KYBER-ENE Energia-alan kyberturvaaminen 1-2

Julkisten tulosten kooste

HUOLTOVARMUUSKESKUS
FÖRSÖRJNINGSBEREDSKAPSCENTRALEN
NATIONAL EMERGENCY SUPPLY AGENCY

KYBER-ENE

Energia-alan kyberturvaaminen 1-2

Julkisten tulosten kooste

Varautumispäällikkö Kalle Luukkainen
Huoltovarmuuskeskus

Johtava tutkija, projektipäällikkö Pasi Ahonen ja
Erikoistutkija Juha Pärssinen, VTT

Automaation tietoturva-asiantuntija Jari Seppälä
Tampereen yliopisto

Tekninen editointi ja taitto: Päivi Vahala | VTT

www.huoltovarmuus.fi

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

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

www.vtt.fi

Teknologian tutkimuskeskus VTT Oy on kansallisella statuksella toimiva Pohjoismaiden johtava tutkimus- ja teknologiayhtiö. Tuotamme tutkimuksen ja tiedon kautta asiantuntijapalveluja kotimaisille ja kansainvälisille asiakkaillemme, liike-elämälle, julkisille sektorille ja kumppaneillemme.

www.tuni.fi

Tampereen korkeakouluyhteisössä tehtävä tutkimus paneutuu etenkin tekniikan, terveyden ja yhteiskunnallisiin kysymyksiin. Yhteisössä toimii lukuisia tutkimusryhmiä ja verkostoja, jotka tekevät monitieteistä ja -alaista tutkimusta yli organisaatiorajojen.

Julkaisija: Huoltovarmuuskeskus
Teksti ja kuvitus: Pasi Ahonen, VTT
Taitto: Päivi Vahala, VTT
Kansikuva: Pasi Ahonen, VTT
Painotalo: Edita
Julkaisuvuosi: 2019

ISBN 978-952-5608-69-4 Energia-alan kyberturva (nid.)
ISBN 978-952-5608-70-0 Energia-alan kyberturva (pdf)

SISÄLTÖ

KUVAT JA TAULUKOT

,

SAATTEEKSI

Kalle Lunkkainen

Huoltovarmuuskeskus
Varautumispäällikkö, kyberturvallisuus
Aleksanterinkatu 48 A 00100 Helsinki
www.huoltovarmuus.fi

Energia-alan kyberturvallisuutta kehittävä KYBER-ENE-hanke toteutettiin useiden alan keskeisten yritysten, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen, Huoltovarmuuskeskuksen ja VTT:n yhteistyönä. Tavoitteena oli tuottaa konkreettisia ja liiketoimintalähtöisiä ratkaisuja energia-alan yritysten tarpeisiin. KYBER-ENE on osa Huoltovarmuuskeskuksen kyberturvallisuuden kehittämiseen tähtäävää Kyber2020-ohjelmaa, ja osa vuosia jatkunutta elinkeinoelämän, hallinnon ja tutkimuksen yhteistyötä kriittisen infrastruktuurin kyberturvallisuuden parissa.

Keskeistä KYBER-ENE-hankkeen onnistumiselle on ollut energia-alan yritysten sitoutuminen. Hankkeen aktiivinen ohjaus ja erityisesti yritysten vertaistuki on auttanut luomaan käytännöllisiä yrityksiä hyödyttäviä tuloksia.

Hankkeen puitteissa kehitettiin kyberturvallisuuden ohjaus- ja toimintamallia erityisesti keskisuurten ja pienempien energia-alan yritysten tarpeisiin. Yrityskohtaisissa työpajoissa päästiin jakamaan ja soveltamaan alan parhaita käytäntöjä. Toisena keskeisenä teemana oli energia-alan IoT-sovellusten kyberturvallisuuden kehittäminen kaikkien alan yritysten tarpeisiin. Hankkeessa kehitettiin myös häiriötilanteiden toimintamalleja sekä yrityskohtaisissa työpajoissa että laaja-alaisissa kyberharjoituksissa.

Tässä julkaisussa kuvatut ja alan toimijoiden kanssa kehitetyt, käytännössä koetellut toimintatavat ja ratkaisumallit hyödyttävät energia-alan toimijoita laajemminkin. Tuloksia tullaan hyödyntämään mm. Kyberturvallisuuskeskuksen yhteistyöverkostoissa. Myös alan ohjelmisto- ja järjestelmätoimittajilla sekä palveluntarjoajilla on keskeinen rooli tulosten viemisessä käytäntöön. Yritysten keskinäinen yhteistyö ja muiden mukana olleiden tahojen tuki on luonut vahvan perustan energia-alan kyberturvallisuuden jatkokehittämiselle.

YHTEENVETO

Pasi Ahonen

Teknologian Tutkimuskeskus VTT Oy
Johtava tutkija, projektipäällikkö
Kaitoväylä 1, 90570 Oulu
www.vtt.fi

Rajaus: Energia-alan tiedonvaihtoryhmä (E-ISAC) sekä Huoltovarmuusorganisaation Voimatalouspooli ovat asettaneet KYBER-ENE hankekokonaisuuden tavoitteet, joten tässä kirjassa keskitytään näihin tavoitteisiin liittyviin tehtäviin ja tuloksiin.

Tausta: Edulliset ympäristömittaukset (*Internet of things*, IoT) kytketään yhä hanakammin Internetin pilvipalveluihin. Internetin toimintaan sidottu automaatio lisää kyberturvallisuusuhkia energia-alan toimijoiden keskuudessa, jolloin kyberriskit uhkaavat jopa tuotantotoiminnan jatkuvuutta, puhumattakaan teknologiavakoilusta.

Uhat: Kyberriskit voivat toteutuessaan uhata energia-alan perustoimintoja, kuten energian tuotantoa, siirtoa, jakelua, sekä niihin liittyviä palveluja. Kotimaiseen energia-alaan kohdistuu mm. seuraavan tyyppisiä kyberturvallisuusuhkia:

- tietojen kalastelua etenkin pilvipalvelujen käyttöönoton jälkeen,
- palvelunestohyökkäyksiä,
- liiketoiminnan esto kiristyshaittaohjelmistoilla,
- järjestelmien ja laitteiden etäohjaukseen liittyvät uhat,
- hyökkäykset haavoittuvien rakennusautomaatiojärjestelmien kautta,
- heikosti suojatun IoT:n käyttöönottoon liittyvät uhat,
- teollisuusvakoilu, tietovuodot, -murrot ja -varkaudet, sekä
- soluttautuminen Suomen kriittiseen infrastruktuuriin.

Yhteistoiminnan vaatimus: Energia-alan täytyy ymmärtää entistäkin paremmin teknisten kyberturvaratkaisujen rajoitteet ja toisaalta uusien uhkien synnyttämät uudet vaatimukset. Tämä edellyttää hyvää yhteistoimintaa useiden eri tahojen kesken, kuten:

- energiayritykset,
- automaatiojärjestelmätoimittajat,
- ICT- ja tietoturvapalvelujen tarjoajat,
- viranomaiset kuten Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus,
- yliopistot ja tutkimuslaitokset.

Hanke: Energia-alan kyberturvallisuutta kehittävät Huoltovarmuuskeskuksen hankkeet KYBER-ENE 1 (11/2017 – 04/2018) ja KYBER-ENE 2 (06/2018 – 06/2019) toteutettiin fokusoituina projekteina

energia-alan avaintoimijoille. Näin haluttiin varmistua riittävän hyvästä tulosten kohdentamisesta, yhteistyöstä ja alalle tärkeiden kysymysten huomioon ottamisesta. Projektien osallistujina olivat kriittisiä energiatuotteita ja -palveluja tuottavat avaintoimijat, sekä energian tuotantoa, siirtoa ja jakelua ylläpitävät ja varmistavat kriittisen infrastruktuurin avaintoimijat.

Tehtäväalueet: KYBER-ENE hankekokonaisuus toimii osana Huoltovarmuuskeskuksen KYBER-2020 ohjelmaa. Hankkeissa keskityttiin seuraaviin tehtäviin:

- Luottamukselliset yrityskohtaiset työpajat energialaitoksissa
- Kyberturvallisuuden hallinnan kehittäminen ja hallintamallin käyttöönotto
- Teollisuuden IoT-toimittajien arviointi
- Teematyöpajat ja seminaarit:
  - Havainnointikyky ja omaisuuden hallinta
  - IoT:n turvallinen hyödyntäminen
  - Yhteistyö- ja uhkakommunikaatio (sisältäen kyberharjoittelun)

Osaksi päivittäistä työtä: Kyberturvallisuuden ylläpito ja kehitys on saatava osaksi päivittäistä rutiinityötä. Olemme vahvasti sitä mieltä, että erityisesti energia-alan PK-yrityksen kyberturvallisuus saadaan varsin hyvälle tasolle laittamalla kyberturvallisuuden perusasiat ensin kuntoon. Myös kehittyneiden hyökkäysten onnistuminen heikentyy huomattavasti, mikäli kaikki yrityksen työntekijät ja kumppanit, aina liiketoimintajohtajasta alihankkijana toimivaan vartijaan asti, osaavat omassa työssään toimia tietoturvallisella tavalla. Perusosaamisen ja tietoisuuden kehittämistä ja levittämistä tulee jatkaa, kunnes kaikki energia-alalla toimivat yritykset on saatu ymmärtämään kyberturvallisuuden kasvanut merkitys oman liiketoimintansa jatkuvuudelle ja toteuttamaan tarvittavat toimenpiteet.

Yritysten työsarka: Hyvä kehitys saadaan vauhtiin jokseenkin tässä järjestyksessä:

- johdon tietoisuus kuntoon,
- nykytilan kartoitus,
- kehityskohteiden tunnistaminen ja keskustelu,
- kehitysryhmän perustaminen,
- vuosisuunnitelma, kehityshankkeiden määrittely,
- kehittämisen budjetointi, tehtävien ja vastuiden jako,
- tilannekuvan seuranta johdossa.

Verkostoituminen: Energia-alan yritysten on verkostoiduttava keskenään:

- luottamuksellisen uhkatiedon jakamiseksi yhteisön sisällä,
- toimivan vertaistuen synnyttämiseksi ja toteuttamiseksi,
- edelläkävijöiltä oppimisen mahdollistamiseksi,
- parhaiden käytäntöjen siirtämiseksi,
- hyvien ja huonojen kokemusten jakamiseksi.

Yhteistyö ja kyberharjoittelu: Kyberturvallisuusharjoittelu on erinomainen tapa tunnistaa puutteita energiayritysten henkilöstön jatkuvuuden hallinnan käytännöissä ja osaamisessa:

- Harjoitus voi osoittaa puutteita esim. kumppanien varautumisessa tai ilmetä vaikeutena hahmottaa omaa tilannekuvaa.
- Uhka- ja häiriötilanneviestintä on yksi tärkeimmistä asioista, joita voidaan tehokkaasti kehittää kyberturvallisuusharjoituksen oppien avulla.
- Puutteet voivat löytyä sekä yrityksen sisäisestä (liiketoiminnot, osastot), että yritysten välisestä viestinnästä (kumppanit, alihankkijat).

Havainto ja varoitus tietomurrosta tulee valitettavasti edelleen useimmiten liian myöhään ja vieläpä uhriyrityksen havaintokyvyn ulkopuoliselta taholta.

KIITOKSET

Erinomaisen suuret kiitokset kaikille teille, jotka osallistuitte KYBER-ENE 1 ja 2 projektien suunnitteluun, toteutukseen sekä samalla tämän julkaisun substanssin kehittämiseen. Tämä on ollut hieno yhteinen matka ja samalla ponnistus, jolla voi tulevaisuudessa olla paljonkin merkitystä yhteiskuntamme turvallisuuden kehittymiselle. Toivottavasti yhteistyö jatkuu.

Seuraavat yritykset ja asiantuntijat osallistuivat tämän julkaisun kuvaamien sisältöjen ja tulosten yhteiseen kehittämiseen sekä antoivat luvan nimensä mainitsemiselle:

ABB Drives:
- Mika J. Kärnä

ABB Distribution Solutions:
- Jani Hirvo, Petri Hovila ja Antti Laine

BaseN (kiitokset tuesta IoT-työpajassa):
- Pasi Hurri, Topi Mikkola ja Kaj Niemi

Fingrid:
- Jyrki Pennanen ja Olli Aaltonen

Fortum:
- Jarmo Huhta

Frontdrivers:
- Kari Helislahti

F-Secure:
- Kristian Berg, Janne Taponen, Jukka Savolainen ja Eemeli Ollila

HELEN:
- Tapio Heinäaro

Huoltovarmuuskeskus:
- Kalle Luukkainen ja Petri Nieminen

Insta Group:
- Tero Leppänen ja Marko Hautakangas

Jyväskylän Energia:
- Aki Finer, Marjut Jaatinen, Mikko Malinen, Marko Metiäinen, Viivi Nuojua ja Riikka Uosukainen

Kuopion Energia:
- Jami Miettinen ja Reijo Malinen

Napapiirin Energia ja Vesi:
- Kasperi Havupolku

Neste:
- Tomi Pitkänen

Nixu:
- Erika Suortti-Myyry

Savon Voima:
- Janne Pollari, Tuukka Miettinen, Timo Kiiski ja Jukka Kauppinen

Suur-Savon Sähkö:
- Pekka Nurmi

Tampereen Sähkölaitos:
- Ville Kouhia, Jouni Lahti, Suvi Suojanen, Jouni Vanhanarkaus ja Mikko Viitanen

Tampereen Yliopisto:
- Jari Seppälä

VTT:
- Pasi Ahonen, Hannu Honka, Jani Koivusaari, Pekka Koponen, Jarkko Kuusijärvi, Sami Noponen, Juha Pärssinen ja Pia Raitio

Traficomin Kyberturvallisuuskeskus:
- Juha Ilkka, Jukka Isosaari, Ilkka Demander, Harri Koivunen, Lotta Kulta, Antti Kurittu, Jukka Käyhkö, Jarmo Lahtiranta, Sami Orasaari, Sauli Pahlman, Miikka Salonen, Saana Seppänen, Erika Suortti-Myyry, Pekka Tetri, Riikka Valtonen, Teemu Väisänen

TVO:
- Jani Järvenpää, Timo Vaahtera, Lauri Tuominen ja Esko Rauta

Valmet:
- Markku Tyynelä, Ari Rajamäki, Teemu Kiviniemi, Kimmo Djupsjöbacka, Lauri Jämsä, Markus Palokangas ja Jani Kivikoski

Wapice (kiitokset tuesta IoT-työpajassa):
- Teemu Niemi

JOHDANTO & KYBER-ENE projektin esittely

Kuva: Pasi Ahonen

1. JOHDANTO & KYBER-ENE PROJEKTIN ESITTELY

Lukijan perehdyttämiseksi tämän kirjasen aihepiiriin, aloitamme alan luonteenomaista taustaa selventävällä johdanto-osuudella, sekä jatkamme lyhyellä ”Energia-alan kyberturvaaminen” eli KYBER-ENE -hankekokonaisuuden yleisesittelyllä.

1.1 Johdanto

Jatkuvasti lisääntyneen verkostoituneen automaation käyttöönoton myötä kyberturvallisuusuhat (ja niiden pakollinen huomioiminen) ovat tulleet jäädäkseen myös energia-alan toimijoiden keskuuteen. Enää ei riitä, että energia-alan automaatiojärjestelmiä hankitaan ja ylläpidetään pelkästään tuotantotehokkuuden ja siihen liittyvän uuden toiminnallisuuden kehittämisen näkökulmista.

Tämä johtuu siitä, että kyberturvallisuusriskit voivat tulevaisuudessa uhata tuotantotoiminnan jatkuvuutta, järjestelmien kehittämisen tietosuojasta puhumattakaan. Tietovuotoja ja -varkauksiahan on jo paljon tapahtunut ja tulee tapahtumaan jatkossakin, mutta lisääntyneet kyberturvallisuusriskit voivat toteutuessaan uhata energia-alan perustoimintoja, kuten tuotantoa, siirtoa, jakelua, sekä niihin liittyviä palveluja.

1.1.1 Energia-alan kyberturvallisuusuhat

Kansainvälisessä katsannossa energia-alaan on kohdistunut kyberturvallisuushyökkäyksiä jo muutaman vuosikymmenen ajan. Varhaisena esimerkkinä toimikoon alla oleva ote RISI (*Repository of Industrial Security Incidents*) -tietokannan ensimmäisestä häiriötapauksesta, jossa kaasuverkon ohjaukseen (tai testaukseen) käytetyssä ohjelmistossa väijyneen troijalaisen väitetään aiheuttaneen massiivisen räjähdyksen Neuvostoliiton Siperian kaasuverkossa kesäkuussa 1982.

> Ref: “Thomas Reed, senior US national security official, claims in his book “At The Abyss” that the United States allowed the USSR to steal pipeline control software from a Canadian company. This software included a Trojan Horse that caused a major explosion of the Trans-Siberian gas pipeline in June, 1982. The Trojan ran during a pressure test on the pipeline but doubled the usual pressure, causing the explosion.”
>
> - www.risidata.com[1] -

Kotimaan osalta olemme olleet kyberturvallisuusasioissa jo varhain liikkeellä. Erityisesti *Ethernet*-pohjaisten lähiverkkojen yleistyessä Suomessa 1990-luvun vaihteen tienoilla, varsinkin alan edelläkävijäyrityksissä (mm. Neste) alettiin ymmärtää tietoverkoissa leviävien haitallisten ohjelmistojen, ns. tietokonevirusten, voivan uhata myös tuotannossa olevien IT-järjestelmien toimintaa. Aloitettiin mm. dataverkkojen segmentointiin liittyvää suunnittelua, jossa rajoitettiin esimerkiksi ”suodattavien datasiltojen” ja reitittimien avulla haitallisten verkkovikojen tai datamyrskyjen vaikutusten siirtymistä verkosta toiseen. Toisaalta myös valokaapeliasennuksin suojauduttiin erityisesti salakuuntelua vastaan, varsinkin rakennusten välisissä datakaapeloinneissa tai muissa ”ulkoisille vaikutuksille” alttiiksi joutuvissa datayhteyksissä.

Vuonna 2005 Suomen Automaatioseura julkaisi laajassa kotimaisessa yhteistyössä kirjoitetun kirjan ”Teollisuusautomaation tietoturva – Verkottumisen riskit ja niiden hallinta” [SA], josta pitkäjänteinen automaation tietoturvatyö voidaan katsoa Suomessa alkaneen.

2010-luvulle saavuttaessa kyberturvallisuuteen liittyvät uhat olivat ehtineet kehittyä tarpeeksi laajoiksi ja vakaviksi, jotta ne alkoivat kiinnostaa jatkuvasti myös tiedotusvälineitä, erityisesti sähköistä mediaa. Kesäkuussa 2010 valkovenäläinen turvallisuusyritys VirusBlokAda raportoi Stuxnetistä, ensimmäisestä verkkomadon tavoin (itsestään) leviävästä haittaohjelmasta, joka vakoilee ja uudelleenohjelmoi teollisuusjärjestelmiä. Erityisesti Stuxnetin jälkeen kiinnostus teollisuu-

[1] https://www.risidata.com/Database/event_date/asc

delle suunnattuihin kyberturvallisuusalan palveluihin heräsi myös Suomessa. Tästä huolimatta kotimaisen teollisuuden panostukset kyberturvallisuuteen eivät nousseet kovin suuriksi.

2010-luvun jälkipuoliskolla energia-alaan kohdistuvat kyberhyökkäykset eivät olleet enää pelkästään yksittäistapauksia, vaan vakavimmat niistä olivat osia laajemmista, jatkuvasti uusiutuvista kyberhyökkäys- tai vakoilukampanjoista. Keskustelu joidenkin valtiollisten tahojen tilaamista, erittäin kehittyneiden kyberkyvykkyyksien väärinkäytöstä on myös lisääntynyt. Osa nykyisistä kyberhyökkäyksistä voi siis liittyä laajempaan valtioiden väliseen hybridivaikuttamiseen, jossa väärinkäytetään esimerkiksi huoltovarmuuskriittisiä yrityksiä palvelevia sopimuskumppaneita, globaaleja tietojärjestelmiä, ja tuotetaan vähitellen eteneviä, pelkoa tai muuta hajaannusta aiheuttavia tapahtumasarjoja.

Valtiolliset uhat ovat valitettavasti myös Suomessa jo todellisuutta, joten seuraavaksi laittomaan tiedusteluun liittyvä esimerkki. Suojelupoliisin viimeisin ”KANSALLISEN TURVALLISUUDEN KATSAUS” mainitsee energiasektoriin kohdistuvan kybervakoilun kiinnostavan myös valtiollisia tahoja.

> Ref: “Myös Suomeen kohdistuva kybervakoilu on aktiivista. Haittaohjelmahyökkäyksiä on tehty aiempaa enemmän epäsuorasti. Ne ovat kohdistuneet varsinaisille vakoilukohteille palveluja tuottaviin yrityksiin sekä kohteita muuten lähellä oleviin tahoihin. Julkisuudessa Venäjän valtioon liitetyt kybervakoiluyritykset ovat kohdistuneet muun muassa valtionhallinnon organisaatioihin, niiden kanssa yhteistyössä toimiviin yrityksiin sekä energiasektorin tuotekehitystä ja palveluja tuottaviin yhtiöihin.”
>
> - www.supo.fi[2] -

Mikäli energia-alan tärkeimpiä kyberturvallisuusuhkia olisi tarvetta yhteenvedonomaisesti listata, niin voisimme yleisen tietoisuuden herättelemiseksi lausua, että kotimaiseen energia-alaan kohdistuu mm. seuraavan tyyppisiä kyberturvallisuusuhkia:

- tietojen kalastelua etenkin pilvipalvelujen käyttöönoton jälkeen,
- palvelunestohyökkäyksiä,
- liiketoiminnan esto kiristyshaittaohjelmistoilla,
- järjestelmien ja laitteiden etäohjaukseen liittyvät uhat,
- hyökkäykset haavoittuvien rakennusautomaatiojärjestelmien kautta,
- heikosti suojatun IoT:n käyttöönottoon liittyvät uhat,
- teollisuusvakoilu, tietovuodot, -murrot ja -varkaudet, sekä
- soluttautuminen Suomen kriittiseen infrastruktuuriin.

Valitettavasti näiden ongelmien ratkaiseminen ei ole yksinkertaista. Ei ole olemassa yhtä ainoaa ratkaisua, joka ratkaisi kaikki energia-alaa koskevat kyberturvallisuusongelmat, eikä tällaista ole tulevaisuudessakaan odotettavissa. Sen sijaan meidän täytyy ymmärtää entistäkin paremmin nykyisten kyberturvaratkaisujen mahdollisuudet ja rajoitteet, sekä toisaalta uusien uhkien synnyttämät uudet vaatimukset. Tämä edellyttää hyvää yhteistoimintaa useiden eri tahojen kesken, kuten mm. energiayritykset, automaatiojärjestelmätoimittajat, palveluntarjoajat ja viranomaiset.

Uskomme, että kyberturvallisuuden ja jatkuvuuden turvaamisen avainasemassa ovat energia-alan tuotanto-omaisuuden omistajat, käyttäjät ja ylläpitäjät, jotka parhaiten tuntevat järjestelmiensä oikean toiminnan ja asianmukaisen käytön. Vain heidän osaamistasoaan kehittämällä ja ylläpitämällä voimme parhaiten vastata jatkuvasti muuttuviin kyberturvallisuusuhkiin.

1.2 KYBER-ENE projektin esittely

1.2.1 Miksi tarvittiin ”Energia-alan kyberturvaaminen”-hankekokonaisuus

Internetissä syntyneet ja kehittyneet kyberturvallisuusuhat lisääntyivät viime vuosina dramaattisesti ja kohdistuivat lisääntyvässä määriin myös energiateollisuuteen, jonka toimintakyky on Suomelle erittäin kriittistä. Energia-alan kriittisen infrastruktuurin avaintoimijathan (mm. sähkö, kaasu, polttonesteet) mahdollistavat muun yhteiskunnan toimintojen jatkuvuuden. Myös automaatiojärjestelmät, jotka ohjaavat energian tuotantoa, siirtoa

[2] https://www.supo.fi/instancedata/prime_product_julkaisu/intermin/embeds/supowwwstructure/76706_2018_Kansallisen_turvallisuuden_katsaus.pdf

ja jakelua, ovat haavoittuvaisia kyberturvallisuus-uhkille.

Aluksi energia-alan avaintoimijoiden kesken tunnistettiin tarve kehittää koordinoitua kansallista yhteistyötä, jotta voitaisiin varmistaa:

- Riittävä energiayritysten välinen yhteistyö, työnjaon määrittely ja vertaistuki
- Osaamisen & kokemusten jako (onnistumiset, virheet, malliratkaisut)
- Yhteistyömallien synnyttäminen ja koestaminen käytännössä
- Pitkäjänteisyys, tiedonjako, harjoittelu ja jatkuva parantaminen

Tämän jälkeen erityisesti Huoltovarmuuskeskuksessa katsottiin, että yllämainitut tarpeet voitaisiin toteuttaa KYBER-ENE hankekokonaisuuden kautta ja täten organisoimalla käytännössä:

- Alueellisten energiayritysten (mm. PK-yritysten) kyberturvatietoisuuden ja osaamisen kehittämistä pitkällä tähtäimellä
- Teematyöpajojen säännöllistä suunnittelua ja toteutusta
- Yrityskohtaisia työpajoja ja yritysten erityiskysymysten käsittelyä
- Edelläkävijäyritysten parempaa tukea PK-yrityksille, sekä vertaistuen kehittämistä energia-alalle soveltuvaan muotoon
- Yhteisen sähköisen tiedonjakoympäristön käyttöönottoa ja kehittämistä yritysten käytännön tarpeista lähtien.

Energiayrityskohtaisten työpajojen taustalla olivat erityisesti seuraavat tarpeet:

- Kehittää monistettavat työpajat kyberturvallisuuden kehittämiseen
  - Kehittää työpajoissa alueellisten energialaitosten kyberturvallisuustietoisuutta käytännössä
  - Testikohteina olivat SSSOY ja Kuopion Energia sekä yhdistelmätyöpaja kahdelle muulle energiayhtiölle
- Pohtia yhdessä energiayhtiöiden hyviä kyberturvallisuuskäytäntöjä
  - Parantaa parhaiten ymmärrystä, jos osallistujat ovat mukana työpajassa koko päivän
  - Selvittää miten laitetaan perusasiat kuntoon
  - Pohtia mikä malli soveltuu mihinkin tarpeeseen (käyttötapausten pohdintaa)
  - Mallien soveltamista käytäntöön yhdessä!
- Synnyttää yritysrajat ylittäviä ”tiimejä” kyberturvallisuuden mallien kehittämiseen
  - Vahvistaa toimivien ratkaisujen valintaa
  - Vahvistaa edelläkävijäyritysten tukea muille ja samalla jakaa kokemustietoa molempiin suuntiin

VTT sai tehtäväkseen projektivedon ja koordinoinnin. Jotta hankkeen edellyttämä yhteistyö saatiin toimimaan, opittiin varsin nopeasti, että yhdessä kehittämistä helpottaa huomattavasti, mikäli hankkeen osallistujat pystyisivät:

- Työntämään taka-alalle omaa asiantuntijuuspainettaan (oman erityisosaamisen liiallista korostamista)
- Välttää oman alansa erityissanaston liiallista käyttöä
- Kuuntelemaan ja ymmärtämään energia-alan erityisiä ongelmakohtia, olkoonpa ne sitten teknisiä, hallinnollisia, inhimillisiä, tai mitä tahansa siltä väliltä.

1.2.2 KYBER-ENE -hankekokonaisuuden lyhyt esittely

Hanke toteutettiin hyvin fokusoituna energia-alan avaintoimijoille, jotta voitiin varmistua riittävän hyvästä tulosten kohdentamisesta, yhteistyöstä ja alalle tärkeiden kysymysten huomioon ottamisesta.

KYBER-ENE hankekokonaisuuden kohderyhmänä ja osallistujina ovat kriittisiä energiatuotteita ja -palveluja tuottavat avaintoimijat, sekä energian tuotantoa, siirtoa ja jakelua ylläpitävät ja varmistavat kriittisen infrastruktuurin avaintoimijat.

Osana Huoltovarmuuskeskuksen KYBER-2020 ohjelmaa:

KYBER-ENE:ssä kehitetään erityisesti energia-alan toiminnan kyberturvallisuuteen liittyviä kyvykkyyksiä, sekä tuotantojärjestelmien ja tietoliikenteen turvallisuuden varmistamista.

Kuva 1. KYBER-ENE hankekokonaisuuden kohderyhmä.

1.2.2.1 KYBER-ENE -hankekokonaisuuden yleiskuva

Seuraavassa esitetään yleiskuva energia-alan kyberturvaamisen (KYBER-ENE) hankekokonaisuudesta, joka suunnattiin energia-alan yrityksille, automaatiojärjestelmätoimittajille, sekä alan palveluntarjoajille.

Hankekokonaisuus saatiin perusteellisen yhteisen valmisteluvaiheen jälkeen käyntiin marraskuussa 2017 energia-alan peruskyvykkyyksiä kehittävällä KYBER-ENE-1 hankkeella (*11/2017 – 04/2018*). Kokonaisuuden pitkäjänteisyys toteutui jatkohankkeena KYBER-ENE-2 (*06/2018 – 06/2019*), johon osallistui jo varsin edustava joukko kohderyhmien yrityksiä. Erityisesti jatkohankkeessa syntynyt verkostoituminen varmisti tavoitteeksi asetettujen tulosten onnistuneen yhteisen kehittämisen hankkeeseen kuuluneissa työpajoissa sekä sähköisessä ryhmätyötilassa.

Seuraavissa luvuissa esitellään KYBER-ENE hankkeissa kehitettyjä tärkeimpiä julkisia tuloksia, jotta muutkin alan yritykset voisivat hyödyntää saavutettuja tuloksia oman kyberturvallisuutensa sekä siihen liittyvän yhteistyön kehittämisessä. Huom! Osa hankkeen tuloksista oli luottamuksellisia tai esim. liian yrityskohtaisia, joten ne jaettiin erikseen ainoastaan tietyille vastaanottajille, kuten luottamuksellisille tiedonvaihtoryhmille.

Kuva 2. KYBER-ENE hankkeiden yleiskuvaus. Ensimmäinen hanke (KYBER-ENE-1) vasemmalla ja sitä pian seurannut hanke (KYBER-ENE-2) oikealla.

Luku 2

KYBERTURVALLISUUDEN KÄYNNISTÄMINEN ENERGIA-ALAN YRITYKSESSÄ

Kuva: Shutterstock

2. KYBERTURVALLISUUSTYÖN KÄYNNISTÄMINEN ENERGIA-ALAN YRITYKSESSÄ

Kyberturvallisuustyön saaminen laaja-alaisesti käyntiin on ajankohtainen asia myös monessa energia-alan yrityksessä. Ei ole järkevää, että tietoturva-asiat ulkoistetaan tai delegoidaan yhden henkilön hoidettavaksi, koska tällä tavoin kehitetyt menettelytavat ja ohjeet eivät yleensä muotoudu kaikkien ymmärrettäviksi, vaan tärkeä yhteinen asia hautautuu muiden töiden alle. Tilanteen parantamiseksi olemme projektissa tehtyjen kokeilujen kautta kehittäneet erilaisia työpajoja, malleja ja kartoitusmenettelyjä, jotka helpottavat kyberturvallisuustyön käynnistämistä kotimaisissa energia-alan yrityksissä. Näistä kerromme seuraavissa alakohdissa tarkemmin, aloitetaan tuotannon kyberturvan hallintamallin esittelyllä.

2.1 Tuotannon kyberturvan hallintamalli ja sen soveltaminen

Olemme havainneet, että energiayrityksissä tarvitaan tuotannon kyberturvatyön yksinkertaista kokonaiskuvaa, jonka avulla voitaisiin helpottaa kyberturvallisuustarpeiden kommunikointia. Kommunikoinnin tarvetta esiintyy yleisesti mm. liiketoimintajohdon ja yrityksen johtoryhmän suuntaan, jotta yrityksessä ymmärretään millaisia tehtäviä ja resursseja kyberturvallisuuden kehittäminen vaatii. Erityisesti on tarvetta kommunikoida johtoryhmälle säännöllisesti, että missä kehittämisen vaiheessa kulloinkin ollaan menossa ja mitä kehitystehtäviä ollaan suorittamassa.

Seuraavassa kuvassa esitetään tuotannon kyberturvan hallintamalli.

Kuva 3. Tuotannon kyberturvatyön hallintamalli ja elementit.

Hallintamallikuvan keskelle sijoitettuihin tummempiin laatikoihin on nostettu kehittymisen mahdollistajat, eli:

- **Joukkueen kokoaminen** ja tiedon jakaminen, sekä
- **Ymmärrä syyt ja opi** turvallisen toiminnan edellytykset

Hallintamallin elementit tukeutuvat hyvän hallintotavan mukanaan tuomaan perustaan, sillä muutoin kehityshankkeet jäävät tuotannosta irrallisiksi kehityspistoiksi. Kehittämisen perustan muodostavat kolme ylintä elementtiä (kuvassa timantin yläosa):

- **Kartoita ja hallinnoi** (nykytilan tuntemiseksi)
- **Rakenna** (suojauskonseptin kehittämiseksi)
- **Palauta** (normaalitilaan palautumisen mahdollistamiseksi)

Kuvan reunoilla on esitetty tuotannon kyberturvatyön kaikki elementit, jotka muodostavat hallintamalliin omat toiminnalliset kokonaisuutensa:

- **Kartoita ja hallinnoi** kriittiset järjestelmät, rajapinnat, sekä liiketoiminnan riskit ja uhat (osa perustaa)
- **Rakenna** suojaus ja ohjeet/mallit (osa perustaa)
- **Varaudu** varasuunnitelmin ja harjoittele menetyksiä
- **Tunnista loukkaukset ja reagoi** välittömin vastatoimin ja tallenna hyökkäyksen jäljet
- **Raportoi** ja minimoi vahingot
- **Palauta** normaali toiminta (osa perustaa)

Hallintamallin ylin elementti ”Kartoita ja hallinnoi” on jatkuva toimintaa, jossa systemaattisesti kehitetään ja ylläpidetään tuotannon ja sen järjestelmien hyvää hallintotapaa. Tähän liittyy myös tuotannon ja sen järjestelmien riskien ja uhkien analysointia ja hallinnointia, sekä nykytilan selvittämistä säännöllisesti, mm. järjestelmäinventaarioiden ja kyberturvallisuuskartoitusten keinoin.

Seuraavassa hieman tarkempaa kuvausta hallintamalliin sisältyvistä elementeistä.

2.1.1 Joukkueen kokoaminen ja tiedon jakaminen

Tuotannon kyberturvallisuus syntyy käytännössä erityisesti tuotannon ihmisten ja tuotantoa tukevan henkilöstön kyberturvallisuuteen liittyvien:

- tietoisuuden kehittymisestä,
- toimintatapojen määrittelystä ja koulutuksesta,
- tuotteiden ja palvelujen valinnasta, käyttöönotosta ja käytöstä, sekä
- ennakkovarautumisesta, kuten tärkeimpien häiriötilanteiden harjoittelusta.

Tarvitaan muutamia sitoutuneita ihmisiä, jotka ottavat vastuun organisaation kyberturvallisuuden kehittämisestä pitkäjänteisesti, sekä kehittämiseen positiivisesti suhtautuvia tukijoukkoja, joiden osaamisesta turvallinen toiminta pitkälti riippuu. Organisaation tulee siis tunnistaa ja sitouttaa tarvittavat avainhenkilöt turvallisuuden pitkäjänteiseen kehittämiseen.

Ketkä sitten pitäisi pyytää mukaan kyberturvallisuuden kehitystiimiin? Vastaus riippuu kysyjän organisaatiosta. Mikäli yrityksessä on jo hyvin toimiva turvallisuuden kehitysryhmä, saattaa olla järkevää yhdistää kyberturvallisuuden kehittäminen siihen, koska kyberturvallisuus on osa kokonaisturvallisuutta. Turvallisuuden vastuuhenkilöt voivat sitten samalla kertaa raportoida ja esittää yrityksen johtoryhmälle myös kyberturvallisuuteen liittyvän tilanteen ja tehtävät. Tämä voi muutenkin parantaa turvallisuusasioiden kommunikointia yrityksen sisällä merkittävästi. Kehitysryhmään kannattanee kutsua mm. seuraavan kaltaisiin rooleihin valtuutettuja henkilöitä:

- tuotannon (automaation) kunnossapidosta ja kehittämisestä vastaavat
- yritys- ja laitostason ICT-järjestelmien ylläpidosta ja kehittämisestä vastaavat
- automaation hankinnoista vastaavat
- tuotannon järjestelmien pääkäyttäjät
- turvallisuudesta ja sen kehittämisestä vastaavat
- kehityshankkeista vastaavat, jne.

Tiedon jakaminen on keskeistä osaamisen ja tietoisuuden jatkuvassa kehittämisessä. Tämän takia kannattanee perustaa jopa sisäinen (turvallinen) sähköinen foorumi, jossa jaetaan aineistoja jotka liittyvät tuotannon kyberturvallisuuden:

- kehityssuunnitelmiin,
- koulutusmateriaaleihin ja tietoiskuihin,
- ohjeisiin, jotta niitä voidaan katselmoida rauhassa ennen käyttöönottoa
- riskeihin joita ollaan kohdattu tai jotka ovat todennäköisiä
- tapahtumiin jotka voisivat vaarantaa omankin tuotannon, jne.

2.1.2 Ymmärrä syyt ja opi turvallisen toiminnan edellytykset

Kyberturvallisuuteen liittyvien heikkouksien ymmärtäminen synnyttää yleensä motivaation nykyisen tilanteen parantamiselle. Tuotannossa on monesti käytössä järjestelmiä, joiden päivityssykli on useita vuosia. Tällöin on tutkimattakin ilmeistä,

että nämä järjestelmät sisältävät myös kyberturvallisuushaavoittuvuuksia. Jos hyökkääjä pääsee jollain keinolla (esim. yksittäistä työntekijää huijaamalla) samaan sisäverkkoon haavoittuvuuksia sisältävien järjestelmien kanssa, on hyökkääjällä helppo työ murtautua kyseisiin järjestelmiin. Mikäli tällaista murtautumista ei havaita nopeasti, voi tilanteesta toipuminen myöhemmin olla varsin vaikeaa ja kallista. Järjestelmiin tunkeutuminenhan on tällöin saattanut levitä laajalle aiheuttaen kalliita tarkastus-, korjaus- ja palautustoimenpiteitä.

Varsinkin jos etähyökkäys kriittisiä järjestelmiä vastaan onnistuisi Internetistä ladattavissa olevia ohjelmistoja ja ohjeita käyttämällä, on syytä alkaa hyvin pikaisesti parantamaan nykytilannetta.

Energiayrityksen turvallinen toiminta kybervakoilua ja -hyökkäyksiä sisältävässä maailmassa edellyttää, mm.:

- koko henkilöstön riittävää kyberturvallisuustietoisuutta,
- jatkuvuutta ja turvallisuutta tukevia toimintaohjeita ja lupamenettelyjä,
- tuotannon suojauskonseptia ja sen jatkuvaa toimeenpanoa,
- vakoilun ja tietomurtojen tunnistamisen kyvykkyyttä,
- toteutuneiden häiriöiden, tehtyjen virheiden ja epäiltyjen hyökkäysten raportoinnin seurantaa
- häiriöistä palautumisen suunnitelmia ja harjoituksia,
- kyvystä löytää uusia varautumistapoja kyberuhkien muuttuessa yhä vaikeammin havaittaviksi.

2.1.3 Kartoita ja hallinnoi kriittiset järjestelmät, rajapinnat, riskit ja uhat

Tuotannolle kriittisten järjestelmien kartoittaminen, ajantasainen dokumentointi ja hyvä elinkaaren hallinta ovat perustavanlaatuisia elementtejä kyberturvallisuuden ylläpitämisessä ja kehittämisessä. Ilman tällaisia elementtejä jatkuvuuden ja turvallisuuden ylläpitäminen ja kehittäminen ovat käytännössä mahdottomia tehtäviä.

Miksi systemaattinen kartoittaminen ja tuotantoomaisuuden hallinnointi sitten usein jäävät puutteellisiksi, vaikka asian tärkeys olisikin itsestäänselvyys? Syitä on varmasti monia, mutta erityisesti toiminnallisuuden ja osaamisen sirpaloituminen useille toisistaan riippumattomille toimijoille on yleistä. Toisaalta ulkoistamisten ja voimalahankintojen mukanaan tuomat ylläpitäjien vaihtumiset tai muut lisääntyneet ylläpitovelvollisuudet (entisten töiden lisäksi) ovat voineet aiheuttaa kohtuuttomia vastuita yrityksen tietyille avainhenkilöille. Omalle kontolle siirtyneiden järjestelmien ylläpidossa on voitu käyttää esim. aivan erilaisia järjestelmiä ja hallintotapoja kuin mihin on totuttu, eikä yhtenäistä omaisuudenhallintatyökalua tai hallintotapaa ole edes näköpiirissä. Kokonaisvaltaisen hallinnointimenettelyn luominen voi tuntua mahdottomalta, varsinkin jos sen tarvetta ei ole edes liiketoimintajohdossa tunnistettu.

Omaisuuden hallinnan käytännöistä kerrotaan enemmän seuraavassa luvussa, mutta jokaisen on tarpeen ymmärtää tämän osa-alueen valtava laajuus ja vaativuustaso, varsinkin kun siihen sisältyy myös kehittyvien kyberuhkien jatkuvasti uudelleen muotoutuvat vaikutukset liiketoiminnan riskeihin. Korostettakoon kuitenkin jo tässä vaiheessa, että erityisesti tuetun elinkaarensa päässä jo olevat, mutta silti vielä tuotannossa olevat järjestelmät, kannattaa nostaa investointisuunnitelmissa prioriteettilistan kärkeen.

2.1.4 Rakenna suojaus ja ohjeet/mallit

Tuotannon suojaamisessa kyberturvallisuusuhkia vastaan korostuu seuraava kysymys: Mitkä ovat tärkeimmät suojausmenettelyt, joiden avulla saavutetaan paras tuotannon jatkuvuuden kokonaisuus?

Jotta suojauskonseptiin kuuluvat menettelyt ja tekniikat voidaan valita, täytyy ensin selvittää meihin kohdistuvat tärkeimmät uhat. Tämä on usein vaikea tehtävä, varsinkin jos yhtään kyberhyökkäystä ei olla aiemmin havaittu. Syyhän voi olla myös puutteellinen havainnointikyvykkyys.

Jos toteutuneita uhkia ei ole vielä tunnistettu, niin tuotannon suojauskonseptin määrittelyä voidaan lähestyä myös pohtimalla, mitkä ovat tärkeimmät juuri meidän tuotantoympäristömme suojausta parantavat ja täten kyberturvallisuutta lisäävät toimintatavat. Tuotannon kyberturvan kehittämisen käynnistämisen kokonaiskuvassa korostuvat seuraavat suojauskäytännöt:

- Automaatio-omaisuuden hallinta
- Hankintojen kyberturvavaatimukset
- Operatiivisten kumppanien & ratkaisujen arviointi ja valinta
- Tietoliikenteen turvallinen arkkitehtuuri
- Turvalliset etäyhteydet

- Pääsyoikeuksien hallinta
- Jatkuvuuden varmistaminen, palautus
- Häiriötilanteiden hallinta ja harjoittelu

Ylläoleviin suojauskäytäntöihin liittyviä ohjeita yhdessä laatimalla ja pilottityyppisiä kokeiluja suunnittelemalla ja toteuttamalla potentiaalisten kumppanien kanssa ollaan todennäköisesti jo oikealla polulla. Tuotannon kyberturvaamisen suojauskonseptin määrittely on iteratiivinen prosessi, jossa soveltuvin konseptikokonaisuus elää ja kehittyy yrityksen välittömien tarpeiden ja vaatimusten, henkilöstön ja kumppaneiden osaamistason, sekä tietysti ympäristön uhkatilanteen mukaan.

Suurta osaa ylläolevista suojauskäytännöistä olemmekin jo käsitelleet aiemmissa teollisuuden kyberturvallisuuden kehityshankkeissa (kuten KYBER-TEO), mutta muutamia näistä käytännöistä on edelleen kehitetty KYBER-ENE hankekokonaisuudessa. Mainittakoon, että erityisesti automaatioomaisuuden hallinta, kumppanien arviointi, sekä häiriötilanteiden hallinta ja harjoittelu kuuluvat näihin energia-alan tärkeisiin kehityskohteisiin.

2.1.5 Varaudu varasuunnitelmin ja harjoittele menetyksiä.

Kriittisen infrastruktuurin jatkuvan toiminnan varmistamiseksi on ollut tärkeää, että tuotannossa käytettävät kriittiset järjestelmät tilataan ja asennetaan kahdennettuina. Tärkeimmät varaosat tulisi löytyä omasta tai kumppanin varastosta, tai ainakin hyvin nopealla toimitusajalla. Mikäli näin ei toimita, niin pienetkin viat voivat aiheuttaa yhteisvaikutuksiltaan merkittäviä taloudellisia tappioita tai häiriötä yhteiskunnan toimintaan.

Mitkä kumppanuudet ja järjestelmät ovat kriittisiä energia-alan yrityksen jatkuvan toiminnan kannalta? Vastaukset tähän kysymykseen näyttävät muuttuvan koko ajan monimutkaisemmiksi ja epävarmemmiksi, sillä esimerkiksi palveluverkostot ovat yleisesti siirtyneet käyttämään ulkomaisissa tietoverkoissa toimivia pilvipalveluja. Näiden luotettavuuden varassa toimivat myös monet kotimaassa tuotetut palvelut. Voi siis olla, että kriittistä varaosaa tai varmuuskopiota ei löydy, mikäli alihankkijan käyttämässä pilvipalvelussa on yllättävä toimintahäiriö.

Varasuunnitelma tulisi laatia tilanteisiin, joissa jokin tärkeä kumppani tai tukijärjestelmä muuttuu toimintakyvyttömäksi. On hyvin ajatuksia herättävää miettiä, että miten toimittaisiin silloin, kun järjestelmätoimittajan etäyhteys sisältääkin tietoturvauhan, tai kun tuotannon automaatiojärjestelmät ylläpitävä palvelukumppani ei olekaan häiriön yllättäessä tavoitettavissa. Kenelle silloin soitetaan ja mitä ehdotetaan jatkotoimenpiteiksi, jotta tuotanto saadaan ylläpidettyä myös jatkossa normaalisti?

Häiriöharjoitusten järjestäminen kyberturvallisuushyökkäyksiä vastaan on muodostumassa tärkeäksi osaksi energia-alan ennakkovarautumista, sillä harjoittelu on osoittautunut hyväksi ja nopeaksi tavaksi havaita toiminnan puutteet ja oleelliset kehityskohteet. Energia-alan avaintoimijoita on jo osallistunut valtakunnalliseen TIETO18-harjoitukseen, joka oli Suomen suurin yritysten ja viranomaisten yhteistoimintaharjoitus laajojen kyberturvahäiriöiden varalta. TIETO18:ssa harjoiteltiin yhteiskunnan keskeisiä palveluita tuottavien yritysten selviämistä kyberhäiriöistä, sekä viranomaisten tukitoimia yritysten toimintakyvyn palauttamiseksi.

Valtakunnalliset harjoitukset eivät kuitenkaan yksin riitä, vaan myös energia-alan PK -yritykset on saatava laajassa mittakaavassa pohtimaan ja harjoittelemaan omaa varautumistaan vakavimpiin häiriöitilanteisiin tai esim. järjestelmämenetyksiin, joita ne saattavat tulevaisuudessa kohdata. Tämä vaatii myös Kyberturvallisuuskeskuksen asiantuntemuksen ja kokemuksen hyödyntämistä esimerkiksi vaikutuksiltaan yleisesti merkityksellisten skenaarioiden määrittelijänä ja muutenkin kyberharjoitusten tukena. Tällä tavoin voitaisiin saavuttaa riittävä vaikuttavuus ja varautumisen parantuminen energia-alan yritysten laajaan kenttään.

2.1.6 Tunnista loukkaukset ja reagoi vastatoimin

Kyberturvallisuusloukkausten tunnistaminen on laaja alue, joka sisältää monia vaihtoehtoisia, mutta samalla toisiaan täydentäviä menetelmiä ja teknologioita. Itse häiriöiden hallinnollinen käsittelyprosessi kannattanee yhdistää tuotannon järjestelmien muuhun häiriöhallintaan, jotta ei luotaisi päällekkäisiä prosesseja, jotka kuitenkin pyrkivät samaan päämäärään eli tuotannon jatkuvuuteen. Lisäksi kannattaa muistaa, että myös ”Raportoi ja minimoi vahingot”-elementti tulee sisällyttää häiriöhallinnan prosessin kuvaukseen.

Kyberturvallisuusloukkausten tunnistamisen järjestelmät jaetaan kahteen päätyyppiin, joista molemmat ovat yleisesti ottaen hyödyllisiä myös energia-alan yritysten jatkuvuuden varmistamisessa:

- Verkkoliikennettä analysoivat järjestelmät (*Network Intrusion Detection System, NIDS*)
- Päätelaitteen tapahtumia analysoivat järjestelmät (*Host-based Intrusion Detection System, HIDS*)

Erityisesti energiayritysten yritysverkkoihin sekä toimistoverkkojen laitteisiin kohdistuvat vakoilu- ja soluttautumisyritykset kuuluvat yllämainittujen, yleiskäyttöisten IDS-järjestelmien vahvuusalueisiin, sen sijaan automaatioverkoissa niiden käyttäminen saattaa olla hyödytöntä tai jopa vahingollista. Hyödytöntä se on silloin, jos asennettu IDS ei ymmärrä automaatiojärjestelmän oikeaa ja väärää toimintaa (tietoliikenneprotokollia, viestinnän merkitystä / metadataa) ja jopa vahingollista silloin, jos automaation toiminta häiriintyy IDS järjestelmän suorituksen tai päivittymisen takia (esim. liikaa kuormaa automaatiolaitteessa tai -verkossa). Erityisesti IPS:n (Intrusion Prevention System) käyttö saattaa vahingoittaa tuotantoa rajoittamalla automaattisesti kriittistä tietoliikennettä.

Energia-alalla kyberloukkauksia kannattaa tunnistaa laaja-alaisesti, ei pelkästään tukeutuen kaupalliseen tai ilmaiseen IDS-tuotteeseen, koska nekään eivät pysty tunnistamaan kaikkia hyökkäyksiä, eivät edes yhdistettyinä kehittyneisiin SIEM (*Security Information and Event Management*) järjestelmiin ja SOC (*Security Operations Center*) palveluihin. Potentiaalisia esimerkkejä kyberloukkausyritysten tunnistamisen käytännön keinoista ovat:

- Epäilyttävien yhteydenottojen havainnointi (lokikirjaus ja myöhempi analysointi)
  - sähköpostit,
  - some-kanavien yhteydenotot,
  - puhelut,
  - satunnaiset keskustelunavaukset esim. lentoasemilla, yleisissä kulkuvälineissä, jne.
- Epäilyttävien yritysvieraiden havainnointi (lokikirjaus ja myöhempi analysointi)
  - myyntiedustajat,
  - alihankkijan sijaiset,
  - ulkomaiset lähetystöt,
  - oppilaitosvieraat, jne.

Useimmat yritysverkot ovat monin tavoin kytkettyjä julkisiin verkkoihin ja pilvipalveluihin, jotka tarjoavat runsaasti hyökkäyspolkuja hyökkääjille. Yleisin tapa suojata automaatioverkkoa ja siihen kytkettyjä automaatiojärjestelmiä on tunnistaa kybervakoilu ja hyökkääjän jalansijan rakentaminen jo toimistoverkoissa tai niiden rajalla, sillä monet hyökkääjät pyrkivät ujuttautumaan sisään julkisten verkkojen ja niissä toimivien palvelujen kautta.

Kun vakoilu- tai hyökkäysepäily sitten tunnistetaan, on tärkeää, että sen jättämät jäljet pystytään tallentamaan ja säilyttämään koskemattomina tarkempaa tutkintaa varten. Jos hyökkääjä on päässyt tuotantoverkon järjestelmiin, tarvitaan useimmiten pikaista apua järjestelmätoimittajalta ja lähiverkko-operaattorilta hyökkäysten jälkien tallentamiseksi ja vahinkojen minimoimiseksi, erityisesti saastuneen laitteen sisältäneen verkkosegmentin irrottamiseksi muusta sisäverkosta. Jos tähän ei olla varauduttu etukäteen, saatetaan olla auttamattomasti liian myöhässä. Luvussa 5 kerrotaan enemmän mm. häiriöhallinnasta, hyökkäykseen reagoimisesta ja vastatoimista.

2.1.7 Raportoi ja minimoi vahingot

Raportointi kuulostaa joidenkin mielestä byrokraattiselta ja jopa turhalta toiminnalta. Mutta jos asiaa ajattelee jatkuvuuden varmistamisen kannalta, niin tapahtumien dokumentointi muuttuu välttämättömäksi toiminnaksi, jonka kautta opitaan aiemmin jo sattuneista vioista ja häiriöistä, sekä kyetään täten varautumaan tuleviin häiriöihin paremmin. Kyberturvallisuudessa pätee sama ilmiö, eli aiemmin jo tapahtuneiden hyökkäysten tai vakoiluyritysten kaltaista toimintaa ilmenee yleensä myöhemminkin. Mm. Ukrainan sähköverkkoyhtiöihin kohdistuneiden hyökkäysten analysointi on todentanut tämän ilmiön. Tällöin jo kehitettyä haittakoodia uusiokäytettiin myös tulevissa hyökkäyskampanjoissa, sekä hyökkäyksen valmistelu, että toteutus varioivat jo aiemmin ”testattuja” toimivia hyökkäystapoja.

Puolustajankin on siis perehdyttävä aiemmin toteutettuihin hyökkäyksiin, mm. lukemalla muiden analysoimista ja raportoimista kyberhyökkäyksistä, joissa usein myös kuvataan yksityiskohtaisesti ne työkalut, joita hyökkääjä on käyttänyt ja millaisia jälkiä hyökkäyksestä on jäänyt. Sama koskee oman yrityksen oppimista - yrityksen järjestelmiin ja sen henkilöstöön kohdistuneet hyökkäykset ja niiden yritykset tulisi dokumentoida ja raportoida hallitusti eteenpäin, jotta niistä voidaan oppia.

Vahinkojen minimoimiseksi on välttämätöntä, että hyökkäysyritykset pystytään tunnistamaan jo alkuvaiheessa, jolloin hyökkääjä ei ole vielä ehtinyt soluttautua laajemmin yrityksen järjestelmiin. Tapahtuneesta aiheutunut vahinko voidaan toivottavasti rajata esim. yhteen verkkosegmenttiin tai järjestelmäkokonaisuuteen, jonka puhdistaminen ja palauttaminen turvalliseen normaalitilaan ei kestä kauan eikä maksa kohtuuttomasti.

2.1.8 Palauta normaali toiminta

Kyberhyökkäyksen paljastuttua tuotannon palauttaminen normaalitilaan edellyttää, että meillä on tarkat tiedot saastuneista järjestelmistä, sekä tarkka ajankohta, jolloin järjestelmä tai siihen liittyvät tiedot saastuivat (tai potentiaalisesti saastuivat) laittoman tunkeutumisen johdosta. Meillä täytyy siis olla tiedossa ja tallennettuna puhdas normaalitila:

- tuotantolaitteet ja ohjelmistot versiotietoineen,
- vikakorjaukset (asennetut patchit),
- tuotannon parametrisointi ja tuotantotiedot, jos kyseessä on esim. info-järjestelmä,
- varmuuskopiot ja palautusjärjestelmät käyttöohjeineen.

Oleellista on myös, että järjestelmiä ei ajeta alas ja aleta palauttamaan johonkin aiempaan tilaan ilman selkeitä todisteita kyberhyökkäyksen todellisesta tilasta, sillä toisinaan hyökkääjät yrittävät pelkästään huijausviestein ja harmittomia haittaohjelmia levittämällä saada yrityksen toimihenkilöt uskomaan, että he ovat vaarallisen hyökkäyksen kohteena. Myös vääriä hälytyksiä on siis kyettävä luotettavasti tunnistamaan ja toimimaan aina vähiten haittaa aiheuttavalla tavalla.

2.2 Yrityskohtainen Start Up –työpaja

Yrityksissä kaikkein tärkeintä ja usein vaikeinta on saada kyberturvallisuuden kehitystyö kunnolla käyntiin. Kuten luvun alussa jo esitimme, tuotannon tietoturva-asioiden ulkoistaminen tai delegoiminen yhden henkilön hoidettavaksi ei toimi. Työn alkuvaiheessa täytyy varmistaa, että yritys- ja liiketoimintajohto ymmärtävät kyberturvallisuuden tärkeyden jatkuvuuden varmistamisessa, ja että kehittämistä varten määritellään riittävä resursointi, yhteistyö ja tehtäväjako. Parhaiten tämä saatiin aikaan KYBER-ENE hankekokonaisuudessa kehitetyssä ja testatussa, yrityskohtaisessa Start up -työpajassa. Start up -työpaja kannattaa järjestää, mikäli yrityksen läpileikkaavassa kyberturvallisuustietoisuudessa on parantamisen varaa.

Seuraavassa kuvassa esitetään projektissa kehitetty kaavio ”Tuotannon kyberturvan kehittämisen käynnistäminen - kokonaiskuva”, joka on tarkoitettu helpottamaan energiayrityksen tuotannon kyberturvan kehittämisen aloittamista.

Kuva 4. Tuotannon kyberturvan kehittämisen käynnistäminen - kokonaiskuva.

Tuotannon kyberturvan kehittäminen käynnistyy neljän pääelementin kautta:

- **Vaihe 1: Motivointi - Ymmärrys - Johto sitoutuu**
  - Yrityskohtainen Start Up -työpaja tärkeimpänä työkaluna
- **Vaihe 2: Nykytilan kartoitus**
  - Tuotannon kyberturvan yleiskartoitus nykytilan selvittämiseksi
- **Vaihe 3: Suunnittelu ja kehitys**
  - Erityisesti toimivan kehitysryhmän perustaminen
- **Vaihe 4: Toteutus ja käytännön toimet**
  - Kyberturvallisuuden hallinnan osa-alueiden määrittely (n. 7 kpl)

Yksi projektin tärkeimmistä tavoitteista oli kyberturvallisuustyön kehittämisen vauhdittaminen energiayrityksissä. Projektissa toteutettiin sarja työpajoja alueellisissa energialaitoksissa. Näissä energiayrityskohtaisissa Start Up –työpajoissa kehitettiin erityisesti alueellisten energialaitosten kyberturvallisuustietoisuutta.

- Vahvistettiin edelläkävijä- ja vertaistukea energiayrityksille ja jaettiin kokemustietoa molempiin suuntiin.
- Yhdessä yli yritysrajojen pohdittiin ja määriteltiin, sovellettiin ja koestettiin toimivia kyberturvallisuuden malleja ja käytäntöjä energiayritysten tarpeisiin.

Alueellisissa energialaitoksissa pidettävien Start up -työpajojen aiheita voivat olla esimerkiksi:

- Automaation kyberturvallisuuden kehitysryhmän perustaminen, tehtävät, vastuuttaminen ja työnjako
- Mitä pitäisi tehdä etukäteen, jotta hyökkääjät eivät onnistuisi? Osaaminen: miten yrityksessä saadaan aikaan tuotantoautomaation tietoturvahallinta ja tietoturvan jatkuva parantaminen?
- Miten selvittää tuotantoverkon kyberturvallisuustilanne? Mm. tuotantolaitokset, sähköverkko, kaukokäyttöverkko, etäyhteydet.
- Käyttö- ja päivystystoimen turvalliset etäyhteydet: Oma henkilöstö & kumppaneiden verkosto.
- Ylläpitosopimusten kyberturvallisuusvaatimukset & automaatiojärjestelmien päivitykset ja vikakorjaukset.

- Yhteiskäyttötunnusten käyttö ja käyttäjätunnusten ja salasanojen riittävä laatu.
- Tuotantoverkon segmentointi ja miksi se on niin tärkeää.
- Automaation varmuuskopioinnin merkitys ja palautumistestaus.

2.2.1 Start Up -työpajan kulun suunnittelu

Yrityskohtaiset Start up -työpajat suunniteltiin jokainen erikseen seuraavan kaavan mukaan:

1. Osa: Kehityskohteet (kesto: n. 2-4 h, viikko ennen työpajaa)
   - Yritys määrittää tuotantonsa tärkeimmät kehityskohteet
   - Tarvittaessa ½ päivän tarvekartoituskäynti

2. Osa: Yrityskohtainen Start Up-työpaja (kesto: n. 1 työpäivä)
   - Suunnittelu
   - Vertais-/edelläkävijätuen varmistaminen
   - Työpajan toteutus

3. Osa: Palaute (kesto: palaute 1 h; jatkotoimien suunnittelu: n. 2-4 h)
   - Palautekysely (mahdollisimman pian työpajan jälkeen)
   - Yrityksen omat jatkotoimet (muutaman viikon sisällä työpajasta)
   - (KYBER-ENE projektin suuntaaminen palautteen perusteella)

Osa 1: **Kehityskohteet:** Tärkeimmät kehityskohteet arvioidaan ja kirjataan ylös joko yrityksen sisäisessä työpajassa, tai sitten projektin puolesta toteutettiin puolen päivän lyhyt tarvekartoitus. Molemmissa tapauksissa alustavien kehityskohteiden määrittelyyn yrityksestä osallistuivat tyypillisesti mm.:

- tietoturvapäällikkö (kartoituksen koordinointi),
- liiketoimintajohto,
- turvallisuus- ja riskienhallintapäällikkö,
- kehitysvastaavat,
- kunnossapitovastaavat,
- hankintavastaavat,
- jne.

Kehityskohteiden määrittelyn tavoitteena on siis saada tunnistettua yrityksen tuotannon kyberturvallisuuden ja sen kehittämisen pahimmat ongelmakohdat ja pullonkaulat, jotka vaativat ehdottomasti parempaa hallintaa.

Osa 2: **Yrityskohtainen Start Up-työpaja:** Edellisen vaiheen tuloksena syntyneiden kehityskohteiden perusteella vaiheessa 2 suunnitellaan ja toteutetaan Start up -työpaja. Tärkeää on määritellä yhdessä työpajalle mm. sen tavoite, agenda, osallistujat, aika ja paikka. Seuraavassa kuvassa on esimerkki yrityskohtaisesta Start up -työpajan agendasta, jossa ennakkoon tunnistettuina kehityskohteina olivat mm. automaatioverkkojen turvallisuuden parantaminen, tuotannon tietoturvahallinta ja jatkuva parantaminen, sekä tietoturvan varmistaminen automaatiohankinnoissa vaatimuksin ja sopimuksin.

Yleensä yhden päivän Start Up-työpajassa voi olla maksimissaan kaksi kehityskohdetta (ryhmätyötä), jotta käsittely ei jäisi liian pinnalliseksi pysyvien tulosten saavuttamisen kannalta. Työpajan osallistujat valitaan tietenkin kehityskohteiden mukaisesti, mutta usein osallistujalista on pääsääntöisesti laajempi mutta saman kaltainen kuin kehityskohteiden määrittelyssäkin (Osa 1). Iltapäivällä pidettävien ryhmätöiden tavoitteena on pohtia yhdessä, miten yrityksen tunnistamia tärkeimpiä kehityskohteita lähdetään parantamaan, esim.:

- ketkä pitää ottaa (kuhunkin) kehitysryhmään mukaan?
- kuka ottaa vastuun kehityskohteeseen liittyvän työn vetämisestä?
- mitä pitäisi olla valmiina esim. vuoden kuluttua, mitkä välivaiheet ovat?
- mitä muita resursseja, hankintoja tai koulutusta onnistuminen vaatii?
- mitkä muut seikat tulee ottaa huomioon, jotta kehittäminen onnistuu?
- millaista muuta tukea kehittäminen vaatii?
- miten kehitystyön edistymistä seurataan?

AGENDA:
8.45 Osallistujien esittäytymiskierros
8.55 INTRO: Työpajan tavoite ja ohjelma
9.05 KEHITYSKOHTEET: Energiayrityksen kyberturvallisuuden kehityskohteet pääpiirteittäin (Energiayritys alustaa)
9.15 VERTAISTUKI: Tietoturvallisuuskulttuurin luominen ja automaation tietoturvallisuuden kehittäminen (Edelläkävijä alustaa + keskustelu)
10.30 TOIMITTAJATUKI: Automaatiotoimittajan tarjonta energiayrityksen automaatioverkkojen turvallisuuden parantamiseen (Automaatiotoimittaja + keskustelu)
(11.30 – 12.30): Lounastauko
12.30 RYHMÄTYÖ: Miten saadaan aikaan tuotantoautomaation tietoturvahallinta ja tietoturvan jatkuva parantaminen? Hallintamalli-alustus & kehitysryhmän muodostamisen pohdintaa.
(*kahvitauko 14.15-14.30*)
14.30 RYHMÄTYÖ: Tietoturvan varmistaminen automaatiohankinnoissa vaatimuksin ja sopimuksin. Alustus: esim. mallisopimusliitteet tai vaatimukset.
15.30 JATKO: Jatkotoimenpiteet, aikataulu ja työnjako (Energiayrityksen omia päätöksiä)
15.45 PALAUTE: Palautelomakkeiden täyttö, palautus & suullinen palautekierros (kaikki)

Kuva 5. Esimerkki yrityskohtaisesta Start up -työpajan agendasta.

Osa 3: **Palaute:** Tärkeä elementti Start up -työpajojen kehittämisessä oli palautteen kerääminen osallistujilta heti tilaisuuden jälkeen. Tähän käytettiin standardimuotoista lomaketta ”Kysely – Palaute ja kiinnostuksen kohteet”, seuraava kuva:

1. Yleispalaute tästä tilaisuudesta (rasita sopivin vaihtoehto):
(1) Erittäin hyödyllinen tilaisuus
(2) Melko hyödyllinen tilaisuus
(3) Melko hyödytön tilaisuus
(4) Täysin hyödytön tilaisuus
Perustelut:

2. Olisitko halunnut vaihtaa työpajan käsittelemiä aiheita?
Mitä aiheita puuttui?

3. Miten kehittäisit työpajan rakennetta ja pidettyjä alustuksia? Esim. mihin pitäisi käyttää enemmän tai vähemmän aikaa?

4. KYBER-ENE jatkot: Mitkä osa-alueet organisaatiossasi vaatisivat kyberturvan kehittämistä tulevien vuosien aikana? Millaista tukea tarvitset jatkossa? Kuka voisi auttaa sinua parhaiten?

5. Mitä muuta meidän pitäisi parantaa näiden tilaisuuksien kehittämiseksi? Sana on vapaa:

Kuva 6. Start up -työpajan palautelomakkeen kysymykset.

Tulokset käsiteltiin projektissa luottamuksellisesti ja hyödynnettiin anonyymisti teollisuuden kyberturvallisuuden jatkokehittämiseksi.

Start up -työpajoissa saatu palaute oli yleisesti varsin kiittävää ja rakentavaa. Lisäksi palautteet käsiteltiin KYBER-ENE hankkeen ohjausryhmässä, jonka seurauksena seuraavien työpajojen suunnitelmaa ja toteutusta muokattiin vähitellen saatujen palautteiden perusteella vielä toimivampaan ja yrityksiä paremmin palvelevaan suuntaan. Esimerkiksi ryhmätöihin käytettävää aikaa haluttiin lisätä alkuperäisestä ja keskittyä niissä vain muutaman aiheen käsittelyyn, mutta sitäkin suuremmalla intensiteetillä.

Johtopäätelmänä voidaan sanoa, että jokainen Start up -työpaja tulee räätälöidä energiayrityksen tarpeista, kehityskohteista ja kyvykkyyksistä lähtien. Todellisten energia-alan yritysten antamien esimerkkien merkitys on erittäin suuri, joten on eduksi, mikäli edelläkävijänä tai vertaistuen antajana toimii jo ennalta tuttu tai ainakin suositeltu henkilö, jotta luottamus olisi mahdollisimman hyvällä tasolla heti työpajan alusta lähtien. Uskomme, että näin toimien syntyy todellista vaikuttavuutta energiayrityksen henkilöstön asenteisiin ja toimintamalleihin, kun opastajakin on jo kokenut itse monta karikkoa ja osaa antaa käytännön vinkkejä niistä selviämiseen.

2.2.2 Case: Start Up -työpajan herättämiä kehitysajatuksia

Tässä alakohdassa esitämme lyhyesti otteen kehitysajatuksista, jotka erään Start Up -työpajan kohdeyrityksen tietoturvavastaava meille lähetti (muutamaa viikkoa oman työpajansa jälkeen). Heidän tavoitteenaan oli kyberturvallisuuden vahva käytännön edistäminen omassa yrityksessään.

Kyberturvallisuuden käytännöllisen edistämisen avaintekijät PK -yrityksessä:

1. Liiketoimintajohdon sitouttaminen kyberturvallisuustyöhön (kaikki liiketoiminnot)
2. Ymmärretään, että yrityksen kyberturvallisuutta tulee edistää ”me-hengessä”
   - Kehittämisen vetovastuullinen nimetään (tietoturvapäällikkö)
   - Kyberturvallisuus ei ratkea yksin tietoturvapäällikön toimesta, vaan kaikki avaintoimijat on saatava mukaan

3. Ymmärryksen parantaminen kyberturvallisuuden perusteista sekä yritystä koskettavista mahdollisista uhkista
    - Työpaja toimi hyvänä lähtölaukauksena, jonka jälkeen parantunut ymmärrys mahdollistaa keskustelun syntymisen, yhdessä tekemisen ja asioiden kunnollisen edistämisen
    - Vaatii jatkuvia panostuksia tietämystason nostamiseen
4. Yrityksen sisäisen kyberturvallisuuden toimintamallin luominen
    - Priorisoidaan löydetyt kehityskohteet ja niiden hallittu toteutus
    - Edistymisen seuranta ja ylätason ohjaaminen johtoryhmässä
    - Ymmärretään resursoinnin merkitys ja panostetaan tarpeisiin
5. Muiden energiayhtiöiden antama vertaistuki
    - Lähes kaikilla energiayhtiöillä on samansuuntaiset kyberturvallisuushaasteet → yhteistyöllä olisi hyvä vaikuttavuus
    - Luottamuksellinen ja säännöllinen tiedon jakaminen tuo luottamusta omaan tekemiseen ja asioiden edistämiseen, kuten E-ISAC ryhmässä (=Energia-alan toimialakohtainen tietoturva-asioiden tiedonvaihtoryhmä, ks. kohta 5.1)
    - Perustetaan alueellisia & itseohjautuvia tiedonvaihtoryhmiä!
6. Edistyksellisistä yrityksistä tuleva mentoreiden tuki
    - Edelläkävijäyritysten kokemuksia jakamalla ja hyödyntämällä saavutetaan merkittävää tukea alueelliselle ja yrityskohtaiselle kehitystyölle
    - Mentori osaa jakaa tietoa oikeassa muodossa ja auttaa käytännön kyberturvallisuustyössä. Samanlaista tukea ei saa kaupallisilta toimijoilta
7. Energiasektorin yhteisten kumppanien käyttäminen kehityshankkeissa ja suojauksen ylläpidossa
    - Parhaan kumppanin löytäminen vertaisverkoston ja mentoreiden avulla. Yhteistyö kumppaneiden hyödyntämisessä.

2.3 Tuotannon yleiskartoitus

Tuotannon kyberturvallisuuden yleiskartoituksen kuvaus vuodelta 2013 löytyy Huoltovarmuuskeskuksen julkaisusta ”Tietoturvaa huoltovarmuuskriittisille yrityksille” -kirjanen [TEO-SUMMARY]. Tuossa kirjasessa yleiskartoitus oli kuvattu sivulta 20 alkaen otsikolla ”Tietoturvan yleiskartoitus tuotannon automaatiossa”. Vuosina 2017-2018 toteuttamiemme voimalaitosten ja muiden tuotantolaitosten yleiskartoitusten perusteella voidaan todeta, että vuoden 2013 yleiskartoituksen kuvaus pätee edelleen varsin hyvin. Yleiskartoituksia on tosin tehty käytännössä joko vielä kevyemmällä menettelyllä, tai toisaalta laajentaen niitä erityisesti kohdennetuilla haavoittuvuusskannauksilla. Mahdolliset haavoittuvuusskannukset tulee kuitenkin toteuttaa ainoastaan, mikäli skannauksen arvioidut hyödyt ylittävät sen riskit. Teknisin työkaluin toteutettava analyysi (kuten verkkoskannaus) tulee aina tehdä erityistä varovaisuutta noudattaen käyttäen asiakkaan kanssa yhdessä sovittuja menettelyjä ja aikatauluja, jolloin riskit tuotannon jatkuvuudelle voidaan minimoida luotettavasti.

Voimalaitoksen yleiskartoituksen päävaiheet ja niissä huomioitavat asiat ovat:

Vaihe	Huomioita
Osallistujien alkuesittelyt	Paikalla työpajaosuudessa mm. laitoksen johto, tuotantopäällikkö, kunnossapitopäällikkö, turvallisuuspäällikkö, tietoturvavastaava, jne.
Työpaja voimalaitoksen nykyisestä dataverkkoarkkitehtuurista, toimintaohjeista ja turvallisuusvaatimuksista	Usein verkkoarkkitehtuurikuvaus kannattaa selittää sanallisesti ja tuoda esiin historialliset seikat sekä tulossa olevat muutokset. Joskus keskustelussa selviää, että arkkitehtuurikuvassa on päivitystarpeita, tai että kuva ei vastaa kaikilta osin todellisuutta. Usein nykyiset toimintaohjeet ja vaatimukset eivät vielä huomioi kyberturvallisuutta riittävästi tai työntekijöiden ymmärtämällä tasolla.
Voimalaitoksen kiertokäynti	Kiertokäynnin toteutuksessa on tärkeää, että kierrosta on opastamassa paikalliset järjestelmät hyvin tunteva henkilö, joka osaa kertoa mitkä laitteet ovat käytössä, mitkä niiden ongelmat ovat, mitä muutoksia on jo suunniteltu, jne. Kiertokäynti auttaa kartoittajia ymmärtämään kartoitettavan laitoksen kokonaisuuden, tarkoituksen, kriittisten järjestelmien suojauksen. Lisäksi nähdään miten todellisuus vastaa ”teoriaa / ohjeita”.

Vaihe	Huomioita
Avainhenkilöiden haastattelut	Haastatteluissa tärkeintä on saada sellaisten avainhenkilöiden luottamus, jotka tuntevat nykytuotannon todellisuuden, siinä olevat heikkoudet ja parannusta vaativat seikat. Nämä kirjataan tasoarvion lisäksi haastattelutaulukkoon. Ilman rehellistä ja avointa keskustelua yleiskartoituksen tulokset jäävät laihoiksi. Tuloksia ei käytetä ”syyllisten hakemiseen”, vaan nykytilanteen parantamiseen.
Tulosten oikeellisuuden pikainen ennakkotarkastelu	Usein kartoituksissa tuloksiin jää aluksi ”vinouma/bias”, koska haastateltavilla on erilaiset näkemykset nykytilasta. Jos vastauksia voidaan käydä yhdessä jo kartoituksen lopussa läpi esim. tietoturvavastaavan kanssa, pystytään tällaiset tilanteet tunnistamaan ja ”skaalaamaan” haastateltavien tulokset paremmin yhteensopiviksi.
Tulosraportin laadinta	Kartoittajat kirjoittavat tuloksista raportin, joka sisältää sekä yksityiskohtaiset löydökset, tietoturvan osa-alueiden tulostasot, että tärkeimmät kehityskohteet.
Kartoitustulosten esittely	Raportin valmistuttua kartoituksen tulokset käydään yhdessä läpi, jotta varmistutaan niiden oikeellisuudesta ja että kaikki raportin vastaanottajat ymmärtävät mitä tulokset tarkoittavat. **Raportti kannattaa luokitella ja säilyttää hyvin luottamuksellisena**, sillä hyökkääjän käsissä sitä voitaisiin käyttää ”vaarallisena aseena” yritystä vastaan, sisältäähän se erittäin arkaluontoista tietoa yrityksen tuotannon kyberturvallisuuden heikoista kohdista.
Keskustelu tuloksista ja suositelluista kehityskohteista	Tulosten läpikäynnin jälkeen tulee käydä jatkokeskustelu ja pitää palavereja siitä, miten löydetyt puutteet korjataan, sekä millaisia kehitysprojekteja ja organisointia tilanteen takia tulee järjestää. Vähitellen tuotantoyritykseen tulisi syntyä oma, toimiva malli tietoturvan jatkuvaan kehittämiseen. Omaan malliin vaikuttavat esim. ulkoistusten taso ja kumppaneiden kyvykkyys.

Kuva 7. Voimalaitoksen yleiskartoituksen päävaiheet ja niissä huomioitavat asiat.

Vieläkin kevyempää kartoitusmenettelyä tarvitaan esimerkiksi silloin, kun halutaan nopeasti saada selville tärkeimmät kehityskohteet kyberturvallisuuden osa-alueissa ja jatkuvuuden varmistamisessa tai jos avainhenkilöiden saatavuudessa haastatteluita varten on merkittäviä ongelmia. Tällöin joudutaan tyytymään suppeampaan joukkoon haastateltavia tai yhteishaastatteluun (mikä voi olla eduksikin tiedon siirtymisessä yrityksen sisällä).

Toisaalta taas haavoittuvuusskannuksin laajennetussa kartoituksessa tulee ottaa turvallisuustekijät erityisen hyvin huomioon, jottei aiheuteta häiriöitä tuotannossa oleviin kohdejärjestelmiin. Usein tämä on onnistunut sopimalla haavoittuvuusskannaukseen sellaisia ajankohtia ja tuotantojärjestelmiä, jotka on voitu turvallisesti irrottaa tuotantoverkosta skannauksen ajaksi. Haavoittuvuusskannerin sisältävä tietokone on sitten yhdistetty erillisellä datakaapelilla skannauskohteeseen (jolloin koneet konfiguroidaan samaan aliverkkoon ja ne voivat kommunikoida suoraan keskenään), jonka jälkeen skannaus on voitu ajaa turvallisesti myös laajimmassa, aikaa vievässä muodossaan (Tenable Nessus, Advanced policy -moodissa). Joissain yksittäisissä erityistapauksissa olemme saaneet luvan skannata tuotantoverkossa olevaa järjestelmää, mutta tällöin kyseessä on yleensä ollut esim. tuore tukipalvelin tai vastaava, jonka etukäteen tiedämme kestävän hyvin kyseistä skannausta. Tällöin esim. virheohjauksen riski on ollut siedettävän pieni ja skannaus on uskallettu toteuttaa, toki esim. järjestelmätuki on silloin oltava nopeasti saatavilla.

Ajan kuluessa kyberturvallisuusuhat ja sen mukana toiminnalle asetettavat vaatimukset kuitenkin muuttuvat. Tästä syystä myös yleiskartoituksessa käytettävien tietoturvallisuuden osa-alueiden vaatimusten tulee päivittyä. Tätä tukevaa työtä kannattaisi jatkaa Huoltovarmuuskeskuksen tulevissakin projekteissa.

2.3.1 Yleiskartoitukseen käytettävät sapluunat

Olemme vuosien kuluessa aiemmissa projekteissa ja myös KYBER-ENE hankekokonaisuuden yhteydessä kehittäneet yleiskartoituksissa käytettäviksi tarkoitetut haastattelutaulukon (MS-Excel) ja raporttipohjan (MS-Word), jotka ovat osoittautuneet tehokkaiksi apuvälineiksi myös energia-alan automaation kyberturvallisuuden kartoituksissa. Seuraavassa lyhyesti näiden tarkemmat kuvaukset.

2.3.1.1 Haastattelutaulukko

Olemme käyttäneet viimeaikaisissa voimalaitoksiin kohdistetuissa yleiskartoituksissamme avainhenkilöiden haastatteluissa MS Excel-vaatimustaulukkoa, jonka ensimmäisiä versioita lähdimme jo 2010-luvun alussa kehittämään Valtionhallinnon tietoturvallisuusohjeen [VAHTI 2/2010] pohjalta. Vuonna 2013 kehitettyä Excel-taulukkoa ei julkaistu, tuolloin viittasimme ainoastaan ”kartoituksen ennalta-asetettuihin tavoitteisiin” Huoltovarmuuskeskuksen julkaisussa [TEO-SUMMARY] (s. 22). Muutamia vuosia myöhemmin myös KYBER-VESI [KYBER-VESI] hanke sovelsi ja jatkojalosti vastaavan taustan omaavia MS Excel-vaatimustaulukoita. KYBER-ENE hankkeessa edellä mainituilta pohjilta jatkojalostettu vaatimustaulukko sisältyy hankekokonaisuuden tulosaineistoon, jonka olemme asettaneet energia-alan huoltovarmuuskriittisten yritysten saataville.

Avainhenkilöiden haastatteluissa tutkitaan yksityiskohtaisin vaatimuksin sekä hallinnollisia että teknisiä osa-alueita. Usein yksi vastaaja vastaa joko hallinnollisiin tai teknisiin vaatimuksiin osaamisensa ja vastuualueensa mukaisesti.

Hallinnollisen kyberturvallisuuden osa-alueita esittelevä esimerkkigrafiikka on esitetty seuraavassa kuvassa.

Kuva 8. Hallinnollisen kyberturvallisuuden osa-alueet esimerkkigrafiikassa.

Vastaavasti teknisen kyberturvallisuuden osa-alueita esittelevä tulosgrafiikka on esitetty seuraavassa kuvassa.

Kuva 9. Teknisen kyberturvallisuuden osa-alueet esimerkkigrafiikassa.

Kukin kyberturvallisuuden osa-alue sisältää 5-12 vaatimusta, joihin annettujen vastausten (1= vaatimus ei toteudu, 5= vaatimus toteutuu osittain, 10= vaatimus toteutuu täysin) keskiarvo tuottaa ko. osa-alueen pistemäärän. Kuvan sininen kehä on asetettu tasoon 5 (=vaatimus toteutuu osittain), joka onkin ollut käyttökelpoinen, sillä tarkoituksena on ollut tunnistaa heikoiten hallinnassa olevat tietoturvallisuuden osa-alueet. Tällöin heikoimpien osa-alueiden tulokset usein jäävät tason 5 alle.

Seuraavassa taulukossa esitämme Esimerkki osa-alueen ”C: Automaatio-omaisuuden hallinta” vaatimukset (6 kpl).

C: Automaatio-omaisuuden hallinta	
	Inventointi: Automaatiojärjestelmä on inventoitu ja luettelo on saatavilla, sisältäen kaikki käytössä olevat fyysiset ja virtuaaliset laitteet, datat, palvelut, ohjelmistot versioineen ja niiden lisenssit.
	Omistus ja vastuuhenkilö: Omistus ja vastuuhenkilö(t) on määriteltyinä kaikille laitteille, rekistereille, tietojärjestelmille ja datalle koskien koko elinkaarta hankinnasta poistoon.
	Katselmointi: Automaatio-omaisuuden inventointi ja järjestelmäkuvaukset, mukaan lukien lakien sisältämät rekisterit, katselmoidaan säännöllisesti.
	Liitäntä kaupungin tai kunnan IT:hen (tms.): Mahdollinen liitäntä kaupungin/kunnan IT:hen; vastuu ja valtuudet on sovittu kirjallisesti. Dataa koskien tietoturva-asiat on huomioitu sopimuksessa.
	Liitäntä muihin järjestelmiin: Liitäntä muihin järjestelmiin (esim. toimittajien); vastuut ja valtuudet on sovittu kirjallisesti. Dataa koskien tietoturva-asiat on huomioitu sopimuksessa.
	Varmenteet: Varmenteiden (sertifikaattien) käyttöön ja uudistamiseen on dokumentoidut käytännöt. Kaikki varmenteet ovat kirjanpidossa ja ajan tasalla.

Kuva 10. Esimerkki osa-alueen ”C: Automaatio-omaisuuden hallinta” vaatimukset.

Huom! Usein käytännössä haastateltavien on ollut tarpeen vastata vaatimuksiin millä tahansa kokonaisluvulla (välillä 1-10), jotta eri osa-alueiden tulokset on saatu paremmin erottumaan toisistaan ja jotta kehittymistä edellisen kartoituksen jälkeen olisi mahdollista seurata tarkemmin. Tällöinhän myös vähittäiset parannukset vaikuttavat osa-alueiden keskiarvoihin ja täten kokonaistulokseen. Kehitystä tekee mielellään silloin, kun se näkyy myös kokonaistuloksissa.

2.3.1.2 Yleiskartoituksen raporttipohja

Hankkeen kuluessa olemme aiemmin toteutettujen kartoitusten pohjalta edelleen kehittäneet tuotannon kyberturvallisuuden yleiskartoitukselle raporttipohjan, jota käyttämällä kartoituksen tulokset voidaan kommunikoida vakioidulla tavalla kohteena olevalle yritykselle. Raporttipohjaa etukäteen tarkastelemalla selviävät myös mm. kartoituksessa käytettävät menetelmät:

- kartoituksen yleiset tavoitteet
- kartoituksen rajaukset
- kartoitusmenetelmät
- tulosten esitysmuoto
- tulosten osa-alueet

Kehitetty raporttipohja sisältyy hankekokonaisuuden tulosaineistoon, jonka olemme asettaneet energia-alan huoltovarmuuskriittisten yritysten saataville. Seuraavassa kuvassa on esitetty kyberturvallisuuden yleiskartoitukselle kehittämämme raporttipohjan sisällysluettelo.

Sisällysluettelo

Kuva 11. Kyberturvallisuuden yleiskartoituksen raporttipohjan sisällysluettelo.

Yleiskartoituksen tulosraportti ja sen sisältämä informaatio kannattaa luokitella salaiseksi ja säilyttää erittäin turvallisessa paikassa mahdollisten hyökkääjien ulottumattomissa. Mikäli tulosraportti päätyisi vääriin käsiin, se tekisi kohdeyritykseen kohdistuvan hyökkäyksen paljon helpommaksi ja ehkä myös todennäköiseksi, sillä se auttaisi hyökkääjää tunnistamaan ja hyväksikäyttämään kohdeyrityksen käytössä olevia erilaisia järjestelmiä ja niiden mahdollisia heikkouksia.

2.4 Kyberturvallisuuden tehtävät ja työnjako

Tuotannon kyberturvan hallintamallin yhteydessä määrittelimme myös kyberturvallisuuden kehittämisen ja ylläpitämisen tärkeimpiä tehtäviä. Tämän tarkoituksena oli antaa myös yritysjohdolle yleiskuva siitä, kuinka laajasta asiasta kyberturvallisuuden varmistamisessa onkaan kyse. Ennen kaikkea tehtävien listaaminen ja luokittelu auttavat määrittelemään vastuulliset tahot ja tarvittavan tuen tai seurannan kullekin tehtäväryhmälle.

Allaolevassa kuvassa (12) esitetään oletusarvoisena työjaon mallina, että järjestelmän tai tuotanto-omaisuuden omistaja (*asset owner*) vastaa pääsyoikeuksien valvonnasta, tuotanto-omaisuuden hallinnasta ja järjestelmien hallinnasta. Toisaalta perustetun tietoturvatiimin vastuulla on tukea vahvasti kyberturvallisuuden suunnitteluun, kehittämiseen ja jalkautukseen liittyviä tehtäviä. Erityisen tärkeää on muistaa, että kyberturvallisuuden kehittämisen kehitysvastaava nimitetään myös (ei näy kuvassa). Yritysjohdon tehtävänä on yleisesti ottaen huolehtia henkilöstön hyvästä johtamisesta ja kumppanuuksien hallinnasta, ottaen huomioon myös kyberturvallisuuteen liittyvät kysymykset, huolehtia riittävästä koulutuksesta, kyvykkäiden kumppanien valinnasta, jne.

Älykkäiden sähköverkkojen (*smart grid*) tapauksessa sähkönsiirtojärjestelmään voidaan liittää esim. uusien tuottajien pienempiä (hajautettuja) energiantuotantoyksiköitä, jolloin tuotanto-omaisuuden omistajuus ja hallinta hajautuvat entistä laajemmalle. Tämä saattaa vaikeuttaa (hiljalleen eriytyvän) tuotanto-omaisuuskokonaisuuden kartoittamista ja täten tahattomasti heikentää kyberturvallisuustilanteen kokonaisuuden näkyvyyttä ja hallintaa.

Kuva 12. Kyberturvallisuuden tehtäviä elinkaaren kaikissa vaiheissa.

Kyberturvallisuuden jatkuva kehittäminen myös tuotannon muutos- ja kartoitusvaiheissa on erityisen tärkeää, siksi listasimme seuraavassa kuvassa erityisesti siihen liittyviä tehtäviä. Tuotannon muutos- ja kartoitusvaiheissa tuotanto-omaisuuden omistaja vastaa elinkaaren erivaiheissa mm. hankintojen vaatimuksista, käyttöönoton vaatimuksista ja valvonnasta, kyberturvallisuuden kartoituksista käytön ja kunnossapidon aikana, sekä järjestelmien turvallisesta hävittämisestä tai kierrättämisestä poistovaiheessa. Tietoturvatiimi luonnollisesti tukee tuotanto-omaisuuden (ja tuotannon) omistajia esimerkiksi näihin liittyvien prosessien, menettelytapojen, vaatimusten ja valvonnan määrittelystä ja toteuttamisesta.

Tulee ymmärtää, että nämä kaaviot ovat ainoastaan suuntaa-antavia ja auttavat yrityksiä kyberturvallisuuden tehtävien hahmottamisessa ja kunkin osa-alueen vastuullisten ja tukihenkilöiden määrittelyssä. Esimerkiksi kukaan ulkopuolinen ei voi kopioida yrityksen organisaatioon jossain muualla käytettyä mallia työnjaosta, vaan tarvittava määrittelytyö on joka tapauksessa erikseen tehtävä kussakin yrityksessä ja yhteistuumin sopien. Ainoastaan näin saadaan aikaan käytännön työssä toimivia ohjeita, resursointia ja työnjaon määrittelyjä.

Kuva 13. Kyberturvallisuuden tehtäviä tuotannon muutos- ja kartoitusvaiheissa.

Luku 3

OMAISUUDEN HALLINNAN JA KYBERHAVAINTOKYVYN KEHITTÄMINEN

Kuva: iStock

3. OMAISUUDEN HALLINNAN JA KYBERHAVAINTOKYVYN KEHITTÄMINEN

Omaisuuden hyvä hallinta ja kyberhavaintokyky kulkevat käsikädessä ja ovat vahvasti riippuvaisia toisistaan, siksi päätimme käsitellä niitä tässä projektissa yhdessä. Perusteluja on useita. Kyberuhat muodostavat monimutkaisen kentän ja kehittyvät jatkuvasti, mikä tarkoittaa uusien havainnointimenetelmien kehittämistä tai ainakin olemassa olevan kyvykkyyden päivittämistä. Toisaalta myös vanhoja, useita vuosia sitten tunnistettuja uhkia vastaan täytyy pystyä edelleen suojautumaan. Tämä kokonaisuus tekee uhkia havainnoivan työtehtävistä erittäin vaativia ja työläitä, mutta hyvä tuotanto-omaisuuden hallinta voi auttaa tässä mm. vähentämällä tarkkailtavien uhkien ja kohteiden lukumäärää.

Jotta lukuisia uhkia vastaan pystyttäisiin suojautumaan myös käytännössä, tai edes tunnistamaan todellisen uhan mahdollisuus, tarvitaan siis välttämättä hyvää tuotanto-omaisuuden hallintaa. Tuotanto-omaisuuden hallinnan merkityksestä kyberturvallisuudelle kirjoitimme erillisen luvun ”KYBER-TEO tuloksia 2014 - 2016” kirjaan [KYBER-TEO], jossa dokumentoimme automaatiota hyödyntävän teollisuuden kyberturvallisuuden kehittämisen käytännön keinoja. Haavoittuvuuksien ja uhkien hallinnan työkalujen ja yhteisöjen tuntemus ovat edelleen tärkeä osa tätä työtä.

Tuotanto-omaisuuden hallinnan avulla voimme mm. saavuttaa parempaa:

- **Haavoittuvuuksien hallintaa:** Haavoittuvuusanalyysiin käytettävien työkalujen tehokkaampi käyttö tuotanto-omaisuuden tietokantoja hyödyntämällä (skannataan kriittiset kohteet säännöllisesti)
- **Uhkien tunnistamista:** Päätelaitteiden ja verkkojen uhkien, sekä resurssien väärinkäytön ja henkilöstöön kohdistuvien reaaliaikaisten uhkien seurannan tarkempi kohdistaminen (osataan seurata kriittisimpiä tai houkuttelevimpia kohteita tarkemmin)
- **Riskien hallintaa:** Audit- ja riskikartoitusten tavoitteiden ja kohteiden tarkempi valinta (kriittisen tuotanto-omaisuuden säännöllinen auditoiminen).

Yleisesti ottaen voidaan sanoa, että ilman nykyisen tuotanto-omaisuuden ajantasaista kirjanpitoa ja hyvää elinkaarenhallintaa (mitä järjestelmiä on uusittava, milloin ja miten?) kyberturvallisuuden ylläpitäminen jää sattumanvaraiseksi toiminnaksi. Periaatteessa varsin yksinkertaiset, mutta ajantasaiset tuotanto-omaisuuden inventaario ja elinkaarisuunnitelma, ovat siis perustavanlaatuisia edellytyksiä tehokkaan haavoittuvuuksien tunnistamisen, uhkien havaitsemisen ja riskien hallinnan onnistumiselle. Omaisuudenhallinta on pohja, jolle lähes kaikki kyberturvallisuusmenettelyt perustuvat. Esimerkiksi hyökkäystilanteiden tutkinta, negatiivisten vaikutusten minimointi, sekä palautus ja häiriötilanteesta toipuminen vaikeutuisivat huomattavasti, mikäli ajantasaisia tuotanto- ja ICT-omaisuustietoja ei olisi saatavilla.

Tuotantojärjestelmien kyberturvallisuuden hallinnan nykytilan kokonaisvaltaiseen kartoittamiseen tarvitaan varsin monen tyyppisiä toimenpiteitä. Käytännössä tulisi kartoittaa esimerkiksi:

- Jatkuvuuden varmistamisen järjestelmien ja palautuskyvyn todellinen tila?
- Verkkolaitteiden tila ja konfiguraatio?
- Automaatiojärjestelmien tila ja konfiguraatio?
- Kiinteistöautomaatiojärjestelmien ylläpidon tila?
- Tukiohjelmistojen tila (joka voi vaikuttaa tuotantoon)?
- Ylläpito- ja kunnossapitosopimusten tila?

Omaisuuden hallinnan käytäntöjen lisäksi tässä luvussa kerrotaan myös automaation turvallisuuden hallinnan arvioinnista, tuotantoverkkojen lokikeräyksen ja monitoroinnin kehittämisestä, SOC-palvelun käyttöönotosta sekä ansoitusmenetelmien hyödyntämisestä.

3.1 Omaisuuden hallinnan käytännöt

Teollisuuden tuotanto-omaisuuden hallinta kattaa useita varsin laajojakin osa-alueita, joista kukin voi vaatia omat määritellyt hallinta- ja menettelytapansa. Myöskään tiettyyn käyttötarkoitukseen kehitettyjen erillisten työkalujen käytöltä tuskin voidaan välttyä. Tämä tuo tietenkin omat haasteensa näiden työkalujen ja prosessien ylläpitoon, sekä mahdollisia uusia tietoturvauhkia. Omaisuuden hallinnassa käytettävät järjestelmärajapinnat tuli-

sikin olla erillisiä varsinaisista tuotantokäytön rajapinnoista, eli hallintarajapinnat on suojattava erikseen.

Kuva 14. Tuotanto-omaisuuden hallinnan osa-alueita teollisuudessa sekä omaisuuden hallinnan tavoitteita. [MIKKONEN], [OKSANEN].

3.1.1 Hankintojen merkitys omaisuuden hallinnassa

Hankinnoilla on erittäin suuri rooli omaisuuden hallinnan onnistumisessa. Hankintasopimuksen yhteydessä on määriteltävä vaatimukset myös kyberturvallisuudelle, sillä muutoin tuotantoon toimitettu tuote tai palvelu voi olla hyvin vaikeaa saattaa laitoksen normaalien kyberturvallisuusmenettelyjen piiriin. Esimerkkinä vaikkapa järjestelmään sisään kirjautuminen tuotannon käyttäjätunnistusmenettelyn kautta (esim. automaation *Active Directory*-palvelu).

Kuva 15. Hankinnoilla on erittäin vahva vaikutus omaisuuden hallintaan.

Vastaavasti esimerkiksi toimittajan vastuut huollon ja ylläpidon tehtävistä tulee määritellä mahdollisimman yksiselitteisesti etukäteen. Tärkeää on huolehtia myös siitä, että toimittaja kykenee palvelemaan myös kyberturvallisuustilan seurannassa kustannustehokkaalla tavalla.

3.1.2 Automaatio-omaisuuden hallinta

Automaatio-omaisuuden hallinta kyberturvallisuuden näkökulmasta perustuu seuraaviin seikkoihin:

- *Paikallista ja tunnista tärkeimmät:*
  - Automaatio-ohjaukset
  - Laitteet
  - Ominaisuudet
- Ymmärrä:
  - Ovatko laitteet kytkettyjä toisiinsa.
  - Perustuvatko laitteet ja tietoliikenne perinteisiin automaation kenttäväylä-ratkaisuihin vai Ethernet-rajapintoihin, joissa käytetään Internet-lähtöisiä TCP/IP-protokollaperheiden tekniikoita.
  - Sijaitsevatko laitteet turvallisella alueella kuten rakennuksessa tai aidatussa laitoksessa vai etäällä.
  - Ovatko ohjauslaitteet viranomaismääräysten alaisia.
  - Onko laitteen menetys merkittävä (talous, terveys, turvallisuus, ympäristö).

Omaisuudenhallinnan parantamiseen liittyvässä käytännön työssä seuraavista neuvoista on varmasti hyötyä:

- Laitteiden ja järjestelmien ryhmittely ja luettelon tekeminen
  - Verkkokaavio → vyöhykkeiden ja tietoväylien määrittäminen.
  - Riskiarvioinnit ottaen huomioon tärkeysjärjestyksen
  - Eri alueiden luotettavuustarve
- Luettelotyökalut - käytettävä varovaisesti automaatioympäristössä
  - Testaus ensin esim. järjestelmässä joka ei ole käytössä, jotta nähdään viitteitä mahdollisista vaikutuksista.
- Täysi haavoittuvuuksien arviointi suunniteltava, jos:
  - Järjestelmän laitteet on kytketty suoraan Ethernet-rajapintojen tietoliikenneratkaisuihin
  - Järjestelmä on kytketty yritys- tai muuhun ulkoiseen verkkoon
  - Järjestelmää käytetään etäyhteyden kautta
  - Mikä tahansa yllä olevista on suunnitelmissa lähitulevaisuudessa.

Käytännössä täytyy siis pystyä tunnistamaan ainakin tärkeimmät tuotanto-omaisuudet. Jotta tuotanto-omaisuutta pystyttäisiin ylläpitämään suunnitellusti koko elinkaaressa, tuotannon järjestelmät kannattaa jakaa pääryhmiin:

- Mitä IT-osasto hallinnoi itse?
- Mitä automaatio-osasto hallinnoi itse?
- Minkä järjestelmien hallinta on ulkoistettu?

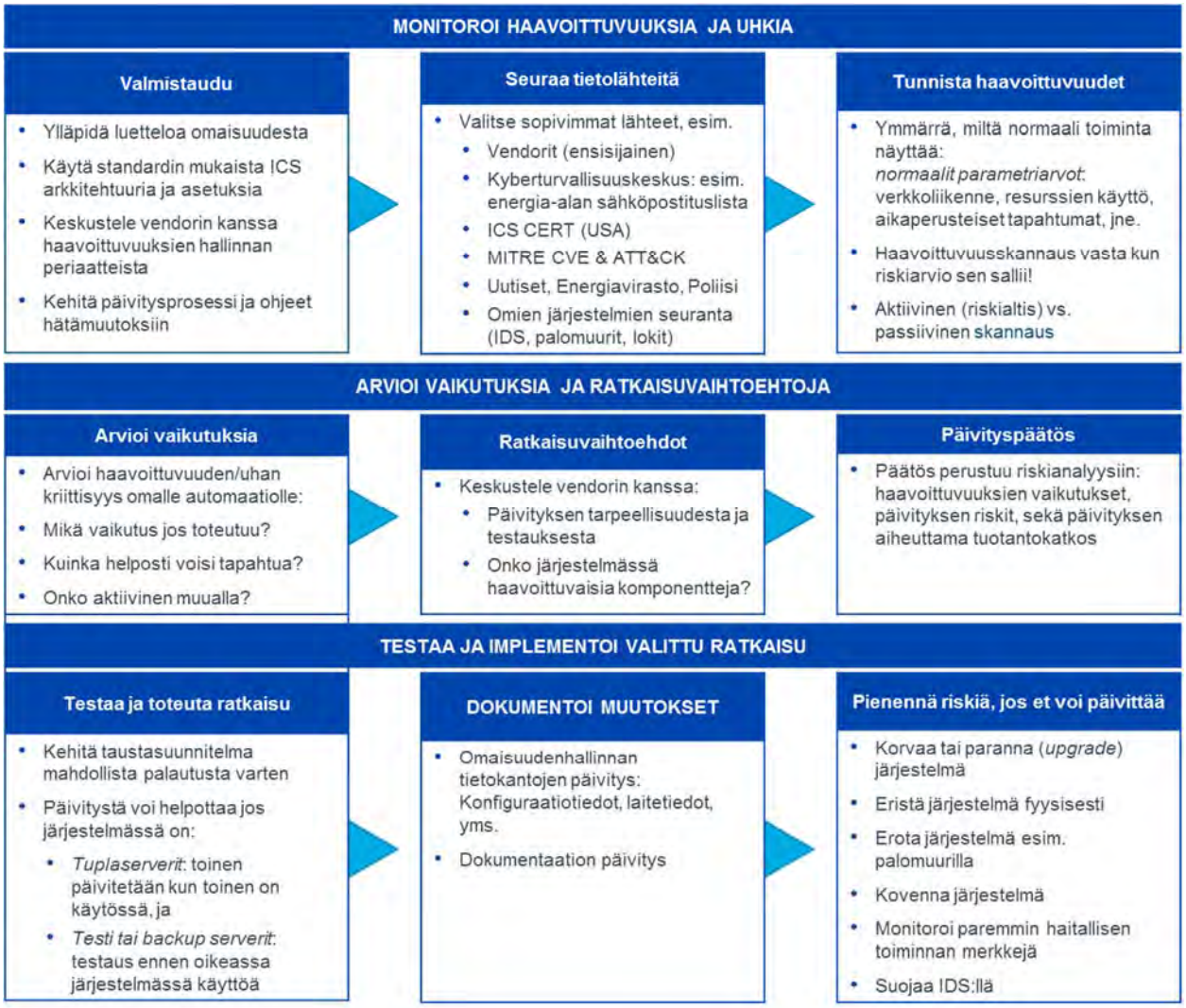
3.1.2.1 Automaation haavoittuvuuksien hallinnan osatehtävät

Automaation haavoittuvuuksien hallinnan vaiheet ja tärkeimmät osatehtävät ovat varsinkin hädän sattuessa kriittisiä asioita ja siksi ne tulisikin ymmärtää varsin perusteellisesti. Asiaan liittyvien hallintatehtävien laajuus ja tarvittavan lähtöinformaation määrä ja hajanaisuus saattavat aiheuttaa jopa vaikean hahmottamisongelman (varsinkin kiireessä ja muiden töiden ohessa tehtynä), joka johtaa vääriin reaktioihin tai huonoon tilanteen hallintaan.

Haavoittuvuuksien hallintaan ja sen kehittämiseen liittyviä osatehtäviä ovat:

- Seuraa (monitoroi) haavoittuvuuksia ja uhkia monipuolisesti
  - Yleisten ja toimittajakohtaisten haavoittuvuuslistojen ja uhkien seuranta
  - Omien järjestelmien haavoittuvuuksien seuranta (esim. vuosittainen inventaario tai skannaus)
  - Säännölliset raportit omiin järjestelmiin liitettyjen muiden palvelujärjestelmien haavoittuvuus- ja uhkatilanteista
- Arvioi vaikutuksia ja eri ratkaisuvaihtoehtoja
- Testaa ja implementoi valittu ratkaisu

Seuraava kuva esittää automaation haavoittuvuuksien hallinnan osatehtävät hieman tarkemmalla tasolla.



Kuva 16. Automaation haavoittuvuuksien hallinnan osatehtävät.

3.1.2.2 Omaisuuden hallintaratkaisujen arvioinnista

Omaisuuden hallintaan liittyviä tavoitteita ja ratkaisuja on lukuisia erilaisia, joten niiden valinta ja arviointi täytyy suunnitella erikseen kuhunkin käyttötarkoitukseen. Taustalla olevana tarpeena oli tuotanto-omaisuuden ja sen hallinnan turvallisuusuhkien ja haavoittuvuuksien parempi tunnistaminen. Omaisuudenhallintaratkaisujen arvioinnille saadaan oikea suunta käyttämällä yleisen tason tarkistuslistaa, mutta tarkemmat kriteerit määräytyvät toki tarpeiden ja käyttötapausten mukaan.

Hallintaratkaisujen arvioinnin lyhyt tarkastuslista:

Soveltuvuus omiin tarpeisiin (esim. monitoimittajaympäristöön, omaan käyttöön, ulkoistettuun käyttöön)

- Käyttäjät tulisi saada mukaan ratkaisujen arviointiin ja valintaan
  - Miten ratkaisu tukee eri tehtäviä?
  - Mitä riskejä ratkaisulla olisi?

Muutoksen hallinnan prosessit ja työnjako

- Keneltä ja mistä järjestelmistä tarvittava tieto saadaan?
- Mitä tiedolla tehdään?
- Miten tieto pysyy ajan tasaisena, kuka päivittää tiedon?

Käytettävyys, käyttöönotto ja ylläpito

- Luotettava toimittaja
  - Kotimainen toimittaja on lähellä ja tavoitettavissa
- Tiedonvaihto toimivaksi
  - Yhteistyön mahdollistaminen

Laajennettavuus tulevaisuuden tarpeisiin ja käyttö muualla (*roll-out*)

- Standardit rajapinnat ja sovellukset (*apps*) tärkeimmille alustoille?
  - Tiedonvaihdon ja keskustelun mahdollistaminen
- Standardit tiedonesitysmuodot
  - Tiedon ymmärtäminen (kone, ihminen)

3.2 Automaation kyberturvallisuuden hallinnan arviointi

Automaation turvallisuuden hallinnan onnistumiseen vaikuttavat lukuisat tekijät. Hyvätkään kyberturvallisuuden hallinnan mallit, prosessit ja toimintaohjeet eivät pelkästään riitä, sillä hyvään turvallisuuteen johtavan asenteen ja toimintatavan täytyy olla sisäistettynä kaikkien kohderyhmän toimijoiden mielissä. Esimerkiksi aikuisviihteeseen hurahtanut huoltomies tai lukituksen palautuksen osalta huolimaton siivoja voivat aiheuttaa voimalaitoksen kyberturvallisuuteen hetkellisen aukon, jota kautta kyberhyökkääjän on helppo ryömiä huomaamatta sisään. Emme siis voi tyytyä kehittämään ja arvioimaan pelkästään (teoreettisia) hallintamalleja, vaan seurannan ja parantamisen täytyy ulottua vahvasti myös käytännön työhön ja tietoisuuden kehittämiseen.

Kyberturvallisuuden hallinnan tason ja toteuman onnistumisen arviointi on siis varsin vaikeaa, erityisesti tehtävän moniulotteisuuden ja ympäristön jatkuvan muutoksen takia. Millä kriteereillä kyberturvallisuuden hallinnan tasoa tai onnistumista kannattaisi käytännössä lähteä arvioimaan?

PERUSTA: Liiketoiminta ja käyttötapaukset vaikuttavat siihen, että millaiset arviointikriteerit ovat relevantteja. Ensin täytyy siis hyvin ymmärtää ja dokumentoida millaisen liiketoiminnan kyberturvallisuutta olemme itse asiassa varmistamassa.

Liiketoiminnan vaikutus käytettäviin arviointikriteeristöihin ilmenee mm. seuraavien alati muuttuvien tekijöiden kautta:

- Liiketoiminnan toimintaympäristö (esim. maakohtainen / globaali?)
- Hyväksyttävyys, lainsäädäntö jota noudatettava
- Hintarajoitukset toteutukselle
- Siirrettävyyden vaatimukset

Käyttötapausten vaikutus käytettäviin arviointikriteeristöihin ilmenee moninaisina vaatimusalueina, joiden yksityiskohtainen sisältö yleensä muuttuu pitkän ajan kuluessa:

- Turvallisuusvaatimukset
- Jatkuvuusvaatimukset
- Käytettävyysvaatimukset
- Yksityisyydensuojavaatimukset
- Uusiokäyttövaatimukset

Liiketoiminnan ja käyttötapausten jatkuvat muutokset näyttävät siis tekevän soveltuvan arviointikriteeristön määrittelemisestä varsin vaikeaa. Lisäksi kehitettyjä kriteeristöjä tulisi jatkuvasti päivittää liiketoiminnan olosuhteiden ja käyttötarpeiden muuttuessa. Kriteeristöt eivät voi olla staattisia myöskään uhkien jatkuvan muutoksen takia.

Eivätkö edes voimassa olevat kyberturvallisuuden hallinnan kansainväliset standardit sitten osoita kaikille, mitkä ovat normaalit ja kaikille soveltuvat arviointikriteerit? Valitettavasti nekään eivät ratkaise koko ongelmaa, sillä valitettavasti esimerkiksi sinänsä mainion IEC 62443-2-4 ”*Security program requirements for IACS service providers*” standardin kuvaamien kyberturvallisuusvaatimusten soveltaminen on pienemmissä yrityksissä usein vasta työn alla. Käytännössä yritysten kyberturvallisuuden hallintakäytäntöjen kypsyystaso ei ole riittävä tällaisten standardien yksikäsitteiseen soveltamiseen. Kansainvälisiä standardeja vasten arvioitaessa kehityskohteita tulee yksinkertaisesti liikaa, eivätkä standardit yleensä pysty yksinään opastamaan energiayritystä riittävästi. Esim. miten löydösten perusteella tunnistetut puutteet kannattaisi kustannustehokkaasti korjata ja millaisia kehityshankkeita tulisi käynnistää? Myöskään omaisuudenhallintastandardit (tärkeimpinä SFS-ISO 55001 ja 55002) eivät ratkaise tätä monimuotoista kehitysongelmaa.

Standardit tulisi kuitenkin aina sovittaa yrityksen kuhunkin liiketoimintakäytäntöön soveltuviksi, muutoin itse liiketoiminnan tehokkuus kärsisi tietoturvatoiminnosta. Tarvittava sovitustyö vaatisi erityisesti alkuvaiheessa paljon aikaa sekä osaavia resursseja, mutta niitä ei ole käytettävissä.

Entä voisiko siirtyminen automaattisten seurantatyökalujen käyttöön ratkaista yrityksen tuotannon kyberturvallisuuden tilannekuvan muodostamisen ongelman? Tämäkään lähestymistapa ei yksin riitä, varsinkin kun työkalujen käyttäjältä tai tulosten vastaanottajalta monesti puuttuu tarvittava

tietotaito ja ymmärrys jatkuvasti tulevien reaaliaikaisten hälytysten tai varoitusten tulkitsemiseksi; Mitä havaintoja pitää oikeasti ilmoittaa eteenpäin? Mitä ohjelmistoja tai laitteita kannattaa todellisuudessa korjauttaa, jos erilaisia varoituksia tulee jatkuvasti vaikkapa 1000 uutta tapausta viikossa? Toisaalta turvallisen toiminnan ohjeiden noudattamista ja soveltamisen laatua, sekä työntekijöiden kyberturvallisuustietoisuuden tasoa voi olla hyvin vaikeaa mitata teknisten työkalujen avulla. Toteutus vaatisi erityisjärjestelyjä, kuten työtekijöille ja heidän työnkuvaansa räätälöityjen sähköisten kyberturvallisuuskurssien kehittämistä ja riittävän suoriutumisen laajaa ja järjestelmällistä seurantaa. Ensin tulee määritellä turvallisen toiminnan yritys- tai laitoskohtaiset ohjeet ja oikeat toimintatavat, sekä suunnitella ja käynnistää tarvittavat koulutuksen kehittämisen hankkeet. Koulutukseen panostaminen on erittäin suositeltavaa, varsinkin jos yrityksen tuotannon kyberturvallisuuden kehittämisen resurssit ovat rajalliset.

Tarvitsemme siis selkeästi parempaa ja käytännöllisempää tukea energiayritysten tietoturvan hallinnan tason ja tuotannon kehityskohteiden selvittämiseksi. Seuraavissa alakohdissa esittelemme näitä tarpeita varten kehittämiämme yksityiskohtaisempia tuloksia ja malleja.

3.2.1 Sapluuna automaatiojärjestelmien auditointikumppanien arviointiin

Kuten edellä asiaa sivusimme, energiayrityksen tuotannon tietoturvallisuudesta vastaavan henkilön voi olla vaikeaa määritellä yksityiskohtaista kriteeristöä, jota vasten kyberturvallisuuden hallinnan nykytilannetta tulisi arvioida. Tällöin nykytilanteen arvioinnissa kannattaa hyödyntää erilaisia kumppanuusverkostoja ja pilotteja, joiden kautta yrityksen tuotannolle soveltuvimpia arviointikäytäntöjä ja kriteerejä voidaan kehittää yhdessä ja iteratiivisesti. Samalla ymmärrys varmastikin lisääntyy ensinnäkin siitä, mitkä ovat yrityksen kriittisimpiä tuotantojärjestelmiä, sekä millä kriteereillä ja millaisten kumppaneiden tuella kutakin niistä kannattaisi tarkemmin auditoida. Auditoinnilla tarkoitetaan tässä yhteydessä ulkoiselta kumppanilta tilatun palvelun käyttöä automaation kyberturvallisuustilanteen arvioimiseksi sovitun kriteeristön pohjalta.

Kuinka sitten valita omalle yritykselle ja sen tuotannolle soveltuvin kyberturvallisuuden auditointikumppani? Seuraavassa kuvassa esitämme itsensä selittävän konseptin automaatiojärjestelmien auditointikumppanin arviointiin ja valintaan.

Kuva 17. Automaatiojärjestelmien auditointikumppanin arviointi ja valinta.

Alla kaksi hyvää lähdettä auditointiin liittyville vaatimuksille, joita kannattanee hyödyntää automaatiojärjestelmien auditointikumppanien arvioinnissa ja valinnassa:

- Automaation kybervaatimusten ymmärrys: IEC 62443-sarja, mm.:
  - IEC 62443-2-4: Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers
  - https://webstore.iec.ch/publication/61335#
- Auditoijien osaaminen: ISA:n ”IACS arvioijan sertifiointi”-koulutus:
  - ISA course: Assessing the Cybersecurity of New or Existing IACS Systems (IC33)
  - https://www.isa.org/training-certifications/isa-training/instructor-led/course-descriptions/ic33/

Varmista tarvittaessa myös riittävä auditointiosaaminen automaatiokumppaneittain, sekä yleisemmin ymmärrys monitoimittajaympäristön tuomista vaatimuksista.

3.2.2 Sapluuna automaatiojärjestelmien itsearviointiin

Pitkällä tähtäimellä tuotannon automaatiojärjestelmien kyberturvallisuutta tulisi pystyä arvioimaan myös yrityksen oman henkilöstön voimin. Perustelu tälle väitteelle on se, että arviointia itse suunniteltaessa ja toteutettaessa tekijöille kristallisoituu suoremmin yrityksen oman kyberturvallisuuden vaatimuskannan merkitys. Arviointien löydöksethän riippuvat suoraan asetetuista vaatimuksista, ja vaatimukset taas riippuvat suoraan siitä millaisia uhkia vastaan yrityksen on suojauduttava. Esimerkiksi loistavasti valitun ”täsmäsuojauksen” ja siihen räätälöidyn teknisen seurannan ansiosta vuosittain tarkistettavien kyberturvallisuusvaatimusten määrä voi vähentyä merkittävästi. Tällöin osa arvioinneista voidaan siis automatisoida ja ajaa tarkistus läpi aina tarpeen vaatiessa, jolloin vuosittaisessa arvioinnissa voidaan keskittyä vaikkapa uusiin uhkiin varautumisen arviointiin tai esim. kumppanin vaihtamisesta aiheutuvien muutosten ja epävarmuuksien arviointiin.

Kuva 18. Automaatiojärjestelmien itsearviointi

Automaation itsearvioinnissa yrityksen oma osaaminen kehittyy kokonaisvaltaisemmin ja löydökset siirtyvät helpommin esim. automaation uusiksi kyberturvallisuusvaatimuksiksi. Itsearvioinnin muita etuja ovat:

- Kriittisten kohteiden tunnistaminen ja tiedonjako paranevat
- Yrityksen omien kyberturvallisuusvaatimusten määrittely paranee
- Arvioinnit ja auditoinnit jatkojalostuvat ja kohdentuvat jatkossa paremmin
- Löydökset ymmärretään paremmin ja kehityshankkeet saavat vauhtia
- Seurannan automatisointiin tarvittava ymmärrys paranee

3.3 Tuotantoverkkojen lokituksen ja monitoroinnin kehitys

Automaatiojärjestelmä on pitkän elinkaaren verkottunut ohjelmistotuote. Sen tehtävinä ovat pääasiassa

- tuotantoprosessin pitäminen halutussa toimintatilassa
- suorittaa korjaavia ohjauksia häiriötilanteissa
- asetusarvomuutoksen saatuaan suorittaa ohjauksia uuteen toimintatilaan pääsemiseksi

Näiden tehtävien aikaansaamiseksi automaatiojärjestelmä mittaa ohjattavaa prosessia eri tavoin. Automaatioon on siis sisäänrakennettuna järjestelmän tilan seuranta.

Viimeisen parinkymmenen vuoden aikana tietoliikenteen rooli automaation toiminnassa on kasvanut. Tämä johtuu siitä, että siirtyminen perinteisistä automaation kenttäväyläratkaisuista TCP/IP-protokollaperheiden maailmaan on samalla tuonut huomattavasti monimutkaisemman ja sitä kautta haavoittuvamman tietoliikenneratkaisun automaation osaksi. On perusteltua sanoa, että tämän muutoksen kautta olemme tuoneet mukaan uuden automaation osajärjestelmän – tietoliikenneverkon.

Automaatiojärjestelmä monitoroi aktiivisesti fyysisestä prosessista automaatiolaitteiden tuottamaa mittaustietoa. Tämä monitorointi on prosessin säädettävyyden edellytys. Tietoliikennekomponenttien sekä muun tietoteknisen infrastruktuurin seuranta ei kuitenkaan ole samalla tasolla kuin prosessin monitorointi. Tämä johtuu pitkälti siitä, ettei tietoteknisen infrastruktuurin ole ymmärretty olevan oleellinen automaatiojärjestelmän osa. Tämä tilanne vaatii muutoksen.

Automaatiojärjestelmän monitorointia ei tehdä vain prosessin säädön mahdollistamiseksi. Sitä tehdään esimerkiksi myös

- Kunnossapidon tukena huoltotarpeen ennakoimiseksi
- Erilaisten häiriöiden aiheuttamien ongelmien helpottamiseksi
- Jonkun tavoitteen todentamiseksi, esimerkiksi ympäristöluvan säilyttämisen edellyttämä raportointi

Seurannalla pyritään siis havaitsemaan tämän hetkinen tila sekä ennustaa tuleva tila.

Seurannalla on myös selkeitä tavoitteita kuten rahan ja ajan säästäminen, laadunvalvonta sekä turvallisuuden varmistaminen. Seurannalla on sen lisäksi selkeät käyttäjät. Seuranta mahdollistaa tilannekuvan tai tilannetietoisuuden, jotka palvelevat tiettyä käyttäjäryhmää esimerkiksi operaattorit, kunnossapitotoiminta, turvallisuudesta tai laadusta vastaavat.

Johtuen automaation sisäänrakennetusta monitoroinnista sekä sen merkittävästä roolista prosessin hallinnassa, automaatiohenkilöstö pyrkii minimoimaan seurattavien näyttöjen ts. seurattavien suureiden määrää. Tämä on todennäköisesti yksi syy miksi tietoliikennekomponentin seuranta ei ole saanut sen tärkeyden arvoista huomiota – tietoliikenneinfrastruktuurin monitoroinnin lisäarvoa ei olla pystytty selkeästi osoittamaan tai myymään automaatioasiakkaille. Se on jäänyt pitkälti erikoistapauksissa käyttöönotettavaksi lisätoiminnallisuudeksi. Erityisen ongelmalliseksi on osoittautunut kyber- tai tietoturva-etuliitteillä perusteltu monitorointi, jonka lisäarvo on perusteltu vain epämääräisellä ”kyber”-tarpeella tuotannollisen tarpeen jäädessä hämäräksi.

Tämän luvun tarkoituksena on kertoa, miksi tietoliikenneinfrastruktuurin monitorointi on tärkeää sekä keskittyä lokitiedon käyttöönoton helpottamiseen osana infrastruktuurin seurantaa.

3.3.1 Monitoroinnin merkitys

Moderni tietotekninen infrastruktuuri on monimutkainen useita keskinäisiä riippuvuuksia sisältävä järjestelmä. Se on jo itsessään eräänlainen automaatiojärjestelmä, jossa säätöä suoritetaan

useilla eri tasoilla. Hyvänä esimerkkinä reititykseen ja ruuhkaisuuteen liittyvät algoritmit, joiden tehtävä on automaattisesti mukauttaa verkon toimintaa kompensoimaan tietoliikenteestä johtuvia häiriöitä ja/tai ilmiöitä.

Automaatiohenkilöstö ymmärtää monitoroinnin merkityksen osana automaation toimintaa. Tietoteknisen infrastruktuurin automaatiotoiminnallisuuden esittäminen on hyvä tapa perustella, miksi myös tietoteknistä infrastruktuuria tulee monitoroida: infrastruktuurin toiminnasta aiheutuvien häiriöiden ratkaiseminen edellyttää toiminnan järjestelmällistä seurantaa. Mitä laajempi infrastruktuuri, sitä laajempi myös seurannan tulee olla, jotta häiriönhallinta helpottuu. Tieto- tai kyberturvallisuuteen liittyvät havainnointikyvyt saadaan infrastruktuurihäiriöiden monitoroinnin sivutuotteena – tietoturva on vain yksi infrastruktuurissa esiintyvä häiriötyyppi.

Tietoteknisen infrastruktuurin järjestelmällinen ja kattava seuranta on automaation tietoteknisen osaprosessin säädön ja häiriöhallinnan mahdollistaja.

3.3.2 Lokitiedon käyttöönotto

Tietoliikenteen monitorointia on käsitelty muun muassa KYBER-TEO-projektissa. Tässä projektissa keskityttiin sen vuoksi lokien käyttöön osana ympäristön monitorointia.

Ensimmäinen ja todennäköisesti tärkein lokien hyödyntämisen mielekkään toteutuksen edellytys on ymmärtää, että lokitiedon käyttöönotto on automaation muutosprojekti. Kuten projektit yleensä niin myös tähän liittyy tavoitteiden asettaminen, riskiarvio, resursoinnin suunnittelu ja aikataulutus.

Malli lokitiedon hyödyntämistä tukevalle ohjeistukselle on esitetty Liitteessä A.

3.3.2.1 Tavoite

Automaatiojärjestelmä kerää jo valmiiksi paljon lokitietoa. Projektin tavoitteeksi kannattaa kustannussyistä asettaa miten saadaan enemmän hyötyä jo kerättävästä tiedosta. Tämän tavoitteen kautta syntyy myös ymmärrys siitä mitä meiltä puuttuu ja mitä puutteiden korjaaminen edellyttää.

Projektin päätavoite: miten enemmän irti nykyisten järjestelmien keräämästä lokitiedosta.

3.3.2.2 Resursointi ja aikataulutus

Tämän luvun tarkoituksena ei ole tarjota valmista projektia vaan kirjata muistettavia asioita. Lokien keruu voi aiheuttaa muutostarpeita fyysisiin laitteisiin esimerkiksi lokienkeruun vaatiman toiminnallisuuden aikaansaamiseksi (tietoliikenteen siirtokapasiteetti, lokituksen päällekytkeminen, jne.). Mielekkään lokienkeruun aikaansaaminen voi edellyttää myös muutoksia automaatiosovelluksiin. Tällainen voi tulla esiin esimerkiksi lokilähteen paremman kohdennettavuuden aikaansaamiseksi tai lokitiedon lähteellä tapahtuvan rikastamisen mahdollistamiseksi. Rikastamisella tarkoitetaan tässä yhteydessä lokitiedon ymmärrettävyyttä parantavan lisätiedon eli metatiedon lisäämistä lokiin.

Aikataulutuksen osalta tärkein huomio on se, että tuotannossa olevaan prosessiin ei ole järkevää tehdä muutoksia. Ota tämä huomioon ja aikatauluta siten, että muutokset testataan etukäteen ja käyttöönotto on osana normaalia huoltotoimintaa, esimerkiksi huoltoseisokissa.

3.3.2.3 Projektin vaiheet

1. **Selvitä mitä jo nykyisin kerätään**. Automaatiojärjestelmä kerää jo valmiiksi paljon lokitietoa. Käy läpi kerätty tieto ja analysoi sen hyödynnettävyys häiriöiden hallinnassa. Mieti sekä tietoteknisen infrastruktuurin häiriöitä sekä tietoturvaan liittyviä tapahtumia. Tukeudu automaatiojärjestelmiesi toimittajiin ja pyydä heiltä selvitys jo kerättävästä lokista sekä sen sisällöstä.

2. **Selvitä miten kerätty lokitieto on hyödynnettävissä**. Lokitieto tietovarastossa ei vielä mahdollista lokitiedon hyödyntämistä. Tiedon indeksointi ja tiedon hakeminen ovat mielekkään hyödyntämisen edellytykset. Todennäköisesti olemassa olevat lokienkeruut eivät monitoimijaympäristössä ole helposti hyödynnettävissä, koska jokaisella toimittajalla on oma tapansa tiedon keräämiseksi. Selvitä miten lokitietoa voi nykytilanteessa hyödyntää sekä kuka siihen pääsee käsiksi ja miten tietoon voi kohdentaa hakuja.

3. **Arvioi mitkä häiriönhallintaan liittyvät tavoitteet jäävät saavuttamatta**. Esimerkiksi tietoturvahäiriöiden osalta tavoitteita voi olla

useita. Tällaisia ovat esimerkiksi luvattomat tai toiminnan kannalta ylimääräiset kirjautumiset, uusien ohjelmistojen tai ohjelmistoversioiden asennukset ja konfiguraatioiden muutokset, prosessiin liittyvät asetusarvomuutokset sekä diagnostiikkatyökaluilla otettavat yhteydet. Hyvä lähestyminen on miettiä millaisia ilmiöitä pitäisi pystyä löytämään ja analysoida onko ne löydettävissä jo kerätyn tiedon perusteella.

4. **Selvitä mitkä edellä listatuista tavoitteista on saavutettavissa nykyisten lokitiedon keräysmenettelyiden virittämisellä**. Muista että automaatiojärjestelmätoimittaja on oleellinen kumppani analysoimaan ja kehittämään omaa lokitiedonkeruutaan.

5. **Mieti miten häiriön aiheuttajien haku lokimassasta mahdollistetaan**. Keskitetty lokienkeruu on yksi vaihtoehto, mutta pitää muistaa, että se voi olla myös kallis kun lokimäärä kasvaa. Hakuja voi tehdä hajautetusti tai jopa paikallisesti kunhan vain on sopivat työkalut. Tämä voi olla kustannustehokkain, joskin työllistävämpi vaihtoehto keskitetylle lokienkeruulle.

6. **Arvioi mitkä tavoitteet jäävät nykyisillä ratkaisuilla saavuttamatta**. Mieti niiden arvo häiriönhallinnalle.

7. **Suunnittele jatkokehitys**. Käynnistä kehitysprojekti, pilotoi ja arvioi. Älä investoi tekniikkaan, ellei hyöty ole selkeä, koska investoinnin käyttöönotto on uusi resursoitava projekti. Tässä vaiheessa olet jo päätynyt jonkinlaiseen hyväksyttävään riskitasoon, koska ymmärryksesi automaatioympäristöstä on lisääntynyt.

8. **Muista että lokitiedon seuraamista voi ulkoistaa**. Esimerkiksi tietoturvahäiriöiden havainnointiin löytyy valmiita palvelukonsepteja, joissa lokitiedon analysointiin ja häiriöiden havainnointiin on olemassa valmiita hyviä työkaluja. Niiden hyödyntäminen voi olla mielekästä esimerkiksi tapauksissa, joissa halutaan 24/7/365 havainnointikykyä. Toisaalta on hyvä miettiä, onko 24/7/365 ulkoistettu havainnointi mielekästä, jos oma reagointi on kuitenkin vain normaalin päivätyöajan puitteissa.

3.3.2.4 Lokitiedon hyödyntämisen kompastuskivet ja ratkaisuehdotukset

Lokitiedon keruu ei ole sama asia kuin lokitiedon hyödyntäminen. Usein lokienhallintaan markkinoitujen järjestelmien (*Security Information and Event Management*, SIEM) myyntipuheet kertovat niiden ratkaisevan kaikki lokienhallintaan liittyvät asiat. Tämä ei pidä paikkansa, koska arviolta 80% lokienhallintaan liittyvästä työstä ja kustannuksista liittyvät lokien saattamiseen analysoitavaksi – siis siihen osuuteen lokienhallinnasta jolla lokit saadaan SIEM-järjestelmään. Toinen yleiseen data-analyysiin liittyvä huomio on ”Garbage-In-Garbage-Out”, mikä tarkoittaa, että huonosta datasta saadaan huonoja tuloksia. Tämä pätee myös lokeihin. Lokienhallinnan hyöty riippuu merkittävästi lokilähteiden laadusta ja lokien sisällöstä.

Suomen kielen termi ATK (automaattinen tietojen käsittely) on hyvä muistaa lokienhallintaa suunnitellessa, jotta lopputuloksena ei ole MTK (manuaalinen tietojen käsittely). Asian esiintuominen tässä yhteydessä voi kuulostaa oudolta, mutta sen viisautena on muistaa automatisoida kaikki mikä on mahdollista. Esimerkiksi jos häiriön selvittämiseen ja sen kommunikointiin tarvitaan automaatiojärjestelmän positiotietoa niin automatisointi tarkoittaa lokitiedon automaattista rikastamista suunnittelujärjestelmän tiedolla, jossa laitteen verkko-osoitteen perusteella lisätään lokiriviin myös positiotieto. Tämä vähentää manuaalista vaihetta, kun lokihaun tuottamassa tuloksessa on jo valmiiksi kaikki tarpeellinen tieto, eikä tietoa tarvitse rikastaa enää manuaalisesti katsomalla toisaalla olevasta dokumentaatiosta.

Lokienhallinta vaatii ylläpitoa. Tämä on hyvä tunnistaa ja yhdistää huoltotoimiin tarkistuksia lokituksen toimivuudesta. Esimerkiksi järjestelmän päivitys voi muuttaa järjestelmästä saatavaa lokitietoa, erityisesti jos on jouduttu säätämään lokitusta paikallisen tarpeen mukaan. Muista ylläpito ja varaudu myös sen vaatimaan työhön ja kustannuksiin. Kustannussuunnittelussa kannattaa myös miettiä onko saavutettava hyöty sopivassa suhteessa kustannuksiin. Jos kustannus on karkaamassa niin voi olla, että ratkaisutapa (”loki mittauksena”) on väärä. Erityisesti tietoturvaan liittyvässä lokituksessa sama tieto voi olla saatavissa usealla tavalla. Esimerkkinä lokitiedon rikastamisen sijainti: muutos automaatiosovellukseen voi

olla kokonaistaloudellisesti kallis ratkaisu ja rikastaminen kannattaakin tehdä automaatiolaitteelta lokeja keräävässä järjestelmässä.

Algoritmi on hyvä havaitsemaan monimutkaisia hiljaisia riippuvuuksia. Tekoälystä, siis markkinoinnissa älykkääksi tulkitulla algoritmilla, on lokienhallinnassa hyötyä. Tällä hetkellä se edellyttää isoja datamassoja, vaikka trendinä on kehittää algoritmeja, jotka toimivat myös pienellä datamassalla. Algoritmit ovat kuitenkin huonoja tulkitsemaan tuloksen aiheuttamaa riskiä prosessille tai yritykselle. Tästä syystä ihmisen hyödyntäminen (*human-in-the-loop*) tuottaa lokienhallinnassa parhaan lopputuloksen. Ihminen on resurssi, joten lokienhallintaan suunnitellessa muista lokienhallinnan operointi.

3.3.3 Johtopäätökset

Ymmärrys tietoteknisen infrastruktuurin roolista automaation osajärjestelmänä on nykyisin oleellista tiedostaa. Kuten muitakin automaation osajärjestelmiä, myös tietoteknistä infrastruktuuria tulee seurata paremman käytettävyyden, luotettavuuden sekä häiriöhallinnan aikaansaamiseksi.

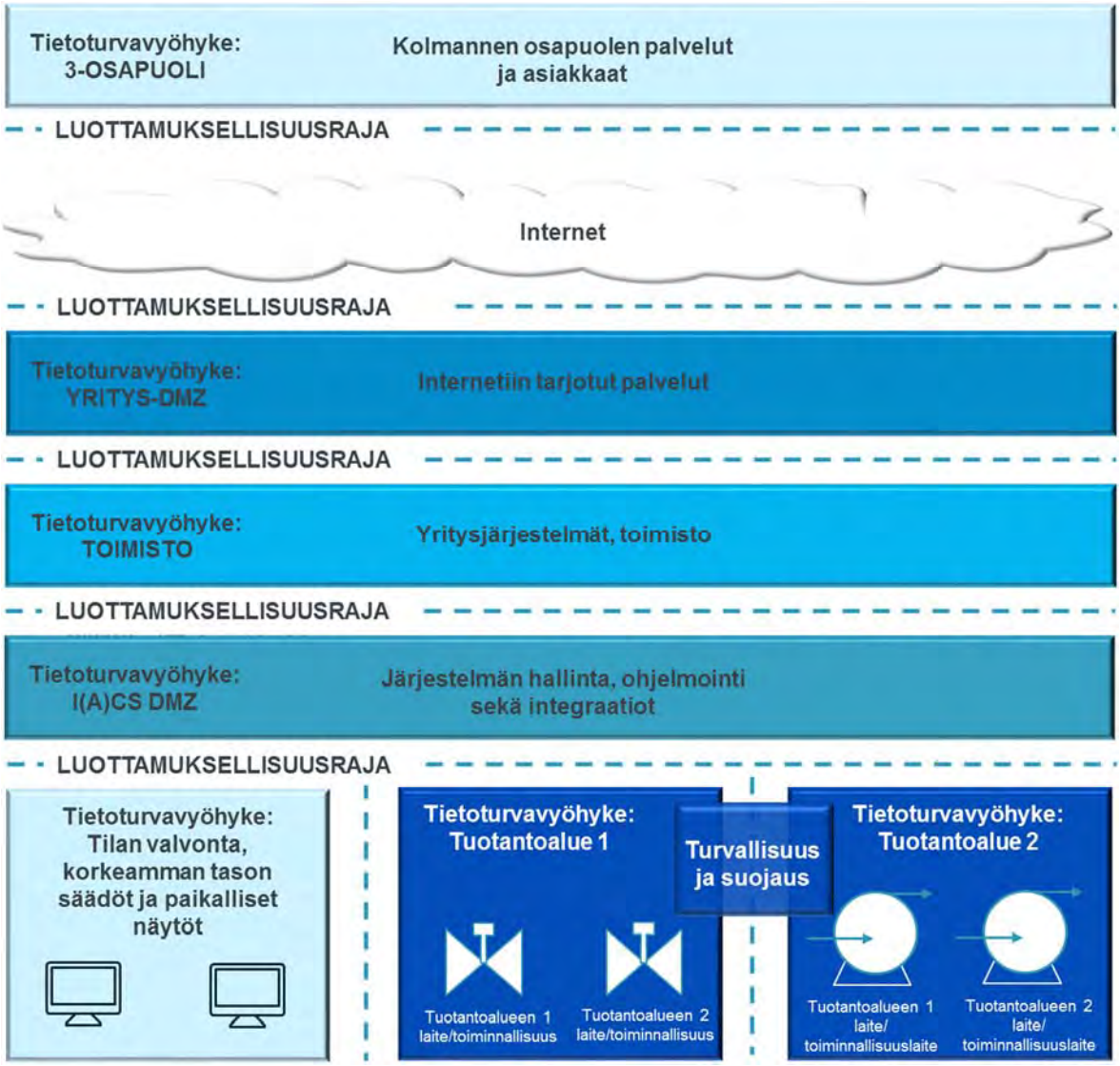
Automaatiojärjestelmään on sisäänrakennettu oman tilan seuranta. Kustannustehokas tapa tietoteknisen infrastruktuurin paremman seurannan hyödyntämiseksi on kartoittaa ja hyödyntää jo olemassa olevaa järjestelmän sisäistä seurantaa. Tämän toteutus edellyttää yhteistyötä järjestelmätoimittajien kanssa.

Lokien käyttö järjestelmän tilan seurannassa tulee projektoida, koska kyseessä on automaatio-organisaation näkökulmasta merkittävä automaatiojärjestelmän muutos. Lokien keruu siten että niiden tietosisältöä voidaan mielekkäästi hyödyntää, on eräs monitoimijaympäristön suurimmista haasteista. Toinen merkittävä haaste on olemassa olevan infrastruktuurin riittävyys ja tekninen kypsyys lokitiedon keräämiseksi. Erityisesti hyödyntämisessä on järkevää tehdä yhteistyötä kaikkien automaation osajärjestelmätoimittajien kanssa, jotta toimiva yhdistelmä keruuta, analyysiä, automatisointia, rikastamista sekä lokeista hakemista voidaan saavuttaa.

Uusien järjestelmien tai vanhojen järjestelmien päivitysten suunnittelussa tulee huomioida tietoteknisen infrastruktuurin seuraaminen. Tässä vaiheessa voidaan helposti teknisesti varautua muun muassa lokitiedon keräämiseen ja siirtämiseen jatkojalostusta varten. Jos tekninen varautuminen unohdetaan, on myöhemmin erittäin haastavaa rakentaa tarvittava toiminnallisuus – jota kuitenkin tullaan nykyautomaatiossa entistä enemmän tarvitsemaan.

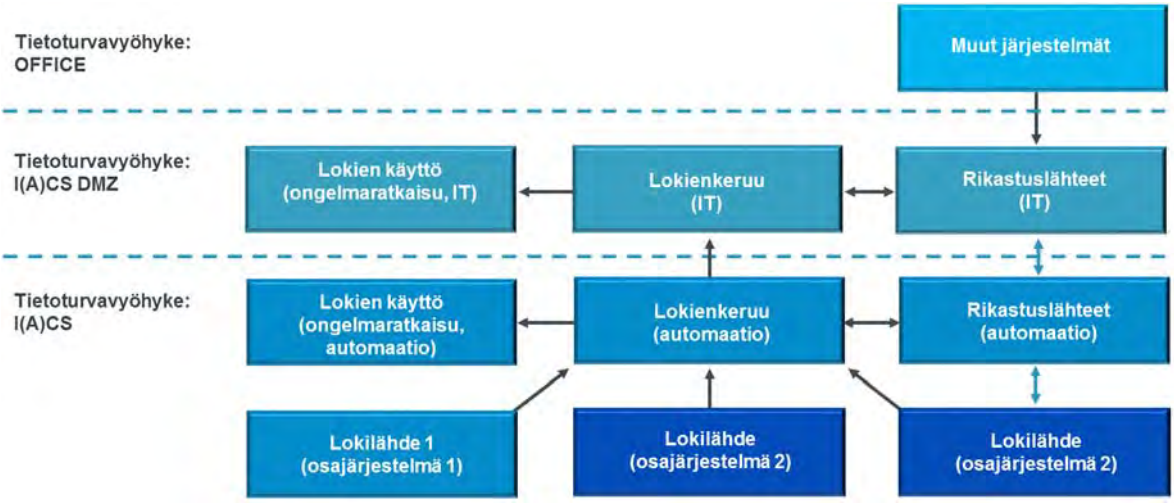
3.3.4 Lokien monitoroinnin referenssimalli ja sen käytännön toteutus eräässä automaatioympäristössä

Lähtötilaksi kannattaa valita IEC 62443 looginen tietoturvavyöhykemalli (*Kuva 19*), jota lokien keruun ja hyödyntämisen tekninen toteutus ei saa rikkoa. Toteutuksen pitää mahdollistaa ICS- ja ICS-DMZ-verkkojen eriyttäminen siten, että lokien hyödyntämismahdollisuus säilyy. Näin voidaan turvata tuotanto myös ongelmatilanteissa, esim. yritysjärjestelmiin kohdistuessa tietoturvauhkia.



Kuva 19. Standardin IEC-62443 tietoturvavyöhykkeet (Security Zones) käytäntöön sovitettuna.

IEC-62443-standardin loogisen mallin mukaan toteutettu lokienkeruu ja monitorointi voi näyttää esimerkiksi seuraavalta:



Kuva 20. Lokituksen toteutus tietovirtoineen suhteessa IEC-62443 tietoturvavyöhykkeisiin.

Kuvan 20 toteutuksen tärkeimmät huomiot:

- Keskeinen tavoite: I(A)CS-DMZ- ja I(A)CS-verkot ovat erotettavissa toisistaan säilyttäen lokien hyödyntämismahdollisuus sekä keruu.
- Lokitietoa voidaan rikastaa sekä I(A)CS-DMZ-vyöhykkeellä että I(A)CS-vyöhykkeillä. Toteutuksessa ei tietoturvasyistä ole hyvä rakentaa tarpeettomia vyöhykkeitä läpäiseviä integraatioita. Tällainen on esimerkiksi Rikastuslähteet (automaatio) ja Rikastuslähteet (IT) välinen sininen yhteys.
- Siniset nuolet kuvaavat vaihtoehtoisia toimintamalleja.
- Suluissa olevat tekstit kuvaavat tiedon pääasiallista hyödyntäjää tai lähdettä.
- Lokienkeruu (IT) ja Lokienkeruu (automaatio) ovat lokisisällöltään identtisiä. Rikastustieto (lokiriviin sisältyvä metatieto) voi olla erilaista rikastuslähteiden saatavuudesta johtuen.

3.3.4.1 Vaiheistus ja päätökset

Vaiheistus ja päätökset, jotka johtivat Kuvassa Kuva 20 esitetyn referenssimallin syntyyn:

- Selvitettiin mitä lokia jo kerättiin
  - Otettiin yhteyttä automaatiotoimittajaan ja kysyttiin mitä lokitietoja kerätään.
  - Otettiin yhteyttä IT:hen ja kysyttiin yhteisten laitteiden ja toiminnallisuuksien osalta (esim. runkoverkko ja palomuurit) saatavien lokien sisältö ja määrä.
- Selvitettiin mitä hyötyä kerätystä tiedosta on
- Kysyttiin automaatiojärjestelmän toimittajalta. Tämän kautta löydettiin esimerkiksi loki, joka ei syntynyt perinteisten lokienkeruun menettelyillä, vaan joka muodostui tekstitiedostona paikalliselle koneelle normaalin järjestelmätoiminnallisuuden seurannan tuloksena.
- Mietittiin, millaisia ongelmia järjestelmässämme on ollut (”käyttötapaukset”)
  - Tavoitteiksi päätettiin ei-toivotun liikenteen havainnointi ja sen jäljittäminen prosessiverkon sisällä olevalle lähteelle.
- Mitä lokeista saatavilla olevaa tietoa puuttui
  - Tavoite oli toteutettavissa olemassa olevien lokilähteiden avulla.
- Mitä jouduttiin rikastamaan manuaalisesti
  - Automaation positiotietoa ei saatu suoraan järjestelmistä, joten kyvykkyys tehtiin manuaalisesti. Luotiin manuaalisesti muunnostiedosto lokienvälitysohjelmistoon, jolla tämä metatieto voitiin automaattisesti lisätä lokiriviin. Positio ja IP-osoitevastaavuus löytyi suunnitteludokumentaatiosta. Toteutus yksinkertaisesti: jos IP-osoite aa.bb.cc.dd niin lisää riville AUTOMAATIO_POSITIO.
- Mietittiin mitä ongelmia voi tulla (”uhkamallinnus, riskianalyysi”)
  - Verkkolaitteiden (kytkin, verkkokortti) toimintahäiriö. Tämä osoittautui yleisimmäksi ongelmaksi.
  - Luvaton diagostiikkayhteys.
  - Luvaton yhteysyritys.
  - Luvaton tietoliikennelaitteen asetusmuutos.
  - Luvallinen tietoliikennelaitteen asetusmuutos, joka aiheuttaa häiriöitä.
- Miten lokitieto voi auttaa näihin ongelmiin.
  - Lokitiedon haulla päästään kiinni häiriöihin, jotka johtuvat tietoteknisen laitteiston aiheuttamista ongelmista.
- Mietittiin myös tukijärjestelmiä ja -palveluita, koska ne edellyttävät sekä rahallista että työajallista investointia.
  - Esitettyjen ongelmien ratkaisuun ei tarvita kaupallisia toteutuksia. ELK-kehys tai Graylog+LogStash pystyvät ratkaisemaan tarpeen. Rahaa ei tarvita, mutta aikaa tarvitaan järjestelmän konfigurointiin. Tässä tapauksessa toteutukseen kului noin 4 työpäivää, josta suurin osa uusien työkalujen opettelua, sekä rikastuksen järkevää toteuttamista.
- Kirjattiin mitä piti muuttaa
  - IP ja POSITIO vastaavuus.
  - Tarpeellisten lokitietojen päällekytkentä lokilähteillä.
- Muutettiin keruuta
  - Ratkaisevat tiedonjyväset löytyivät verkkolaitteiden ja erään automaatioon liittyvän osajärjestelmän paikallisista lokitiedoista. Tarvittiin vain ratkaisu, jolla lokitiedosta voidaan tehokkaasti hakea sekä lokitietoa voidaan rikastaa. Toteutettiin LogStash-

ohjelmalla, joka ratkaisi myös lokien uudelleenlähetysongelman.
    - Samalla päätettiin luoda automaation operointijärjestelmään hälytys, jolla operaattorille voidaan kertoa tietotekniseen infrastruktuuriin liittyvästä häiriöstä. Tämän tavoitteena on helpottaa häiriönhallintaa ohjaamalla huomio oikeaan osaamistarpeeseen (tietoverkkolaitteiden tuntemus). Toteutus edellytti uutta automaatiosovellusta, joka kykenee välittämään hälytystiedon automaatiojärjestelmän normaaliin hälytysvirtaan.
- Automaatio keräsi jo valmiiksi paljon lokia.
    - Tapauksessa osoittautui, että lähes kaikki tarpeellinen lokitieto kerättiin jo valmiiksi automaatiojärjestelmän toimesta. Puuttuva toiminnallisuus liittyi vain kykyyn hakea lokitiedosta, sekä tiedon rikastamiseen automaation suunnittelutiedolla.
- Mihin lokit kannatti kerätä
    - Tässä tapauksessa yksi keskitetty lokijärjestelmä oli toteutettavissa, koska ympäristö oli rajallinen. Toteutuksessa haku on helppoa, mutta samalla jouduttiin toteuttamaan lokien uudelleenohjausta koska verkkolaitteet eivät kyenneet toimittamaan lokitietoaan useaan lokitallentimeen → vaati myös alkuperäisten aikaleimojen säilyttämisen (editoimalla uudelleenlähetysten aikaleimoja).
- Miten kerätty tieto saatiin hyödynnettäväksi (80% tehdystä työstä liittyi tähän)
    - Lokitieto oli siirrettävissä.
    - Lokien katseluun saatiin yksi käyttäjärajapinta.
    - Merkittävin työ tehtiin tiedon siirrossa ja rikastamisessa, jotta lokitiedosta hakeminen, tulkinta ja havainnoista keskustelu helpottui.
- Auditointiperiaatteen huomiointi: ”Jos asiaa ei ole dokumentoitu niin sitä ei ole olemassa”.
    - Tässä tapauksessa ymmärrettiin vasta jälkikäteen tehdä riittävä dokumentaatio toiminnallisuuden uudelleenrakentamiseksi. Uudelleenrakentamista tarvittiin, koska alkuperäinen lokienhallintaratkaisu ei tukenut riittävää käyttäjähallintaa.
    - Lisäksi havaittiin, ettei erästä tärkeää lokitietolähdettä ollut dokumentoitu mitenkään, koska se oli vain paikallisesti tallennettu tekstitiedosto. Lähde selvisi vahingossa keskusteltaessa automaatiotoimittajan kanssa käyttötapauksesta.
- Realismin huomiointi: ”Jos asia on dokumentoitu niin sitä ei välttämättä ole olemassa”
    - Tässä tapauksessa kävi ilmi, että runkoverkon laitteiden oletusasetusten mukaiset lokitiedot eivät olleet oletusasetusten dokumentaation mukaisia.
- Käytettiin muistilistoja suunnittelutyökaluina ja dokumentointipohjina.
    - Yliopistojen tietoturvatyövaliokunnan ”Lokeista hyötyä”-projektin tuottamat muistilistat olivat erittäin hyödyllisiä, katso Liite A ja [YO-SECTV].
- Tehtiin monistettava ratkaisu
    - Monistettavuus huomioitiin dokumentoimalla projektin tärkeimmät epäonnistumiset, onnistumiset, sekä tehdyt valinnat perusteluineen.
- Ympäristössä toteutettiin sekä kehittämisen aikana osallistuttiin kyberharjoituksiin, joiden kautta opittiin
    - jos et tunne omaa ympäristöäsi
    - jos et tiedä riippuvuuksia,
    - jos et osaa automatisoida ja
    - jos et varaudu hyvissä ajoin

  niin ympäristön puolustaminen tietoteknisestä infrastruktuurista johtuvia häiriötilanteita vastaan on erittäin vaikeaa.
- Lopputuloksena saavutettiin toimivan lokienkeruun lisäksi ymmärrys, että lokienhallinta on tärkeä osa häiriötilanteisiin varautumista.

3.4 SOC-palvelun käyttöönottoon valmistautuminen

SOC-palveluista puhutaan nykyään paljon myös energia-alan yritysten kybersuojaamisen käytännön toteutuksen yhteydessä. Tässä yhteydessä SOC eli *Security Operations Center* tarkoittaa yrityksen kyberturvallisuustilanteen seurantaan keskittynyttä toimintoa joka hankitaan ulkoiselta palveluntarjoajalta, jolla on riittävät resurssit, työkalut ja osaaminen kyseiseen toimintaan. Tässä kohdassa käsittelemme lyhyesti SOC-palveluiden käyttöönottoon valmistautumista energia-alan yrityksissä.

SOC-palvelu voi olla käytännössä toteutettu kyberturvallisuusvalvomona, johon suurin osa palveluun liittyvästä avaintoiminnasta on keskitetty.

Esimerkiksi:

- Kansainvälisen uhkatiedon kerääminen ja analysointi
- Asiakkaalta kerätyn datan (esim. lokit, virushälytykset, verkkoliikennetapahtumat) ja sen aiheuttamien hälytysten analysointi ja tutkinta
- Löydösten välitön raportointi asiakkaalle
- Säännöllinen (mm. tilastollinen) raportointi asiakkaalle
- Tietoturvapoikkeamien hallinta. Esim. välitön reagointi ja tuki tietoturvauhkien ja häiriöiden vaikutusten minimoimiseksi ja syiden selvittämiseksi.

Käytännössä SOC-palvelussa työskentelevät asiantuntijat ja tukihenkilöt voivat tietenkin tehdä työtä etänä eri paikkakunnilta, samaa tai eri asiakaskuntaa palvellen. Osalla palveluntarjoajista SOC-palvelun yhteyteen tarjotaan esimerkiksi kyberhäiriötilanteen hallintaa (*Incident Response*) ja turvallisen tilanteen palauttamista (*Incident Recovery*), jotta asiakkaan kyberturvatilanne saataisiin hätätilanteissa nopeasti selvitettyä ja palautettua normaaliksi. Nämä voivat olla energiayrityksille tärkeitä, varsinkin jos automaatio- ja IT-palvelut on muutenkin jo ulkoistettu ja niiden tuki ja vastuut jakautuneet usealle taholle ja yhteistoiminta häiriötilanteessa ei ehkä toimi hyvin. Tärkeintä on varmistaa, että esim. palautustilanteessa ei kuitenkaan tehdä tuotantoa häiritseviä toimenpiteitä ilman asiakkaan lupaa.

3.4.1 Ennen hankintapäätöstä selvitettäviä asioita

Energiayrityksen kannattaa pohtia ja selvittää ainakin seuraavia asioita ennen lopullista SOC-palvelun hankintapäätöstä:

- Millaisia uhkia SOC-palvelun tulisi pystyä tunnistamaan?
  - SOC-palvelun integrointi lokitiedon keräykseen ja muihin asiakkaan monitorointijärjestelmiin?
- Kenellä SOC toimittajalla on parhaat työkalut ja osaaminen energiayritystä koskevien uhkien tunnistamiseksi?
  - Parhaat työkalut, osaamiset ja verkostot ovat onnistumisen edellytys!
- Mitkä järjestelmät ovat kriittisimpiä?
  - Mitä järjestelmiä ja verkkoja tulisi seurata?
  - Seurannan ja tuen saatavuus, esim. 24x7?
- Miten hyvin SOC-palveluntarjoaja ymmärtää asiakkaan ympäristöä?
  - Palvelukoe (POC) jossa testataan tunnistaako SOC-palveluntarjoaja asiakkaan verkkoon lisättyä (haitallista) testitoimintaa?
  - Huom! Usein tarvitaan ”opetteluvaihe”, jonka kuluessa palveluntarjoaja oppii esim. tunnistamaan väärät hälytykset ja ymmärtämään eri tyyppisten häiriöiden seuraukset tuotannon jatkuvuudelle.
  - Tapahtumahorisontti (historiatieto) ja *baseline* -kehitys ja tehokas hyödyntäminen?
  - Tarkemman ja nopeamman reagoinnin mahdollistaminen.
- Mitä muuta informaatiota SOC-palvelulle täytyisi välittää, jotta uhkien tunnistaminen toimisi luotettavasti (ilman vääriä positiivisia hälytyksiä). Esim.:
  - Mitä tietoja tuotanto-omaisuudesta? Esim. haavoittuvuudet?
  - Millaisia kulunvalvonnan tietoja?
  - Sallitut etäyhteydet?
  - Voimassa olevat muutostyöluvat järjestelmiin?
- Miten hyvin viestintä SOC-palvelun kanssa toimii käytännössä?
- Miten hyvin SOC-palvelun tarjoama tuki sopii energiayrityksen tarpeisiin käytännössä?

Lisäksi hankintavaiheessa tietysti huomioidaan SOC-palveluun liittyvät kustannukset ja mahdolliset riskit. Kasvavia riskejä voi syntyä esimerkiksi silloin, mikäli luottamuksellista tiedonvaihtoa syvennetään siten, että kriittisistä haavoittuvuuksista ja riskeistä tiedotetaan automaattisesti myös SOC-palveluntarjoajaa. Tällöinhän palveluntarjoajaan saatetaan luottaa yhtä paljon, ellei jopa enemmän, kuin pääosaan omaa henkilöstöä. Riskinähän voi olla, että palveluntarjoajan liiketoiminta (tai data) myydään esimerkiksi ulkomaille.

3.4.2 HAVARO tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä

Yksi tapa parantaa kyberhavainnointikykyä on ottaa käyttöön tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä HAVARO, joka on Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen erityisesti huoltovarmuuskriittisille yrityksille ja valtionhallinnolle tarjoama palvelu. HAVAROssa eri lähteistä saataviin tietoturvauhkia koskeviin tunnisteisiin pohjautuen organisaation verkkoliikenteestä havainnoidaan haitalliseksi tunnistettua tai normaalista poikkeavaa liikennettä. Kyberturvallisuuskeskus vastaanottaa tiedot poikkeamista ja analysoi ne. Jos kyseessä on tietoturvauhka, siitä varoitetaan organisaatiota. HAVAROsta saatavan tiedon perusteella voidaan myös varoittaa muita toimijoita havaitusta uhasta. Siten järjestelmä auttaa yksittäisten organisaatioiden lisäksi muodostamaan kokonaiskuvaa suomalaisiin tietoverkkoihin kohdistuvista tietoturvauhkista. Järjestelmä havaitsee haittaohjelmia ja hyökkäyksiä, joita kaupalliset tietoturvaohjelmat eivät tunnista. Tämä perustuu siihen, että Kyberturvallisuuskeskus saa tunnistetietoja viranomaisyhteistyön kautta. Kansallisena tietoturvaviranomaisena Kyberturvallisuuskeskuksella on ainutlaatuinen näkymä suomalaisen yhteiskunnan tietoturvaympäristöön ja kansainvälisen viranomaisyhteistyön kautta Kyberturvallisuuskeskus saa tietoa myös globaaleista tietoturvauhista. [HB], [HC], [HD].

Suomalaisille asiakkaille tarjotaan spesifistä tietoturvatietoutta ja ne pääsevät hyödyntämään HAVARO-yhteisön tuottamaa tietoa ja palveluita. HAVARO ei ole tarkoitettu organisaation ainoaksi tietoturvaratkaisuksi, vaan se on suunniteltu täydentämään tietoturvaan panostavan organisaation muita tietoturvaratkaisuja. HAVARO on siis osa yrityksen tietoturvan kokonaisratkaisua. HAVAROn käyttöönotto on vapaaehtoista ja siihen liittyminen tapahtuu käytännössä niin, että ensin asiakasyrityksen julkisen (Internet) verkon liittymään lisätään tietoliikennettä seuraava laite eli sensori. Sensori haistelee sekä yritykseen sisään tulevaa, että ulos lähtevää haitalliseksi tunnistettua tai normaalista poikkeavaa liikennettä sen tyypin, määrän ja ajankohdan suhteen.

3.4.2.1 HAVARO2

Parhaillaan käynnissä olevassa uudistuksessa nykyinen HAVARO-järjestelmä korvataan uudella palvelumallilla, jossa viranomaispalvelusta siirrytään kaupallisten toimijoiden ja Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen yhdessä tuottamaan palveluun. Uudistetun palvelun käyttöön on tarkoitus siirtyä vuonna 2020. Uudessa palvelussa tietoturvan palvelukeskukset (SOC) hoitavat osan tapahtumien käsittelystä ja raportoinnista. Samalla palvelussa siirrytään markkinaehtoiseen rahoitukseen. Palvelussa tulee olemaan kansainvälisestikin ainutlaatuinen konsepti: viranomaiset sekä kaupalliset tietoturvayritykset ja heidän asiakkaansa muodostavat palveluekosysteemin eli verkoston, jonka avulla edistetään kansallista tietoturvan havainnointikykyä ja kokonaistilannetta. Tuotantomalli uudistetaan niin, että palvelukokonaisuus muodostuu Kyberturvallisuuskeskuksen ja tietoturvayritysten tarjoamista maksullisista palveluista. [HA]

Palvelun keskeiset ominaisuudet säilyvät, vaikka uudistus vaatii myös teknisiä muutoksia. Kyberturvallisuuskeskuksen tietoturva-ammattilaiset tekevät kehitystyötä yhteistyössä useiden kaupallisten tietoturvapalveluja tarjoavien yritysten kanssa. HAVARO2-palvelun voi tulevaisuudessa hankkia kaupallisesta tietoturvan palvelukeskuksesta (SOC), joka on mukana HAVARO2-palvelutuotannossa. Suurten yritysten tapauksessa yritys voi itse huolehtia omasta SOC-toiminnostaan. Palvelun tuottamisen perustana on kansallisen kyberturvallisuuden tilannekuvan ylläpitäminen ja huoltovarmuuden varmistaminen. Palvelu suunnataan ensisijaisesti huoltovarmuuskriittisille yrityksille ja organisaatioille. Palvelua voidaan kuitenkin tarjota muillekin tietyt ehdot täyttäville organisaatioille.

3.5 Ansoitusmenetelmien hyödyntäminen

Olemme tämän luvun aiemmissa alakohdissa keskittyneet kyberturvallisuuden ja jatkuvuuden parantamiseen melko perinteisin menettelyin. Järjestelmällinen omaisuuden hallinta on kaiken perusta ja kyberturvallisuuden hallinnassa määritellään kyberturvallisen toiminnan yrityskohtainen malli. Lokikirjauksilla, monitoroinnilla ja SOC-palveluilla pyritäänkin sitten jo tunnistamaan kyberturvallisuuden loukkauksia, sillä suojausmenettelyt ovat hyökkääjien ohitettavissa, mikäli heillä on

riittävästi resursseja. Aiemmin kuvatut havainnointimenettelyt ovat olleet varsin perinteisiä siinä mielessä, että niissä hyökkääjien toimintatapoja ei ole pyritty selvittämään mitenkään erityisin menettelyin. Hyökkääjien toimintatapojen selvittäminen helpottaisi uusien hyökkäyksien torjuntaa merkittävästi ja juuri tätä voidaan parantaa ansoitustekniikoiden avulla, joista kerromme tässä alakohdassa lisää.

Suomen uuden tiedustelulainsäädännön tultua voimaan keväällä 2019 Suojelupoliisin (Supo) resurssit ja työvälineet tulevat parantumaan merkittävästi. Suojelupoliisi raportoi kuitenkin jo viime vuonna useista kybervakoilutapauksista, joiden taustalla arvioidaan olleen valtiollinen taho. Lisäksi havaittu vakoilu on kohdistunut myös yrityksiin ja yksityishenkilöihin, joten jatkossakaan valtion resurssit eivät kuitenkaan riittäne kaiken elinkeinoelämään kohdistuvan vakoilumassan tunnistamiseen ja torjuntaan.

Supon Juhlavuosikirja 2018 [SUPO] korostaa kyberturvallisuustietoisuuden merkitystä laajemminkin:

> *"Kybervakoilu ei välttämättä enää kohdistu suoraan kiinnostuksen kohteena olevaan organisaatioon, vaan sen sijaan kohdetta lähellä oleviin organisaatioihin ja henkilöihin, jotka eivät ole yhtä tietoisia tietoturvan merkityksestä. Kohdeorganisaatiota lähellä olevia tahoja voidaan hyödyntää joko suoraan tiedon hankinnassa tai väylänä varsinaisen kohteen järjestelmiin."*

Meidän tulisi siis tunnistaa kaikenlaiset vakoilun esiasteet ja erilaiset tietovuodot mahdollisimman varhaisessa vaiheessa, jotta kyberturvallisuusuhat eivät rantautuisi energia-alan yrityksiin myöskään alihankinta- tai muiden kumppanien ja verkostojen luottamuksellisiin yhteistyösuhteisiin piiloutuneina. Elinkeinoelämän yleisen uhkatietoisuuden parantaminen korostuneekin edelleen viranomaisyhteistyössä, joka Suomessa onkin huippuluokkaa.

Ongelma piilee siinä, että hyökkääjät pyrkivät huijaamaan meitä ja käyttävät erilaisia varsin kehittyneitäkin tekniikoita, joilla he voivat etukäteen tutkia toimintaamme ja esimerkiksi selvittää yrityksemme käyttämät sisäiset ja ulkoiset kumppanit ja järjestelmät avointen lähteiden tiedustelulla (OSINT – *Open Source Intelligence*). Esimerkiksi sosiaalinen media on hyökkääjien aarreaitta, sillä sitä kautta voi usein helposti selvittää yrityksen työntekijöiden henkilötietoja, perheenjäseniä, tyypillistä käyttäytymistä, verkostoja, jne. Hyökkääjien strategiana on siis tuntea meidän heikkoutemme mahdollisimman hyvin etukäteen, jolloin he voivat valita hyökkäysvektoreiksi luottamuksemme jo ansainneet, mutta samalla ehkä kaikkein haavoittuvimmat kohteet, kuten tutut alihankkijat, harrastuspiirit, lounasravintolat, jne. Kun asiallinen sähköpostiviesti näyttää tulevan tutulta henkilöltä ja avaamme tällaisen viestin, niin silloin meidän yritys-PC kaapataan huomaamatta hyökkääjän etäkäyttöön. Tästä hyökkääjien on helppo siirtyä huomaamatta yrityksen sisäverkon muihin järjestelmiin, joista he ovat varsinaisesti kiinnostuneita. Myös energiayritysten voimaloiden ja sähkönjakelun tietojärjestelmät ja dataverkot ovat nykyään hyökkäyskohteina.

Valitettavasti myös julkiset kilpailutukset ovat nykyään kyberhyökkääjien aarreaittoja, sillä niihin perehtymällä kuka tahansa voi saada selville tarkkojakin tietoja esim. voimalaitoksissa tai sähköverkoissa käytetyistä automaatiojärjestelmistä (mikäli esim. tarjousasiakirjat tai niiden liitteet sisältävät nämä tiedot).

3.5.1 Ansoitustekniikoiden ominaisuuksia ja etuja

Hyökkääjien jo käyttöönottamien varsin kehittyneiden vakoilu- ja kyberhyökkäysmenetelmien johdosta myös meidän kannattaisi ehkä suhtautua hieman ennakkoluulottomammin uudenlaisiin kyberhavaintokyvyn kehittämisen teknologioihin. Eräs varsin potentiaalinen alue on *deception technologies* eli petokseen, huijaukseen ja ansoitukseen liittyvät, varsin helposti automatisoitavat teknologiat. Näitä teknologioita laillisella tavalla hyödyntämällä voisimme mahdollisesti tunnistaa yrityksiimme kohdistuvat tietovuodot ja vakoiluyritykset paljon tehokkaammin kuin aikaisemmin. Suosittelemme alueen teknologiataustaan ja lailliseen hyödyntämiseen perehtymistä, katso aluksi esim. [DECEIT] (Teemu Väisänen) ja [DECEPTION].

Huijaamiseen ja petokseen käytettävät teknologiat ovat perinteisesti olleet rikollisten käytössä. Miksi meidän, jotka haluamme kunnioittaa voimassa olevia lakeja ja asetuksia, sekä erityisesti puolustaa kriittistä infrastruktuuriamme, kannattaisi hyödyntää näitä epäilyttäviä, usein salassa käytettäviä ansoitusteknologioita?

- Me emme nykyisin pysty havaitsemaan meihin kohdistuvaa vakoilua ja tietovuotoja riittävän tehokkaasti. Tavallisesti joku ulkopuolinen, kuten poliisi, informoi meitä itseämme koskettavasta kyberturvaloukkauksesta ja silloin voi olla jo liian myöhäistä.
- Erilaisia kyberuhkia on olemassa liian paljon, jotta voisimme tunnistaa ne erikseen perinteisin menettelyin, kuten antivirusohjelmistoin (jotka voivat tahattomasti aiheuttaa esim. katkoja automaatiojärjestelmään).
- Kohdistetut kyberhyökkäykset voivat kestää pitkään, mikä on erittäin suuri ongelma niiden aiheuttamien suurten riskien takia. Siksi meidän tulisi pystyä tunnistamaan ne jo aiemmin.
- Puolustajan täytyy suojata kaikki järjestelmät (vaikeaa), mutta silti hyökkääjälle riittää löytää vain yksi aukko puolustuksesta (helppoa). Tämä asetelma tulisi kääntää toisin päin ja juuri ansoitustekniikat ovat erityisen hyvin soveltuvia hyökkääjän tunnistamiseen tietyssä kohteessa.
- Kalliit IDS/IPS ja SIEM järjestelmät saattavat helposti generoida liikaa hälytyksiä jotka jonkun tulisi analysoida tarkemmin. Analysointiin tarvittavat osaajaresurssit ovat kuitenkin varsin kalliita ja osaajia on vähän saatavilla.
- Suojattavat verkot ja ohjausjärjestelmät saattavat olla liian monimutkaisia ja toiminnaltaan dynaamisia (tilanteen mukaan muuttuvia) edes puolustajan ymmärtää riittävällä tasolla epäilyttävän toiminnan tunnistamiseksi.

Ansoittaminen (järjestelmien puolustamiseksi):

- Ansana voidaan käyttää mitä tahansa resurssia, jota ei normaalisti käytetä: Jos joku yrittää käyttää kyseistä resurssia, generoidaan hälytys. (Toki lokitapahtumia ja hälytyksiä tulee generoitua myös tuotantokäytössä olevista järjestelmistä, mutta tällöin vääriä hälytyksiä syntyy tyypillisesti paljon enemmän.)
- Ansoja voidaan hyödyntää hyökkääjän etenemisen seuraamisessa ja hyökkäystekniikoiden tutkinnassa: Mitä, missä, miten ja milloin näitä resursseja käytettiin? Mistä hyökkäys tuli ja mihin se yritti mennä seuraavaksi?
- Ansoilla voidaan myös harhauttaa hyökkääjää monin eri tavoin, esimerkiksi paljastamaan hyökkääjästä joitain ominaisuuksia kuten teknisiä kyvykkyyksiä tai jopa motiiveja.

Harhauttaminen (järjestelmien puolustamiseksi):

- Harhauttamisessa hyökkääjän toimintaan voidaan yrittää vaikuttaa esimerkiksi johdattelemalla hyökkääjää haluttuun suuntaan, asettamalla tarjolle harhaanjohtavaa lisätietoa, tai muutoin hyökkääjän päätöksentekoon vaikuttamalla:
  - Harhautustekniikoilla voidaan houkutella hyökkääjä ansoihin, esimerkiksi vuotamalla tietoa ”kriittisistä kohteista”.
  - Harhautukseen käytetyt resurssit voivat olla lisäksi ansoja, joiden käyttöä monitoroidaan.
  - Harhauttamalla suojataan omia järjestelmiä ja kriittistä tietoa hidastamalla hyökkäystä. Harhauttaminen on myös sotilaallisen johtamissodankäynnin osatekijä.

Energiayrityksillä näyttäisi olevan edessään paljon työtä varsinkin vakoilun ja kehittyneiden hyökkäysten havaitsemiseen ja torjuntaan liittyen. Mistä yrityksen eri liiketoiminnot voisivat esimerkiksi tarkistaa, että ovatko he itse tai heidän kumppaninsa tietyllä ajan hetkellä aktiivisten vakoiluyritysten kohteina vaiko eivät? Kybervakoilua ja sen yrityksiähän esiintyy Suomessa jatkuvasti. Kuka meidän työntekijöitämme vakoilee ja millaisia tekniikoita tai strategioita hyökkääjät tulisivat mahdollisesti käyttämään jatkossa? Kenen hyväksi hyökkääjät toimisivat ja millaisiin päämääriin he vakoilullaan ja hyökkäyksillään pyrkisivät? Kybervakoilun kenttä on kuitenkin luultavasti niin haastava, että kaikkiin kysymyksiin ei varmaankaan koskaan saada tyhjentäviä vastauksia, olivatpa yritysten ja viranomaisten käyttämät tunnistusteknologiat miten hyviä tahansa. Kansainvälisen valtiollisen vakoilun resurssit ovat varmastikin erittäin mittavat ja mikäli ne suuntautuvat entistä kohdistetummin myös Suomeen, niin tällöin meidän tulee käyttää rajallisia resurssejamme koordinoidusti ja parhaita teknologioita hyödyntäen.

Ansoitus- ja harhautustekniikoilla on monenlaisia etuja, jotka tekevät niistä erityisen kiinnostavia myös puolustajan näkökulmasta, esimerkiksi:

- **Sisäpiiriuhat**: Tehokas sisäpiiriuhkien paljastaminen. Minimoidaan väärät hälytykset

(*false-positives*) asentamalla ansoja aliverkkoihin tai resursseihin, joihin kenellekään ei normaalisti anneta pääsyoikeutta.

- **Pitkäkestoisuus**: Kohdistettuun hyökkäykseen liittyvä ulkoinen ja sisäinen tiedonhankinta saattaa edetä varsin hitaasti ja hiljaisesti, silti hyökkääjien lankeaminen jo yhteenkin sisäiseen ansaan voi paljastaa varsin tehokkaasti heidän läsnäolonsa sisäverkossa.
- **Räätälöitävyys**: Hyökkääjät käyttävät kampanjoissaan tiettyjä levittäytymistekniikoita, joiden tunnetuille etenemispoluille voidaan asettaa erilaisia ansoja.
- **Johdattelu**: Puolustaja voi houkutella hyökkääjän toimimaan haluamallaan tavalla, kuten etsimään salaiseksi luokiteltua tietoa ja tätä tehdessään paljastamaan läsnäolonsa.
- **Harhautus**: Harhautuksen avulla puolustaja voi hidastaa hyökkäystä ja vaikeuttaa oikeiden resurssien löytämistä. Hyökkääjä voi esimerkiksi luulla olevansa oikeassa (tai väärässä) kohteessa.
- **Pelote:** Hyökkäyksiä voitaneen joissain tapauksissa myös estää pelotteella, jolloin hyökkääjä ei halua edetä sisäverkkoon siellä olevien ansojen takia.

3.5.2 Soveltamisessa huomioitavia asioita

Ansoitustekniikoiden käyttöönottoa hidastaa kuitenkin se tosiseikka, että myös vastapuoli oletettavasti tuntee kyseiset tekniikat ja työkalut varsin hyvin. Vakoilija saattaa olla esimerkiksi itsekin käyttänyt tai ainakin testannut erilaisia ansoitustyökaluja ja opetellut nopeasti tunnistamaan käyttääkö hyökkäyskohde tietynlaisia ansoja. Hyökkääjä esimerkiksi ensin hyvin varovasti tiedustelee hyökkäyskohdetta ja pyrkii ennalta tunnistamaan (*fingerprinting*) kaikki sellaiset ansat joita puolustajat saattavat käyttää ja täten yrittävät välttää niihin lankeamisen. Esimerkiksi avoimena lähdekoodina ladattavan hunajapurkin (*honeypot*) oletusasetukset kuten laitenimet, sarjanumerot, metadata, käytetyt sovellusportit, sertifikaatit, tai palomuurisäännöt voivat nopeasti paljastaa hyökkääjälle, että kohde onkin hyvin tunnettu *honeypot*. Jopa tunnetusta Shodan työkalusta (https://www.shodan.io/) löytyy valmiiksi toteutettu ”honeypot or not”-toiminto, jolla voi selvittää onko tietyssä IP-osoitteessa ansoja. Myös esimerkiksi virtualisointiympäristön käyttö saattaa epäilyttää joitain hyökkääjiä, sillä niitä käyttämällä puolustajan on helppoa vaikkapa tallentaa kaikki hyökkääjän ko. kohteessa tekemät toimet sekä kokeilla erilaisia houkuttelevia asetuksia.

Ansoitukseen ja harhautukseen käytettävät työkalut kannattaa siis valita erittäin huolellisesti sekä asetukset määritellä sopivalla tavalla huomaamattomiksi, jotta hyökkääjät eivät osaisi tunnistaa niitä. Kaikkein turvallisinta luultavasti olisi, mikäli puolustaja kykenisi omista tavoitteistaan lähtien kehittämään ja ylläpitämään kaikki ansoituksessa käytettävät ohjelmistonsa. Toki suurikin osa esimerkiksi tarvittavasta kehitystyöstä voidaan silti ulkoistaa. Haittapuolena tässä lähestymistavassa lienee vaadittu työmäärä, varsinkin jos ansoja pitäisi sitten vielä jatkuvasti päivittää ja ylläpitää. Ansan konfigurointi mahdollisimman passiiviseksi ja näkymättömäksi saattaakin olla tietyissä tapauksissa järkevää, jolloin sen ylläpidon tarvekin luultavasti vähenisi.

Ansoista kannattaa siis kehittää mahdollisimman vaikeasti tunnistettavia:

- Kehitä omat uniikit ansat ja suunnittele itse harhautukset
- Älä kopioi hyvin tunnettuja ansoja
- Vaihda oletusasetukset joksikin muuksi
- Katselmoi lähdekoodi, jotta sinne ei jää mitään tunnistettavaa
- Räätälöi valitsemasi kehitysalusta

Asiaa kannattaa ajatella niin päin, että vakoilun tulisi aina tulla kalliimmaksi kuin mitä sen hyödyt olisivat. Mitä toimenpiteitä tämä edellyttäisi meiltä?

Todennäköisesti meidän tulee kehittää kriittisten kohteidemme, kumppaniemme ja tietopääomiemme kyberturvallisuuden seurantaa myös yksittäisen kohteen tasolla. Tämä edellyttää asianmukaisen seurannan huolellista suunnittelua ja toteutusta, sekä mahdollisesti luottamuksellista viranomaisyhteistyötä. Myös ansoitustekniikoita on kuitenkin mahdollista käyttää tähän tarkoitukseen.

Käyttöönoton kannalta ansoitustekniikoissa on se hyvä puoli, että ansoja voidaan tarvittaessa asentaa vain vähän tai vaihtoehtoisesti ainoastaan konfiguroida jo käytössä olevien järjestelmiemme käyttämättömiä osasia ansoiksi (= lokikirjaus). Toisaalta taas laajempien ansoituskokonaisuuksien kehittäminen, testaaminen ja asentaminen voivat olla varsin suuriakin ponnistuksia, joihin tuskin kannattaa lähteä ilman vahvaa ansoitustekniikoiden osaamista & kokemusta. Unohtamatta jo asennettujen ansakenttien ja niiden seurantajärjestelmien riittäviä ylläpitoresursseja.

Luku 4

IOT:N TURVALLINEN HYÖDYNTÄMINEN

Kuva: Shutterstock

4. IOT:N TURVALLINEN HYÖDYNTÄMINEN

Esineiden Internetin eli IoT- (*Internet of Things*) ratkaisujen jatkuva esiinmarssi tulee todennäköisesti vaikuttamaan yhä voimakkaammin ihmisten mieltymyksiin ja kulutuskäyttäytymiseen, sekä näiden seurannan tehostumiseen. Samalla teollisuuden IIoT-ratkaisujen (*Industrial Internet of Things*) käyttöönotto yleistyy voimakkaasti.

Teollisuuden IoT-ratkaisuissa hyödynnetään helposti ja nopeasti asennettavissa olevia yleiskäyttöisiä mittausanturialustoja, joista vaikkapa mobiilioperaattoreiden tarjoamien langattomien IoT-verkkojen ja yhdyskäytävien kautta kerättävä mittausdata yhdistetään erilaisten pilvipalveluiden kehittyneisiin data-analyysityökaluihin. Energiapalveluiden hallintaa tukemaan saadaan tätä kautta vaivattomasti kehittyneitä analyysityökaluja, joilla voidaan esimerkiksi ennakoida ja leikata paikallisia energian kulutushuippuja ja täten optimoida vaikkapa ympäristöystävällisen energian tuotannon määrää kullakin ajanhetkellä.

Valtakunnan sähköverkon tasolla tehotasapainoa ylläpidetään taajuusohjatuilla reserveillä sekä manuaalisilla säädöillä. Käytössä on sekä energiayrityskohtaista, että Fingridin hallinnoimaa automaatiota ja manuaaliohjauksia, joilla tuotannon ja kulutuksen välisiä vaihteluja tasataan sähköverkkojen eri tasoilla. Mikäli yllättävä energian kulutuksen (paikallinen) kasvu tai lasku olisi riittävän voimakas, se voisi aiheuttaa ongelmia koko Suomen hetkellisen tehotasapainon hallintaan. Mikäli tulevaisuudessa satojen tuhansien kotitalouksien hyödyntämiä ja kiinteistön energiankulutusta säätäviä IoT-laitteita saataisiin dataverkon kautta laajamittaisesti hyökkääjän haltuun, voitaisiin niiden kautta toteuttaa vakavia kyberhyökkäyksiä erilaisia datapalveluja vastaan (hajautetut palvelunestohyökkäykset) sekä erityisesti itse energiapalvelujen tarjoajia vastaan. Jos energiakuormiakin voidaan ohjata, niin kyseisten palvelujen energiakulutuksen aggressiivinen yhtäaikainen nosto tai vapauttaminen saattaisi aiheuttaa sähköverkkoon dominoefektin, joka aiheuttaisi valtakunnallisen häiriön sähköverkkoon. Tilanteesta palautuminen voisi muodostua työlääksi, mikäli häiriöiden aiheuttajaa ei saataisi nopeasti poistettua.

IoT:n tuomien suurempien tai pienempien hyötyjen negatiivisena vastakohtana saattaa siis olla kokonaisturvallisuuden hallinnan monimutkaistuminen. Väitämme, että edellä mainittujen kuluttajien ja teollisuuden IoT-ratkaisujen yleistyminen saattaa pitkällä tähtäimellä lisätä sähköntuotantoon ja jakeluun kohdistuvia kyberhäiriöitä. Ongelmia voi tulla esimerkiksi yhä lisääntyvistä riippuvuussuhteista eri järjestelmien välillä ja tätä kautta kokonaisjärjestelmän monimutkaistumisesta ja häiriötilanteissa oikean toimintatavan löytämisen vaikeutumisesta.

Hyökkääjän näkökulmasta myös hyökkäyksissä tarvittavan tiedon hankinta helpottuu, kohteiden hyökkäysrajapinta kasvaa ja toisaalta IoT:n hyödyntäjän kannalta ratkaisujen ”liikkuvat tekijät” ja taustaratkaisujen ”kehityskumppanit” saattavat lisääntyä räjähdysmäisesti vaikeuttaen puolustamista.

IoT ratkaisujen turvallinen käyttöönotto on siis erittäin tärkeää. Valitettavasti energia-alan yrityksille kuitenkin tarjotaan edelleen myös varsin kehittymättömiä IoT-ratkaisuja, joiden:

- Kyberturvallisuusratkaisuja ja -menettelyjä ei ole dokumentoitu
- Toteutuksessa käytettyjä alustoja ja sovelluksia ei ole testattu
- Palvelun toteutuksessa käytettyjä kumppaneita ei ole yksilöity
- Käyttöönottoa ei ole ohjeistettu ja tuettu riittävästi
- Tuettu elinkaaren kesto ja ylläpitopalvelut ovat epäselviä
- Kenttälaitteissa ei ole ominaisuuksia etänä tapahtuvaan päivittämiseen
- Tuen yhteydenottopiste voi sijaita missä tahansa
- Palvelutason kuvaus on jätetty liian avoimeksi

Myös IoT-ratkaisuissa kyberturvallisuuden huomiointi on siis erittäin tärkeää. Ratkaisussa käytetyt elementit kuten anturit, kehitysalustat, viestintäverkot, pilvipalvelut, ohjelmistot ja sovellukset tulee suunnitella alusta alkaen kyberturvallisesti (*secure-by-design*). Suunnittelun turvallisuuden arviointi jälkikäteen on yleensä varsin vaikeaa, mutta joskus esim. yrityksen tai tuotteen kyberturvallisuussertifikaatit tai jopa testiraportit voivat auttaa tunnistamaan vastuulliset, hyvin varautuneet toimijat vähemmän kypsemmistä toimijoista.

Energiayrityksen suunnitellessa IoT:n hyödyntämistä sen tulee ottaa huomioon paljon erilaisia näkökulmia. Kullekin yritykselle parhaiten soveltuvat IoT:n käyttötapaukset ja niiden pilotointi ja käyttöönoton priorisointi kannattaa pohtia monesta näkökulmasta. Mahdolliset uudet liityntärajapinnat ja vaikutukset muihin järjestelmiin tulee dokumentoida hyvin. Hankintavaatimuksissa ja sopimuksissa tulee ottaa IoT-ratkaisujen kyberturvallisuus huomioon. Ennen laajempaa käyttöönottoa IoT-ratkaisuja kannattaa koestaa erilaisissa pilottiympäristöissä, jolloin niiden vahvuudet ja heikkoudet paljastuvat. IoT-ratkaisun tietoturvallisuus tulee varmistaa viimeistään silloin, kun pilotoinnista ollaan siirtymässä aitoon tuotantokäyttöön.

Lisäksi saattaa olla järkevää hyödyntää kyberturvallisuuden tilaa seuraavia lisäpalveluja myös IoT-palvelun kautta toteutettujen kyberhyökkäysten ja niiden leviämisen tunnistamiseen. Tällöin asiakkaan IoT-ratkaisun elementeistä tulee tietenkin pystyä luotettavasti keräämään esimerkiksi lokitietoa keskitettyä analyysia varten, jolloin palvelun tietoturvallisuusasiantuntijat voivat verrata asiakkaan järjestelmien nykytilaa jo aiemmin tunnistettuihin IoT:n kyberuhkiin. Mikäli merkkejä kyberhyökkäyksestä ilmenee, palveluntarjoaja antaa siitä varoituksen palvelun tilanneelle energiayhtiölle. Tällaisessa tilanteessa olisi suotavaa, että energiayritys antaisi myös Kyberturvallisuuskeskukselle valtuudet ilmoittaa kyseisestä uhkasta myös muille energia-alan yrityksille, jolloin kyberturvallisuuden tilannetietoisuus paranisi laajemminkin energia-alalla.

4.1 IoT:n yleiset uhat ja ohjeet

4.1.1 IoT:n yleisiä tunnistettuja uhkia

Syksyllä 2015 oma arviomme IoT:n lisääntyvään hyödyntämiseen liittyvistä tulevaisuuden riskiskenaarioista eri toimialoilla sisälsi mm. [FIIF]:

- Etäyhteyden kaappaaminen sähköverkon ohjausjärjestelmään
- Hyökkääjän pääsy pumppuaseman ohjausjärjestelmään
- Haittaohjelman pääsy elintarviketuotannon järjestelmään
- Hajautettu palvelunestohyökkäys logistiikkajärjestelmään
- Hakkerikuluttajan murtautuminen kassajärjestelmään
- Valmistusta ohjaavan verkon häirintä etäyllläpitoyhteyden kautta
- Terveystietojen vuotaminen hoitodataa sisältävältä palvelimelta
- Taloautomaation kybervandalismi

IoT-ratkaisuihin liittyvät kyberturvallisuusuhat olivat vuoden 2018 kuluessa huolestuttavan voimakkaassa kasvussa [F-SECURE]. Negatiivinen kehitys on oletettavasti voimistunut IoT-laitteiden, ICT:n ja automaation järjestelmäintegraation lisääntymisen myötä. 2000-luvun ensimmäisellä vuosikymmenellä kuluttajille suunnattuihin Linux-pohjaisiin Internet-reititinlaitteisiin kohdistui lähinnä satunnaisia, oletussalasanoihin liittyviä uhkia, eivätkä haitantekijät kyenneet synnyttämään laajempaa haittaa aiheuttavia häiriöitä.

Yllä mainitun F-Securen raportin mukaan vuonna 2015 hyökkäyksistä alkoi tulla monimutkaisempia ja ne kohdistuivat myös muita teknologia-alustoja kuin Linuxia vastaan. Esimerkiksi *Moose* hyökkäsi telnet-protokollan kautta erilaisia IoT-laitteita vastaan ja asensi niihin SOCKS- ja http- välityspalvelimia, joita hyväksikäyttämällä hyökkääjä pystyi generoimaan esim. valeseuraajia ja -tykkäyksiä lähinnä Instagramissa.

Syksyllä 2016 Githubiin ilmestyi *Gafgyt*-haittakoodin pohjalta edelleen kehittynyt *Mirai*, joka osasi ”yhteisön” tukemana muutamassa kuukaudessa hyväksikäyttää satoja erilaisia salasanoja. Lokakuussa 2016 syntyikin ensimmäinen laaja kaapattujen Internet-reitittimien *botnet* (zombie-laitteiden muodostama ohjelmistorobottien verkosto), jota ohjaamalla hyökkääjä sai aikaan historiallisen suuren hajautetun palvelunestohyökkäyksen lamauttaen suuren osan Yhdysvaltain Itärannikon Internetistä. Suomessa *Mirain* leviäminen saatiin onneksi nopeasti estettyä erityisesti Kyberturvallisuuskeskuksen nopean tiedotuksen ansiosta. [F-SECURE].

Vuonna 2017 mm. *Mirain* koodin pohjalta syntyi paljon uusia haittaohjelmia, jotka hyödynsivät mm. web-kameroiden haavoittuvia HTTP-käyttöliittymiä, louhivat kohteissa virtuaalivaluuttaa, tunkeutuivat Android-laitteisiin debug-rajapinnan kautta, piiloutuivat Tor-ohjelmistojen avulla, sekä osasivat hyödyntää useita erilaisia hyökkäysvektoreita. [F-SECURE].

Euroopan unionin verkko- ja tietoturvavirasto ENISA julkaisi marraskuussa 2017 erinomaisen raportin “Baseline Security Recommendations for

IoT" [ENISA], josta lukija saa käsityksen IoT:hen liittyvistä kyberuhkista ja suosituksista erilaisissa kriittisissä infrastruktuureissa. ENISAn raportti esittelee mm. asiantuntijahaastatteluihin perustuvan listan tärkeimmistä IoT-hyökkäysskenaarioista kriittisyysjärjestyksessä (kirjoittajan käännös englannista huomioiden raportin sisältämät skenaariotarkennukset):

- IoT:n hallintajärjestelmän haltuunotto
- Aktiivilaitteen kalibrointiarvojen tai raja-arvojen ja asetusten muokkaus
- Botnet-verkon muodostaminen ja komentojen syöttäminen laitteeseen
- Hyökkäys aktiivilaitteen ja sen ohjaimen väliseen verkkolinkkiin
- Hyökkäys verkossa siirrettävää tietoa vastaan
- Hyökkäys toimilaitteisiin niiden asetusten manipuloimiseksi
- Protokollahaavoittuvuuksien hyväksikäyttö
- Hyökkäys kohteita vastaan joilla on yhteys varsinaiseen kohteeseen
- Virtalähteen tilatiedon manipulointi

Tällaiset yleisen tason hyökkäysskenaariot lisäävät lähinnä ymmärrystä siitä, minkä tyyppisiä hyökkäyksiä on aiemmin toteutunut muissa organisaatioissa.

Vuoden 2018 aikana myös tiettyyn kybervaikuttamiseen pyrkivät valtiolliset tahot näyttivät kiinnostuneen erityisesti reitittimien hyödyntämisestä, sillä lähes kaikki tärkeimmät reititinvalmistajat joutuivat kehittyneen hyökkäyskampanjan kohteeksi. Ilmestyi mm. *VPNFilter*-haittaohjelmaperhe, josta tunnistettiin samankaltaisuuksia *BlackEnergyn* kanssa. VPNFilter pystyi mm. vakoilemaan tiettyjen SCADA-järjestelmien datakommunikaatiota, tunnistamaan kohteiden salasanoja sekä tuhomaan kohdelaitteiden firmware-ohjelmistoja. [F-SECURE].

Hyökkäävät tahot voisivat siis turvattomien IoT-ratkaisujen kautta mm.:

- Ottaa haltuun IoT-verkkoihin kytkettyjä laitteita ja edetä tietoverkoissa
- Uhata uhreja maineen menetyksellä ja kiristää rahaa (*Bitcoins*)
- Häiritä sopimustoimittajia ja urakoitsijoita manipuloimalla logistiikkatietoja
- Häiritä tuotantojärjestelmien toimintaa ja aiheuttaa tuotannon menetyksiä

4.1.1.1 Millaisia heikkouksia IoT-toimituksiin saattaa liittyä?

Energia-alalla IoT-ratkaisuja on jo alettu ottamaan käyttöön, mutta varsin maltillisesti. Ennen IoT:n tuotantokäyttöä yritysten kannattaa toteuttaa hyvin suunniteltuja IoT-pilotteja ja kohdistaa ne pieniriskisiin kohteisiin, jotta mahdolliset ongelmat eivät pääsisi aiheuttamaan vahinkoja kriittisiin kohteisiin. Kaikkien uusien järjestelmien kyberturvallisuudesta tulee varmistua ennen niiden siirtämistä tuotantokäyttöön, tämän periaatteen tulee koskea myös IoT-ratkaisuja.

Markkinoilla voi esiintyä "IoT-ekosysteemejä", vaikka niiden elinkaarenhallinta olisi vasta konseptivaiheessa. Kyseisten osajärjestelmien toteutukset saattavat olla nopeasti kehitettyjä ja kyberturvallisuustestaus voi olla käytännössä olematonta. Kriittisenkään komponentin (esim. IoT-yhdyskäytävän) kehittäminen ei edellytä valmistajalta kunnollista tietoturvatestausta. Mikäli jokin laite toimii normaaliolosuhteissa suhteellisen luotettavasti, se ei silti heti ole kyberturvallinen tai edes luotettava vähänkään erilaisessa ympäristössä. IoT-järjestelmien kokonaistoimituksiin saattaa oletusarvoisesti kuulua esim. seuraavaa:

- Langattomia antureita, joissa on käytössä jo turvattomiksi osoitettuja tietoturvaominaisuuksia tai *firmware*-koodiin sisällytettyyn salausavaimeen perustuvia langattomia rajapintoja.
- IoT-yhdyskäytäviä tai Internet-verkkoon kytkettäviä ohjauspaneeleita, jotka sisältävät tarpeettoman paljon avoimia tietoliikenneportteja tai joiden kyberturvallisuutta ei ole asiantuntevasti testattu.
- Pilvipalvelujen asiakaskäyttöliittymiä ja teknisiä liityntärajapintoja (API), jotka sisältävät jatkuvasti esim. tietomurrot mahdollistavia haavoittuvuuksia tai heikkoja avaimia.
- Pilvipalveluja, joiden käyttöehtoihin kuuluu asiakkaan tieto-omaisuuden suojaaminen palveluntarjoajan vapaasti määrittämin teknisin menettelyin ja palvelukumppanein. Esim. asiakkaan datan tallennus ja tiedon prosessointiin sovellettava lainsäädäntö voi tulla vaihtelevasti eri maista.
- Sovelluksia, joiden toimintalogiikka ja asetukset voivat muuttua ennakoimattomalla tavalla koska tahansa.

4.1.2 Yleisen tason ohjeita IoT-uhkiin varautumiseksi

Tarpeettomien uhkien välttämiseksi liian pikaiset ja täten riskialttiit IoT-laitteiden tai ekosysteemien käyttöönotot kannattaa kieltää yritystasolla. Energiayrityksen tulisi kehittää IoT:n yleiselle hyödyntämiselle oman liiketoiminnan huomioivat perusvaatimukset ja malliratkaisut pilottiprojektien kautta, jolloin suurimmat ongelmat voidaan ennakoida hallitusti ennen IoT:n laajempaa käyttöönottoa. Vain huolellinen IoT:n kyberturvallisuuteen perehtyminen, kyberturvallisten toimintavaatimusten asettaminen, sekä pitkäjänteinen IoT järjestelmätoimittajien, tuotteiden ja palvelujen evaluointi, pilotointi, sekä käyttöönoton vaiheistaminen ovat turvallisia tapoja käyttöönottaa kustannustehokkaita IoT-ratkaisuja vaativiin tuotantoympäristöihin. IoT-ratkaisujen turvallisuuteen ja häiriöttömään käyttöönottoon ei tule luottaa ilman ratkaisutoimittajien ja ratkaisujen perusteellista etukäteiskoettelua.

Tuotannon ja ylläpidon tulee ymmärtää IoT:n kyberturvallisuusvaatimukset myös käytännön tasolla, eikä se voi siirtää kokonaisvastuutaan asiassa ulkopuolisille toimijoille. Vähitellen lisääntyvä ymmärrys ja toimiva yhteistyö IoT-ratkaisutoimittajien ja palveluntarjoajien kanssa edistää parhaiten tuotannon omistajan johtamaa, kyberturvallista IoT-ratkaisua.

4.1.2.1 Tarkastuslista: Mitä osakokonaisuuksia IoT-järjestelmiltä tulisi vaatia?

Kohderyhmä: Tämä kysymyslista on tarkoitettu energiayritysten liiketoimintajohdon ja kehitystiimien käyttöön niiden harkitessa IoT-järjestelmien hankintaa ja käyttöönottoa. Käytä tarvittaessa asiantuntijan apua, jotta ymmärrät mitä kussakin liiketaloudellisessa tilanteessa ja käyttötapauksessa on realistista käytännössä vaatia ja mitä vaikutuksia kullakin tietoturvavaatimuksella voi olla kokonaisuuden jatkuvuudelle.

Tarkoitus: Tarkoituksena on auttaa päättäjiä hahmottamaan yhdellä silmäyksellä IoT-ratkaisuhankintoihin liittyviä tärkeimpiä vaatimuskokonaisuuksia ja tehtäväalueita. Lista auttaa ymmärtämään kyberturvallisuusalueen laajuutta ja vaativuutta, jolloin erilaisten IoT-toteutusvaihtoehtojen liiketoiminnallista kannattavuutta voidaan arvioida paremmin.

> *Ref:* Baseline Security Recommendations for IoT, in the context of Critical Information Infrastructures, Nov. 2017.
>
> - ENISA Europe[3] -

Tarkastuslista

Tutustu ja ymmärrä [ENISA] raportissa mainitut osakokonaisuudet. Tärkeimpiä IoT-ratkaisuhankintoihin ja -palveluihin vaadittavia osakokonaisuuksia ovat:

- **Sopimukset**: Laadi yksityiskohtainen sopimus kerättävän datan käyttöoikeuksista ja turvallisesta käsittelystä (huomioi myös kolmas osapuoli ja mahdollinen IoT-palveluyrityksen myynti).
- **Omaisuus**: Evaluoi, käyttöönota, käytä ja ylläpidä tietoturvalliset tietojärjestelmien ja konfiguraatiohallinnan ratkaisut. Haavoittuvuuksien ja vikojen korjauspalvelujen tulee olla osa toimivia elinkaarenhallintapalveluja.
- **Luottamus**: Vaadi kullekin IoT-laitteelle koko elinkaaren kestävä luottamusankkuri. Ratkaisun tulee todentaa luotetun latausympäristön (*secure boot*) oikea toiminta ennen digitaalisesti allekirjoitettujen päivitysten ja ohjelmistojen latausta laitteeseen.
- **Toteutus**: Ratkaisun tulee käyttää yleisesti turvallisena pidettyjä tietoliikenneprotokollia sekä standardoitujen kryptoalgoritmien testattuja toteutuksia, jotka voidaan ajan kuluessa korvata taas paremmilla.
- **Testaus**: Pyydä IoT-toimittajaa selittämään, miten he ovat toteuttaneet *secure-by-design* periaatetta tuotekehityksessään ja miten heidän tarjoamansa IoT-järjestelmä on tietoturvatestattu.
- **Käyttö**: Määrittele jokaiselle IoT-laitteelle sallittu käyttötapa ja -ympäristö ja valvo turvallisen käytön toteumaa.
- **Palautuminen**: Vaadi IoT-järjestelmän automaattinen häiriöistä palautuminen (*self-repair/healing*) ja testaa häiriötilanteita, mikäli mahdollista.

[3] https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

- **Yksityisyys**: Arvioi uuden IoT-sovelluksen vaikutus koko järjestelmän yksityisyydensuojaan. IoT-ratkaisun kaikkien toimijoiden tulee toteuttaa EU:n tietosuojadirektiivin (GDPR) maakohtaiset asetukset.

4.2 Skaalautuvien IoT-ratkaisujen arkkitehtuureista

Monet IoT-ratkaisujen toimittajat ovat luonnollisesti pyrkineet siihen, että heidän ratkaisujaan olisi mahdollisimman helppoa ostaa. Tämä voi kuitenkin tarkoittaa käytännössä sitä, että toimitettavan järjestelmän eri komponentit, niiden alkuperä ja toimittaja jäävät ostajalle epäselviksi. Esimerkiksi sovittu mittausdata luvataan toimittaa luotettavasti pilvipalveluun ja järjestää näin syntyviin tietokantoihin asiakkaan tarvitsemat ”analyysipalvelut”. Mutta miten ostaja kykenee arvioimaan esimerkiksi elinkaaren hallinnan vahvuuksia ja heikkouksia kokonaisratkaisun osalta, mikäli hallintaan oleellisesti vaikuttavista komponenteista ja kumppaneista ei ole saatavissa riittävästi tietoa? Miten ratkaisukokonaisuuden kyberturvallisuuden varmistamista ja ylläpitoa kyetään tällöin luotettavasti arvioimaan?

Jotta rakentava keskustelu toimittajien ja asiakkaiden kanssa voitaisiin saada alkuun, tarvitaan riittävästi ymmärrystä skaalautuvien IoT-ratkaisujen toiminnallisista arkkitehtuureista ja IoT-ratkaisuelementtien muodostamista verkostoista. Näistä kerrotaan tarkemmin seuraavissa alakohdissa.

4.2.1 Skaalautuvien IoT-ratkaisujen toiminnallinen arkkitehtuuri

Minkä tyyppisiä kumppaneita ja toiminnallisia kokonaisuuksia hyvin skaalautuvien IoT-ratkaisujen tulisi pitää sisällään? Useimmissa tapauksissa luotettavia toimijoita tarvitaan käytännössä seuraaville tasoille (kaikkia tasoja ei aina tarvita):

- Likiverkossa (PAN - *Personal Area Network*) tapahtuva tiedonkeruu
- IoT-operaattorin toimittama tiedonsiirto laajoilta alueilta
- IoT-alustatoimittaja
- Asiakkaan omat ICT-verkot ja järjestelmät
- Loppukäyttäjät laitteineen ja sovelluksineen

Teollisuuskohteissa IoT-sovellukseen liittyvä edullinen tiedonkeruu voi alkaa vaikkapa antureista, joihin on integroitu ainoastaan langattoman likiverkon eli WPAN (*Wireless Personal Area Network*) teknologia, jonka kantama on tyypillisesti yhdestä metristä muutamiin kymmeniin metreihin (*Proximity network*). Näiden suosituimpia teknologioita ovat Bluetooth (IEEE 802.15.1) ja ZigBee (IEEE 802.15.4). Näin kerättyä dataa voidaan tietenkin käyttää suoraan apuna paikallisessa tuotannon ohjaamisessa, mutta IoT-ratkaisuissa sitä voidaan siirtää erilaisten yhdyskäytävien (esim. *IoT-gateway*) ja WAN-tiedonsiirtoverkkojen kautta keskitettyihin tietovarastoihin tarkempaa analyysia varten.

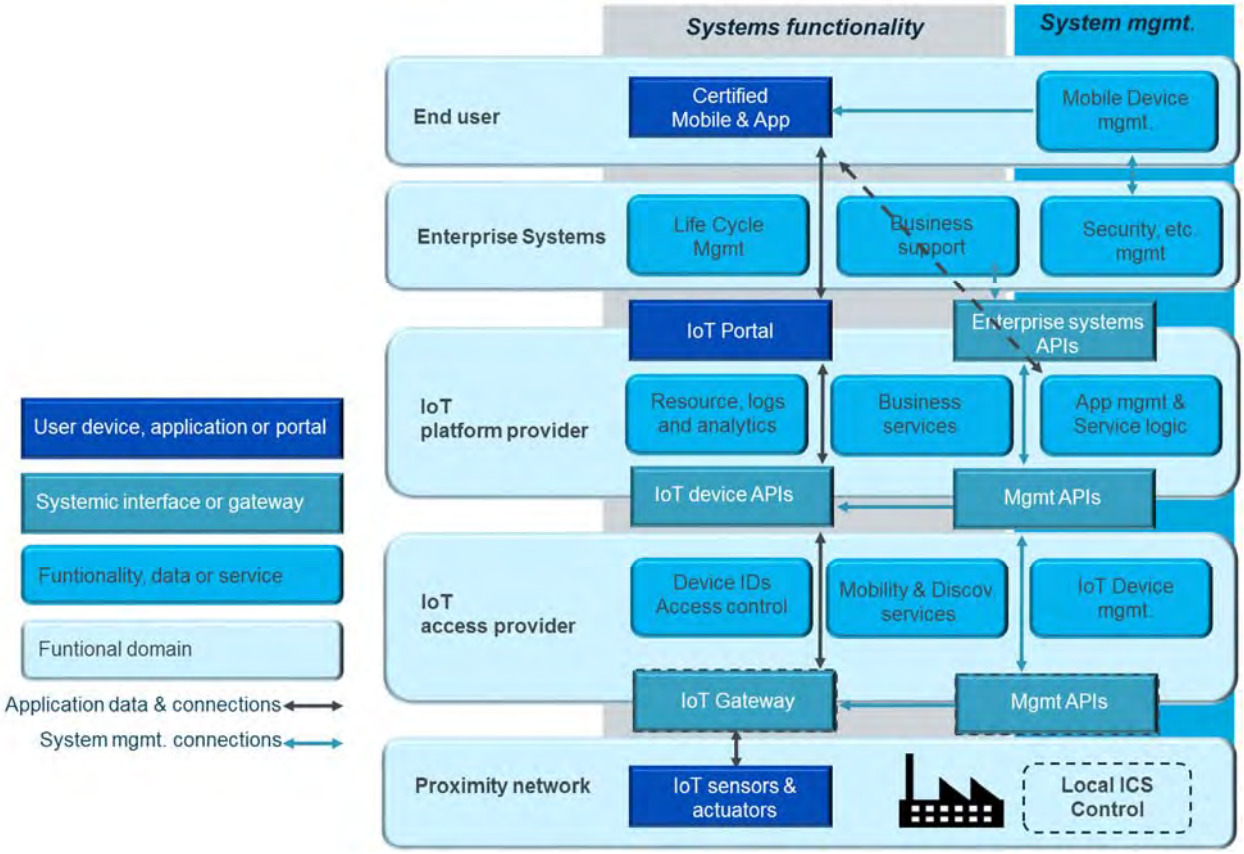
Useissa tapauksissa (IoT-sovelluksissa) lähiantureilta kerätty tieto halutaan saada siirrettyä globaalisti saatavilla olevaan pilvipalveluun, jota usein hallinnoi siihen erikoistunut IoT-alustatoimittaja eli (*IoT platform provider*). IoT-alustatoimittaja tarjoaa yleensä ainakin datan tallentamiseen ja analyysiin liittyviä palveluja.

Mikäli kerättävä data siirretään maastosta pilven suuntaan langattomasti, tehtävässä hyödynnetään IoT-mobiilioperaattoria, joka palvelee alueellista tai jopa globaalia langatonta IoT-tiedonkeruuta (*IoT access provider*). Muutamia tärkeimpiä Suomessa tuettuja langattomia IoT-teknologioita ovat:

- LoRaWAN (*Digita* operoi)
- Sigfox (*Connected Finland* operoi)
- NB-IoT ja LTE-M (*DNA, Elisa* ja *Telia* operoivat tai tulevat operoimaan)

Viime kädessä ainoastaan IoT-ratkaisun tilaajan (omistajan) määrittelemät toimihenkilöt saavat pääsyn IoT-alustan palvelindataan, jossa he voivat analysoida käytettävissä olevilla työkaluilla omistajan sensoreilta kerättyä tai koostettua dataa ja tehdä mittaukseen perustuvia johtopäätöksiä esim. tuotantojärjestelmien ohjauksen suhteen. Mikäli IoT-toimittaja haluaisi palvelusopimukseen lausekkeen käyttöoikeudestaan omistajan dataan (esim. alustansa algoritmikehitystyön tarkoituksiin), tilaajan kannattaa ehdottomasti selvittää olisiko ko. datan luovuttaminen liian kriittistä oman ydinliiketoiminnan suojaamisen ja jatkuvuuden kannalta.

Mikäli sovelluksia käytetään mobiililaitteilla, niihin liittyvät sovellukset voidaan ladata toteutuksesta riippuen esimerkiksi IoT-alustatoimittajan ekosysteemistä, asiakasyrityksen omilta kehittäjiltä, taikka tuettujen mobiililaitteiden kehittäjien ekosysteemipalveluista.



Kuva 21. Skaalautuvan IoT-ratkaisun toiminnallinen arkkitehtuuri.

Yksi teknisen toteutuksen turvallisuuden kannalta tärkeimmistä asioista on, että sovellusdatan käsittelyn ja järjestelmähallinnan rajapinnat ovat vahvasti eriytettyjä – toisin sanoen sovellusdatan (*Application data*) käyttämät datayhteydet ja rajapinnat eivät ole samoja kuin järjestelmän hallintaan ja ylläpitoon (*System management*) käytetyt toiminnallisuudet ja rajapinnat. Lisäksi järjestelmäsuunnittelussa kannattaa ottaa huomioon, että toiminnan jatkuvuuden kannalta on parasta, että kukin toiminnallinen osa-alue kykenee toimimaan määrätyn ajan itsenäisesti, vaikka yhteydet muihin toimintoihin hetkeksi katkeaisivatkin (*stand-alone*-toiminto, riittävä datan puskurointi, jne.). Näiden ominaisuuksien ansiosta arvokasta dataa ei heti häviäisi myöskään poikkeustilanteissa.

4.2.2 Tarkastuslista IoT-ratkaisuelementtien muodostamalle verkostolle

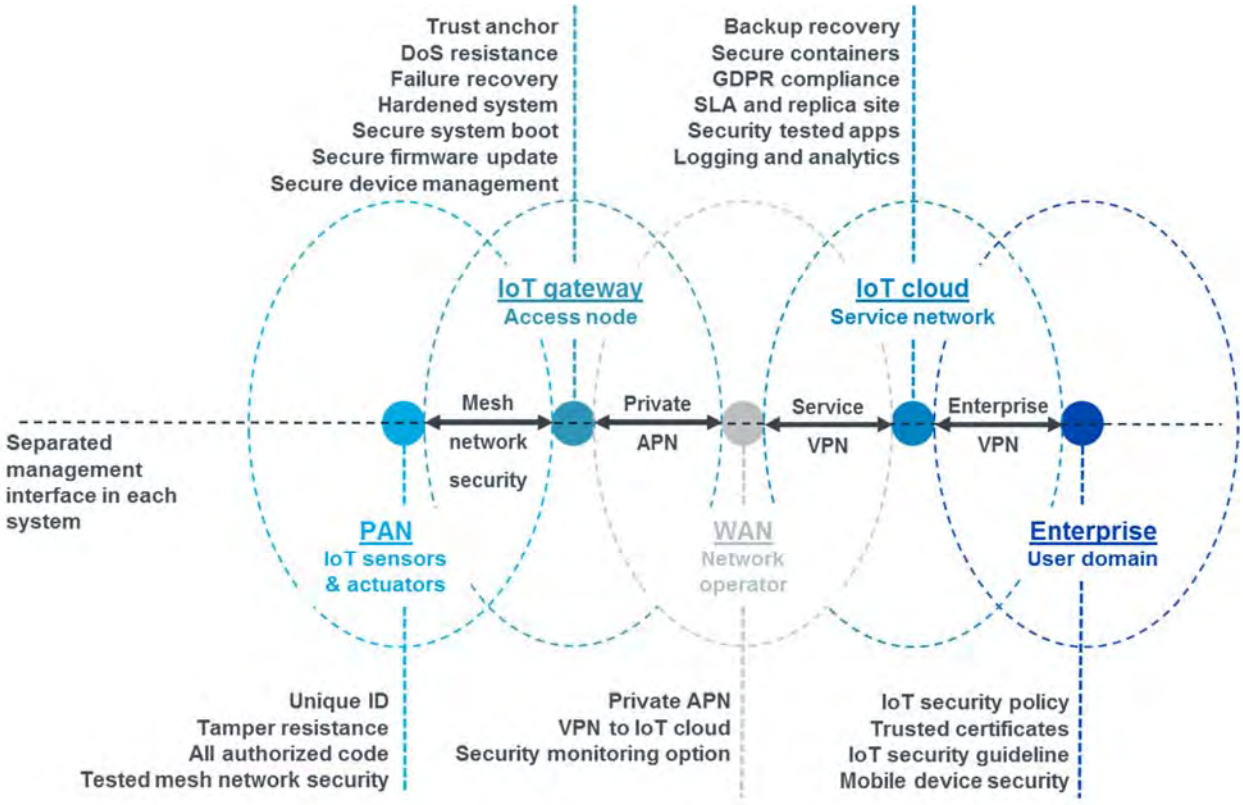
Kohderyhmä: Energiayritysten liiketoimintajohdon ja kehitystiimien tueksi niiden etsiessä ja arvioidessa yritykselleen soveltuvia IoT-ratkaisuja, järjestelmiä ja palveluja. Tarkastuslista on tarkoitettu erityisesti IoT-ratkaisuja suunnittelevien, arvioivien ja testaavien asiantuntijoiden käyttöön.

Tarkoitus: Tarkoituksena on helpottaa energiayritystä arvioimaan IoT-teknologiatoimittajia ja heidän ratkaisujensa soveltuvuutta kyberturvallisuuden ja jatkuvuudenhallinnan näkökulmasta. IoT-palveluyritysten kyvykkyydet ja ratkaisujen ominaisuudet paljastuvat hyvin määriteltyjen, rajattujen pilottiprojektien kautta. Tämä tarkastuslista nostaa esiin IoT-ratkaisuihin usein kuuluvat toimija verkkoalueet ja niiden tärkeimmät kyberturvallisuusominaisuudet, tavoitteena helpottaa keskusteluja suojaamisen mahdollisuuksista IoT-toimittajien kanssa. Fokus on teknisissä ratkaisuissa ja ominaisuuksissa.

Tausta: Asiakkaan ympäristöön sijoitettavat elementit (kuten anturit, toimilaitteet tai tietoliikenneyhdyskäytävät) yhdistetään usein IoT-ratkaisutoimittajan tarjoamaan joukkoon erilaisia tietoliikenneverkkoja ja ICT-järjestelmiä. Seuraavassa kuvassa on esitetty konseptikuva IoT-ratkaisujen yleisimmistä toimi- ja verkkoalueista kyberturvallisuuden päävaatimusluokkineen. Kuvan kieleksi valittiin englanti, sillä IoT-toimittajien ratkaisukuvaukset ovat pääosin englanninkielisiä → helpompi vertailtavuus.

Allaolevassa kuvassa toimi- ja verkkoalueiden turvallisuusominaisuuksia on esitetty muutamien esimerkkien kautta:

- PAN: Likiverkoissa *mesh*-verkon teknologialähtöinen tietoturva
- IoT gateway: IOT-operaattorilla IoT-radioverkon liittymä- / teknologialähtöinen tietoturva
- WAN: Mobiilioperaattorin verkossa liittymä- / teknologialähtöinen tietoturva
- IoT Cloud: Pilvipalveluissa palveluntarjoajan tarjoama ICT-tietoturvallisuus
- Enterprise: Asiakkaan yritysverkossa yritystasoinen ICT-tietoturvallisuuspolitiikka



Kuva 22. IoT-ratkaisujen yleisimmät toimi- ja verkkoalueet päävaatimusluokkineen.

Tarkastuslista

PAN: Likiverkon antureiden tärkeimpiä kyberturvallisuuteen liittyviä ominaisuuksia ovat yleensä:

- *Unique ID* - Antureiden yksilöllinen tunniste
- *Tamper resistance* - Fyysisen manipuloinnin suojaus
- *All authorized code* - Ohjelmistokoodin autenttisuus
- *Tested mesh network security* - Testattu laiteverkkoturvallisuus

IoT gateway: IoT-operaattorin yhdyskäytävälaitteiden osalta olisi hyvä olla selvillä seuraavista teknologisista kyvykkyyksistä:

- *Trust anchor* - Käytössä turvallinen alusta (kuten TPM - *Trusted Platform Module*) ja salainen avain joihin laitteen oikea toiminta perustuu
- *DoS resistance* - Kyvykkyys sietää palvelunestohyökkäyksiä
- *Failure recovery* - Kyvykkyys palautua vikatilanteista
- *Hardened system* - Järjestelmästä on poistettu kaikki ylimääräinen toiminnallisuus
- *Secure system boot* - Järjestelmä käynnistetään turvalliselta perustalta
- *Secure firmware update* - Laitteen varusohjelmisto voidaan päivittää turvallisesti
- *Secure device management* - Laitteen tilaa voidaan hallita turvallisesti sen elinkaaressa

WAN: Mobiilioperaattorin verkossa tulisi olla saatavilla seuraavat palvelut:

- *Private APN* - Verkkoon varataan yksityinen kytkentäpiste

- *VPN to IoT cloud* - Asiakkaan palvelu kytketään pilveen VPN:n avulla
- *Security monitoring option* - Verkossa on mahdollisuus ottaa käyttöön kyberturvallisuuden seurantapalvelut

IoT Cloud*:* IoT-pilvipalvelutarjoajan verkossa olisi hyvä olla saatavilla:

- *Backup recovery* - Varmuuskopioista palauttaminen onnistuu (mm. asiakkaan data ja konfiguraatio, verkon konfiguraatio, jne.)
- *Secure containers* - Turvalliset kontit
- *GDPR compliance* - Yhteensopivuus EU:n tietosuoja-asetuksen kanssa
- *SLA and replica site* - Palveluntasosopimus ja varakonesali
- Security tested apps - Tietoturvatestatut sovellukset
- Logging and analytics - Lokien keräys ja analytiikkapalvelut

Enterprise*:* Asiakkaan yritysverkossa tärkeimpiä IoT-kyberturvallisuuteen liittyviä kehityskohteita ovat usein:

- IoT security policy - IoT tietoturvapolitiikka
- Trusted certificates - Luotetut varmenteet
- IoT security guideline - IoT tietoturvaohjeistus
- Mobile device security - Mobiililaitteen tietoturvallisuus

4.2.3 Tarkastuslistat yleiskäyttöisten verkkoliityntöjen hyödyntämisestä IoT:ssä

Kohderyhmä: Energiayritysten kehitystiimien tueksi, kun ne määrittävät, arvioivat ja testaavat yritykselleen soveltuvia yleisiä tietoliikenneratkaisuja, järjestelmiä ja palveluja, jotka liittyvät IoT-ratkaisuihin. Tarkastuslista on tarkoitettu erityisesti IoT:n kokonaisratkaisuja määrittävien, arvioivien ja testaavien asiantuntijoiden käyttöön.

Tarkoitus:

Tarkoituksena on helpottaa energiayritystä arvioimaan yleisten tietoliikenneratkaisujen mahdollista soveltuvuutta IoT-kokonaisratkaisun tavanomaisen tiedonsiirron tarpeisiin, erityisesti kyberturvallisuuden ja jatkuvuudenhallinnan näkökulmista. IoT-ratkaisujen ominaisuudet paljastuvat (rajattujen) pilottiprojektien kautta. Tämä tarkastuslista nostaa esiin tärkeimpien yleiskäyttöisten dataverkkojen tietoturvauhkia ja muutamia suojauskeinoja, tavoitteena helpottaa keskusteluja suojaamisen mahdollisuuksista IoT-toimittajien kanssa.

Tausta: IoT-ratkaisun turvattomuuden syy voi olla sisäisen likiverkon (PAN) liian avoin liityntä (ks. konseptitason suojaamisohjeita kuvassa 22). Väylän avoimuus on riski, mikäli hyökkääjä voi saada fyysisen pääsyn ratkaisun tietoliikenneväylään eli datakaapeliin tai langattoman verkon kuuluvuusalueelle. Väylän salakuuntelu ja haltuunotto voivat onnistua, mikäli hyökkääjä saa (hetkeksi) toimivan yhteyden väylään. Tällöin hyökkääjältä onnistuu:

- Ylimääräisen laitteen tai ohjelmiston asentaminen väylään
- Komentokanavan luonti ja (salattu) etäkäyttö hyökkääjän hallussa olevalta komentopalvelimelta
- Sisäverkkovakoilu ja eteneminen muihin verkkoalueisiin ja kriittisiin kohteisiin

Salakuuntelu onnistuu teknisesti, mikäli väylästä puuttuu laitteiden vahva tunnistus ja viestien salaus. Joskus näitä ei toimiteta oletusasetuksena, syynä IoT-tuotteen edullisuus tai vaatimukset mahdollisimman helposta käyttöönotosta. Tällaiset tietoturvapuutteet mahdollistavat väylän salakuuntelun ja täten mahdollisesti myöhemmin koko sisäverkon tietoliikenteen ja sen laitekannan laittoman ennakkokartoittamisen.

Tarkastuslista - Yleiskäyttöiset dataverkot

Suurin osa IoT-ratkaisuista hyödyntää myös tavanomaiseen käyttöön suunniteltuja dataverkkoja tai paikannusteknologioita. Tällaisissa ratkaisuissa voidaan suoraan tai välillisesti hyödyntää esimerkiksi seuraavia teknologiarajapintoja:

- Ethernet (paikallisverkko):
  - Uhat: Suora kytkentä yhteiseen paikallisverkkoon sisältää monenlaisia riskejä kuten erilaisia ruuhka- ja vikatilanteita, salakuuntelua ja tietomurtoja
- WLAN/WiFi (langaton paikallisverkko):
  - Uhat: Avoimissa WLAN-verkoissa esiintyy paljon ongelmia kuten yllättäviä vikatilanteita, radiohäirintää, viestimyrskyjä ja salakuuntelua. Jopa WPA2-toteutuksia on todettu turvattomiksi
- Julkiset mobiiliverkot (yleinen tiedonsiirto):
  - Uhat: Verkon saatavuuden heikentäminen, erilaiset julkisen verkon kautta toteutetut hyökkäykset

- GPS/GLONASS/GALILEO (paikkatiedon haku):
  - Uhat: Satelliittisignaalia voidaan häiritä → paikkatiedon häirintä tai manipulointi

Erilaisten yleiskäyttöisten rajapintojen turvallisuudessa on paljon erilaisia riskejä, uhkia tai muita ongelmia, joiden välttämiseksi tulisi käyttää useampia suojauskeinoja.

Ethernet: SUOJAUSKEINOJA:
- Vältä ylimääräisten Ethernet-liityntöjen asentamista IoT-verkkoon
- Estä viestimyrskyt jo rajapinnassa (*frame filtering*), mikäli mahdollista
- Käytä huolto- ja muihin datayhteyksiin myös sovellustason tunnistusta
- Estä tarpeeton pääsy kriittisiin osiin järjestelmäverkkoa
- Tarkista laite haittaohjelmien varalta ennen sen liittämistä verkkoon

WLAN/WiFi: SUOJAUSKEINOJA:
- WLAN-tukiaseman hallintaliittymä tulee suojata turvallisin asetuksin ja hyvällä salasanalla
- WLAN:ssa tulee vaatia vähintään WPA2-salaus ja turvallinen salasana
- WLAN-tukiaseman käyttöä reitittimenä tulee välttää, jos mahdollista
- WLAN-tukiaseman varusohjelmiston (*firmware)* tulee olla päivitettävissä turvalliseen versioon (etänä vain hallintaverkon kautta)
- WLAN-tukiaseman haavoittuvuus- ja vikakorjaukset tulee asentaa säännöllisesti
- WLAN-verkon käyttö reaaliaikaisen kriittisen informaation välitykseen sisältää riskejä (esim. vikaantuminen)
- Sovella Ethernet-suojauskeinoja mahdollisuuksien mukaan (edellä)

Julkiset mobiiliverkot: SUOJAUSKEINOJA:
- Vältä 2G-verkkoa, siirry 3G, 4G, 5G-verkkoon
- Hanki pääsyrajoitettu SIM-kortti (*Private APN*) tiedonsiirtoa varten (tämä ei yksin riitä suojaukseksi)
- Myönnä verkkopääsy vain rajattuihin laitteisiin, mikäli mahdollista
- Selvitä miten teleoperaattori vastaa mobiiliverkkoliitynnän turvallisuudesta ja hanki tarvittavat tietoturvan lisäpalvelut (riskianalyysinne mukaisesti)
- Selvitä voiko valetukiasema huijata tiedonsiirtoratkaisuanne
- Estä oletusarvoisesti kaikki yhteydenotot julkisen verkon suunnasta

GPS / GLONASS / GALILEO satelliittipaikannus: SUOJAUSKEINOJA:
- Korjauta järjestelmistä mahdolliset satelliittipaikannukseen liittyvät ohjelmistohaavoittuvuudet ja viat
- Päivitä järjestelmät uuteen testattuun versioon mahdollisimman usein
- Selvitä voitaisiinko satelliittisignaalin mahdollinen äkillinen häiriö tai manipulaatio huomioida sovellusohjelmiston koodissa (häirinnän havaitseminen)
- Varmista myös vaihtoehtoisten paikannusjärjestelmien (satelliitit, WiFi, mobiiliverkko) oikea toiminta

Tarkastuslista - Likiverkko

Suojauskeinoja IoT:n käyttämän likiverkon turvaamiseen:
- TEE HANKALAKSI ylimääräisen IoT-laitteen lisääminen järjestelmään (vahva laitetunnistus)
- ERIYTÄ KRIITTISET laitteet omaan aliverkkoonsa ja estä asiaton dataliikenne
- PRIORISOI VIESTIT kriittisyyden mukaan (mikäli mahdollista)
- VARMISTA VIESTIEN OIKEELLISUUS myös sovellustasolla
- ÄLÄ JULKISTA viestien yksityiskohtaista rakennetta (jos turvallisuuskriittinen sovellus)
- TUNNISTA LAITTEITA jotka aiheuttavat järjestelmähäiriöitä
- TUNNISTA ASIATTOMIA langattomia laitteita ja verkkoja toimialueen läheisyydessä

4.3 IoT-hankinnat ja kyberturvallisuuden kehittäminen

Automaatio- ja IoT-järjestelmien toiminnan ymmärtäminen ja hyvä hallinta koko elinkaaressa perustuu myös riskiarvioinneille ja vaatimuksille, joita järjestelmälle asetetaan etukäteen. Tämä on ehdottomasti toivottu kehityssuunta, sillä tietoturvaa ei tulisi lisätä järjestelmiin jälkikäteen (se on usein tehotonta ja kallista).

Kuva 23. Automaatio- ja IoT-järjestelmien kyberturvallisuuden kehittäminen hankintojen kautta.

Riskien ja uhkien arviointi: ARVIOI liiketoiminnan riskit:

Liiketoiminnan riskejä tulee arvioida ennen hankintoja sekä jatkuvasti ainakin liiketoimintaympäristön muuttuessa. Riskiarvio-matriisin laadinta tai päivittäminen yhteistyössä avainhenkilöstön kanssa on tehokas tapa arvioida riskejä. Arviointitiimiin kannattaa ottaa mukaan asiantuntijajäseniä paitsi johdosta ja liiketoiminnoista, myös mm. järjestelmäkehityksestä, IT-tuesta ja pääkäyttäjistä, sekä esimerkiksi alan kyberturvallisuuteen perehtynyt asiantuntija. Vain tunnistettujen riskien ja uhkien kautta kyetään määrittelemään kuhunkin ympäristöön ja ratkaisuun soveltuvat kyberturvallisuusvaatimukset.

Hankintavaatimusten ja ohjeiden kehittäminen: KEHITÄ hankintojen vaatimuskanta:

Yrityksen kannattaa määritellä tulevia IoT-hankintoja varten yleispäteviä kyberturvallisuuteen ja jatkuvuuteen liittyviä vaatimuksia, joita voidaan harkitusti soveltaa eri projekteissa. Vaatimuskannan pohjaksi kannattaa ottaa koeteltu, käytännöllinen standardi, joka sisältää myös mm. henkilöturvallisuuteen ja yksityisyyteen liittyviä vaatimuksia. Omalle liiketoiminnalle soveltuvan IoT-vaatimuskannan kehittämiseksi kannattaa järjestää työpajoja, joihin voi jo tässä vaiheessa ottaa rajoitetusti mukaan jopa järjestelmätoimittajia, jotta voidaan jo etukäteen arvioida vaatimuksiin liittyvää kustannustasoa sekä käytännön toteutusvalmiuksia.

Vaatimuskantaa voidaan käyttää myös riskienhallintatyökaluna, jota soveltamalla kuhunkin hankintaan voidaan kiinnittää tietyn hyväksytyn riskitason toteuttavat vaatimukset.

Kyvykkyyksien kehittäminen ja ratkaisujen valinta: HANKINNOISSA ratkaisujen läpikäynti toimittajien kanssa & vaatimusten kiinnitys:

Hankintaprosessiin sisällytettävässä toimittajien soveltuvuusanalyysissä on oleellista varmistaa sellaisten IoT -alustojen ja sovelluspalvelujen valinta,

joiden kyberturvallisuus on testattu ja ylläpito varmistettu mm. ajantasaisin haavoittuvuuskorjauksin ja päivityksin. Tämän validoimiseksi potentiaalinen toimittaja kannattaa kutsua erityiseen työpajaan hankintavaatimusten läpikäyntiä varten, jossa IoT-toimittaja voi tuoda esiin evidenssiä omista hyvistä käytännöistään kyberturvallisuuden kehittämiseen ja ylläpitoon liittyen. Jokaisessa IoT-projektissa tuskin edellytetään kaikkien vaatimuskannassa olevien kyberturvallisuusvaatimusten täyttämistä, sen sijaan niissä keskitytään erityisesti kyseiseen käyttötapaukseen liittyvien uhkien poistamiseen tähtäävien vaatimusten valintaan. Näin varmistetaan projektin kustannustehokkuus.

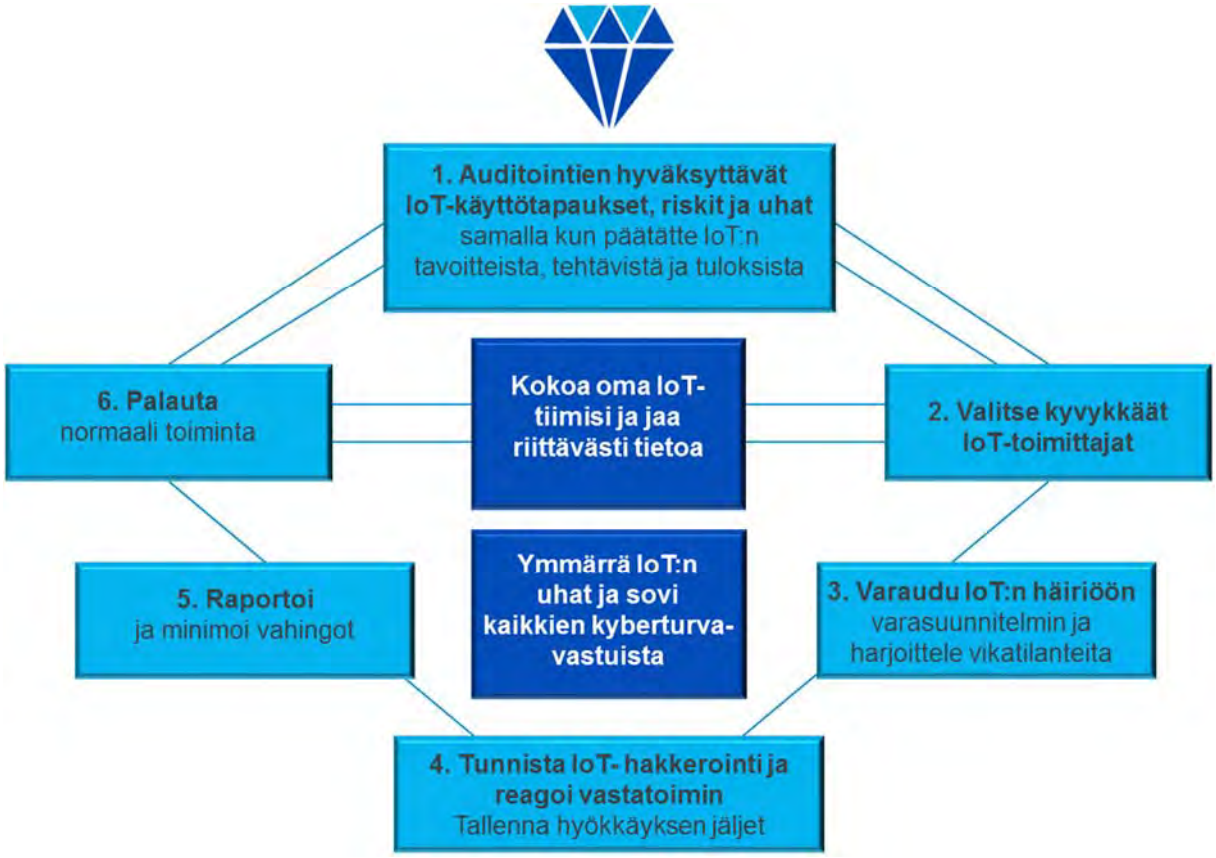
Varsinkin järjestelmän pitkää elinkaarta edellyttävät asennuskohteet pakottavat myös kriittiseen ekosysteemitarkasteluun, jossa eri palveluntarjoajien toimintakykyä ja kyberturvallisuuden kehittämistä arvioidaan pidemmän aikavälin kuluessa. Yleisesti ottaen isoimpia hankintoja ei tule tehdä pelkästään lyhyen aikavälin kuluessa kertyneiden kokemusten perusteella.

Verifiointi ja testaus: VARMISTA vaatimusten toteutumisen verifiointi projekteissa:

Vaatimusten esittäminen ennen projektia ja toimittajan vastaukset ja vakuuttelut omasta osaamisestaan eivät vielä riitä varmistamaan projektin kyberturvallisuuden toteumaa. IoT-toimittajan tulee viimeistään projektin loppuvaiheessa kyetä esittämään todisteita esimerkiksi toteutetuista järjestelmäkovennuksista, kyberturvatestauksista ja koodikatselmoinneista, joista ennen projektia sovittiin. Lyhytkin raportti kustakin sovitusta toimenpiteestä voi vakuuttaa tilaajalle, että projektissa on tehty kyberturvan osalta huolellista työtä. Ylläpidon palveluiden ja päivitysten toimivuus kannattaa myös todentaa jo projektin kuluessa, sillä ne tulevat olemaan erittäin tärkeitä turvallisuuden ylläpidolle käyttövaiheessa. Mikäli toimitettavaan järjestelmään sisältyy lokikeräystä ja lokiseurantaa, kannattaa niidenkin oikeasta toiminnasta varmistua yhdessä jo ennen järjestelmän virallista käyttöönottoa. Näin saadaan myös tietoturvan seuranta otettua hallitusti käyttöön heti alusta alkaen.

4.4 Teollisuuden IoT-toimittajien arviointi ja ratkaisujen evaluointi

Uusien IoT-teknologioiden avulla teollisuuslaitokset pystyvät nopeasti ja edullisesti ottamaan käyttöön reaaliaikaista tiedonkeruuta vaikkapa tuotantotilojen lämpötilasta, kosteudesta ja paineesta, koneiden ja laitteiden osien kunnosta, tai osin jopa itse tuotantoprosessin toiminnasta. Uuden teknologian käyttöönotto ei kuitenkaan yleensä tapahdu ilman riskejä. Siksi ennen jokaisen IoT-järjestelmän hankintaa tuleekin luotettavasti selvittää potentiaaliset haitalliset vaikutukset esimerkiksi muun tuotantoverkon jatkuvaan toimintaan ja avautuviin uusiin kyberhyökkäysvektoreihin, tai esimerkiksi lisääntyviin integraatio- ja ylläpitovaatimuksiin.



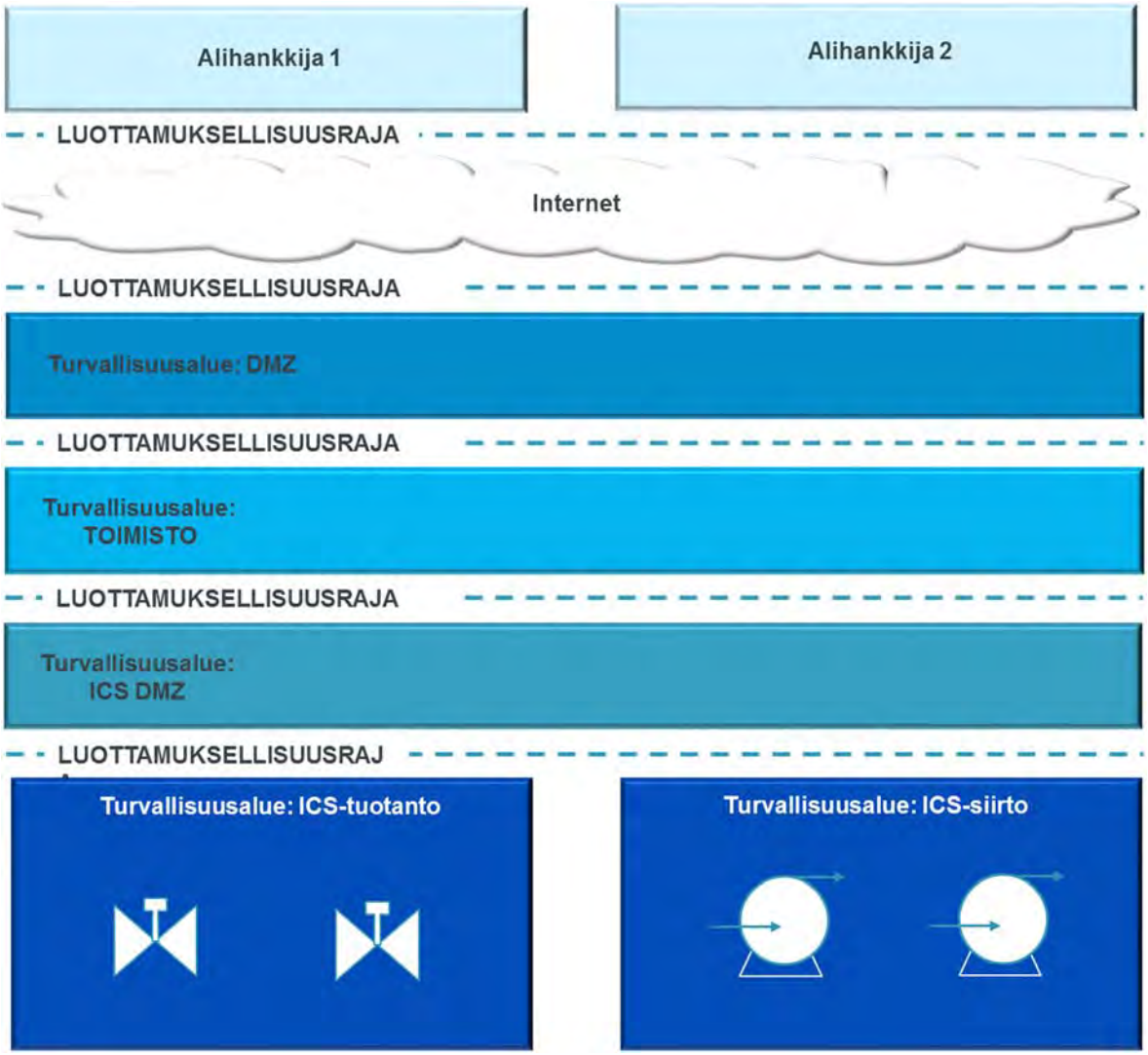
Kuva 24. Energiayhtiön askeleet ketterään ja turvalliseen IoT:hen.

Epävarmuuksia tuovien asioiden selvittäminen etukäteen edellyttää myös potentiaalisten IoT-toimittajien kyberturvallisuuskyvykkyyksien koestamista sekä heidän tarjoamiensa ratkaisujen yksityiskohtaisempaa evaluoimista. Seuraavissa alakohdissa kerrotaan lisää siitä, miten potentiaalisen IoT-toimittajan tulee valmistautua arviointikokoukseen, jossa energiayritys arvioi toimittajan kyvykkyyttä, ratkaisua ja palvelua kyberturvallisuuden näkökulmasta.

4.4.1 IoT-toimittajien ennakkovalmistautuminen

Energiayhtiöille on viime vuosien kuluessa kehittynyt paljon potentiaalisia mahdollisuuksia kehittää esimerkiksi energiatehokkuutta tai kuluttajille suunnattuja palveluja erilaisten IoT-ratkaisujen kautta. Houkuttelevilta näyttäviin IoT-tarjouksiin ei kuitenkaan tulisi oikopäätä tarttua. Päinvastoin, ainoastaan potentiaalisimmat palveluntarjoajat kannattaa kutsua kahdenvälisiin kokouksiin, joissa energiayritys pyytää IoT-tarjoajaa esittelemään omaa palveluaan ennalta mietittyä systematiikkaa noudattaen. Tämän jälkeen toimittajan arviointikokouksessa aletaan käydä yhdessä läpi energiayrityksen asettamia vaatimuksia, joihin toimittajakandidaatti pyrkii parhaansa mukaan vastaamaan.

IoT-toimittajan antamista vastauksista riippuu kannattaako kahdenvälisissä välisissä neuvotteluissa edetä enää pidemmälle. Toimittajan kannattaisi siis valmistautua oman IoT-palvelunsa kyberturvallisuusvaatimusten toteutumisen esittelyyn varsin huolellisesti.



Kuva 25. Valmistautumisohje IoT-toimittajille - Esittäkää ratkaisunne arkkitehtuurikuvaus (ja sijoittakaa sen elementit) kuvan tietoturvavyöhykkeisiin. (Huom! Sama arkkitehtuuri kuin kuvassa 19, joka esiteltiin jo kohdassa 3.3.4)

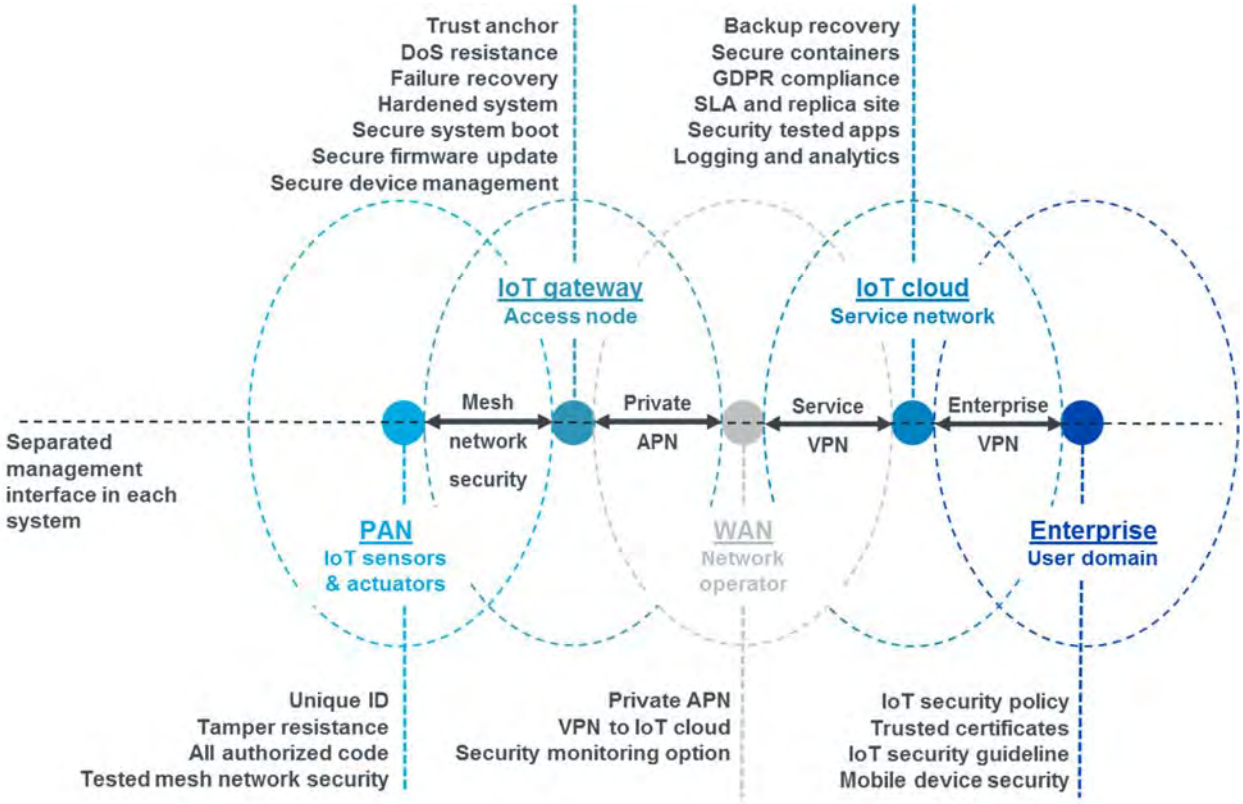
Jotta kokouksesta tulisi mahdollisimman informatiivinen, energiayrityksen kannattaa jo hyvissä ajoin ennen kokousta pyytää IoT-toimittajaa:

- Sijoittamaan IoT-ratkaisunsa pääelementit yllä olevan kuvan verkkoalueisiin ja piirtämään niiden väliset datayhteydet
- Loogisen kuvan muodossa esittämään oman IoT-ratkaisunsa riippuvuudet ja rajapinnat myös muihin järjestelmiin, joita heidän ratkaisunsa toiminta edellyttää

Toimittajan IoT-ratkaisun elementeistä, ominaisuuksista ja riippuvuuksista muihin järjestelmiin kannattaa lisäksi keskustella jo kohdassa 4.2.2. esitellyn kuvan ”IoT-ratkaisujen yleisimmät toimi- ja verkkoalueet päävaatimusluokkineen” kautta.

Toimittajalta kannattaa kysyä esimerkiksi: Mitkä alla olevan kuvan toimialueista, verkoista ja tietoturvaominaisuuksista hallitaan teidän IoT-palvelunne kautta?

- PAN-likiverkon ja sen sensorien tietoturvaaminen?
- IoT-radioverkkoliittymän ja yhdyskäytävän tietoturvaaminen?
- Mobiilioperaattoriliittymän tietoturvallisuus?
- IoT-pilvipalvelun ICT-tietoturvallisuus?
- Asiakkaan IoT-sovelluksen tietoturvallisuus?



Kuva 26. Valmistautumisohje IoT-toimittajille - Mitkä kuvan toimialueista, verkoista ja tietoturvaominaisuuksista hallitaan teidän IoT-palvelunne kautta?
(Huom! Kuva esiteltiin jo kohdassa ”4.2.2 Tarkastuslista IoT-ratkaisuelementtien muodostamalle verkostolle”)

Arviointikokouksessa IoT-toimittajaa pyydetään kertomaan tarkemmin, myös kaaviokuvia esittäen, miten kyberturvallisuus on huomioitu heidän tarjoamassaan:

- IoT-palvelun politiikoissa ja prosesseissa koko elinkaaren ajan?
- IoT tuotteen kehitysvaiheen turvallisuusmenettelyissä?
- IoT tuotteen ominaisuuksissa ja niiden kehittämisessä?
- IoT tuotteen ylläpidossa, korjauksissa ja päivityksissä?
- IoT tuotteen etähallinnan turvallisuudessa?

4.4.2 IoT-hankintojen alkuvaiheen lyhyt tarkastuslista

Kohderyhmä: Energiayritysten liiketoimintajohdon ja kehitystiimien alkuvaiheen tueksi niiden etsiessä ja arvioidessa yritykselleen soveltuvia IoT-ratkaisuja, järjestelmiä ja palveluja. Tarkastuslista on tarkoitettu erityisesti IoT-ratkaisuhankintoja suunnittelevien ja arvioivien asiantuntijoiden käyttöön.

Tarkoitus: Tarkoituksena on helpottaa energiayritystä arvioimaan IoT-ratkaisujen tuomia riippuvuuksia jatkuvuudenhallinnan näkökulmasta. IoT-palveluyritysten kyvykkyydet ja ratkaisujen ominaisuudet paljastuvat hyvin määriteltyjen, rajattujen pilottiprojektien kautta. Tämä tarkastuslista nostaa esiin energiayrityksen tärkeimmät alkuvaiheen tehtävät ennen kuin ne käyttöönottavat IoT-ratkaisuja. Tavoitteena on välttää pahimmat uudet kyberturvallisuus- ja jatkuvuusongelmat.

Tausta: Miten energiayrityksen kannattaisi IoT-hankintojen alkuvaiheessa valmistautua, jotta suurimmilta kyberturvallisuus- ja jatkuvuusongelmilta vältyttäisiin? Kannattaa kutsua ainoastaan lupaavimmat palveluntarjoajat kahdenvälisiin kokouksiin, joissa energiayritys pyytää IoT-toimittajaa esittelemään omaa palveluaan. Kokouksessa käydään yhdessä läpi energiayrityksen asettamia vaatimuksia, joihin toimittajakandidaatti pyrkii parhaansa mukaan vastaamaan.

Jotta kokouksesta tulisi mahdollisimman informatiivinen, energiayrityksen kannattaa jo hyvissä ajoin ennen kokousta pyytää IoT-toimittajaa:

- Sijoittamaan IoT-ratkaisunsa pääelementit kuvan 25 verkko-alueisiin ja piirtämään niiden väliset datayhteydet
- Esittämään loogisen kuvan muodossa oman IoT-ratkaisunsa riippuvuudet ja rajapinnat myös muihin järjestelmiin, joita heidän ratkaisunsa toiminta edellyttää

Tarkastuslista

Miten energiayrityksen kannattaa valmistautua IoT-hankintojen alkuvaiheessa, jotta suurimmilta kyberturvallisuus- ja jatkuvuusongelmilta vältyttäisiin?

Oman organisaation kokonaisymmärryksen parantaminen IoT-järjestelmistä ja niiden ekosysteemeistä ennen hankintojen tekemistä.

Määritelkää käyttötapaukset huolellisesti, sillä ne määrittävät kaikki ratkaisuun sovellettavat erilaiset vaatimukset. Käyttötapausten kuvausten olisi hyvä sisältää ainakin seuraavien asioiden määrittelyt:

- Mitä tarkoitusta varten IoT-ratkaisu kehitetään?
  - Millä tavoin ratkaisu parantaa liiketoimintaa? (esim. lisää rahaa, varmuutta tai ennustettavuutta…)
- Mitkä yritykset ja henkilöroolit käyttäisivät IoT-ratkaisua suoraan omassa työssään?
  - Mihin tehtäviin he ratkaisua käyttävät?
- Mitkä järjestelmät hyödyntävät suoraan IoT-järjestelmää tai sen tuottamaa tietoa?
  - Mihin tehtäviin ne ratkaisua hyödyntävät?
- Mitkä järjestelmät hyödyntävät välillisesti IoT-järjestelmää tai sen tuottamaa tietoa?
  - Mihin tehtäviin ne ratkaisua hyödyntävät?
- Mitä muita tarkoituksia IoT-ratkaisu voisi tulevaisuudessa palvella, mikäli sitä kehitetään edelleen tai sen käyttöä laajennetaan alkuperäisestä?

Keskustelujen käyminen arkkitehtuurikuvien kautta, sillä niiden avulla saa hyvän käsityksen ratkaisuun liittyvistä elementeistä ja niiden välisistä yhteyksistä:

- Energiayrityksen tulee kehittää arkkitehtuurikuvien avulla oma monistettava IoT-ratkaisukonsepti, jossa:
  - omat vahvuudet ja osaamiset tulevat parhaiten hyödynnettyä
  - palveluyritysten roolit ja vastuualueet selkeytetään
- Arkkitehtuurikuvan tulee sisältää ratkaisussa käytettävät erilaiset verkot ja toimialueet, mukaan lukien
  - tietoturvan DMZ-vyöhykkeet,
  - kuvaukset miten tietoa siirretään järjestelmästä toiseen
- Ratkaisutoimittajia tulee haastaa arkkitehtuurikuvan kautta
  - pyytämällä heitä sijoittamaan kuvaan oman ratkaisunsa eri elementit ja tarvittavat datayhteydet
  - havainnoi mitä osa-alueita toimittaja ei omalla ratkaisullaan pysty kattamaan?
- Arkkitehtuurikuva tulee päivittää aina toimintaympäristön ja ratkaisujen kehittymisen myötä

Tarvittaessa erityisvaatimusten kehittäminen IoT:n kyberturvallisuudelle ja vaatimusten valinta eri projekteissa uhka-analyysinne mukaisesti.

IoT-toimittajien koestaminen ja ratkaisujen pilotointi ennen laajamittaista toimittajan valintaa.

Kyberturvallisuuden ylläpidon ja seurannan varmistaminen toimittajan kanssa jo alkuvaiheessa.

4.4.3 IoT-toimittajien ja ratkaisujen arvioinnista

Teollisuusyrityksistä löytyy lukemattomia erilaisia tapoja valita heille soveltuvia teknologia- ja palvelutoimittajia, sillä kyseisiä palveluja hankitaan varsin erilaisiin ympäristöihin ja erilaisia käyttötarpeita ja käyttötapauksia varten. Joskus soveltuvia teknologiatoimittajia on vähän ja asialla on kiire, jolloin tilaaja voi olla vaatimuksineen heikoilla, varsinkin ison toimittajan tapauksessa. Sen sijaan IoT-ratkaisuja hankittaessa kannattaa panostaa alusta alkaen myös kyberturvallisuuden osalta kyvykkään toimijan valintaan, sillä valinnanvaraa pitäisi olla runsaasti. Tietoturvallisuuden kehittämiseen ja ylläpitämiseen liittyvä toiminta on kuitenkin varsin saman tyyppistä tuotteesta tai toimialasta riippumatta, toki joitakin erityispiirteitä lukuun ottamatta.

Liitteessä B esitetyt IoT-toimittajien ja ratkaisujen arvioinnin tarkastuslistat on tarkoitettu energiayritysten IoT-ratkaisuja tai palveluja suunnittelevien ja evaluoivien asiantuntijoiden, sekä kaikkien muidenkin tällaisiin hankintoihin osallistuvien toimihenkilöiden käyttöön. Tarkastuslistojen tavoitteena on mm. helpottaa energiayritystä arvioimaan IoT-palvelutarjoajien kyvykkyyksiä, erityisesti kyberturvallisuusvaatimuksiin liittyen. Luotettavaa IoT-toimittajaa käyttämällä voidaan esimerkiksi pienentää maineriskejä, joita turvattomien palvelujen käyttöönotto voisi yritykselle mahdollisesti aiheuttaa.

4.5 IoT-pilottiprojektit

Tässä alaluvussa kuvataan yksityiskohtaisen esimerkin kautta varsin tarkka esitys eräästä projektin kuluessa käsitellystä energia-alan IoT-pilottiprojektin mallikuvauksesta, jonka pohjalta kyberturvallisuuteen liittyvää analyysiä on hyvä lähteä suorittamaan. Samalla listataan muutamia tässä esimerkkitapauksessa tunnistettuja riskejä. Kyseessä on mielestämme varsin mallikas yrityslähtöisen käyttötapauksen kuvaus, josta lukija voi ottaa oppia myös oman energiayrityksensä IoT-käyttötapausten yksityiskohtaiseen kuvaamiseen.

4.5.1 IoT Case: Kaukolämmön kysyntäjousto (KLKJ)

4.5.1.1 Johdanto

Tämä Case-esimerkki kehitettiin yrityslähtöisesti KYBER-ENE 2 -hankkeen IoT-työpajojen tarpeisiin ja se kuvaa kaukolämmön kysyntäjoustoksi (KLKJ) kutsuttua ajatusta sekä sen teknisiä toteutustapoja. Case-esimerkki ei silti sellaisenaan kuvaa minkään tietyn energiayhtiön ympäristöä. Asioiden ja käsitteiden esittelyssä on hyödynnetty julkaisuja ”Suomalainen kaukolämmitys” [KAUKOLÄMMITYS] sekä ”Kaukolämmön kysyntäjousto” [VALOR]. KYBER-ENE 2 hankkeessa tämän Case-esimerkin alkuperäisenä tehtävänä oli yhtäältä auttaa osallistujia ymmärtämään KLKJ-käyttötapausta ja toisaalta auttaa tunnistamaan kuvatun kaltaiseen KLKJ-kokonaisuuteen liittyviä riskejä, hyökkäysvektoreita sekä niiden rajoittamista.

4.5.1.2 Kaukolämpö

Kaukolämmitys on keskitetty laajojen alueiden, kuten kokonaisten kaupunkien, niiden osien tai useiden rakennusten muodostaman ryhmän lämmöntuotanto ja -jakelujärjestelmä. Kaukolämmityksen lämpöenergia tuotetaan keskitetysti lämmitysvoimalaitoksissa tai lämpökeskuksissa ja jaetaan kaukolämpöverkoston välityksellä asiakkaille. [KAUKOLÄMMITYS, s. 11].

Kuuma kaukolämmön kiertovesi pumpataan kaukolämpöverkostoa pitkin asiakkaille. Asiakkaan lämmönjakokeskuksessa lämpöenergia siirtyy kiinteistön lämmitysjärjestelmän kiertoveteen tai lämpimän käyttöveden valmistukseen, ja jäähtynyt kaukolämpövesi palaa uudelleen lämmitettäväksi lämmöntuotantolaitokseen. [KAUKOLÄMMITYS, s. 11].

Nykyaikainen kaukolämpöjärjestelmä koostuu kolmesta pääosasta [KAUKOLÄMMITYS, s. 17]:

- Lämmöntuotantolaitokset (lämmitysvoimalaitokset ja lämpökeskukset)
- Kaukolämmön jakeluverkosto
- Kaukolämmön asiakaslaitteet (mittauskeskus ja lämmönjakokeskus)

Kaukolämmityksen liittymis- eli talojohto päättyy asiakaslaitteisiin lämmönjakohuoneessa. Asiakaslaitteisiin luetaan kuuluvaksi mittauskeskus ja lämmönjakokeskus. [KAUKOLÄMMITYS, s. 18].

Lämmön mittauskeskuksen hankkii, omistaa ja huoltaa lämmönmyyjä. Mittauskeskus sisältää lämpömäärän laskijalaitteen, johon on kytketty meno- ja paluuveden lämpötila-anturit sekä virtausanturi. [KAUKOLÄMMITYS, s. 18].

Lämmönjakokeskuksen, joka käsittää lämmönsiirtimet, säätöautomatiikan, pumput jne., omistaa ja huoltaa kaukolämpöasiakas. Lämmönsiirtimiä on yleensä vähintään kaksi, lämmityksen lämmönsiirrin huonetilojen lämmitykseen ja käyttöveden lämmönsiirrin lämpimän käyttöveden valmistamista varten. Myös muita lämmityskohteita, kuten ilmanvaihtoa tai ilmastointia varten asennetaan oma lämmönsiirrin säätölaitteineen. [KAUKOLÄMMITYS, s. 19].

4.5.1.3 Kaukolämmön kysyntäjousto

Kaukolämmön kysyntäjousto on kaukolämmön kulutuksen ja sitä kautta lämpötehon tarpeen ajoituksen muuttamista tavanomaiseen lämmitystarpeeseen verrattuna heikentämättä asiakkaiden kokemaa palvelun laatua. [VALOR, s. 3/32].

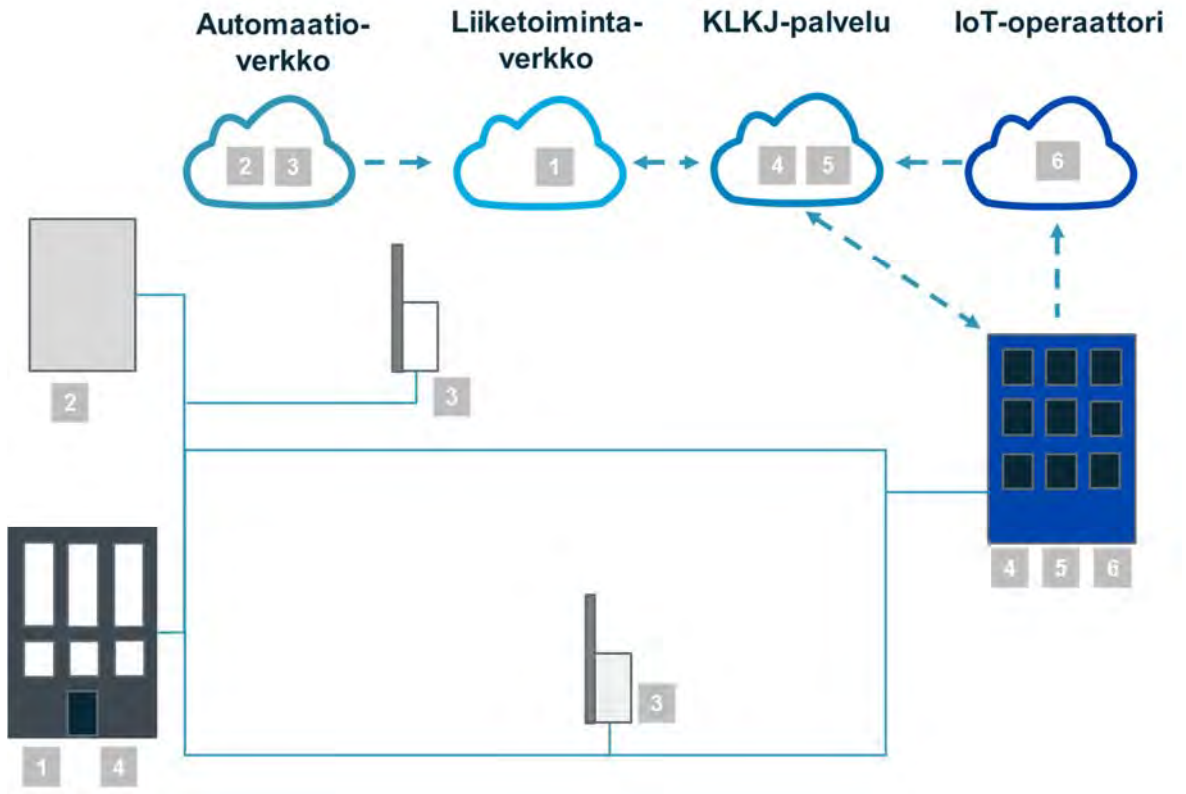
Kysyntäjoustossa lämpöenergiaa ei välttämättä säästy, vaan tavoitteena on lämmönkulutuksen

ajallinen siirto tai hetkellinen leikkaus koko kaukolämpöjärjestelmän kannalta optimaalisemmaksi – eli kysyntäjoustossa tarkastelu keskittyy hetkellisen lämpötehon tarpeeseen, ei lämpöenergian käyttöön. Kysyntäjouston tavoitteena on yleensä loiventaa kulutushuippuja öljykattiloiden tai muun kalliin huippu- tai varatuotannon käytön vähentämiseksi tai välttämiseksi eli huippulämmön toimittamista pyritään leikkaamaan mutta silti varmistaen riittävän peruslämmön toimittaminen. Tämä lähtökohtaisesti parantaa energiantuotannon taloudellisuutta ja vähentää ympäristöhaittoja. [VALOR, s. 3/32].

Järjestelmätason hyötyjen ja niiden ennakoitavuuden maksimoinnin kannalta kysyntäjouston ohjaus pitäisi olla kaukolämpöyhtiöllä. Tämä tarkoittaa, että kaukolämpöyhtiö antaa signaalin, jonka mukaan kysyntäjoustojärjestelmään liittyneet kiinteistöt toteuttavat kaukolämpötehon hetkellistä tarvetta alentavia toimenpiteitä mahdollisimman ennakoitavalla ja asukkaiden kokeman palvelutason säilyttävällä tavalla. Jotta asiakkaan kokema palvelun laatu ei heikkenisi havaittavasti, toteutus on järkevää hoitaa alentamalla tai rajoittamalla patteriverkoston veden lämpötilaa hetkellisesti – ei ilmanvaihdon tai lämpimän käyttöveden rajoituksin. [VALOR, s. 3/32].

4.5.1.4 Kaukolämmön kysyntäjouston tekninen ratkaisukuvaus

Seuraavassa kuvassa on esitetty KLKJ-ratkaisun elementit.



Kuva 27. KLKJ-ratkaisun elementit.

1. Kunkin energiayhtiön liiketoimintaa johdetaan useilla toisiinsa liittyvillä järjestelmillä. KLKJ-kokonaisuudessa voimalaitosten optimaalista tuotantoa ohjataan energianhallintajärjestelmällä. KLKJ-kokonaisuuteen liittyy myös ainakin laskutusjärjestelmä sekä asiakkaille tarjottavat siihen liittyvät sähköiset palvelut. Jo ennestään jokaisessa kiinteistössä on energiayhtiön mittauskeskus, joka tuottaa kaukolämmön laskutustietoa erilliseen luentajärjestelmään.
2. Voimalaitoksia ohjataan niiden omista valvomoista käytössä olevan automaatiojärjestelmän avulla.
3. Alueellisia lämpökeskuksia käynnistetään tarpeen mukaan ja niitä ohjataan tyypillisesti suurimpien laitosten valvomoista käsin.

4. Energiayhtiön taustajärjestelmät on integroitu riittävällä tasolla KLKJ-taustajärjestelmiin. Kentältä noudetaan ainakin kiinteistökohtaista olosuhdetietoa. Tätä tietoa tulee toisaalta IoT-operaattorin järjestelmistä (huoneistotieto) sekä toisaalta suoraan lämmönjakohuoneiden ohjausyksiköiltä. On myös mahdollista, että Energiayhtiö lähettää kiinteistöjen suuntaan ohjaustietoa, mikäli sellaisia toimintoja palveluun sisältyy.
5. Kiinteistön lämmönjakokeskuksen yhteyteen liitetään KLKJ-palvelun tapauksessa erillinen tietoverkkoon liitetty ohjausyksikkö, ellei siellä sellaista jo ollut. Ohjausyksikkö voidaan liittää esimerkiksi tavallisella 4G-modeemilla, operaattorin M2M-liittymällä tai kiinteistön omalla internet-yhteydellä.
6. Kiinteistöstä kerätään olosuhdetietoa huoneistokohtaisen tavoitelämpötilan seuraamiseksi ja asumisolosuhteiden laadun varmistamiseksi. Oleellista ovat anturien hyvä hinta-laatusuhde (mittauksen luotettavuus), yleisesti langattomuus ja signaalin hyvä eteneminen kiinteistön rakenteissa, helppo asennettavuus sekä pitkäikäinen pariston kesto. Näin ollen teknologioiksi on ainakin aiemmin valikoitunut yleisesti Sigfox tai LoRa. Olosuhdetieto voidaan kerätä paikalliseen keskittimeen tai suoraan IoT-operaattorin pilveen.

Kiinteistön järjestelmäkomponentteja on esitetty tarkemmin seuraavassa kuvassa.

Kuva 28. Kiinteistön järjestelmäkomponentteja.

4.5.1.5 Kaukolämmön kysyntäjouston kyberturvallisuusriskejä

Energiayhtiö

Energiayhtiön kannalta KLKJ tuo seuraavia kyberturvallisuusriskejä, mikäli hyökkääjä onnistuu:

- Vaikuttamaan energiayhtiön tuotantolaitosten tai kaukolämpöverkon optimaaliseen toimintaan esimerkiksi olosuhdetietoja vääristämällä.
- Hyödyntämään KLKJ-palvelun ja energiayhtiön muiden järjestelmien välisiä integraatioita lateraalisen etenemisen kanavana esimerkiksi laskutus- tai jopa automaatiojärjestelmien suuntaan.
- Tunkeutumaan palveluun liitettyihin kiinteistöihin.
- Tunkeutumaan itse KLKJ-palveluun ja pääsemään käsiksi siellä olevaan tietoon.
- Tunkeutumaan KLKJ-palveluun liittyvien kumppanien järjestelmiin ja sitä kautta laajemmalle.

Energiayhtiön kannalta kaikki edellä mainitut aiheuttavat merkittävän taloudellisen riskin sekä myös imagohaitan. KLKJ-palvelukokonaisuuteen liittyviä tietoturvapuutteita voi olla myös vaikea

korjata tai rajoittaa, mikäli korjaukset edellyttävät kiinteistöissä ja huoneistoissa tehtäviä toimenpiteitä. *Mitä muita energiayhtiön riskejä tunnistat?*

Kiinteistöt

Kiinteistöjen kannalta KLKJ-palveluun liittyminen tuo seuraavia kyberturvallisuusriskejä:

- Kiinteistön omaa taloautomaatiota joudutaan avaamaan aiempaa enemmän internetiin.
- Kiinteistön muut järjestelmät voivat vaarantua, mikäli hyökkääjä pääsee KLKJ-palvelun kautta kiinteistön tietoverkkoon.
- Kiinteistön lämmityksen toiminta voi tulla myös entistä riippuvaisemmaksi ulkopuolisesta tahosta.

Mitä muita kiinteistöjen riskejä tunnistat?

Asukkaat

Kerrostaloasukkaat eivät yleensä suoraan liity KLKJ-palveluun vaan energiayhtiö tekee sopimuksen taloyhtiön kanssa. Näin ollen kaikki asukkaat eivät välttämättä ole edes tietoisia siitä, että heidän asuntonsa liittyy tämän tyyppisen palveluun. Omakotikiinteistöjen asiakkaat ovat tietoisia palvelusta ja voivat jopa vaikuttaa itse valittuihin teknisiin ratkaisuihin.

Kaikkien asukkaiden kannalta KLKJ-palvelu muodostaa ainakin yksityisyydensuojaan liittyvän riskin, mikäli huoneistokohtaisten olosuhdetietojen katsotaan kuuluvan yksityisyydensuojan piiriin. Mahdollinen ongelma voi olla myös tasapuolisuuden vaatimus, mikäli talon kaikkien asuntojen olosuhdetietoa ei seurata samalla menetelmällä ja tarkkuudella.

Riskinä voi olla myös KLKJ-palvelun kautta kiinteistön muita järjestelmiä vastaan hyökkääminen siten, että se aiheuttaa asukkaille haittaa. *Mitä muita asukkaiden riskejä tunnistat?*

Mitä edellä mainittujen riskien realisoitumiseen vaikuttavia hyökkäysvektoreita tunnistat? Miten kyberturvallisuusriskejä voisi pienentää poistamalla tai rajoittamalla tunnistettuja hyökkäysvektoreita?

4.5.2 Tarkastuslista teknologiatoimittajien IoT-pilottien suunnittelulle

Energiayritysten IoT-teknologioiden käyttöönotto edellyttää monitahoisia pilottiprojekteja, jotka tulee suunnitella ja toteuttaa huolellisesti.

Kohderyhmä: Energiayritysten liiketoimintajohdon ja kehitystiimien tueksi niiden etsiessä ja arvioidessa yritykselleen soveltuvia IoT-ratkaisuja, järjestelmiä ja palveluja. Tarkastuslista on tarkoitettu erityisesti IoT-ratkaisuja suunnittelevien, arvioivien ja testaavien asiantuntijoiden käyttöön.

Tarkoitus: Tarkoituksena on helpottaa energiayritystä arvioimaan IoT-teknologiatoimittajia ja heidän ratkaisujensa soveltuvuutta jatkuvuudenhallinnan näkökulmasta. IoT-palveluyritysten kyvykkyydet ja ratkaisujen ominaisuudet paljastuvat (rajattujen) pilottiprojektien kautta. Tämä tarkastuslista nostaa esiin tärkeimpiä pilottien suunnittelussa huomioitavia seikkoja.

Tausta: IoT-pilottihankkeiden suunnittelu ja toteutus voivat näennäisestä yksinkertaisuudestaan huolimatta olla vaikutuksiltaan varsin monitahoisia projekteja, joten suunnitteluun kannattaa varata riittävästi aikaa. Kyberturvallisuuteen ja jatkuvuuteen liittyvien vaikutusten ja riippuvuuksien selvittäminen saattaa edellyttää hyvinkin erilaisten kumppanien ja asiantuntijoiden konsultointia pilotin kuluessa. Useimmilla energia-alan PK-yrityksillä on vaikeuksia luotettavasti ja omin neuvoin selvittää kaikki tärkeimmät uudet riippuvuudet, joita uudet IoT-ratkaisut tuovat tullessaan.

Esimerkkejä IoT-ratkaisujen mukanaan tuomista uusista riippuvuuksista ja epävarmuuksista:

- *Miten uudet langattomat IoT-anturit vaikuttavat muiden tarpeellisten radioverkkojen kuuluvuuteen?*
- *Miten paljon IoT-järjestelmän päivittäminen vaikuttaa muiden järjestelmien tai verkkojen toimintaan?*
- *Mitä uusia tietokantoja uudesta IoT-toiminnosta syntyy?*
- *Mihin kaikkialle dataa kerätään ja kenellä tietoihin on oletusarvoisesti pääsy?*

Tällaisten kysymysten selvittämiseen tarvitaan usein vähintään välillistä apua teknologiatoimittajalta. Käytännössä IoT-ratkaisutoimittajia voidaan parhaiten arvioida erilaisten IoT-pilottiprojektien yhteydessä, kun niihin sisällytetään myös arviointiosuus.

Tarkastuslista

Seuraavassa esitetään lyhyt tarkastuslista teknologiatoimittajien kanssa toteutettavien IoT-pilottiprojektien suunnittelulle.

- CASE-MÄÄRITTELY: Määrittele IoT-pilotin käyttötapaukset yhdessä liiketoimintojen kanssa ja dokumentoi ne hyvin. Kommunikoi käyttötapaukset hyvissä ajoin teknologiatoimittajille.
- PILOTIN TAVOITTEET: Selvitä teknologisen pilotin tavoitteet etukäteen ennen pilotin käynnistämistä. Näin voit arvioida pilotin eri vaiheiden onnistumista heti alusta alkaen. Tavoitteenasi voi olla esimerkiksi seuraavien asioiden parempi ymmärtäminen tai todentaminen käytännössä:
  - Teknologiaratkaisun soveltuvuuden ja toimivuuden todentaminen käyttötapauksiasi vastaan
  - Teknologiaratkaisun eri elementtien toiminnan ja kokonaisuuden parempi ymmärtäminen
  - Yrityksesi yleisen IoT-ratkaisumallin kirkastaminen
  - Teknologiatoimittajan kyberturvallisuuteen liittyvän osaamisen ja kyvykkyyden todentaminen käytännössä
  - Teknologiatoimittajan kyberturvallisuusosaamisen ja soveltuvuuden kehittäminen pitkällä tähtäimellä (jos kyseessä on tuleva kumppanuus)
- UUDET RIIPPUVUUDET: Selvitä toimittajan avustuksella mitä uusia riippuvuuksia (teknologiset, operatiiviset) IoT-ratkaisu tuo teille?
  - Uudet järjestelmärajapinnat ja pilvipalvelut (omistaja, ylläpitäjä)
  - Uudet tietokannat (omistaja, ylläpitäjä)
  - Ekosysteemit (mitä uusia ekosysteemejä ratkaisun mukana tulee, kehen ekosysteemeissä luotetaan, miten niitä kehitetään, ketkä niitä ylläpitävät, millaisia ekosysteemien elinkaaret ovat)
  - Uudet sopimukset (vastuut, sitoumukset, kolmannet osapuolet)
  - IoT-yhdyskäytävät (omistaja, ylläpitäjä)
  - Uudet sovellukset (omistaja, ylläpitäjä)
  - Kyberuhat joita uuteen kokonaisuuteen voi liittyä, joita tulee seurata, ja joita vastaan tulee suojautua
- TEKNOLOGIAN TOIMIVUUS: Koesta pilotissa käytettyjen ratkaisujen vaikutukset eri tilanteissa:
  - Radioverkkojen toimivuus normaali- ja erikoistilanteissa
    - asennuksissa, päivityksissä,
    - vikatilanteissa, ja
    - erilaisten poikkeavien tapahtumien aikana
  - Arkkitehtuurin skaalautuvuus, mikäli käyttöä laajennetaan nopeasti
  - IoT-alustan käytön aikainen toimivuus ja käyttökelpoisuus tarpeeseen. Loppukäyttäjän kokema sovellusten toiminta ja palvelukokemus
  - Yhteensopivuus aiemmin rakennettujen ja tulevien ICT-järjestelmien ja verkkojen kanssa
- YHTEISTYÖN TOIMIVUUS: Arvioi pilotissa koko ajan sitä, miten toimittaja kykenee toimimaan yhteistyössä juuri sinun yrityksesi kanssa:
  - Käyttötapausten ymmärrys ja huomiointi pilotin aikana
  - Vaatimusten ymmärrys ja huomiointi pilotin aikana
  - Palvelualttius: palvelun saanti ja laatu erilaisissa ongelmatilanteissa
  - Korjausten ja päivitysten saanti, kun haavoittuvuuksia ilmenee
  - Ylläpitotoimien aikataulutuksen joustavuus
  - Suhtautuminen mahdolliseen yhteiseen kehittämiseen ja yleisiin järjestelmän kehitysehdotuksiin

Luku 5

YHTEISTYÖN KEHITTÄMINEN KYBERTURVALLISUUDEN ALUEELLA

Kuva: iStock

5. YHTEISTYÖN KEHITTÄMINEN KYBERTURVALLISUUDEN ALUEELLA

Kyberturvallisuuden kehittäminen on kokonaisvaltaista työtä, jossa tarvitaan monipuolista osaamista ja erilaisia taitoja. Kokonaisvaltaisena kehittämisenä ei enää pidetä esimerkiksi sellaista suunnittelua, jossa suurin osa voimavaroista käytetään vuodesta toiseen järjestelmien teknisen tason eristämiseen ulkomaailmasta esimerkiksi kallein palomuurein, IDS/IPS- ja virustorjuntaohjelmistoin. Erilaisia teknisiä turvaelementtejä tarvitaan ja niiden hyvästä ylläpidosta täytyy huolehtia. Silti oman henkilöstön sekä kumppaniverkoston kyberturvallisuustietoisuus ja säännöllinen harjoittelu ovat nousseet tärkeimmiksi kehityskohteiksi varauduttaessa energiayrityksen tietojen kalastelu-, vakoilu- ja soluttautumisyrityksiin. Useimmiten hyökkääjä pääsee kehittyneiden teknisten muurien ohitse ihmisiä huijaamalla, joten fokuksen on oltava ihmisten kybertietoisuuden ja -osaamisen kehittämisessä.

Toiseksi tärkeäksi asiaksi on noussut sektorilähtöinen kyberturvallisuuden kehittäminen, joka on osoittautunut erittäin hyväksi lähestymistavaksi monestakin syystä:

- Kokemuksemme mukaan energiatoimialan ihmiset saavat parasta tukea kyberturvallisuuden kehittämiseen erityisesti vertaistuen avulla toisiltaan.
- Toimialan sisäinen luottamus on erinomainen pohja arkaluontoisenkin keskustelun synnyttämiselle esimerkiksi toteutuneista uhkista.
- Kyberturvallisuutta ei voida kehittää energiasektorille ilman toimialatuntemusta, sillä ilman sitä tehdään kyberturvallisuuden virheinvestointeja.
- Toimiala määrittelee parhaiten itse kyberturvallisuutensa käyttötapaukset. Vasta tämän jälkeen soveltuvat turvaamisratkaisut voidaan määrittää.
- Kyberturvallisuustuotteet ja palvelut kehittyvät kullakin toimialalla esitettyjen tarpeiden kautta.
- Myös kyberturvallisuusosaajat tarvitsevat sektoriosaamista, jotta he pystyisivät auttamaan energiayritysten kyberturvallisuuden kehittämistä käytännöllisellä tavalla.

Erinomaista luottamusta osoittaa, mikäli yhteistyö kehittyy koko sektoria hyödyttäviksi pilottiprojekteiksi ja demonstraatioiksi asti, joissa yhteisesti pohdittuja ongelmia ja käyttötapauksia ratkotaan ja koestetaan yhteistyössä muiden toimijoiden kanssa. Tämä tuo konkreettista hyötyä useimmille energia-alan yrityksille, jotka pohtivat esimerkiksi millaisia menetelmiä, työkaluja, kumppaneita tai palveluja heidän kannattaisi omassa kyberturvallisuuden kehittämistyössään ja omassa toimintaympäristössään käytännössä hyödyntää.

Lopuksi korostamme sitä tosiseikkaa, että luottamus perustuu käytännössä aina henkilöiden väliseen yhteisymmärrykseen ja luottamukseen. Mikäli yritys osallistuu johonkin luottamukselliseen tiedonvaihtoryhmään, on syytä varmistaa tehtävään allokoitavien henkilöiden (esim. pääkontakti ja varahenkilö) saatavuus ja yhteistyöhalukkuus.

5.1 ISAC-ryhmien perusteet ja käytännöt

5.1.1 Mitä ISAC-ryhmät oikein ovat ja mikä on niiden tarkoitus?

Suomessa Liikenne- ja viestintävirasto Traficomin osana toimiva Kyberturvallisuuskeskus ja sen tilannekuva- ja verkostopalvelut auttavat eri toimijoita ylläpitämään ja kehittämään tietoturvallisuuttaan [TILANNE]. Palvelun erilaisissa vuorovaikutteisissa yhteistyöverkostoissa eri yhteistyöryhmien jäsenet voivat organisaationsa luonteesta riippuen tarjota verkoston hyväksi esimerkiksi asiantuntemustaan, analyysiresursseja, tietolähteitä tai omia verkostojaan ja kansainvälisiä yhteyksiä.

Toimialakohtaiset tietoturva-asioiden tiedonvaihtoryhmät (*ISAC, Information Sharing and Analysis Centre*) ovat eri sektoreille perustettuja valtakunnallisia organisaatioiden välisiä yhteistyöelimiä, joiden toiminta perustuu säännöllisiin tapaamisiin sekä yhdessä sovittuihin toimintamalleihin ja osallistujiin. Tiedonvaihtoverkostojen tarkoitus on mahdollistaa tietoturva-asioiden luottamuksellinen käsittely osallistujien kesken sekä tähän perustuva organisaatioiden tietoturvaosaamisen li-

sääminen. Toimialakohtaisissa tiedonvaihtoryhmissä osallistujat käsittelevät tietoturvaan liittyviä asioita ja ilmiöitä luottamuksellisesti ja samalla organisaatioiden tietoturvaosaaminen kehittyy laajemminkin. Verkostoissa jaettu tieto hyödyttää samalla koko Suomen tilannekuvaa.

Energia-alan tiedonvaihtoryhmä on toiminut erityisen mallikelpoisesti, joten Kyberturvallisuuskeskus palkitsi energia-alan tiedonvaihtoryhmän (E-ISAC) kesällä 2018 Tietoturvan suunnannäyttäjä -palkinnolla. E-ISAC-ryhmä on alusta saakka ollut aktiivinen tiedonjakofoorumi, jossa jäsenet ovat vaihtaneet hyviä ja huonoja kokemuksiaan kiitettävällä tavalla [VERKOSTOJA].

Kyberturvallisuuskeskus ylläpitää ainakin seuraavien toimialojen valtakunnallisia tiedonvaihtoryhmiä:

- Elintarviketuotanto ja -jakelu
- Energia-ala
- Internet-palveluntarjoajat
- Kemia ja metsäteollisuus
- Logistiikka- ja liikenne
- Media
- Pankit
- SOTE
- Valtionhallinto
- Vesi

5.1.2 ISAC-ryhmän hyödyt

Valtakunnallisissa ISAC-ryhmissä on jo käytössä useita hyviä toimintatapoja, jotka auttavat ryhmän sisäisen luottamuksen kehittämisessä ja luottamuksellisen tiedon jakamisessa. Tärkeimpiä energia-alan (E-ISAC) ryhmässä käytettyjä hyviä toimintatapoja ovat esimerkiksi:

- Kokousten isännöinnin vuorottelu.
- Kyberturvallisuuskeskuksen toimiminen sihteerinä.
- TLP-koodiston käyttö luottamuksellisen aineiston jakamisessa.
- Teemakokousten pitäminen. Kokouksissa pidettäviin esityksiin tai alustuksiin pyritään aina valmistautumaan hyvin.
- Ylläpidetään tarpeen mukaan aktiivista viestintää myös kokousten ulkopuolella.

E-ISAC ryhmän jäsenet ovat kokeneet ainakin seuraavia hyötyjä:

- Ymmärryksen kasvu
  - Löytynyt hyvä motivaatio kehittymiselle ja kehittämiselle
- Luottamus
  - Riippumattomien luotettavien kumppaneiden määrä kasvanut
  - Myös itseluottamus löytyi verkoston avulla ja siirtyi kokonaisuuden kehittämiseksi ja käytännön tekemiseksi
- Ryhmä toimii ajatuslähteenä
  - Rakentuu, laajentuu ja vahvistuu oman aktiivisuuden kautta ja auttaa kehittämisessä, priorisoinnissa ja käytännön toteutuksessa.
  - Tutkija riippumattomuuden takuumiehenä
- Tulokset
  - Kymmeniä uusia hallinnollisia ja teknisiä toimenpiteitä.
  - Tietoturvallisuus parantunut kaikilla osa-alueilla.

5.1.3 Kannattaisiko perustaa alueellisia ISAC-ryhmiä?

Edellä listatut ISAC-ryhmät ovat valtakunnallisia ryhmiä, joissa osallistujien lukumäärä on tyypillisesti noin 10-20 osallistuvaa henkilöä / yritystä. Mikäli ryhmän kokoa kasvatetaan tätä suuremmaksi, alkaa ongelmaksi muodostua luottamuspula. Käytännössä tämä tarkoittaa sitä, että ryhmässä käytävä keskustelu muuttuu yleisluontoisemmaksi tiedonvaihdoksi, eikä esimerkiksi omassa yrityksessä tapahtuneista ongelmista enää välttämättä haluta kertoa muille, sillä isommasta ryhmästä arkaluontoinen tieto saattaa helpommin levitä ryhmän ulkopuolelle. Ryhmään osallistuvan henkilön vaihtuessa luottamusta saatetaan joutua rakentamaan uudelleen lähes alusta alkaen ja jopa koko ryhmän toimintakyky saattaa heiketä joksikin aikaa. Yksi tapa varmistaa luottamuksen jatkuvuus on toimia kutsuperiaatteella, eli ryhmä valitsee sisäisesti kuka seuraavaksi soveltuisi ryhmän uudeksi jäseneksi.

Suomessa on satoja energia-alalla toimivia PK-yrityksiä, joille olisi erityisen tärkeää päästä säännöllisesti osallistumaan E-ISAC -tyyppisen ryhmän toimintaan ja täten oppimaan alan edelläkävijöiltä sekä erityisesti vertaistuen kautta.

Kannattaisiko tulevaisuudessa perustaa ”alueellisia energia-alan ISAC-ryhmiä”, jotta verkostotyyppisen tuen tai palvelun piiriin saataisiin kaikki tällaista apua tarvitsevat yritykset? Vastaus esitettyyn kysymykseen ei ole yksinkertainen. Tämä johtuu muun muassa seuraavista seikoista:

- ISAC-ryhmien toiminta perustuu pitkälti vapaaehtoisuuteen. Edelläkävijä- tai vertaistukeen ei voida pakottaa ketään yksilöitä tai yrityksiä.
- Suomessa teollisuuden ja energia-alan kyberturvallisuuteen liittyvää osaamista on rajallisesti saatavilla.
- Verkostoituminen voi lisätä työmäärää ainakin alkuvaiheessa, kunnes siitä saatavat hyödyt ylittävät verkostoitumiseen käytetyn ajan. Osallistuminen perustuu koettuun hyötyyn, ei määräykseen osallistua.
- Yritysten salassapitokäytännöt saattavat estää luottamuksellisen tiedonvaihdon osapuolten kesken.

Toisaalta alueellisten energia-alan ISAC-ryhmien perustamista puoltavat mm. seuraavat mahdollisuudet:

- Yleensä eri alueilla on muutamia edelläkävijäyrityksiä, jotka voivat olla halukkaita kehittämään oman alueensa kumppaniverkoston kyberturvallisuutta laajemminkin.
- Nykyisten kumppanuuksien luottamusta voitaisiin parantaa kyberturvallisuuden kehittämiseen liittyvällä yhteistyöllä.
- Mikäli kyberturvallisuuteen liittyvä energia-alan alueellinen yhteistyö käynnistettäisiin, niin siitä alalle voisi viritä muutakin yhteistä kehitystyötä.

Projektin kuluessa olemme saaneet useita signaaleita siihen suuntaan, että energiayritykset tarvitsevat yhä enemmän myös alueellista yhteistyötä. Yhteistyöverkostoihin perustuvan tuen piiriin olisi hyvä saada ainakin kipeimmin tällaista apua tarvitsevat yritykset. Hyvän alueellisen yhteistyön synnyttämiseksi ja toteuttamiseksi tarvitaan todennäköisesti ainakin seuraavia asioita:

- Hyödynnetään jo nykyisin spontaanisti toimivien alueellisten (energia-alan) kyberturvaverkostojen opit ja kokemukset
  - Jyväskylä, Mikkeli & Rovaniemi?
  - Huomioidaan myös Kaupunkiverkot KV11-ryhmittymän opit
- Nimetään alueelliset vetäjät jotka toimivat toiminnan vetureina
  - Kenen tulisi nimetä alueelliset vetäjät ja millä mandaatilla?
  - Vetäjiksi esim. sopivat ja tehtävään halukkaat energiayritykset tai viranomaistahot (Traficom?)
- Ymmärrys alueellisen tuen tarpeista ja lähtökohdista
  - Alueelliset suunnittelupalaverit, joissa kerätään tarpeet
- Valtakunnallinen tuki työlle
  - Esim. Traficom ja E-ISAC auttavat mahdollisuuksien mukaan?
- Käynnistys projektimuotoisesti
  - Käynnistetään muutamia alueellisia ISAC-ryhmiä ensin, jotta opittuja toimintatapoja ja tuloksia voidaan monistaa muillekin

Nykyisin toimivat valtakunnalliset ISAC-ryhmät toimivat pääosin varsin perinteisillä tavoilla, kuten pitämällä fyysisen läsnäolon vaativia kokouksia ja mahdollinen lisätuki esimerkiksi sähköpostiviestinnän kautta. Tähän on tietysti hyviä syitä:

- Luottamus syntyy ja säilyy yleensä parhaiten silloin, kun ollaan fyysisesti samassa paikassa ja tehdään yhdessä hieman muutakin kuin turvallisuustyötä.
- Henkilöiden sitoutumisen tason havaitsee helpommin paikan päällä kuin etäkokouksissa.
- Viestintä: Kaikki käyttävät yleensä sähköpostia, mutta eivät ehkä voi sitoutua käyttämään samoja sähköisiä ryhmätyötiloja.

Toisaalta yleinen kehitystoiminta ja yhteistyö ovat tänä päivänä siirtymässä koko ajan enemmän tietoverkkolähtöiseksi toiminnaksi. Etätyöskentelyä hyvin tukevia (•) ja toisaalta mahdollisesti haittaavia (sisennetty) seikkoja ovat:

- Joustava ryhmätyötilaan liittyminen ja käyttäjän tunnistaminen
  - Mahdolliset huijausyritykset (esim. O365-tunnusten kalastelu)
  - Kuka omistaa työtilaan kertyvän datan ja suojelee sitä?
- Mahdollisuus joustavaan palavereihin osallistumiseen
  - Mutta miten käy henkilökohtaisen sitoutumisen, tuleeko vapaamatkustajia?
- Ryhmässä tehty työ tulee helpommin ja välittömämmin dokumentoitua
  - Miten estetään tietovuodot?
  - Miten tiedon saa myöhemmin poistettua?
  - Miten poistuvien jäsenten antamat tiedot tulisi hävittää, jos he vaativat sitä?
- Jatkuva tietoturvatietoisuuden kehittäminen ja keskustelu
  - Informaatiotulva, kuluu paljon aikaa?

Tällä hetkellä vaikuttaisi siis siltä, että myöskin energia-alan aluetasolle tarvittaisiin uusia tiedonvaihtoryhmiä. Alueellista luottamusta synnytettäisiin ja ylläpidettäisiin niissäkin perinteisesti paikan päällä pidettävissä kokouksissa ja toisaalta paikallista yhteistoimintaa voitaisiin ketterästi syventää myös sopivia sähköisiä ryhmätyöalustoja hyödyntämällä.

5.2 Energiayrityksen häiriöhallinta, yhteistyö ja varautuminen

Olemme kuvanneet teollisuusautomaation häiriöhallinnan yhteistoimintamallin jo aiemmassa projektissa (kuvaus löytyy KYBER-TEO kirjan luvusta 10) [KYBER-TEO]. Se antaa varsin kattavan kuvan siitä, miten myös energia-alalla häiriöiden hallinnan yhteistoiminta voidaan jakaa viiteen mahdollisimman itsenäiseen tasoon:

- Häiriön havaitseminen
- Tutkinta ja luokittelu
- Johdon kommunikointi ja koordinointi
- Lievennys, vastatoimet ja palautuminen
- Opit & parannukset

Tämän kirjan luvussa 3 on jo keskitytty erityisesti *häiriön havaitsemiseen* (mm. omaisuuden hallinta, lokitus, SOC-palvelut, ansoitustekniikat). Toisaalta *Tutkinta ja luokittelu* -vaiheessa toiminta painottuu ICT-asiantuntijoiden suorittamaan tapahtuma-analyysiin, sekä mahdolliseen yhteistyöhön järjestelmätoimittajien ja tietoturvapalveluntarjoajien kanssa. Tarkoituksena on todentaa häiriön aiheuttaja ja sen vaikutukset, jotta johto kykenisi tekemään tilanteen mukaisia päätöksiä heille informoidun tiedon pohjalta.

Johdon kommunikointi ja koordinointi -vaihe on yksi tämän alaluvun fokusalueista. Tarkoituksemme on yksityiskohtaisesti kuvata perusteita siitä, miten päättäjät voisivat entistä paremmin varautua tilanteisiin, joissa kyberhäiriö todella uhkaa energiayrityksen toimintaa? Väitämme, että yritysten varautuminen kehittyy parhaiten yhteistoiminnallisia kyberharjoituksia järjestämällä, joissa keskitytään sisäisen ja/tai ulkoisen päätöksenteon ja viestinnän harjoitteluun kyberhäiriön uhatessa tai toteutuessa.

Ensin kuitenkin pohdimme, että millaisten tietojen palauttamiseen meidän kannattaa kyberhäiriöissä varautua. Tätä varten esittelimme eräässä tämän projektin työpajassa *kannattelevan tiedon* -käsitteen.

5.2.1 Kannattelevan tiedon -käsite

Miksi me itse asiassa suojaamme automaatioon ja tuotantoon liittyviä ICT-järjestelmiä? Käytännössä tarkoituksenamme on suojella tuotannon mahdollistavaa tietoa sekä tuotantoa ohjaavia ja tukevia järjestelmiä kaikin tavoin siten, että toiminta voisi jatkua kaikissa eteen tulevissa häiriötilanteissa mahdollisimman nopeasti.

Kehitimme *kannattelevan tiedon* -käsitteen: tietoja, joiden menetys voi vaarantaa tuotannon järjestelmän palauttamisen (esimerkiksi häiriötilanteesta).

Kuva 29. Jatkuvuuden turvaamista ja varmistamista kannattelevia tietoja

Perinteisin osa-alue on tietenkin jatkuvuuden turvaaminen. Haluamme varautua mahdollisimman hyvin tilanteisiin, joissa energia- tai sen tukijärjestelmän ohjelmistot ja tiedot saastuvat esimerkiksi haittaohjelmatartunnan takia. Tällöin kannattelevana tietona toimivat järjestelmän varmuuskopioiden sisältämä data sekä tietenkin tieto siitä, missä varmuuskopiot sijaitsevat. Lisäksi on muistettava, että voimme luottaa varmuuskopioiden puhtauteen ja aitouteen ainoastaan, jos varmuuskopiot säilytetään hyvin valvotussa tilassa (tai muussa teknisessä ympäristössä). Kannattelevia tietoja etukäteen tunnistamalla ja suojaamalla voimme oleellisesti parantaa kykyämme palauttaa järjestelmät häiriötä edeltäneeseen, turvalliseen tilaan.

Vastaavasti meidän tulee jo etukäteen selvittää ne kannattelevat tiedot, joita ehdottomasti tarvitsemme erilaisissa järjestelmien ylläpidon tehtävissä. Ainakin osa ylläpitoonkin liittyvistä yksityiskohtaisista tiedoista kannattaa säilyttää ainoastaan tätä tietoa tarvitsevien tiedossa (+varahenkilöt), jotta hyökkääjän olisi vaikeampaa esim. etukäteen vakoilla ylläpitäjiä ja tunnistaa ylläpidon heikot kohdat. Jos hyökkääjä saa esim. ylläpitäjän huijauksen ja vakoilun avulla selvitettyä hyökkäyskohteena olevan järjestelmän ylläpidon yksityiskohtaiset toimintatavat ja aikataulut, muuttuu suojausten ja havainnointimenettelyjen ohittaminen paljon helpommaksi.

Kun menemme vielä askeleen pidemmälle varautumisessa, meidän tulee selvittää, mitkä tiedot kannattelevat (kyberuhkien) havaitsemiskyvyn jatkuvaa säilyttämistä sille asetetulla tasolla. Jos esimerkiksi palomuuriemme tai IDS-järjestelmiemme säännöt ja lokit paljastuvat tai joku asiaton pystyy niitä manipuloimaan, niin tuskin enää kykenemme havaitsemaan ainakaan kohdistettua kybervakoilua tai muuta ammattimaista rikollista toimintaa omissa sisäverkoissamme.

5.2.2 Häiriöhallinnan tehtäviä ja yhteistyökohteita

Energiayrityksen tärkeänä tehtävänä on kyetä hallitsemaan erilaisia häiriötä, jotka uhkaavat energian tuotannon, siirron, tai jakelun jatkuvuutta. Häiriöt ovat perinteisesti aiheutuneet sääilmiöistä (kuten myrsky, tykkylumi, jne.), mutta jatkossa myös kyberturvallisuusuhkista aiheutuvat häiriöt on kyettävä havaitsemaan ja hallitsemaan. Seuraavaksi keskitymme pienten ja keskisuurten (PK-) energiayritysten käytännön tehtäviin, joiden avulla erityisesti kyberturvallisuuden häiriöhallintaa toteutetaan. Kyberturvallisuusuhkien havaitseminen on hyvin erilaista toimintaa verrattuna

sääilmiöiden aiheuttamien uhkien havaitsemiseen ja niihin varautumiseen. Lisäksi kyberuhka on yleensä heti havainnosta lähtien täysillä päällä, jolloin tehokkaaseen reagointiinkin tarvitaan ripeyttä ja hyvää osaamista.

5.2.2.1 Energiayrityksen häiriöhallinnan käytännön tehtäviä

Seuraavassa listataan PK-energiayrityksen kyberhäiriöhallintaan liittyviä käytännön tehtäviä havaintojen tekemisestä aina palautumiseen asti. Eri vaiheiden tehtävien tulee voida olla käynnissä ainakin osin myös rinnakkain, mutta tärkeää on huolehtia siitä, että tuotantotoimintaan vaikuttavia päätöksiä tehdään ainoastaan hyvin informoidun tiedon, eli faktojen, pohjalta.

Havaintojen tekeminen seuraavista asioista:

- Tietojen kalasteluyritykset (sähköposti, puhelu, vieras, kumppani)
- Järjestelmä toimii väärin
- Havainto vanhentuneesta tai korjaamattomasta järjestelmästä
- Haittaohjelmahavainto (ilmoitus, kiristys, hidastuminen)
- Epäilyttävä etäyhteys (loki, epäilyttävä muutos)
- Epäilyttävä kirjautuminen/poistuminen
- Epäilyttävä henkilö käynyt tiloissa
- Järjestelmän toiminta muuttunut
- Tietomurtoyritys

Havainnon vahvistaminen ja raportointi:

- Mikäli mahdollista, niin otetaan kopiot kyseeseen tulevista lokeista ja muusta todistusaineistosta mahdollista jatkoanalyysiä varten
- Käydään relevantin järjestelmäasiantuntijan kanssa havainto yhdessä läpi (mitä tapahtui, kenelle, milloin, miten…)
  - Päätellään voiko kyseessä oikeasti olla kyberhyökkäys tai muu häiriö?
- Jos kyseessä vaikuttaisi olevan todellinen häiriö tai sen uhka, niin laaditaan raportti, johon kirjataan:
  - Havainnon tekijä, pvm, aika
  - Havainnon paikka/kohde
  - Tapahtuman yksityiskohdat
- Päätetään miten ja kenelle asiasta raportoidaan sisäisesti (mukaan lukien järjestelmä- tai muu tukikumppani):
- Tiketti, kasvotusten informointi, puhelu, sähköposti?
- Etukäteen tulee olla määritettynä (prosessikuvaus) milloin raportit käsitellään ja miten prosessi etenee

Häiriön potentiaalisten vaikutusten selvittäminen ja priorisointi:

- Tarkempi tapahtuma-analyysi:
  - Häiriön aiheuttajan tarkempi analyysi hyökkäyksen tapahtumien tutkimiseksi ja todentamiseksi
  - Mihin häiriö kohdistuu?
- Mihin kaikkialle häiriöllä voi olla vaikutuksia
- Arvioidaan vaikutukset pahimmassa skenaariossa (esim. jos kohde menetetään)
- Priorisoidaan häiriön vakavuus ja kiireellisyys
- Raportoidaan johdolle analyysin edistymisestä ja tuloksista

Päätöksenteko vastatoimista ja palauttamisesta:

- Ensin päätetään, että ketkä osallistuvat päätöksentekoon?
  - Esim. yritysjohto, liiketoimintajohto, tuotanto, turvallisuus, IT, automaatio, käyttö, kunnossapito, jne.
- Päätökset - Miten ja miksi reagoidaan?
  - Verkkoliikennerajoitus? (esim. irrotus verkosta tai uusi palomuurisääntö häiriön leviämisen estämiseksi)
  - Järjestelmän sammutus (uhkan leviämisen estämiseksi)
  - Päivitys, vikakorjaus? (haavoittuvuuksien poistamiseksi järjestelmästä)
  - Järjestelmän siivous, puhdistus? (haittaohjelman poistamiseksi järjestelmästä)
- Päätökset - Kuka reagoi ja milloin?
  - Esim. järjestelmätoimittaja asentaa haavoittuvuuskorjaukset valvotusti sovittuun aikaan
- Päätökset - Kuka palauttaa ja milloin?
  - Järjestelmien uudelleen asennus?
  - Palautus varmuuskopioista sovittuun palautuspisteeseen (ajankohtaan ennen tartuntaa)?
  - Muutosten testaus?
  - Järjestelmien uudelleen käynnistys?

Palautumisen toimet:

- Toteutetaan toimenpiteet järjestelmien toipumiseksi ja palauttamiseksi
- Prosessien ajaminen alas/ylös
- Palauttamisen toimet dokumentoidaan ja tulokset raportoidaan
- Tapahtuneesta opitaan esim. vuosittaisessa harjoituksessa

5.2.2.2 Häiriöhallinnan yhteistyökohteita

Edellä kuvatuista prosesseista ja tehtävistä nähdään, että tehokas ja faktoihin perustuva häiriöhallinta edellyttää jo perustasollaan varsin paljon sisäistä ja ulkoista kommunikaatiota sekä hyvää yhteistyökykyä. Varautumisen perustaso täytyy tietysti laittaa ensisijaisesti toimintakuntoon esim. yrityksen sisäisten kyberharjoitusten kautta syntyneiden havaintojen ja oppien avulla.

Siinä vaiheessa, kun yrityksessä halutaan kehittää häiriöhallintaan liittyvää varautumistoimintaa vielä pidemmälle, kannattaa sopivan yhteisön mukaan ottamista miettiä tarkemmin. Seuraavassa kuvassa esitetään muutamia mahdollisia häiriöhallinnan yhteistyökohteita eri toimijoille, joihin liittyy sekä yrityslähtöistä tiedonkeruuta (vasemmalla), sekä luottamusverkostolle mahdollisesti jaettavia ”syötteitä” (oikealla).

Kuva 30. Häiriöhallinnan yhteistyökohteita eri toimijoille.

Yllä olevassa kuvassa energiayritys kerää itselleen tarpeellista tietoa eri kanavien kuten mm. toimittajaraporttien, omaisuuskannan ja tuotantohäiriöiden raporttien kautta, mutta voi mahdollisuuksiensa mukaan myös jakaa siitä koostettua kokemustietoa omalle luotetulle yhteisölleen. Mikäli muutkin toimisivat samalla tavalla, niin koko yhteisön energiayritykset saisivat erittäin arvokasta kokemustietoa toisiltaan oman kybertilannekuvan ja kyberturvallisuuden kehittämisen pohjaksi.

Vastaavalla tavalla automaatiotoimittaja kerää mm. järjestelmälokitietoa, järjestelmäraportteja ja haavoittuvuustietoja asiakkaan palvelemiseksi, mutta myös oman vikakorjausprosessinsa kehittämiseksi. Tavoitteena tulee olla nopeampi uusiin uhkiin reagointi ja korjausten jakaminen. Tietoturvayritys taas voisi hyödyntää energiayritysten yksityiskohtaista loki- ja tapahtumatietoa sekä yhdistää sitä kansainväliseen uhkatietoon. Tuloksena kybertapahtumien analysoinnin tarkkuuden kehittyminen ja joskus voisi syntyä uusia uhkien havaitsemiseen liittyviä tunnisteita.

5.2.3 Energiayrityksen häiriöhallinnan suunnittelun tarkastuslistat

Kohderyhmä: Pienten ja keskisuurten (PK) energiayritysten liiketoimintajohdon, viestinnän, järjestelmävastuullisten, käytön, kunnossapidon sekä heidän palvelukumppaniensa tausta-aineistoksi, kun opetellaan ja määritellään kyberhäiriöiden hallinnan ja häiriötilanteista palautumisen käytäntöjä.

Tarkoitus: Tarkoituksena on helpottaa energiayritystä kehittämään käytännössä toimivia kyberhyökkäysten ja muiden häiriöiden hallinnan suunnitelmia ja ohjeita. Tavoitteena on välttää pahimmat tietoturva-, tietosuoja- ja jatkuvuusongelmat erilaisissa häiriötilanteissa.

Tausta: Energiayrityksen yhtenä tärkeänä tehtävänä on kyetä hallitsemaan erilaisia häiriötä, jotka uhkaavat energian tuotannon, siirron ja jakelun jatkuvuutta. Häiriöt ovat perinteisesti aiheutuneet sääilmiöistä (kuten myrsky, tykkylumi, jne.), mutta myös kyberturvallisuusuhkista aiheutuvat häiriöt on kyettävä havaitsemaan ja hallitsemaan. Tässä keskitymme PK-energiayritysten suunnitelmiin ja tehtäviin, joiden avulla erityisesti kyberturvallisuuden häiriöhallintaa toteutetaan.

Kyberturvallisuusuhkien havaitseminen on hyvin erilaista toimintaa verrattuna sääilmiöiden aiheuttamien uhkien havaitsemiseen ja niihin varautumiseen. Kyberuhka on yleensä heti havainnosta lähtien täysillä päällä, jolloin tehokkaaseen reagointiin tarvitaan hyvää osaamista, ripeyttä ja ennakkovarautumista.

5.2.3.1 Häiriöhallinnan toimeenpanon suunnittelu

PK-energiayrityksen häiriöhallinnan toimeenpanon suunnittelussa tulee huomioida seuraavaa:

- Automaation elinkaaren mukainen suunnittelu, jossa mm. havainnointi ja kumppanituki ulottuvat koko elinkaareen
- Häiriöhallinnan tärkeimpien tehtävien määrittely
- Järjestelmien tukipalvelukumppanien tietojen selvittäminen etukäteen ja tarvittavan yhteistyön nopea käynnistäminen:
  - Mitä tukea saatte ulkoiselta ylläpitäjältä sopimuksen mukaan?
  - Millaisilla vasteajoilla sopimuskumppaninne todellisuudessa reagoisivat häiriöön eri tilanteissa?
- Mitä lokitietoa kriittisistä järjestelmistä kerätään ja miten se on saatavillanne?
- Häiriöhallinnan vastuiden ja tehtävien jako
- Häiriöhallinnan kommunikointimallin määrittely
- Häiriöhallinnan suunnitelmien testaus ja parantaminen kyberharjoittelun kautta

5.2.3.2 PK-energiayrityksen kyberhäiriöhallinnan suunnittelun tarkastuslista

Ehdotamme PK-energiayrityksen kyberhäiriöhallinnan suunnittelun tueksi seuraavaa tarkastuslistaa (osa-alueittain):

Johtaminen ja viestintä:

- Kuka teillä johtaa vakavaa häiriötilannetta?
  - Entä vähemmän vakavaa häiriötä tai epäilystä
- Ketkä tukevat häiriön hallintaa ja missä rooleissa?
- Missä tapauksessa ja millä ehdoilla kyberongelmien häiriöilmoitus tehdään?
  - Sisäinen ilmoitus (esim. esimiehelle, liiketoimintajohdolle, turvallisuudelle)?
  - Virallinen ilmoitus? (minkä kokoiset häiriöt ilmoitetaan virallisesti?)
- Mihin kaikkialle teidän tulee tai kannattaa tehdä virallinen häiriöilmoitus (vakavissa häiriöissä)?
  - Minkä kokoiset häiriöt ilmoitetaan Energiavirastolle, Kyberturvallisuuskeskukselle tai Poliisille?
  - Kuka tekee viralliset ilmoitukset?
- Missä vaiheessa siirrytte kriisiviestintätilanteeseen?
- Onko kriisiviestintäsuunnitelmanne ajan tasalla?
- Kuka viestii tiedotusvälineille?
- Kuka johtaa kriisiviestintää poikkeustilanteessa?
- Mitä kanavia pitkin viestitte a) sisäisesti b) sidosryhmille c) medialle d) kansalaisille suoraan

Häiriöiden tunnistaminen:

- Kenen tehtävänä on tunnistaa kyberhäiriöitä tai niiden uhkia?
- Minkä tyyppisiä tapahtumia tulee seurata?
  - Tietojen kalastelu, järjestelmä toimii väärin, vanha tai viallinen järjestelmä, haittaohjelma, epäilyttävä etäyhteys tai kirjautuminen/poistuminen, epäilyttävä henkilö käynyt tiloissa, järjestelmän toiminta muuttunut, tietomurto
- Mitä apuvälineitä häiriöiden tunnistamiseen käytetään?
  - Murtohälyttimet ja hälytysten kirjaaminen
  - Automaattiset lokiseurantatyökalut ja lokien tallennus

- Erityiset tietoverkkoihin ja -järjestelmiin tunkeutumisen havaitsemisjärjestelmät

Havainnon vahvistaminen ja raportointi:

- Miten eri järjestelmien lokeista, käyttöjärjestelmistä ja datasta otetaan kopiot tarkempaa tutkintaa varten?
  - Kuka ottaa ko. kopiot?
- Kuka osaa alustavasti tutkia ja arvioida onko kriittisiin järjestelmiin onnistuttu tunkeutumaan?
  - Tarvitaanko avuksi eri asiantuntijoita eri järjestelmille?
- Onko kehitetty valmis raportointilomake tai raportointijärjestelmä, jonka kautta kyberhäiriöt tai niiden uhka raportoidaan yrityksen sisällä?
- Onko kehitetty valmis raportointilomake tai raportointijärjestelmä, jonka kautta kyberhäiriöt tai niiden uhka raportoidaan tärkeimmille kumppaneille ja asiakkaille?
- Kuka päättää käytännössä, miten ja kenelle kyberhäiriöt tai niiden uhka raportoidaan sisäisesti (mukaan lukien järjestelmä- tai muu tukikumppani):
- Onko etukäteen määriteltynä (prosessikuvaus) milloin raportit käsitellään ja miten prosessi etenee?

Häiriön potentiaalisten vaikutusten selvittäminen ja priorisointi:

- Ketkä osallistuvat häiriön potentiaalisten vaikutusten arvioitiin?
- Ketkä osallistuvat häiriön aiheuttajan tarkempaan analyysiin hyökkäystapahtumien tutkimiseksi ja todentamiseksi?
- Kuka priorisoi häiriön vakavuuden ja kiireellisyysasteen?
- Kuka raportoi analyysin edistymisestä ja tuloksista johdolle?
- Kuka raportoi analyysin edistymisestä ja tuloksista kumppaneille ja tärkeimmille asiakkaille?
- Kuka raportoi medialle, millä ehdoilla ja missä tilanteessa?
- Millaisia vaikutuksia medialle tiedottamisella tulisi olla?
- Millaisia negatiivisia vaikutuksia tiedottamisesta ei saisi tulla?

Päätöksenteko vastatoimista ja palauttamisesta:

- Kuka päättää, että ketkä osallistuvat päätöksentekoon vastatoimista ja palauttamisesta?
- Tuleeko järjestelmän pääkäyttäjän tai ylläpitäjän osallistua päätöksentekoon?
- Missä tilanteessa järjestelmä voidaan irrottaa verkosta häiriön leviämisen estämiseksi?
- Missä tilanteessa järjestelmä voidaan sammuttaa?
- Missä tilanteessa tuotantoprosessi voidaan ajaa alas/ylös?
- Missä tilanteessa järjestelmä uudelleen asennetaan?
- Missä tilanteessa järjestelmä voidaan päivittää (haavoittuvuuksien poistamiseksi järjestelmästä)?
- Missä tilanteessa järjestelmä voidaan vikakorjata (*patching*)?
- Missä tilanteessa järjestelmä palautetaan varmuuskopioista?
- Miten hävinneet asetukset palautetaan varmuuskopioista palauttamisen jälkeen (mikäli varmuuskopiot eivät sisältäneet kaikkia asetuksia)?
- Milloin tehdyt muutokset pitää testata? Kuka testaa?
- Missä tilanteessa järjestelmä voidaan käynnistää uudelleen?
- Missä tilanteessa järjestelmä voidaan puhdistaa (haittaohjelman poistamiseksi järjestelmästä)?
- Onko päätetty kuka käytännössä suojaa järjestelmää hyökkäykseltä ja kuka palauttaa järjestelmän toimintakykyiseksi ja milloin?
- Miten palauttamisen toimet dokumentoidaan ja tulokset raportoidaan?

5.3 Kyberturvallisuusharjoittelu

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus julkaisi äskettäin oppaan kyberharjoitusten järjestämisestä [HARJOITUSOPAS].

Kyberturvallisuusharjoitusten järjestäminen on nykyaikainen ja onnistuessaan erittäin tehokas tapa kehittää yrityksen kyberturvallisuuskyvykkyyttä käytännössä. Tämä johtuu siitä, että osallistujat joutuvat päättämään harjoituksessa annettavien syötteiden vaatimista toimenpiteistä yleensä varsin lyhyessä ajassa ja jopa paineenkin alaisena.

Tällöin tulee luonnollisesti tehtyä myös virheitä, mutta ne usein myös opettavat harjoittelijaa kaikkein parhaiten. Harjoitus paljastaa osallistujille hyvin konkreettisesti, että ei ole helppoa muodostaa selkeää tilannekuvaa tai edes viestiä omasta tilanteestaan tehokkaasta muille, mikäli syötteenä ollaan saatu vaikkapa epävarmaa tai ristiriitaista tietoa. Usein kyberturvallisuusharjoittelu keskittyy erityisesti häiriöhallinnan harjoitteluun, jossa harjoittelijat kohtaavat erilaisia käytännön kyberuhkia ja häiriöitä. Harjoituksissa oman nykyisen osaamisen ja myös kumppaneiden varautumisen puutteet paljastuvat nopeasti.

5.3.1 Kyberturvallisuusharjoittelun tarkoitus

Ennen kuin yrityksessä aletaan suunnitella kyberturvallisuusharjoitusten järjestämistä, niiden suuri merkitys ja tarkoitus koko organisaation kyberturvallisuuden kehittämiselle tulee tiedostaa. Harjoitusten tavoitteet tulee määritellä mahdollisimman selkeästi. Yleensä kyberturvallisuusharjoittelun tarkoituksena on selvittää varautumisen nykytila, sekä erityisesti tunnistaa nykyiseen varautumiseen liittyviä puutteellisia osa-alueita:

- Osaammeko viestiä kyberhäiriötilanteissa oikealla tavalla?
- Miten kumppanimme tulisivat häiriötilanteessa meitä tukemaan?
- Onko organisaatiomme todellisuudessa riittävän hyvin varautunut erilaisiin kyberhäiriötilanteisiin?
- Mitkä ovat nykyisen varautumisemme puutteet?
- Löytyykö harjoituksen kuluessa ”pimeitä alueita”, joiden merkitystä varautumiselle emme ole muistaneet ollenkaan?

Kun varautumisen nykytila ja konkreettiset puutteet saadaan harjoituksen kautta dokumentoiduksi, onnistutaan näihin löydöksiin perustuvat kehittämistoimenpiteetkin paljon helpommin rahoittamaan. Harjoitukseen toivottavasti osallistunut liiketoimintajohtokin ymmärtää nyt paljon konkreettisemmin kaikki ne riskit, joita vastaan kyberharjoittelulla pyritään varautumaan. Kussakin harjoituksessa henkilöstön (ja kumppanien) reagoinnin tarkkailuun kannattaa siis allokoida jopa useampiakin henkilöitä, jotta nykyvarautumisen puutteet tulevat kattavasti kirjatuiksi.

5.3.2 Kyberturvallisuusharjoituksen suunnittelun tarkastuslista

Kohderyhmä: Tarkastuslista on tarkoitettu energiayrityksen kaikille työntekijöille, jotka osallistuvat organisaation oman kyberturvallisuusharjoituksen suunnitteluun. Energiayrityksen liiketoimintajohdon, viestinnän, ICT-osaston, järjestelmävastuullisten, käytön, kunnossapidon sekä heidän palvelukumppaniensa tausta-aineistoksi, kun valmistaudutaan määrittelemään tai tarkentamaan yrityskohtaisia käytäntöjä kyberhäiriöiden hallintaan ja häiriötilanteista palautumiseen.

Tarkoitus: Tarkastuslistan tavoitteena on korostaa harjoituksen ennakkosuunnittelun tärkeyttä, auttaa tavoitteellisten harjoitusten järjestämisessä sekä niiden kohderyhmälähtöisessä räätälöinnissä. Usein tavoitteena on myös oppiminen jo harjoituksen aikana. Tarkoituksena on myös auttaa energiayritystä kehittämään käytännössä toimivia kyberhyökkäysten ja muiden häiriöiden hallinnan suunnitelmia ja ohjeita.

Tausta: Kyberturvallisuusharjoituksen suunnittelu on tehtävä organisaatio- ja kohderyhmälähtöisesti, jotta voitaisiin saavuttaa sille asetetut tavoitteet. Sama harjoitus ei siis käy sellaisenaan kaikille. Suunnittelun organisaatio- ja kohderyhmälähtöisyys tarkoittaa sitä, että harjoitettavan yrityksen organisaatiorakenne, henkilöstön avainroolit ja tehtävänkuvat huomioidaan harjoituksen toteutuksen suunnittelussa. Esimerkiksi harjoituksessa käytettävien skenaarioiden tulisi olla sellaisia, että osallistujat kokevat niiden liittyvän selkeästi myös omiin työtehtäviinsä. Harjoitusskenaarioiden määrittelyyn ja muuhun kyberharjoituksen suunnitteluun kannattaa pyytää apua Kyberturvallisuuskeskuksesta: Kyberharjoitukset@traficom.fi

Kohderyhmän kyberturvaosaamisen taso tulee huomioida harjoituksessa eteen tulevien tilanteiden ja tehtävien suunnittelussa. Mikäli osallistuja ei ymmärrä harjoituksen syötteitä ollenkaan, on harjoitus hänelle liian vaikea. Toisaalta joukossa saa toki olla myös muutamia aloittelijoita, jotka harjoituksen kautta samalla oppivat yksityiskohtia yrityskohtaisen varautumisen laajasta kokonaisuudesta.

Tarkastuslista

Harjoituksen tavoite ja kohderyhmä:

- Harjoituksen tavoitteena voi olla (yksi tai useampia):
  - Organisaation varautumisen nykytilan selvittäminen
  - Varautumisen heikkouksien tunnistaminen, oppiminen
  - Kyberturvallisuuden tärkeyden esilletuonti riskien kautta
  - Osallistujien herättäminen kyberturvallisuuden tärkeyteen
- Harjoituksen kohderyhmä voi olla (yksi tai useampia):
  - Yritys- ja liiketoimintajohto
  - Käyttö- ja kunnossapitohenkilöstö
  - ICT-osasto
  - Operaattorit
  - Kriittisten järjestelmien omistajat

Harjoituksen ennakkotehtävä:

- Harjoituksen tehoa kannattaa lisätä lähettämällä osallistujille ennakkotehtävä hyvissä ajoin ennen harjoitusta
  - Ennakkotehtävä virittää osallistujien mielenkiinnon aihealueeseen ja parantaa harjoitukseen valmistautumista
  - Hyvä ennakkotehtävä palauttaa osallistujien mieliin heidän omat ohjeensa ja kriittiset riippuvuutensa (kumppaneista, järjestelmistä)
  - Ennakkotehtävän tulokset ovat usein luottamuksellisia, sillä niitä voidaan käyttää myös tekijäänsä vastaan (→ ei levitystä oman organisaation ulkopuolelle)

Harjoituksen konsepti:

- Päätä harjoituksen konsepti tavoitteiden ja kohderyhmän mukaisesti:
  - työpöytäharjoitus,
  - skenaarioharjoitus, vai
  - tekninen harjoitus
  - (tai näiden yhdistelmä)
- Työpöytäharjoitus (Yksi uhkaskenaario esitellään → ryhmäpohdinta)
  - Sopii ensimmäiseksi harjoitukseksi, halpa järjestää
  - Sopii johdon harjoitukseksi
  - Yleensä ei ole tekninen eikä monimutkainen harjoitus
- Skenaarioharjoitus (Useita uhkaavia syötteitä jotka etenevät järjestyksessä)
  - Sopii erilaisiin yhteistyötä ja kommunikaatiota edellyttäviin harjoituksiin
  - Vaatii osallistujilta tilannekuvan muodostamista ja nopeaa päätöksentekokykyä
  - Lähes kaikki harjoituskonseptit sisältävät skenaarioharjoituksen elementtejä
- Tekninen harjoitus (syötteet ja vasteet teknisessä ympäristössä)
  - Sopii teknisesti edistyneille osallistujille ja teknisen kyvykkyyden harjoitteluun
  - Vaatii teknisen harjoitusympäristön, joka voi lisäksi olla räätälöity harjoitusta varten
  - Vaatii yleensä paljon ennakkovalmistautumista, työläs järjestää

Harjoituksen skenaariot:

- Mikäli kyseessä on skenaarioharjoitus, niin osaskenaarioiden pohjalta muodostetaan harjoituksen tärkein elementti, uhkaavat syötteet.
  - Syötteiden tulisi muodostaa loogisesti etenevä kokonaisuus ja harjoittelijat yrittävät muodostaa tapahtumista tilannekuvaa
  - Syötteet tulevat tietyltä lähettäjältä ja kohdistuvat vastaanottajiin. Syötteen sisältönä voi olla esim. epäilys, uhka, uutinen, varoitus, haavoittuvuus tai häiriöilmoitus
  - Oleellista on tarkkailla miten osallistujat esim. ryhmänä reagoivat ja viestivät syötteen seurauksena
  - Syötteiden tulee tukea mielellään kahta tai kolmea vaihtoehtoista polkua, jotta harjoituksen kulku voi tarvittaessa mukautua harjoittelijoiden reaktioihin ja päätöksiin

Harjoituksen toteutus:

- Harjoitus voidaan toteuttaa läsnäharjoituksena (*face-to-face*), etäharjoituksena, tai näiden yhdistelmänä
- Läsnäharjoituksen etuja ovat
  - Yhteisen kokemuksen imu → todellisuuden tuntu
  - Osallistujien tutustuminen toisiinsa
  - Ongelmat näkyvät → välitön tuki & harjoitusta voidaan muuttaa

- Etäosallistumisen hyötyjä ja haittoja voivat olla
  - Harjoituksen kattavuutta ja uskottavuutta lisää jos ”koko ketju” joutuu reagoimaan skenaarioiden tapahtumiin
  - Huomio voi keskittyä liikaa tekniikkaan, tekniset viiveet
  - Luottamus voi kärsiä etäosallistujien takia (esim. salanauhoituksen pelko)

5.3.3 Kyberturvallisuusharjoitus - Case

Toteutimme toukokuussa 2019 KYBER-ENE 2 projektin yhdessä suunnitteleman kyberturvallisuusharjoituksen noin 50 projektiin osallistuneen henkilön voimin. Tilaisuus koettiin varsin onnistuneeksi ja laajalti myönteisen palautteen perusteella päätimme julkaista ko. harjoituksen suunnitteluun ja toteutukseen liittyviä yksityiskohtia myös tässä kirjassa (ei kuitenkaan luottamuksellista tietoa). Toivomme tämän case-esimerkin rohkaisevan kaikkia energia-alan yrityksiä aloittamaan suunnittelu liittyen räätälöityihin kyberharjoituksiin, joissa omaan varautumiseen liittyvä valmistautuminen viedään käytännön toiminnan tasolle asti. Harjoittelu on mielestämme tehokkain tapa parantaa omia varautumissuunnitelmia myös oikeaa häiriötilannetta peilaten.

Seuraavissa alakohdissa kuvataan siis noin tusinan eri yrityksen kesken toteutettu yhteisharjoitus. Toisaalta yrityskohtaisissa harjoituksissa voidaan haluttaessa keskittyä enemmän yrityskohtaisten toimintamallien ja ohjeiden testaamiseen ja parantamiseen kuin yritysten väliseen yhteistoimintaan. Pääsääntöisesti harjoitus kannattaa kohdistaa oletettuihin heikkouksiin, ei niinkään asioihin jotka jo ovat kunnossa. Luultavasti yrityksen oma toimintamalli tulisi ensin saada kuntoon, jotta voidaan harjoitella uskottavaa yhteistoimintaa ja tehokasta viestintää myös yhdessä muiden toimijoiden kanssa?

5.3.3.1 Harjoituksen tavoite ja kohderyhmä

HARJOITUKSEN IDEA: Tunnistetaan varautumisen ja yhteistoiminnan puutteita sähkönjakelun häiriöön mahdollisesti johtavissa tilanteissa!

TAVOITE: Yhteistyön ja viestinnän toimivuuden koestaminen osallistujayritysten kesken & oman häiriötilannetoiminnan, varautumisen ja kriittisten kumppanuuksien kirkastaminen.

OSALLISTUJAT: Projektiin osallistuvien yritysten luotetut toimihenkilöt ja työntekijät. Lisäksi NDA vaadittiin kaikilta ennen kyberharjoitukseen pääsyä:

- Pääosassa ENERGIAYHTIÖT jotka mukana harjoituksessa
  - Liiketoimintajohto & käyttö- ja kunnossapitovastaavat
  - Toimintatapojen harjoittelu: toiminta uhka- ja häiriötilanteessa
- AUTOMAATIOTOIMITTAJIEN asiakaspalveluhenkilöt
  - Tietoturvatukena myös tietoturvan palveluyritykset
- PALVELUKUMPPANIEN simulointi (harjoituksen tukihenkilöt esiintyivät harjoituksessa tietoliikenne- ja konesalioperaattoreina):
  - Rajallinen tuki uhka- ja häiriötilanteessa (kaikki tarvitsevat tukea yhtaikaa)
  - Esim. korjaukset tulevat palvelusopimuksen mukaisesti tai myöhässä
- TARKKAILU: Lisäksi yksi harjoituksen ulkopuolinen tarkkailija ja yksi edelläkävijäyrityksen edustaja tekivät havaintoja harjoituksen kulusta (molemmat tulivat KYBER-ENE hankkeisiin osallistuneista yrityksistä).

5.3.3.2 Harjoituksen ennakkotehtävä

Luottamuksellinen ennakkotehtävä kyberharjoitukseen osallistuville yrityksille:

1. *Luettele kaksi kappaletta harjoitukseen valitsemaanne yritystason tai voimalaitoksen kriittistä ICT-tukijärjestelmää joiden toiminta saattaisi vaarantua kyberhyökkäyksessä, sekä kummankin tärkein ulkoinen ylläpitäjä.*

Lisäksi selvittäkää itseänne varten etukäteen (tietoa ei tarvitse lähettää):

- Mitä tukea saatte ulkoiselta ylläpitäjältä sopimuksen mukaan?
- Millaisilla vasteajoilla sopimuskumppaninne ehkä todellisuudessa reagoisivat häiriöön eri tilanteissa?
- Mitä lokitietoa yo. kriittisistä järjestelmistä kerätään ja miten se on saatavillanne?

2. *Luettele kaksi kappaletta harjoitukseen valitsemaanne jakeluverkon kriittistä ICT-tukijärjestelmää joiden toiminta saattaisi vaarantua kyberhyökkäyksessä, sekä kummankin tärkein ulkoinen ylläpitäjä eli sopimuskumppani.*

Lisäksi selvittäkää itseänne varten etukäteen (tietoa ei tarvitse lähettää):

- Mitä tukea saatte ulkoiselta ylläpitäjältä sopimuksen mukaan?
- Millaisilla vasteajoilla sopimuskumppaninne ehkä todellisuudessa reagoisivat häiriöön eri tilanteissa?
- Mitä lokitietoa yo. kriittisistä ICT-järjestelmistä kerätään ja miten se on saatavilla?

3. *Palauttakaa mieleenne oman yrityksenne (kyberongelmiin soveltuva) häiriöhallinnan prosessi.*

Lisäksi selvittäkää itseänne varten etukäteen (tietoa ei tarvitse lähettää):

- Kuka johtaa vakavaa häiriötilannetta? Entä vähemmän vakavaa häiriötä tai epäilystä?
- Ketkä tukevat häiriön hallintaa ja missä rooleissa?
- Missä tapauksessa ja millä ehdoilla kyberongelmien häiriöilmoitus tehdään?
  - Sisäinen ilmoitus (esim. esimiehelle, liiketoimintajohdolle, turvallisuudelle)?
  - Virallinen ilmoitus? (minkä kokoiset häiriöt ilmoitetaan virallisesti?)
  - Kenellä on oikeus tehdä mitkäkin viralliset ilmoitukset?
- Mihin kaikkialle teidän tulee tai kannattaa tehdä virallinen häiriöilmoitus (vakavissa häiriöissä)?
  - Minkä kokoiset häiriöt ilmoitetaan Energiavirastolle, Kyberturvallisuuskeskukselle tai Poliisille?
- Missä vaiheessa siirrytte kriisiviestintätilanteeseen?
- Onko kriisiviestintäsuunnitelmanne ajan tasalla?
- Kuka johtaa kriisiviestintää poikkeustilanteessa?
- Mitä kanavia pitkin viestitte a) sisäisesti b) sidosryhmille c) medialle d) kansalaisille suoraan?

5.3.3.3 Harjoituksen eteneminen ja konsepti

Kyseessä oli käsitetasolla pidetty skenaarioharjoitus, joka eteni seuraavassa järjestyksessä:

INTRO: Aluksi esitettiin harjoituksen etenemisen kuvaus → kyseessä on roolipeli!

RYHMIINJAKO: Jako kolmeen ryhmään:

- Ryhmä 1: Energiayritysten osallistujia (4 yritystä)
- Ryhmä 2: Energiayritysten osallistujia (toiset 4 yritystä)
- Automaatiojärjestelmätoimittajien ja tietoturvayritysten ryhmä

ENSIMMÄINEN OSA-SKENAARIO: Kyberuhka havaitaan yrityksissä:

- Tapahtumat annetaan ryhmille lapuilla osaskenaarion mukaisesti edeten (järjestäjät)
  - A. Miten osallistujat reagoivat tapahtumiin yrityskohtaisesti? (näistä tehtiin yrityskohtaiset muistiinpanot)
  - B. Ryhmäkeskustelu ja vastaukset tapahtumiin (näistä tehtiin ryhmäkohtaiset muistiinpanot)
- Yhteenveto: Ryhmät kertovat miten osaskenaarioon reagoitiin ja mitä opittiin: keskustelua yhdessä.

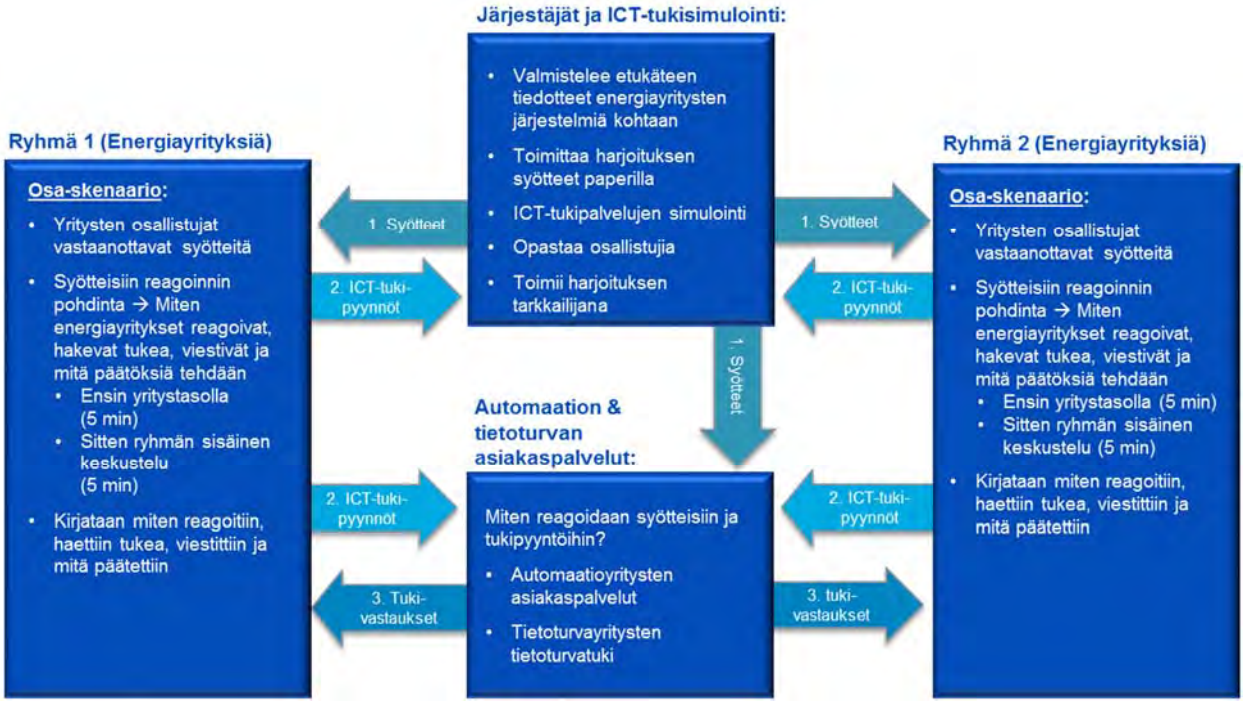
TOINEN OSASKENAARIO: Kyberuhka toteutuu häiriönä energiayrityksen jakeluverkon tukijärjestelmässä:

- Tapahtumat annetaan ryhmille lapuilla osaskenaarion mukaisesti edeten (järjestäjät)
  - A. Miten osallistujat reagoivat tapahtumiin yrityskohtaisesti? (näistä tehtiin yrityskohtaiset muistiinpanot)
  - B. Ryhmäkeskustelu ja vastaukset tapahtumiin (näistä tehtiin ryhmäkohtaiset muistiinpanot)
- Yhteenveto: Ryhmät kertovat miten osaskenaarioon reagoitiin ja mitä opittiin: keskustelua yhdessä.

OPIT JA TARPEET: Sekä yrityskohtainen että yhteinen keskustelu

- Yrityskohtainen keskustelu harjoituksen opeista ja lista oman yrityksen varautumistarpeista
- Tulevien kyberharjoitusten suunnittelu ryhmissä ja ryhmien tulosten yhteinen purku- ja keskustelutilaisuus
- Lopuksi palautelomakkeen täyttö (anonyymisti)

Skenaarioharjoituksemme ryhmäjaon ja viestinnän konsepti oli siis seuraava:



Kuva 31. KYBER-ENE 2 kyberharjoituksen ryhmäjaon ja viestinnän konsepti. Lisäksi energiayritysten ryhmät (1 & 2) saivat vertaistukea toisiltaan.

Järjestäjät lähettivät suunnitellun minuuttiaikataulun mukaisesti syötteitä energiayrityksille (ryhmät 1 ja 2) sekä heidän automaatiojärjestelmiensä asiakaspalveluiden edustajille (lisättynä tietoturvan tukiyritysten edustajilla). Energiayritykset pystyivät sitten tekemään kysymyksiä tai palvelupyyntöjä harjoitukseen osallistuneiden palveluyritysten edustajille koko harjoituksen ajan. Palveluntarjoajat vastasivat kykynsä mukaan. Harjoituksen viestintä toteutettiin kokonaisuudessaan paperilomakkeilla.

5.3.3.4 Harjoituksen skenaariot

Seuraavassa listaamme KYBER-ENE 2 projektin yhteisessä kyberharjoituksessa käyttämämme syötteet aikajärjestyksessä. Hyökkäysuhan alla olleiden järjestelmien tiedot sekä automaatiopalveluntarjoajien, ICT- sekä tietoturvatoimittajien tiedot anonymisoitiin, sillä muutoin emme olisi saaneet tätä listaa julkaista. Huom: syötteissä ”KTK” = Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus.

ENSIMMÄINEN OSA-SKENAARIO: Kyberuhka havaitaan yrityksissä:

9.45: KTK → Kaikille: ”<Tiettyjä yritys- ja voimalaitosjärjestelmiä> vastaan on esiintynyt kohdistettua (käyttäjätunnus, salasana) tietojen kalastelua energia-alalla Suomessa. Kehotamme varovaisuuteen näihin järjestelmiin kirjautumisessa. Kehotamme kirjautumaan etänä esim. automaatio-ohjaukseen ainoastaan, mikäli teillä on MFA-tunnistus käytössä”.

9.55: KTK → Kaikille: ”<Ylläpidon etäyhteystunnuksia> sekä niihin liittyviä <Android-älypuhelimia> (joille tulee etäyhteyksien MFA koodit) on otettu hyökkääjän haltuun suomalaisessa energia-alan palveluyrityksessä. Mikäli epäilette että teidän etäyhteysjärjestelmiinne on tunkeuduttu, niin vaihtakaa niiden salasanat välittömästi. Päivittäkää myös älypuhelimenne (Android, iOS)-käyttöjärjestelmät ja varusohjelmistot välittömästi uusimpiin versioihin ja varmistakaa että niiden suojaus on riittävä.”

10.00: Energiayritysten teleoperaattoreilta → Yrityskohtainen varoitus kullekin energiayritykselle: ”Olemme havainneet merkkejä palveluihimme kohdistetusta kyberhyökkäyksestä, joten pahimmassa tapauksessa vaarana on hyökkäysten leviäminen myös teidän järjestelmiinne.

Koska tilanne on vakava, halusimme heti informoida teitä ja kehotamme myös varovaisuuteen asiakaspalvelustamme tulevien viestien suhteen, sillä niiden manipulointi saattaa olla toistaiseksi mahdollista. Olemme jo ryhtyneet kaikkiin vastatoimiin."

10.05: Järjestäjä → Automaatiojärjestelmätoimittajalle: <Teidän XYZ-järjestelmiä> vastaan on havaittu kohdistettuja kyberhyökkäysyrityksiä voimalaitosautomaatiota ja <esim. AB-pumppausasemia> vastaan. Hyökkäyksissä on yritetty hyödyntää tietoliikenteen häirintää (teleoperaattoriyhteyksiin on kohdistunut palvelunestohyökkäyksiä) sekä käyttämienne operaattoritunnusten ja salasanojen urkintaa.

10.10: Automaatiojärjestelmätoimittaja → Varoitus energiayrityksille: "<Automaatiojärjestelmiämme XYZ> vastaan on havaittu kohdistettuja kyberhyökkäysyrityksiä voimalaitosautomaatiota ja <AB-pumppausasemia> vastaan. Myös muut hyökkäyskohteet Suomessa ovat mahdollisia. Hyökkäyksissä on yritetty hyödyntää tietoliikenteen häirintää sekä operaattoritunnustemme ja salasanojemme urkintaa."

10.20: KTK → Kaikille: "<Tietyistä yritys- ja voimalaitosjärjestelmistä> on löytynyt haavoittuvuuksia." "Järjestelmistämme on löytynyt uusi tietoturvahaavoittuvuus, joka mahdollistaa järjestelmän etäkäytön ja järjestelmämuutokset. Haavoittuvuuteen löytyy korjauspäivitys ja sen voi ladata ko. järjestelmätoimittajilta."

<u>TOINEN OSASKENAARIO</u>: Kyberuhka toteutuu häiriönä energiayrityksen jakeluverkon tukijärjestelmässä:

12.30: KTK → Kaikille: "Konkreettisia hyökkäysyrityksiä kohdistumassa <tiettyjä jakeluverkon käytöntuki- ja valvontajärjestelmiä> kohtaan. Eri SCADA-palvelujen tarjoajat ilmoittavat että ao. häirintää on havaittu:

1. Palvelumme tietoliikennerajapintoja on yritetty häiritä virheellisellä tietoliikenteellä. Häiriöiden lähdettä selvitetään.
2. Järjestelmämme signaaliviestintää on yritetty manipuloida. Aiheuttajaa selvitetään.
3. Operaattoriemme salasanoja on yritetty vaihtaa ilkivaltaisesti. Harkitsemme rikosilmoitusta ja järjestelmämme turvataan jatkossa vahvemmin."

12.38: Järjestäjä → vain <yksi energiayritys>: Valvomossa V1 on havaittu haittaohjelma joka pyrkii muuttamaan ala-aseman katkaisimen asentoa.

12.45: Iltalehti → Kaikille: "<Energiayritysten tiettyjen ICT-tuen ja jakeluverkon käytön tukiyritysten> yksittäiset työntekijät ovat kertoneet, että kyberuhka on todennäköisesti jo levinnyt myös asiakkaiden eli energiayritysten järjestelmiin":

1. "Yksittäisiä virheellisiä paikkatietoja esiintynyt (järjestelmässämme). Vikaa tutkitaan."
2. "Palvelujen tietoliikenteessä on toistuvia häiriöitä. Vikaa tutkitaan."
3. "Tietoliikenne- ja konesalipalveluissa sekä turvallisuusvalvonnassa on toistuvia tietoliikenneongelmia. Vikaa tutkitaan."
4. "Kahden operaattorimme käyttäjätunnuksia oli otettu ilkivaltaisesti haltuun, toiminta palautettiin normaaliksi sulkemalla ko. tunnuksia."
5. "Konesalipalveluiden varmuuskopiointitoiminnossa esiintynyt toistuvia häiriöitä. Vikaa tutkitaan."

13.00: Järjestäjä → vain <yksi jakeluverkon automaatiotoimittajayritys>: <Käyttämänne sähköverkon käytönhallintajärjestelmän (sekä kahden muun automaatiotoimittajan jakeluverkon käytönvalvontajärjestelmien)> näyttöjä pimenee satunnaisesti:

- Joidenkin järjestelmien näyttöruutuja pimenee eikä järjestelmiin useimmiten saa enää etäyhteyttä.
- Tiedonsiirtojärjestelmät näyttävät toimivan edelleen.
- Palvelimet näyttävät toimivan edelleen.

13.00: <Jakeluverkon automaatiotoimittajayrityksiltä> → Varoitus energiayrityksille: "<Asiakaspalvelumme> varoittavat järjestelmiimme kohdistuvista vakavista kyberhyökkäyksistä. Järjestelmät tulee puhdistaa ja asentaa uusimmat päivitykset:

- Järjestelmissä olevaa energiayrityksen dataa saatetaan tuhota.
- Energiayrityksen datan takaisinsaannilla saatetaan kiristää.
- Järjestelmissä olevaa energiayrityksen dataa saatetaan viedä Internetiin

13.05: Järjestäjä → Energiayrityksille: <Tiettyjen jakeluverkon automaatiotoimittajayritysten käytönvalvontajärjestelmien> näytöt pimenevät:

- Järjestelmien näyttöruudut pimenevät eikä järjestelmiin saa enää etäyhteyttä.
- Tiedonsiirtojärjestelmät ja palvelimet näyttävät toimivan edelleen.

5.3.3.5 Harjoituksen pikaohjeet ja tukipyyntölomake

Harjoituksen alussa ja sen aikana osallistujia opastettiin mm. seuraavalla tavalla:

Mihin harjoituksessa keskitytään?

Osallistujat:

- Tärkeintä on sitoutuminen harjoituksen ohjeisiin ja tavoitteisiin, ette saa takertua harjoituksen puutteisiin/vikoihin
- Keskittykää viestintään ja tilannekuvaan eteen tulevissa syötteissä:
  - Ensin yrityskohtainen reagointi: paperille tai sähköisesti (yritys itse dokumentoi)
  - Sitten pienryhmän yhteistä keskustelua (ryhmän sihteeri dokumentoi). Ryhmän vastauksen kirjaaminen (sihteeri kellottaa)
  - Ohjetta voi soveltaa tilanteen mukaan, siten että pienryhmä toimii parhaiten

Toiminnan tarkkailun tavoite:

- Oman toiminnan realistinen kirjaaminen (osallistujat) + esityskalvo (järj.)
- Ulkopuolinen tarkkailija: Ulkopuolisen palautteen saaminen

Tulokset:

- Saatte faktaa nykytilasta kehityksenne pohjaksi
- Viekää tykönänne havainnot käytäntöön – kirjoittakaa oikeasti toimivia varautumisohjeita!

Yrityskohtaisen tukipyyntölomakkeen malli

Template tukipyynnöille (printataan osallistujille)

Yrityskohtainen tukipyyntö

Klo:

Lähettäjä:

Kenelle:

Pyyntö:

Vastaus yritykselle

Klo:

Vastaaja:

Vastaus:

Pyyntö:

Kuva 32. KYBER-ENE 2 kyberharjoituksessa käytetty tukipyyntölomake.

Luku 6

JOHTOPÄÄTÖKSET

Kuva: Shutterstock

6. JOHTOPÄÄTÖKSET

Energia-alan kyberturvallisuutta jo useita vuosia kehittäessämme olemme tehneet seuraavia havaintoja ja johtopäätöksiä.

Osaksi päivittäistä työtä – Kyberturvallisuuden ylläpito ja kehitys on saatava osaksi päivittäistä rutiinityötä. Olemme vahvasti sitä mieltä, että erityisesti energia-alan PK-yrityksen kyberturvallisuus saadaan varsin hyvälle tasolle laittamalla kyberturvallisuuden perusasiat ensin kuntoon. Myös kehittyneiden hyökkäysten onnistuminen heikentyy huomattavasti, mikäli kaikki yrityksen työntekijät ja kumppanit, aina liiketoimintajohtajasta alihankkijana toimivaan vartijaan asti, osaavat omassa työssään toimia tietoturvallisella tavalla. Perusosaamisen ja tietoisuuden kehittämistä ja levittämistä tulee jatkaa, kunnes kaikki energia-alalla toimivat yritykset on saatu ymmärtämään kyberturvallisuuden kasvanut merkitys oman liiketoimintansa jatkuvuudelle ja toteuttamaan tarvittavat toimenpiteet.

Hyvä kehitys saadaan vauhtiin jokseenkin tässä järjestyksessä:

1. johdon tietoisuus kuntoon,
2. nykytilan kartoitus,
3. kehityskohteiden tunnistaminen ja keskustelu,
4. kehitysryhmän perustaminen,
5. vuosisuunnitelma, kehityshankkeiden määrittely,
6. kehittämisen budjetointi, tehtävien ja vastuunjako,
7. tilannekuvan seuranta johdossa.

Verkostojen alati korostuva merkitys – Kyberturvallisuusuhat leviävät tänä päivänä erittäin nopeasti mm. siksi, että rikolliset tahot jakavat erilaisia hyökkäyspalveluja tehokkaasti salatuissa verkkoyhteisöissään. Myös energia-alan yritysten on välttämättä verkostoiduttava keskenään. Tähän on useita hyviä syitä:

1. luottamuksellisen uhkatiedon jakamiseksi yhteisön sisällä,
2. toimivan vertaistuen synnyttämiseksi ja toteuttamiseksi,
3. edelläkävijöiltä oppimisen mahdollistamiseksi,
4. parhaiden käytäntöjen jakamiseksi,
5. hyvien ja huonojen kokemusten jakamiseksi - verkosto antaa turvaa!

”Hyvän verkoston kautta ymmärtää turvallisten käytäntöjen syyt ja vahinkojen kautta synnytetyt opit paremmin kuin lukemalla kymmenen eri tietoturvastandardia.”

Resurssien puute – Vaikka yritysjohdon tietoisuus olisikin kunnossa, ei se valitettavasti aina johda toimihenkilöiden riittävän työmäärän allokointiin kyberturvallisuusohjeiden jalkauttamiseksi käytännön toiminnan tasolle asti. Edes edelläkävijöiden ja vertaistuen avulla ei voida korvata sitä puuttuvaa aikaa, jota kyberturvallisuuskäytäntöjen kehittäminen ja tietoisuuden kasvattaminen yrityksessä vaatii. Esimerkiksi laitoksen ainoa osa-aikainen tietoturvan vastuuhenkilö ei riitä, varsinkin mikäli kenelläkään ei ole aikaa perehtyä turvallisten toimintamallien ja ohjeiden määrittelyyn tai osallistua järjestettyihin koulutustilaisuuksiin.

Tarvitaan laajempaa viranomaistahojen tukea kyberturvallisuuden kehittämiselle. Alan yrityksissä on haluttu jopa todellisia sanktioita niille yrityksille, jotka eivät kykene kehittämään kyberturvallisuuttaan energia-alan kriittisyyden edellyttämälle tasolle. Kyberturvallisuuskeskuksen vetämässä kehitysprojektissa on tarkoitus kartoittaa kotimaisten kriittistä infrastruktuuria tarjoavien organisaatioiden kyberturvallisuuden kypsyystaso, saada ymmärrystä parannuskohteista, sekä tieto siitä mille tasolle organisaatio sijoittuu omaan toimialaansa verrattuna.

Omaisuuden hallinta – Asianmukainen tuotantoteknisen (OT) ja ICT-omaisuuden hallinta on yksi tärkeimmistä lähtökohdista kyberturvallisuusuhkien havaintokyvyn kehittämisessä. Tuntemattoman laitteen oikeaa toimintaa ei voida tarkistaa, mutta kaikkea kriittistäkään omaisuutta tuskin voidaan valvoa aukottomasti koko sen elinkaaren ajan. Siksi tarvitaan OT- ja ICT-kumppaneita ja palveluntarjoajia, joiden osaamiseen voi luottaa ja jotka osaavat toimia kyberturvallisella tavalla kaikissa tilanteissa. Silti eri toimintojen kyberturvallisuuden toteumaa tulisi tänä päivänä kyetä seuraamaan vähintään perustason menettelyin. Eri järjestelmien ja varsinkin etäyhteyksien tapahtumista on generoitava lokimerkintöjä, joiden asianmukaisuutta myös seurataan ammattimaisesti ja säännöllisesti. Lokien hyvä hallinta ei kuulosta monimutkaiselta, mutta sen laaja käytännön toteutus uusine riippuvuuksineen on käytännössä valtava ja moniulotteinen automaation päivitysprojekti. Toisaalta myös ansoitusmenettelyjen kohdistettu hyödyntäminen energia-alalla vaikuttaa edelleen varsin lupaavalta keinolta.

HAVARO on Kyberturvallisuuskeskuksen palvelu, joka havainnoi vakavia tietoturvauhkia ja varoittaa niistä. Huoltovarmuuskriittiset energiasektorin organisaatiot voivat parantaa tietoturvaloukkausten havainnointikykyä ryhtymällä HAVARO:n tai tulevaisuudessa HAVARO2:n asiakkaaksi.

IoT vyöryy – *Internet of things* eli esineiden Internet on paraikaa lyömässä vahvasti läpi myös energia-alan yrityksissä. Mikäli kuluttajien käyttöön tarkoitettuja IoT-laitteita ja pilvipalveluja kytkettäisiin energiayrityksen liiketoiminnan ohjausjärjestelmiin, oltaisiin erittäin vaarallisilla vesillä. Tämä johtuu kuluttajapuolen IoT-ratkaisujen monista heikkouksista:

1. ratkaisut ovat harvoin kokonaisuudessaan tietoturvallisia
2. laitteen tuettu elinkaari voi olla varsin lyhyt ja esim. varusohjelmistopäivityksiä voi olla huonosti saatavilla,
3. halvat pilvipalveluratkaisut eivät skaalaudu yritystason ratkaisuiksi,
4. onnistunuttakaan pilottia ei voi siirtää suoraan tuotantokäyttöön,
5. mukana tulevat ekosysteemit voivat olla hallitsemattomia.

Erittäin tärkeää onkin kyetä ensin määrittelemään yrityksen tärkeimmät omat IoT-käyttötapaukset ja arvioida IoT:n riskejä ensin niiden kautta. Yhtä tärkeää on kyetä arvioimaan ja valitsemaan luotettavat ja turvalliset IoT-kumppanit ja mahdollisesti heidän kauttaan yrityksessä käyttöön otettavat IoT-verkot ja palvelut. Energiayrityksen on luotava oma kaava IoT:n käyttöönotolle, eli kaikkien yritykseen hankittavien ratkaisujen on kyettävä noudattamaan sovittua yleisarkkitehtuuria. Lisäksi IoT-kehityshankkeiden yhteiset pelisäännöt on kyettävä määrittelemään, sekä valvomaan, että kaikki IoT-projekteihin otettavat toimijat kykenevät noudattamaan näitä sääntöjä asianmukaisesti. Ilman näitä sääntöjä ajaudutaan ennen pitkää moniriippuvuuksien kaaokseen.

Yhteistyö ja kyberharjoittelu – Olemme havainneet lukuisia kertoja, että turvallinen toimintatapa ei siirry yrityksen työtekijöiden mieliin kirjoittamalla massiivinen tietoturvapolitiikka taikka yleiskirje kyberturvallisuusuhkien vaaroista. Kyberturvallisuushäiriöt voivat aiheuttaa samanlaisia seurauksia kuin mikä tahansa muu tuotantoon liittyvä häiriö, joten kokonaan uusia häiriöhallinnan prosesseja ei kannata luoda kyberturvallisuuden vuoksi. Kyberturvallisuushäiriöiden tunnistaminen ja ennakoiminen vaativat kuitenkin hyvin eriluonteista osaamista kuin vaikkapa myrskytuhoihin varautuminen. Tämän vuoksi kyberturvallisuusuhkien tunnistamiseksi tulee ottaa käyttöön uudenlaisia havainnointimenettelyjä, sekä perehdyttää työntekijät uhkien uusiin virtauksiin säännöllisesti.

Kyberturvallisuusharjoittelu on erinomainen tapa tunnistaa puutteita energiayritysten henkilöstön jatkuvuuden hallinnan käytännöissä ja osaamisessa. Harjoitus voi osoittaa puutteita esim. kumppaneiden varautumisessa tai ilmetä suoraan vaikeutena hahmottaa omaa tilannekuvaa. Uhka- ja häiriötilanneviestintä on yksi tärkeimmistä asioista, joita voidaan tehokkaasti kehittää kyberturvallisuusharjoituksen oppien avulla. Puutteet voivat löytyä sekä yrityksen sisäisestä (liiketoiminnot, osastot), että yritysten välisestä viestinnästä (kumppanit, alihankkijat). Havainto ja varoitus tietomurrosta tulee valitettavasti edelleen useimmiten liian myöhään ja uhriyrityksen oman havaintokyvyn ulkopuolelta.

Luku 7

TULEVAISUUDEN TARPEET JA JATKOTYÖ

Kuva: Pixabay

7. TULEVAISUUDEN TARPEET JA JATKOTYÖ

7.1 Energia-alan kyberturvallisuus tarvitsee tukea

Energia-ala on ollut maailmalla jo useita vuosia kehittyneiden kyberhyökkäysten kohteena, tunnetuimpina ilmiöinä mm. BlackEnergy, Industroyer, Dragonfly, Havex ja TRITON. Nämä kehittyneet uhat ovat jo pakottaneet suuria kansainvälisiä energiayrityksiä kehittämään kyberuhkiin liittyvää varautumista ja tietoisuustasoa myös Suomessa. Tuen tarve on suurempi pienissä ja keskisuurissa yrityksissä, joiden henkilöstö ei ole vielä verkostoitunut kyberturvallisuuden alueella. Kyberuhat kohdistuvat lisääntyvässä määriin energiaverkoston heikoimpiin lenkkeihin, eli puutteelliset tietoturvaresurssit ja -tietoisuuden omaaviin kumppaneihin ja työntekijöihin. He tarvitsevat selkokielistä ja pitkään jatkuvaa apua alan kokeneemmilta toimijoilta.

7.2 Energia-alan yritysten kyberturvallisuuden kehittämistarpeet

KYBER-ENE 1 ja 2 projekteissa olemme välillä 11/2017 - 06/2019 järjestäneet teema- ja yrityskohtaisissa kehitystyöpajoissa noin kuukausittain vakiomuotoisia tarvekyselyjä osallistuvien energiayritysten toimihenkilöille. Tuloksena muodostuneet tarpeet voidaan vetää lyhyesti yhteen seuraavasti:

- Suurimmat kehittämistarpeet kohdistuvat erityisesti PK-yrityksiin
- Yritysjohdon tuki kyberturvallisuuden kehitystyölle on usein vajavaista → Johdon motivoinnille ja sitouttamiselle on edelleen iso tarve
- Tietoturvavastaava jää usein liian yksin vaativassa tehtäväkentässä
- Tietoturvatehtävien vastuujako ei ole tarpeeksi kattava ja velvoittava
- Tietoturvatilan seurannan tasossa on liikaa vaihtelua yritysten välillä
- IoT:n käyttöönotto lisää riippuvuuksia, vaikka osaamispuutteita ilmenee
- Energia-alan kyberturvallisuuden yhteistyöryhmiä tarvitaan lisää, jotta vertais- ja edelläkävijätuki jalkautuisi kaikkiin yrityksiin
- Tukea kyberturvallisuusharjoitteluun tarvitaan, sillä harjoitusten järjestäminen vaatii paljon monipuolista osaamista ja valmistautumista.

Traficomin Kyberturvallisuuskeskuksessa on kevättalvella 2019 käynnistynyt kriittistä infrastruktuuria tarjoavien organisaatioiden kyberturvallisuuden kypsyyttä mittaava projekti, jonka pilottivaihe käsittää energia-alan. Myöhemmin samankaltaista mittausta on tarkoitus tehdä muille kriittisen infrastruktuurin toimijoille. Pilottihankkeen tavoitteena on kartoittaa ja analysoida toimijakohtaisesti suomalaisen kriittisen infrastruktuurin osalta sähkön tuotannon, jakelun ja käytön liiketoimintakriittisten järjestelmien keskeisimmät kyberriskit, toimijoiden riskinottohalukkuus ja kyberriskien hallintaan kohdistettujen resurssien ja kontrollien taso suhteessa eri vertailuryhmiin. Kartoituksen tuloksena yhteiskunnalla on parempi kyky varmistaa huoltovarmuuden lisäämiseen tähtäävien panostusten oikea kohdentuminen.

7.3 Jatkotyösuunnitelmia

Jatkotyön osalta on käyty alustavia keskusteluja alla listatuista aiheista, mutta mitään päätöksiä niiden toteuttamisesta tai aikatauluista ei ole tehty.

Kohdistettuja projekteja eri kypsyystasojen yritysryhmille, esimerkiksi:

- Automaatioon kohdistuvien kyberhyökkäysten laajamittainen demonstrointi alan yrityksille
  - Yritysten havahtuminen kyberturvallisuusuhkien todellisuuteen
  - Red team -hyökkäysten järjestäminen uusille yrityksille
- Kyberharjoitusten laajamittainen järjestäminen energia-alan yrityksille
  - Yritysten nykyiset ongelmat ja toimivat ratkaisut on tehtävä entistä näkyvämmiksi
- Kyberhäiriön tilannekuvaviestintään tarvitaan yhteisiä työkaluja
  - Viestintää tarvitaan muuallakin kuin sähköverkon valvomossa
- Energia-alan ISAC (E-ISAC) ryhmän osaamisen siirto entistä laajemmin toimialan hyödyksi
  - Miten houkutella tukea tarvitsevat ihmiset mukaan yhteisöihin ja oppimaan alan edelläkävijöiltä ketään liikaa kuormittamatta?
- Energiayrityksen turvallisen IoT-ympäristön valinta, kehitys ja ylläpito
  - IoT lisää riippuvuuksia ja lisää monimutkaisuutta → riskit kasvavat

LÄHDEAINEISTO

Kuva: Colourbox

Lähdeaineisto

[DECEIT] Teemu Väisänen, Fraud and deceit – deception techniques used in nature are copied in cyberspace, VTT, 5.4.2018. https://vttblog.com/2018/04/05/fraud-and-deceit-deception-techniques-used-in-nature-are-copied-in-cyberspace/

[DECEPTION] Webinar: Cyber deception - Defend your organisation from cyber attacks, VTT, 21.3.2018. https://www.vtt.fi/medialle/tapahtumat/cyber-deception-webinar

[ENISA] ENISA: Baseline Security Recommendations for IoT, in the context of Critical Information Infrastructures, November 2017. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[FIIF] Finnish Industrial Internet Forum (FIIF) 22.9.2015 “Industrial Internet Opportunities & Cyber Security”, Luento: Pasi Ahonen ”Cyber Security Risks of Industrial Internet in different Sectors of Industry”

[F-SECURE] F-Secure: IoT threat landscape, Old hacks, new devices, 2019, https://s3-eu-central-1.amazonaws.com/evermade-fsecure-assets/wp-content/uploads/2019/04/01094545/IoT-Threat-Landscape.pdf

[HA] https://www.kyberturvallisuuskeskus.fi/fi/havaro-palvelu

[HARJOITUSOPAS] Traficomin julkaisuja 26/2019. Kyberharjoitusohje. Käsikirja harjoituksen järjestäjälle. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kyberharjoitusopas.pdf

[HB] https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/05/ttn201605241520.html

[HC] https://www.varmuudenvuoksi.fi/aihe/huoltovarmuus/106/havaro_turvaa_yhteiskunnan_huoltovarmuuskriittisia_toimintoja

[HD] https://www.tekniikkatalous.fi/uutiset/yle-haittaohjelma-vei-kayttajatunnuksia-fingridista-verkkohyokkayksista-jo-yli-600-punaista-halytysta/1bed7b48-7fad-3d9b-9a83-117db22111f3

[KAUKOLÄMMITYS] MIKKELIN AMMATTIKORKEAKOULU, MIKKELI 2015, C: OPPIMATERIAALIA – STUDY MATERIAL 16. SUOMALAINEN KAUKOLÄMMITYS. Veli-Matti Mäkelä, Oulun ammattikorkeakoulu. Jarmo Tuunanen, Mikkelin ammattikorkeakoulu. https://www.theseus.fi/bitstream/handle/10024/97138/URNISBN9789515885074.pdf

[KYBER-TEO] ”KYBER-TEO tuloksia 2014 - 2016”, Julkisten tulosten kooste. VTT TECHNOLOGY 298. https://www.vtt.fi/inf/pdf/technology/2017/T298.pdf

[KYBER-VESI] KYBER-VESI-hanke, jonka kehittämät oppaat ja työkalut ovat vesihuoltolaitosten saatavilla Huoltovarmuuskeskuksen ja Vesilaitosyhdistyksen kautta. Viittaus: https://www.huoltovarmuuskeskus.fi/vesihuoltolaitosten-kyberturvallisuuteen-uusia-tyokaluja-kyber-vesi-hankkeesta/

[MIKKONEN] Mikkonen, H. 2009: Kuntoon perustuva kunnossapito, KP-Media Oy, JAMK

[OKSANEN] Oksanen S. 2016: Laitedokumentaation hallinnan kehittäminen

[SA] Teollisuusautomaation tietoturva – Verkottumisen riskit ja niiden hallinta. Suomen Automaatioseura ry. Helsinki 2005. 160 s. ISBN 978-952-5183-38-2 ISSN 1455-6502, SAS julkaisusarja nro 29

[SUPO] Supo, Juhlavuosikirja 2018, https://www.supo.fi/instancedata/prime_product_julkaisu/intermin/embeds/supowwwstructure/77292_WWW_SUPO_Juhlakirja_70_2019_FI.pdf

[TEO-SUMMARY] Huoltovarmuuskeskuksen verkkojulkaisu ”Tietoturvaa huoltovarmuuskriittisille yrityksille”, 18.12.2013, https://cdn.huoltovarmuuskeskus.fi/app/uploads/2016/08/31144429/2013_TEOsummary_www.pdf

[TILANNE] Traficomin Kyberturvallisuuskeskuksen tilannekuva- ja verkostopalvelut: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen

[VAHTI 2/2010] VAHTI 2/2010: Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta: https://www.vahtiohje.fi/web/guest/2/2010-ohje-tietoturvallisuudesta-valtionhallinnossa-annetun-asetuksen-taytantoonpanosta Liite 5: Tietoturvallisuustasojen yksityiskohtaiset vaatimukset, Osuus 2 Tietojärjestelmien hallinnan vaatimukset

[VALOR] Energiateollisuus. Kaukolämmön kysyntäjousto. VALOR Partners Oy, 31.8.2015. https://energia.fi/files/439/Kaukolammon_kysyntajousto_loppuraportti_VALOR.pdf

[VERKOSTOJA] Traficomin Tietoturva nyt! Viranomaisten kyberyhteistyö on verkostoja, tiedonjakoa ja useita kahvikuppeja, 09.08.2018 https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/08/ttn201808091242.html

[YO-SECTV] Yliopistojen tietoturva-asioiden tiedonvaihtoryhmä (ISAC, Information Sharing and Analysis Centre). "Lokeista hyötyä”-yhteistyöprojekti. 2018-2019.

LIITTEET

Kuva: Biznes Tuba

Liite A: "Lokitiedon hyödyntämistä tukeva ohjeistus"

Referenssi: [YO-SECTV] Yliopistojen tietoturva-asioiden tiedonvaihtoryhmä (ISAC, Information Sharing and Analysis Centre). "Lokeista hyötyä"-yhteistyöprojekti. 2018-2019.

Tässä liitteessä kuvattu ohjeistus on perusta, jolle toimiva lokienhallinta voidaan mielekkäästi rakentaa. Tämän jälkeen alkaa varsinainen lokienhallinnan suunnittelu ja toteutus, joissa lokilähde kerrallaan sovelletaan seuraavassa lueteltuja dokumentteja, arvioidaan ja perustellaan tarvittavat investoinnit, sekä muodostetaan tietoinen riskitaso lokienkeruuseen liittyen.

Lokitiedon hyödyntämisen suunnittelua ja käyttöä tukemaan on hyvä luoda tarkistuslistoja, joiden tehtävänä on sujuvoittaa sekä lokien hallintaa yleisellä tasolla, että nykyisten tai uusien lokilähteiden käyttöönottoa osana tietoteknisen infrastruktuurin monitorointia.

Tässä esitetyt dokumentit ja muistilistat ovat esimerkkikokonaisuus, joka on eräissä organisaatioissa käytössä. Muistilistojen kautta lokienhallinta pyritään pilkkomaan hallittaviksi kokonaisuuksiksi, joissa osa-alueeseen kohdistetun listan avulla mahdollistetaan tarpeellisten näkökulmien säännönmukainen huomioiminen.

Listoja ja dokumentteja laatiessa on hyvä selkeästi kirjata kaksi asiaa: 1) kenelle dokumentti tai lista on tarkoitettu ja 2) mihin käyttöön dokumentti tai lista on ja ei ole tarkoitettu. Näin yksittäinen dokumentti tai lista toimii myös itsenäisesti, eikä koko dokumenttipatteristoa tarvitse muistaa ulkoa voidakseen hyödyntää kyseistä dokumenttia tai listaa.

<u>Esimerkkidokumentit ja -listat:</u>

Lokiperiaatteet (*policy*, sääntö)

Kenelle tarkoitettu:

- Johdolle kirjoitettu ja johdon hyväksymä dokumentti, joka on tarkoitettu koko organisaatiolle ja sidosryhmille.

Mihin käyttöön:

- Kirjoitettu selkokielellä ja kuvaa lokienhallinnan yleiset suuntaviivat. Se on organisaation ylimmän johdon tahdonilmaisu lokienkäsittelyyn ja sen tavoitteisiin liittyen. Toimii selkäno-jana kaikessa lokeihin liittyvässä toiminnassa.
- Lokiperiaatteiden tarkoitus on varmistaa, että organisaation tietojenkäsittelyn valvonta on tarkoituksenmukaista ja tukee ympäristön turvallista ja häiriötöntä toimintaa sekä antaa työkaluja toiminnan kehittämiselle.

Mitä ei ole:

- Ei ole tietosuojailmoitus, jossa kerrotaan miten rekisteröidyn toimintaa seurataan.

Lokienhallinnan roolit ja vastuut (Lokiperiaatteet -dokumentin liite)

Kenelle tarkoitettu:

- Johdolle kirjoitettu ja johdon hyväksymä dokumentti, joka on tarkoitettu koko organisaatiolle sekä sidosryhmille.

Mihin käyttöön:

- Listaus rooleista sekä kuvaus näiden vastuista liittyen nimenomaisesti lokeihin. Dokumentissa vastuutetaan lokienhallinta omalle organisaatiolle sekä tuodaan esiin sidosryhmien velvollisuudet.

Lokityypit (Lokiperiaatteet -dokumentin liite)

Kenelle tarkoitettu:

- Johdolle kirjoitettu ja johdon hyväksymä dokumentti, joka on tarkoitettu koko organisaatiolle sekä sidosryhmille.
- Ohje on tarkoitettu lokien suunnittelua tekevälle, lokien keruusta vastaavalle, lokien kanssa toimivalle henkilöstölle sekä lokituksesta kiinnostuneille.

Mihin käyttöön:

- Ohje kuvaa esimerkinomaisesti erilaisia lokityyppejä suositeltavine minimisisältöineen. Listatut lokit eivät muodosta tyhjentävää listaa eikä suositukset ole määrääviä. Muutokset suositeltaviin ovat mahdollisia, jos järjestelmä/sovellus ei sellaisia pysty tuottamaan tai ei ole muuten mielekästä kerätä kyseistä tietoa. Muutokset suositellaan kirjattavaksi osana lokidokumentaatiota.

Mitä ei ole:

- Tyhjentävä listaus kerätystä lokitiedosta.

Lokien hallintaohje

Kenelle tarkoitettu:

- Ohje on tarkoitettu lokien suunnittelua tekevälle, lokien keruusta vastaavalle sekä lokien kanssa toimivalle henkilöstölle.

Mihin käyttöön:

- Dokumentin tavoitteena on kertoa miten lokipolitiikka sekä sitä tukevien dokumenttien sisältö jalkautetaan käytännön toimiksi.
- Dokumentti ohjeistaa huomioimaan tarpeelliset näkökulmat lokienhallinnassa sekä katsomaan lokienhallintaa kokonaisuutena, jotta lainmukainen käsittely voidaan toteuttaa sekä todistusarvo varmistaa. Ohje on toteutettu muistilistoina eri osa-alueille, joista vaikuttavuuden kannalta tärkein on jalkautuksen muistilista.

Mitä ei ole:

- Tyhjentävä kuvaus lokien hallinnan teknisestä toteutuksesta.

Lokijärjestelmäohje

Kenelle tarkoitettu:

- Dokumentti on tarkoitettu lokijärjestelmän teknisille ylläpitäjille, lokijärjestelmän parissa työskenteleville teknisille asiantuntijoille tai lokienkeruuta palveluna toteuttavalle kumppanille.

Mihin käyttöön:

- Dokumentin tarkoitus on toimia teknisen dokumentaation tuottamisen tukena, jotta voidaan luoda riittävä lokijärjestelmäkuvaus siitä, miten järjestelmä on toteutettu. Lokijärjestelmäkuvaus on lokijärjestelmäkohtainen.
- Tämä dokumentti siis toimii tarkastuslistana siitä mitä suunnittelussa ja toteutuksessa tulee huomioida sekä mitä lokijärjestelmäkuvauksessa tulee mainita (teknisen dokumentaation muistilista).

Mitä ei ole:

- Yksittäisen lokijärjestelmän käyttöohje.

Lokien tuottamisohje

Kenelle tarkoitettu:

- Järjestelmien ja palveluiden omistajille käytettäväksi yhdessä lokijärjestelmän ylläpitäjien kanssa.

Mihin käyttöön:

- Dokumentin tarkoitus on auttaa lokilähteen käyttöönotossa ja hallinnassa ja tuoda esille ne seikat, joihin tulee ottaa kantaa otettaessa lokilähdettä käyttöön lokin hyödyntämiseksi. Lokin käyttötarkoitus voi olla esimerkiksi palvelun kehitys ja ylläpito sekä tietoturvan/-suojan valvominen ja varmistaminen. Tarkastuslista pitää käydä läpi jokaisen lokilähteen suhteen. Lokilähde voi olla esimerkiksi järjestelmä tai yksittäinen sovellus.
- Tarkistuslista, jossa määritellään mm. miten lokia kerätään, mitä varten lokilähde on olemassa, mitä pitää sopia, kuka maksaa mitäkin keruun kustannuksista, millaiset lokit tulee (myös) siirtää pois paikallisesta järjestelmästä.

Mitä ei ole:

- Lokitiedon muodon kuvaus.

Palvelu/järjestelmäkatalogi

Kenelle tarkoitettu:

- Dokumentti on tarkoitettu järjestelmien ja palveluiden omistajille käytettäväksi yhdessä lokijärjestelmän ylläpitäjien kanssa.

Mihin käyttöön:

- Tässä dokumentissa kerrotaan mitä lokitetaan. Dokumentti sisältää järjestelmästä otettavat lokit selityksineen (eli se mitä tuottamisohjeessa sanotaan).

Mitä ei ole:

- Ei ole osa lokienhallinnan dokumentaatiota, koska palveluiden ja järjestelmien kuvaus on usein organisaatiokohtainen toimintamalli.

Lokidokumentaation käyttöohje

Kenelle tarkoitettu:

- Kaikille näitä lokiohjeita käyttäville henkilöille.
- Sisäisestä auditoinnista vastaaville sekä annettavaksi ulkoisissa auditoinneissa kuvauksena lokienhallinnasta.

Mihin käyttöön:

- Tämä dokumentti kuvaa miten lokiperiaatteita ja siihen liittyviä dokumentteja on tarkoitus käyttää ja mitä kaikkia ohjeita ja vastuumäärityksiä on olemassa.
- Dokumentti, joka sisältää näiden lokienhallintaan liittyvien dokumenttien sisällön, tavoitteen ja kohdeyleisön.

Liite B: IoT toimittajien ja ratkaisujen arvioinnin tarkastuslistat

Tässä liitteessä esitellyt tarkastuslistat on tarkoitettu energiayritysten IoT-ratkaisuja tai palveluja suunnittelevien ja evaluoivien asiantuntijoiden käyttöön.

Tavoitteena on helpottaa IoT-palvelutarjoajien luotettavuuden ja erityisesti kyberturvallisuuteen liittyvien kyvykkyyksien arviointia.

Listat ovat osin päällekkäisiä ja niitä voidaan käyttää tarvittaessa itsenäisesti.

Kysymyslistat on pyritty laatimaan tarkentuvaksi listaksi, ensin pääkysymykset ja sitten tarkentavat kysymykset.

Kysymykset ovat laadittu käyttäen pohjana ENISA:n dokumenttia “Baseline Security Recommendations for IoT, in the context of Critical Information Infrastructures” [ENISA].

Viittaukset (kuten [GP-PS-01]) osoittavat pohjana olleen ENISA-dokumentin vaatimuksiin, joista kysymykset on johdettu.

TIETOTURVAPOLITIIKKOIHIN LIITTYVIÄ KYSYMYKSIÄ

Miten kyberturvallisuus on otettu huomioon tarjoamanne IoT-järjestelmän kehityksen ja käytön aikana?

Onko teillä käytössä jokin (jos niin mikä) turvallisen ohjelmistokehityksen toimintamalli?

- Miten tietoturvapolitiikoiden ja vaatimusten mahdolliset muutokset viedään teidän kehitysprosessiinne?

Kertokaa miten tarjoamanne IoT-järjestelmän osat sijoittuvat suhteessa IEC-62443:n referenssiarkkitehtuuriin ja millaisia suojauksia (luottamusrajoja) eri komponenttien välillä käytetään?

- Sijoittakaa IoT-ratkaisunne komponentit verkkoaluekuvaan

Miten, milloin ja kenen toimesta tarjoamanne IoT-järjestelmän ja siihen kuuluvien sovellusten kyberturvallisuutta on testattu?

- Miten testaaminen on dokumentoitu?

Onko järjestelmässä käytettyjen sovellusten ohjelmistokoodi katselmoitu?

Miten katselmointi on dokumentoitu?

[GP-PS-01 GP-PS-02 GP-PS-05 GP-PS-06 GP-PS-07]

Miten henkilö- ja ympäristöturvallisuus on otettu huomioon tarjoamanne IoT-järjestelmän kehityksen ja käytön aikana?

Miten käyttäjän fyysinen turvallisuus on varmistettu?

Miten laitteen fyysinen turvallisuus on otettu huomioon tilanteessa, jossa jotkin IoT-järjestelmään kuuluvat laitteet käyttävät tehonsäästöä?

Miten laitteen toiminnan luotettavuus ja turvallisuus on huomioitu virransäästötilassa?

[GP-PS-03 GP-PS-04]

Miten yksityisyyden suojaaminen on otettu huomioon tarjoamanne IoT-järjestelmän kehityksen ja käytön aikana?

Miten IoT-järjestelmän käyttäjien ja IoT-mittauskohteen yksilöiden yksityisyyden suojaaminen on toteutettu?

Miten käsittelemänne tieto on kuvattu ja miten siitä kerrotaan käyttäjille?
Onko järjestelmän tarjoamaa yksityisyyden suojaa arvioitu suhteessa

- paikalliseen lainsäädäntöön ja kulttuuriin?
- käyttötarkoitukseen ja käyttötapauksiin joissa järjestelmää käytetään?

[GP-PS-08 GP-PS-09]

Miten tarjoamanne IoT-järjestelmän sisältämät riskit on tunnistettu ja arvioitu?

Onko IoT-järjestelmän toiminnallisuus, käyttötarkoitus ja -ympäristö kuvattu?

Onko riskien arviointiin otettu mukaan järjestelmässä käytetyt kolmannen osapuolen ohjelmistot, komponentit ja palvelut?

- Kuka vastaa kolmannen osapuolen toimittamien osien kyberturvallisuuden seuraamisesta ja ratkaisujen arvioinnista?

Onko IoT-järjestelmän riskejä arvioitu suhteessa

- paikalliseen lainsäädäntöön ja kulttuuriin?
- käyttötarkoitukseen ja käyttötapauksiin joissa järjestelmää käytetään?

[GP-PS-11 GP-PS-12]

Miten omaisuuden hallinta on otettu huomioon tarjoamanne IoT-järjestelmän kehityksen ja käytön aikana?

Miten konfiguraation hallita on toteutettu tarjoamassanne IoT-järjestelmässä?

[GP-PS-10]

ORGANISAATIOON, HENKILÖSTÖÖN JA PROSESSEIHIN LIITTYVIÄ KYSYMYKSIÄ

Kuinka tarjoamanne IoT-järjestelmän turvallisuudesta huolehditaan käyttöiän lähestyessä loppua ja sen loputtua?

Kuinka pitkään toimittamanne IoT-järjestelmän tuki jatkuu?

- Kuinka pitkään järjestelmän pilvipalvelussa toteutetut osat on tuettu?
- Kuinka pitkään järjestelmään kuuluvat IoT-laitteet on tuettu?
  - Miten IoT-laitteet päivitetään?
  - Pitääkö laitteet vaihtaa niiden päivittämiseksi?
- Kuinka pitkään järjestelmän eri osiin on saatavilla kriittisiä korjauksia (käyttöiän mukaisten päivitysten loputtua) tietoturvan tai yksityisyyden vaarantaviin vikoihin?

Miten seuraatte sitä, että esiintyykö toimittamassanne järjestelmässä uusia tietoturvaongelmia?

- Kuinka kauan seuraatte uusien vikojen esiintymistä toimituksessa?
- Miten ilmoitatte vioista asiakkaalle?

[GP-OP-01 GP-OP-02 GP-OP-03]

Onko tarjoamanne IoT-järjestelmän toteuttamisessa käytetty yleisesti hyviksi tunnettuja ratkaisuja?

Perustuvatko järjestelmässä käytetyt tietoliikenneprotokollat ja salausalgoritmit avoimiin standardeihin vai suljettuihin (proprietary) ratkaisuihin?

- Miksi käytetyt ratkaisut on valittu?
- Käytetäänkö salausalgoritmien toteutuksessa valmiita kirjastoja vai onko toteutus tehty itse?
- Mitkä järjestelmässä käytetyt ratkaisut ovat suljettuja? Miksi ne eivät ole avoimia?

[GP-OP-04]

Miten etsitte, analysoitte ja käsittelette haavoittuvuuksia ja tietoturvaloukkauksia?

Miten ja mille tahoille ilmoitatte löydetyistä haavoittuvuuksista ja tietoturvaloukkauksista?

Mitä tahoja (verkkopalveluita, sähköpostilistoja yms.) seuraatte saadaksenne tietoa haavoittuvuuksista jotka voivat koskea teidän toimittamianne IoT-järjestelmiä tai niissä käytettyjä kolmannen osapuolen toimittamia palveluja, ohjelmistoja tai laitteita?

Miten ulkopuolisen tahon löytämä haavoittuvuus voidaan ilmoittaa teille?

- jotka liittyvät käyttämiinne ja toimittamiinne IoT-järjestelmiin

Oletteko osallistunut tai osallistumassa *bug-bounty* -ohjelmiin tai vastaaviin?

[GP-OP-05 GP-OP-06 GP-OP-07 GP-OP-08]

Millaista tietoturvaan ja yksityisyyteen liittyvää koulutusta olette järjestäneet henkilöstöllenne?

Kuinka usein koulutuksia järjestetään?

Kuinka seuraatte ketkä henkilöstöstänne ovat käyneet tietoturvakoulutuksissa?

[GP-OP-10]

Kuka omistaa tarjoamanne IoT-järjestelmän tuottaman datan?

Oletteko varmistaneet datan omistajuuden sopimuksilla?

Käsitelläänkö toimittamanne IoT-järjestelmän dataa kolmannen osapuolen käyttämissä pilvipalvelussa?

- Miten kolmas osapuoli suojaa käsittelemänsä datan?
- Miten kolmas osapuoli ilmoittaa, jos heidän säilyttämänsä dataan kohdistuu tietoturvaloukkauksia?

[GP-OP-12 GP-OP-13]

Kuinka olette arvioineet käyttämienne laitteisto- ja ohjelmistotoimittajien kyberturvallisuuden?

Onko käyttämillänne toimittajilla heidän johtonsa hyväksymä tietoturvapolitiikka joka ohjaa tietoturvan toteuttamista?

Millaisia teknisiä kyberturvaratkaisuja käyttämänne toimittajat käyttävät?

Miten käyttämänne toimittajat ilmoittavat havaitsemistaan haavoittuvuuksista ja tietoturvaloukkauksista teille?

- Entä heidän käyttämänsä kolmannet osapuolet?

[GP-OP-14]

TEKNISEEN TOTEUTUKSEEN LIITTYVIÄ KYSYMYKSIÄ

Miten tarjoamassanne IoT-järjestelmässä on estetty se, ettei järjestelmän jonkin osan vikaantuessa aiheudu henkilö- tai ympäristövahinkoja?

Osaavatko kriittiset IoT-järjestelmään kuuluvat osat, esimerkiksi pilvipalvelu tai IoT-yhdyskäytävä, tehdä itsenäistä vianmääritystä tai häiriötilanteesta elpymistä?

Kykenevätkö järjestelmään kuuluvat IoT-päätelaitteet itsenäiseen toimintaan (ilman verkkoyhteyttä)?

Miten IoT-päätelaitteet ja -yhdyskäytävät toimivat, jos ne menettävät yhteyden käyttämäänsä pilvipalveluun?

Menevätkö järjestelmän eri osat, kuten IoT-päätelaitteet, sammuessaan tunnettuun turvalliseen tilaan?

[GP-TM-15 GP-TM-16 GP-TM-17 GP-TM-06]

Miten IoT-laitteiden todentaminen (*authentication*) on toteutettu tarjoamassanne IoT-järjestelmässä?

Miten IoT-päätelaitteet ja -yhdyskäytävät liittyvät todennetusti muuhun järjestelmään?

Miten laitteiden ja yhdyskäytävien salasana/tunniste voidaan vaihtaa)?

[GP-TM-21 GP-TM-22]

Miten IoT-järjestelmän käyttäjien todentaminen (*authentication*) on toteutettu tarjoamassanne IoT-järjestelmässä?

Pakotetaanko järjestelmän oletuskäyttäjätilien ja salasanojen vaihtaminen?

Miten varmistetaan salasanojen riittävä pituus?

- Onko järjestelmässä mahdollista käyttää monivaiheista todennusta (MFA - *Multi-Factor Authentication*)

Eihän salasanoja ole talletettu selväkielisenä IoT-järjestelmässä?

- Miten salasanat on suojattu?

Miten salasanojen palauttaminen on suojattu?

[GP-TM-23 GP-TM-24 GP-TM-26]

Miten todentaminen (*authentication*) käyttäytyy poikkeustilanteessa?

Kuinka monta kertaa IoT-järjestelmä antaa käyttäjän yrittää virheellistä salasanaa?

- Mitä sen jälkeen tapahtuu?

Havaitseeko IoT-järjestelmä, jos siihen yritetään tunkeutua kokeilemalla salasanoja (brute-force attack)?

- Miten järjestelmä toimii, kun se havaitsee salasanojen kokeilua?

Palautuuko järjestelmä jossain tilanteissa oletustunnuksiin ja -salasanoihin?

- Missä tapauksissa?
- Miten näissä tapauksissa laite voidaan kytkeä uudestaan toimittajan palveluun – vai voidaanko?

[GP-TM-25]

Millaisia tietoturvaominaisuuksia tarjoamassanne IoT-järjestelmässä on?

Ovatko tietoturvaominaisuudet ja turvalliset asetukset käytössä oletusarvoisesti?

- Onko jokaisella toimitetulla järjestelmällä oma yksilöllinen oletussalasanansa joka ei ole laskettavissa joistakin sen ominaisuuksista?
- Onko järjestelmästä oletusarvoisesti poistettu käytöstä tarpeettomat palvelut ja ohjelmistot sekä fyysiset liittimet kuten USB?

[GP-TM-08 GP-TM-09]

Miten toimittamanne IoT-järjestelmää päivitetään?

Onko järjestelmään kuuluvien IoT-päätelaitteiden ja -yhdyskäytävien ohjelmistoja mahdollista päivittää turvallisesti langattoman yhteyden yli (OTA - over-the-air)?

Miten päivityspakettien turvallisuus on varmistettu?

- Onko päivityspaketit allekirjoitettu?
- Kenen toimittamalla varmenteella?

Onko päivitykset mahdollista automatisoida?

- Onko automaattinen päivittäminen oletuksena päällä?

Onko käyttäjillä mahdollisuus päättää, mitkä päivitykset asennetaan?

Säilyvätkö käyttäjän laitteeseen tekemät asetukset päivityksen yhteydessä?

Jos päivitys epäonnistuu, mihin tilaan IoT-laite käynnistyy?

- Palaako IoT-laite oletustilaan, edelliseen versioon vai johonkin muuhun tilaan?

[GP-TM-05 GP-TM-18 GP-TM-19 GP-TM-20]

Miten tarjoamanne IoT-järjestelmän muuttumattomuus ja eheys (*integrity*) on suojattu?

Miten järjestelmän käynnistyminen luotettuun tilaan on varmistettu?

- Suojataanko järjestelmää käyttämällä
  - luotettua suojattua käynnistystä (*trusted boot*, *TPM - Trusted Platform Module*), ja
  - laitteessa olevan käyttöjärjestelmän, ohjelmistojen ja asetusten allekirjoituksia?
- Käynnistyykö järjestelmä turvalliseen tilaan myös virhetilanteen jälkeen?

[GP-TM-06]

Miten laitteen eheys (*integrity*) ja luottamuksellisuus (*confidentiality*) on suojattu pääsynvalvonnalla (*access control*)?

Voidaanko laitteissa käyttää eri tilanteisiin ja ympäristöihin soveltuvia tietoturvatasoja?

[GP-TM-29 GP-TM-30]

Miten IoT-päätelaitteet ja -yhdyskäytävät ovat suojattu fyysisiä hyökkäyksiä vastaan?

Voidaanko IoT-laitteen data tyhjentää etähallinnalla, jos se on varastettu?

Havaitsevatko IoT-laitteet luvattoman muuttamisen (tamper) ja miten muuten ne on suojattu?

Havaitsevatko IoT-laitteet, jos niitä yritetään purkaa ja miten ne toimivat sellaisessa tilanteessa?

Onko IoT-laitteiden tallennusjärjestelmät suojattu salauksella?

Onko laitteen fyysiset portit, kuten USB, suojattu tai onko ne mahdollista ottaa pois käytöstä?

[GP-TM-31 GP-TM-32 GP-TM-33]

Miten tiedon siirto ja säilytys on suojattu tarjoamassanne IoT-järjestelmässä?

Mitä salausmenetelmiä ja -protokollia järjestelmässä on käytettävissä?

- Miksi ne on valittu?
- Onko käytetyt salausalgoritmit toteutettu käyttäen luotettavia kirjastoja vai oletteko koodanneet ne itse?
- Miten kirjautuminen ja siihen liittyvä dataliikenne mukaan lukien salasanat on suojattu?

Kuinka järjestelmän eri osat mukaan lukien IoT-laitteet, IoT-yhdyskäytävät ja pilvipalvelussa olevat ohjelmistot todentavat (authenticate) toisensa?

- Miten eri laitteet, mukaan lukien päätelaitteet ja yhdyskäytävät, toimivat havaitessaan luvattoman yhteydenoton?

[GP-TM-38 GP-TM-39 GP-TM-40 GP-TM-41 GP-TM-42 GP-TM-43 GP-TM-44]

Miten tarjoamanne IoT-järjestelmän käyttämä salaus ja avainten hallinta on toteutettu?

Mitä salausalgoritmeja ja avainten pituuksia järjestelmässä käytetään?

Miten avainten luominen, jakaminen, vaihtaminen ja säilyttäminen on toteutettu?

- Miten riittävä satunnaisuus on varmistettu avaimia luotaessa?

Miten järjestelmässä käytetty salaus ja avainten-hallinta skaalautuvat siihen kuuluviin IoT-päätelaitteisiin?

- Miten salaus on toteutettu niissä järjestelmään kuuluvissa laitteissa, joissa on vain vähän laskentakapasiteettia ja tehoresursseja käytössä?
- Miten salausavain jaetaan järjestelmässä esimerkiksi pieniin antureihin?

[GP-TM-34 GP-TM-35 GP-TM-36 GP-TM-37]

Miten valtuuttaminen (*authorization*) on toteutettu järjestelmässä?

Käyttävätkö järjestelmässä olevat sovellukset esimerkiksi pienimmän valtuuden periaatetta (PoLP - the Principle of least privilege)?

Onko järjestelmässänne etuoikeutettuja ohjelmia tai ohjelmakoodia (privileged code)?

Miten järjestelmässä etuoikeutettu koodi, prosessit ja data on suojattu?

[GP-TM-27 GP-TM-28]

Miten tarjoamanne IoT-järjestelmä on suojattu verkkohyökkäyksiä vastaan?

Miten järjestelmää on kovennettu tai miten sitä olisi mahdollista koventaa?

- Voidaanko esimerkiksi tiettyjä tietoliikenneprotokollia tai portteja sulkea pois käytöstä?

Onko laitteissa mahdollista rajoittaa tulevan ja lähtevän tietoliikenteen lähteitä ja -kohteita, sekä dataliikenteen määrää?

Tukeeko IoT-järjestelmä siihen kuuluvien IoT-laitteiden ja yhdyskäytävien jakamista alueisiin?

Suojaavatko järjestelmässä käytetyt tietoliikenneprotokollat tai muut tietoturvaratkaisut tilanteessa jossa yksi verkkoon kuuluvista laite on joutunut hyökkääjän haltuun?

- Käyttävätkö kaikki saman tuoteperheen laitteet samaa salausavainta?

Miten järjestelmä käyttäytyy, jos siihen kohdistetaan palvelunestohyökkäys?

- Miten järjestelmä toipuu palvelunestohyökkäyksen jälkeen?

Miten järjestelmälle (ja sen Web-rajapinnalle) annetut syötteet tarkastetaan ennen niiden prosessointia?

[GP-TM-45 GP-TM-46 GP-TM-50 GP-TM-47 GP-TM-48 GP-TM-49 GP-TM-51]

Miten järjestelmän Web-rajapinta on suojattu verkkohyökkäyksiä vastaan?

Miten järjestelmän Web-rajapinta on suojattu ja kovennettu hyökkäyksiä vastaan?

- Onko Web-rajapinta testattu esimerkiksi haavoittuvuusskannereilla tai käyttämällä eettisiä hakkereita?

Missä tilanteissa järjestelmä ja sen Web-rajapinta tuottavat ulospäin näkyviä virheilmoituksia?

- Miten järjestelmän tuottamat ilmoitukset ja sille annetut syötteet suodatetaan?
- Onko virheilmoituksista mahdollista päätellä järjestelmän ominaisuuksia?

[GP-TM-52 GP-TM-53 GP-TM-54]

Onko järjestelmän toteutuksessa käytetty laitteistopohjaisia tietoturvamekanismeja?

Käytetäänkö järjestelmässä esimerkiksi

- luotettua suojattua käynnistystä (*trusted secure boot*),
- luotettua ajoympäristöä (*trusted execution* environment),
- kriittisten muistialueiden suojausta,
- tallennusjärjestelmän salausta, tai
- luvattoman järjestelmän muuttamisen (*tamper*) havainnointia.

[GP-TM-01 GP-TM-02 GP-TM-03]

Miten järjestelmä noudattaa tietosuojalakeja, kuten GDPR-asetus?

Miten IoT-järjestelmän käyttäjät voivat vaikuttaa siihen mitä ja kuinka paljon järjestelmä kerää heistä tietoa?

- (tai esimerkiksi henkilöt jotka ovat samassa tilassa missä IoT-päätelaite tekee mittauksia)

Miten varmistetaan se, että kerättyä tietoa käytetään vain ilmoitettuun tarkoitukseen?

- Miten käyttötarkoituksen muutos ilmoitetaan?

Miten IoT-järjestelmän käyttäjät voivat tarkastaa, hakea, korjata ja poistaa IoT-järjestelmän heistä keräämää tietoa?

- (tai esimerkiksi henkilöt jotka ovat samassa tilassa missä IoT-päätelaite tekee mittauksia)

[GP-TM-10 GP-TM-11 GP-TM-12 GP-TM-13 GP-TM-14]

Miten tarjoamassanne IoT-järjestelmässä monitoroidaan siihen kuuluvien laitteiden toimintaa ja häiriöitä?

Havaitseeko monitorointi myös IoT-järjestelmään tai sen osiin kohdistuvia verkkohyökkäyksiä?

Tehdäänkö tarjoamallenne IoT-järjestelmälle tietoturva-auditointeja ja/tai -testausta?

[GP-TM-56 GP-TM-57]

Miten tarjoamanne IoT-järjestelmän tapahtumat talletetaan lokeihin ja miten lokit on suojattu?

Mitkä tapahtumat talletetaan ja kuinka pitkäksi aikaa?

- Mihin lokit tallennetaan
- Miten lokit on suojattu luvatonta muuttamista tai poistamista vastaan?

Miten ja kuinka nopeasti lokit saadaan tutkittavaksi?

- Voidaanko lokeja tutkia, jos IoT-järjestelmällä ei ole yhteyttä sen toteutuksessa käytettyyn pilvipalveluun?
- Onko käyttäjällä mahdollisuus saada lokitiedot jotka koskevat hänen omaa toimintaansa tai omia laitteitansa?

[GP-TM-55]

Muutama vuosi sitten energia-alan avaintoimijat tunnistivat tarpeen parantaa toimialansa kyberturvallisuutta ja -tietoisuutta sektorilähtöisesti siten, että edelläkävijäyritysten kyberkokemuksia ja osaamista jaettaisiin entistä suoremmin sitä tarvitseville yrityksille. Tämän johdosta Huoltovarmuuskeskus käynnisti syksyllä 2017 uuden sektorikohtaisen projektin (KYBER-ENE 1) sekä kesällä 2018 jatkoprojektin (KYBER-ENE 2), joissa keskityttiin energia-alan keskeisimmiksi tunnistettuihin kehityskohteisiin:

- Kyberturvallisuustyön käynnistäminen yrityksissä.
- Omaisuuden hallinnan ja havaintokyvyn kehittäminen.
- IoT:n turvallinen hyödyntäminen.
- Yhteistyö, häiriöhallinta ja kyberharjoittelu.

Kansallisen infrastruktuurin häiriönsietokyvykkyyden nostamiseksi kyberturvallinen toimintatapa on saatava osaksi energiayritysten tavallista työtä. Toisaalta hyvää kyberturvallisuuden vertaisverkostoa ei korvaa mikään, sillä sen kautta saa tietoa esim. akuuteista kyberuhista, muille sattuneista vahingoista, sekä hyvin toimivista ratkaisuista.

HUOLTOVARMUUSKESKUS
FÖRSÖRJNINGSBEREDSKAPSCENTRALEN
NATIONAL EMERGENCY SUPPLY AGENCY