KYBERTURVARISKIEN KARTOITUS

FINGRID — ÄLYKKÄÄN SÄHKÖJÄRJESTELMÄN SELVITYS

Helsinki, 2017-12-07

Marko Buuri
Johtava riskienhallintakonsultti

Laura Noukka
Laadunvarmistus

F-Secure

Sisältö

RAPORTISTA

Tämän raportin on laatinut F-Secure Cyber Security Services osana älykkään sähköjärjestelmän eli älyverkon selvityksiä Fingridin ja työ- ja elinkeinoministeriön toimeksiannosta. Kaikki raportissa oleva ja muutoin toimeksiannossa syntynyt aineisto on tarkoitettu älyverkkotyöryhmän käytettäväksi osana työryhmän johtopäätöksiä ja suosituksia.

Raportti ei ole aihealueen kattava yleisselvitys. Aiheen käsittelyä rajoittavat valittu työmenetelmä, laadintaan käytettävissä ollut aika, käytettävissä ollut taustamateriaali, tiedot tulevan älyverkon toimintaperiaatteista ja teknologioista, sekä työpajoihin osallistuneiden tuntemus aiheesta.

Raportin jakelusta ja salassapidosta päättää tilaaja.

1. TIIVISTELMÄ

Työ- ja elinkeinoministeriö on asettanut työryhmän selvittämään älykkään sähköjärjestelmän eli älyverkon mahdollisuuksia sähkömarkkinoille. Työryhmän tehtävänä on selvittää ja esittää konkreettisia toimia, joilla älyverkot voivat palvella asiakkaiden mahdollisuuksia osallistua aktiivisesti sähkömarkkinoille ja edistää yleisesti toimitusvarmuuden ylläpitoa. Työryhmän tulee antaa mietintönsä 30. syyskuuta 2018 mennessä.

Älykäs sähköjärjestelmä tuo olennaisia uudistuksia siihen, miten sähkön tuotanto ja kysyntä jatkossa kohtaavat ja miten sähkömarkkinat toimivat. Teknologian ja palveluiden kehittyminen mahdollistavat sähkön kysyntäjoustojen reaaliaikaisen toteutumisen. Älykäs automatiikka ohjaa sähkön kulusta hetkiin, jolloin se on edullisinta. Sähköä varastoivat elementit, kuten sähköautot, voivat myös automaattisesti myydä sähköä silloin kun se on taloudellisesti kannattavaa. Älykkään sähköjärjestelmän toimintojen odotetaan toteutuvan Suomessa 2020 –luvulla.

Sähköjärjestelmä on osa yhteiskunnan kriittistä infrastruktuuria. Sähkön saatavuus on keskeistä lähes kaikkien muiden kriittisten infrastruktuuripalveluiden tuottamiselle. Sähköjärjestelmän muuttuminen keskitetystä sähköntuotannosta ja yksisuuntaisesta sähkönjakelusta aiempaa hajautuneemmaksi ja monisuuntaiseksi muuttaa myös sähköjärjestelmään kohdistuvia kyberturvallisuusriskejä.

Älykkään sähköjärjestelmän toteuttaminen edellyttää uudenlaista teknologiaa ja tietojenvaihtoa. Turvallisuustavoitteiden toteutuminen tarkoittaa näiden molempien näkökulmien suojaamista. Tästä syystä on erityisen keskeistä varmistaa, ettei lisääntyvä älykkyys lisää sähköjärjestelmän haavoittuvuutta kyberturvallisuusuhkia vastaan. Järjestelmän laajentuessa siihen liittyy lukuisia internetiin liitettyjä ohjattavia energialaitteita, kuten aurinkopaneeleja, akkuja ja sähköautoja.

F-Secure Cyber Security Services järjesti Fingridin ja työ- ja elinkeinoministeriön pyynnöstä kaksi riskityöpajaa älyverkkojen kyberturvallisuuskysymysten tunnistamiseksi. Toimeksiannon tavoitteena on tunnistaa kyberturvallisuusriskejä ja niiden mahdollisia hallintakeinoja älyverkkojen jatkotyötä varten. Tämä raportti kuvaa työn tuloksena tunnistetut vakavimmat kyberturvariskit.

Toimeksiannon aikana ei ollut tiedossa älykkääseen sähköjärjestelmään liittyviä tarkempia teknisiä määrityksiä. Tästä johtuen käsittelytapa perustuu ylätason riskien ja niiden mahdollisten seurausten sekä juurisyiden tunnistamiseen.

1.1. VAKAVIMMAT RISKIT

Seurauksiltaan vakavimpia riskiskenaarioita tunnistettiin neljä. Kolme skenaariota koskevat älyverkon joustoresurssien tietoja ja toimintaa, ja yksi reaaliaikaisen sähkömarkkinapaikan toimintaa.

Joustojen toteutuminen sovittuina aikoina on keskeistä sähköjärjestelmän tasapainon ja luotettavan toiminnan kannalta. Joustoresurssien ohjausjärjestelmien ja niiden käyttämän ohjaustiedon manipuloinnilla voi olla mahdollista aiheuttaa heilahduksia, jotka aiheuttaisivat häiriöitä sähkönjakeluun. Tämä on vakavin tunnistetuista riskeistä, sillä se aiheuttaa uhkan koko yhteiskunnan kriittiselle infrastruktuurille.

Joustoresurssien käyttöönottoon ja toimintaan tarvitaan perustietoja, jotka säilötään operatiivisia ohjaustarpeita varten palveluntarjoajien tietojärjestelmissä, sekä oletettavasti myös keskitetyssä tietojärjestelmässä. Ohjauksessa tarvittavien tietojen virheellisyys tai tuhoutuminen estää olennaisesti joustavan sähköjärjestelmän odotettua toimintaa ja aiheuttaisi taloudellisia menetyksiä joustopalveluiden tarjoajille. Pahimmillaan laaja perustietojen tuhoutuminen voisi vaikuttaa operatiivisesti ja aiheuttaa sähkönjakelun epävakautta.

Joustojen toteutumisesta kerätään mittaus- ja tasetietoa, jonka avulla todetaan toteutuneet joustot ja maksetaan sovitut korvaukset. Mittaustietojen puuttuminen tai manipulointi voi johtaa järjestelmän eri osapuolten taloudellisiin menetyksiin, sekä heikentää luottamusta ja siten investointeja joustaviin järjestelmiin.

Älykkään sähköjärjestelmän keskiössä on nykyistä lyhyemmissä jaksoissa toimivat sähkömarkkinat. Kaupankäynnin nopeutuminen minuuteissa tai sekunneissa mitattaviin jaksoihin tarkoittaa kaupankäynnin automaation lisääntymistä. Tämä tekee markkinasta herkemmän tahattomille tai tahallisille kaupankäynnin algoritmien virhetilanteille. Pahimmillaan markkinoiden automatiikan manipulointi voisi johtaa siihen, että sähkönjakelu häiriintyy.

Vakavimpia riskiskenaarioita käsitellään tarkemmin luvussa 3.

1.2.SEURAAVAT VAIHEET

Tämä raportti on osa älyverkkotyöryhmän selvityksiä. F-Secure suosittelee, että raportti lähetetään kommentoitavaksi tilaajan valitsemille sidostahoille. Esiselvityksen myöhemmissä vaiheissa tuloksia on tarkoituksenmukaista käyttää älyverkon toiminnallisten ja turvallisuusvaatimusten määrittämiseen, näiden kustannus-hyöty –analyysiin, ja muiden valmisteluun liittyvien päätösten tukena.

Erityisen tärkeää jatkotyössä olisi varmistaa, että kyberturvallisuuteen liittyvät kysymykset ovat osa tiedonvaihtovision ja teknisten määritysten, kuten seuraavan sukupolven AMR-järjestelmän, valmistelua.

2. KARTOITUKSEN TOTEUTUSTAPA

Tehty kyberturvariskien kartoitus liittyy työ- ja elinkeinoministeriön selvitykseen älykkään sähköjärjestelmän eli älyverkon mahdollisuuksista Suomessa. Riskikartoitustoimeksianto on yksi osa selvitystä, jossa pyritään avaamaan useita älyverkon mahdollisuuksiin ja vaatimuksiin liittyviä kysymyksiä. Älyverkkotyöryhmän tulee antaa mietintönsä viimeistään syyskuussa 2018.

Kartoituksen pääasiallisena työmenetelmänä järjestää kaksi työpajaa, joihin kutsuttiin älyverkkotyöryhmän sidosryhmien edustajia. Työpajojen valmistelu, järjestäminen ja tulosten dokumentointi ajoittuivat syyskuusta joulukuuhun 2017. Tämä raportti pitää sisällään työn aikana saavutetut tulokset.

Toimeksiannon toteutti ja tämän raportin laati johtava riskienhallintakonsultti Marko Buuri, F-Secure Cyber Security Services.

2.1. DOKUMENTAATIO

Seuraavat älyverkkoihin liittyvät asiakirjat olivat käytettävissä tätä kartoitusta tehtäessä.

- Suomen älyverkkovisio, 31.10.2016
- Tiedonvaihtovisiota koskeva väliraportti, 27.4.2017
- Tiedonvaihtovisio, 1.9.2017 luonnos
- Pöyryn toimittamaa tiedonvaihtovision taustamateriaalia

2.2. TYÖPAJAT

Toimeksiannon aikana järjestettiin 22. syyskuuta ja 20. lokakuuta työpajat, joiden tarkoitus oli kartoittaa eri sidostahojen asiantuntijanäkemyksiä älykkään sähköjärjestelmän riskeihin liittyen. Työpajojen työskentelytapana oli asiaan liittyvien uhkatoimijoiden, niistä aiheutuvien turvallisuuspoikkeamien, ja poikkeamiin mahdollisesti johtavien heikkouksien tunnistaminen. Lisäksi ensimmäisessä työpajassa kuultiin Jyrki Pennasen (Fingrid) alustus alan kyberturvallisuuskysymyksiin sekä Jimmy Forsmanin (Pöyry) esitys tiedonvaihtovision luonnoksesta. Työpajojen tulokset on eritelty luvussa 4.

Työpajoihin osallistuivat seuraavat henkilöt.

Molemmat työpajat	
Tuomas Rytkönen	Energiateollisuus ry
Tarvo Siukola	Energiavirasto
Jukka Rinta-Luoma	Fingrid
Jyrki Pennanen	Fingrid
Heidi Uimonen	Fingrid
Risto Lindroos	Fingrid
Pasi Kuokkanen	Suomen sähkönkäyttäjät ry
Tatu Pahkala	Työ- ja elinkeinoministeriö
Erika Suortti-Myyry	Viestintävirasto
Sami Orasaari	Viestintävirasto
Marko Buuri	F-Secure, työpajojen koordinaattori

Työpaja 22.9.	
Ville Väre	Energiavirasto
Jimmy Forsman	Pöyry
Sami Repo	Tampereen teknillinen yliopisto
Työpaja 20.10.	
Juha Leinonen	Pöyry
Jari Seppälä	Tampereen teknillinen yliopisto

2.3. RAJOITUKSET

Tätä riskikartoitusta tai raporttia laadittaessa ei ollut tiedossa millainen älyverkko ja reaaliaikamarkkina Suomessa tulee toteutumaan, millaisia teknisiä ratkaisuja tai arkkitehtuureja tiedonvaihtoon tullaan toteuttamaan, tai mitään teknisiä yksityiskohtia älyverkon säädön toiminnasta tai integraatioista. Tästä johtuen käsittelytavaksi valittiin taso, jossa teknologiasidonnaiset kysymykset eivät olennaisesti vaikuta riskien määrityksiin.

Työssä tavoiteltiin keskeisten kyberturvallisuusriskien tunnistamista, joilla tarkoitetaan tässä yhteydessä tietojärjestelmien ja tietojen manipulointia siten, että niistä aiheutuu haittaa älykkäälle sähköjärjestelmälle tai sen osapuolille. Tämän toimeksiannon osana ei käsitelty tietosuojakysymyksiä.

Riskikartoitusten tulosten laajuus riippuu aina käytettävissä olevasta ajasta. Riskien tunnistamiseen ja arviointia on tarkoituksen mukaista jatkaa alueilla, jotka mahdollisesti eivät tämän kartoituksen perusteella ole riittävän kattavia.

3. TUNNISTETUT RISKIT

Tämä luku kuvaa toimeksiannon aikana työpajoissa käsitellyt riskiskenaariot. Kustakin riskistä on kuvattu tapahtuman lisäksi siihen liittyvät taustatekijät, kuten mahdolliset uhkatoimijat ja oletetut heikkoudet, riskin oletettavat seuraukset, sekä mahdollisia hallintakeinoja. Kuvattujen hallintakeinojen luettelo ei ole tarkoitettu tyhjentäväksi, vaan keskustelun avaukseksi mahdollisten keinojen valikoimasta.

3.1. JOUSTORESURSSIN KÄYTÖN ESTYMINEN TAI VIRHEELLINEN KÄYTTÖ

Joustoresurssin käytön estymisellä tarkoitetaan tilannetta, jossa joustojärjestelmään ilmoitettu resurssi tai resurssit eivät ole teknisesti ohjattavissa säädön edellyttämällä tavalla. Tällainen tilanne voi toteutua teknisen vian tai virheellisten määritysten vuoksi, mutta myös tahallisen häirinnän seurauksena.

Keskeisenä tekijänä riskissä on joustoresurssien kytkeminen internetiin ohjausta ja tiedonvaihtoa varten. Tämä altistaa ne julkisesta verkosta peräisin oleville uhkille.

Riskien vaikutus laajenee joustavien resurssien kapasiteetin kasvaessa suhteessa sähköjärjestelmän kokoon. Älykkään sähköjärjestelmän ytimessä on ajatus siitä, että tarjonta ja kysyntä kohtaavat optimaalisella tavalla. Mikäli kysynnän joustot eivät toteudu ennakoidulla tavalla, voi järjestelmässä syntyä merkittävää alitarjontaa. Tämä voi johtaa sähköjärjestelmää epävakauttaviin häiriöihin, jotka voivat näkyä sähkönkäyttäjille sähkön laadun heikkenemisenä tai sähkökatkoina.

3.1.1. Taustatekijät

Riskiin vaikuttavia tausta- ja olosuhdetekijöitä on useita. Osa tekijöistä on tahattomia virheitä. Esimerkiksi joustoresurssien ohjaustietojen signalointiin käytettävien tietoliikenneratkaisujen tilapäiset häiriöt ovat todennäköinen tilanne, jossa tällaisia ongelmia syntyy. Myös erilaiset inhimilliset virheet asetusten määrityksissä sekä laitteiden logiikoiden toteuttamisessa ovat mahdollisia.

Riskien toteutumiseen voivat vaikuttaa myös tahalliset toimenpiteet. Tietoliikenteen ja ohjauslaitteiden toimintaa voi mahdollisesti häiritä erilaisilla palvelunestohyökkäyksillä, joko kuormittamalla liittymiä tai vaikuttamalla ohjauslaitteen toimintaan sen teknistä vikaa hyödyntämällä. Ohjauslaitteissa voi olla myös huonosti suojattuja ohjausrajapintoja, jotka altistavat sen luvattomille toimenpiteille internetiin liitettynä. Erityisen todennäköinen juurisyy erilaisille ongelmille ovat laitteet ja järjestelmät, jotka eivät ole turvallisia oletusasetuksilla.

3.1.2. Seuraukset

Riskien seuraukset kohdistuisivat sähköjärjestelmän luotettavuuteen. Huomattavan suuren yksittäisen joustoyksiköiden toiminnan estäminen tai erityinen ohjailu voi vaikuttaa sähköverkkojen toimintaan siten, etteivät verkon normaaliin tasapainottamisen mekanismit toimi normaalisti. Vastaava vaikutus saataisiin ohjailemalla useita pienempiä joustoyksiköitä samanaikaisesti. Verkon taajuus voi alkaa heilua ja toiminnallinen vakaus vaarantua. Jos määrätyt raja-arvot ylittyvät, herkimmät suojalaitteet voisivat irrottaa tuotanto- ja kulutuskohteita. Tilanne voi vaurioittaa sähkölaitteita ja aiheuttaa sähkökatkoja.

Yksittäisen asiakkaan näkökulmasta voi esiintyä haitallisia seurauksia joustoresurssien toiminnasta. Esimerkiksi lämmitysjärjestelmä voi kytkeytyä pois päältä pitkäksi aikaa ja kiinteistön vesiputket jäätyä.

Riskin toteutuminen voi johtaa erityisiin varotoimenpiteisiin, kuten joustotoimintojen tilapäiseen rajoittamiseen selvitysten ja lisäsuojausten toteuttamisen ajaksi. Tästä aiheutuisi taloudellista haittaa järjestelmän osapuolille, sillä reaaliaikaisen markkinan taloudelliset hyödyt jäisivät saavuttamatta.

Palveluntarjoajien ja laitevalmistajien maine kärsisi onnistuneista hyökkäyksistä. Tämä olisi haitallista näiden toimijoiden taloudellisten toimintaedellytysten näkökulmasta.

3.1.3. Hallintakeinoja

Riskin hallitsemiseksi älykkään sähköjärjestelmän jatkosuunnittelussa tulisi kiinnittää huomiota seuraaviin seikkoihin.

Mahdollinen hallintakeino on rajoittaa yksittäisten joustokohteiden maksimikokoa. Tällä tarkoitettaisiin sitä, että yksittäisen ohjausjärjestelmän takana olevalle kapasiteetille asetettaisiin yläraja. Ylärajan ylittäminen voisi olla sallittua erityisten luotettavuutta varmistavien toimenpiteiden kautta (ks. seuraava suositus). Hallintakeinolla rajoitettaisiin yksittäisen järjestelmän vian tai tahallinen häirinnän vaikutusta järjestelmälle. Hallintakeinon hyötyä rajoittaisi se, jos vastaavalla tekniikalla toteutettavia järjestelmiä olisi kuitenkin useita. Jos tällaisesta suositusta toteutuksesta löytyisi tekninen haavoittuvuus, voisi pahantahtoinen toimija pyrkiä vaikuttamaan useisiin kohteisiin samanaikaisesti, jolloin kokonaisvaikutus voisi vastata yhden suuren yksikön häiriötä.

Toisena keinona suurilta joustotoimijoilta voidaan edellyttää erityisiä toimenpiteitä oman toiminnan luotettavuuden varmistamiseksi. Esimerkiksi ohjaus- ja viestintäjärjestelmien kahdentamisella voidaan nostaa operatiivista toimintavarmuutta. Toimenpiteiden toteuttaminen ja seuranta voi olla osin omavalvontaan perustuvaa, mutta markkinapaikan sääntöihin olisi liitettävä vaatimuksia riittävästä osaamisesta tietoturvan hallinnassa. Suurimpien joustoyksilöiden osalta voitaisiin harkita riskiperusteisesti erityisiä valvonta- ja auditointitoimenpiteitä, joista vastaisi erikseen osoitettava taho.

Kolmas mahdollinen hallintakeino liittyy itse signalointikanavan toteutukseen. Suurten joustoyksiköiden tapauksessa olisi tarkoituksen mukaista harkita viestintäjärjestelmiä, jotka ei ole liitetty yleisiin verkkoihin (internetiin). Vaikka matkapuhelinverkkojen avulla tapahtuva ohjailu olisi edullisin ratkaisu, turvallisemmalla yhteystavalla voitaisiin rajoittaa merkittävästi tietoliikenteen keinoin tapahtuvan häirinnän mahdollisuutta.

Neljäntenä toimenpiteenä riskiä voidaan rajoittaa vaikuttamalla ohjauslaitteiden turvallisuuteen esimerkiksi standardisoinnilla sekä valmistajia ja haltijoita koskevilla velvoitteilla. Standardisoinnissa on tarkoituksenmukaista selvittää mahdollisuudet ja keinot kyberturvallisuutta varmistaviin vaatimukseen. Vaatimukset voivat kohdistua itse laitteen ominaisuuksiin, kuten millaisia ohjausprotokollia laitteisiin saa toteuttaa. Laitteilta tulisi myös edellyttää turvallisiin raja-arvioihin palautumista tilanteissa, joissa ohjaussignaalit ovat poikkeuksellisia tai niitä ei ole vastaanotettu määräajassa.

Vaatimuksia voitaisiin kohdistaa myös valmistajien velvollisuuksiin. Tällaisilla vaatimuksilla voitaisiin edellyttää esimerkiksi tarvittaessa ohjelmistopäivitysten kautta toteutettavia turvallisuusparannuksia kyberturvauhkien muuttuessa. Standardisointi keinona varmistaisi sen, että kaikki hyväksytyt laitteet toteuttavat tarkoituksen mukaisen perustason. Kyberturvallisuusasioiden sivuuttamisesta ei saisi syntyä kilpailullista hyötyä ohjauslaitteiden markkinoilla.

Lisäksi joustoresurssien haltijoilta voitaisiin joiltakin osin edellyttää tietoturvallisuustasosta huolehtimista. Verkonhaltijalla voisi olla mahdollisuus asettaa vaatimuksia verkkoon liitettävien laitteiden turvallisuudelle, ja tarvittaessa estää häiriöitä aiheuttavien laitteiden käyttäminen.

Viidentenä keinona on rakentaa arkkitehtuuri, jossa kriittiset tiedot hajautetaan useisiin toisistaan erillisiin tietovarantoihin. Tietovarantojen sisältöjä voidaan verrata automaattisesti. Tällöin yksittäisten tietosisältöjen luvattomat muutokset olisi mahdollista havaita.

3.2. JOUSTORESURSSIEN PERUSTIETOJEN TUHOUTUMINEN TAI VIRHEELLISYYS

Joustoresurssien perustietojen tuhoutuminen tai virheellisyys voi tapahtua teknisen virheen tai tahattomien tai tahallisten toimenpiteiden seurauksena. Tilanteesta aiheutuisi luultavasti taloudellisia tappioita joustooperaattoreille virheellisten tarjousten seurauksena. Riskillä voi joissakin tilanteissa olla operatiivisia vaikutuksia, mikäli toteutuneen tilanteen seurauksena joustoresursseja ei voitaisi hyödyntää tilapäisesti lainkaan tai vain osittain. Pahimmillaan virheelliset tiedot voivat johtaa vääränlaisiin oletuksiin joustoresurssien saatavuudessa tai tehossa myös operatiivisessa ohjauksessa.

Joustoresurssien perustiedoilla tarkoitetaan jakeluverkkoon liitettyjen hajautettujen joustavien resurssien kuvailutiedoista, jollaisia voisivat olla tiedonvaihtovision mukaan esimerkiksi

- tieto joustohalukkuudesta,
- käyttöpaikkatiedot,
- tieto merkittävimpien joustavien resurssien tyypeistä (esim. lämmitysjärjestelmä, akku), sekä
- tieto ohjaus- ja mittaustavasta.

Perustietoja tarvitaan joustoresurssin teknisen toiminnan ja joustoprofiilin määrittämiseksi. Tiedot ovat tarkoituksen mukaista kerätä ennen jouston aloittamista, sillä niitä tarvitaan joustavan säädön toteuttamisessa. Tiedot tallennettaisiin joustotoimijanlisäksi keskitettyyn tietojärjestelmään, johon sähköjärjestelmän eri osapuolet kytkeytyvät tiedon jakamista varten.

Tilanteen palautuminen riippuisi joustotoimijalla tai keskitetyssä järjestelmässä olevista varmistus- ja palautusmekanismeista. Jos ne eivät toimi odotetusti, perustiedot voidaan kerätä manuaalisten toimenpiteiden kautta uudelleen. Tällöin järjestelmän palautuminen normaalitilaan kestää luonnollisesti pidempään. Tilanteesta aiheutuvat taloudelliset vahingot ovat odotettavasti suhteellisia häiriön kestoon.

3.2.1. Taustatekijät

Joustoresurssien tuhoutumiseen tai virheellisyyteen voivat vaikuttaa erilaiset uhkatoimijat. Osa uhkatoimijoista voi aiheuttaa haittaa toimimalla huolimattomasti tai vastoin parempaa tietoa. Esimerkiksi inhimillinen virhe perustietojen keräämisessä tai tallentamisessa tietojärjestelmiin voi johtaa tietojen osittaiseen muuttumiseen. Voidaan myös ajatella, että inhimilliset virheet tietojärjestelmien ylläpidossa voisivat johtaa tietojen tuhoutumiseen tai muuttumiseen.

Toiset uhkatoimijat pyrkivät tietoisesti vahingoittamaan sähköjärjestelmää tai sen yksittäisiä osapuolia. Esimerkiksi rikollinen, jonka tarkoituksena olisi kiristää sähköjärjestelmän osapuolia esimerkiksi salaamalla joustoresurssien perustiedot, voisi murtautua niiden käsittelyyn käytettäviin tietojärjestelmiin. Vaihtoehtoisesti hän hankkii luvallisen käyttäjän tai ylläpitäjän käyttövaltuudet haitallisten toimenpiteiden toteuttamiseen.

Edellä kuvattujen lisäksi on syytä tunnistaa uhkatoimija, jonka tarkoituksena on aiheuttaa epävakautta sähköjärjestelmään tai heikentää mielikuvia järjestelmän luotettavuudesta. Tarkoitusperät tällä toiminnalla voivat liittyä yhteiskunnallisen epävakauden aiheuttamiseen.

3.2.2. Seuraukset

Riskin toteutumisen vaikutukset havaittaisiin heti, jos tilanne kohdistuisi operatiivisesti tärkeisiin tietoihin. Tällöin riskin seuraukset kohdistuvat taloudellisiin vaikutuksiin, sähköjärjestelmän vakauteen ja yleiseen luottamukseen.

Riskin seurauksena voi olla merkittävää haittaa järjestelmän joustoon osallistuville toimijoille. Haitta syntyisi

tilanteessa, että perustietojen virheellisyyden vuoksi joustoresursseja ei hyödynnettäisi lainkaan tai vain osittain. Tällöin luonnollisesti joustoon osallistumisen taloudelliset hyödyt jäisivät saamatta.

Joustoresurssien perustietojen tuhoutuminen tai virheellisyys voisi teknisestä toteutustavasta riippuen aiheuttaa sähköjärjestelmän säätömekanismien toiminnan häiriöitä. Mikäli virhe koskisi merkittävää joustoresurssia, voi sähköjärjestelmän vakaus olennaisesti vaarantua. Tämä tapahtuisi silloin, kun tietojen tuhoutuminen vaikuttaisi suoraan järjestelmän tekniseen toimintaan. Tällöin tavanomaiset tuotannon ja kysynnän marginaalit eivät riittäisi järjestelmän tasapainottamiseen. Sähköjärjestelmän tasapaino häiriintyisi olennaisesti, ja tilanne voisi johtaa sähkönjakelun häiriöihin.

Riskien seurauksena yleinen luottamus sähköjärjestelmän vakauteen voi vaarantua.

3.2.3. Hallintakeinoja

Riskin hallitsemiseksi älykkään sähköjärjestelmän jatkosuunnittelussa tulisi kiinnittää huomiota seuraaviin seikkoihin.

Koska perustietojen oikeellisuudella on vaikutusta sähköjärjestelmän vakauteen, on vastuu tietojen oikeellisuudesta oltava selkeä. Tietosisältöä ylläpitävät hajautetusti sähköjärjestelmän eri osapuolet. Vastuiden tulisikin olla selkeitä tietojen perustamisen ja säännöllisen seurannan näkökulmasta. Ongelmatilanteissa virheen tehneen tahon sanktiointi voi tulla kyseeseen.

Tietosisällön suojaustoimenpiteillä on keskeinen merkitys perustietojen suojauksen kannalta. Suojaustoimenpiteillä tulisi pyrkiä siihen, että tietosisällön virheelliset muutokset eivät aiheuta epävakautta sähköjärjestelmässä. Perinteisten tietojärjestelmäsuojausten ohella esimerkiksi data-analytiikan keinoin on mahdollista arvioida sitä, ovatko annetut syötteet ylipäänsä mahdollisia, kokoluokaltaan tai trendiltään uskottavia, ja järjestelmän toiminnan kannalta turvallisia.

Tietojen poistotoimenpiteiden tulisi olla peruutettavissa. Tietosisällön säännöllisellä varmuuskopiolla varmistetaan tietojen saatavuus tilanteissa, joissa esto- ja peruutustoimenpiteet eivät ole riittäviä.

3.3. JOUSTORESURSSIEN MITTAUS- JA TASETIETOJEN TUHOUTUMINEN TAI VIRHEELLISYYS

Joustoresurssien mittaus- ja tasetietojen tuhoutuminen tai virheellisyys voi tapahtua teknisen virheen tai tahallisen toimenpiteen seurauksena. Riskien operatiiviset vaikutukset eivät ulottuisi suoraan joustoresurssien toimintaan, sillä se ei teknisesti estäisi resurssien osallistumista joustoihin. Sen sijaan joustojen toteutumisesta automatiikalla kerättävä mittaustieto ei olisi saatavilla, tai osoittautuisi olennaisesti virheelliseksi. Tilanne olisi ongelmallinen maksettavien korvausten näkökulmasta ja voisi ainakin yksittäistapauksissa johtaa pitkittyneisiin riitatilanteisiin.

Joustoresurssien mittaus- ja tasetiedoilla tarkoitetaan niiden käyttötietoa, joiden perusteella joustoon osallistuneet toimijat ovat oikeutettuja taloudellisiin kompensaatioihin. Kompensaatioiden näkökulmasta on keskeistä, että jouston määrä ja ajoitus tallennetaan tarkasti. Tiedot kerättäisiin keskitettyyn tasetietojärjestelmään.

3.3.1. Taustatekijät

Mittaustiedot kerätään ja käsitellään automatisoiduissa prosesseissa. Tahattoman virheen mahdollisuus on siksi hyvin epätodennäköinen mutta voisi tapahtua joissakin tilanteissa manuaalisten korjausten yhteydessä. Pääasiassa riskin voi kuitenkin nähdä muodostuvan tahallisen väärinkäytöksen mahdollisuudesta.

Joustoresurssien mittaus- ja tasetietoihin liittyy taloudellinen intressi. Tietoja manipuloimalla on mahdollista saavuttaa huomattavia voittoja, esimerkiksi saamalla perusteetonta kompensaatiota joustoon osallistumisesta. Tietoihin liittyvät väärinkäytökset aiheuttaisivat voimakasta luottamuksen heikkenemistä järjestelmään, jos väärin toiminut osapuoli olisi esimerkiksi jousto-operaattori.

Taseselvitykseen liittyvän tietojärjestelmän tietomurron yhteydessä verkkorikollinen taho voisi pyrkiä ottamaan tietosisällön panttivangiksi. Tämä tapahtuisi salaamalla tai muutoin muuttamalla tiedot siten, että ne olisivat käyttökelvottomia. Rikollisen tavoitteena olisi saada maksusuorite esimerkiksi kryptovaluuttana tietojen palauttamiseen tarvittavaa salausavainta tai muuta keinoa vastaan.

3.3.2. Seuraukset

Riskin seuraukset kohdistuvat taloudellisiin vaikutuksiin ja yleiseen luottamukseen. Seurausten ytimessä olisivat kiistat toteutuneiden joustojen korvausten tasosta. Mittaustietojen puuttuessa jouduttaisiin tukeutumaan mahdollisesti tulkinnanvaraisiin lähteisiin asiaan liittyvässä todistelussa. Tulkinnat korvausten määrästä voivat yksittäistapauksissa vaihdella eri osapuolten kesken siinä määrin, että asiat riitautuvat. Tilanne olisi omia heikentämään luottamusta älykkään sähköjärjestelmän toiminnasta, ja vaikuttaisi varmasti osapuolten riskiarvioihin. Tämä voi heikentää halukkuutta osallistua joustoihin ja viivästyttää merkittäviä investointipäätöksiä järjestelmään.

3.3.3. Hallintakeinoja

Riskin hallitsemiseksi älykkään sähköjärjestelmän jatkosuunnittelussa tulisi kiinnittää huomiota seuraaviin seikkoihin.

Yhtenä hallintakeinona voitaisiin arvioida mahdollisuus sanktioida mittaustiedon manipulointi ja sen välityksen häirintä. Joustoresurssin haltijan tulisi osaltaan huolehtia siitä, että laitteen toiminta tai muut laitteet eivät vaikuta mittaustiedon oikeellisuuteen tai sen keräämiseen. Vastaavasti palveluntarjoajilla on oltava oikeat kannustimet varmistaa tiedon oikea-aikaisuus ja oikeellisuus.

Taseselvityksen mittaus- ja tiedonsiirtoketjun tekniset suojaukset ovat keskeinen keino estää tahallisia väärinkäytöksiä. Ketjuun liittyviä laitteita ja tietojärjestelmiä on useita mittalaitteista laskutusjärjestelmiin saakka. Prosessin luotettavuuden varmistamiseksi kaikkien niiden turvallisuustaso on varmistettava.

Ristiriitatilanteiden ratkaisemisessa käytetään sopimuksissa määriteltyjä instrumentteja, olisi kyseessä sitten jousto-operaattorin ja sen asiakkaan välisestä ristiriidasta, tai jousto-operaattorin ja jakeluverkkoyhtiön välisestä. Sopimusrakenteiden suunnittelussa tulisi huomioida mahdollisuus eri osapuolten näkemyseroihin toteutuneista joustoista. Kun molemmat osapuolet saavat mittatietonsa omista järjestelmistään, näkemyserot ovat jossakin suhteessa jopa todennäköisiä. Lisäksi pitäisi myös kiinnittää huomiota siihen, että jousto-operaattorin ja avoimen toimituksen sähkönmyyjän välisten ristiriitatilanteiden ratkaisemiseen on instrumentit. Näiden välillä ei välttämättä ole sopimusta.

Teknisenä ratkaisuna voidaan hyödyntää kolmannen osapuolen tuottamaa mittaustietoa. Mittaukseen käytettävän järjestelmän voi toimittaa luotettu osapuoli, jolla ei ole taloudellista intressiä mittatietojen tuloksiin.

3.4. REAALIAIKAISEN MARKKINAN HÄIRIÖ

Älykkään sähköjärjestelmän keskeinen osa on nykyistä reaaliaikaisempi sähkömarkkina, jossa kaupankäynti voisi tapahtua minuuttien tai jopa sekuntien jaksoissa. Kaupankäynnin nopeutuminen tarkoittaa, että se siirtyy yhä enemmän automaattien ja algoritmien tehtäväksi.

Algoritmien optimointiin liittyy merkittävillä sähköntuottajilla ja -käyttäjillä merkittäviä taloudellisia intressejä. Myyjä haluaa tuotteelleen parhaan mahdollisen hinnan ja ostaja hankkia mahdollisimman halvalla. Mitä herkemmin algoritmit reagoivat markkinoiden muutoksiin ja toisten markkinaosapuolten tekemisiin, sitä enemmän markkinoilla on mahdollista saada etua. Tämä lisää algoritmien ylireagoinnin ja siitä aiheutuvien häiriöiden mahdollisuutta.

3.4.1. Taustatekijät

Reaaliaikaisen markkinan häiriö voi syntyä tahattomasti nopean kaupankäynnin algoritmien virheiden vuoksi. On myös mahdollista, että tahallinen uhkatoimija pyrkii manipuloimaan kaupankäyntiä saadakseen perusteetonta etua tai pyrkiäkseen hämmentämään sähkömarkkinoiden toimintaa.

Voidaan kuvitella uhkatoimija, jonka tarkoituksena on huojuttaa sähkömarkkinan toimintaa manipuloimalla kaupankäyntiä. Tällainen toimija voi esimerkiksi pyrkiä toimimaan markkinoilla tavalla, joka saa muiden toimijoiden osto- ja myyntialgoritmit käyttäytymään epätoivotusti. Erityisen tuloksellista tämä olisi silloin, jos manipuloinnilla olisi mahdollista saada aikaan joukkokäyttäytymistä, joka voimistaisi muutosta ja tekisi koko markkinasta epästabiilin. Tällainen voisi olla esimerkiksi voimakas markkinoiden heilahtelu, joka vaikuttaisi mahdollisesti myös sähkönkäyttäjien joustoresurssien ohjailuun automaattisesti.

Selkeän turvallisuusnäkökulmasta suojattavan kohteen muodostaa itse kaupankäynnin alusta. Uhkatoimija, jonka tavoitteena on markkinan manipulointi, voi nähdä alustan houkuttelevana kohteena. Alustan väärinkäyttö tai siihen murtautuminen voi olla mahdollista, jos sen turvallisuussuunnittelu ei ole riittävää. Alustaan murtautumisella voi olla mahdollista saada myös taloudellista etua suhteessa muihin markkinatoimijoihin.

3.4.2. Seuraukset

Riskin seuraukset olisivat odotettavasti taloudellisia, mutta mahdollisesti myös vaarantaisivat sähköjärjestelmän toiminnallisen vakauden. Uhkatoimija voi hankkia taloudellisia hyötyjä muiden kustannuksella, jos hän löytää tavan manipuloida markkinoiden toimintaa huomaamatta. Tämä voisi tapahtua erityisillä syötteiden yhdistelmillä, jotka aiheuttavat ennalta arvattavia reaktioita muiden osapuolten osto- ja myyntialgoritmeissa. Mikäli tällainen toiminta jatkuu pitkän ajan kuluessa, voivat vääryydellä saadut taloudelliset hyödyt olla mittavia.

Sähköjärjestelmän vakaus vaarantuu tilanteessa, jossa markkinoilla sovitut toimitukset eivät toteudu kuten pitäisi. Tällöin tuotantoon ja kysyntään syntyy olennainen epätasapaino. Sellainen uhkatoimija, jonka tavoitteena on sähköjärjestelmän vakauden horjuttaminen, voisi toimia tarkoituksella tällä tavalla.

3.4.3. Hallintakeinoja

Riskin hallitsemiseksi älykkään sähköjärjestelmän jatkosuunnittelussa tulisi kiinnittää huomiota siihen, miten markkinapaikan haitallista toimintaa voidaan estää ennalta ja miten siihen voitaisiin reagoida tehokkaasti.

Markkinan suunnittelu ja pelisäännöt tulisi laatia siten, että häiriökäyttäytymiselle asetetaan selkeät tunnusmerkit ja sanktiot. Näin on nykytilanteessa jo osin tehty, mutta näiden sääntöjen riittävyyttä tulisi tarkastella tulevien kaupankäynnin muutosten näkökulmasta.

Markkinapaikan nopeaa ja kaoottista heilahtelua voidaan torjua erilaisilla tarjouksia rajoittavilla säännöillä.

Esimerkiksi yksittäisen tarjouksen kokoa tai muutosta markkinatasoon voitaisiin rajoittaa. Tällaisilla rajoituksilla on negatiiviset puolensa. Hyötyjen ja haittojen tasapainottamista tulisi arvioida jatkotyössä.

Eräänä hallintakeinona voitaisiin toteuttaa markkinan toiminnan reaaliaikainen seuranta ja mahdollisuus reagoida nopeasti erityistoimenpiteillä järjestelmän vakauttamiseksi. Erityistoimenpiteet itsessään voivat olla osittain automatisoituja sääntöjä esimerkiksi kaupankäynnin ylikuumenemisen ja heilumisen rajoittamiseksi.

4. SUOSITUKSIA JATKOTYÖLLE

Tämä raportti on ensimmäinen älyverkkotyöryhmän kyberturvallisuutta koskevista selvityksistä. Edellä kuvatut ehdotukset hallintakeinoiksi ovat tarkoitettu keskustelunavaukseksi. Toteutettavia hallintakeinoja valittaessa ja suunniteltaessa on tärkeää arvioida niillä saavutettavat hyödyt ja haitat. Tämä arviointi ei ollut osa nyt tehtyä työtä. Älyverkkotyöryhmän pohdittavaksi jää, millaisten hallintakeinojen valikoimaa älyverkon jatkovalmistelussa on tarkoituksenmukaista soveltaa.

Älyverkkotyöryhmän myöhemmissä vaiheissa tämän raportin tuloksia tulisi käyttää älyverkon toiminnallisten ja turvallisuusvaatimusten määrittämiseen, näiden kustannus-hyöty –analyysiin, ja muiden valmisteluun liittyvien päätösten tukena. Erityisen tärkeää jatkotyössä olisi varmistaa, että kyberturvallisuuteen liittyvät kysymykset ovat soveltuvin osin mukana tiedonvaihtovision ja aihepiiriin liittyen teknisten määritysten, kuten seuraavan sukupolven AMR-järjestelmän, valmistelussa.

Tiedonvaihtovision osalta tulisi arvioida vaikutukset, jotka erilaisten tietotyyppien virheellisyydestä tai viivästymisestä voi aiheutua. Virheet tietoprosesseissa voivat olla taustatekijänä kaikissa tässä raportissa eritellyissä riskeissä. Joihinkin tietotyyppeihin voidaan katsoa liittyvän myös luottamuksellisuusnäkökulmia. Tietosuojanäkökulmasta elinolosuhteita ja siten myös sähkönkäyttöä kuvaavat tiedot ovat henkilötietoja. Osa vaihdettavista tiedoista voi olla luottamuksellisia kilpailullisista syistä.

Älykkään sähköjärjestelmän teknisten määritysten valmistelussa tulisi huomioida internetiin kytkettyjen laitteiden tekninen turvallisuus koko niiden elinkaaren aikana. Tämä tarkoittaa turvallisten ohjelmistojen saatavuuden varmistamista ja internetiin kytkettyjen ohjausrajapintojen toteuttamista siten, että ne luvaton ohjailu ei ole mahdollista. Vastuu laitteiden turvallisuudesta tulisi olla selkeä osapuolten kesken.

Sähkömarkkinan muutoksia valmisteltaessa tulisi arvioida millaisilla säännöillä ja automatiikalla voitaisiin estää sellaisten markkinahäiriöiden syntyminen, joilla voisi olla vakavia vaikutuksia sähkön toimitukseen. Kaupankäynnin nopeutuessa ja automatisoituessa myös hallintakeinoilla tulisi pystyä reagoimaan tahallisiin tai tahattomiin häiriöihin nopeasti.

F-Secure suosittelee, että raportti lähetetään kommentoitavaksi soveltuville sidostahoille riskejä ja hallintakeinoja koskevien näkemysten täydentämiseksi.

5. JÄLKISANAT

Tämä raportti pitää sisällään kyberturvariskien kartoituksen aikana tehdyt havainnot. Raportin tuloksia on tarkoituksenmukaista hyödyntää älyverkkotyöryhmän myöhemmissä vaiheissa älyverkon toiminnallisten ja turvallisuusvaatimusten määrittämiseen, näiden kustannus-hyöty –analyysiin, ja muiden valmisteluun liittyvien päätösten tukena.

F-Secure ja toimeksiannon vastuukonsultti vastaavat mielellään kaikkiin tilaajan kysymyksiin toimeksiantoon ja raporttiin liittyen.