojen, kaistan- leveyden käytön ja verkon suorituskyky mittareiden seuranta	Opera- tiivinen palvelu- tuotanto
NM-CNU-2	Ydinverkon (UP) valvonta	Syvä pakettien tarkastus	Haitallinen liikenne verkossa	Liikenteen seuranta DPI: n avulla.	Opera- tiivinen palvelu- tuotanto
NM-CNU-3	Ydinverkon (UP) valvonta	Säädettävä sisällön valvonta	Liikenteen viivästykset	Liikenteen seuranta DPI:n avulla voidaan käyttää eri "tasoilla" ja siten suoritusky- kyvaikutuksia voidaan hallita	Opera- tiivinen palvelu- tuotanto
NM-RSPI-1	SIM-kortin etävalmis- teluinfra- struktuurin valvonta	Ulkoisten SIM-kortin etäprovisioin- tiliittymien valvonta	Haitallisen koodin tai tietojen lisää- minen käyttäjän laitteeseen tai verkkoon	SIM-kortin etävalmistelu- infrastruktuurin elementtien välisten liitännöiden valvonta	Opera- tiivinen palvelu- tuotanto
NM-RSPI-2	SIM-kortin etävalmis- teluinfra- struktuurin valvonta	Valmistelu- tietojen seuranta	Haitallisen koodin tai tietojen lisää- minen käyttäjän laitteeseen	eUICC:lle toimitettujen tietojen eheyden ja rakenteen seuranta.	Opera- tiivinen palvelu- tuotanto
NM-RSPI-3	SIM-kortin etävalmis- teluinfra- struktuurin valvonta	Luottamuksen turvallisuuden valvonta edellyttää SIM-kortin tarjoamista	Tunnistetietojen menettäminen voi johtaa järjestelmän vaarantumiseen	SIM-kortin etävalmistelun suojaavien tunnistetietojen turvallisuuden valvonta.	Opera- tiivinen palvelu- tuotanto

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuul- linen taho
NM-RSPI-4	SIM-kortin etävalmis- teluinfrast- ruktuurin valvonta	eUICC-infra- struktuurin toimittajan seuranta	Suojaamaton eUICC-etä-SIM- kortin lupainfra- struktuuri voi johtaa verkon vaarantumiseen	Valvotaan, että eUICC- etävalmisteluinfrastruktuurin toimittaja on sertifioitu GSMA:n mukaisesti ja vastaa sen käytön kriittisyystasoa.	Hankinta- toimi
NM-RSPI-5	SIM-kortin etävalmis- teluinfrast- ruktuurin valvonta	eUICC- toimittajan seuranta	Suojaamattomat eUICC-sirut voivat johtaa turvattomiin laitteisiin, jotka voivat hyökätä verkkoon	Valvotaan, että eUICC-etä- sirujen toimittaja on serti- fioitu GSMA:n mukaisesti ja vastaa sen käytön kriittisyys- tasoa (jos päätöksen tekee tämä osapuoli).	Hankinta- toimi
NM-RBM-1	RAN- ja runko- liityntä- verkon valvonta	Korkean riskin alueiden määritelmä	Liian paljon (kallista) tai liian vähän (hyökkäyksiä ei havaita)	Häirintä- ja valetukiasemien tehokkaan kontrolloimisen mahdollistamiseksi määrite- tään korkean riskin alueet (esim. suurlähetystöt, valtionraja, valtion virastot, sotilaskohteet).	Riskien- hallinta
NM-RBM-2	RAN- ja runko- liityntä- verkon valvonta	Väärä tukiaseman turvavalvonta	Tietojen luovutta- minen suojaamat- tomien rajapintojen kautta	Tarkkaile luovutusvirheitä ja muita verkon poikkeavuuksia mahdollisten väärennettyjen tukiasemien havaitsemiseksi.	Opera- tiivinen palvelu- tuotanto
NM-RBM-3	RAN- ja runko- liityntä- verkon valvonta	Backhaul- käyttäjätason turvallisuus- valvonta	Tietojen luovutta- minen suojaamat- tomien rajapintojen kautta	Valvotaan, että käyttäjä- tietojen siirto S1-U- ja X2-U- liitäntöjen kautta on ehyttä, luottamuksellista ja toistosuojattua	Opera- tiivinen palvelu- tuotanto
NM-RBM-4	RAN- ja runko- liityntä- verkon valvonta	Ilmaraja- pinnan turvallisuus- valvonta	Tietojen luovutta- minen suojaamat- tomien rajapintojen kautta	Valvotaan, että käyttäjätie- tojen siirto S1-U- ja X2-U- liitäntöjen kautta on ehyttä, luottamuksellista ja toistosuojattua	Opera- tiivinen palvelu- tuotanto
NM-RBM-5	RAN- ja runko- liityntä- verkon valvonta	Backhaul- ohjauskoneen turvallisuus- valvonta	Valvontatietojen muuttaminen voi johtaa käyttäjien turvailmoituksiin	Valvotaan, että ohjaustietojen siirto S1-C- ja X2-C-liitäntöjen kautta on ehyttä, luottamuk- sellista ja toistosuojattua	Opera- tiivinen palvelu- tuotanto

7.3 Varautumisen ja kriisistä palautumisen kontrollit

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuulinen taho
DP-RM-1	Riskinhallinta	Vakiomuotoisen riskienhallintastandardin ja viitekehyksen käyttö	Ennalta arvaamaton riski voi johtaa väärään priorisointiin ja valmistautumattomuuteen	Käytä riskienhallintastandardia ja viitekehystä, esim. ISO 31000, COSO, ISO/IEC 27005 tai YHDYSVALTAIN NIST SP 800-53	CSO, IT-osasto
DP-RM-2	Riskienhallinta	Henkilöstö resurssointi	Henkilöresurssien puute voi aiheuttaa kyvyttömyyden ylläpitää luotettavaa verkkoa.	Resurssitarveanalyysin sisällyttäminen riskienhallintasuunnitelmaan.	CSO, HR
DP-A-1	Saatavuus	OmaisuuDENhallintajärjestelmä	Päivitetyn omaisuusluettelon puute voi johtaa verkon tietoturvaheikkouksiin tai verkon toiminnan ongelmiin.	OmaisuuDENhallintajärjestelmän käyttö, joka kattaa: <ul style="list-style-type: none"> - Verkkolaitteet - Palvelimet ja datakeskukset - Verkko-osat - Turvallisuusinfrastruktuurin - Ohjelmisto- ja palvelutiedot - Fyysisen infrastruktuurin - Telineet ja kaapit - Verkon kaapeloinnin - Sähköinfrastruktuurin - Kriittiset tiedot - Ympäristön seurantajärjestelmät. 	IT-osasto, Työpaikan resurssit, CSO-toimisto, operatiivinen tiimi
DP-A-2	Saatavuus	OmaisuuDENvalvonta	OmaisuuDENvalvomattomuus voi johtaa verkon tietoturvaheikkouksiin tai verkon toiminnan ongelmiin	OmaisuuDENhallintajärjestelmän tietojen perusteella valvotaan: <ul style="list-style-type: none"> - Kriittisyyttä koskevia tietoja - Toimittajien tukitietoja - Fyysistä sijaintia ja turvatoimia - Vastuuhenkilötietoja - Verkkoinfrastruktuuri kaavioita - OmaisuuDEN luovutustietoja - Varaston seurantatietoja. 	IT-osasto, Työpaikan resurssit, CSO-toimisto, operatiivinen tiimi
DP-A-3	Saatavuus	Julkisen varoitustajärjestelmän (PWS) käyttö	Viivästyneet katastrofi/onnettomuustiedot voivat johtaa ihmishenkien menetyksiin	PWS-järjestelmän käyttö katastrofiviestinnässä julkisessa tai yksityisessä verkossa lakisääteisistä ja turvallisuusvaatimuksista riippuen.	CSO-toimisto, operatiivinen tiimi, HR

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuulinen taho
DP-A-4	Saatavuus	Palvelujen saatavuus – kansalliset verkkovierailut	Käyttäjä ei voi soittaa puheluita tai saada data-yhteyttä katastrofi/hätätilanteessa	Ota käyttöön kansallinen verkkovierailu.	Operaatiivinen tiimi, CSO:n toimisto
DP-A-5	Saatavuus	Palvelun saatavuus – laskutus	Käyttäjä ei voi soittaa puheluita tai saada data-yhteyttä katastrofitilanteessa	Laskutusjärjestelmän säätäminen: Häätätilanteessa poistetaan tileillä mahdollisesti olevat estot puheluihin tai data-yhteyksien soittamiseen.	Operaatiivinen tiimi, CSO:n toimisto
DP-A-6	Saatavuus	Vaihtoehtoinen runkoverkko-yhteys	Palvelu ei ole käytettävissä rikkoutuneen takaisinkytkennän vuoksi	Tukiaseman riskiprofiilista riippuen: Runkoliityntäyhteys järjestetään satelliittiviestintälinkin kautta.	Operaatiivinen tiimi, CSO:n toimisto
DP-A-7	Saatavuus	Liikenteen priorisointi	Liikennepuuhkat voivat johtaa siihen, että kriittinen liikenne ei pääse läpi.	Liikenteen priorisointi kansallisen turvallisuuden kannalta käyttämällä Quality of Service (QoS) -luokkia katastrofitoimintaan.	Operaatiivinen tiimi, CSO:n toimisto
DP-A-8	Saatavuus	Vikasieto-ominaisuuksien käyttö	Verkko ei ole käytettävissä ylikuormituksen tai tuhoutumisen vuoksi	Vikasieto-ominaisuudet otetaan käyttöön tukiasemien ja verkkotoimintojen säilyttämiseksi, esim. UPS, uudet pilvi-instanssit.	Operaatiivinen tiimi, CSO:n toimisto
DP-A-9	Saatavuus	Varaosien hallinta	Palvelu ei ole käytettävissä puuttuvan varaosan vuoksi	Varaosien hallinta: Lisätään varaosien varastomääriä välttämättömille komponenteille ja tehdään ennakkoon varaosien vaihtosopimuksia.	Operaatiivinen tiimi, CSO-toimisto, hankintatiimi
DP-A-10	Saatavuus	Varavoima	Verkko ei toimi	Varavoimakone ja polttoainetta hankitaan kaikille verkon kriittisille osille, myös erillisverkoille.	Operaatiivinen tiimi, CSO:n toimisto

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuulinen taho
DP-A-11	Saatavuus	Ydintietoliikenneverkon uudet toiminnot	Ydinverkon toimintojen menettäminen voi johtaa siihen, että verkko ei ole käytettävissä	Kartoitetaan ennakoon vaihtoehtoiset instanssit, joissa verkkotoiminnot voidaan luoda uudestaan ja ottaa käyttöön katastrofin sattuessa.	Operaatiivinen tiimi, pilvipalvelujen tarjoaja
DP-A-12	Saatavuus	Uusi runkoverkko	Ydinverkon menetys	Riskiprofiili huomioiden tehdään sopimus sellaisen toimijan kanssa, jolla on kuorma-autoissa tai konteissa toimivia verkkolaitteita. Ne otetaan käyttöön, jos ydinverkko menetetään.	CSO, operaatiivinen tiimi, hankinta
DP-A-13	Saatavuus	Kehän suojaus	Fyysisten kontrollien puutteet voivat johtaa käytettävyyden, eheyden ja luottamuksellisuuden sekä koko verkon tuhoutumiseen	Datakeskusten ja tukiasemien fyysinen suojaus myös alihankkijoiden sekä erillisverkkojen ja niitä tukevan IT-infran osalta. Tämä voi sisältää aidat, portit, esteet ja valvontajärjestelmät sisään- ja uloskäyntipisteiden seuraukselliseksi ja valvomiseksi.	CSO-tiimi
DP-A-14	Saatavuus	Fyysinen kulunvalvonta	Fyysisten kontrollien puutteet voivat johtaa käytettävyyden, eheyden ja luottamuksellisuuden sekä koko verkon tuhoutumiseen	Fyysisiä kulunvalvontatoimenpiteitä, kuten avainkortteja tai PIN-pohjaisia järjestelmiä, toteutetaan konealien ja tukiasemien eritukipisteissä myös alihankkijoiden sekä erillisverkkojen osalta.	CSO-tiimi
DP-A-15	Saatavuus	Videovalvonta	Fyysisten kontrollien puutteet voivat johtaa käytettävyyden, eheyden ja luottamuksellisuuden sekä koko verkon tuhoutumiseen	Otetaan käyttöön videovalvontajärjestelmät, joissa kamerat on sijoitettu strategisesti valvomaan laitoksen sisäänkäyntejä, uloskäyntejä, käytäviä ja kriittisiä alueita. On huolehdittava siitä, että kameroista ei näe käytössä olevia PIN-koodeja tai salasanoja.	CSO-tiimi
DP-A-16	Saatavuus	Fyysisen tunkeutumisen havaitseminen	Fyysisten kontrollien puutteet voivat johtaa käytettävyyden, eheyden ja luottamuksellisuuden sekä koko verkon tuhoutumiseen	Fyysisen tunkeutumisen havaitsemisjärjestelmät, joilla havaitaan luvattomat tunkeutumisyrietykset tai epäilyttävä toiminta datakeskuksissa tai tukiasemissa, alihankkijoiden ja erillisverkkojen tiloissa. Näihin järjestelmiin voi kuulua liiketunnistimia, ovitunnistimia ja tärinän ilmaisimia, jotka laukaisevat hälytyksiä tai ilmoituksia vartijoille.	CSO-tiimi

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuulinen taho
DP-A-17	Saatavuus	Turvallisuushenkilöstö	Fyysisten kontrollien puutteet voivat johtaa käytettävyyden, eheyden ja luottamuksellisuuden sekä koko verkon tuhoutumiseen	Koulutettu turvahenkilöstö, joka on sijoitettu datakeskukseen tai päivystämään tukiasemia valvomaan pääsyä, suorittamaan partiointia, reagoimaan tapahtumiin ja varmistamaan turvallisuusprotokollien noudattamisen.	CSO-tiimi
DP-A-18	Saatavuus	Paloilmoitinjärjestelmät	Infrastruktuurin tuhoutuminen	Datakeskukset ja tukiasemat on varustettu paloilmoitinjärjestelmillä, kuten savunilmaisimilla, lämpöantureilla ja palovaroittimilla. Palonsammutusjärjestelmät, kuten sprinklerit tai kaasupohjaiset sammutusjärjestelmät, asennetaan myös potentiaalini minimoimiseksi. Tukiasemien osalta on otettava huomioon, että savu voi kulkeutua pitkiä matkoja ja aiheuttaa vääriä positiivisia tuloksia.	CSO-tiimi
DP-A-19	Saatavuus	Ympäristövalvonta	Infrastruktuurin tuhoutuminen	Asianmukaisten ympäristötarkastusten käyttö laitteiden optimaalisten olosuhteiden varmistamiseksi. Tämä sisältää lämpötilan ja kosteuden valvontajärjestelmät, LVI-järjestelmät (lämmitys, ilmanvaihto ja ilmastointi), UPS (Universal Power Supply) ja varavirtageneraattorit sähkökatkosten ja häiriöiden vaikutusten lieventämiseksi.	CSO-tiimi
DP-A-20	Saatavuus	Turvalliset telineet ja kaapit	Fyysisten kontrollien puutteet voivat johtaa käytettävyyden, eheyden ja luottamuksellisuuden sekä koko verkon tuhoutumiseen	Tietojen sisällä olevat laitteet ja kaapit, jotka on suojattu lukoilla tai lukituissa tiloissa luvattoman laitteistoon koskemisen estämiseksi myös erillisverkoissa.	CSO-tiimi
DP-A-21	Saatavuus	Vierailijoiden hallinta	Fyysisten kontrollien puutteet voivat johtaa käytettävyyden, eheyden ja luottamuksellisuuden sekä koko verkon tuhoutumiseen	Ota käyttöön tiukat vierailijoiden hallintaprotokollat, jotka vaativat kävijöitä kirjautumaan sisään, antamaan henkilöllisyystodistuksen ja olemaan valtuutetun henkilöstön mukana paikan päällä. Vierailijoiden pääsy on yleensä rajoitettu tietyille vierailualueille ja sitä valvotaan tarkasti. Alihankkijoilla on yleensä ajallisesti rajoitettu ja rajoitettu pääsy alueelle. Yhteisiä keskuksia varten olisi oltava selkeät yhteisesti hyväksytyt menettelyt.	CSO-tiimi

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuul- linen taho
DP-PF-1	Kumppanien kautta realisoituvat riskit	Verkon seuranta poikkeamien varalta	Havaitsematta jääneet poikkeamat voivat johtaa vakaviin vaikutuksiin ja liian myöhäisiin korjaustoimiin	Hankintatoimen kontrollit	IT-osasto, operatiivinen tiimi, hankinta, pilvipalveluntarjoaja
DP-PF-2	Kumppanien kautta realisoituvat riskit	Hankintojen valvonta	Riittävien hankintojen turvatarkastusten/testauksen puute voi johtaa siihen, että tuotteilla ja palveluilla ei ole riittävää tietoturvaa, mikä voi johtaa siihen, että hyökkääjät vaarantavat verkon toiminnan	Hankintatoimen kontrollit	IT-osasto, operatiivinen tiimi, hankinta, pilvipalveluntarjoaja
DP-PF-3	Kumppanien kautta realisoituvat riskit	Kumppanin suorituskyvyn testaaminen	Suojaustoimintojen validoinnin ja kumppanien tietoturvan suorituskyvyn puute voi johtaa heikkoon suojauksen laatuun ja hyödynnettävissä oleviin haavoittuvuuksiin verkossa	Hankintatoimen ja valvonnan kontrollit	IT-osasto, operatiivinen tiimi, hankinta, pilvipalveluntarjoaja
Ulkoiset kyberhyökkäykset					
DP-ECA-1	Ulkoiset kyberhyökkäykset	Varasuunnitelma	Puuttuvat tai saavuttamattomat varmuuskopiot tai tiedot voivat estää palauttamisen eikä verkkoa saada toimimaan.	Omaisuuksiluokituksen kriittisyyden ja riskin perusteella olisi kehitettävä varmuuskopiointi- ja tietojen peilaussuunnitelma, joka sisältää matkaviestinverkon tiedot.	IT-osasto, operatiivinen tiimi
DP-ECA-2	Ulkoiset kyberhyökkäykset	Maantieteellinen monimuotoisuus varmuuskopiointia ja peilausta varten	Alueellinen katastrofi voi tuhota ennallistamiseen tarvittavat tiedot	Useiden sijaintien käyttö peilaukseen ja varmuuskopiointiin. Erityiset maantieteelliset riskit olisi otettava huomioon. Jos varmuuskopioita tai peilauksia tehdään yllämainittujen rajojen, on tutkittava oikeudelliset seuraukset	IT-osasto, operatiivinen tiimi
DP-ECA-3	Ulkoiset kyberhyökkäykset	Varmuuskopioiden turvallisuus	Tietovuoto	Varmuuskopioihin pääsy estetään tietoturvaliikkeen mukaisilla pääsynhallintakontrollilla.	IT-osasto, operatiivinen tiimi

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuul- linen taho
DP-ECA-4	Ulkoiset kyberhyök- kät	Varmuus- kopiointi palautetaan	Varmuuskopiointia ei saada palau- tettua eikä verkkoa toimimaan menet- telyn puutteen vuoksi	Varmuuskopioiden palautta- miseksi on oltava käytössä ennalta suunnitellut ja harjoi- tellut menettelyt. Menette- lyissä on otettava huomioon salausavainten saatavuus, jos varmuuskopiot salataan katastrofin aikana.	IT-osasto, opera- tiivinen tiimi
DP-ECA-5	Ulkoisen kyber- hyökkäys	Lainsää- dännön noudatta- minen katastrofi- tilanteessa	Lakisääteisten velvoitteiden laiminlyönti ja siitä aiheutuvat turvalli- suusriskit ja haitat yhteiskunnalle ja yksilöille	Listataan yritystä koskevat lainsäädännön vaatimukset säännöllisesti ja arvioidaan, kyetääkö vaatimukset toteuttamaan kaikissa tilan- teissa. Tehdään tarvittaessa korjaustoimenpiteet.	IT-osasto, opera- tiivinen tiimi
DP-ECA-6	Ulkoisen kyber- hyökkäys	Varmuus- kopiointin ja palautuksen testaus	Varmuuskopiota ei voi palauttaa. Menetetään tietoja ja verkkoa ei saada toimimaan	Varmuuskopiointi- ja peilaus- menettelyt on testattava säännöllisesti sen varmistami- seksi, että varmuuskopiot voidaan palauttaa onnistu- neesti, ja näiden testien tulokset on dokumentoitava. Tarvittaessa tehdään korjaus- toimenpiteet, kunnes palautus toimii.	IT-osasto, opera- tiivinen tiimi
DP-ECA-7	Ulkoisen kyber- hyökkäys	Muutoksen- hallintasuun- nitelma	Puuttuvat menet- telyt voivat johtaa korjaamattomiin järjestelmiin, joita hyökkääjä voi hyödyntää	Muutoksenhallintasuunnitel- massa määritellään testaus, validointi, menettelyt ja vastuut minkä tahansa ohjelmiston tai laitteiston asentamiseen, muuttamiseen, testaamiseen, kovettamiseen ja päivittämiseen. Viestintä olisi sisällytettävä muutoksenhallinta- suunnitelmaan.	Hankinta IT-osasto, opera- tiivinen tiimi
DP-ECA-8	Ulkoisen kyber- hyökkäys	Turvalli- suuden kovennusten hallinta	Puuttuva kovettu- minen mahdollistaa kyberhyökkäyksen	Tietoliikenneinfrastruktuurien kovettamisohjeistuksen toteuttaminen tulee olla osa hankintaa, tuotteen hyväksymistä ja ohjelmiston käyttöönottoa.	Hankinta IT-osasto, opera- tiivinen tiimi

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuul- linen taho
DP-ECA-9	Ulkoinen kyber- hyökkäys	IT-järjestel- miin tunkeu- tumisen havaitse- minen	Hyökkääjät voivat murtautua matka- puhelinverkon taustalla olevaan IT-infrastruktuuriin eikä sitä huomata	Tunkeutumisen havaitsemis- järjestelmän (IDP) / tunkeutu- misenestojärjestelmän (IPS) käyttöönotto.	IT-osasto, opera- tiivinen tiimi
DP-ECA-10	Ulkoinen kyber- hyökkäys	Lokien tallennus	Hyökkääjät pois- tavat paikallisia lokeja peittääkseen jälkensä, eikä hyökkäyksen koko laajuutta siksi tiedetä	Lokit on tallennettava paikalli- sesti ja keskitetysti.	IT-osasto, opera- tiivinen tiimi
DP-ECA-11	Ulkoinen kyber- hyökkäys	Keskitetty lokianalyysi	Lokikorrelaatio ei ole mahdollista ja osa hyökkäyksestä voi jäädä huomaamatta.	Lokien keskitetty analyysi (mukaan lukien korrelaatio).	IT-osasto, opera- tiivinen tiimi
DP-ECA-12	Ulkoinen kyber- hyökkäys	Lokien suojaus	Hyökkääjä voi muokata tai poistaa lokeja estääkseen hyökkäyksen havaitsemisen	Lokitietojen poistaminen ja muuttaminen estetään kokonaan.	IT-osasto, opera- tiivinen tiimi
DP-ECA-13	Ulkoinen kyber- hyökkäys	Lokin aikaleima	Korrelaatiota, perussyyanalyysiä tai hyökkäyksen aikajanaa ei voida määrittää ilman luotettavia aikaleimoja.	Lokien aikaleima on oltava käytössä.	IT-osasto, opera- tiivinen tiimi

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuul- linen taho
DP-ECA-14	Ulkoinen kyber- hyökkäys	Synkronoidun ajan validointi	Korrelaatiota, perussyyanalyysiä tai hyökkäyksen aikajanaa ei voida määrittää ilman luotettavia aikaleimoja	Säännöllinen synkronoidun ajan validointi verkossa.	IT-osasto, opera- tiivinen tiimi
DP-ECA-15	Ulkoinen kyber- hyökkäys	Lokin tarkistus- menettely	Lokeja ei tarkisteta ja hyökkäys jää havaitsematta	Lokitiedot analysoidaan ja havainnot käsitellään vastuuhenkilöiden toimesta säännöllisesti.	IT-osasto, opera- tiivinen tiimi
DP-ECA-16	Ulkoinen kyber- hyökkäys	Automaat- tinen lokianalyysi	Lokitietoja on niin paljon, ettei niitä ehditä analysoida ja hyökkäys jää havaitsematta	Reaaliaikaisen automaattinen lokianalyysin ja siihen sisälly- tetyn automaattihälytyksen käyttäminen.	IT-osasto, opera- tiivinen tiimi
DP-ECA-17	Ulkoinen kyber- hyökkäys	IT &; Telco-loki- korrelaatio	IT- ja telekommuni- kaatioprotokollia käyttäviä hyökkä- yksiä ei välttämättä tunnisteta ajoissa	Puhelinlokien ja IT-lokien yhdistäminen hybridihyök- käyksien havaitsemiseksi.	IT-osasto, opera- tiivinen tiimi
DP-ECA-18	Ulkoinen kyber- hyökkäys	Kirjaamisen laajuus	Tarpeettomien tai tietoturvan kannalta kriittisten tietojen kirjaaminen järjestelmään voi johtaa käyttäjän tietosuojasään- nösten rikkomiseen tai tietoturvan heikkenemiseen	Analysoi, mitä tietoja järjestel- mään on välttämätöntä kirjata ja mitä tietoja ei saa kirjata. Kouluta käyttäjät analysoinnin perusteella kirjaamaan vain tarpeellinen tieto. Poista tarpeeton ja tietoturvan kannalta vaarallinen tieto järjestelmästä.	IT-osasto, opera- tiivinen tiimi

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuullinen taho
DP-ECA-19	Ulkoiset kyberhyökkäykset	Verkkoarkkitehtuuri ja rajapinnat	Verkkotopologian heikko suunnittelu voi johtaa havaitsemattomiin hyökkäysten onnistumiseen	Suunnittele verkkoarkkitehtuuri, rajapinnat, kaavoitusdokumentaatio huolellisesti käyttäen tietoturva-asiantuntijoita apuna suunnittelussa.	IT-osasto, operatiivinen tiimi
DP-ECA-20	Ulkoiset kyberhyökkäykset	Palomuurien signaali	Signaalointipalomuurien puute paljaissa rajapinnoissa voi johtaa verkon vaarantumiseen	Signaalointirajapintoja varten tehdään erityisiä uhkatiedustelua sisältäviä signaalointipalomuuereja, jotka valvovat liikennettä, luovat lokeja ja automatisoivat niiden käsittelyn.	IT-osasto, operatiivinen tiimi
DP-ECA-21	Ulkoiset kyberhyökkäykset	Vahvojen telealgoritmien käyttö	Heikkojen algoritmien käyttö voi johtaa onnistuneeseen hyökkäykseen ja verkon vaarantumiseen.	Käytetään vahvoja ilmarajapinta-algoritmeja. Heikommat algoritmit poistetaan käytöstä ja estetään niiden käyttö yksityisessä verkossa, jossa on tunnettuja laitteita.	Operatiivinen tiimi
DP-ECA-22	Ulkoiset kyberhyökkäykset	Konfiguraation valvonta	Havaitsemattomat kokoonpano- ja mallimuutokset voivat johtaa laajoihin tietoturvaavaoittuvuuksiin.	Suojauskokoonpanon muutoksia seurataan. Esimerkiksi Kubernetes kirjataan tai muutokset Software Defined Networks (SDN) -ohjaimen kokoonpanoon liikenteen ohjausta tai tilaajaprofiilitietoja varten.	Operatiivinen tiimi
DP-ECA-23	Ulkoiset kyberhyökkäykset	Altistuksen testaus	Havaitsematon altistuminen voi johtaa kyberhyökkäyksen onnistumiseen ja järjestelmän vaarantumiseen	Toteutetaan turvallisuusarvioita ja -tarkistuksia paljastamaan televiestintäomaisuuden ja heikkojen kokoonpanojen, kuten julkisten rajapintojen, verkkovierailurajapintojen, altistumista.	Operatiivinen tiimi, IT-osasto

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuullinen taho
DP-ECA-24	Ulkoinen kyberhyökkäys	Testaus- ja validointisuunnitelma	Uudet ohjelmistot voivat tuoda mukanaan uusia haavoittuvuuksia tai johtaa järjestelmänepävakauteen ja kyberhyökkäyksen onnistumiseen	Kehitä testaussuunnitelma osana muutoksenthallintaprosessia. Testaussuunnitelman olisi katettava toiminta- ja turvallisuustestaus ja testauksen on mentävä hyväksytysti läpi ennen tuotantoon siirtoa.	IT-osasto, operatiivinen tiimi
DP-ECA-25	Ulkoinen kyberhyökkäys	Toimittajan tietoturvesti-Testin kattavuus	Puutteelliset tietoturvestit voivat johtaa korjaamattomiin ohjelmistojen haavoittuvuuksiin, jotka mahdollistavat kyberhyökkäyksen onnistumisen	Toimittajan tietoturvestien sisältö ja tulokset analysoidaan. Tämän perusteella tehdään tarvittaessa täydentävä testisuunnitelma. Sen tulisi sisältää kattavat tietoturvestit (DAST, SAST, pentesting) ja täydentää toimittajan tekemä testauspuutteiden osalta. Testausten tulosten perusteella vaaditaan korjaussuunnitelma, jonka toteutusta valvotaan.	Hankinta IT-osasto, operatiivinen tiimi
DP-ECA-26	Ulkoinen kyberhyökkäys	Ohjelmistotestaus	Puutteellisesta ohjelmistotestauksesta voi aiheutua järjestelmäkatkos, verkkokatkos tai se voi mahdollistaa kyberhyökkäyksen onnistumisen.	Testisuunnitelmaan tulee sisällyttää testimenetelmä (esim. laboratoriosolmujen tai alhaisen kriittisyyden solmujen käyttö), jotta vältetään kaskadivaikutukset, suuremmat seisokit tai tapahtumat.	IT-osasto, operatiivinen tiimi
DP-ECA-27	Ulkoinen kyberhyökkäys	Toimittajan validointi	Puutteelliset tietoturvestit voivat johtaa haavoittuvuuksia sisältäviin järjestelmiin tai komponentteihin, jotka mahdollistavat kyberhyökkäyksen onnistumisen	Toimittajalta pyydetään tiedot suoritetuista tietoturvesteistä. Testausten tulee olla riittävän kattavia (DAST, SAST, pentesting), jotta sen perusteella voidaan arvioida toimittajan kyky toimittaa turvallisia järjestelmiä tai komponentteja.	Hankinta-tiimi IT-osasto, operatiivinen tiimi
DP-ECA-28	Ulkoinen kyberhyökkäys	Testin dokumentointi	Epäselvä testien kattavuus ja löydösten käsittely voivat johtaa havaitsemattomiin haavoittuvuuksiin, jotka mahdollistavat kyberhyökkäyksen onnistumisen	Turvatestisuunnitelmassa olisi kuvattava, mitä asiakirjoja testeistä ja niiden tuloksista vaaditaan. Tulosten käsittelyprosessin olisi myös oltava osa turvatestisuunnitelmaa.	Hankinta-tiimi IT-osasto, operatiivinen tiimi

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuul- linen taho
DP-ECA-29	Ulkoinen kyber- hyökkäys	Korkean riskin toimittaja- testaus	Korkean riskin toimittajat voivat aiheuttaa suuremman riskin järjestelmälle	Turvatestaussuunnitelmaan olisi sisällyttävä korvaavia toimenpiteitä suuririskisten toimittajien käytölle esimer- kiksi ylimääräisten testitapa- usten ja seurantavaatimusten avulla	Hankinta- tiimi IT-osasto, opera- tiivinen tiimi
DP-ECA-30	Ulkoinen kyber- hyökkäys	Tietoturvan hyväksyntä- testaus toimittajan osalta	Ohjelmisto voi sisältää haavoittu- vuuksia, jotka mahdollistavat kyberhyökkäyksen onnistumisen.	Toimittajan tietoturvestin tulokset käydään läpi ja tulok- sissa esiintyvien puutteiden osalta vaaditaan sekä valvo- taan toimittajan korjaavien toimenpiteiden suunnitelma ja toteutus.	Hankinta IT-osasto, opera- tiivinen tiimi
DP-ECA-31	Ulkoinen kyber- hyökkäys	Muutoksen- hallinta- ja korjaussuun- nitelma	Muutosprosessin puutteet voivat aiheuttaa verkko- katkoksen ja mahdollistaa kyber- hyökkäyksen onnis- tumisen verkkoon	Kehitä muutoksenhallinta- ja korjausprosessit, joihin sisältyy hyväksymistesta- ukset. Niiden läpimeno hyväksytysti on edellytys tuotantoon siirtoon.	IT-osasto, opera- tiivinen tiimi
DP-ECA-32	Ulkoinen kyber- hyökkäys	Muutos- pyyntö- prosessi	Asianmukaisten hyväksymisten puute muutoksessa voi aiheuttaa talou- dellisia menetyksiä, verkkokatkoksen ja mahdollistaa kyber- hyökkäyksen onnis- tumisen verkkoon	Luo virallinen prosessi muutospyyntöjen lähettämiseksi, mukaan lukien tarvittavat asiakirjat ja hyväksyntävaatimukset.	IT-osasto, opera- tiivinen tiimi, CSO
DP-ECA-33	Ulkoinen kyber- hyökkäys	Muutosten hyväksyn- täprosessi	Asianmukaisten hyväksymisten puute muutoksessa voi aiheuttaa talou- dellisia menetyksiä, verkkokatkoksen ja mahdollistaa kyber- hyökkäyksen onnis- tumisen verkkoon	Määritä muutospyyntöjen hyväksymisen tai hylkäämisen kriteerit ja vastuut varmis- taen, että asianmukaiset sidosryhmät ovat mukana päätöksentekoprosessissa.	IT-osasto, opera- tiivinen tiimi, CSO

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuul- linen taho
DP-ECA-34	Ulkoinen kyber- hyökkäys	Muutoksen vaikutusten arviointi	Virheellinen muutos voi aiheuttaa verkko- katkoksen ja mahdollistaa kyber- hyökkäyksen onnis- tumisen verkon kriittisiin osiin	Arvioi ehdotettujen muutosten mahdollisia vaiku- tuksia esimerkiksi järjestel- miin, prosesseihin, resurs- seihin, turvallisuuteen ja sidosryhmiin, kuten kriittiseen infrastruktuuriin sekä asiak- kaisiin. Tämä arviointi auttaa määrittämään muutokseen liittyvän riskin tason ja kontrollitoimenpiteiden yksityiskohdat.	IT-osasto, opera- tiivinen tiimi
DP-ECA-35	Ulkoinen kyber- hyökkäys	Muutosten priorisointi	Korjaamaton kriit- tinen järjestelmä voi aiheuttaa verkkokatkoksen ja mahdollistaa kyber- hyökkäyksen onnis- tumisen verkon kriittisiin osiin	Priorisoi muutokset niiden kiireellisyyden, vaikutuksen, altistumisen, matkapuhelin- verkon solmukohdan kriitti- syyden ja lakisääteisten vaati- musten ja kriittisen infra- struktuurin asiakkaiden yhdenmukaistamisen perus- teella. Tämä auttaa kohdentaa resurssit tehokkaasti ja varmistamaan, että kriittisiin muutoksiin puututaan nopeasti.	IT-osasto, opera- tiivinen tiimi
DP-ECA-36	Ulkoinen kyber- hyökkäys	Muutos- viestintä	Muutoksilla voi olla vaikutuksia riippu- vaisiin järjestelmiin ja kumppaneihin, joiden on varaudut- tava mahdollisiin vaikutuksiin	Laadi viestintäsuunnitelma, jolla tiedotetaan asiaankuulu- ville sidosryhmille, kuten riipu- puvaisille kriittisen infrastruk- tuurin tarjoajille tai asiakkaille tulevista muutoksista, niiden vaikutuksista ja tarvittavista toimista tai valmisteluista. Systemaattinen, ajantasainen ja selkeä viestintä auttaa mini- moimaan häiriöt ja mahdol- liset taloudelliset seuraukset.	IT-osasto, opera- tiivinen tiimi
DP-ECA-37	Ulkoinen kyber- hyökkäys	Muutosten testaus ja validointi	Testaamattomat muutokset voivat aiheuttaa verkko- katkoksia ja kyber- hyökkäyksen onnistumisen	Luo menettelyt muutosten testaamiseksi ja validoimiseksi kontrolloidussa ympäristössä ennen niiden toteuttamista tuotantoympäristössä (katso testaussuunnitelma).	IT-osasto, opera- tiivinen tiimi
DP-ECA-38	Ulkoinen kyber- hyökkäys	Muutoksen toteutus	Strukturoimat- toman muutoksen toteutus voi johtaa verkkokatkoksiin ja kyberhyökkäyksen onnistumiseen	Määritä hyväksytyjen muutosten toteuttamisen vaiheet ja vastuut, mukaan lukien tarvittava koordinaatio eri ryhmien tai osastojen kanssa. Korjaussuunnitel- massa tai ohjelmiston käyt- töönottosuunnitelmassa on huomioitava matkapuhelin- verkon sisäiset kriittisyydet ja riippuvuudet tekemällä ohjel- mistopäivitykset tarvittaessa vaiheittain.	IT-osasto, opera- tiivinen tiimi

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuulinen taho
DP-ECA-39	Ulkoinen kyberhyökkäys	Muuta dokumentaatiota	Dokumentoimat tomat muutokset vaikeuttavat mahdollisten virheiden korjaamista ja verkkokatkoksista palautumista.	Ylläpidä dokumentaatiota kaikista muutoksista ajantasaisesti, mukaan lukien muutosten tarkoitus, laajuus, toteutustiedot ja niihin liittyvät riskit tai ongelmat sekä eri vaiheiden hyväksynät. Tämä dokumentaatio, johon on tarjolla erilaisia muutoshallintatyökaluja, tehostaa auditointeja, viankorjausta ja tiedon jakamisesta sekä parantaa muutosprosessin laatua. Omaisuustietokanta ja ohjelmistoluettelo (SBOM) on päivitettävä vastaamaan viimeisintä tilaa esimerkiksi korjausten yhteydessä.	IT-osasto, operatiivinen tiimi
DP-ECA-40	Ulkoinen kyberhyökkäys	Muutoksen tarkastelu ja arviointi	Muutoksen aiheuttama, aluksi käyttäjille huomaamaton virhe voi johtaa pitkällä aikavälillä merkittäviin tietoturvaluutteisiin ja verkko-ongelmiin.	Tarkista ja arvioi toteutetun muutoksen vaikutus verkon suorituskykyyn, turvallisuuteen ja käytettävyyteen heti muutoksen tuotantoon siirron jälkeen.	IT-osasto, operatiivinen tiimi
DP-ECA-41	Ulkoinen kyberhyökkäys	Automaattinen vastaus	Vastauksen viivästyminen voi antaa hyökkääjälle mahdollisuuden murtautua tietoihin tai järjestelmiin laajasti	Automaattisen hyökkäyksen vastausjärjestelmän käyttö (SOAR).	IT-osasto, operatiivinen tiimi
DP-ECA-42	Ulkoinen kyberhyökkäys	Loppukäyttäjän käyttöoikeuksien valvonta	Puutteellinen tai heikko todennus voi antaa luvattomille käyttäjille pääsyn verkon tietoihin ja mahdollistaa kyberhyökkäyksen	Loppukäyttäjän pääsyyn matkapuhelinverkkoon on aina käytettävä 3GPP TS33.501 -suojausprotokollia.	Operatiivinen tiimi
DP-ECA-43	Ulkoinen kyberhyökkäys	Ydinverkon käytönvalvonta (sisäinen)	Luvaton pääsy ydintietoliikenneverkkoon	Ydinverkko ja verkkovierailuyhteys voidaan suojata käyttämällä turvaominaisuuksia, kuten Service Communication Proxy (SCP) laajennetuilla turvaominaisuuksilla, NRF-verkkoarkistotoiminnon käytöllä, TLS:llä ja OAuth:illa OAuth:n valtuuttamiseksi. Nämä ominaisuudet on paitsi toteutettava, myös otettava käyttöön.	Operatiivinen tiimi

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuulinen taho
DP-ECA-44	Ulkoisen kyberhyökkäys	Ydinverkon käytönvalvonta (ulkoisen)	Luvaton pääsy ydintietoliikenne verkkoon	Runkoverkko ja verkko-vierailuyhteys suojataan signalointipalomuureilla.	Operaatiivinen tiimi
DP-ECA-45	Ulkoisen kyberhyökkäys	RAN-käytön valvonta	Luvaton pääsy RANIin ja ytimeen	Radio Access Network (RAN) -pääsynhallinnan tulisi käyttää VPN/IPSec ydinverkkoon ja uusien tukiasemien tulisi ilmoittautua standardoiduilla keinoilla, kuten 3GPP TS 33.310.	Operaatiivinen tiimi, IT-osasto
DP-ECA-46	Ulkoisen kyberhyökkäys	Vanha käyttö-oikeuksien hallinta	Luvaton pääsy vanhan järjestelmän kautta.	Yksi merkittävä heikkous matkapuhelinoperaattoreiden pääsynvalvonnassa ovat vanhat käyttöönotot, joissa on hyvin usein paljon heikompi pääsynhallinta esim. ryhmätilit, kovakoodatut salasanaat, ei todennusta ollenkaan jne. Näiden heikkouksien kontrolloimiseksi tulisi ryhmätilit poistaa ja muutoin kirjautumisia seurata reaaliaikaisesti ja lokeja analysoida tavanomaista enemmän. On myös tehtävä aktiivinen etenemissuunnitelma vanhojen vähemmän turvallisten laitteiden asteittaiseksi poistamiseksi.	Operaatiivinen tiimi
DP-ECA-47	Ulkoisen kyberhyökkäys	Tilin käytännöt	Hyökkääjä pääsee järjestelmään hankkimalla uuden tilin käyttäjän manipuloinnin avulla.	Tilikäytäntöjen luominen ja kouluttaminen loppukäyttäjille, runkoverkolle, verkko-vierailuille, RAN-, OSS/BSS- ja pilvipalveluille.	IT-osasto, operaatiivinen tiimi, myynti
DP-ECA-48	Ulkoisen kyberhyökkäys	Tilin luominen ja hallinta - valmistelu	Käytäntöjen noudattamatta jättäminen voi johtaa siihen, että tileillä on liikaa oikeuksia.	Käytä automaattisia työkaluja tilin luomiseen varmistaaksesi laadun ja käytäntöjen noudattamisen, esim. OSS/BSS ja pilvi.	IT-osasto, operaatiivinen tiimi

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuullinen taho
DP-ECA-49	Ulkoinen kyberhyökkäys	Tilin luominen ja hallinta – hyväksymisprosessi	Käytäntöjen noudattamatta jättäminen voi johtaa siihen, että tileillä on liikaa oikeuksia	Hyväksyntäprosessit: Ota käyttöön tilin luomista koskevat muodolliset hyväksyntäprosessit, jotka edellyttävät valtuutusta asianmukaisilta hallintatasoilta. Tähän olisi sisällyttävä SIM-kortin vaihtohyökkäysten estäminen (esim. menettely, jonka mukaan uuden tilin / kadonneen puhelimen tapauksessa on annettava passi).	IT-osasto, operatiivinen tiimi, asiakaspalvelutiimi
DP-ECA-50	Ulkoinen kyberhyökkäys	Tilin luominen ja hallinta – yksilölliset tunnistet	Käytäntöjen noudattamatta jättäminen voi johtaa siihen, että tileillä on liikaa oikeuksia.	Pakota järjestelmä hyväksymään vain yksilölliset käyttäjätunnukset estääksesi tilin jakamisen ja varmistaaaksesi jäljitettävyyden. Estä jaetut tilit BSS/OSS:lle tai pilvelle.	IT-osasto, operatiivinen tiimi, myynti
DP-ECA-51	Ulkoinen kyberhyökkäys	Vahvan tunnistautumisen mekanismien käyttö - Salasanat	Heikot kirjautumismenettelyt voivat johtaa tilin vaarantumiseen	Vahvat salasanakäytännöt: Ota käyttöön tiukat salasana-vaatimukset, mukaan lukien vähimmäispituus, monimutkaisuus ja säännölliset muutokset.	IT-osasto, operatiivinen tiimi, myynti
DP-ECA-52	Ulkoinen kyberhyökkäys	Vahvan tunnistautumisen mekanismien käyttö - MFA	Heikot kirjautumismenettelyt voivat johtaa tilin vaarantumiseen	Monimenetelmäinen todennus (MFA): Vaadi MFA:ta kriittisten järjestelmien ja arkaluonteisten tietojen käyttämiseen.	IT-osasto, operatiivinen tiimi, myynti
DP-ECA-53	Ulkoinen kyberhyökkäys	Vahvan tunnistautumisen mekanismien käyttö – salasanoiden hallinta	Heikot kirjautumismenettelyt voivat johtaa tilin vaarantumiseen	Salasanojen hallinta: Käytä turvallisia salasanojen hallintatyökaluja ja estä salasanojen uudelleenkäyttö eri tileillä.	IT-osasto, operatiivinen tiimi
DP-ECA-54	Ulkoinen kyberhyökkäys	RBAC-roolimäärittäminen	Työtehtäviä laajempia järjestelmäoikeudet voivat johtaa verkon virheellisiin asetuksiin, väärinkäyttöön ja niistä aiheutuviin taloudellisiin menetyksiin.	Roolipohjainen käyttöoikeuksien hallinta (RBAC) – roolimäärittäminen: Määritä rooleja työtehtävien perusteella ja varmista, että käyttäjillä on vain tarvittavat käyttöoikeudet rooleihinsa. Suorita säännölliset käyttövaltuus tarkistukset ja auditoinnit, joilla varmennetaan, ettei käyttäjillä ole liian laajoja oikeuksia verkossa.	IT-osasto, operatiivinen tiimi

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuul- linen taho
DP-ECA-55	Ulkoinen kyber- hyökkäys	RBAC - vähiten oikeuksia	Työtehtäviä laajemmat järjestel- mäoikeudet voivat johtaa verkon virheellisiin asetuk- siin, väärinkäyttö- ksiin ja niistä aiheu- tuviin taloudellisiin menetyksiin.	Varmista, että käyttäjillä on tehtäviensä suorittamiseen vain vaadittavat vähimmäis- käyttöoikeudet. Suorita säännölliset käyttövaltuus tarkis- tukset ja auditoinnit, joilla varmennetaan, ettei käyttä- jillä ole liian laajoja oikeuksia verkossa.	IT-osasto, opera- tiivinen tiimi
DP-ECA-56	Ulkoinen kyber- hyökkäys	Laajojen käyt- töoikeuksien hallinta - Käytön rajoitukset	Laajat oikeudet mahdollistavat hyökkääjälle verkossa olevien tietojen ja verkon täydellisen tuhoamisen.	Rajoita etuoikeutettujen tilien käyttöä sekä valvo ja kirjaa niiden toimintaa tarkasti. Säännölliset käyttövaltuus tarkistukset ja auditoinnit.	IT-osasto, opera- tiivinen tiimi
DP-ECA-57	Ulkoinen kyber- hyökkäys	Laajojen käyt- töoikeuksien hallinta - just-in-time	Laajat oikeudet mahdollistavat hyökkääjälle verkossa olevien tietojen ja verkon täydellisen tuhoamisen.	Just-in-Time Access: Anna etuoikeutettu käyttöoikeus vain tarvittaessa ja rajoite- tuksi ajaksi.	IT-osasto, opera- tiivinen tiimi
DP-ECA-58	Ulkoinen kyber- hyökkäys	Laajojen käyt- töoikeuksien hallinta - sala- sanalla hallinta	Tunnistetietojen suojaamaton tallennus voi johtaa käyttäjätilin väärin- käyttöön ja verkkoon murtautumiseen.	Tallenna etuoikeutetut tunnis- tetiedot suojattuun tilaan. Rajoita ja valvo niiden jakelua sekä käyttöä. Tätä voidaan tukea käyttämällä suojattuja laitteita, kuten laitteiston suojausmoduuleja (HSM) tai älykortteja.	IT-osasto, opera- tiivinen tiimi
DP-ECA-59	Ulkoinen kyber- hyökkäys	Tilin käytöstä poistaminen ja valmistelun poistaminen - Automaat- tinen varauksen purkaminen	Hyökkääjä voi käyttää käyttämät- ömiä käyttäjätilejä hyökkäyksen käyn- nistämiseen ja murtautumisen havaitsemisen vält- tämiseen, mikä voi johtaa pitkäaikaisiin väärinkäyttöksiin, tietojen anastuk- seen, tietojen katoamiseen ja muuttumiseen sekä verkon ongelmiin.	Ota käyttöön automaattinen prosessi ja hälytykset tilien poistamiseksi käytöstä välittö- mästi työsuhteen päättymisen tai työroolien muutosten jälkeen.	IT-osasto, opera- tiivinen tiimi

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuullinen taho
DP-ECA-60	Ulkoinen kyberhyökkäys	Tilin käytöstä poistaminen ja valmistelun poistaminen - säännölliset tarkastukset ja tilitarkastukset	Huomaamatta jäänyt käyttäjätilin vaarantuminen voi johtaa väärinkäytöksiin, tietojen katoamiseen, muutoksiin ja anastukseen sekä verkko-ongelmiin.	Tarkasta käyttämättömät käyttäjätilit säännöllisesti tunnistaaksesi ja poistaaksesi käytöstä tilit, joita ei enää tarvita.	IT-osasto, operatiivinen tiimi, HR
DP-ECA-61	Ulkoinen kyberhyökkäys	Tilin käytöstä poistaminen ja valmistelun poistaminen - käyttämättömät tilit	Huomaamatta jäänyt käyttäjätilin vaarantuminen voi johtaa väärinkäytöksiin, tietojen katoamiseen, muutoksiin ja anastukseen sekä verkko-ongelmiin.	Lukitse käyttäjätili tilanteissa, missä käyttäjä poistuu tilapäisesti työtehtävistään. Tarkista säännöllisesti, onko järjestelmässä aktiivisena käyttäjätilejä, joiden käyttäjä on tilapäisesti poissa, esimerkiksi vanhempainvapaalla. Lukitse tili henkilön poissaolon ajaksi.	IT-osasto, operatiivinen tiimi, HR
DP-ECA-62	Ulkoinen kyberhyökkäys	Kulunvalvonta ja kirjaaminen - Käyttölokkit	Huomaamatta jäänyt käyttäjätilin vaarantuminen voi johtaa väärinkäytöksiin, tietojen katoamiseen, muutoksiin ja anastukseen sekä verkko-ongelmiin.	Ylläpidä yksityiskohtaisia lokeja käyttäjätilin käyttötoiminnoista, mukaan lukien onnistuneet ja epäonnistuneet kirjautumisyriytykset sekä tilin käyttöoikeuksien muutokset. Analysoi lokeja säännöllisesti siten, että poikkeavat tapahtumat löydettäisiin.	IT-osasto, operatiivinen tiimi
DP-ECA-63	Ulkoinen kyberhyökkäys	Kulunvalvonta ja kirjaaminen - Reaaliaikainen seuranta	Huomaamatta jäänyt käyttäjätilin vaarantuminen voi johtaa väärinkäytöksiin, tietojen katoamiseen, muutoksiin ja anastukseen sekä verkko-ongelmiin.	Ota käyttöön reaaliaikainen seuranta ja automaattinen hälytysraportointi epäilyttävien toimintojen havaitsemiseksi ja nopean reagoinnin mahdollistamiseksi.	IT-osasto, operatiivinen tiimi
DP-ECA-64	Ulkoinen kyberhyökkäys	Pääsyn valvonta ja kirjaaminen - kirjausketjut	Huomaamatta jäänyt käyttäjätilin vaarantuminen voi johtaa väärinkäytöksiin, tietojen katoamiseen, muutoksiin ja anastukseen sekä verkko-ongelmiin.	Varmista, että käyttäjätilin käytöstä jäävät merkinnät ovat täydellisiä sisältäen aikaleiman, käyttäjätilin nimen sekä suoritettujen toimenpiteiden ja estä tietoihin tehtävät jälkikäteiset muutokset.	IT-osasto, operatiivinen tiimi

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuulinen taho
DP-ECA-65	Ulkoinen kyber- hyökkäys	Tilin käyttö- käytännöt - Poliitiikan dokumen- tointi	Politiikan täytän- töönpanon puutteel- linen dokumentointi ja ohjeistus voi johtaa liian laajoihin käyttöoikeuksiin, väärinkäyttöksiin, verkko-ongelmiin ja taloudellisiin menetyksiin.	Dokumentoi kaikki tilin käyttö- käytännöt ja -menettelyt selkeästi ja varmista, että ne tiedotetaan ja koulutetaan kaikille käyttäjille.	IT-osasto, opera- tiivinen tiimi
DP-ECA-66	Ulkoinen kyber- hyökkäys	Tilin käyttö- käytännöt - käytäntöjen täytäntöön- pano	Politiikan täytän- töönpanon puut- teellinen valvonta voi johtaa liian laajoihin käyttö- oikeuksiin, väärin- käyttöksiin, verkko- ongelmiin ja taloudellisiin menetyksiin.	Varmista käyttöoikeuskäytän- töjen johdonmukainen täytän- töönpano kaikissa järjestel- missä ja sovelluksissa koulu- tuksella ja säännöllisillä auditoinneilla.	IT-osasto, opera- tiivinen tiimi
DP-ECA-67	Ulkoinen kyber- hyökkäys	Käyttäjien koulutus ja tietoisuus - Säännöllinen harjoittelu	Tietoturvatietoi- suuden puute voi johtaa tietoturvan heikkenemiseen, tietojen anastuk- seen ja verkon ongelmiin.	Järjestä säännöllisiä koulutus- tilaisuuksia tilin käyttöoikeuk- sien hallinnasta, mukaan lukien salasanojen hallinnan ja tietojenkalasteluyritysten tunnistamisen parhaat käytännöt.	IT-osasto, opera- tiivinen tiimi
DP-ECA-68	Ulkoinen kyber- hyökkäys	Käyttäjien koulutus ja tietoisuus - Turvallisuus- tietoisuus	Tietoturvatietoi- suuden puute voi johtaa tietoturvan heikkenemiseen, tietojen anastuk- seen ja verkon ongelmiin.	Ota käyttöön jatkuvia tietu- turvan tietoisuusohjelmat/ koulutukset, jotta käyttäjät pysyvät ajan tasalla uusista uhista ja tilin suojauksen tärkeystä. Valvo, että kaikki käyttäjät suorittavat vaaditut koulutukset todistetusti.	IT-osasto, opera- tiivinen tiimi
DP-ECA-69	Ulkoinen kyber- hyökkäys	Kolmannen osapuolen tilin käyttö - toimittajan käyttöoikeuk- sien hallinta	Kolmannen osapuolen käyttö- oikeuksien valvonnan puute voi johtaa liian laajoihin käyttöoikeuksiin, väärinkäyttöksiin ja taloudellisiin menetyksiin.	Toimittajan käyttöoikeuksien hallinta: Ota käyttöön tiukka käyttöoikeuksien hallinta ja valvonta/kirjaaminen kolmannen osapuolen toimi- joille ja varmista, että heillä on pääsy vain siihen, mikä on välttämätöntä heidän tehtä- viensä suorittamiseksi. Suorita säännöllisesti käyttövaltuus tarkistukset ja auditoinnit.	IT-osasto, operatii- vinen tiimi, hankinta

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuullinen taho
DP-ECA-70	Ulkoinen kyberhyökkäys	Kolmannen osapuolen tilin käyttö – Sopimukset	Kolmannen osapuolen käyttöoikeuksien valvonnan puute voi johtaa liian laajoihin käyttöoikeuksiin, väärinkäyttöihin ja taloudellisiin menetyksiin.	Sopimukset: Sisällytä erityisiä tilin pääsynhallintavaatimuksia kolmansien osapuolten kanssa tehtäviin sopimuksiin, kuten VPN-vaatimukset sekä valvonta- ja lokivaatimukset.	IT-osasto, operatiivinen tiimi, hankinta
DP-ECA-71	Ulkoinen kyberhyökkäys	Etäkäytön suojaus	Heikkojen etäkäytömekanismien käyttö voi johtaa verkossa olevien tietojen anastukseen, tietojen virheisiin, tietojen menettämiseen ja verkko-ongelmiin.	Pakota käyttöön turvalliset etäkäytömekanismit, kuten VPN ratkaisut, vahvalla todennuksella ja salauksella.	IT-osasto, operatiivinen tiimi
DP-ECA-72	Ulkoinen kyberhyökkäys	Reagointi tapaukseen tilin vaarantuessa	Tilin vaarantumista koskevan häiriösuunnitelman puuttuminen voi johtaa korjaustoimien viivästymiseen, laajaan tilin väärinkäyttöön ja tietovarkauteen sekä verkko-ongelmiin.	Tee suunnitelma, miten tilivarkauden sattuessa tili eristetään, hävitetään ja tarvittaessa palautetaan. Testaa suunnitelman toteuttamiskelpoisuus.	IT-osasto, operatiivinen tiimi
DP-ECA-73	Ulkoinen kyberhyökkäys	Käyttäjien informointi	Käyttäjän tietämättömyys käyttäjätilin vaarantumisesta voi johtaa korjaustoimien viivästymiseen, laajaan tilin väärinkäyttöön ja tietovarkauteen sekä verkko-ongelmiin.	Määritä menettelyt, joilla käyttäjille ilmoitetaan vaarantuneista tileistä ja ohjataan heitä palautusprosessin läpi. Tämä voidaan tehdä OSS / BSS:n, pilviliien lisäksi myös loppukäyttäjien tileille.	IT-osasto, operatiivinen tiimi
DP-ECA-74	Ulkoinen kyberhyökkäys	Käyttäjätilin vaarantumisen analyysi	Tietämättömyys käyttäjätiliä suojaavien kontrollien heikkouksista voi johtaa laajaan käyttäjätilien väärinkäyttöön, tietovarkauteen sekä verkko-ongelmiin.	Tee nopeasti analyysi käyttäjätilivarkauteen johtaneiden heikkouksien tunnistamiseksi ja aseta analyysin tuloksia hyväksikäyttäen tehokkaammat kontrollit käyttäjätilin suojaksi.	IT-osasto, operatiivinen tiimi

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuul- linen taho
DP-ECA-75	Ulkoinen kyber- hyökkäys	Kattava suunnitelma häiriö- tilanteisiin reagoimiseksi	Puutteellinen häiriötilannesuun- nitelma voi johtaa verkon toipumisen viivästymiseen.	Häiriönhallintasuunnitel- massa tulee määrittää prosessin kulku havaitsemi- sesta täydelliseen toipumi- seen saakka. Prosessin eri vaiheiden vastuut on määri- tettävä yksilöidysti siten, että vastuut ovat tiedossa 24/7. Prosessiin tulee sisällyttää koko mobiiliverkkoinfrastruk- tuuri toimitusketju / toimittaja riippuvuuksineen. Suunni- telma tulee testata säännölli- sesti, jotta prosessin kulku ja siinä olevat vastuut ovat tiedossa kaikilla osapuolilla.	IT-osasto, opera- tiivinen tiimi
DP-ECA-76	Ulkoinen kyber- hyökkäys	Toimittaj- atietojen tuki haavoittu- vuuksille	Toimittajan tuen puute häiriötilan- teissa voi johtaa verkon toipumisen viivästymiseen, lakisääteisen rapor- tointivelvollisuuden laiminlyöntiin ja taloudellisiin mene- tyksiin sekä kyber- hyökkäyksen onnistumiseen	Sisällytä hankintasopimuk- seen velvollisuus haavoittu- vuustietojen jakamisesta ja niihin liittyvästä tuesta koskien myös alihankkijoita.	IT-osasto, operatii- vinen tiimi, hankinta
DP-ECA-77	Ulkoinen kyber- hyökkäys	Toimittajien tuki vaar- tilanteiden raportoin- nissa	Toimittajan tuen puute häiriötilan- teissa voi johtaa lakisääteisen rapor- tointivelvollisuuden laiminlyöntiin ja siitä aiheutuviin yhteiskunnallisiin sekä organisatori- siin haittoihin ja uhkien toteutumiseen	Hankintasopimuksissa on oltava vaatimus, että toimit- taja tukee poikkeamien rapor- toinnissa NIS2-vaatimusten mukaisesti.	IT-osasto, operatii- vinen tiimi, hankinta
DP-ECA-78	Ulkoinen kyber- hyökkäys	Toimittajien tuki onnetto- muuksien lieventämi- seen	Toimittajan tuen puute häiriötilan- teissa voi johtaa lakisääteisen rapor- tointivelvollisuuden laiminlyöntiin ja siitä aiheutuviin yhteiskunnallisiin sekä organisatori- siin haittoihin ja uhkien toteutumiseen	Hankintasopimuksessa tulee edellyttää toimittajan tukevan häiriötilanteessa (esim. hätä- korjaukset, asiantuntijatiedot).	IT-osasto, operatii- vinen tiimi, hankinta

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuul- linen taho
DP-ECA-79	Ulkoinen kyber- hyökkäys	Toimittajien tuki häiriö- tilanteisiin reagoinnin testauksessa	Toimittajan tuen puute häiriötilan- teissa voi johtaa lakisääteisen rapo- rintivelvollisuuden laiminlyöntiin ja siitä aiheutuviin yhteiskunnallisiin sekä organisatori- siin haittoihin ja uhkien toteutumiseen	Häiriönhallintasuunnitelman testaukseen tulee ottaa mukaan toimittaja, jotta reagoinnissa osataan ottaa kokonaisuus huomioon.	IT-osasto, opera- tiivinen tiimi, hankinta
DP-ECA-80	Ulkoinen kyber- hyökkäys	Uhkien seuranta	Uhkien ymmärtä- misen puute voi johtaa viivästynei- siin lieventämistoi- miin ja järjestelmän vaarantumiseen.	Laaditaan uhkakuvakartta neljännesvuosittain käyttäen hyväksi luotettavaksi todet- tuja lähteitä. Uhlakuvakartta esitetään ylätasolla yhtiön hallitukselle.	IT-osasto, opera- tiivinen tiimi
DP-ECA-81	Ulkoinen kyber- hyökkäys	Uhkien seuranta	Uhkien ymmärtä- misen puute voi johtaa viivästynei- siin lieventämistoi- miin ja järjestelmän vaarantumiseen.	Käytä uhkatiedusteluohjelmaa.	IT-osasto, opera- tiivinen tiimi
DP-ECA-82	Ulkoinen kyber- hyökkäys	Uhkien seuranta	Uhkien ymmärtä- misen puute voi johtaa viivästynei- siin lieventämistoi- miin ja järjestelmän vaarantumiseen.	Tarkista ja päivitä uhkatiedus- teluohjelma säännöllisesti.	IT-osasto, opera- tiivinen tiimi
DP-ECA-83	Ulkoinen kyber- hyökkäys	Uhkien seuranta	Uhkien ymmärtä- misen puute voi johtaa viivästynei- siin lieventämistoi- miin ja järjestelmän vaarantumiseen.	Varmista, että uhkatiedusteluohjelma hyödyntää uusimpia uhkatiedustelujärjestelmiä.	IT-osasto, opera- tiivinen tiimi
DP-ECA-84	Ulkoinen kyber- hyökkäys	Uhkien seuranta	Tehoton uhkien jakaminen viiväs- tyttää lieventäviä toimia ja lisää kyberhyökkäyksen onnistumisen riskiä	Käytä standardoituja keinoja uhkatietojen vaihtamiseen.	IT-osasto, opera- tiivinen tiimi
DP-HSF-1	Laitteisto- ja ohjelmisto- viat	Kuorman hallinta	Valvomaton ja hallitsematon ylikuormitus voi johtaa järjestelmä- katkoksiin	Kuormituksen valvonta- ja hallintajärjestelmän käyttö, esim. SDN-ohjain, SCP jne.	IT-osasto, opera- tiivinen tiimi

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuul- linen taho
DP-HSF-2	Laitteisto- ja ohjelmisto- viat	Korvaava laitteisto	Laitteiston myöhäinen vaihto voi johtaa palvelin- virheeseen ja tietojen menetykseen	Tunnista laitteiston vaihto- tarve omaisuudenhallintatyö- kalun avulla.	IT-osasto, opera- tiivinen tiimi, hankinta- tiimi
DP-HSF-3	Laitteisto- ja ohjelmisto- viat	Vikasieto- palvelimet	Palautus on hidasta tietojen mene- tyksen vuoksi	Käytä vikasietopalvelimia palautukseen.	IT-osasto, opera- tiivinen tiimi
DP-IA-1	Sisäpiirin hyökkäys (HR)	Turvallisuus- selvitys	Epäluotettava henkilö voi päästä käiksi kriittisiin resursseihin	Tee uudelle työntekijälle turvallisuus selvitysmenettely. Turvallisuus selvityksen tulee vastata matkaviestinverkossa tehtävien kriittisyyttä.	IT-osasto, hankinta- tiimi, opera- tiivinen tiimi, HR
DP-IA-2	Sisäpiirin hyökkäys (HR)	Tehtävien eriyttäminen	Turvallisuus- kontrollit ohitetaan	Vaaralliset työyhdistelmät identifioidaan ja tehtävät eriytetään niin ettei synny vaarallisia työyhdistelmiä.	IT-osasto, hankinta- tiimi, opera- tiivinen tiimi
DP-IA-3	Sisäpiirin hyökkäys (HR)	Tehtävien eriyttäminen	Tahallinen tai tahaton merkittävä virhe järjestelmän käytössä johtaa verkon ongelmiin tai lisääntyneeseen tietoturvaan	Riskiä sisältävien toimintojen toteutus pakotetaan teke- mään vähintään kahden henkilön toimesta (esim. tekijä ja hyväksyjä).	IT-osasto, hankinta- tiimi, opera- tiivinen tiimi
DP-IA-4	Sisäpiirin hyökkäys (HR)	Lähtevä työntekijöitä koskevat menettelyt	Työntekijän käyttö- oikeudet jäävät voimaan ja niitä hyödynnetään hyökkäyksessä	Kun työntekijä lähtee pois organisaatiosta, hänen käyttöoikeutensa poistetaan järjestelmästä viimeistään seuraavana päivänä lähtemi- sestä. Avaimet fyysisiin tiloihin otetaan pois lähdön yhteydessä.	IT-osasto, hankinta- tiimi, opera- tiivinen tiimi

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuul- linen taho
DP-LP-1	Osaavan henkilöstön puute	Eläkkeelle siirtyminen	Verkon ja järjestelmien ylläpitoon ei ole tarvittavaa osaamista, mikä aiheuttaa verkko-ongelmia ja lisääntyvän tietoturvauhan	Kun työntekijän eläköitymiseen on kaksi vuotta aikaa, analysoidaan resurssointiin liittyvät tarpeet ja tehdään korvaussuunnitelma sisältäen mahdollisen rekrytoinnin tai olemassa olevien työntekijöiden koulutuksen.	IT-osasto, hankintatiimi, operatiivinen tiimi, HR
DP-LP-2	Osaavan henkilöstön puute	Etäkäyttö	Työntekijät eivät pääse työpaikalle logistisista tai terveydellisistä syistä johtuen, eikä verkon ylläpitoa saada tehtyä	Varmistetaan, että verkon ja järjestelmien ylläpito on mahdollista etäkäyttötöyökaluilla.	IT-osasto, hankintatiimi, operatiivinen tiimi
DP-LP-3	Osaavan henkilöstön puute	Etäkäyttö	Työntekijät eivät pääse työpaikalle logistisista tai terveydellisistä syistä johtuen, eikä verkon ylläpitoa saada tehtyä	Etäkäytön skaalautuvuutta ja liitettävyyttä tulee testata säännöllisesti.	IT-osasto, hankintatiimi, operatiivinen tiimi
DP-LP-4	Osaavan henkilöstön puute	Etäkäyttö	Työntekijät eivät pääse työpaikalle logistisista tai terveydellisistä syistä johtuen, eikä verkon ylläpitoa saada tehtyä	Käytetään luotettavia etätodennus- ja valtuutusmenettelyjä ja kahta eri verkkoyhteyttä, jotta etäkäyttö on aina työntekijän saatavilla.	IT-osasto, hankintatiimi, operatiivinen tiimi
DP-LP-5	Osaavan henkilöstön puute	Etäkäyttö	Työntekijät eivät pääse työpaikalle logistisista tai terveydellisistä syistä johtuen, eikä verkon ylläpitoa saada tehtyä	Etätyötä koskevat säännöt ja prosessit, jotka ovat linjassa organisaation muiden sääntöjen kanssa hyväksytään johdon toimesta.	IT-osasto, hankintatiimi, operatiivinen tiimi, HR
DP-LP-6	Osaavan henkilöstön puute	Varahenkilöt	Usea työntekijä on sairaana samanaikaisesti, eikä verkkoa ei voida operoida	Varmistetaan, että jokaista verkon operointiin liittyvää toimintoa osaa hoitaa vähintään kolme työntekijää.	IT-osasto, hankintatiimi, operatiivinen tiimi, HR

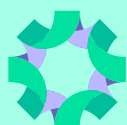
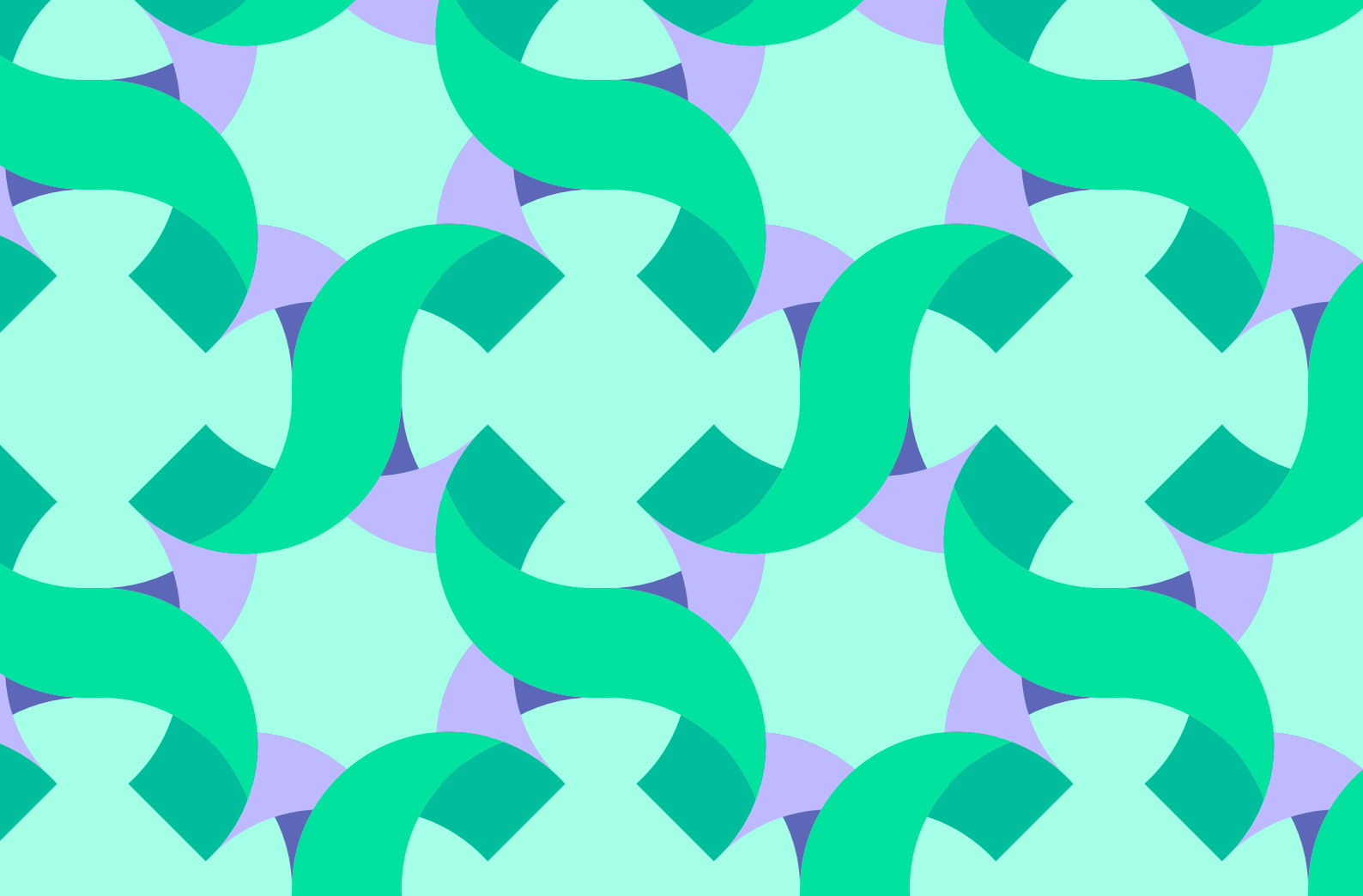
Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuulinen taho
DP-LP-7	Osaavan henkilöstön puute	Varahenkilöt	Usea työntekijä on sairaana samanaikaisesti, eikä verkkoa ei voida operoida	Osa-aikaiset työntekijät otetaan kokopäiväisiksi kriittisenä aikana.	IT-osasto, hankintatiimi, operatiivinen tiimi, HR
DP-BCP-1	Liiketoiminnan jatkuvuus-suunnitelma (BCP)	Palvelun jatkuvuus	Epäselvä lähestymistapa palveluiden jatkumiseen voi johtaa palvelukatkoksiin	Palveluiden jatkuvuutta koskeva strategia tulee dokumentoida, mukaan lukien keskeisten palvelujen ja prosessien palautumisaikaa koskevat tavoitteet.	CSO
DP-BCP-2	Liiketoiminnan jatkuvuus-suunnitelma (BCP)	Valmiussuunnitelma	Puutteellinen ja toteuttamatta jäänyt varautumissuunnitelma voi johtaa verkon käyttökatkoon	Tee kriittisten järjestelmien valmiussuunnitelmat ja dokumentoi ne, mukaan lukien selkeät vaiheet, vastuut ja menettelyt yleisiä uhkia varten, aktiivoinnin laukaisevat tekijät, vaiheet ja palautumisaikavoitteet. Harjoittele suunnitelman toteuttamista, jotta vastuut ja tehtävät tulevat selväksi vastuullisille henkilöille.	CSO
DP-BCP-3	Liiketoiminnan jatkuvuus-suunnitelma (BCP)	Valmiussuunnitelma	Puutteellinen ja toteuttamatta jäänyt varautumissuunnitelma voi johtaa verkon käyttökatkoon	Seuraa valmiussuunnitelmien aktivointia ja suorittamista rekisteröimällä onnistuneet ja epäonnistuneet palautumisajat. Valmiussuunnitelmien aktivointia koskeva päätöksentekoprosessi vastuineen dokumentoidaan yksityiskohtaisesti. Valmiussuunnitelmien aktivointi ja toteutus kirjataan, mukaan lukien tehdyt päätökset, seuratut vaiheet ja lopullinen toipumisaika.	CSO
DP-BCP-4	Liiketoiminnan jatkuvuus-suunnitelma (BCP)	Kriittisten toimintojen priorisointi	Tietoliikenneverkon katkeaminen kriittisiltä toimijoilta johtaa yhteiskunnan ja organisaatioiden vakavien uhkien toteutumiseen	Laaditaan listaus kriittisistä aloista ja palveluista, jotka ovat olennaisia ja/tai riippuvaisia verkko- ja palvelutoiminnan jatkuvuudesta.	CSO

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuulinen taho
DP-BCP-5	Liiketoiminnan jatkuvuus-suunnitelma (BCP)	Riippuvaisten kriittisten alojen valmiussuunnitelmat	Tietoliikenneverkon katkeaminen kriittisiltä toimijoilta johtaa yhteiskunnan ja organisaatioiden vakavien uhkien toteutumiseen	Toteutetaan valmiussuunnitelmia riippuvaisille ja toisistaan riippuvaisille kriittisille aloille ja palveluille. Määritetään riippuvaisia kriittisiä yrityksiä ja palveluja palveluntarjoajat voivat ottaa huomioon palvelut, jotka ovat riippuvaisia verkko- ja palvelutoiminnan jatkuvuudesta ja jotka ovat olennaisia yhteiskunnan ja/tai talouden kriittisten toimintojen ylläpitämiseksi ja joiden poikkeamalla olisi merkittäviä haitallisia vaikutuksia kyseisen palvelun tarjoamiseen. Valmiussuunnitelmaan voidaan sisällyttää niiden organisaatioiden osalta varaverkko, joka toteutetaan konteissa/kuorma-autoissa sijaitsevien verkkolaitteiden avulla.	CSO
DP-BCP-6	Liiketoiminnan jatkuvuus-suunnitelma (BCP)	Jatkuvuusstrategian tarkistaminen	Puutteellinen ja päivittämätön valmiussuunnitelma voi johtaa palvelukatkoksiin	Tarkista ja päivitä palvelun jatkuvuusstrategia säännöllisesti. Dokumentoi jatkuvuusstrategia sisällyttäen siihen muutoslokin ja muutosten sisältö.	CSO
DP-BCP-7	Liiketoiminnan jatkuvuus-suunnitelma (BCP)	Valmiussuunnitelmien tarkistaminen	Puutteellinen ja päivittämätön varautumissuunnitelma voi johtaa käyttökatkoon	Tarkista ja päivitä valmiussuunnitelmat aiempien tapahtumien ja muutosten perusteella. Dokumentoi valmiussuunnitelma sisällyttäen siihen muutosloki ja muutosten sisältö.	CSO
DP-BCP-8	Liiketoiminnan jatkuvuus-suunnitelma (BCP)	Jatkuvuus-suunnitelma	Varayhteyden toimimattomuus voi johtaa liiketoiminnan pysähtymiseen	Kriittisten yritysten, jotka käyttävät matkapuhelinverkkoa toissijaisena verkkona, tulisi säännöllisesti testata verkon toiminta osana katastrofikoulutusta / emulointia.	Operaatiivinen tiimi, IT-osasto, CSO

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuul- linen taho
DP-BCP-9	Liiketoiminnan jatkuvuus-suunnitelma (BCP)	BCP-sisältö	Puutteellinen BCP-suunnitelma saattaa viivästyttää palvelujen palauttamista	BCP-suunnitelman olisi sisällettävä: <ol style="list-style-type: none"> 1. Organisaation toiminnan kuvaus 2. Sidosryhmien sitouttaminen 3. Toimittajien tuen saatavuus 4. Yritykseen kohdistuvien vaikutusten arviointi (BIA) ja riskinarviointi 5. Liiketoiminnan jatkuvuusstrategiat 6. Liiketoiminnan jatkuvuussuunnitelmat 7. Koulutus 8. Testaus ja harjoittelu 9. Jatkuva parantaminen 10. Dokumentointi 	CSO
DP-BCP-10	Liiketoiminnan jatkuvuus-suunnitelma (BCP)	Palautumis-suunnitelman sisältö	Puutteellinen palautumissuunnitelma voi johtaa palautumisen viivästymiseen	Seuraavien asioiden olisi oltava osa sellaisen julkisen operaattorin tai kriittisen yrityksen elvytys-suunnitelmaa, joka käyttää matkaviestinverkkoja ensisijaisena viestintävälineenään. <ul style="list-style-type: none"> - Katastrofisuunnitelman laatiminen - Häättilannesuunnitelma - Osastokohtaiset toimintasuunnitelmat vastuu määrittelyineen - Tekniset oppaat ja vaiheittaiset toimintasuunnitelmat elvytysstrategian mukaista palautumista varten - Tarkistuslistat nopeisiin toimiin ja vahvistukseen - Suunnitelmien varmuuskopiot - Yhteystietoluettelot ja hätyhteyshenkilöt - Ulkoisen viestinnän suunnitelma - Sisäinen hätäviestintäsuunnitelma - Kriisinhallinta 	CSO

Numero	Kontrolli-alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuulinen taho
DP-BCP-11	Liiketoiminnan jatkuvuus-suunnitelma (BCP)	Palautumissuunnitelmaa koskevien tietojen säilyttäminen	Palautussuunnitelman puuttuminen kriisitilanteessa johtaa palautumisen viivästymiseen	Palautumissuunnitelman säilyttämisessä on otettava huomioon katastrofin, tallentamismuodon ja toimitilojen luonne, niin että suunnitelma on kaikissa tilanteissa saatavilla. Jos suunnitelma on pilvitalennustilassa ja yritys kärsii kyberhyökkäyksestä, pilvitalennustilaa ei ehkä voi käyttää. Tulvat voivat tehdä alemmista kerroksista ja niissä olevista materiaaleista saavuttamattomia jne.	CSO
DP-BCP-12	Liiketoiminnan jatkuvuus-suunnitelma (BCP)	Avainhenkilöiden koulutus	Kouluttamaton henkilöstö suorittaa väärä toimia katastrofitilanteissa, mikä johtaa palautumisen viivästymiseen	Avainhenkilöitä on tiedotettava suunnitelmista ja siitä, miten niihin päästään käsiksi ja koulutettava heidät toteuttamaan suunnitelmat. Heidän osaltaan on myös tehtävä suunnitelmat loma-aikojen järjestelyistä niin, että kaikkiin avainhenkilörooleihin on aina saatavilla tekijä.	CSO, kaikki
DP-BCP-13	Liiketoiminnan jatkuvuus-suunnitelma (BCP)	Kiireelliset toimenpiteet	Normaalissa toiminnassa käytetään turvattomia hätätoimenpiteitä, jotka mahdollistavat muiden uhkien toteutumisen	Turvallisuuden vaarantavat hätätoimenpiteet nopeaa toipumista varten olisi dokumentoitava ja niiden käyttöön tulee laatia sekä kouluttaa säännöt. Säännöissä määritetään, milloin hätätoimenpiteitä voidaan käyttää ja kuinka kauan.	CSO
DP-BCP-14	Liiketoiminnan jatkuvuus-suunnitelma (BCP)	Työntekijöiden sitoutuminen	Työntekijät eivät ole halukkaita tekemään enemmän kuin minimitoimet hätätilanteessa, mikä viivästyttää palautumista	Hyvällä esihenkilötyöllä sekä palkitsemalla hyviä suorituksia osoitetaan yrityksen sitoutumista työntekijöihin ja saadaan siten motivoitunut henkilöstö.	CSO, HR

Numero	Kontrolli- alue	Kontrollin nimi	Riskikuvaus	Kontrollikuvaus	Vastuul- linen taho
DP-BCP-15	Liiketoiminnan jatkuvuus-suunnitelma (BCP)	Palautumisstrategian yksityiskohdat	Palautumisstrategian yksityiskohtien puute voi johtaa palautumisen viivästymiseen	Palautumisstrategia sisältää ainakin seuraavat tiedot: <ol style="list-style-type: none"> 1. Painopisteiden määrittely 2. Palautumisaikatavoitteet (RTO) ja palautumispistetaavoitteet (RPO) 3. Vaihtoehtoiset sijaintipaikkajärjestelyt 4. Vaihtoehtoiset järjestelmät ja varmuuskopiointiratkaisut 5. Viestintäsuunnitelmat 6. Resurssien kohdentaminen 7. Toimittajien hallinta 8. Vaaratilanteiden hallinta ja reagointi 9. Testaus ja harjoitukset 10. Prosessikuvaukset 11. Jatkuva parantaminen 12. Vaatimustenmukaisuus. 	CSO
DP-BCP-16	Liiketoiminnan jatkuvuus-suunnitelma (BCP)	Palautumisstrategia	Palautumisstrategian puutteet voivat aiheuttaa palautumisen viivästymisen	Tarkasta ja päivitä palautumisstrategia säännöllisesti vaatimustenmukaisuuden ja tehokkuuden varmentamiseksi. Organisaation hallituksen tulisi hyväksyä palautumisstrategian vuosittain.	CSO



Huoltovarmuusorganisaatio