Raportti TIKKA 2016-tietoturvallisuuden arviointityökalun kehittämisestä

28-04-2016

Jouko Tervo

Sisällysluettelo

TIKKA 2016 – Tietoturvallisuuden arviointityökalun kehittäminen

1 JOHDANTO

1.1 Yhteiskunnalle kriittisen sähköverkon ohjaus ja valvonta

Yhteiskuntamme on erittäin riippuvainen sähköstä. Sähkön häiriötön siirto ja jakelu ovat elintärkeitä lähes kaikille yhteiskunnan ja elinkeinoelämän sektoreille. Sähkön paikallisesta siirrosta ja jakelusta vastaavat sähköverkkoyhtiöt ovat huoltovarmuuskriittisiä yrityksiä, joiden toiminta tulee varmistaa kaikissa olosuhteissa.

Sähkön siirto- ja jakeluverkon toiminta on hyvin pitkälle automatisoitu ja automaation määrä lisääntyy edelleen jatkossa. Sähköverkon ohjaus ja valvota on tyypillisesti keskitetty yhteen valvomoon verkkoyhtiössä. Sähköverkon toimilaiteet, kuten tärkeimmät katkaisijat, erottimet, muuntajat jne., on liitetty käytönvalvontajärjestelmään (SCADA), jonka avulla kerätään verkon tilatietoa ja ohjataan toimilaitteita. Tyypillinen SCADA- järjestelmä muodostuu varmennetusta keskusasemasta (palvelimista ja niiden tietokannoista) sekä sähköverkon asemilla sijaitsevista ala-asemista (RTU). Sähköverkon tärkeimmät toimilaitteet on kytketty ohjausta ja valvontaa varten ala-asemiin paikallisverkoilla, jotka käyttävät kasvavassa määrin ethernet-pohjaista lähiverkkotekniikkaa. Ala-asemat on yhdistetty keskusaseman palvelimiin tietoliikenneverkolla, joka kriittisiltä osiltaan pyritään aina varmentamaan. Uusissa ratkaisuissa käytetään standardia IP-tiedonsiirtotekniikkaa. Käytönvalvontajärjestelmän tietoliikenneverkko pyritään aina mahdollisimman hyvin eristämään julkisista tietoverkoista sekä myös yrityksen sisäisestä, toimistokäytössä olevasta tietoverkosta.

Sähköverkossa olevat toimilaitteet on laajasti suojattu epänormaaleja ja vikatiloja vastaan relesuojauksella. Suojareleet on liitetty sähköasemilla oleviin lähiverkkoihin ja suojareleisiin voidaan olla etäyhteydessä esim. parametrien muuttamiseksi tai tapahtumalokien lukemiseksi.

Sähköverkon sujuva ja nopea käyttötoiminta (valvonta ja ohjaus) edellyttävät keskijännitteisen jakeluverkon osalta myös reaaliaikaisen kytkentätilainformaation sijoittamista paikkatietopohjaiseen järjestelmään. Tästä järjestelmästä käytetään nimitystä käytöntukijärjestelmä (DMS).

Sähköverkon ohjausta ja valvontaa tehdään verkkoyhtiön valvomotilojen lisäksi myös etäyhteydellä käytönvalvojien kotoa. Järjestelmätoimittajat lisäksi ylläpitävät SCADA-, DMS- ja relesuojausjärjestelmiä etäyhteyksien avulla omista toimistotiloistaan. Näihin etäyhteyksiin käytettään normaalisti julkisten tietoliikenneverkkojen yli rakennettuja suojattuja kanavia, ns. VPN-tunneleita.

Kaikki edellä mainitut verkostoautomaatiojärjestelmät ja monet muut sähköyhtiöiden käytössä olevat järjestelmät on liitetty sähköyhtiön yritystietoverkkoon ja sen kautta ulkoisiin dataverkkoihin ja julkiseen internetverkkoon.

Sähköverkko kehittyy jatkossa entistä enemmän älykkäämpään suuntaan paikallisen pientuotannon ja erilaisten joustavien kulutustapojen lisääntyessä. Lisäksi jakeluvarmuutta pyritään lisäämään mm. jakeluverkkoa silmukoimalla ja kehittyneitä ohjausjärjestelmiä käyttöönottamalla. Sähköverkko kehittyy ICT-teknologiaan vahvasti luottavaksi älykkääksi sähköverkoksi eli smart grid-verkoksi.

1.2 Maailma on muuttunut tietoturvattomaksi – järjestelmien tietoturva uhattuna

Syitä verkostoautomaatiojärjestelmien tietoturvan heikentymiseen on lukuisia, mm:

- Kaupallisten ohjelmistojen käyttö verkostoautomaatiojärjestelmissä on tavanomaista
- Tietojärjestelmien integraatiot lisääntyvät nopeasti yleistyvien IP-teknologian ja langattomuuden vauhdittamina
- Uhkaavien tahojen määrä on kasvanut ja rikolliset ovat muuttuneet ammattimaisiksi
- Uutena uhkana valtiolliset vakoilu- ja kyberyksiköt
- Laaja valikoima vakoilu- ja murto-ohjelmistoja on helposti kaikkien saatavilla
- Globaalia internet-tietoverkkoa käytetään osana yrityksen tietojärjestelmäkokonaisuutta
- Palveluketjut ovat monimutkaistuneet; käytetään lukuisia ulkopuolisia toimittajia ja alihankkijoita erilaisten rakentamis-, huolto- ja ylläpitopalvelujen tuottamisessa

Kuva 1 - Tietoturvauhkien takana olevia tahoja

Tietoturvallisuus ja sitä heikentävät haavoittuvuudet eivät aina liity tietotekniikkaan. Siksi tietoturvallisuuden arvioinnissa on tärkeää huomioida sähköverkkotoiminnan jatkuvuuteen ja turvallisuuteen vaikuttavat turvallisuusasiat laaja-alaisesti:

- Tietoturvallisuuden johtaminen sisältäen vastuiden jaon
- Henkilöturvallisuus
- Verkkotoiminnan keskeiset tietojärjestelmät, kuten käytönvalvonta- , käytöntuki- ja verkkotietojärjestelmät sekä verkoston suojausjärjestelmät. Sähköasemilla ja jakeluverkossa olevat älykkäät laitteet (IED) ovat osa verkostoautomaatiota
- Käytönvalvonnan ja suojauksen tietoliikenneverkko ja -yhteydet
- Järjestelmien sisäiset tietoverkot, yhteydet toimistoverkkoon käyttötoimintaan liittyviltä osilta ja etäyhteydet
- Tilaturvallisuus (fyysinen turvallisuus)
- Suojattavan omaisuuden ja tiedon hallinta
- Toiminnan jatkuvuuden varmistaminen

2 HANKKEEN TAVOITTEET, OHJAUSRYHMÄ JA TUKIJAT

2.1 Kehittämistyölle asetetut tavoitteet

Itsearviointityökalun avulla parannetaan verkkoyhtiön tietoturvallisuutta sekä osaltaan sähkön siirto- ja jakelutoiminnan jatkuvuutta. Kokonaisuus muodostuu mm. seuraavista osatavoitteista:

1. Lisätään yleistä tietoutta ja osaamista sähkön käytön ja sähköverkon ohjaus- ja valvontajärjestelmien tietoturvallisuudesta
2. Itsearvioinnin avulla verkkoyhtiön johto saa käsityksen sähkön siirto- ja jakelutoiminnan tietoturvallisuuden nykytilan tasosta ja kehittämistä vaativista alueista. Tieto nykytilasta on välttämätöntä tietoturvallisuuden parantamisessa, kuten esimerkiksi kehitys-suunnitelmien laadinnassa
3. Kehitetään sähköyhtiön henkilöstön osaamista ja ymmärrystä tietoturvasta ja viestitään henkilöstölle tietoturvan merkityksestä
4. Muokataan sähköyhtiöiden henkilöstön asenteita, jotta tietoturvallisuus huomioitaisiin paremmin päivittäisessä työskentelyssä
5. Itsearvioinnin kautta tunnistetaan helppoja kohteita tietoturvallisuuteen parantamiseksi nopeasti sekä pitempää kehitystyötä vaativia osa-alueita
6. Työssä käsitellään ja kirjataan sähkön siirron ja jakelun jatkuvuuden kannalta oleelliset turvallisuusteen vaikuttava asiat ja rakenteet tietoturvallisuuden osa-alueittain.

Riskien ja uhkien tärkeysluokitteluun käytetään arvioita niiden vaikuttavuudesta verkkoliiketoimintaan sekä sähkön siirron ja jakelun jatkuvuuteen

7. Kehitetään sähköverkkotoiminnan tietoturvallisuuden itsearvioinnissa käytettävä helppokäyttöinen sähköinen työkalu. Kehitystyössä huomioidaan verkkoyhtiöiden toiveiden lisäksi Energiateollisuus ry:n (ET), Sähköturvallisuuden edistämiskeskus ry:n (STEK), Huoltovarmuuskeskuksen (HVK) sekä Viestintäviraston Kyberturvallisuus-keskuksen näkemyksiä. Tietoturvallisuuden itsearviointityökalun toteutus suunnitellaan siten, että se keskittyy erityisesti sähköverkkotoiminnan jatkuvuuden varmistamiseen (toimitusvarmuuden parantamiseen). Työkalu sisältää seikkaperäisen sähköisen käyttöohjeen
8. Pilotoidaan kehitetty arviointityökalu 2-3 sähköverkkoyhtiön avustuksella. Yhtiöt valitaan mahdollisimman hyvin alaa edustavasti. Pilotointiin kuuluu oleellisena osana palautetilaisuus, jossa kerätään kehitysehdotuksia ja kokemuksia työkalun käytöstä
9. Tehdä pilotoinnista saadun palautteen perusteella työkaluun tarvittavat muutokset
10. Julkistetaan kehitystyön tulokset ohjausryhmän vahvistaman suunnitelman mukaisesti ja jaetaan tietoturvallisuuden itsearviointityökalu veloituksetta sähköverkkoyhtiöiden käytettäväksi. Työkalua voivat soveltuvin osin hyödyntää tietoturvallisuuden arvioinneissa myös kaukolämpöä, kaasua ja vettä siirtävät ja jakelevat yritykset ja yhteisöt
11. Laatia kirjallinen loppuraportti työn tuloksista

2.2 Hankkeen ohjausryhmä ja resurssit

Hankkeen ohjausryhmässä toimivat Kim Malmberg Netcontrol Oy, Janne Pollari Savon Voima Verkko Oy, Jukka Perttala (sihteeri) ja Jouko Tervo (pj) Konsulttitoimisto Reneco Oy.

Työn päävastuullisena tekijänä toimi Jouko Tervo.

Ohjausryhmä järjesti työn aikana 5 kokousta.

Kiitokset ohjausryhmän jäsenille hyvistä neuvoista, kommenteista ja arvokkaasta lähtöaineistosta.

2.3 Hankkeen taloudelliset tukijat

Hanketta tukivat taloudellisesti Sähköturvallisuuden Edistämiskeskus ry (STEK) ja Energiateollisuus ry (ET).

3 TYÖKALUN KEHITTÄMISEN PÄÄVAIHEET JA TYÖMÄÄRÄ

3.1 Esiselvitykset

Työn alussa

1. Perehdyttiin tietohakujen avulla alan standardeihin, ohjeisiin ja muihin käytössä oleviin työkaluihin
2. Selvitettiin haastattelujen, keskustelujen ja tietohakujen avulla työkalun toivottuja ominaisuuksia ja vaatimuksia
3. Testattiin muita julkisesti saatavilla olevia tietoturvallisuuden työkaluja

Haastatteluja ja asiantuntijatapaamisia järjestettiin yhteensä 4 tahon kanssa seuraavasti:

- Sähköverkkoyhtiöt
  - Fingrid Oyj
  - Savon Voima Verkko Oy
- Käytönvalvontajärjestelmän toimittaja
  - Netcontrol Oy
- Huoltovarmuuskeskus (HVK)

Ohjausryhmässä käytiin läpi työkalun ominaisuuksia ja toiminnallisia vaatimuksia 10.12.2015 ja 26.1.2016 järjestetyissä kokouksissa.

Esiselvitykset tehtiin marraskuu-joulukuu 2015 aikana.

3.2 Suunnittelu- ja kehittämisvaihe

Työkalun suunnittelun alkuvaiheessa kiinnitettiin sen toimintaperiaate, jonka keskeisenä lähtökohtana oli tutkittavan yrityksen tietoturvallisuuden tason määrittäminen valikoituihin väittämiin vastaamalla. Omaisuuksiin lisätiin myös mahdollisuus kirjata keskusteluja ja kommentteja sekä määrittää heikon tietoturvallisuuden tason saaneille kohteille kehitys-toimenpiteitä.

Monipuolinen tulosten raportointi katsottiin kehittämisessä myös välttämättömäksi.

Sähköinen työkalu päätettiin luottamuksellisuus- yms. syistä suunnitella itsenäiseksi, työasemassa toimivaksi sovellukseksi. Lähtökohtana oli myös, että sen tulisi olla helppokäyttöinen ja toimia normaalissa toimistotyöasemassa vakio-ohjelmistoilla.

Ohjausryhmä käsitteli työkalun toiminnallisuutta ja ominaisuuksia tammi- ja helmikuun kokouksissaan.

Työkalun kehittäjä kävi pitämässä tietoturvallisuuden itsearvioinnista esityksen Sähkötutkimuspoolin seminaarissa 4. helmikuuta.

Suunnittelu- ja kehittämisvaihe ajoittui joulukuu 2015 - helmikuu 2016 väliselle ajalle.

3.3 Työkalun pilotointi

Pilotoinniin aikana työkalua testasivat ja kommentoivat ohjausryhmässä edustettujen tahojen lisäksi:

- Fingrid Oyj/Jyrki Pennanen ja Ari Silverberg
- Oulun Energia Siirto ja Jakelu Oy/Timo Määttä+taustatiimi
- Loiste Sähköverkko Oy/Eero Luhtaniemi+taustatiimi

Piloitoinnissa ja testauksessa esiin tulleet puutteet ja parannusehdotukset vietiin mahdollisimman nopeasti työkaluun kehittäjän toimesta.

Pilotointi järjestettiin maalis-huhtikuun aikana 2016.

Pilotoinnin avulla saadut kokemukset ja kommentit olivat tärkeitä lopputuloksen kannalta. Yleisesti työkalua pidettiin erittäin tarpeellisena ja toteutusta hyvin toimivana.

3.4 Työkalun hyväksyminen ja lanseeraus

Ohjausryhmä käsitteli pilotoinnista saatua palautetta ja työkalun valmiutta lanseeraukseen kokouksissa 7.4 ja 28.4. Ohjausryhmä piti kehitettyä työkalua tarpeellisena ja toteutusta käytettyyn aikaan ja resursseihin nähden oikein onnistuneena. Kokouksessa 28.4 ohjausryhmä hyväksyi TIKKA 2015-työkalun lanseerattavaksi rahoittajatahojen kanssa sovittavan menettelyn mukaisesti ja hyväksyi työn laskutettavaksi.

Pilotoinnin loppuvaiheessa työkalun kehittäjä järjesti tapaamiset STEKin ja Energiateollisuuden Verkkoyksikön johdon kanssa, joissa käsiteltiin työkalun lanseeraukseen liittyviä toiveita ja näkemyksiä. Työkalun kehittämisessä oli lähtökohtana, että se on veloituksetta saatavissa kaikille sen käytöstä kiinnostuneille tahoille. Nyt kehitetty versio on suunnattu erityisesti sähköverkkoyhtiöille ja tapaamisissa parhaaksi vaihtoehdoksi arvioitiin malli, jossa työkalu viedään verkkoyhtiöiden ladattavaksi niiden käytössä olevaan Sähköverkkoextra-portaaliin. Portaali sijaitsee Adato Oy:n sivuilla, http://www.adato.fi/Default.aspx?tabid=433 . Lanseeraus Adaton portaalissa tehdään alustavasti viikolla 19.

Alkuvaiheessa STEK ilmoitti todennäköisesti pitäytyvänsä nettisivuilleen liitettävään uutiseen/ tiedotteeseen.

Erityisesti tietoturvallisuuden itsearviointityökalu TIKKA 2016 on tarkoitettu sähköverkkoyhtiöiden tietoturvallisuuden arviointiin sekä itsenäisenä työkaluna että käyttämällä sitä auditointien apu- ja väliarvioinnin apuvälineenä. Tämä raporttia laadittaessa työkalun lanseeraus on vielä tekemättä.

Kehitystyön lopuksi kehittäjä laati tämän raportin.

3.5 Käytetty työaika

Työkalun kehittämiseen on käytetty yhteensä noin 6 henkilötyökuukautta (24 vko) jakaantuen seuraavasti:

- Esiselvitykset ja taustatyö	4 vko
- Suunnittelu- ja kehittämisvaihe	12 vko
- Pilotointi	4 vko
- Viimeistely	3 vko
- Raportointi ja lanseerauksen valmistelu	1 vko
Yhteensä	24 vko = 120 työpäivää

Kehittämiseen kului huomattavasti enemmän työaikaa, kuin alun perin arvioitiin (arvio 51 työpäivää). Erityisesti tietoturvallisuusstandardien läpikäynti ja kysymysten laadinta vaativat huomattavasti suunniteltua enemmän aikaa. Aikaa kului myös arvioitua enemmän työkalun virittelyyn.

3.6 Työkalun jatkokehittäminen ja käytön laajentaminen

Työkalun saamaa vastaanottoa sähköverkkoyhtiöiden keskuudessa seurataan ja palautetta tullaan keräämään aktiivisesti. Samassa yhteydessä laatija voi antaa pienimuotoista opastusta työkalun käyttämisessä.

Adaton kanssa pyritään työkalun latausportaali järjestämään niin, että portaalista saadaan tunnistettua lataajayritykset. Tätä tietoa hyväksikäyttäen sähköverkkoyhtiöitä lähestyttäisiin kuluvan vuoden syksyllä ja kysyttäisiin työkalun käyttökokemuksista ja pyydettäisiin palautetta jatkokehittämistä varten. Siitä päätettäisiin erikseen saatujen kokemusten ja palautteen perusteella.

Huoltovarmuuskeskus (HVK) on käynnistämässä verkkoyhtiöiden varautumisessa käytetyn HUOVI-portaalin uudistamista. HVK:n kanssa keskustellaan lanseerauksesta saatujen kokemusten jälkeen työkalun mahdollisesta hyödyntämisestä HUOVI-portaalin jatkokehittämisessä.

Työkalun johtamista ja hallintoa, henkilöstöä, tilaturvallisuutta ja suojattavan omaisuuden ja tiedon hallintaa koskevat alueet ovat kysymyksiltään sangen toimialariippumattomia, joten kohtuullisen pienellä työllä työkalun saa päivitettyä soveltuvaksi esim. veden, kaasun ja kaukolämmön jakelun tietoturvallisuuden arviointiin. Hieman suuremmalla työpanoksella työkalu soveltuisi esim. kiinteistöjen turvallisuuden ja kiinteistöautomaation tietoturvallisuuden arviointiin.