TECHNOLOGY • RESEARCH HIGHLIGHTS • VISIONS • SCIENCE •
298

KYBER-TEO – tuloksia 2014–2016

Julkisten tulosten kooste

Pasi Ahonen et al.

VTT TECHNOLOGY 298

KYBER-TEO – tuloksia 2014–2016

Julkisten tulosten kooste

Pasi Ahonen et al.

VTT

Muut kirjoittajat näkyvät Kiitokset-kohdassa.

ISBN 978-951-38-8541-0 (nid.)
ISBN 978-951-38-8540-3 (URL: http://www.vtt.fi/julkaisut)

VTT Technology 298

ISSN-L 2242-1211
ISSN 2242-1211 (Painettu)
ISSN 2242-122X (Verkkojulkaisu)
http://urn.fi/URN:ISBN:978-951-38-8540-3

JULKAISIJA – UTGIVARE – PUBLISHER

Teknologian tutkimuskeskus VTT Oy
PL 1000 (Tekniikantie 4 A, Espoo)
02044 VTT
Puh. 020 722 111, faksi 020 722 7001

Teknologiska forskningscentralen VTT Ab
PB 1000 (Teknikvägen 4 A, Esbo)
FI-02044 VTT
Tfn +358 20 722 111, telefax +358 20 722 7001

VTT Technical Research Centre of Finland Ltd
P.O. Box 1000 (Tekniikantie 4 A, Espoo)
FI-02044 VTT, Finland
Tel. +358 20 722 111, fax +358 20 722 7001

Juvenes Print, Tampere 2017

Saatteeksi

Vuosia jatkunut hyvä yhteistyö elinkeinoelämän, hallinnon ja tutkimuksen kesken on tuonut lukuisia kyberturvallisuuden ratkaisumalleja konkreettisten ja liiketoimintalähtöisten tarpeiden ratkaisemiseksi. KYBER-TEO-hanke toteutettiin vuosien 2014–2016 aikana. Toteutetuissa projekteissa on ollut mukana monia alan keskeisiä yrityksiä, Kyberturvallisuuskeskus, Huoltovarmuuskeskus ja VTT.

Käytännön kybertoimintaympäristöjä on kehitetty yhteistyössä huoltovarmuuskriittisten yritysten kanssa. Varsinkin kyberturvallisuustestaustoimintaan ja harjoitustoimintaan kehitettiin toimintamalleja, jotka koettiin käytännön harjoituksissa hyödyllisiksi. Samoin on saatu aikaiseksi yrityksiä hyödyttäviä tuloksia teollisuusautomaation edellyttämän elinkaaritarkastelun huomioonottamiseksi. Myös monitorointi, eli tietoturvapoikkeamien havainnointikyvyn parantaminen, on ollut vahvasti mukana KYBER-TEO-projekteissa.

Tässä julkaisussa kuvatut ja alan toimijoiden kanssa kehitetyt, käytännössä koetellut toimintatavat ja ratkaisumallit hyödyttävät varsinaisia teollisia toimijoita, joiden menestys riippuu toimintavarmasta teollisuusautomaatiosta, mutta myös alan ohjelmisto- ja järjestelmätoimittajia sekä palveluntarjoajia. Yhteistyö on ollut tuloksellista, ja jatkokehittämiselle on luotu vahva perusta.

Huoltovarmuuskeskus
Sauli Savisalo
Infrastruktuuriosaston johtaja
Aleksanterinkatu 48 A
00100 Helsinki
www.huoltovarmuus.fi

Sisältö

Kuvat

Yhteenveto

Kyberturvallisuusuhkiin varautumisen tarve lisääntyy, sillä elinkeinoelämän ja teollisuuden automaatiojärjestelmäriippuvuus kasvaa jatkuvasti. Integroitujen kokonaisjärjestelmien, toimintojen ja yhteistyöverkostojen monimutkaistuessa korostuu yritysten kantapään kautta opittujen kyberkokemusten jakamisen tärkeys, jotta saadaan kehitettyä koko yhteisön varautumista. Yhteistyön vaatima avoimuus ei kuitenkaan saa vaarantaa tietoa jakavan organisaation omaa turvallisuutta edes väliaikaisesti.

Hallitun avoimuuden odotetaan parantavan kokonaisvarautumista välttämättömän yhteisymmärryksen ja kumppanuuksien lisääntyessä. Tämä mahdollistaa varautumistoimenpiteiden paremman yhteensovittamisen. Uusia pilottihankkeita sekä erilaisia kohdennettuja selvityksiä, tutkimuksia ja käytännön kokeita tulee tehdä jatkuvasti, jotta pysyttäisiin nopeasti kehittyvien ja muuttuvien kyberuhkien tasalla. Syvää yhteistyötä tarvittiin ja tarvitaan uusien kyberturvallisuutta parantavien toimenpiteiden jalkauttamisessa yritysten käytännön toimintaan.

Tässä julkaisussa kuvataan KYBER-TEO ”Kyberturvallisuuden kehittäminen ja jalkauttaminen teollisuuteen” -hankekokonaisuuden julkisia tuloksia. Kyseessä oli kaikkiaan kolme vuotta kestänyt kansallinen hankekokonaisuus vuosina 2014–2016. Päätilaaja oli Huoltovarmuuskeskus. Tarvittiin yhteisen hyvän tuottamista eli julkisia tuloksia ja niiden levittämistä, ja toisaalta osallistuneet yritykset tilasivat vuosittain luottamuksellista kehitystukea kyberturvallisuuden parantamiselle tai kyberturvallisuuspalvelujensa kehittämiselle. Kyseessä ei ole käsikirja, joten emme käsittele kattavasti aivan kaikkia tietoturvan osa-alueita. Sen sijaan esittelemme sitä, miten me käytännössä kehitimme kyberturvallisuutta suomalaisissa alan yrityksissä.

KYBER-TEO-kokonaisuuden päätavoite oli kehittää ja testata uusia palveluja osallistuvissa teollisuus- ja palveluyrityksissä kyberturvallisuuden ja jatkuvuuden varmistamiseksi ja muun suomalaisen teollisuuden hyödynnettäväksi. Hankekokonaisuuden yritysosallistujissa tapahtui luonnollisesti vuosittaista vaihtelua, eikä aivan kaikkien osallistuneiden yritysten listaaminen ole oleellista syntyneen julkisen tiedon jakamisen kannalta. Eräät osallistuneet yritykset eivät

halunneet tulla julkisuuteen yrityksensä nimellä. Kunnioitimme myös näitä päätöksiä.

Hankkeen työpaketit (TP) olivat

- TP 1: Kybersuojauksen käytännöt ja kartoitukset
- TP 2: Kyberturvallisuuden jalkauttaminen kotimaiseen tuotantoon
- TP 3: Tuotantoautomaatioverkon monitorointipalvelut.

Kyberturvallisuuden käytännöt ja kartoitukset (TP1) koettiin työalueeksi, jossa lähes kaikilla teollisuusyrityksillä tulisi olla jatkuvaa nykytilanteen kartoittamista ja oman toiminnan kehittämistä. Kyberturvallisuuden jalkauttaminen kotimaiseen tuotantoon (TP2) sisälsi pääosin teknisempien menettelyjen kehittämistä, kuten koventamisen ja kyberturvallisuustestauksen, joilla varmistettiin ja todennettiin kyberturvallisuusvaatimusten toteutumista tuotantojärjestelmissä. Kolmantena alueena oli tuotantoautomaatioverkon monitorointipalvelut (TP3), jonka yhteydessä kehitettiin menetelmiä tuotannonohjausverkkojen kyberturvallisuuden tilannekuvaan, samalla täydentäen aktiivisten kyberturvallisuusratkaisujen puutteita ja osoittaen suuntaa vastatoimenpiteille.

Tämän julkaisun tavoitteena on kyberturvallisuustietoisuuden parantaminen laajasti automaatiota hyödyntävän teollisuuden toimijoiden keskuudessa. Tietoisuuden lisäämisen avulla pyrimme helpottamaan kyberturvallisuuden jalkautusta käytännön toimintaan. Tällainen kehitys ei käynnisty itsestään, vaan se vaatii huolellista perehtymistä kyberturvallisuuden yleiseen kenttään, omiin erityisongelmakohtiin tuossa kentässä sekä luonnollisesti riittävää johdon sitoutumista. Projektissa laajennettiin ja kehitettiin käytännön yhteistyöverkostoja, joiden kautta teollisuusyritykset saivat ja saavat konkreettista tukea omiin kyberturvallisuuden kehityshankkeisiinsa.

Osallistuneet yritykset ilmaisivat vahvasti, että yhdessä tehty työ on synnyttänyt tarvittavaa tietoisuutta, kyvykkyyksiä, osaamista, yhteistyötä ja valmiuksia sekä palveluja, joiden avulla automaation kyberturvallisuuden kehittäminen tuli mahdolliseksi isossa mittakaavassa.

Kehittäminen edellyttää lähes aina tietoisuuden perustasoa, jotta yrityksen päättäjät ja käytännön toimijat ymmärtävät riittävästi kyberuhkien todellisista vaikutuksista ja kohdistumisesta omaan toimintaansa. Vasta tämän jälkeen yritykseen voi syntyä tarvittava vastuiden määrittely ja resursointi mm. tuotantoon soveltuvien kyberturvallisuusuhkien havaitsemiseen, torjuntaan ja ennakkovarautumiseen.

Teollisuusautomaation kyberturvallisuuden kehittäminen Suomessa vaatii kaikkien toimijoiden osallistamista. Tämä johtuu mm. siitä, että kyberturvallisuuden ratkaisee lopulta ”arvoketjun heikoin toimija” tai ”järjestelmän huomaamaton haavoittuvuus”.

Turvallisen toiminnan vastuuta ei voi ulkoistaa, sillä viime kädessä tuotanto-operaattori vastaa itse kaikkien tarvittavien turvamenettelyjen käyttöönotosta, käytön valvonnasta ja kehittämisestä.

KYBER-TEO-projekteissa vuosina 2014–2016 kehitettiin yritysten yhteistyötä ja edellytyksiä parantaa monia erilaisia automaation kyberturvallisuuteen vaikuttavia asioita:

- Alan edelläkävijäyrityksissä kehitettiin ja testattiin automaation kyberturvallisuuden kehittämisen palveluja, parhaita käytäntöjä ja ratkaisuja.
- Määriteltiin kyberturvallisuuden työnjako ja tehtävät automaation elinkaaressa.
- Parannettiin ammattilaisten kyberturvallisuustietoisuutta julkisten tulosten esittelytilaisuuksissa kertomalla uhkista ja seurauksista sekä varautumiseen kehitetyistä käytännöistä ja koetelluista ratkaisuista.
- Kehitettiin ja koestettiin automaation kyberturvatestauksen ympäristöjä.
- Kehitettiin ja koestettiin automaation kyberturvaharjoittelun ympäristöjä.
- Kehitettiin ja koestettiin automaatioverkkojen kyberturvamonitoroinnin konsepteja ja menetelmiä.
- Kehitettiin ja pilotoitiin automaation kyberturvallisuuden sähköistä yhteistyöfoorumia.

Teknologian tutkimuskeskus VTT Oy
Pasi Ahonen, johtava tutkija
KYBER-TEO 2014–2016 -projektipäällikkö
Kaitoväylä 1
90571 OULU
www.vtt.fi

Kiitokset

Suuret kiitokset kaikille tämän julkaisun tulosten ja sisällön tuottamiseen osallistuneille henkilöille! Seuraavat yritykset ja asiantuntijat osallistuivat julkaisun tulosten yhteiseen tuottamiseen sekä antoivat luvan nimensä mainitsemiselle:

ABB Drives:
- Pekka Alho
- Pasi Koivumäki
- Mika J. Kärnä
- Juho Salminen

ABB Medium Voltage Products:
- Jani Hirvo
- Mikko Lähdesmäki
- Mats Lövdahl
- Janne Starck

Huoltovarmuuskeskus:
- Tero Kauppinen (nyt eläkkeellä)
- Kalle Luukkainen
- Erkki Räsänen
- Sauli Savisalo

Insta DefSec:
- Marko Hautakangas
- Tero Leppänen
- Tatu Männistö
- Mikko Salonen

NESTE:
- Pasi Lehtinen

Netcontrol:
- Kim Malmberg

Nixu:

- Pietari Sarjakivi

Nordic LAN&WAN Communication:

- Juha Pasanen
- Kari Salmela

Prosys OPC:

- Jouni Aro
- Pyry Grönholm

Orion:

- Ulla Palmila

Outotec:

- Patrik Granholm

Schneider Electric:

- Kalle Aalto
- Harri Hamberg
- Mika Kiiveri
- Arto Laurila
- Tero Laaksonen
- Veli-Matti Luukko

Tampereen teknillinen yliopisto:

- Mikko Salmenperä
- Jari Seppälä

Teollisuuden Voima:

- Timo Kauraoja
- Petri Leppimäki
- Esko Rauta
- Janne Rintamaa

Turun seudun puhdistamo:

- Jyrki Haapasaari

Valmet:

- Tero Hakala
- Markku Tyynelä

Viestintäviraston Kyberturvallisuuskeskus:

- Erika Suortti-Myyry
- Sami Orasaari
- Mikko Viitaila

VTT:

- Pasi Ahonen
- Kimmo Halunen
- Jouni Hiltunen
- Hannu Honka
- Jukka Julku
- Anni Karinsalo
- Pasi Keski-Korsu
- Sami Lehtonen
- Sami Noponen
- Pia Olli
- Heimo Pentikäinen
- Juha Pärssinen
- Mirko Sailio
- Tuomo Soivuori
- Visa Vallivaara
- Teemu Väisänen

Johdanto aiheeseen

Mikä automaatiojärjestelmä?

Teollisuusautomaatiojärjestelmiä ovat tehtaiden ja erilaisten tuotantolaitosten tuotannonohjausjärjestelmät. Näiden ylläpitämiseksi tarvitaan erilaisia kiinteistötekniikan sekä ympäristöolosuhteiden säätöjärjestelmiä, joten nekin lukeutuvat meitä kiinnostaviin automaatiojärjestelmiin.

Tarvitsemme myös peruskäsitteistön määrittelyn, jotta lukija ymmärtää esittämämme asiat mahdollisimman yksiselitteisesti. Käsitteistön pohjaksi valitsimme IEC-62443-standardin ”Teollisuuden tietoliikenneverkot, verkkojen ja järjestelmien tietoturvallisuus” (ent. ISA-99), sillä sen sisältö on kehitetty erityisesti (automaatiota hyödyntävän) teollisuuden käyttöön. Ko. standardin perusteisiin johdattava osa 1-1 ”Terminologia, käsitteet ja mallit” [IEC62443-1-1] sekä osat 2-1 ja 3-1 on jo käännetty suomeksi. Lisäksi teollisuutemme on, ainakin osin, jo alkanut soveltaa ko. standardisarjaa, mm. sen kattavuuden takia.

Tässä julkaisussa kyberturvallisuuden kehittäminen koskee esim. öljynjalostusta ja jakelua, vesihuoltoa, sekä sähköntuotantoa, -siirtoa ja -jakeluverkkoja. Tunnustettuja kehitystarpeita on myös sektoreilla, jotka eri tavoin hyödyntävät tuotannossaan automaatiota ja tiedonsiirtoverkkoja (mm. yleisesti prosessiteollisuus, kappaletavaravalmistus, liikenne, sekä terveydenhuolto), joten näiden alojen toimijat kuuluvat myös kohderyhmäämme.

Erityisen oleellisia kyberturvallisuuden kannalta ovat automaatiojärjestelmien yhteydet ulkoiseen maailmaan. Tämä on varsin selkeästi todettavissa jo Suomen Automaatioseura Ry:n (SAS) julkaisusarjasta nro 35 [SAS1]. Eri järjestelmien välinen integraatio on tosin sittemmin jo kovasti lisääntynyt ja monimutkaistunut. Lisäksi kiinteistöautomaatio ja tuotantologistiikan automatisointi ovat vallanneet lisää alaa ja käytetty teknologiakin on osin konvergoitunut esim. Ethernet-liityntöjen laajentuneen käytön myötä. Suomen Automaatioseuran erinomaisessa kyberturvallisuuteen keskittyvässä verkkojulkaisussa "Teollisuusautomaation tietoturva" [SAS2] on esitetty automaatiojärjestelmän malli, joka sisältää myös liitynnät kenttälaitteisiin ja kenttäväyliin. Suosittelemme vahvasti tuohon julkaisuun perehtymistä, sillä se antaa

edelleen erinomaista taustatietoa esim. oman yrityksen kyberturvallisuuden kehittämiselle.

Tämä julkaisu käsittelee tuotantoon liittyviä automaatiojärjestelmiä ja tehdasverkkoja sekä osin myös uudenlaista konseptia, jota kutsutaan nimellä teollinen internet. Teollisessa internetissä on kyse fyysisistä laitteista, jotka pystyvät aistimaan ympäristöään ja viestimään tai toimimaan aistimansa perusteella älykkäästi.

Automaation kyberturvallisuuden haasteet ja tavoitteet

Tietotekniikka ja automaatio kehittyvät ja etenevät yhä laajemmin ja yhä syvemmälle yhteiskunnan kaikkiin toimintoihin. Monimutkaisuus lisääntyy ja myös kybertoimintaympäristöön liittyvät uhkatekijät monipuolistuvat. Samalla riippuvuusketjut pitenevät, niiden hallinta vaikeutuu, ja riskit kasvavat.

Riskejä voidaan hallita laajan ja monitasoisen tavoitteellisen yhteistyön avulla:

- turvallisista teollisista komponenteista ja järjestelmistä laajoihin monitoimittajaympäristöihin
- turvallisuusajattelun jäsentämisestä eri organisaatiotasojen kesken, esim. operatiivisesta tasosta strategiseen tasoon
- toiminnan kannalta kriittisimpien järjestelmien tunnistamisesta koko järjestelmäympäristön, omien ja kumppaneiden etäyhteyksien sekä pilvipalveluiden suojaamiseen, käyttötarkoituksensa kannalta sopivimmilla ratkaisuilla
- palveluiden ja toimitusketjujen hallinnasta investointipäätösten valmistelusta alkaen järjestelmien elinkaaren loppuun
- ottaen liiketoimintalähtöisesti ja toimialoittain huomioon kansainvälisen asiakaskentän vaatimukset, suositukset ja sääntely
- havainnointi- ja reagointikyvyn parantamisesta ennakointiin, yritysstrategian tukemiseen ja yritysriskien hallinnan kehittämiseen
- luottamuksellisen tiedonvaihdon kehittämisestä käytännön harjoittelemiseen
- koeteltujen ratkaisumallien kautta konkreettisiin hyötyihin mm. yhteisten kustannussäästöjen kautta.

Pyrkimyksenä on edistää sähköisen ja verkotetun yhteiskunnan turvallisuutta, jolloin kyberturvallisuuden suunnittelussa tulee yhdistyä tietoturvallisuuden, jatkuvuudenhallinnan ja yhteiskunnan kriisivarautumisen ajattelutavat. Kyberturvallisuudessa varaudutaan siihen, miten sähköisten ja verkotettujen järjestelmien häiriöt vaikuttavat yhteiskunnan kriittisiin toimintoihin, sekä tunnistetaan ja ehkäistään näitä häiriöitä.

Tavoitteena on ollut, että huoltovarmuuden kannalta kriittisin elinkeinoelämä on suojattu vakavien ja laajojen kyberuhkatilanteiden varalta ja että yrityksillä on kyky

palautua kyberuhkatilanteista nopeasti palveluntarjoajiensa ja kumppaneidensa tuella. KYBER-TEO-hankekokonaisuus on tukenut näitä tavoitteita.

Referenssit

[IEC62443-1-1] IEC-62443-standardin ”Teollisuuden tietoliikenneverkot, verkkojen ja järjestelmien tietoturvallisuus” perusteisiin johdattava osa 1-1 ”Terminologia, käsitteet ja mallit”

[SAS1] Suomen Automaatioseura Ry, ”Automaatiosuunnittelun prosessimalli; Yhteiset käsitteet verkottuneen suunnittelun perustana” (SAS julkaisusarja nro 35), Helsinki 2007. https://www.automaatioseura.fi/site/assets/files/1367/automaatio-suunnittelun_prosessimalli.pdf

[SAS2] Suomen Automaatioseura Ry, "Teollisuusautomaation tietoturva" (SAS julkaisusarja nro. 29) kirjan verkkopainos, 2010. https://www.viestintavirasto.fi/attachments/tietoturva/TeollisuusautomaationTietoturva.pdf

1. Kyberturvallisuus automaation elinkaaressa

Kyberturvallisuuden sisällyttäminen osaksi automaation elinkaaren hallintaa on välttämätöntä kyberturvallisuuden ja jatkuvuuden kehittämisessä ja ylläpitämisessä. Suuri toimijoiden ja tehtävien määrä (elinkaaren aikana) aiheuttavat jatkuvia kyberturvallisuusriskejä, joiden tunnistaminen ja hallitseminen vaativat paljon jatkuvaa työtä.

Oppi 1. Automaation pitkän elinkaaren hallinta vaatii paljon kyberturvallisuuspohdintaa.

Vaikeinta automaation kyberturvallisuudessa on pitkän elinkaaren hallinta, sillä…

…kyberuhkia tulee koko ajan lisää,
mutta ongelmat eivät vähene lisäämällä uusia teknologioita ja prosesseja vanhojen päälle, vaan
määrittelemällä jatkuvuuden varmistamisen konseptit,
joissa kyberturvallisuus on aina mukana, sekä
sopimalla ymmärrettävät pelisäännöt ja vastuut
omalle henkilöstölle ja kumppaneille.

Hyvien peruskäytäntöjen ja työkalujen soveltaminen ja yhteistyö ovat toimivia tapoja automaation turvallisuuden ja jatkuvuuden varmistamisessa.

Eri standardit määrittelevät automaatiojärjestelmän elinkaaren eri tavoin. Suomen Automaatioseuran (SAS) julkaisussa [SAS1] on kuvattu automaatiojärjestelmän elinkaaren vaiheet, niiden väliset etapit sekä tärkeimmät tulokset. Siinä vaiheet ovat

- MÄÄRITTELY
- SUUNNITTELU
- TOTEUTUS
- ASENNUS

- TOIMITUKSEN TESTAUS
- KELPUUTUS
- TUOTANTO.

Tämä perinteinen malli oli askeleittain etenevä prosessi, jossa kunkin vaiheen työ pohjautui vahvasti edellisten vaiheiden tuloksiin. Malli kuvasi myös tarvittavat ja tuotettavat tiedot, tuen ja resurssit, mikä olisi ollut ihanteellista myös kyberturvallisuuden kehittämisen kannalta. Perinteistä mallia sovellettaessa on varsinkin nykyään huomioitava riittävä iterointi ja takaisinkytkentä kyberuhkien jatkuvasti muuttuessa. Miten esim. pitkäkestoisen ja laajan kehitysprojektin eri osapuolten uusien kontribuutioiden saatavuus ja täten esim. riittävät vikakorjaukset saadaan toimitettua, mikäli uusia kyberturvallisuusuhkia havaitaan? Tällaiset muutokset ja korjaavien lisätoimien tarve kannattaa huomioida projekti- ja palvelusopimuksissa jo varhaisessa vaiheessa, jottei lopulliseen toimitukseen jää tunnettuja haavoittuvuuksia.

Isossa-Britanniassa (UK) panostetaan huomattavia summia kansalliseen kyberturvallisuuteen, ja se onkin tuottanut hyviä tuloksia. Erityisesti kansallisen infrastruktuurin kyberturvaamiseen keskittyvä CPNI (*The Centre for the Protection of National Infrastructure*) antaa automaation elinkaaren kyberturvallisuutta kuvaavassa dokumentissaan [CPNI1] selkeän mallin automaatiojärjestelmän (IACS) elinkaarelle. Kullekin kyberturvallisuuden tehtävämäärittelylle osoitetaan tarkka paikka osana elinkaarta. Tätä menetelmää kannattaa hyödyntää Suomessakin.

Esimerkki. Ison-Britannian CPNI: Automaatiojärjestelmän elinkaarimalli [CPNI1]. Kirjoittajan käännös.

- **Suunnitteluvaihe:**
  - Konseptointi
  - Alustava suunnittelu
  - Yksityiskohtainen suunnittelu
- **Käyttöönottovaihe:**
  - Tehtaan hyväksymistestaus (*Factory Acceptance Testing*)
  - Asennus
  - Asiakkaan hyväksymistestaus (*Site Acceptance Testing*)
- **Käyttö:**
  - Käyttö ja ylläpito
  - Muutostyöt ja jälkiasennukset
- **Käytöstä poisto:**
  - Käytöstä poisto ja tuhoaminen

Erityisesti kyberturvallisuuden hyvää hallintotapaa esittelevä hyvä käytäntö “CPNI*: Security for Industrial Control Systems, Establish ongoing governance*” [CPNI2] kannattaa hyödyntää, sillä se opastaa keskeisten kyberturvallisuusalueen tehtävien organisoinnissa ja hallinnoinnissa. CPNI tarjoaa yleensäkin päteviä kyberturvallisuuden malleja, käytäntöjä ja ohjeita.

Suomessakin erityisesti eri toimijoiden välinen roolijako kaipaa selkeyttämistä. Jo tilausvaiheessa tulee varmistaa mm. kaikkien osapuolten riittävä kyberturvallisuusosaaminen, vastuunjaon selkeys sekä ulkoistettavien palvelujen, päivitysten ja vikakorjausten saatavuus. Valitettavan usein myös oman henkilöstön osaamisen kehittäminen ja jakaminen osoittautuvat liian vähäisiksi (esim. palkataan ainoastaan yksi kyberturvallisuutta ymmärtävä toimihenkilö ja siirretään kaikki kyberturvaan liittyvät vastuut hänelle). Käytännössä toteutuneet kyberuhat kuitenkin osoittavat, että kyberturvallisuus täytyy huomioida automaation elinkaaren kaikissa vaiheissa: aina alkuvaiheen esitutkimuksesta ja määrittelystä hyvin palvelleen järjestelmän, laitteen ja ohjelmiston käytöstä poistoon saakka.

1.1 KYBER-TEOn elinkaarimalli

Kuvaamme seuraavaksi KYBER-TEO-projektissa tekemäämme työtä automaation elinkaaressa kyberturvallisuuden tehtävänmäärittelyn ja vastuunjaon osalta.

Toimivin ja täten kustannustehokkain kyberturvallisuuden hallinta saadaan aikaan kehittämällä ja koestamalla toimivat menetelmät kyberturvallisuuden sisällyttämiseksi kaikkiin automaatiohankintoihin. Tällöin jo tuotantoon otetut automaatiojärjestelmät ja niiden ylläpitotoimet eivät tuo yllättäviä kyberturvallisuusuhkia tuotannossa olevaan järjestelmään. Lisäksi toki edellytetään aktiivista omistajuutta ja mm. jatkuvaa riskienhallintaa.

Huomioita 1. Kyberturvallisuuden kehittämisinvestointien suurin vaikuttavuus elinkaaressa saadaan aikaan hankintavaiheessa.

Investoinneille saadaan suurin vaikuttavuus esittämällä toimittajille jo hankintavaiheessa tärkeimmät kyberturvallisuusvaatimukset ja valitsemalla ainoastaan kyberturvallisia palveluja ja tuotteita.

Jo hankintavaiheessa kannattaa tehdä omia varautumissuunnitelmia ja rakentaa luotettava kumppanuusverkosto koko elinkaaren palvelujen takaamiseksi.

Kyberuhat muuttuvat nopeasti, joten myös tuotanto- ja ylläpitovaiheissa tulee tehdä jatkuvaa riskianalyysiä ja ylläpitää suunnitelmia riskien hallitsemiseksi.

Suomessakin olemme oppineet kantapään kautta, että kaikki toimijat on otettava mukaan automaation kyberturvallisuuden kehittämiseen! Esimerkiksi tuotantojärjestelmän ylläpidossa toimiva alihankkijan työntekijä on välinpitämättömyyttään tuonut haittaohjelman sisältävän PC:n tuotantoalueelle ja täten aiheuttanut haittaohjelman leviämisen asiakkaan tuotantoverkkoon. Joskus on ollut jopa mahdollista, että

vastaavalla tavalla edennyttä tiedusteluprosessia ei ole tunnistettu, koska ”tartuntaa” ei heti havaittu eikä sisäverkon laitonta tiedustelua näin ollen osattu edes epäillä.

Jokaisen toimijan täytyy tuntea turvalliset menettelytavat omissa työtehtävissään ja myös toimia ohjeiden osoittamalla tavalla. Jotta tähän tilanteeseen päästäisiin, on välttämätöntä määritellä tuotannon kyberturvallisuuden päätehtävät toimijoittain automaation koko elinkaaressa. Vähitellen kaikkien toimijoiden aina tuotantoinsinööristä siivoojaan täytyy ymmärtää laiminlyöntien vakavat seuraukset tuotannolle. Kaikki osapuolet täytyy saada noudattamaan kyberturvallisuusohjeita ja turvallisia käytäntöjä ja täten turvallisuutta ylläpitävään piiriin. Yksikin toimija voi huolimattomuuttaan tuhota kaiken turvallisuuden eteen tehdyn työn.

1.1.1 Toimijat

Aluksi listaamme tärkeimmät automaation kyberturvallisuuden varmistamiseen vaikuttavat toimijat. Päivitämme tässä listan, jonka esittelimme jo vuoden 2014 yhteen vetäneessä tulosjulkaisussamme, ks. [KYBER-TEO2014].

TILAAJA: Automaatiota hyödyntävä teollisuuden tuotantoyritys tai kriittisen infrastruktuurin palveluja ylläpitävä yritys. Vastaa oman tuotantonsa ja toimintansa operoinnista, kyberturvallisuudesta ja jatkuvuudesta (Esim. Fortum, Neste, Orion, Teollisuuden Voima, Turun seudun puhdistamo, Valio, Wärtsilä). Tänä päivänä tilaajat käyttävät paljon alihankkijoita ja ulkoistavat monia toimintojaan.

PÄÄPROJEKTITOIMITTAJA: Vastaa tilaajan laajan hankkeen toteutuksesta, jossa esim. rakennetaan, laajennetaan tai päivitetään tilaajan automatisoituja tuotantolinjoja tai yksiköitä. Pääprojektitoimittaja (esim. Neste Jacobs, Outotec) määritellään usein vastaamaan myös hankkeen muiden järjestelmätoimittajien ja alihankkijoiden projektityöstä.

INTEGRAATTORIT: Integraattorit asentavat ja yhdistävät toimitukseen kuuluvat järjestelmät kuten koneet, laitteet, sovellukset ja automaatiojärjestelmät toimivaksi kokonaisuudeksi. Yleensä integraattori myös testaa kokonaisjärjestelmän toimivuuden. (Esim. Outotec, Insta.)

AUTOMAATIOJÄRJESTELMÄTOIMITTAJAT: Suunnittelevat, kehittävät ja toimittavat tilaajan hankintaan liittyvät automaatiojärjestelmät. Ylläpitävät järjestelmiään ja palvelevat tilaajaa esimerkiksi takuuaikana tai huoltosopimuksella myös toimituksen jälkeen (esim. ABB, Honeywell, Siemens, Schneider Electric, Valmet). Jotkut toimittajat tarjoavat tänä päivänä myös toimittamiensa järjestelmien tai tuotantoyksiköiden operointipalvelua.

LAITE-, SOVELLUS- JA OHJELMISTOTOIMITTAJAT: Kehittävät ja ylläpitävät automaatiojärjestelmissä käytettäviä koneita, laitteita, sovelluksia ja ohjelmistoja

(esim. ABB, Beckhoff, Microsoft, Netcontrol, Prosys OPC). Sovelluskehittäjät tyypillisesti kehittävät ja muokkaavat automaatiossa hyödynnettäviä ohjelmistoja.

KYBERTURVALLISUUSEXPERTIT: Kyberturvallisuusalan asiantuntijat tukevat omalla erityisosaamisellaan automaatiojärjestelmien kyberturvallisuuden eri osa-alueita (esim. Cysec, F-Secure, Insta DefSec, Nixu, Nordic LAN&WAN Communication, Viestintäviraston Kyberturvallisuuskeskus, Sectra, Tampereen teknillinen yliopisto, VTT).

1.1.2 Kyberturvallisuuden päävastuumatriisi

Seuraavassa kuvassa esitetään teollisuuden kanssa yhteistyössä kehittämämme yleinen vastuumatriisi kyberturvallisuuden päävastuista automaation elinkaaressa. Se toimii lähtökohtana ja yleiskuvana päätehtävistä ja työnjaosta toimijoittain ja sitä tulee soveltaa ja muokata tilaajan kuhunkin tilanteeseen soveltuvaksi.

Kyberturvallisuuden työnjakomallien tulee tukea jo olemassa olevia yhteistyömalleja ja toimintatapoja, sillä kyberturvallisuuden hallintaa ei kannata rakentaa yrityksissä omaksi erilliseksi järjestelmäkseen. Kokemus osoittaa, että liian monet rinnakkaiset mallit ja ohjeet johtavat lopulta ohjeiden noudattamatta jättämiseen, sillä ne voivat muodostua tehokkaan työnteon kannalta ristiriitaisiksi.

Toimija / Elinkaaren vaihe	TUOTEKEHITYS	HANKINTA	TESTAUS & KÄYTTÖÖNOTTO	TUOTANTO & YLLÄPITO	KÄYTÖSTÄ -POISTO
TILAAJA	Varmistaa kumppanuus-verkostonsa jatkuvuuden	Johtaa, jakaa vastuut ja asettaa vaatimukset	Suunnittelee ja valvoo käyttöönoton	Osaamisen, omaisuuden, riskien ja muutosten hallinta ja tilanneseuranta	Määrittelee poisto luvan ja prosessin
PÄÄPROJEKTI-TOIMITTAJA	Hallinnoi projektin turvallisuus-vaatimuksia	Jakaa toimitus-sopimuksen tehtävät	Koordinoi ja valvoo projektin testauksen	(Dokumentaation ylläpito)	Toteuttaa poisto-prosessin
INTEGRAATTORI	Hallinnoi integroinnin turvallisuuden-vaatimuksia	Dokumentoi integraation turvallisuuden	Varmistaa integroinnin turvallisuuden	(Dokumentaation ylläpito)	Toteuttaa poisto-prosessin
AUTOMAATIO-JÄRJESTELMÄ-TOIMITTAJA	Varmistaa ja testaa teknologian turvallisuuden	Kuvaa järjestelmän turvallisuuden	Koventaa, testaa ja kouluttaa toimituksen	Kovennuksen ylläpito, korjaaminen, raportointi, tutkinta, palautus	Toteuttaa poisto-prosessin
LAITE-, SOVELLUS-, OHJELMISTO-TOIMITTAJA	Varmistaa ja testaa teknologian turvallisuuden	Kuvaa tuotteen turvallisuuden	Koventaa, testaa ja kouluttaa tuotteen	Tuotteen korjaaminen ja testaus	Toteuttaa poisto-prosessin
	TUOTE-KEHITYS	HANKINTA	TESTAUS & KÄYTTÖÖNOTTO	TUOTANTO & YLLÄPITO	POISTO

Kuva 1. Automaation elinkaari – Kyberturvallisuuden päävastuumatriisi.

1.1.3 Kyberturvallisuuden tehtäväkokonaisuuksia toimijoittain

Päävastuumatriisi saattaa muistuttaa yksisuuntaista vesiputousmallia, mutta se ei ole sitä. Tilaajan asema koko tuotantoketjun valvonnan järjestäjänä ja oman tuotannon kyberturvallisuuden kehittämisen suunnannäyttäjänä on erittäin vastuullinen. Tilaajan velvollisuuksiin kuuluu mm. järjestää mm. tuotannon ja ylläpidon aikainen järjestelmien valvonta häiriöiden ja väärinkäytösten varalta. Valvonnan tuloksena kertynyt tietämys haavoittuvuuksista ja uusista uhkista viedään takaisinkytkentänä luotettuun kumppanuusverkostoon ja toimittajien ”tuotekehitykseen”. Tilaajan on pidettävä huolta siitä, että riittävä kybertapahtumien valvonta ja häiriöhallintaan tarvittava yhteistyö suunnitellaan ja toteutus myös testataan käytännön harjoituksin. Häiriöharjoituksissa syntyy tietämystä ongelmakohdista, jotka kanavoituvat suoraan asianomaisille osapuolille. Luotettu toimitus- ja tuotantoverkosto oppii näin jatkuvasti yhdessä uusia konkreettisia varautumiskeinoja.

Kyberturvallisuusasiantuntijat tukevat tilaajaa ja muita osapuolia heikoissa kohdissa tarvittavan kyberosaamisen kehittämiseksi ja esim. tarvittavien seurantapalvelujen toteuttamiseksi. Tänä päivänä kyberturvallisuuden tekninen seuranta edellyttää lähes aina erittäin vahvaa kyberuhkaosaamista sekä kehittyneiden seurantajärjestelmien jatkuvaa käyttöä. Tätä ei tilaaja yleensä pysty omin voimin toteuttamaan. Tehtäväkokonaisuudet esitetään kuvassa 2.

Elinkaaren vaihe / Toimija	TUOTE-KEHITYS	HANKINTA	TESTAUS & KÄYTTÖÖN-OTTO	TUOTANTO & YLLÄPITO	KÄYTÖS-TAPOISTO
TILAAJA	Tilaajan kyberturvallisuuden ja jatkuvuuden vaatimusten ja ohjeiden laadinta ja viestintä.	Määrittelee: yhteiset käytännöt, politiikat, suojavyöhykkeet. Määrittelee: vaatimukset, suojaustasot etäyhteysmallit. Määrittelee: toimitussisältö ja -rajat. Valvoo: koko elinkaari & sopimukset. Jakaa vastuut. Edistää tietoisuutta.	Vastaanoton valvonta ja katselmointi. Validointikatselmointi. Kelpuutuskatselmointi. Jatkuvuussuunnitelmien laadinta. Harjoitussuunnitelmien laadinta.	Omaisuuden hallinta (työkuvat) ja jatkuvuus elinkaaressa. Muutosprosessien määrittely ja valvonta. Koulutusjärjestelyt. Varautumisen: kapasiteetti, riskit, katselmoinnit, harjoitukset. Tilanneseurannan & häiriöhallinnan järjestelyt.	Myöntää poistoluvat. Menettelytapojen ja uusiokäytön määrittely & valvonta.

Elinkaaren vaihe / Toimija	TUOTE-KEHITYS	HANKINTA	TESTAUS & KÄYTTÖÖN-OTTO	TUOTANTO & YLLÄPITO	KÄYTÖS-TÄPOISTO
PÄÄ-PROJEK-TITOIMIT-TAJA	Projektin turvallisuusvaatimusten laadinta ja noudattamisen valvonta.	Tilauksen sisällön määrittely. Projektin kyberturvallisuussuunnitelman laadinta. Ohjelmisto- ja palvelulisenssien hallinta.	Käyttöönotto ja valvonta, mm.: -Projektikäytännöt -Tietoliikenneratkaisut. -Rajapinnat. -Yhdyskäytävät. -Osoitteet.	*(Dokumentaation säilytys ja ylläpito.)*	Projektin päättämisen menettelytapojen määrittely & valvonta.
INTEG-RAAT-TORI	Integroinnin turvallisuusvaatimusten määrittely ja noudattaminen.	Vastaa integroinnin arkkitehtuurista ja turvallisuudesta.	Asennus ja konfigurointi. Rajapintojen integrointi. Kovennuksen testaus ja raportointi.	*(Dokumentaation säilytys ja ylläpito.)*	Noudattaa hävitysmenettelyjä.
AUTO-MAATIO-JÄRJES-TELMÄ-TOIMIT-TAJA	Turvallisten T&K-prosessien ja alustojen määrittely, testaus, katselmointi. Kyberturvallisuustekniikan toteutus ja käyttöönotto järjestelmään. Järjestelmän haavoittuvuuksien seuranta ja vikakorjaukset.	Verkkoarkkitehtuurin ja järjestelmäkuvauksen laadinta. Järjestelmäohjeiden ja prosessien määrittelyt: mm.: -Pääsynvalvonta. -Identiteetinhallinta. Toimitusprosessin turvallisuuden määrittely ja vastuu.	Toimituksen paketointi, asennus, esiasetukset, päivitykset. Kyberturvallisuustestaus ja kovennus. Käyttäjätilien siirto. Varmennus ja palautus. Turvalliset etäyhteydet. Järjestelmäkoulutus.	Kenttäasennusten ylläpito ja dokumentointi. Huoltosopimuksen toimet, korjaukset, riskianalyysit, raportointi. Muutosten testaus. Kovennuksen ylläpito. Lokien seuranta, häiriötutkinta, palautus.	Määrittelee & noudattaa poiston menettelytapoja. Uusiokäyttö.
LAITE-, SOVEL-LUS-, JA OHJEL-MISTO-TOIMIT-TAJA	Alustojen kyberturvallisuuden arviointi. Kyberturvallisuuden toteutus, testaus ja ylläpito (mt. vikakorjaukset).	Tuotekuvausten, ohjeiden ja prosessien laadinta. Toimitusprosessin turvallisuuden määrittely ja vastuu.	Alusta, laite-, sovellus- ja ajurituki. Testaus, paketointi, päivitysten jako. Kovennuksen tuki. Koulutus, käyttäjätiliohjeistus.	Tuotetuki, Huoltosopimuksen toimet, korjausten toimitus. Muutosten testaus. Varalaitteiden toimitus.	Määrittelee & noudattaa menettelytapoja. Uusiokäyttö.

Kuva 2. Automaation elinkaari – Kyberturvallisuuden varmistamiseen ja avustamiseen liittyviä tehtäväkokonaisuuksia toimijoittain.

1.2 Referenssit

[CPNI1] CPNI, “SECURITY FOR INDUSTRIAL CONTROL SYSTEMS, MANAGE INDUSTRIAL CONTROL SYSTEMS LIFECYCLE, A GOOD PRACTICE GUIDE”, Version Final v1.0. https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/SICS%20-%20Manage%20ICS%20Lifecycle%20Final%20v1.0.pdf

[CPNI2] CPNI, “SECURITY FOR INDUSTRIAL CONTROL SYSTEMS, ESTABLISH ONGOING GOVERNANCE, A GOOD PRACTICE GUIDE”, Version Final v1.0. https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/SICS%20-%20Establish%20Ongoing%20Governance%20Final%20v1.0.pdf

[KYBER-TEO-2014] Kyberturvallisuuden kehittäminen ja jalkauttaminen teollisuuteen vuonna 2014. KYBER-TEO 2014 Tuloksia, https://www.huoltovarmuuskeskus.fi/julkaisut/

[SAS1] Suomen Automaatioseura Ry, ”Automaatiosuunnittelun prosessimalli; Yhteiset käsitteet verkottuneen suunnittelun perustana” (SAS julkaisusarja nro 35), Helsinki 2007. https://www.automaatioseura.fi/site/assets/files/1367/automaatiosuunnittelun_prosessimalli.pdf

2. Politiikat ja ohjeet

Miksi kyberturvallisuuspolitiikka on usein huonosti tunnettu ja ymmärretty käsite teollisuustuotannossa? Tuotannon kyberturvallisuuspolitiikka saattaa pahimmillaan olla liian teknokraattisesti kirjoitettu ja vaikeasti hahmotettava, usein IT-terminologiaa viljelevä dokumentti, jonka yhtymäkohdat käytännön tuotantotason työhön ovat epäselvät.

Selkeä kyberturvallisuuspolitiikka ja yksinkertaiset ohjeet ovat perusta kyberturvallisuuden kehittämisessä ja ylläpitämisessä. Tämä koskee erityisesti teollisuusautomaation kyberturvallisuutta, jossa joudutaan usein toimimaan monitoimittajaympäristössä yhteistyössä useiden eritasoisten toimijoiden kanssa. Tällöin toiminnan kokonaisturvallisuuden varmistamista ja ohjeiden noudattamisen valvontaa joudutaan kehittämään erityisen huolellisesti.

Oppi 2. Selkeällä kyberturvallisuuspolitiikalla ja toimivilla ohjeilla pääsee pitkälle.

Kyberturvallisuutta ei voi kopioida toisilta.

Tuotantoyrityksen uhkiin ja toimintatapaan soveltuvat ohjeet kannattaa räätälöidä kullekin henkilöstöryhmälle erikseen ja panostaa tiedottamiseen ja toimeenpanoon.

Hyvä kyberturvallisuuspolitiikka

- ottaa huomioon yrityksen liiketoimintamallin ja riskianalyysien tulokset
- yhdistää kyberturvallisuuden osaksi muuta turvallisuutta ja jatkuvuutta
- on helposti ymmärrettävä, looginen ja hyvin tiedotettu
- toimii perustana tarkempien kyberturvallisuusohjeiden laadinnalle

2.1 Politiikka ja maine

Laaja-alaisemmin tarkasteltuna yrityksen maineen ylläpitoon liittyy monenlaisia politiikkaan, toimintakulttuuriin, kansainvälisiin toimintatapoihin, lakeihin ja sääntöihin liittyviä tekijöitä, ei pelkästään kyberturvallisuuspolitiikat.

UUSIA MAINEUHKIA: Automaatiojärjestelmätoimittajan tai automaatiota hyödyntävän yrityksen yleistä mainetta ja liiketoimintaa saatetaan omaehtoisesti tai vahingossa vahingoittaa:

- TOIMITTAJAT: myymällä kehittyneitä kyberturvallisuuden seuranta- ja testaustuotteita tai palveluja epädemokraattisiin maihin, joissa tuotteita voidaan käyttää ihmisoikeuksien loukkauksiin
- HYÖDYNTÄJÄT: ostamalla ja käyttämällä omassa liiketoiminnassa automaatio- tai kyberturvallisuustuotteita, jotka ovat peräisin maista, joissa yrityksiä velvoitetaan asentamaan ja piilottamaan esim. etähaltuunoton mahdollistavia takaportteja ulkomaille toimitettaviin tuotteisiin

2.2 Lähtökohtia kyberturvallisuuspolitiikalle

Seuraavaksi luodaan lyhyt katsaus kyberturvallisuuspolitiikkojen parhaisiin lähteisiin kahdelta eri suunnalta. Ensin esitellään lyhyesti automaatiospesifistä standardia IEC 62443 ja sitten SANS-instituutin (https://www.sans.org/) kehittämiä kyberturvallisuuspolitiikan malleja. IEC-standardi ja politiikan SANS-mallipohjat täydentävät toisiaan ja kumpaankin kannattaa tutustua, sillä yhdessä nämä antavat arvokkaan näkemyksen, kun yrityksen tuotannon kyberturvallisuuspolitiikkoja luodaan tai päivitetään.

Uusien teknologioiden osalta kannattaa analysoida tarvitsevatko ne oman kyberturvallisuuspolitiikan. IoT (*Internet of Things*) on eräs tämän hetken kuuma aihe. Onko olemassa riski, että IoT-laitteita asennetaan vaivihkaa sisäverkkoon ja vasta jälkikäteen huomataan mukana tulleet kyberuhat? IEC 62443-standardista ja SANS:n mallipohjista puuttuvat myös oman laitteen käyttäminen työtehtäviin (*BYOD, Bring Your Own Device*). BYOD-aihe on hyvin laaja alkaen satunnaisesta sähköpostien luvusta omalla laitteella jatkuen oman tabletin päivittäiseen käyttämiseen työtehtävissä.

2.2.1 Standardi IEC 62443

Standardi IEC/TS 62443-1-1 (IEC/TS 62443-1-1:fi, 2013, SFS) [IEC62443-1-1] on yksi tärkeimmistä automaatioalan standardeista, joka korostaa kyberturvallisuuspolitiikkojen muodostavan säännöt sille, miten organisaatio suojaa herkkiä ja kriittisiä järjestelmäresursseja. Politiikat ovat dokumentteja, joita vasten voidaan mitata sääntöjen noudattamista esimerkiksi auditoinneissa.

Tämä standardi jakaa politiikat kolmeen pääosioon: SÄÄNNÖT, joita täydentävät MENETTELYT, ja näiden lisäksi on mahdollista laatia OHJEITA. Ohjeet kertovat yleensä asian toteuttamisen yhdellä tavalla, joka on suotava muttei pakollinen tapa. Ohjeet voivat olla moniselitteisiä, joten sen takia ohjeita vastaan ei yleensä auditoida.

IEC-standardi kohdentaa huomiota politiikkojen koordinointiin, koska organisaation eri osastot ovat erilaisia ja sen takia politiikat saattavat hajaantua liikaa ilman koordinointia. Koordinointi automaation ja yritystason IT:n kanssa on erityisen tärkeää. Elinkaariajattelua tuodaan myös esille, eli järjestelmän elinkaaren eri vaiheissa politiikoilla on erilaiset profiilit. Kunkin politiikan tulee sisältää lyhyt mutta tarkka kappale ko. politiikan tarkoituksesta ja soveltamisalasta. Politiikkadokumenttien kielen tulee olla yksiselitteistä, jotta erottuu selkeästi, että mikä on vaatimus ja mikä valinnainen ohje.

2.2.1.1 Yritystaso, säännöt

Yritystason politiikka määrittää organisaation yleiset kyberturvallisuustavoitteet, esimerkiksi toimistoverkossa luottamuksellisuus voi olla ykköstavoite, kun taas automaatioverkossa toiminnan jatkuvuus on luonnollinen ykköstavoite. Vastuut ja velvollisuudet tulevat myös esille yritystason politiikassa. Selkeä tiedottaminen kaikille työntekijöille on tärkeää.

2.2.1.2 Menettelyt

Kyberturvallisuusmenettelyillä toteutetaan yritystason politiikoissa määritellyt tavoitteet ja vaatimukset. Menettelyjen toteutus perustuu prosesseihin, joissa käsitellään kaikki politiikkojen näkökohdat. Menettelyihin kuuluvat seuraavat pääosiot:

a) järjestelmäsuunnittelu

b) hankinta

c) asennus

d) prosessin toiminta

e) järjestelmän ylläpito

f) henkilöstö

g) auditointi

h) koulutus.

Huomautus: Menettelylistasta puuttuu elinkaaren loppuvaihe, mm. datan ja laitteiden käytöstä poistaminen (esim. datan siivoaminen, datan tuhoaminen, laitteiden kierrätys ja laitteiden poisto).

Menettelyprosesseissa määritellään toimenpiteiden sekä vastuut ja velvollisuudet että toimenpiteiden ajankohdat.

IEC-standardi painottaa lisäksi politiikkojen ja menettelyjen tehokkuuden mittaamista, jotta voidaan tarkistaa, tuottavatko ne sitä, mitä tavoitellaan. Tehokkuutta pitäisi mitata myös kustannusten näkökulmasta, esimerkiksi onko riskin pienentämiseksi tehty investointi vastannut saavutettua tulosta.

Huomautus: IEC-standardin kattamista aiheista puuttuu mm. kyberturvallisuustapahtumien käsittely; mitä tehdään, kun jotain poikkeuksellista on havaittu (esim. välittömät toimet, raportointi, tutkinta, palautus normaalitilanteeseen, oppiminen jne.).

2.2.2 SANS-tietoturvapolitiikat

SANS-instituutti on laatinut sarjan tietoturvapolitiikkojen mallipohjia, jotka on päivitetty vuonna 2014 [SANS-2014]. SANS-instituutti määrittää eroavaisuudet POLITIIKAN, STANDARDIN ja OHJEISTUKSEN välillä niin, että politiikka on dokumentti tiettyjä vaatimuksia ja sääntöjä varten, joita täytyy noudattaa. Standardi taas sisältää järjestelmä- tai menettelytapakohtaiset vaatimukset, joita täytyy noudattaa. Esimerkkinä vaatimukset tietyn käyttöjärjestelmän sisältävän työaseman koventamisesta DMZ-alueeseen sijoittamiseksi. Standardissa voidaan myös määrittää teknologiavalintoja. Ohjeistus käsitetään kokoelmana parhaita käytäntöjä. Ohjeistus ei sisällä pakollisia vaatimuksia, vaan vahvoja suosituksia.

SANS-mallipohjat sisältävät yhteensä 27 politiikkaa, standardia tai ohjeistusta. Näitä voi käyttää tarkistuslistana, että kaikki oleelliset asiat on käsitelty. Vahva suositus on, että kannattaa lukea kaikki SANS-politiikat. Mikäli jokin politiikka jätetään määrittelemättä, sen tarpeettomuus tulisi dokumentoida ja olla tietoinen valinta perustuen riskiarviointiin. Yksittäinen edellä mainittu politiikka voi sinällään olla yritykselle tarpeeton.

SANS-instituutti jakaa tietoturvapolitiikat neljään ryhmään; *yleinen tietoturva*, *verkkojen tietoturva*, *palvelinten tietoturva* ja *sovellusten tietoturva*. Nämä mallipohjat voivat päivittyä, eli lukijan kannattaa tarkistaa uusimmat versiot SANS:n verkkosivuilta.

2.2.2.1 Yleinen tietoturva

Yleinen tietoturva sisältää seuraavat mallipolitiikat: hyväksyttävä salaus, hyväksyttävä käyttö, puhdas työpöytä (*Clean Desk*), digitaalisten allekirjoitusten hyväksyminen, katastrofista toipumisen suunnittelu, sähköposti, loppukäyttäjän salausavaimen suojaus, tietoturvaetiikka, pandemiaan reagoinnin suunnittelu, salasanan laatimisen ohjeistus, salasanan suojaus, ja tietoturvavasteen suunnittelupolitiikka.

2.2.2.2 Verkkojen tietoturva

Verkkojen tietoturva sisältää seuraavat mallipolitiikat: hankinnan arviointi, Bluetoothin lähtökohta (baseline), vaatimuspolitiikka, etäkäyttö, etäkäytön työkalut, reitittinten ja kytkinten tietoturva, langaton kommunikaatio ja langaton kommunikaatiostandardi.

2.2.2.3 Palvelinten tietoturva

Seuraavat mallipohjat kuuluvat palvelinten tietoturvaan: tietokannan käyttötietojen (*credentials*) ohjelmointi, tietojen lokistandardi, laboratoriotietoturva, palvelinten tietoturva, ohjelmistoasennukset, teknisten laitteistojen hävittäminen ja työaseman tietoturvapolitiikka.

2.2.2.4 Sovellusten tietoturva

Sovellusten tietoturva sisältää vain yhden politiikan eli web-sovellusten tietoturvan.

2.3 Cybersecurity Guideline – Case

2.3.1 Työn tausta

Laadimme KYBER-TEO-projektissa tuoteperhekohtaisen kyberturvallisuusohjeen yhdessä ABB Drivesin kanssa. Tämä edustaa parhaimmillaan yhteistyötä, jossa kehitettiin automaatiojärjestelmien suunnitteluun ja toteutukseen liittyvien tuotteiden käyttöönoton ja käytön kyberturvallisuuspolitiikkoja ja ohjeita. Samalla tuotettiin automaatiota hyödyntäville tuotantoyrityksille konkreettisia käyttötapausesimerkkejä, jotka nekin asetettiin julkisesti saataville.

ABB:n kansainvälisestä liiketoiminnasta johtuen seuraavaksi lyhyesti esitelty tekninen ohje (*guideline*) on kirjoitettu englanninkielisenä.

2.3.2 Cybersecurity for ABB Drives

As a best practice, we present here some selected portions from the Cybersecurity guideline developed for ABB Drives [ABBDRIVES-CYBER].

2.3.2.1 Generic risk reduction methods and cybersecurity policies

There is no single solution to managing the cybersecurity risk in an industrial control system, nor is there a completely secure system. Hence, like many other instances, ABB recommends “defense in depth,” which means the coordinated use of multiple security countermeasures and addressing people, technology, and operations in several layers.

In the defense-in-depth architecture, the control system LAN (local area network) is clearly separated from other corporate networks with firewalls, and there are separate demilitarized zone (DMZ) areas for each function, such as for historian, security and authentication.

The majority of cybersecurity risks can be controlled by feasible network architectures, access control and physical security mechanisms. Undisturbed security and management also requires a strict cybersecurity policy and approach that includes various viewpoints and activities to keep up the targeted level of cybersecurity in automation.

The basic risk reduction methods and cybersecurity policies are listed below:

Physical security mechanisms

- Tamper detection of unauthorized access (for example, inspecting sealing)
- Tamper-resistant equipment (for example, disabling debug interfaces)
- Locking of facilities and rooms
- Locking devices for the cabinets
- Physical access based on work permits, asset security and CCTV monitoring (video surveillance)

Electronic access control

- Firewalling the external access, which should deny any access from unauthorized parties
- Account-based electronic access control
- Encryption of remote access data in transit

Network architectures and protocols

- Segmented network solution architecture with separated automation segments
- Segmentation of data networks into independent subnetworks that minimize any problem propagation
- Allocating secure gateways and DMZs that enable application-level control
- Site and automation firewalls in use with appropriate maintenance
- Virtual private network (VPN) solutions for remote access and strict access control
- Cryptographic protocols and algorithms for securing data communication using authentication, integrity and confidentiality protection, and replay protection

Cybersecurity procedures and policies

- Background checks, instructions and training of personnel and subcontractors
- Guides on what actions are permitted, using which tools, by whom, and when
- Logging and cybersecurity monitoring methods in automation systems and networks

Computer policies

- Backup and update in use and recovery tested
- Endpoint protection in use with appropriate maintenance
- Allowed applications specified and others removed
- Media encryption solution in use

Account management

- Authentication methods before devices, software or users get access to the network
- Access account management process in use and roles defined
- Removal procedure for default accounts and passwords

Patch management

- Managed installation of software and security patches, including change management

2.3.2.2 Cybersecurity versus safety

Cybersecurity in automation aims for retaining a continuous operation. This means that the safety and operational continuity requirements become first, and the cybersecurity requirements follow these. For example, antivirus software must not be permitted to halt the operation of a safety system or process control system under any circumstances.

The same priority applies to remote access solutions. No technological solution may be permitted to hinder a local operator from controlling the operation equipment locally, even if the secure remote access would go to error condition.

The first objective in automation is to maintain the safe operation and data even in the following cases:

- Control, support and backup system malfunction
- Human operator mistakes
- Remote access situations
- Maintenance operations
- Online support

The cybersecurity objectives are subordinate to safe operation requirements. The identification of cyberattacks, industrial espionage and malicious and unauthorized software are important subordinate goals.

2.3.2.3 Roles and responsibilities

Usually, the owner of the business has the main responsibility for selecting, deploying and maintaining the cybersecurity of applied technical solutions. However, it is practically impossible for one player to control all aspects of cybersecurity and production continuity. Co-operation is needed with many partners to design, construct and maintain a feasible level of cybersecurity for continuous operation.

These are examples of partners and their roles ensuring valuable cybersecurity co-operation:

- **Systems integrators**. Competence in and experience of integration challenges, possible platform weaknesses and cybersecurity bottlenecks in system integration.
- **Telecommunication network operator**. Establishing and cybersecurity monitoring of private access points and possibly VPNs for customers.
- **Office security services**. Physical access control and monitoring of facilities, rooms, cabinets, etc.
- **Automation vendor**. Validation and approval of all cybersecurity solutions, before their actual commissioning in the field. Adviser on secure usage of devices and applications, upgrades, patches, maintenance and monitoring services, etc.
- **Network equipment vendor and LAN operator services**. Establishing and maintaining a secure network architecture together with managed switches (VLANs), routers (networks), firewalls (access control), and monitoring services (identification of malicious behavior or software).
- **Software providers**. Maintenance of operation system software, antivirus software, management software, etc.

2.3.2.4 Generic cybersecurity solutions

Automation system operation can fail totally due to the reason that cybersecurity was not put in place and protection features were not used.

Secure operation must be tested in all possible use cases of an automation system. Penetration testing can reveal the hidden threats in the overall system, so such an opportunity should be arranged at the integration site before letting the automation system setup go to the production phase. In penetration testing, external experts that are familiar with e.g., hacking tools and methods may be needed.

Cybersecurity levels and their accompanying requirements help to understand whether cybersecurity is covered sufficiently in a project or in an operational automation service. Good examples of cybersecurity requirements and levels can be found in IEC 62443-3-3, *System Security Requirements and Security Levels*. Requirements should be applied according to identified threats.

The targeted cybersecurity level can be maintained by constantly monitoring the new vulnerabilities in products that are used and applying the related software patches whenever possible. Networks need to be monitored against unauthorized access and spy software. It is not possible to act without knowing what threats can be encountered every day. It is important to track who is present in a network and if someone is trying to access it without permission, for example through a firewall protection layer. There are also network cybersecurity monitoring services available that can be used and guided specifically to report any anomalies or attacks that occur during the operation of an automation system.

Cybersecurity must be considered in all phases. Otherwise, the risk can find its way to the target without notice. The table below lists typical cybersecurity considerations in different project phases.

Phase	Cybersecurity activity
Development & pilot phases	Install the firewalls and remote access (VPN) solution according to company policy and cybersecurity requirements.
	Enable remote access only for authorized vendor personnel with authorized user accounts.
	Restrict (each user account) access from different vendors to subnetworks or machines belonging to the delivery.
	Install trusted signed SW packages only from trusted sources (eg, from ABB Drives site with HTTPS).
	Install vendor-approved patches.
Commissioning phase	Hardening of systems. Check and ensure that there is a specific cybersecurity configuration in all network and automation devices, systems and software according to the deployment guidelines. All unnecessary software and features should be removed from the delivery.
	Test that all systems and cybersecurity mechanisms work according to the specifications.
	Communicate to all users and train them in the established cybersecurity and change management procedures.
	Establish network cybersecurity monitoring systems and ensure that these cannot negatively affect the system operation under any circumstances.
Maintenance	Keep up the hardening by strict access and change control, allowing only planned changes and patches to systems including ABB products, network devices and operation systems.
	Monitor the system logs for unauthorized access or other suspect behavior.
	Plan and test system upgrades and new features in test facilities before applying them to production systems.

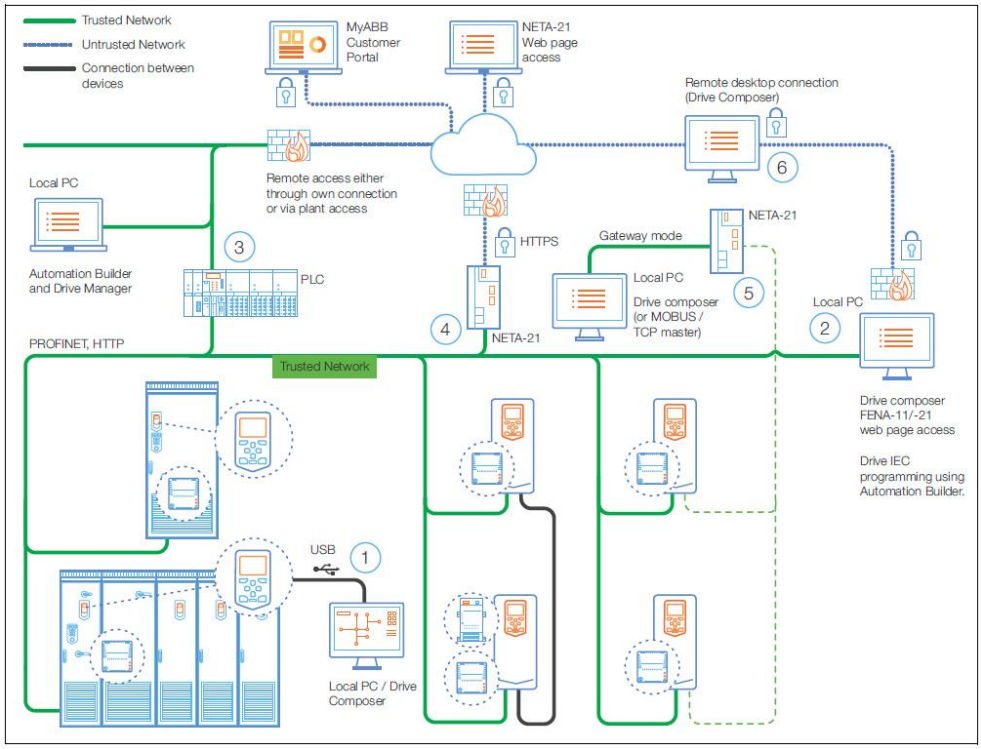
Figure/Kuva 3. Cybersecurity activities in each phase.

2.3.2.5 Case 1 – Industrial automation example (factory environment)

This example describes generic means of protecting the industrial automation environment against unauthorized access.

Industrial automation systems vary a lot in practice. There are a large number of different networks and automation application architectures implemented globally within different industrial sectors, such as manufacturing, process industry, power generation and distribution. That is why this example is for general use only and does not offer all of the necessary details for implementing a secure system. As far as deployment of ABB drive and connectivity products, all guidelines and instructions are real and valid though.

Next Figure depicts a fictitious plant network utilizing ABB Drives products that is usually connected securely to the customer's corporate networks (not visible in the image) via public or private networks, but also to other automation field networks within the plant.



Figure/Kuva 4. Industrial automation plant. Different network possibilities and their secure deployment [ABBDRIVES-CYBER].

2.3.2.5.1 Use cases

Figure above shows several different use cases and communication possibilities. See the figure for the numbers referred to below. The shown use cases are:

Commissioning of the drives and production line using the Drive composer start-up and maintenance tool and/or Automation Builder suite tool via:
1. local connections (point-to-point serial communication, ie, USB) or
2. shared (with control) upper-level physical fieldbus network (eg, PROFINET) using Ethernet tool communication and/or
3. communicating also through PLC system using Drive Manager device tool or
4. NETA-21 remote monitoring tool web interface or
5. NETA-21 acting as a gateway between or
6. third-party remote desktop connection.

Maintenance and troubleshooting using the aforementioned tools and communication networks

Remote support and remote condition monitoring services

On-demand based remote monitoring over untrusted network (public Internet) using the NETA-21 remote monitoring tool.

2.3.2.5.2 Components

The illustrated architecture includes the following components:

In the public networks, there are services such as:
- MyABB Customer Portal (cloud service)
- Remote monitoring via web page access, e.g., NETA-21 remote monitoring tool.
- Remote desktop connections (Drive composer)

In the trusted plant network, there are:
- Firewalls in front of public networks
- PLCs and local PCs (different software tools installed)
- Drives that are connected to Ethernet fieldbus (e.g., PROFINET) via FENA-11/-21
- Drives that are connected to a local PC via USB
- NETA-21, that is also connected to public networks via firewall
- NETA-21 that is connected to the drives with EIA-485 and to a local PC using gateway mode

2.3.2.5.3 Cybersecurity risk mitigation and secure deployment

The idea is to create defense-in-depth protection for each network by allocating firewall solutions to the front of internal trusted networks of each network. Carefully manage firewalls, their configurations and access rules.

Ethernet fieldbus adapters FENA-11/-21 deployment
FENA-11/-21 must be positioned in a trusted network (strictly limited and well hosted portion of a network or control system)

On the FENA-11/-21 service configuration page (web page) certain Ethernet services can be disabled. All services are enabled by default. It is recommended to disable services that are not used after commissioning:

- PC tool communication or access to FENA-11/-21 web pages
- Change of IP settings remotely using ABB IP configuration tool
- Remote access to drives with Drive composer tool via Ethernet tool network
- Ping response

ACS880 industrial drives deployment
User lock: For better cybersecurity, it is possible to set a master password to prevent e.g., the changing of parameter values and/or the loading of firmware and other files.

The user lock feature makes it possible to prevent:

- firmware upgrades
- safety functions module (FSO-12/-21) configuration
- parameter restoration
- loading of adaptive or application programs
- changing home view of control panel
- editing drive texts
- editing the favorite parameters list on the control panel
- configuration settings available through control panel such as time/date formats and enabling/disabling clock display.

User access levels: Configure for local user interfaces (Drive composer and control panels) parameter access rights using parameter lock feature.

Drive composer PC tool Ethernet tool communication deployment
Drive composer establishes Ethernet communication only with “recognized devices”, that is, FENA-11/-21 Ethernet fieldbus adapters. This is the default mode of operation.

Remote monitoring tool NETA-21 deployment
Configure the cybersecurity features of NETA-21 according to the principle of denying everything that is not needed nor used.

- Change the default administrator password.
- Create only those accounts that will be used locally or remotely, using roles with as few access rights as possible. Use strong passwords.
- Check that the latest firmware version of the NETA-21 tool is being used, to have the latest software versions and security patches in use.

For secure access, use HTTPS, which is a combination of HTTP with an added encryption layer of SSL/TLS protocols to create a secure channel over an insecure network.

If the highest possible degree of product hardening is required, then it is possible to also do the following modifications:

- Tool settings (factory tools): disable the SSH service (factory support account) when SSH console for support and diagnostics is not needed.
- Locale settings: disable NTP (Network Time Protocol) requests that NETA-21 can send to external servers, or replace with local NTP time servers if such are available.
- Device interfaces / Ethernet (interface settings): disable the background scan that broadcasts UDP discovery requests on the local network to discover Ethernet-connected ABB drives.

The following network services should be disabled if they are not used:

- NBT NS discovery (NetBIOS name discovery service)
- FTPS service, even though no FTP(S) accounts exist by default
- Ethernet tool network, automatic discoverability of NETA-21 within local network

If NETA-21 and Drive composer are used at the same time over Ethernet, the PC tool friendly mode should be used in NETA-21.

Actively monitor the internal network. Specifically track for any unauthorized devices.

2.4 Referenssit

[ABBDRIVES-CYBER] Cybersecurity for ABB drives, Technical guide, 3AXD10000492137 Rev A, EN, EFFECTIVE: 2016-06-09
https://library.e.abb.com/public/e71305ed2cd747b3b65a2becaf9a58bd/EN_Cybersecurity_guide_A_A4.pdf

[IEC62443-1-1] IEC/TS 62443-1-1 Standardi (IEC/TS 62443-1-1:fi, 2013, SFS)

[SANS-2014] https://www.sans.org/security-resources/policies

3. Uudet vaatimukset

3.1 Uusia uhkia

Kyberturvallisuuden tutkimusalue on kehittynyt nopeasti valtavan laajaksi. Tämä johtuu mm. siitä, että verkkorikollisilla on ollut käytettävissään suljettuja yhteisöjä ja teknologioita, esim. *Tor-verkko*, joissa kehittää jatkuvasti uusia teknisiä ja yhteisöllisiä keinoja ansaita tietoverkoissa rahaa laittomasti jäämättä kiinni. Voidaan jopa sanoa, että rikolliset ovat ottaneet onnistuneesti ”tuotantokäyttöön” uniikkia ohjelmistoteknologiaa ja uudenlaista yhteistoimintaa. Alalle on kehittynyt valtavasti myös rikollista palvelutoimintaa.

Täten myös uhrit ja viranomaiset joutuvat tutustumaan jatkuvasti uusiin salassa kehitettyihin kybermaailman työkaluihin ja kehittämään menetelmiä aina uudenlaisen verkkorikollisuuden tunnistamiseksi ja estämiseksi. Tämä johtaa tietysti myös jatkuvasti uusiutuviin kyberturvallisuusvaatimuksiin, joihin esim. järjestelmien ylläpitäjien tulee tutustua ja ottaa käyttöön mahdollisimman tehokkaita suojauksia.

Uudentyyppisiä kyberuhkia lisääviä trendejä ovat mm. kiristyshaittaohjelmien levittäminen ja rahastus (esim. Bitcoinin avulla), harhauttaminen valemediaa ja uutisia levittämällä, IoT-laitteiden laiton haltuunotto ja hyväksikäyttö, sekä kaksikäyttötuotteiden väärinkäyttö, kuten turvallisuusanalyysiin käytettävien työkalujen käyttö kyberhyökkäyksiin ja vahvan salauksen käyttö viranomaisilta pakoiluun. Esimerkiksi tietoturvayhtiö Trend Micro tutki viime vuonna Ranskan kyberrikollisuutta, ks. “The French Underground, Under a Shroud of Extreme Caution”, 2016 [TREND-FR]. Trend Micron tutkimuksen tulosesimerkkejä (alamaailmasta ostettavista rikollisista palveluista ja tuotteista):

- *Salauspalvelu (Fully undetectable crypting service)*
- *Varmistettu verkkopalvelu (Bulletproof-hosting service)*
- *Tietojenkalastelun (phishing) työkalu, web-sivu, web-kehityspalvelu*
- *Botnettien eli kaapattujen koneiden vuokraus*
- *Pääsy haltuunotetuille tileille tai verkkoihin*
- *Väärennetyn kansallisen henkilökortin, identiteetin tai todistuksen myynti*
- *PDF-tiedostojen editointipalvelu (sis. meta-tiedot)*
- *Laiton pääsy haavoittuville web-sivustoille (SQL injection-avulla)*

- *Varastetun datakaappauksen myynti*
- *Ohjelmistojen haavoittuvuusskannauspalvelu*

Esimerkkejä kyberrikollisille tarjottavista kursseista:

- *Miten kyberrikollisten yhteistyö toimii?*
- *Kuinka käyttää etäkäyttö-troijalaista?*
- *Miten levittää haittaohjelmia?*
- *SQL injection -toteutus*
- *Miten rahastaa haltuunotetuilla käyttäjätileillä?*
- *Miten lähettää ja vastaanottaa laittomia tavaroita ja maksuja anonyymisti?*
- *Pankkikortti- ja pankkitilihuijaaminen*

Lisäksi on todettava, että valtiollinen (pitkälle kehittynyt) tiedustelutoiminta kohdistuu aktiivisesti myös Suomeen.

3.2 Standardien merkitys

Standardien merkitys teollisuuden kyberturvallisuuden parantamisessa on merkittävä, sillä niiden kautta voidaan asettaa myös laajempia yhteisiä tavoitteita ja referenssimalleja. Standardien kautta saadaan välitettyä tietoa mm. tärkeimmistä tehtävistä (käyttöä mm. tarkastuslistoina), vaatimuksista, sanastoista ja mahdollisesti soveltamisohjeista oman toiminnan ja työnjaon pohjaksi. Standardien soveltaminen osaksi omaa toimintaa edellyttää yrityskohtaista räätälöintiä ja mikä vielä tärkeämpää, uusien konseptien ja ohjeiden toimivuuden testausta ennen niiden laajamittaista käyttöönottoa.

Miksi kyberturvallisuusvaatimusten esittäminen saattaa olla niin vaikeaa automaatiojärjestelmien hankintavaiheessa? Esimerkkejä:

- TILAAJA: Hankintaorganisaatio ei ymmärrä kyberturvallisuusvaatimusten merkitystä liiketoiminnalle ja joutuu projektin kustannuksia säästääkseen vähentämään turvallisuusvaatimuksia. Yritys ei ole kyberturvallisuustietoinen eikä omista kyberturvallisuuden vaatimuskantaa jota soveltaa eri projektien hankinnoissa
- TOIMITTAJA: Jotkut automaatiotoimittajat eivät tiedä miten vastata kyberturvallisuutta koskeviin kysymyksiin ja miten kyberturvavaatimukset kannattaa toteuttaa tehokkaasti asiakkaan tuotantoympäristö huomioiden.

Miten kyberturvallisuus saadaan luonnolliseksi osaksi yrityksen hankintaprosesseja? Tätä on jo esitelty julkisessa tulosraportissamme [KYBER-TEO-2014] ”Kyberturvallisuuden kehittäminen ja jalkauttaminen teollisuuteen vuonna 2014”. Avainhenkilöstön tulee mm. läpikäydä yhdessä soveltuvia standardeja ja määritellä kyberturvallisuuden perusvaatimukset tuotantotoiminnassa. Vaatimukset tulisi katselmoida säännöllisesti suunnittelu- ja hankintaosaston henkilöstön kanssa, jotta ne

myös ymmärretään ja otetaan käyttöön kyberturvallisuusliitteissä, jotka otetaan osaksi hankinnan kaikkia tarjouspyyntöjä ja sopimuksia.

Oppi 3. Kyberturvallisuus vaatii jatkuvaa toimintaympäristön seurantaa ja oman ja ulkoistetun toiminnan kehittämistä.

Turvallisuusvaatimusten tulee uusiutua uusia teknologioita, kyberuhkia ja käyttötapauksia vastaaviksi, joten kyberturvallisuus edellyttää jatkuvaa toimintaympäristön seurantaa ja oman ja ulkoistetun toiminnan kehittämistä.

Relevanttien kyberturvallisuusvaatimusten ymmärtämiseen tarvitaan mm. kyberturvallisuuspäälliköiden, IT-osaston, hankintatoimen, projektipäälliköiden ja ulkoisten kyberturvallisuusasiantuntijoiden vuoropuhelua.

Olemme aiemmissa projekteissa (mm. COREQ-VE ja COREQ-ACT) kehittäneet valmiin kyberturvallisuusvaatimuskannan ja ohjeita automaatiohankintoja varten, joten niitä ei käsitellä tässä sen enempää. Sen sijaan keskustelemme sellaisista uusista kyberturvallisuusvaatimuksista, joita ei ole vielä otettu Suomessa riittävän laajalla rintamalla käyttöön. Taustalla ovat mm. kyberrikollisuuden ja valtiollisen tiedustelun kehittyminen edelleen ja kohdistuminen myös Suomeen sekä mm. uusien EU-direktiivien velvoittavat vaikutukset.

3.3 NIS-direktiivin vaikutuksista standardeihin

Eurooppalaisiin kansallisvaltioihin on jo joitakin vuosia kohdistunut painetta kyberturvallisuuteen liittyvän lainsäädännön uudistamiseksi muutaman vuoden kuluessa ja mm. EU-direktiivien vaatimusten täyttämiseksi. Huoltovarmuuskriittisiin toimijoihin kohdistuu uusia vaatimuksia erityisesti NIS-direktiivin johdosta [NIS-DIR] ”Toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa”. NIS-direktiivi kohdistuu erityisesti seuraaviin kriittisiin infrastruktuureihin ja asettaa jäsenmaiden toteutettaviksi erityisiä velvoitteita toimialoille:

- energia
- liikenne
- pankkiala
- finanssimarkkinoiden infrastruktuurit
- terveydenhuoltoala
- juomaveden toimittaminen ja jakelu
- digitaalinen infrastruktuuri.

Millaisia konkreettisia vaatimuksia ja pakotteita tämän seurauksena on odotettavissa huoltovarmuuskriittisille toimijoille ja toimittajille? Tämä on toistaiseksi keskeneräinen asia. NIS-direktiivin mukaan [NIS-DIR]:

”Tehokas reagointi verkko- ja tietojärjestelmien turvallisuuden asettamiin haasteisiin edellyttää sen vuoksi unionin tason kokonaisvaltaista lähestymistapaa, joka kattaa valmiuksien luomista ja suunnittelua koskevat yhteiset vähimmäisvaatimukset, tiedonvaihdon, yhteistyön sekä yhteiset turvallisuusvaatimukset keskeisten palvelujen tarjoajille ja digitaalisen palvelun tarjoajille.”

NIS-direktiivi johtaa varsin konkreettisiin vaatimuksiin kokonaisvaltaisen turvallisuusajattelun kautta erityisesti ”minimitason” tietoturvakontrollien määrittelyyn ja tietoturvatapahtumien luottamuksellisen tiedonvaihdon toteuttamiseksi koko EU:ssa.

Mitä teknisiä arkkitehtuuri- ja toteutusvaatimuksia tästä aiheutuu esimerkiksi automaatiojärjestelmätoimittajille ja IT-palvelutarjoajille? Tätäkään ei vielä aivan varmasti tiedetä. Toisaalta ETSI (European Telecommunications Standards Institute) on parasta aikaa standardisoimassa NIS-direktiivin käytännön implementointiin liittyviä teknisiä yksityiskohtia työryhmässä CYBER-0021. Standardista on jo olemassa (varhainen) raporttiluonnos “TR 103 456, Implementation of the Network and Information Security (NIS) Directive”. Työryhmä-0021 on jo helmikuussa 2017 kollektiivisesti lausunut, että ko. raporttiluonnoksessa kuvattu lähestymistapa ja rakenne vastaavat aiottua tarkoitusta ja että raportti tulisi todellakin helpottamaan NIS-direktiivin implementointia. TR 103 456 on tarkoitus julkaista heinäkuun lopussa 2017:

- TIEDONVAIHTO: Tekniseksi tietoturvatapahtumien luottamuksellisen tiedonvaihdon toteuttamisen pohjaksi CYBER-0021 on ehdottanut globaalisti tunnustettuja STIX 2.0 / TAXII / CyBOX -alustoja, joita soveltamalla voitaisiin määritellä tarvittavat datasyntaksi, semantiikka ja tiedonsiirto.
- KYBERTURVAKONTROLLIT: CYBER-0021 on ehdottanut pohjastandardeiksi ETSI TS 102 165-1, ETSI TR 103 305, ISO/IEC 15408 ja relevantteja osia ISO/IEC 27k -sarjasta.

Seuraavassa kohdassa nostetaan esiin vaatimuksia, jotka eivät ole riittävästi kuuluneet käytännössä tuotannossa toteutettujen vaatimusten joukkoon.

3.3.1 Nousevia vaatimuksia

ETSIn tekninen raporttisarja TR 103 305 [ETSI-103305] nostaa esiin tärkeitä nousevia vaatimuksia, joihin liittyvää osaamiskehitystä ja käytännön toteutusta olemme KYBER-TEO-projektin kuluessa jo ainakin osin kehittäneet tai testanneet. Seuraavassa taulukossa joitakin yhä lisääntyvää huomiota ja jatkotyöstöä ansaitsevia esimerkkivaatimuksia. Lähde: [ETSI-103305].

KONTROLLI-LUOKKA	NOUSEVIA VAATIMUKSIA (esimerkkejä havainnoistamme)
CSC 1: Luettelo sallituista ja ei-sallituista laitteista	Käytetään verkkotyökalua, joka etsii ja kirjaa verkon laitteet automaattisesti. Käytetään (802.1x:n) verkkotason laitetodennusta. Järjestelmä valtuutetaan sertifikaateilla ennen yksityiseen verkkoon liittämistä.
CSC 3: Turvalliset asetukset laitteille ja ohjelmistoille	Säilytetään käyttöjärjestelmien levykuvia (*imaget*) ja ohjelmistojen asetuksia turvassa. Päivitetään kaikki levykuvat, joita käytetään järjestelmien uudelleenkäyttöönotossa. Tiedostojen *integrity checking* -työkaluilla varmistetaan, ettei kriittisiä tiedostoja ole muokattu. Automaattinen monitorointi ja hallinta asetuksille, jotka voidaan etänä testata ja pakottaa (työkaluineen).
CSC 4: Jatkuva haavoittuvuuksien arviointi ja korjaaminen	Automaattiset haavoittuvuusskannaukset viikoittain tai useammin. Haavoittuvuusskannaus myös sisäänkirjautumistilassa erillistä käyttäjätunnusta käyttäen. Haavoittuvuustietokanta päivitetään vähintään kuukausittain. Verrataan tapahtumalokeja haavoittuvuusskannausten tuloksiin. Haavoittuvuuksien riskit luokitellaan vaikutuksen mukaan. Automaattiset yikakorjausten- ja päivitystenhallintatyökalut käytössä. Skannausaktiviteettien ja niihin liittyvien ylläpitäjien tunnusten lokiseuranta.
CSC 19: Tietoturvahäiriöihin vastaaminen ja hallinta	Kyberhairioiden hallintakaytannot ja kuvaukset henkilöston rooleista. Määritetään häiriöiden käsittelyprosessin ja päätöksenteon johtohenkilöt. Kommunikoidaan henkilöstölle, miten kyberhäiriöistä ja poikkeamista pitää raportoida häiriöhallintatiimille: raportointiviive, sisältö ja käytännöt, ml. CERT-ilmoituskäytännöt ja kolmansien osapuolten yhteystiedot. Järjestetään hallintatiimin kanssa säännöllinen häiriöskenaarioiden läpikäynti henkilöstölle, jotta kaikki ymmärtävät nykyiset uhat ja riskit sekä omat velvollisuutensa.
CSC 20: Penetraatiotestit ja Red teamin harjoitukset	Suunnitellaan ja järjestetään säännölliset ulkoiset ja sisäiset penetraatiotestit. Toteuta säännölliset Red teamin harjoitukset, joissa testataan yrityksen valmiuksia tunnistaa ja pysäyttää hyökkäyksiä. Dokumentoi ja suunnittele harjoitustulosten pisteytys. Kehitä harjoitustestialusta sellaisille harjoituksille ja testeille, joita ei esim. riskien takia kannata toteuttaa todellisessa tuotantoympäristössä.

Kuva 5. Nousevia kyberturvallisuusvaatimuksia.

Nousevien kybervaatimusten myötä yrityksen omia kyvykkyyksiä tulee kehittää pitkällä aikajänteellä, sillä turvallinen toimintatapa edellyttänee tulevaisuudessa yhä kehittyneempiä henkilöstön kybertaitoja.

3.4 Turva-automaatiovaatimusten analyysi vuonna 2014

Analysoimme KYBER-TEO-2014-projektissa turva-automaatiojärjestelmiin tuolloin uutuutena tulossa olevia kyberturvallisuusvaatimuksia.

Class	Objective	Security Act
Change management	Agreed changes	Control each update task
Compensating controls	No holes in protection	Agree about compensating controls
Hardening	Hardened systems & applications	Harden all workstations and servers
Hardening	Maintained SIS hardening	Verify SIS changes & hardening
Instrument integrity	Maintained instrument integrity	Integrity retaining security countermeasures
Malicious code protection	Limited risk due to portable media	Restrict the use of portable media
Risk assessment	Identified & managed risks	Conduct Safety & Security risk assessments
Safety life cycle (SLC)	Coordinated security in SLC	Engage security responsible
Safety manuals	Documented SIS security countermeasures	Document SIS countermeasures and impacting interfaces
Secure remote access	Approved secure remote access	Verify approved accesses
Secure remote access	Monitored remote access	Authorization & monitoring of all remote accesses
Secure remote access	Secure SIS remote access policy	Ensure SIS remote access policies
Security monitoring	Monitored SIS system security	Standard SIS security monitoring
Security procedures	Documented cyber security	Document & maintain system and security countermeasures
Security standards	Follow up of security standards	Adopt standard requirements
Security testing	Tested security countermeasures	Revalidate changes to security methods
SIS protection	Maintain SIS operation & performance	Ensure that security mechanisms don't affect SIS
SIS protection	Secured SIS	Address security in safety life cycle
SIS protection	Maintain SIS operation & performance	Ensure that security countermeasures don't affect SIS
SIS protection	Avoid the impact to SIS operation	Evaluate security countermeasures
SIS protection	Fail safe SIS communication	Design of fail-safe SIS communication interface
SIS protection	Layered SIS protection	Agree multiple compensating controls
SIS protection	Unaffected SIS bypass	Ensure that security countermeasures don't affect SIS
SIS protection	Analysed changes	Analyze the impacts to safety before changes
SIS protection	Firewall protected integrated system	Install dedicated stateful firewalls
SIS protection	Layered SIS protection	Multiple firewalls, password mgmt, device network security
SIS security concept	Coordinated security in SLC	Document all SIS security countermeasures in detail
SIS support system	Independent SIS support system operation	Segregate SIS support system
SIS support system	Fully independent support system	Dedicated programming devices to SIS
System & information disposal	Planned decommissioning	Coordinate the decommissioning planning

Kuva 6. Turva-automaation kyberturvavaatimuksia. Analyysin kohteena oli [ISA-TR84].

Yllä analyysimme tuloksena yhteenveto toimista, joihin ISAn raportti [ISA-TR84] mielestämme kehotti. Turva- ja teollisuusautomaation kyberturvallisuuden riskit ja turvamenettelyt ovat konvergoituneet ainakin osittain. ISAn tekniseen raporttiin

TR84.00.09-2013 [ISA-TR84] oli siis ilmestynyt kyberturvallisuuteen liittyviä ohjeita ja vaatimuksia, joita analysoimalla yritimme ennustaa kyberturvamenettelyjen jalkautumista uusiin tuotteisiin ja kenttäasennuksiin.

Mallikelpoista ISAn suojausohjeessa [ISA-TR84] on ollut automaation koko elinkaaren huomioon ottaminen turvallisuuteen liittyvissä prosesseissa, sekä turva-automaatiojärjestelmien (*SIS – Safety Instrumented System*) erottaminen muista automaatiojärjestelmistä. Standardi IEC 61511, eli prosessiteollisuuden sovellusstandardi toiminnallisen turvallisuuden yleisstandardista IEC 61508, huomioi nykyisellään kyberturvallisuuden.

3.5 Referenssit

[ETSI-103305] ETSI TR 103 305 -sarjan tekniset raportit: “Security Assurance by Default; Critical Security Controls for Effective Cyber Defense”

[ISA-TR84] ISA:n tekninen raportti ISA-TR84.00.09-2013, Security Countermeasures Related to Safety Instrumented Systems (SIS)

[KYBER-TEO-2014] Kyberturvallisuuden kehittäminen ja jalkauttaminen teollisuuteen vuonna 2014. Huoltovarmuuskeskus, https://www.huoltovarmuuskeskus.fi/julkaisut/

[NIS-DIR] EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI (EU) 2016/1148, 6. heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa (NIS-Direktiivi) http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016L1148&from=EN

[TREND-FR] Trend Micro, The French Underground, Under a Shroud of Extreme Caution, 2016, https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-french-underground.pdf

4. Tuotanto-omaisuuden hallinta

Tuotanto-omaisuuden hallinta (*asset management*) on vakiintunut peruskäsite turvallisen ja jatkuvan toiminnan organisoimiseksi teollisuudessa. Kaikki tuotantoon liittyvät tekijät inventoidaan eli mm. tunnistetaan, luokitellaan ja dokumentoidaan säännöllisesti, ja niiden tilaa seurataan. Tuotanto-omaisuutta ovat varsinaisten tuotantolaitteistojen lisäksi myös tieto-omaisuus, jota käyttämällä tuotantoa voidaan ylläpitää myös häiriötilanteissa tai kehittää tehokkaammaksi ja joustavammaksi. Sekä tuotanto- että tieto-omaisuuteen voi kohdistua tänä päivänä vakavia kyberturvallisuusuhkia, joiden takia niiden normaalitilaa uhkaavia muutoksia ja haavoittuvuuksia tulee pystyä seuraamaan jopa reaaliaikaisesti. Tämä edellyttää automaattisia menetelmiä ja työkaluja, joilla tarvittava seuranta pystytään toteuttamaan luotettavasti ja tehokkaasti.

Huomioita 2. Miksi tuotanto-omaisuuden hallinta on tärkeää?

Miksi tuotanto-omaisuuden hallinta on keskeistä kyberturvallisuuden kannalta?

- Kyberuhat kohdistuvat kriittiseen tuotanto- ja tieto-omaisuuteen, niiden oikeaan toimintaan ja konfiguraatioon
- Tuotanto-omaisuuden hallinnan ja seurannan avulla voidaan ylläpitää ajantasaista tilannekuvaa haavoittuvista kohteista

Miten tuotanto-omaisuuden hallinta tukee kyberturvallisuuden tilannekuvaa koko elinkaaressa? *Asset management* -järjestelmää voidaan hyödyntää mm.

1. kyberturvallisuussuunnitelmien laadinnassa (suojattavat kohteet)
2. haavoittuvuuksien hallinnassa (käytössä olevat tuotteet)
3. kyberuhkien ja -häiriöiden hallinnassa (häirinnän kohteet)
4. kyberturvallisten konfiguraatioiden seurannassa ja jakelussa.

Automaation pitkä elinkaari ja usein varsin laaja toimittajaverkosto tekevät tuotanto-omaisuuden virheettömästä hallinnasta käytännössä mahdotonta. Siksi tilannekuvan muodostaminen on elintärkeää nopean reagoinnin varmistamiseksi, mutta johtaa jatkuvan fyysisen ja sähköisen seurannan tarpeeseen: Ovatko tuotantovälineet

edelleen oikeilla paikoillaan ja toiminnassa? Vastaako tuotannossa olevien laitteiden konfiguraatio turvallista tilaa? Onko tuotantoverkossa jotain sinne kuulumatonta toimintaa, laitteita tai ohjelmistoja, jotka liittyvät esim. tiedusteluun tai yritysvakoiluun? Nämä ovat kysymyksiä, joihin pyritään tänä päivänä vastaamaan lisääntyvässä määrin automaattisten haavoittuvuuksien ja uhkien hallinnan menetelmien työkalujen avulla. Automaattinen seuranta on kuitenkin usein edelleen varsin ongelmallista tai työlästä järjestää ja ylläpitää. Tehokkaat seurantajärjestelmät voivat itsessäänkin lisätä uhkia, mikäli seurantaa ei kyetä hallinnoimaan turvallisesti ja valvomaan sen oikeaa käyttöä.

Oppi 4. Tuotanto-omaisuuden uskottava seuranta vaatii jatkuvaa työtä ja vahvaa osaamista.

Uudet vaatimukset ehdottavat automatiikan lisäämistä kyberturvallisuusuhkien ja haavoittuvuuksien seurantaan.

Seurantateknologiat ovat kuitenkin vielä kehitysvaiheessa ja osaamisvaje on ilmeinen.

Tuotanto-omaisuuden hallinta edellyttää tieto-omaisuuksien jatkuvaa seurantaa, mutta automatisoitujen työkalujen käyttö sisältää riskejä.

4.1 Haavoittuvuuksien ja uhkien hallinta – Case

Teollisuustuotantoa ja kriittisiä palveluja tarjoavien yritysten olisi tärkeää pystyä seuraamaan käyttämiensä järjestelmien ja tuotantovälineiden turvallisuushaavoittuvuuksien ja uhkien tilannekuvaa varsin tarkasti. Tähän liittyvä teknologia on paraikaa murrosvaiheessa, jossa uusia käytäntöjä ja työkaluja syntyy nopeasti. Seuraavassa esittelemme osan tekemästämme selvityksestä haavoittuvuuksien ja uhkien hallintaan mahdollisesti soveltuvista standardeista ja työkaluista. Hallittavana kohteena olivat lähinnä toimistojärjestelmät, mutta myös tuotantoautomaatiojärjestelmät tulevat kyseeseen, sillä niidenkin sisäisten haavoittuvuuksien ja uhkien hallintaan täytyy tulevaisuudessa panostaa merkittävästi enemmän kuin nykyään.

4.1.1 Haavoittuvuuksien ja uhkien tunnistamisen edellytykset

IT-omaisuuden hallinnalla käsitetään mm. IT-laitteiden, ohjelmistoversioiden ja lisenssien hallintaa niiden koko elinkaaressa. Se on välttämätön edellytys myös kyberturvallisuushaavoittuvuuksien ja uhkien selvittelyssä, sillä haavoittuvuudet tulee pystyä luotettavasti löytämään kaikista yrityksen käytössä olevista tuotteista ja palveluista. Haavoittuvuuksien ollessa läsnä myös uhkien toteutuminen on paljon todennäköisempää, joten molempien hallintakäytännöt ovat tarpeen.

Tuotannossa oleviin IT-järjestelmiin kohdistuvien haavoittuvuuksien ja uhkien systemaattinen tunnistaminen edellyttää:

- ASIALLISTA OMISTUSTA: Oman IT-ympäristön järjestelmien kartoittamista, dokumentointia, seurantaa ja oikean toiminnan syvällistä ymmärtämistä.
- OSALLISTUMISTA FOORUMEIHIN: Tiedon keruuta ja jakamista soveltuvissa haavoittuvuuksien ja uhkien seurantafoorumeissa.
- HAAVOITTUVUUKSIEN HALLINTAA: Kyberturvallisuushaavoittuvuuksien seurantaa ja tunnistamista, sekä niiden kohdistuvuuden selvittämistä.
- UHKIEN ja POIKKEAMIEN HALLINTAA: Kyberturvallisuusuhkien seurantaa ja tunnistamista, sekä niiden vaikutusten selvittämistä.
- TYÖKALUJA: Työkaluja, joiden avulla verkossa olevia järjestelmiä voidaan systemaattisesti ja automaattisesti seurata ja tunnistaa niiden ongelmia.

Mobiilijärjestelmien seuranta saattaa unohtua, kun suunnitellaan yrityksen kyberhaavoittuvuuksien ja -uhkien seurannan kehittämistä. Tämä olisi virhe, sillä mobiilijärjestelmät ovat samalla tavalla haavoittuvia kyberturvallisuusuhkille kuin tietokonejärjestelmätkin, mutta niiden laitehallinta saattaa olla puutteellista. Mobiilijärjestelmien kyberturvallisuusuhkista ja niiden hallinnasta on hyvää tietoa mm. NATO CCDCOE:n dokumentissa *Defending mobile devices for high level officials and decision-makers, Teemu Väisänen et al.*: https://ccdcoe.org/multimedia/defending-mobile-devices-high-level-officials-and-decision-makers.html

4.1.2 Teknisiä protokollia

Seuraavaksi esittelemme muutamia merkittäviä standardeja, joita on kehitetty kyberhaavoittuvuus- ja uhkatiedon automaattiseksi selvittämiseksi ja koostamiseksi, mm.:

- *Security Content Automation Protocol (SCAP)*
- *Security Threat Information eXpression (STIX)*
- *Internet Object Description Exchange Format (IODEF).*

Kukin näistä standardeista pyrkii hieman erilaisen ja/tai eritasoisen tiedon välittämiseen mm. yhteistyöverkostoissa, kumppanuuksissa tai järjestelmissä. Seuraavassa esitellään lyhyesti myös muutamia muita soveltuvia alustoja tai standardeja.

4.1.2.1 Kohdistettujen hyökkäysten selvittäminen – MISP

MISP (*Malware Information Sharing Platform*) http://www.misp-project.org/index.html on avoimen yhteisön ylläpitämä avoimen lähdekoodin alusta, jota käyttämällä voidaan jakaa, tallettaa ja korreloida kohdistettujen hyökkäysten *Indicators of Compromises* (IoC) tietoa. Se on hyvä alustaratkaisu kyberturvallisuustapahtumien (*incidents*) ja haittaohjelmien yhteisölliseen analysointiin.

MISPin ydin on hajautettu IoC-tietokanta, joka sisältää sekä teknistä että ei-teknistä tietoa tapahtumista ja haittaohjelmista. MISP sisältää myös graafisen käyttöliittymän ja tarvittavat API-toteutukset MISPin integroimiseksi käyttäjän oman organisaation erilaisiin tietoturvallisuuden seurantajärjestelmiin. Perusformaatti on varsin yksinkertainen JSON (*JavaScript Object Notation*) tapahtumien ja attribuuttien nopeaksi jakamiseksi. JSON-skeema on kuvattu tarkasti, ja useita esimerkkiskeemoja on saatavilla MISP feedeissä. Järjestelmään kuuluu selkeä ”MISP export -toiminto”, joka tukee integrointia yrityksen muihin järjestelmiin muuntamalla datan eri formaatteihin, kuten:

- Output-formaatteja: IDS-formaatit, OpenIOC, plain text, CSV, MISP XML ja JSON
- Export-kohteita: host IDS, STIX (XML and JSON), NIDS export (Suricata, Snort and Bro) ja RPZ zone. Lisäksi uusia formaatteja voi lisätä MISP-moduuleita käyttämällä.

MISP-alusta tukee sekä yksityisten että julkisten MISP-yhteisöjen luontia, ylläpitoa ja operointia kansainvälisesti. Sopivan olemassa olevan yhteisön löytämiseksi kannattaa olla yhteydessä tunnettuihin MISP-yhteisöihin, sillä niillä on erilaisia sääntöjä mm. jäseneksi pääsemiseksi. Yhteisö voi myös olla liittynyt muihin vastaaviin yhteisöihin tai toimia ainoastaan eristyneessä eli *island*-moodissa. Jotkin yhteisöt sallivat jopa osallistujan synkronoida oman MISP-instanssinsa yhteisön tietokannan kanssa.

MISPissä on myös ns. *feed*-toiminnallisuus, jonka avulla yhteisön MISP-tapahtumia (*events*) voidaan hakea serveriltä ilman eri sopimusta. Kaksi erilaista OSINT-feediä on saavilla kaikissa MISP-asennuksissa jo oletusarvoisesti. Feedejä jaetaan PyMISP feed -generaattorin avulla, ks. “Using open source intelligence feeds, OSINT, with MISP”, https://www.vanimpe.eu/2016/03/23/using-open-source-intelligence-osint-with-misp/

4.1.2.2 Security Content Automation Protocol (SCAP)

SCAP, *Security Content Automation Protocol,* on NISTin kehittämä standardi haavoittuvuuksien hallinnan, tieto-omaisuuden inventaarion ja politiikan mukaisuuden arvioinnin automatisoimiseksi, https://scap.nist.gov/. SCAP käyttää ja yhdistelee olemassa olevia muita standardeja, mm.:

- *Common Vulnerabilities and Exposures (CVE)*
- *Common Configuration Enumeration (CCE)*
- *Common Platform Enumeration (CPE)*
- *Open Vulnerability and Assessment Language (OVAL).*

SCAP-ohjauskehys (*SCAP control framework*) yhdistelee näitä standardeja eri järjestelmien ja ohjelmistojen alustavaksi sekä jatkuvaksi arvioimiseksi. Mm. Sec Pod ylläpitää laajoja ilmaisia SCAP-tietovarantoja toimivine *Search*-työkaluineen:

- SecPod: www.Secpod.com
- SecPod SCAP repo: www.scaprepo.com

SCAP on arvioitu varsin toimivaksi työkaluksi vaatimustenmukaisuuden (*compliance*) tarkasteluun ja kehittämiseen. Sen kehitys jatkuu, ja kehittäjät toivovat yleisön laajaa kontribuointia.

4.1.2.3 Structured Threat Information eXpression (STIX)

STIX (*Structured Threat Information eXpression)* standardi on osoittanut, että koneluettavan uhkatiedon vaihto ja käyttö onnistuvat myös operatiivisessa SOC-toiminnassa. Monet kaupalliset työkalut tukevat STIX 1:stä ja sekä kaupalliset että viranomaistahot tuottavat ja kuluttavat standardin mukaisia syötteitä. Informaation siirtoon on suositeltu käytettäväksi *Trusted Automated Exchange of Indicator Information* (TAXII) protokollaa.

Standardin kehittäminen on nykyisin OASIS-järjestön (*Organization for the Advancement of Structured Information Standards*) teknisen komitean CTI (*Cyber Threat Intelligence*) vastuulla, katso https://oasis-open.github.io/cti-documentation/. STIX 1 versiossa esiintyneet XML:stä aiheutuneet ongelmat luvataan korjata STIX 2:ssa, jonka versio 2.0 (kehitteillä) määrittelee pääosin kehykset, joiden päälle tulevaisuuden ominaisuudet voidaan rakentaa. STIX-versiot 1 ja 2 eivät kuitenkaan ole yhteensopivia.
STIX:n tavoitteena on ollut uhkatiedon ”*threat intelligence*” määrittely mahdollisimman strukturoidulla ja laajennettavalla tavalla, jotta ajankohtaisen uhkatiedon levittäminen olisi helpompaa automatisoida, mutta myös ihmisten ymmärtää. STIX 1:n välittämät uhkatiedotteet voivat sisältää mm. seuraavia tietoja:

- Millaisia hyökkäystoimia muualla on ilmennyt?
- Miten nämä hyökkäystoimet voidaan havaita ja tunnistaa?
- Miten tietyn hyökkäyksen vaikutuksia voi lieventää?
- Keitä hyökkääjät ovat?
- Mitä hyökkääjät tavoittelevat?
- Millaisia kyvykkyyksiä hyökkääjillä on?
- Millaisia taktiikoita, tekniikoita ja proseduureja hyökkääjät käyttävät?
- Millaisia haavoittuvuuksia tai heikkouksia hyökkääjät hyväksikäyttävät?

STIX 1:ssä voidaan tarvittaessa hyödyntää myös mm. seuraavia strukturoituja kieliä:

- CybOX – *Cyber Observable Expression* (tulevaisuudessa osa STIX 2:ta?)
- MAEC – *Malware Attribute Enumeration and Characterization*
- CAPEC – *Common Attack Pattern Enumeration and Classification*
- CVRF – *Common Vulnerability Reporting Framework*.

STIXissä lähes kaikki on ollut optionaalista, joten parhaimmillaan kielen hyötykäyttö voisi olla ilmaisuvoimaista ja joustavaa. Yhteisö kasvanee edelleen ja saa lisää käytännön hyödyntäjiä varsinkin Yhdysvaltain viranomaistahoista. STIX on siis suuria lupauksia herättävä, mutta sen haittapuolet johtunevat samasta syystä kuin edutkin eli määrittelyjen laajuudesta. STIXiä tukevia tuotteita ovat mm. Carbon Black, IBM

QRadar, McAfee Advanced Threat Defense, Splunk App for Enterprise Security ja Tripwire Enterprise. Myös NATOn *Cyber Data Information Exchange* (CDXI) on hyödyntänyt STIXiä.

4.1.2.4 The Incident Object Description Exchange Format (IODEF)

IODEF (Incident Object Description Exchange Format) on IETF:n (https://www.ietf.org/) kehittämä dataformaatti kyberhäiriöiden viestimiseen CSIRT-tiimien välillä. IODEF:n määrittelemät XML-pohjaiset viestit on tarkoitettu ihmisten luettaviksi, ei niinkään koneiden käyttöön. IODEF kuvataan IETF-standardissa RFC 5070, joka määrittelee XML-datamallin (skeeman) ja siihen liittyvän DTD:n (*Document Type Definition*).

IODEF:llä voidaan lähettää XML-viesteinä mm. hälytyksiä, varoituksia ja häiriötietoja, sekä muuta relevanttia tietoturvatietoa yksittäisten laitteiden ja monitorointipisteistä keskitettyihin analyysikeskuksiin. IODEF-skeema määrittelee yli 30 luokkaa ja aliluokkaa kyberhäiriödatalle, jotka liittyvät seuraavan tyyppisiin asioihin:

- kontaktit
- kustannusvaikutukset
- aika
- käyttöjärjestelmät ja sovellukset
- kommentit, liittyen esim. varmuuteen ja sensitiivisyyteen.

Myös IODEF sallii olemassa olevien kuvauskielten hyödyntämisen, kuten CAPEX, CPE, CVE ja OVAL, mutta sen ehkä suurin ongelma on alkuperäinen tarkoitus jakaa häiriödataa (*incident*), ei niinkään *indicators of compromise* (IoC) -dataa. IETF:n RFC 6545 määrittelee Real-time Inter-network Defense (RID) -tiedonsiirtomenetelmän "*incident-handling*"-ratkaisujen tarpeisiin.

4.1.3 Haavoittuvuuksien hallinnan tietokantoja ja työkaluja

4.1.3.1 Haavoittuvuustietokannat

Tärkeimpiä haavoittuvuustietokantoja ovat mm.

- MITRE CVE: http://cve.mitre.org/
- NIST NVD: https://nvd.nist.gov/
- SecPod SCAP repo: http://www.scaprepo.com
- Rapid 7: https://www.rapid7.com/db/
- SCIP AG, VulnDB: https://vuldb.com/
- CMU/SEI/CERT: https://www.kb.cert.org/vuls/
- Offensive Security: https://www.exploit-db.com/
- eri käyttöjärjestelmien omat haavoittuvuustietokannat
- eri ohjelmien omat tietokannat jne.

Käytimme muutamia päiviä näiden haavoittuvuuskantojen pienimuotoiseen testaamiseen, tarkoituksena tehdä muutamia mittauksia kannoista saatavan tiedon käyttökelpoisuudesta ja määrästä. Emme jaa testauksen tuloksia alla olevaa enempää.

MITRE CVE: Tämä on virallinen CVE-tietokanta, johon muut tietokannat pohjaavat hakunsa ja jota MITRE ylläpitää. Kaikki osumat ovat CVE-merkinnällä varustettuja haavoittuvuuksia.

NIST NVD: NVD-haun kautta pääsee tutkimaan CVE-kannan sisältöä. Koko kannan tai muutokset voi ladata paikalliselle palvelimelle XML-muodossa. Ohjaa myös osoitteen cve.mitre.org hakuun. Integraatio CCE-kantaan on sivuston mukaan tulossa.

SecPod SCAP Repo: Tarjoaa alustan haavoittuvuustietojen hakemiseen useista eri tietokannoista: CCE (*Common Configuration Enumeration*), CPE (*Common Platform Enumeration*), CVE (*Common Vulnerabilities and Exposures*), CWE (*Common Weakness Enumeration*), OVAL (*Open Vulnerability and Assessment Language*) ja XCCDF (*Extensible Configuration Checklist Description Format*). Hakea voi siis myös peruskuvauksen halutusta palvelusta OVAL-muodossa. Tarjoaa REST-rajapinnan, jonka avulla tiedonhakua voidaan automatisoida.

Rapid 7: Tarjoaa haavoittuvuustuloksia myös CVE-kannan ulkopuolelta. Lisäksi palvelussa on mahdollista hakea Metasploit-työkalun moduuleja, joiden avulla tiettyyn ohjelmistoon liittyviä haavoittuvuuksia voi testata helposti. Tietokanta on integroitu Rapid 7 Nexpose -haavoittuvuusskanneriin.

SCIP AG, VulnDB: Sisältää arkistoa ja statistiikkaa raportoiduista haavoittuvuuksista. Listaa arvion yksittäisen haavoittuvuuden markkinahinnasta, jolla voisi pimeiltä markkinoilta ostaa työkalut haavoittuvuuksien hyödyntämiseen. Hinta on kuitenkin automaattisella algoritmilla tehty arvio, joka ei välttämättä vastaa reaalimaailmaa.

CMU/SEI/CERT: Automaattisesta integraatiosta sivusto tarjoaa ainoastaan RSS-feedin.

Offensive Security: Sivusto listaa valmiita ohjeita haavoittuvuuksien testaamiseen. Lisäksi tarjotaan Shellcodeja, jotka ovat käyttöjärjestelmäkomentoja hyökkäysten testaamiseen, esimerkiksi mm. buffer overflow -hyökkäyksiä.

4.1.3.2 Haavoittuvuusskannauksen työkaluja

Millä työkalulla olisi kannattavaa tehdä toistuvaa oman verkon haavoittuvuusskannausta? Yleistetty haavoittuvuusskannereiden vertailu on hyvin hankalaa. Valintaan vaikuttaa skannerin haavoittuvuuksien löytämistarkkuuden lisäksi ohjelmiston käy-

tettävyys, tulosten raportointi, tuetut käyttöjärjestelmät, valmistajan luotettavuus, tukitoimet ja referenssit sekä pienet erot ominaisuuksissa, jotka saattavat vaikuttaa hankintapäätökseen.

Jotkin skannerit sopivat paremmin pieneen verkkoon tai yksittäiseen kohteeseen kuin laajan verkon skannaukseen. Useampi blogikirjoitus ja sectools.org suosittelevat noin kymmentä eri skanneria, joista ainoastaan yksi (*OpenVAS*) on ilmainen ja muut vaativat lisenssin. OpenVASia voi tosin joskus olla vaikea saada toimintakuntoon. Ohjelmien lisenssimaksut sijoittuvat noin 2000–3000 euron vuositasoihin, joskin esim. Core Securityn *Core Impact* -skanneri voi olla huomattavasti kalliimpikin. Projektissa yleisimmin käytetty haavoittuvuusskannuksen työkalu oli Tenable Securityn Nessus.

Työkaluista on hankala tehdä arviointia, mikäli niitä ei päästä testaamaan. Demonkin kokeilu saattaa vaatia pyynnön ja hyväksynnän ohjelmiston toimittajalta. Evaluointi on kuitenkin tärkeää toteuttaa ennen tuotteen hankintaa, jotta vältytään yllätyksiltä. Varteenotettavia tuotteita ovat esimerkiksi

- Tenable Security: *Nessus, Passive Vulnerability Scanner, and Security Center*
- Rapid 7: Nexpose
- BeyondTrust: *Retina CS.*

4.1.4 Johtopäätökset

Lupaavia teknologioita ovat mm. SCAP (haavoittuvuuksien hallinta) sekä MISP ja STIX (uhkien, poikkeamien ja häiriöiden hallinta). Todennäköisesti kaikkia kyberturvallisuuden varmistamiseen liittyviä tarpeita ei saada tyydytettyä vain yhden standardiperheen avulla, vaan käyttöön tulee ottaa useita eri standardeja (ks. esim. SCAP). Sopivimmat vaihtoehdot riippuvat yrityksen jo käytössä olevista työkaluista ja tietokannoista mm. IT-omaisuudenhallinnan osalta.

Potentiaalisia yhteistyötahoja

Kyberturvallisuuskeskus: Jakaa jatkuvasti ja laajasti haavoittuvuustiedotteita ja varoituksia erilaisilla teemoilla. Kyberturvallisuuskeskus saa tai vaihtaa jatkuvasti haavoittuvuus- ja uhkatietoja lähinnä muiden kansallisten CERTien kanssa.

Haavoittuvuuskannat: Kannoista saatava tieto tukee yrityksen haavoittuvuuksien automaattisen analyysin tarpeita ja valittuja automaattisia työkaluja. Esim.:

- MITRE CVE: http://cve.mitre.org/
- NIST NVD: https://nvd.nist.gov/
- SecPod SCAP Repo: http://www.scaprepo.com

Uhkien ja poikkeamien jakaminen: Yritykselle soveltuvimmat MISP ja STIX yhteisöt kannattaa selvittää ja pohtia mukaan liittymistä.

Automatisoinnista

Automatisointia voitaneen toteuttaa monilta osiltaan esitettyjen työkalujen avulla, mutta yksityiskohdat riippuvat käyttötarpeesta. Automatisoida voidaan ainakin periaatteessa

- tieto-omaisuuden keskitetty koostaminen ja tallentaminen
- haavoittuvuuksien lataaminen tietolähteistä ja koostaminen tietokantaan
- käytössä olevien IT-tuotteiden tunnettujen haavoittuvuuksien selvittäminen
- uhkien yhteisölliseen käsittelyyn liittyviä toimia MISP- ja STIX-yhteisöpalvelujen ja feedien avulla.

5. Arkkitehtuureista

5.1 Turvallisten arkkitehtuurien merkitys

Lisääntyvien uhkien myötä tuotantoympäristön tietoliikennettä, dataa ja laskentaa erottelevien suoja-alueiden, aliverkkojen ja virtuaaliympäristöjen turvallista toteutusta ja seurantaa on vahvistettava. Automaation valvottua verkkoarkkitehtuuria tarvitaan viimeistään teollisen Internetin ja vapaiden taajuuksien ja mobiiliverkkojen langattoman tiedonsiirron tunkeutuessa tuotantoon. Kyberturvallisuuden varmistaminen edellyttää mm. yhdyskäytävälaitteiden ja -ohjelmistojen sekä langattomien verkkojen (mm. kiinteistöautomaatiosovellusten) turvallista toteutusta ja ylläpitoa, sekä käyttäytymisen valvontaa.

Olemme käsitelleet jo aiemmissa projekteissamme teollisuusautomaation kyberturvallisia *verkkoarkkitehtuurimalleja*, katso esim. [TEO-SUMMARY]. Pelkät mallit eivät kuitenkaan tietenkään riitä, vaan niitä täytyy osata soveltaa kuhunkin tapaukseen soveltuvalla tavalla. Esimerkiksi kahden peräkkäisen ja erimerkkisen palomuurin käyttäminen tehdasverkon ja automaatioverkon toisistaan erottamiseen voi tuntua liian kalliilta tai työläältä. Onko järkevää, että sekä IT- että automaatio-osastot erikseen hankkivat ja hallinnoivat omia palomuurejaan ja siihen liitettyjä tunkeutumisen havaitsemisjärjestelmiään (IDS)? Yleisesti ottaen tämä ei liene järkevää, vaan järkevintä olisi perustaa yhteinen työryhmä joka etsii ja koestaa toimivimmat ratkaisut yhteistyössä. Kaksi niukoilla resursseilla ylläpidettyä suojausjärjestelmää tuskin yltää vastaavaan uhkien tunnistustarkkuuteen ja analyysiin kuin yksi ammattimaisesti ylläpidetty SOC (*Security Operations Center*) tai muu vastaava kyberturvallisuuspalvelu. Asianmukainen uhkiin reagointi vastatoimineen on tosin varmistettava myös ulkoistettuja palveluja käytettäessä, esim. jottei itse aiheuteta toimintakatkoja!

Kustannuksien ja kompleksisuuden rajoittamiseksi on syytä kehittää koko yrityksen kattavat arkkitehtuurimallit, joita soveltamalla kukin tuotantoyksikkö pystyy systemaattisesti kehittämään ja ylläpitämään oman tuotantonsa turvallisuutta. Toteutukseen ja ylläpitoon tarvitaan siis yhtiötason tukea. Verkkoarkkitehtuurien turvalliset vaihtoehdot kannattaa tunnistaa, testata ja kiinnittää esim. tuotannon, IT:n ja auto-

maation yhteisissä kehityshankkeissa. Tuotantoyksikön arkkitehtuurivalinnat riippuvat mm. suojattavan tuotannon arvosta, toteutuneista ja todennäköisistä riskeistä, kriittisten järjestelmien ja datan jakautumisesta yksikössä sekä käytettävissä olevasta osaamisesta, pääoma- ja ylläpitoresursseista, ulkoisista ja sisäisistä palveluista, häiriöihin varautumisen tasosta jne.

Automaation elinkaaressa kyberturvallisuuden kehittämisen ja ylläpidon henkilöstökustannukset on yleensä aliarvioitu myös tuotantokäytön osalta. Esim. hankintahinnaltaan edullisia tai ilmaisia tunkeutumisen havaitsemisjärjestelmiä (IDS) on hankittu myös tehdasverkkojen uhkien tunnistamiseksi, mutta hyvä ajatus on usein valunut hukkaan järjestelmän vaatiman osaamisen kehittämisen ja ylläpidon puuttuessa. Tietoturvasta on saattanut tulla rasite, vaikka se on tuotannon jatkuvuuden edellytys.

5.2 Arkkitehtuurit liittyvät kaikkeen

”Arkkitehtuureja” on useita eri *tyyppejä* ja kunkin automaatiojärjestelmän toteutukseen välttämättä sisältyvien erilaisten arkkitehtuurien ja konseptien kyberturvallisuus tulee huomioida riittävällä tasolla. Käytännön projekteissa tulee selvittää kenen toimesta ja missä vaiheessa vaihtoehtoiset arkkitehtuurit tulee analysoida ja kiinnittää tilaajan ja toimittajien kesken? Analysoitavia asioita ovat mm.

- fyysinen & looginen dataverkkoarkkitehtuuri, tietoliikennearkkitehtuuri
- automaatiojärjestelmäarkkitehtuuri
- toimilaitteen toteutusarkkitehtuuri
- automaatio-ohjelmisto- ja sovellusarkkitehtuuri
- hallinta- tai ylläpitoarkkitehtuuri
- tietoturva-arkkitehtuuri
- seuranta-arkkitehtuuri
- jne.

Automaation ekosysteemivalintaa tehdessä kiinnitetään samalla monia arkkitehtuurivalintoja, jotka ovat määräytyneet ensisijaisesti kyseessä olevan ekosysteemin avaintoimijoiden liiketoiminnallisten tavoitteiden perusteella, mutta osin myös verkottuneen kehitystyön käytäntöjen kautta. Eri vaihtoehtoihin liittyvät mahdollisuudet ja uhat tulisi selvittää ja arvioida mm. voiko riippuvuus tietystä ekosysteemistä tuoda tulevaisuudessa kohtuuttomia uhkia omalle liiketoiminnalle. Tosin tätä voi olla varsin vaikea arvioida nykyisessä suurille muutoksille alttiissa turvallisuus- ja talouspoliittisessa ilmapiirissä.

Sitoutuminen mihin tahansa vaihtoehtoon voi olla ongelmallista. Miten luottamus tulee kehittymään mm. Yhdysvaltojen, Ruotsin, Japanin, Saksan tai Kiinan maaperällä pääkonttoriaan tai palvelinkeskustaan pitävän yrityksen automaatiojärjestelmien turvallisuuteen ja kilpailukykyyn? Asettaako ko. maan lainsäädäntö yritykselle

esim. henkilöseurannan tai luottamuksellisen tiedon luovuttamisen velvoitteita kansallisen turvallisuuden tai terrorismin vastaisen taistelun nimissä? Kansallisen turvallisuuden osalta avustusvelvoite on todellisuutta jo ainakin suurvaltojen lainsäädännössä ja sen toimeenpanossa.

Mikäli realistisena uhkakuvana pidetään valtiollisten toimijoiden toteuttamaa yritysvakoilua ja soluttautumista, huoltovarmuuskriittisen yrityksen tulee huomioida nämä riskit omissa ekosysteemivalinnoissaan. Tällöin voidaan asettaa tavoitteeksi, että varajärjestelmien tulee olla pääjärjestelmätoimittajasta riippumattomia sekä teknologisesti että maantieteellisesti, mutta myös poliittisesti. Esim. tietoliikennejärjestelyt vaativat tyypillisesti erilliset varajärjestelmät päätelaitteineen, verkkoineen ja operaattoreineen.

5.2.1 Automaatiohankinta jäädyttää arkkitehtuurivalintoja

Automaation, koneiden ja laitteiden hankinnoista vastaavilla henkilöillä tulisi olla yhtenevä käsitys arkkitehtuuri- ja ekosysteemivalintojen vaikutuksista toiminnan turvallisuuteen. Riittävän ymmärryksen hankkiminen edellyttääkin tavallisesti keskusteluja usean erikoisalan osaajan ja asiantuntijan kanssa. Hyvä käytäntö on sopia esimerkiksi yhteistyöpalavereja oman automaatiohenkilöstön ja tärkeimpien automaatiotoimittajien asiantuntijoiden kanssa. Agendalla tulisi olla kunkin osapuolen määrittelemien arkkitehtuuriratkaisujen läpikäyntiä, samalla kriittisesti eri vaihtoehtojen hyviä ja huonoja puolia tarkastellen ja tulevaisuus huomioiden. Seuraavassa kuvaamme esimerkinomaisesti muutamien automaatiojärjestelmäarkkitehtuurien perustavanlaatuisia ominaisuuksia.

Fyysinen dataverkkoarkkitehtuuri koostuu fyysisistä kytkentälaitteista (kytkimet, yhdyskäytävät, tukiasemat, reitittimet, väyläohjaimet, palomuurit), väylistä ja johdoista, joiden suojaukseen tarvitaan fyysistä pääsynhallintaa: Laaja kenttä, joka oli aiemmin voimakkaasti eriytynyt mm. kiinteisiin automaatio- ja turvaväyliin, erillisiin kiinteistöautomaatioverkkoihin, sekä paikallisverkkoihin (LAN ja WLAN), mutta kehittyy hyvin nopeasti ja konvergoituu vaatien vaikeiden teknologiavalintojen tekemistä. Teollisuuden ja kiinteistöjen johdollisten verkkojen ylläpito saattaa rapautua ajan myötä vaatien sekä teknologista uudelleen ajattelua ja fyysistä uusintaa.

Looginen dataverkkoarkkitehtuuri pohjautuu loogisiin (usein toiminnallisiin) tasoihin jaetuista alueista (*zones*), joiden väliselle liikenteelle asetetaan tiukkoja, pääasiassa ohjelmallisia rajoituksia, kuten palomuurisääntöjä, suodatussääntöjä ja virtuaalisia aliverkkomäärittelyjä, tarkemmin alueet on määritelty standardisarjassa IEC 62443 [IEC62443]. Loogisen verkkoarkkitehtuurin suurimpia ongelmia ovat palomuuri- ja suodatussääntöjen rapautuminen ajan myötä, sekä riittämätön kyberturvallisuustestaus. Yrityksen itsensä määrittelemä tuotannon kyberturvallisuuden tavoitetaso ohjaa mm. dataverkkojen eriyttämisen laajuutta ja syvyyttä. Oleellista on, että kutakin verkkoa pystytään kaikissa elinkaaren vaiheissa uskottavasti ylläpitämään ja

valvomaan määritellyn *kriittisyystason* mukaisesti. Koko elinkaaren kestävään valvontaan yrityksen oman henkilöstön toimet eivät yksin riitä, sillä tällä hetkellä myös tuotannon verkkoteknologiat ja automaatiosovellukset kilpailevine ekosysteemeineen kehittyvät hyvin nopeasti, lisääntyvistä kyberuhkista puhumattakaan.

Toimilaitteen toteutusarkkitehtuuri, mm. logiikkaohjaimen sulautettu laskenta- ja järjestelmäalusta, saattaa tänä päivänä olla hyvinkin monimutkainen kokonaisuus sisältäen useita kehittyneen alustan tarjoamia suojaustekniikoita. Suojaustekniikoiden täysimääräinen hyödyntäminen ja käyttöönotto ovat usein se heikko lenkki, sillä olemassa olevia suojausmenetelmiä jätetään usein ottamatta käyttöön. Syitä voivat olla esim. osaamattomuus ja kokemattomuus, mutta myös testimahdollisuuksien ja ajan puute. Suojaustekniikoista mainittakoon esim. pääsynvalvonta eri muistialueisiin (muistin jakaminen eri sovelluksille), pääsynvalvonta I/O-rajapintoihin (sarja, väylä jne.) ja oheislaitteisiin, järjestelmän käynnistysprosessin valvontamekanismi, *debug*-rajapintojen pääsynvalvonta ja käytöstä poisto, sisäinen käyttöjärjestelmä kaikkine turvallisuusominaisuuksineen ja asetuksineen, ja esim. sovellusten asentamisen ja käynnistymisen esto- ja valvontamekanismit. Toimilaitteen arkkitehtuurin ja sovellusten turvallisesta toteuttamisesta on yleensä vastuussa toimilaitteen kehittäjä ja valmistaja, mutta erittäin tärkeä vaihe on myös integrointi osaksi suurempaa kokonaisuutta. Valmistajan tulisi pystyä tukemaan integraattorina toimivaa yritystä myös tietoturvaan liittyvissä ongelmissa ja valinnoissa.

Mihin konsepteihin ja arkkitehtuureihin automaation kyberturvallisuuden kehittämisessä kannattaisi fokusoida? Vastaus riippuu paitsi toimijan omista vahvuuksista ja osaamisalueista, myös tunnistetuista puutteellisen osaamisen alueista, joiden analyysiin ja kehittämiseen tarvitaan ulkopuolista apua. Mikäli yhdenkään automaatiojärjestelmään sisältyvän konseptin tai niiden käytännön toteutus (esim. kovennuksen taso tai ylläpito) on vajavaista, se saattaa yksinkin muodostaa hyökkäysvektorin koko järjestelmää vastaan.

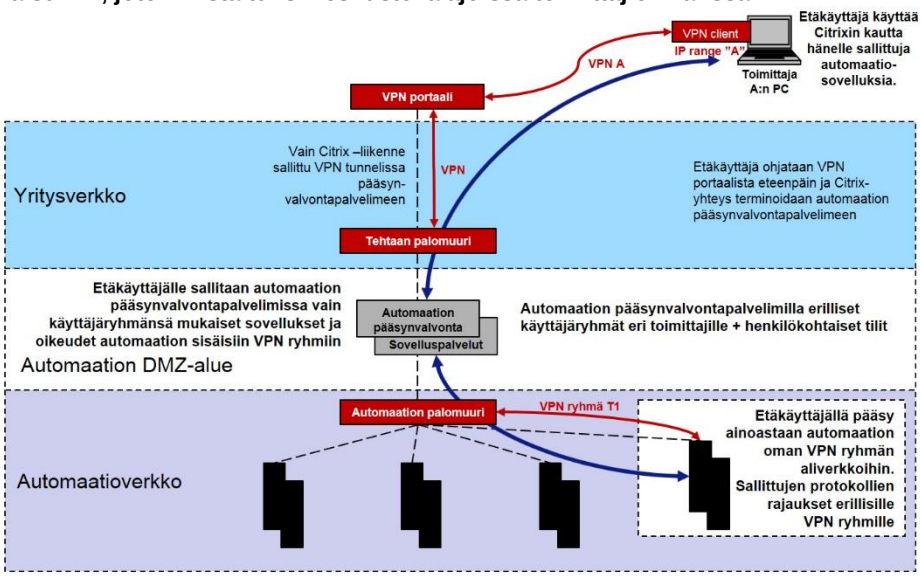
Virtualisoinnin hyväksikäyttö on tullut jäädäkseen myös automaatioon, sillä sen avulla voidaan rajoittaa esimerkiksi vanhentuneiden ja päivittämättömien järjestelmien haavoittuvuuksista aiheutuvia uhkia. Ilmeisenä haittapuolena on tietenkin se, että se tuo mukanaan IT-pohjaiset virtuaalialustat ja -järjestelmät omine, jatkuvasti kehittyvine osaamisvaatimuksineen. Hyödyntämiseen vaikuttaa siis myös käytettävissä oleva IT-osaaminen. Virtuaalisten ympäristöjen käytöllä voidaan kuitenkin samalla myös helpottaa kompleksisuuden hallintaa.

5.3 Etäyhteyskonseptien vaikutus arkkitehtuureihin

Hankinnoista keskusteltaessa ja päätettäessä täytyy huomioida myös koko yrityksen ja kyseisen tuotantoyksikön ICT-arkkitehtuurit. Kysymyksessähän voi olla esim.

paljon automaatiota sisältävän tuotantoyksikön laajennus monitoimittajaympäristössä, jolloin arkkitehtuurivalintoja voi käytännössä rajoittaa esim. yksittäisen tuotantolinjan automaatiotoimittajan kiinnittäminen liian varhaisessa vaiheessa.

Yritystasolla määriteltävä tuotannon turvallinen etäyhteyskonsepti on yksi tärkeimmistä muihin arkkitehtuurivalintoihin vaikuttavista periaatteista tai säännöistä. Tuotannon etäyhteyskonseptin tulee mm. pääsääntöisesti kieltää etenkin jatkuvat, päästä-päähän salatut VPN-yhteydet toimittajan verkosta (tehtaan) automaatiolaitteeseen. Kiellolla voi olla merkittäviä vaikutuksia automaatio- ja konetoimittajien etäylläpitopalvelujen vakiokäytäntöihin ja -ratkaisuihin, joten niistä tulisi keskustella ajoissa toimittajien kanssa.



Kuva 7. Automaation etäyhteyksien arkkitehtuurikonsepti – Esimerkki.

Automaation etäyhteysratkaisujen arkkitehtuuriin, kyberturvallisuuteen ja käytettävyyteen vaikuttavia toiminnallisia tekijöitä on valitettavasti lukuisia. Alla on esimerkkilista projektissa käyttämistämme etäyhteysratkaisujen vertailun arviointikriteereistä:

- Ajetut tietoturvatestit / sertifikaatit (Security tests/certifications)
- Datavirran optimointi (Streaming optimization)
- Dynaamiset IP osoitteet (Connection using dynamic IP addresses)
- Etäkäyttäjien pääsynhallinta (Remote user account)
- Etäkäyttäjän toimintojen sulkeminen (Disabling of remote user)
- Etäkäyttäjän tunnistamisen menetelmätuki (Remote user authentication)
- Etälaitteen haittaohjelmaskannaus (Malware scanned client)
- Etäpalvelujen yhdyskäytävän käyttö (Remote services Gateway)
- Etäsovellusten ajo paikallisessa laitteessa (Seamless applications)
- Etätiedoston siirto (File Transfer)

- Etätuki (Remote View/Assistance)
- Etäyhteyden päättämisen kriteeristö (Remote session termination)
- Etäyhteyden vanhentuminen (Remote account expiration)
- Etäyhteyksien lokiominaisuudet (Remote connections log)
- Etäyhteyksien monitorointiominaisuudet (Remote connections monitoring)
- IP protokollaversiot (IP protocol version)
- Istunnon nauhoitus (Session recording)
- Käytettävyys (O&M usability)
- Laajennettavuus (Extensions)
- NAT tuki (NAT Pass-through)
- Paikallisen printterin käyttö (Printer Redirection)
- Paikallisen tiedostojärjestelmän käyttö (File System Redirection)
- Paikallisten porttien käyttö (Port Redirection)
- Palomuurituki (Connectivity through firewalls and routers)
- Pääsynvalvonta LANiin (LAN access control)
- Pääsynvalvontamenetelmät etäsovelluksiin (Application control)
- Pääsyoikeuksien pyyntö (Access Permission Request)
- Pääsypyyntöjen rajoittaminen (Request Filtering)
- Selainpääsy (Web access)
- Suora etäohjaus (Remote Control)
- Tuetut protokollat (Protocol: link, Internet, transport, remote desktop e.g. VNC, RDP…)
- Tuetut salausalgoritmit (Encryption algorithm)
- Tuetut tietoturvaprotokollat (Security protocol)
- Tunnetut haavoittuvuudet (Known vulnerabilities)
- Useamman näytön käyttö (Multiple monitors)
- Uudelleenkäynnistys etänä (Remote Boot)
- Videotuki (Video support)
- Yhteyden avaus palvelimen suunnasta (Listening mode)
- Yhtäaikaiset istunnot (Multiple sessions)
- Yhtäaikaiset yhteydet (Simultaneous connections)
- Äänen uudelleenohjaus (Audio redirection)

Mikäli automaatiojärjestelmä- tai konetoimittajille sallittaisiin päästä-päähän etäyhteyksiä, olisi tuotanto-operaattorin luotettava vahvasti näiden ”etäkumppaniensa” kykyyn huolehtia järjestelmiensä ja työtekijöidensä tietoturvan tasosta, sekä halusta noudattaa tuotantoyrityksen määrittelemää muutostenhallintapolitiikkaa. Entä mitä tapahtuu kyberturvallisuudelle, kun jokin kumppaniyritys myydään, sen toimintoja ulkoistetaan tai työntekijät vaihtuvat? Tällaisten seikkojen johdosta esim. konetoimittajien suosimat, mutta tuotannon näkökulmasta riskialttiit päästä-päähän etäyhteysarkkitehtuurit ja niihin liittyvät teknologiat ja toimintamallit tulee pääsääntöisesti kieltää turvattomina.

Automaation etäseurannan ja -ylläpidon onnistumisessa kysymys on paljolti siitä, miten ja milloin arkkitehtuuriin vaikuttavat asiat dokumentoidaan ja kommunikoidaan. Jos tilaajalle tarjotun automaatiotoimituksen ja sen ylläpidon tietoliikennearkkitehtuuria ei ole asiallisesti kuvattu edes tarjouksen liitteissä, millä todennäköisyy-

dellä tilaaja saa kehitysprojektinkaan kuluessa riittävästi dokumentaatiota toimitukseen sisältyvistä valinnoista? Millä keinoin tilaaja voi tehdä päätelmiä esim. eri automaatiotoimittajien järjestelmien sopivuudesta omaan tietoliikennearkkitehtuuriinsa ja etäyhteyskonseptiinsa? Entä mikä on automaatiotoimittajan suosittelemien tietoturvallisuusratkaisujen soveltuvuus tuotantoympäristön tietoturva-arkkitehtuuriin?

Kaikki tietoliikennetarpeet tulee selvittää ja tiedottaa etukäteen, jotta turvallista ja luotettavaa tuotannon dataverkkoarkkitehtuuria voidaan ylläpitää.

5.3.1 OPC UA -standardin hyödyt etäyhteyksissä

OPC Unified Architecture (OPC UA) -standardin mukaisten ratkaisujen käyttö vaikuttaa ainakin tämänhetkisen tiedon valossa hyödylliseltä, sillä se antaa yhteisiä kiintopisteitä useille eri arkkitehtuurivalinnoille samalla kertaa. OPC UA -standardin IEC 62541 (ks. esim. peruskonsepti [OPC-UA]) ympärille on helpompi rakentaa yhtenäisiä laiteprofiileja, strukturoituja sovellusarkkitehtuureja, tietoliikennearkkitehtuureja, tietoturva-arkkitehtuureja jne. OPC UA:han kuuluu sisäänrakennettu vahva tietoturva, joka mahdollistaa tietoliikenteen salaamisen, sovellusten todentamisen X.509-sertifikaatein sekä käyttäjien todentamisen salasanoin, X.509-sertifikaatein tai ulkopuolisten järjestelmien avulla. Laajoissa asennuksissa tarvittavaa julkisten avainten ja varmenteiden infrastruktuuria (*PKI – Public Key Infrastructure*) ja sen hallintaprotokollia voidaan hyödyntää täysmääräisesti.

OPC UA -standardin tietoturva on arvioitu *German Office for Information Security*n (BSI) toimesta. Raportti löytyy OPC Foundationin sivuilta osoitteesta https://opcfoundation.org/security/. Lopputuleman kyberturvallisuuden ja luotettavuuden taso riippuu viime kädessä toteutuksen turvallisuudesta, ks. esim. esityksemme *OPC Day Finland 2016* -tilaisuudessa, jossa kuvaamme muutamien OPC UA -toteutusten vähittäistä kyberturvallisuustestausta [OPC-DAY2016].

Erityisesti etäyhteysjärjestelyissä ja teollisen Internetin toteutuksissa yhdyskäytävien turvallinen käyttö ja hallinta korostuvat. OPC UA yhdyskäytävä (*gateway*) auttaa verkkojen erottamisessa toisistaan, sillä molemmista suunnista otetut datayhteydet terminoidaan aina yhdyskäytävään. Näin ollen täysin suorat yhteydet automaatiosta muihin verkkoihin vältetään, vaikkakin testaamattomat toteutukset saattavat sisältää haavoittuvuuksia, jotka voivat mahdollistaa yhdyskäytävän väärinkäytön.

OPC UA yksinkertaistaa palomuurisääntöjen määrittelyä ja lukumäärää merkittävästi, jolloin verkkojen välisen liikenteen hallinta paranee. OPC UA -pohjaisissa ratkaisuissa järjestelmistä tarvitsee avata vain yksittäisiä tietoliikenneportteja, kuten muitakin TCP/IP-protokollia käytettäessä, mikä helpottaa turvallista palomuurikonfigurointia. Sen avulla voidaan myös välttää VPN-yhdyskäytävien avaaminen kokonaisten aliverkkojen välille. OPC UA hyödyntää vaihtoehtoisia siirtoprotokollia, joista yleisimmin käytetty, OPC UA:n oma UA TCP -protokolla, on hyvin tarkkaan opti-

moitu. Toisena vaihtoehtona on käytettävissä HTTPS. Paraikaa on myös valmistumassa uusia vaihtoehtoja turvallisen Publisher-Subscriber-tiedonsiirron mahdollistamiseksi sekä nopeaan lähiverkkokommunikointiin UDP:llä että pilvipalveluihin suuntautuvilla AMQP- ja MQTT-protokollilla.

5.3.2 Kiinteistöjen valvontayhteyksien turvallinen toimintamalli – Schneider Electric Case

Kiinteistöjen valvontayhteyksissä tulee kiinnittää huomiota arkkitehtuurin lisäksi myös käyttäjien- ja muutoksenhallinnan prosesseihin sekä laitteiston käyttöönoton prosessiin. Arkkitehtuuri määrittelee tekniset rajapinnat ja valvontayhteyttä varten rakennettavat laite- ja ohjelmistokokoonpanot. Tilaajan on kuitenkin syytä vaatia toimittajalta arkkitehtikuvauksen lisäksi dokumentaatiota siitä, kuinka toimittaja hallitsee valvontayhteyksien käyttäjiä, miten käyttäjien muutoksia hallitaan ja kuinka käyttöoikeuksien myöntäjiä eli admin-henkilöitä valvotaan. Myös laitteiston käyttöönoton prosessista on hyvä vaatia dokumentaatio, kuuluuko esimerkiksi oletussalasanojen vaihto dokumentoituun toimintamalliin. Toimittajalta pyydettävästä dokumentaatiosta voi käyttää pohjana ISO/IEC27001- tietoturvallisuuden hallintajärjestelmän standardin vaatimuksia.

Koko valvontajärjestelmän käyttörajapinta on mahdollista hankkia toimittajalta myös pilvipalveluna. Tässä ratkaisussa tuotantolaite kommunikoi turvallisesti laitevalmistajan keskitetyn pilvipalvelun palvelimen kanssa. Käyttäjä ei siis ota yhteyttä suoraan kiinteistön tuotantolaitteeseen vaan toimittajan luotettuun palveluun, joka varmistaa turvallisten yhteyksien muodostamisesta kiinteistön toimilaitteeseen. Palvelun käyttörajapintana toimii selain tai mobiilisovellus.

Keskitetty kiinteistöjen valvontajärjestelmä tuo monia etuja. Se mahdollistaa mm. tehokkaan käyttäjien hallinnan. Jokaisella käyttäjällä on henkilökohtainen käyttäjätunnus ja salasana, jolla hän voi hallinnoida juuri niitä laitteita, joihin hänelle myönnetään pääsyoikeus. Käyttäjien vaihtuessa muutokset voidaan tehdä keskitetysti kaikkiin laitteisiin. Keskitettyyn pilvipalveluun on myös paljon kannattavampaa rakentaa erilaisia luvattoman tunkeutumisen havainnointi- ja puolustautumismenetelmiä kuin erillisiin palvelimiin.

5.4 Referenssejä

[CPNI-RA] “CONFIGURING & MANAGING REMOTE ACCESS FOR INDUSTRIAL CONTROL SYSTEMS, APRIL 2011”, CPNI

[OPC-UA] IEC TR 62541-1:2016, OPC unified architecture – Part 1: Overview and concepts

[OPC-DAY2016] ”OPC UA Security Testing (Brief introduction)”, OPC Day 18.10.2016, Pasi Ahonen & Sami Noponen, VTT Technical Research Centre of Finland, http://www.automaatioseura.fi/site/assets/files/1552/pasi_ahonen_opcdayfinland2016_opc_ua_security_testing.pdf

[TEO-SUMMARY] Tietoturvaa huoltovarmuuskriittisille yrityksille, Kooste automaatiota hyödyntävälle teollisuudelle suunnattujen tietoturvaprojektien tuloksista, Huoltovarmuuskeskus, VTT, 2013, https://www.huoltovarmuuskeskus.fi/julkaisut/

[IEC62443] Standardisarja IEC 62443 Teollisuuden tietoliikenneverkot. Verkkojen ja järjestelmien tietoturvallisuus, http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx

6. Tietoisuuden kasvattaminen

Kyberturvallisuuden merkitys koko yhteiskuntamme toiminnalle kasvaa joka kuukausi. Olemme jo tänä päivänä erittäin riippuvaisia julkisten tietoverkkojen saatavuudesta tai jonkin kriittisen yrityksen oikeasta toiminnasta. Tästä todistavat lukuisat esimerkit maailmalta ja Suomesta, mm. internetiin liitettyjen halpojen kuluttajalaitteiden aiheuttamat palvelunestohäiriöt muille palveluille, mm. [MIRAI], sekä terveydenhuoltoalan toimijoihin kohdistuvat kiristyshaittaohjelmat ja muut uhat, katso esim. Kyberturvallisuuskeskuksen raportti Terveydenhuoltoalan kyberuhkia [TERVEYSUHKIA].

Uhat rantautuvat yrityksiin valitettavasti myös työntekijöiden sekä heille läheisten ihmisten välityksellä! Tämä johtuu mm. mobiililaitteen käytöstä sekä työhön että vapaa-aikaan, mutta myös sosiaalisen median ja sen lukuisten sovellusten vyörystä työpöydille. Esimerkiksi läheisen ihmisen suositteleman linkin avaaminen saattaa aiheuttaa haittaohjelman asentumisen huomaamatta työkoneelle. Jotta voisimme ylläpitää yhteiskuntaa ylläpitävät kriittiset palvelut ja kriittisen infrastruktuurin jatkuvasti toiminnassa, kansalaisen tulee vastaanottaa ja omaksua riittävästi kyberturvallisuuteen liittyvää informaatiota ja koulutusta vauvasta vaariin. Yksi esimerkki myös kansalaisten huomioimisesta oli VTT:nkin miehittämä (salakirjoituskiekkoja, salausten murtamista ja *Damn Vulnerable Web Application* -kokeilemista) Tutkijoiden yö -tapahtuma Tiedekeskus Heurekassa ja siihen liittyvät harjoitukset Oulussa, ks. [HEUREKA].

Tässä julkaisussa keskitymme kuitenkin teollisuusyrityksiin, jotka kehittävät tai hyödyntävät automaatiota omassa tuotantotoiminnassaan. Seuraavassa kerrotaan kokemuksia kyberturvallisuustietoisuuden kehittämisestä tällaisten yritysten tarpeisiin.

6.1 Kyberturvallisuustietoisuuden kehittäminen yrityksessä

Tietoisuuden lisäämisen avulla pyritään helpottamaan kyberturvallisuuden jalkautusta käytännön toimintaan automaatiota kehittävissä ja hyödyntävissä yrityksissä.

Tietomurroista vaikenemisen kulttuuri hidastaa merkittävästi yritysjohdon riskitietoisuuden kehittymistä. Kyberturvallisuuden kehitys ei käynnisty yrityksessä itsestään, vaan onnistuminen vaatii innostuneen vetäjän ja huolellista perehtymistä kyberturvallisuuden yleiseen kenttään, yrityksen omiin erityisongelmakohtiin tuossa kentässä, sekä luonnollisesti riittävää yritysjohdon sitoutumista.

Kehityksen jarru tai katalysaattori saattaa olla yrityksen kehityspäällikkö tai tietoturvapäällikkö, jos tällaisia tehtäviä on edes nimetty. Kehittämisen käytiin saattaminen edellyttää tietoisuuden riittävää leviämistä, jotta yrityksen toimijat ymmärtävät riittävästi kyberuhkien todennäköisestä kohdistumisesta omaan toimintaansa. Vasta tämän jälkeen yritykseen voi syntyä tarvittava vastuiden määrittely ja resursointi tuotantoon soveltuvien kyberturvallisuusuhkien havaitsemiseen, torjuntaan ja ennakkovarautumiseen.

6.1.1 Yrityksen sisäinen kyberturvallisuusseminaari

Tietoisuuden parantaminen yrityksessä voidaan saada alkuun esim. herättävän kyberturvallisuusseminaarin avulla, jossa havainnollistetaan, millä tavoin automaatiojärjestelmiin on aiemmin tunkeuduttu, millaisia työkaluja, palveluja tai sosiaalista tiedustelua hyökkääjät käyttävät ja millaisia vahinkoja kotimaassa tai ulkomailla on tällä tavoin saatu aikaan.

Mitä muita aineksia tietoisuutta hedelmällisesti kehittävän automaation kyberturvallisuusseminaarin sitten tulisi sisältää? Seuraavassa esitellään lyhyesti automaatioyrityksille suunnattuja (yrityksen sisäisiä) seminaareja.

6.1.1.1 Agenda – Automaation kyberturvallisuusseminaari yritykselle

Yrityksen henkilöstön tietoisuutta herättelevän kyberturvallisuusseminaarin agenda on muotoutunut usein seuraavalla tavalla.

Esimerkki. Agenda – Yritystä herättelevä puolen päivän kyberturvallisuusseminaari.

Osuus 1: Perusteet

1. Automaation kyberturvallisuuden ja IT-tietoturvan vertailua
2. Automaation kyberturvallisuuden tilanne
    - Uhkat, trendit
        - Millä tavoin automaatiojärjestelmiin on aiemmin tunkeuduttu?
        - Millaisia työkaluja, palveluja tai sosiaalista tiedustelua hyökkääjät käyttävät?
        - Millaisia vahinkoja kotimaassa tai ulkomailla on tällä tavoin saatu aikaan?
    - Suomen automaation kyberturvallisuustilanne
    - Mitä Suomessa on meneillään automaation tietoturvan kehittämiseksi?
3. Kyberturvallisuuden tehtävät, roolit ja työnjako automaation elinkaaressa
    - Kokonaiskuva kyberturvallisuustehtävien työjaosta
    - Tärkeimpiä tehtäviä: Tilaaja (hankinta, IT, automaatio jne.), projektitoimittaja, järjestelmätoimittaja, jne.
    - Keskustelua yrityksen omasta työnjaosta?

Osuus 2: Jalkautusesimerkkejä

4. Esimerkkejä tietoturvan jalkauttamisesta tuotantoon yrityksen toiveiden mukaisesti, esim.:
    - Kyberturvallisuusvaatimukset ja hankintaohjeet
    - Järjestelmien koventaminen automaation elinkaaressa
    - Automaation kyberturvallisuustestaus ja sen kehittäminen
    - Esimerkkejä kybersuojausten jalkauttamisesta muissa yrityksissä
5. Kysymykset, keskustelu, jatkotoimenpiteet

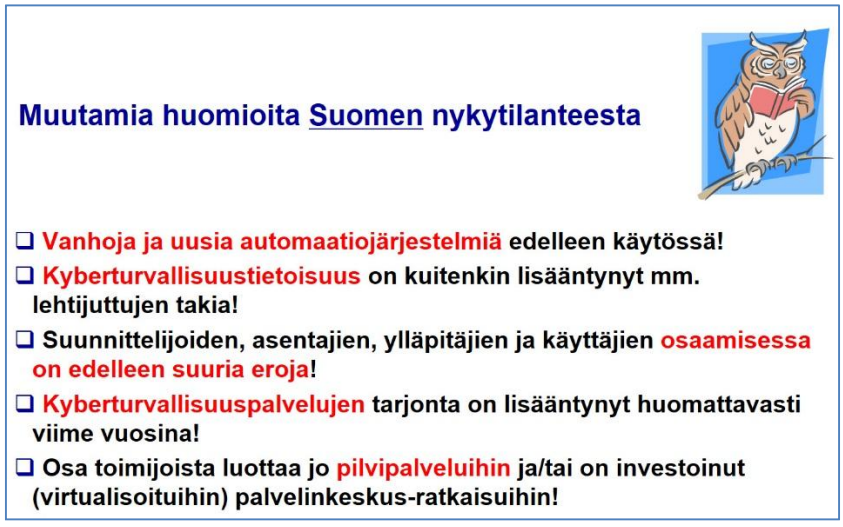
Painottamalla erityisesti automaation kyberturvallisuuden tilannetta ja akuutteja kyberturvallisuusuhkia ja -trendejä olemme herättäneet henkilöstössä ja johdossa reaktioita, jotka ovat johtaneet vakavaan sisäiseen keskusteluun ja kyberturvallisuuden kehitysryhmien perustamiseen. Tällaisessa tapauksessa sisäinen seminaari on onnistunut erittäin hyvin tietoisuuden herättämisessä.

Kasvavia yleisluonteisia uhkia, joilla voi olla automaation kyberturvallisuuteen vaikuttavia elementtejä ja jotka koskettavat myös Suomea, ovat mm.

- verkkorikollisuus yleensä
- ilkivalta verkossa
- hybridiuhat (kriittinen infrastruktuuri)
- terrorismi ja sen suunnittelu (mahdollisesti).

6.1.1.2 Esimerkkikalvoja – Automaation kyberturvallisuuden tilanne

Kuva 8. Esimerkkikalvo – Yleisimpiä tietoturvan loukkauksia.



Kuva 9. Esimerkkikalvo – Muutamia huomioita Suomen nykytilanteesta.

6.1.2 Foorumeihin liittyminen

Kun kiinnostus kyberturvallisuusasioihin on herännyt, mikä olisi tehokas tapa jatkaa aihepiiriin perehtymistä välittömästi?

Kyberturvallisuuden todellisuuteen heräämisen jälkeen yrityksen avainhenkilöiden liittyminen Kyberturvallisuuskeskuksen sähköpostituslistoille [POSTITUSLISTAT] helpottaa huomattavasti säännöllistä perehtymistä kyberturvallisuusuhkiin. Erityisesti ajantasainen tieto automaatiojärjestelmien haavoittuvuuksista ja toteutuneista uhkista lisääntyy tällöin nopeasti. Toisaalta avainhenkilöt saavat myös tämän väylän kautta tiedon yhteisistä kyberturvallisuusseminaareista, -työpajoista ja tulosten esittelytilaisuuksista, joista on kerrottu lisää myöhemmin.

Automaation kyberturvallisuudesta kiinnostuneille tarkoitettujen foorumien ja postituslistojen kautta saattaa päästä esim. keskusteluihin jo pidemmälle edenneiden kollegoiden kanssa, joilta voi saada syvempää kokemusperäistä tietoa kyberturvallisuuden jalkauttamisesta käytännössä yrityksen tuotantoon. Viranomaisethan voivat olla esteellisiä suosittelemaan esim. tietyn valmistajan tuotteita ja ratkaisuja, mutta olemassa olevien tuotteiden haavoittuvuuksista kyllä saa sähköpostituslistojen kautta erittäin hyvin tietoa.

Alustavista suunnitelmista ”Automaation kyberturvallisuuden yhteistyöportaalin” perustamiseksi kerrotaan tämän luvun lopussa.

6.2 Yhteiset työpajat

Teollisuusautomaation kyberturvallisuuden todellinen kehittyminen Suomessa vaatii kaikkien alan toimijoiden osallistamista. Tämä johtuu mm. siitä, että kyberturvallisuuden tason toteuman ratkaisee lopulta ”arvoketjun heikoin toimija” ja ”tietoverkon huomaamaton turva-aukko”. Kaikki automaation tietoturvan toteumaan vaikuttavat henkilöt eivät valitettavasti vieläkään ole ymmärtäneet tilanteen vakavuutta, joten tarvittavia kehitysohjelmia ei ole kaikkialla käynnistetty.

Turvallisen toiminnan vastuuta ei voi ulkoistaa, sillä yritysjohto ja tuotannon johto vastaavat viimekädessä itse tarvittavien kyberturvamenettelyjen käyttöönotosta ja valvonnasta. Riittävän kyberturvallisuustason ja siihen pääsemiseksi tarvittavan panostuksen määrää ei joko tunneta tai siitä ei välitetä. Tällöin tuotantotoiminnassa otetaan harkitsemattomia riskejä jatkuvuuden suhteen. Yhteiset työpajat ovat seminaareja syvällisempiä tilaisuuksia, joissa osallistujien kesken voidaan keskustella arkaluonteisemmistakin asioista ja ideoita voi syntyä esim. yhteisistä pilottiprojekteista.

Seuraavissa alakohdissa esitellään tiivistetysti muutamia nostoja KYBER-TEO 2014–2016 -projektikokonaisuuden yhteydessä pidetyistä yhteisistä työpajoista. Ne eivät ole kattavia kuvauksia ko. työpajoista, vaan antavat lukijalle käsityksen niiden huippukohdista. Kyberharjoittelutyöpajat käsitellään erikseen luvussa 7 ”Harjoittelu & koulutus”.

6.2.1 Testaus-työpajat

Projektin kuluessa pidettiin myös kyberturvallisuustestaukseen liittyvä työpaja, jossa käsiteltiin mm. testauksen jalkautusprosessia yrityksen omaan tuotekehitysprosessiin. Tämä on kuvattu Testaus-luvun kohdassa ”Tietoturvatestauksen kehittämisen prosessi”. Kokemuksiamme automaation kyberturvallisuustestauksesta on vedetty yhteen seuraavassa.

Muutamia huomioitamme automaatioverkon laitteiden testauksesta:

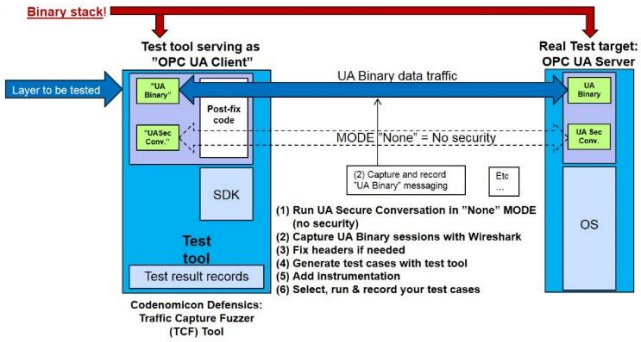
Monet kenttäväyläprotokollat ovat turvattomia, joten kannattaa keskittyä laitteiden robustisuuden (mm. *fuzzing*) testaukseen:

- Yhdenkin laitteen haavoittuvuudet voivat mahdollistaa hyökkäykset verkon muihin osiin, joten syvyyspuolustus tulisi aina toteuttaa.
- Tietoturvaominaisuuksia on vähitellen tulossa myös kenttäväyliin, mutta tällöinkin ongelmaksi usein jää suojauksen kattavuuden puutteet. Käyttöönotto saattaakin edellyttää kaikkien verkkojen ja laitteiden uusimista.

Toiminnallisuutta löytyy yleensä paljon protokollapinon ylemmiltä kerroksilta, jolloin siellä on myös paljon testikohteita, jotka sisältävät haavoittuvuuksia ja vaarallisia riippuvuuksia.

Monimutkaisemmat testausskenaariot:

Paljon toiminnallisuutta ja komponentteja sisältävien testiympäristöjen haasteena on mahdollisimman todenmukaisen konfiguraation asettaminen sekä erilaisten konfiguraatioiden testaus kattavasti. Vaikka varsinaisena testikohteena olisikin ainoastaan tietty testiympäristön osa, myös laajempaa kokonaisuutta on hyvä testata, jotta tunnistetaan heikoin lenkki, esim. konfigurointiin tarkoitetut Windows- ja Android-ohjelmistot. Kuvassa 10 on esimerkki projektissa esiin tulleista OPC-UA-palvelimen *fuzz*-testauksen valmisteluun liittyvistä toimenpiteistä.



Kuva 10. Projektissa tutkittu OPC-UA-testitapaus.

6.2.2 Monitorointi-työpajat

Projektissa pidettiin useita mielenkiintoisia esityksiä automaatioverkon monitorointia käsittelevissä työpajoissa. Tavoitteena oli avoimin mielin keskustella automaatioverkkojen monitoroinnin perusteista ja toteutuksesta. Näin siitäkin huolimatta, että uusien ideoiden kaupallistaminen itse ei yleensä ole järkevää tai on vähintään monen vuoden päässä.

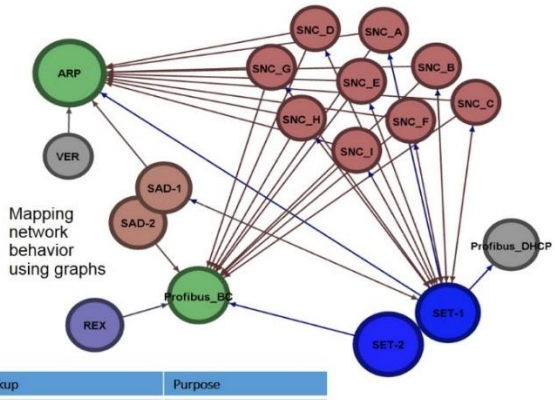
Osa kyberturvallisuuspalveluja tarjoavista yrityksistä on pilotoinut tai tuotteistanut teollisuuden verkkoliikenteen seurantaan soveltuvia palveluja, joissa on samoja piirteitä kuin työpajoissa esitellyissä monitorointikonsepteissa. Tänäkin päivänä erilaisten verkon seurantaan tarkoitettujen palvelujen toiminta kuitenkin edellyttää ammattimaista tapahtuma-analyysiä. Koneet eivät edelleenkään korvaa ihmistä hyvän palvelun toteuttamisessa.

6.2.2.1 Esimerkki

Eräs tällainen kiinnostava, jo vuoden 2014 työpajassa esitetty konsepti on LHT (*Link History Tree*), jota VTT:n Mirko Sailio on kehittänyt pitkään useissa eri tutkimusprojekteissa, mm. EU ECOSSIAN -projektin yhdeksi komponentiksi. LHT:ssä “järjestelmät” ja “liikenne” havaitaan seuraavin periaattein:

- Kukin MAC-osoite (OSI-taso 2) tulkitaan erilliseksi järjestelmäksi.
- MAC osoitteita tulee
    - järjestelmien verkkokorteista
    - protokollista (erityisesti broadcast/multicast).
- Liikenne on järjestelmien välistä (tietoliikennepaketti, jossa näkyy molemmat MAC-osoitteet), ja se voi olla yksi tai kaksisuuntaista.

Menetelmä havaitsee automaattisesti poikkeamat verkon laitteissa ja yhteyksissä.



Abbr	MAC	MAC address lookup	Purpose
SET	[redacted]	Siemens AG A&D ET	Siemens CPU
SNC	[redacted]	Siemens Numerical Control Ltd., Nanjing	HMI type 1
REX	[redacted]	Hilscher GmbH	Rexroth CPU
SAD	[redacted]	Siemens AG, A&D AS EWK PU1	HMI type 2
VER	[redacted]	MSC VERTRIEBS GMBH	
ARP	[redacted]	Broadcast	Address resolution
Profibus_		Profibus _BC broadcast	Multicast protocol
Profibus_		Profibus_DHCP device discovery	Multicast protocol

Kuva 11. Työpajassa esitelty VTT PrintoCent -liikenteen kaappaus ja sen tulkinta (LHT).

6.2.3 Medianäkyvyys-työpajat

Projektissa nähtiin, että medianäkyvyys on tänä päivänä välttämätöntä suuren yleisön ja samalla automaation kohderyhmien (laajasti ottaen) kyberturvallisuustietoisuuden kasvattamiseksi ja kyberturvallisuustilanteen laajamittaiseksi parantamiseksi. Medianäkyvyyttä toteutettiin pääosin projektin resurssien rajoissa ja projektin osallistujia kannustettiin parantamaan automaation kansallista kyberturvallisuustietoisuutta käytettävissä olevin voimavaroin. Koimme, että tällä tavoin toimien kehittämistä ja parantamistyötä saadaan laajamittaisemmin jalkautumaan avaintoimijoille myös tulevaisuudessa.

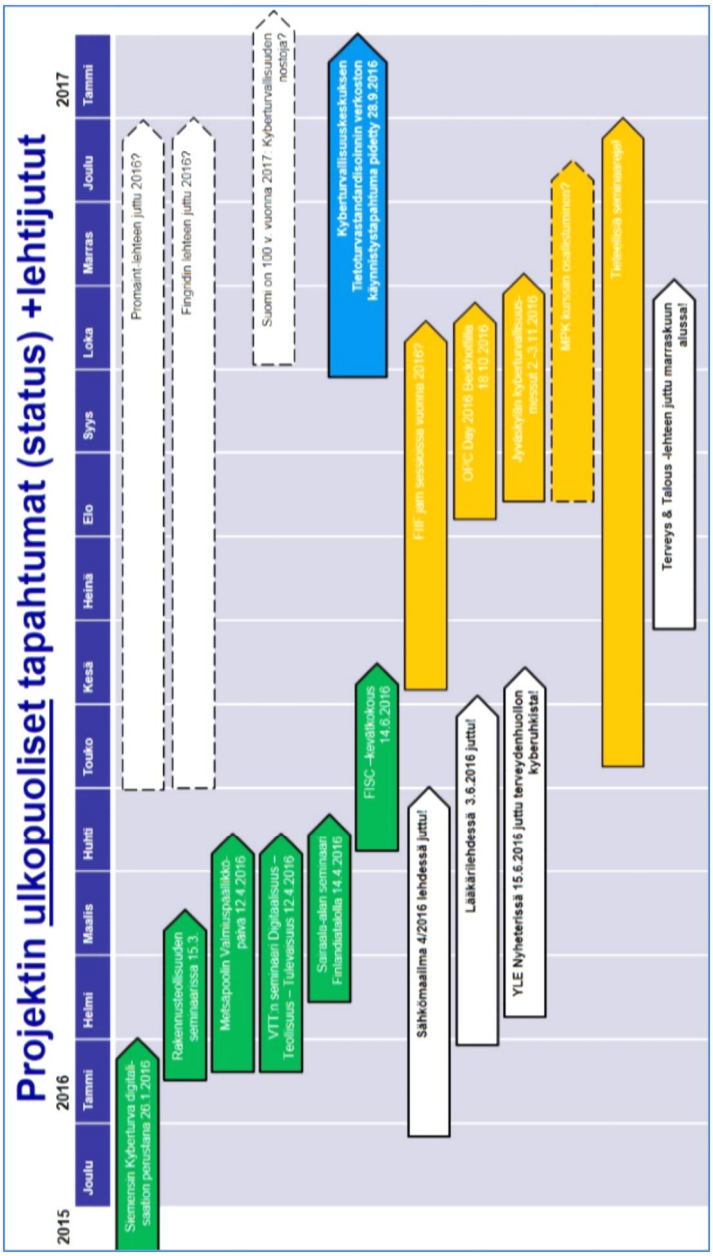
Tiedottamisemme päämääränä on ollut tavoittaa ennen kaikkea kotimaisen teollisuuden johto ja asiantuntijat, kriittiset yritykset, ml. teollisuus, palveluntarjoajat, järjestelmätoimittajat, sekä näiden kumppanit.

Tärkeinä näkyvyyden osa-alueina pidimme mm.

- teollisuuden ja automaation eri toimialoja (tietoisuus, palvelujen kysyntä)
- terveydenhuoltoalaa (tietoturvatietoisuuden parantaminen)
- teollisen internetin foorumeja (tietoturvatietoisuuden kehittäminen)
- tieto- ja kyberturvallisuuden palveluyrityksiä (palvelujen kehittäminen)
- julkista mediaa (tietoturvatietoisuuden lisääminen).

Pääsanomamme mediassa on ollut:

- Kehitystä on mahdollista saada aikaan yrityksissä yhteistyöllä.
- Kyberturvallisuuden avulla kilpailukyky säilyy ja paranee (USA:n markkina jne.).
- Jatkuvuuden parantuminen, ei katkoja tuotannossa!
- Toimivat verkostot ovat avain onnistumiselle.



Kuva 12. KYBER-TEO-projektin ulkopuolisen medianäkyvyyden suunnitelmia lokakuussa 2016.

6.3 Yhteistyöportaalista

Hankkeen Medianäkyvyys-työpajan yhteydessä syntyi ajatus automaation kyberturvallisuuden yhteistyöportaalista. Koimme, että syvempi pitkäjänteinen yhteistyö vaatisi paremmat sähköiset työkalut kuin sähköpostit ja puhelut, joiden avulla tiedon kasaantumista ja jakamista on vaikeata hallita pitkällä aikajänteellä. Ajatuksena oli, että uusi portaali voisi mahdollistaa koherentimman tiedonvälityksen ja luottamuksellisen keskustelun automaation toimijoiden välillä, ainakin kotimaassa. Portaalissa voisi esim. kysellä ja selvittää teollisuuden toimijoiden kokemuksia, tulevaisuuden tarpeita, tieto-omaisuuden hallintaan liittyviä kysymyksiä, kehittää yhteisiä ohjeistoja ja esim. päivittää aiemmin kehitettyä hankintavaatimuskantaa (COREQ-ACT) jne.

Uuden yhteistyöportaalin tarkoituksena olisi siis kotimaisen automaation kyberturvallisuuden yhteistyön, -palvelujen ja -näkyvyyden dramaattinen parantaminen, aiheeseen liittyvän materiaalin ja palvelujen välittäminen sekä pedagogisen näkökulman vahvistaminen. Seuraavassa katsaus KYBER-TEO-projektin suunnitelmiin automaation kyberturvallisuuden yhteistyöportaalin kehittämiseksi.

6.3.1 Portaalin tavoite

Portaalin tavoitteena on radikaalisti lisätä automaatiotoimittajien verkoston ja automaatiota hyödyntävän kotimaisen teollisuuden kybertietoisuutta ja -yhteistyötä. Suomenkielistä automaation kyberturvallisuuspalvelujen kehittämisportaalia tarvitaan em. tavoitteen saavuttamiseksi kattavasti ja nopeasti.

Portaalin avulla myös synnytetään ja pilotoidaan uusia kyberturvallisuuspalveluja ja -yhteistyötä yhdessä kotimaisen teollisuuden, palveluntarjoajien, tutkimuslaitosten ja viranomaisten kanssa. Portaalin yleiskäyttäjäksi liittymisen tulee olla helppoa, mutta portaali toimisi tulevaisuudessa myös kanavana erilaisiin muihin luottamuksellisiin tiedonvaihtoryhmiin, joiden synnyttämistä portaalin avulla edistetään. Portaalista ei saa kuitenkaan tulla yksinomaan yritysten mainoskanava.

Uskomme, että portaalilla olisi mahdollista aikaansaada kotimaisen automaation kyberturvallisuuden yhteistyön ja näkyvyyden konkreettinen parantuminen, ja täten kyberturvallisuuden parempi jalkautus kriittiseen infrastruktuuriin ja laajemminkin elinkeinoelämäämme. Myös koordinointi mm. erilaisten yhdistysten kanssa on tärkeää, mikäli yhteistyökontakti on käytettävissä.

Portaalin missio on saattaa yhteen automaation kyberturvallisuuteen vaikuttavat käytännön toimijat, sekä mahdollistaa toimiva, luottamuksellinen yhteistyö.

Kohderyhmiä:

- Teollisuussektoreiden yhdistykset ja yritykset
- Automaatioalan yhdistykset ja yritykset
- Huoltovarmuuskeskuksen poolit
- Kunnat ja kaupungit
- Maanpuolustuskoulutusyhdistys (Puolustusvoimat)

Projektissa tarkoituksenamme oli kartoittaa ja kehittää mm. portaalin palvelukonseptia, mahdollisia sidosryhmiä ja sisällöntuottajia, mutta käytännössä itse toimintaa ei saatu voimallisesti vauhtiin. Portaalin vahva omistajuus on kriittistä onnistumiselle, samoin houkutteleva käyttöliittymä. Portaalin operoijan tulisi olla riippumaton ja aktiivinen taho. Kehitysehdotuksia olisi hyvä saada käyttöön kohderyhmiltä, sekä kriittisen infrastruktuurin yrityksiltä ja yhdistyksiltä, mukaan lukien vesihuolto, terveydenhuolto, rakennusteollisuus, elintarvikehuolto jne. Tulisi perustaa aktiivinen kehitysryhmä, jonka ehdotusten ja neuvojen avulla portaalia määritellään ja kehitetään.

6.3.2 Portaalin rakenteesta ja luottamustasoista

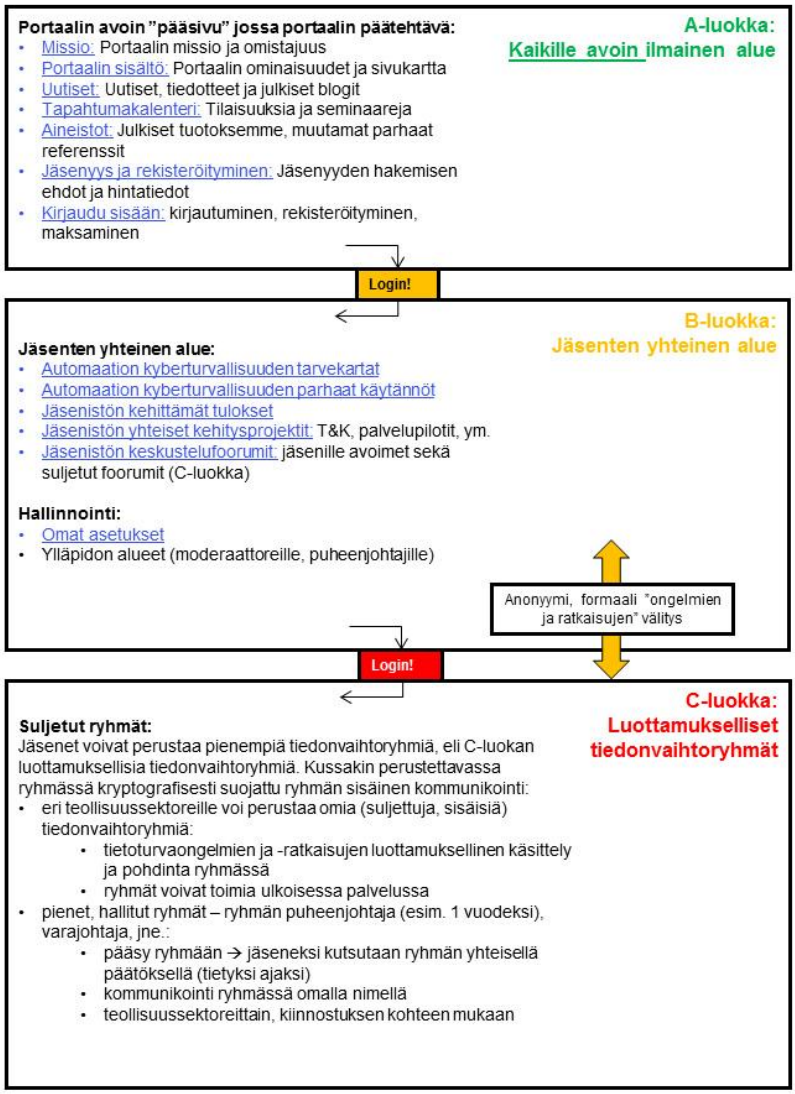
Kehitimme projektissa hierakkisen mallin portaalissa tehtävän yhteistyön jakamiseksi erilaisiin toiminnallisiin alueisiin, jotta osallistujat voisivat edetä syvempään keskinäiseen yhteistyöhön luottamuksen vähittäisen kehittymisen avulla.

Tuotteistetussa portaalissa toiminnallisuus ja sisältö voisivat olla ryhmiteltynä kolmeen luottamustasoon:

- A-luokka: Kaikille avoin ilmainen alue (pääsivu, uutiset, tapahtumakalenteri, hinnoittelu, ym.)
- B-luokka: Jäsenten yhteinen alue (vaatii rekisteröitymisen luonnollisena henkilönä → jäsenmaksu)
- C-luokka: Luottamukselliset tiedonvaihtoryhmät (erilliset ryhmät sektoreille / tarpeille)

Portaalin yleiskäyttäjäksi olisi helppo liittyä (A-luokan avoin alue ja B-luokan jäsenten yhteinen alue), mutta lisäksi portaali voisi toimia myös kanavana erilaisiin muihin vielä luottamuksellisempiin tiedonvaihtoryhmiin, joiden syntymistä edistettäisiin portaalissa tehtävän yhteistyön kautta.

Seuraavassa kuvassa on esitetty eräs malli automaation kyberturvallisuuden yhteistyöportaalin rakenteelle ja luottamustasoille. Tämä ei ole tietenkään lopullinen malli tai rakenne, vaan tarkoituksena on keskustelun vieminen konkreettiselle tasolle sekä antaa keskustelun pohjaksi malli jota voi edelleen kehittää ryhmässä. Nykyisiä sosiaalisen median sovelluksia voi toki myös käyttää yhteistyöhön ja sen kehittämiseen, mutta tällöin jokaisen on ymmärrettävä niihin syötettävän tiedon luottamuksellisuuden sekä osallistujien yksityisyyden mahdolliset ongelmat. Tämä tosin voi olla ongelma lähes kaikissa muissakin digitaalisten yhteistyöalustojen teknisissä ratkaisuissa.



Kuva 13. Automaation kyberturvallisuuden yhteistyöportaalin rakenne ja luottamustasot.

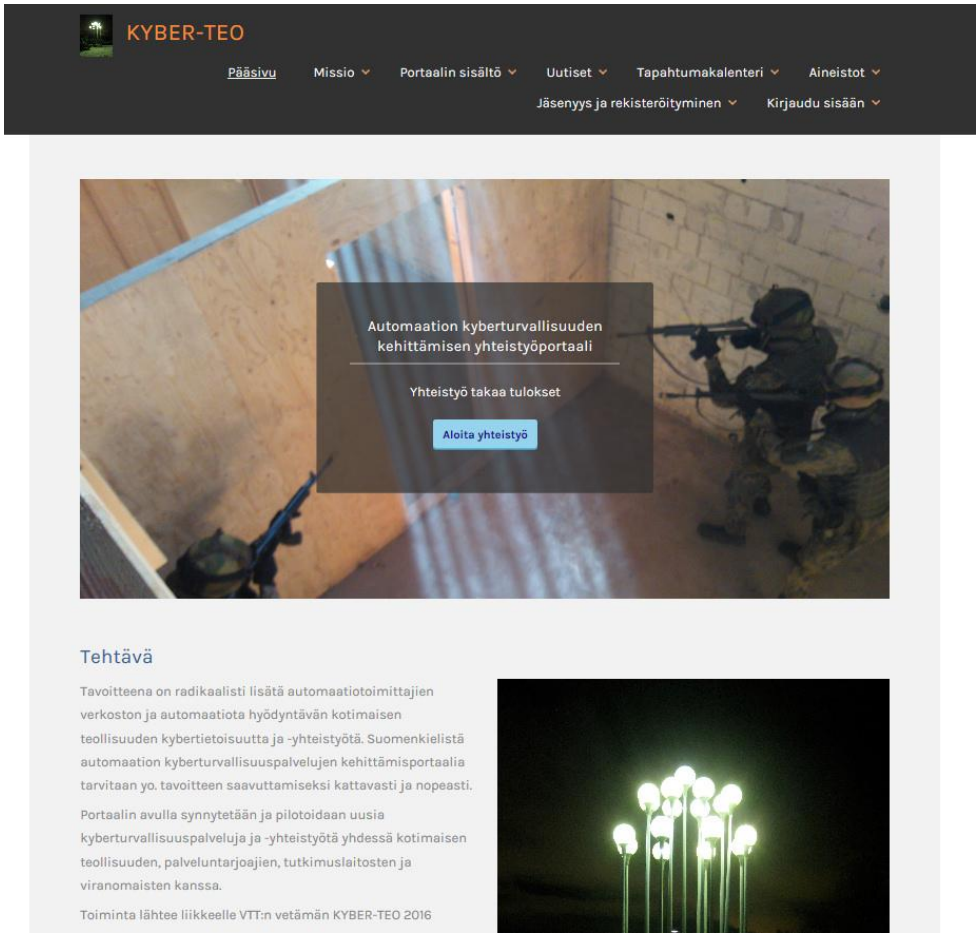
Julkisella yleisöllä olisi pääsy A-luokan alueelle, jossa jaetaan automaation kyberturvallisuuteen liittyvää perusinformaatiota sekä tärkeimpiä julkisia tuloksia. Tämä mahdollistaa asiasta kiinnostumisen ja ennen kaikkia sen ymmärtämisen, että asian kehittämiseksi on tehty jo pitkään töitä ja esimerkiksi hyviä malliratkaisuja, standardeja ja referenssejä on paljon saatavilla.

Jäsenten yhteisellä (B-luokka) alueella tapahtuisi jäsenten välinen, hieman luottamuksellisempi yhteinen kehitystyö tai pilottien suunnittelu, sekä aiheeseen liittyvät keskustelut ja tiedonjakaminen. C-luokan suljetut ryhmät mahdollistaisivat erittäin luottamuksellisten pienten ryhmien perustamisen ja täten arkaluontoisten keskustelujen ja informaation jakamisen. Näiden tekninen toteutus tulisi olla eriytetty siten, että niillä ei ole suoraa yhteyttä muuhun portaaliin.

B- ja C-luokan alueita ei avata tässä julkaisussa enempää, sillä niiden määrittelytyö on vasta alkuvaiheessa.

6.3.3 A-luokan alue – kaikille avoin

Julkiselle yleisölle avoin alue koostuisi pääsivusta sekä muusta julkisesta informaatiosta. Pääsivulla kuvattaisiin myös sivuston tavoite ja tehtävä. Pääsivun yksi visuaalinen luonnos on esitetty seuraavassa kuvassa (KYBER-TEO-projektissa tehty luonnos).



Kuva 14. Hahmotelma portaalin pääsivusta (luonnos, KYBER-TEO-projekti).

Portaalin julkisen alueen tavoitteena olisi mm. tuottaa perustietoa automaation kyberturvallisuudesta laajalle yleisölle. Tämä voisi tarkoittaa myös mm. suurta yleisöä kiinnostavia uutisia, listaa tärkeimmistä yhteyshenkilöistä, tapahtumakalentereja sekä helppoa ja ymmärrettävää tapahtumaseurantaa. Myös esim. blogikirjoitukset ajankohtaisista teemoista ja tiivistelmät monimutkaisista mutta kiinnostavista asioista tai tutkimustuloksista voisivat kuulua ainakin osin myös tälle julkiselle alueelle.

Julkisen alueen perustamisen tärkeä motiivi on tietysti myös herättää ja kannustaa yhteistyöhön niitä automaation kyberturvallisuuden toteumaan osaltaan vaikuttavia henkilöitä, jotka eivät vielä ole olleet tietoisia esim. jo kehitetystä kotimaisesta yhteistyöstä, malleista ja vaatimuksista. Heidänkin tulee saada mahdollisuus osallistua.

6.4 Referenssit

[HEUREKA] https://www.heureka.fi

[MIRAI] https://www.viestintavirasto.fi/kyberturvallisuus/varoitukset/2016/varoitus-2016-04.html

[POSTITUSLISTAT] https://www.viestintavirasto.fi/kyberturvallisuus/viestintavirastontietoturvapalvelut/hvk-toimijoille/postituslistat.html

[TERVEYSUHKIA] https://www.viestintavirasto.fi/attachments/tietoturva/Terveydenhuoltoalan_kyberuhkia.pdf

7. Harjoittelu & koulutus

7.1 Harjoittelu

Kyberharjoittelu on osoittautunut erittäin tärkeäksi tavaksi kehittää erityisesti automaation kyberturvallisuutta.

Konkreettisen harjoittelun jälkeen kukin osallistuja tulee pohtineeksi kriittisesti omaa ja oman yrityksensä toimintaa: Toiminko itse riittävän turvallisella tavalla työssäni ja yksityiselämässäni? Voiko yksityiselämäni esim. sosiaalisessa mediassa vaikuttaa työni turvallisuuteen? Ovatko käyttämäni tai hallinnoimani tuotantolaitteet tai järjestelmät altistuneet turhaan kyberturvallisuusuhkille? Onko tuotannossamme riittävät varajärjestelyt ja toimivatko ne? Harjoittelemmeko me toimintaamme häiriötilanteiden varalle?

Mitä kyberharjoittelu on? Kyberharjoittelulla tarkoitamme organisoituja työpajoja, jossa luentoja ja käytännön harjoituksia yhdistelemällä kehitetään osallistujien kyberturvallisuustietoisuutta ja osaamista. Työpajassa pidetään tyypillisesti alustuksia työpajan teemaan liittyen, minkä jälkeen esitellään demonstraatio tai osallistujat kokeilevat itse alustuksessa käsiteltyyn teemaan liittyvää *hands-on*-harjoitusta.

Kokemustemme perusteella kyberharjoittelutyöpaja kannattaa jakaa toisistaan erottuviin jaksoihin, joista kukin sisältää esim. alustuksen, demonstraation, osallistujien omaa harjoittelua, sekä kysymyksiä ja keskustelua liittyen jakson fokusaiheeseen. Koska informaatiota tulee yleensä paljon kussakin jaksossa, on tärkeää, että etenemisvauhti ei ole liian kova ja että jaksojen väleihin jätetään aikaa myös osallistujien väliselle vapaalle keskustelulle. Tämä voi laajentaa näkökulmaa ja antaa vinkkejä opitun soveltamisesta omassa työssä. Koko harjoitus voi kestää esim. 1–3 päivää, ja siinä voi olla esim. 4–10 erilaista jaksoa, joten riittävä tauotus on tärkeää myös jaksamisen ja vireyden ylläpitämisen kannalta!

Harjoittelutilaisuuksien järjestäminen vaatii monenlaista osaamista. Ensisijaisesti tulee tietysti olla hyvä näkemys siitä, mihin kyberturvallisuuden osa-alueeseen tai

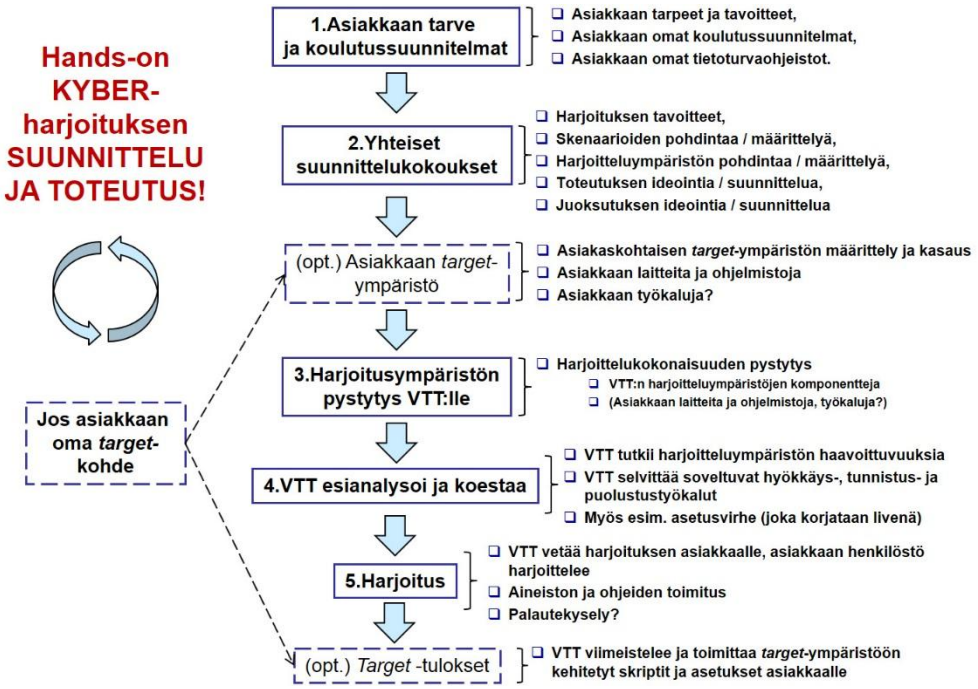
teemaan tuleva harjoitus kannattaa kohdistaa, jotta osallistujat saisivat omalle toiminnalleen suurimman hyödyn. Asiakas ei välttämättä ennakkoon tiedä, mikä kyberturvallisuuden osa-alue vaatisi eniten parantamista omassa yrityksessä tai omassa toiminnassa. Usein esimerkiksi tarve jonkin järjestelmän tai tietyn teknisen ongelman ratkaisemisesta laajentuukin näkemykseksi turvallisen toimintatavan kehittämisestä tuotannon koko henkilöstölle. Automaation kehitystyö ja automatisoidun tuotannon ylläpitäminen kokonaisuudessaan sisältävät valitettavasti niin monta yksityiskohtaa, että tärkeintä on ensin saavuttaa koko yrityksen kattava riittävä tietoisuus ja jokaisen yksilön oikea toimintatapa. Uhat toteutuvat usein henkilöstön huolimattomuuden tai tietämättömyyden kautta.

Kyberturvallisen automaatiojärjestelmän kehittäminen ja ylläpitäminen ovat osaamisen kehittämisen erityiskohteita, sillä automaatiohäiriöiden vaikutukset voisivat ulottua arvaamattoman nopeasti laajaan osaan muutakin tuotantoa, ja täten uhata yrityksen liiketoiminnan jatkuvuutta.

Seuraavaksi käsittelemme kyberharjoituksen suunnittelua, jonka jälkeen esittelemme esimerkin avulla yhtä projektin kyberharjoituksista.

7.1.1 Harjoituksen suunnittelu

Harjoitusten tulee olla asiakastarpeiden mukaisia. Seuraavassa kuvassa on esitetty yksinkertaistettu kaavio kyberharjoituksen suunnittelun ja toteutuksen etenemisestä. Asiakkaan kyberturvallisuuden kehitystavoitteet, avainhenkilöstön mahdolliset kyberturvallisuuden puutteet (jos tiedossa), sekä koulutussuunnitelmat ja mahdolliset tietoturvallisuuteen liittyvät ohjeistot kannattaa mahdollisuuksien mukaan käydä läpi jo ensimmäisessä suunnittelukokouksessa. Tämä antaa mahdollisuuden liittää harjoituksen oheen myös oman ohjeistuksen läpikäyntiä. Mikäli puutteita havaitaan, ohjeistusta kannattaa kehittää tarkemmaksi ja yksiselitteisemmäksi mieluiten jo ennen kyberharjoitusta, jolloin ohjeiston noudattamisen tärkeyttä voidaan korostaa harjoituksessa tehtävien löydösten jälkeen. Esim. pieni konfiguraatiovirhe yhdyskäytävän SSH-tunnelointiasetuksissa saattaa mahdollistaa automaatioverkon huomaamattoman hyväksikäytön tai jopa haltuunoton.



Kuva 15. Kyberharjoituksen suunnittelu asiakkaan kanssa ja kehittämisen eteneminen. Projektin kuluessa kehitetty VTT:n käyttämä malli.

Kuvassa 15 kuvataan kyberharjoituksen suunnittelun ja kehittämisen päävaiheet sekä katkoviivoituksella optionaaliset vaiheet, jotka toteutuvat, mikäli asiakas haluaa harjoitella omassa kohdeympäristössään. Mikäli asiakas uskoo harjoittelun nimenomaan omalla kohteella tarpeelliseksi, se antaa meille mahdollisuuden kehittää asiakasta varten räätälöidyn kyberharjoituksen. Tällöin kyberturvallisuusasiantuntijoiden tulee etukäteen tutkia asiakkaan järjestelmistä löytyviä haavoittuvuuksia tai muita vakavia ongelmia. Asiakaskohtaisessa kyberharjoituksessa kehittäjiä ja ylläpitäjiä sitten opastetaan esim. omin käsin kokeilemaan soveltuvia testaustyökaluja, kokeillaan kyberhyökkäyksen tunnistamista ja soveltuvia suojautumiskeinoja juuri asiakkaan automaatiojärjestelmässä. Tässä tapauksessa on yleensä tehokkainta, että asiakas kasaa itse harjoitukseen valitun kohdejärjestelmänsä (*target*-ympäristö) ja toimittaa sen luottamuksellisesti harjoituksen toteuttajalle esianalyysiä varten. Viimeistään tällöin on syytä sopia luottamuksellisuudesta esim. salassapitosopimuksin, mutta yleensähän NDA kannattaa tietysti laatia jo ennen harjoitteluprojektin käynnistämistä.

Yrityskohtaisen kyberharjoituksen suunnittelussa kannattaa mielestämme huomioida mahdollisuuksien mukaan

- asiakkaan tarpeet ja tavoitteet (harjoituksen osumistarkkuus)
- asiakkaan omat koulutussuunnitelmat (esim. harjoituksen sopiva ajankohta)
- asiakkaan omat tietoturvaohjeistot (oman ohjeistuksen hyödyntäminen)
- harjoituksen tavoitteet
- skenaarioiden pohdintaa/määrittelyä (esim. mitkä käyttötapaukset)
- harjoitteluympäristön pohdintaa/määrittelyä (mikä on käytännöllistä, kriittistä)
- toteutuksen ideointia/suunnittelua (esim. työnjako)
- juoksutuksen ideointia/suunnittelua (harjoituksen jouheva eteneminen).

7.1.2 Esimerkki – Hyökkäys & Suojautuminen -työpaja

Tässä kohdassa kuvaamme tarkemmin ensimmäistä kehittämäämme ja toteuttamaamme kyberharjoitusta, nimittäin ”Hyökkäys & Suojautuminen” -työpajaa. Hankekokonaisuudessa toteutettiin tämän jälkeen myös yksi ”Asiakaskohtainen harjoitus” sekä ”Hyökkäyksen tunnistus ja suojautuminen” -harjoitus, mutta niiden yksityiskohtia emme mm. tilan puutteen vuoksi avaa enempää.

7.1.2.1 Työpajan suunnittelusta

Kyberharjoittelu-työpajan suunnittelu ja valmistautuminen tulee aloittaa hyvissä ajoin ennen työpajaa, jotta tarvittava valmistautuminen voitaisiin edes teoriassa saavuttaa. Tämän olemme oppineet myös oman kantapään kautta. Valmistautumisen seurantapalavereissa suunnitelmaan kannattaa sisällyttää myös käytännön tehtävien lista, sekä kunkin tehtävän valmistumispäivämäärät, toteuttajat, työmääräarviot, tarvittava tuki, nykytila (status) sekä muut onnistumiseen vaikuttavat asiat. Usein jonkin tehtävän tekeminen edellyttää jonkin edellisen tehtävän valmistumista, esim. tunnistustyökalun valinta ja sen käytön suunnittelu edellyttävät sitä vastaavan hyökkäystyökalun valintaa, asentamista ja kokeilemista harjoituskohteeseen. Vasta tämän jälkeen voidaan varmistua, että hyökkäyksen tunnistusharjoitus on toimiva. Mm. tällaisten seikkojen sekä resurssien varmistamisen vuoksi edistymisen jatkuva seuranta on paikallaan.

Esimerkkiharjoitukseksi otamme joulukuussa 2015 pidetyn ”Hyökkäys & Suojautuminen” -työpajan, sillä sen järjestäminen onnistui mielestämme hyvin. Kyseisen työpajan järjestämiseksi määrittelimme mm. seuraavia tehtäviä, joiden edistymistä seurasimme säännöllisesti:

Esimerkki. ”Hyökkäys & Suojautuminen” -työpajan kehittämisen tärkeimpiä tehtäviä.

YLEISET JÄRJESTELYT
- Testikohdepyynnöt, kutsut, tilajärjestelyt, tarjoilut

TESTIYMPÄRISTÖ
- Testiympäristö – Asennus ja käyttöönotto
- Testiympäristö – Ylläpito

HARJOITUKSEN ASETTELU (*set up*)
- Työpajassa käytettävien skenaarioiden määrittely
- Arkkitehtuuri – Määrittely ja toteutus
- PCt, virtuaalikoneet ja palvelimet: asennus ja ylläpito
- Kenraaliharjoitus – VTT:n tiimillä
- Laitteet ja ohjelmistot paikan päälle
- Materiaalit osallistujille

TESTAUSJÄRJESTELMÄT
- Testauslaitteet, verkot ja ohjelmistot – Asennus ja käyttöönotto
- Testauslaitteet, verkot ja ohjelmistot – Ylläpito

MONITOROINTIJÄRJESTELMÄT
- Monitorointilaitteet ja ohjelmistot – Asennus ja käyttöönotto
- Monitorointilaitteet ja ohjelmistot – Ylläpito

HYÖKKÄYKSET JA VASTATOIMET
- Hyökkäysten määrittely ja toteutus
- Vastatoimien määrittely ja toteutus

7.1.2.2 Työpajan agenda

”Hyökkäys & Suojautuminen” -työpajassa halusimme jokaisen osallistujan oppivan ymmärtämään mahdollisimman konkreettisesti vastapuolen eli hyökkääjän asenteen – mitä työkaluja hyökkääjällä on käytettävissään ja miten hän niitä pystyy käyttämään. Tämä antoi samalla realistisen kuvan hyökkääjän mahdollisuuksista ja hyökkäysvektoreista, eli hyökkäyssuunnista. Toisaalta osallistujat toivottavasti ymmärsivät myös, että hyökkääjän tarvitsemat kyvykkyydet eivät välttämättä tarvitse olla suuret, jos he osaavat valita soveltuvat hyökkäystyökalut tai hyödyntävät rikollisten verkkopalveluja.

Toinen erittäin tärkeä aspekti tässä harjoituksessa olivat hyökkäyksen tunnistaminen ja demonstroiminen käytännössä sekä suojautumiskeinojen pohtiminen. Suojautumiskeinoja haluttiin käsitellä konkreettisen kyberhyökkäyksen yhteydessä, sillä ilman minkäänlaista käsitystä hyökkääjän asenteesta ja työkaluista, hyökkäyksen tunnistaminen ja puolustautuminen jäävät molemmat helposti liian vajavaisiksi. Tämän yksipäiväisen työpajan agenda muotoutui pitkällisen työstön jälkeen lopulta seuraavaksi:

Esimerkki. ”Hyökkäys & Suojautuminen” -työpajan agenda.

Tervetuloa ja osallistujien esittely

Orientaatio ja osallistujien PC:hen tutustuminen

- Yleistä työpajasta
- Ympäristön esittely
- Automaatioympäristön esittely
- Monitoroinnin esittely
- PC:iden käytön opettelu yhdessä
- Virtuaalikoneiden käyttö, IP-osoitteet, komentorivi ym.
- Hyökkäystyökalujen käyttöön tutustuminen

1. Jakso – Murtautuminen toimistoverkkoon
2. Jakso – Hiljainen verkkotiedustelu

Lounas

3. Jakso – Aggressiivinen tiedustelu
4. Jakso – Palvelunesto
5. Jakso – Automaatioverkkoon tunkeutuminen

Työpajan yhteenveto

Toteutunut agenda näytti siis varsin ”väkivaltaiselta”, mutta toisaalta näin saatiin herätettyä osallistujien mielenkiinto aihepiiriin erittäin hyvin. Näyttää myös siltä, että osallistujien mielenkiinto aihepiiriin on säilynyt myös tämän jälkeen, sillä esim. osaamisen laajuus ja taso näyttävät parantuvan koko ajan. Erilaisten hyökkäysten tunnistaminen, kyberturvallisuustestaus ja automaatioverkkojen seuranta ovatkin olleet erityisiä mielenkiinnon kohteita koko hankekokonaisuuden ajan.

7.1.2.3 Työpajan tarkoitus ja tavoitteet

On hyvin eri asia toteuttaa tai osallistua työpajaan, jossa tarkoituksena on erilaisten työkalujen opettelu ja oppiminen, kuin työpajaan, jossa tarkoituksena on oppia hyökkääjän ajatusmalli. Kullakin Kyberharjoittelu-työpajalla on siis omat tavoitteensa. Seuraavassa esitetään joulukuussa 2015 toteutetun työpajan tavoitteet, joita oli ehkä liikaakin yhteen työpajaan.

Esimerkki. ”Hyökkäys & Suojautuminen” -työpajan tarkoitus ja tavoitteet.

Tuoda uhat näkyviin koulutettaville!

- Hyökkääjän ajatusmalli ja tavoitteet esiin!
- Yritysten edustajat ymmärtävät paremmin todellisia kyberuhkia, joita kohdistuu heidänkin käyttämiinsä järjestelmiin.

Tutustua käytännössä tärkeimpiin kybertyökaluihin (hyökkäys, seuranta, tunnistus).

Oppia alkeet hyvistä kyberkäytännöistä, toimintatavoista ja soveltuvista työkaluista.

Tuoda esiin haavoittuvuuksia ja tunnistaa samalla ehkä myös oman yrityksen kyberturvallisuuden tarpeita.

OPTIO: Erityisessä yrityskohtaisessa harjoituksessa voitaisiin lisäksi

- koestaa henkilöstön kybervalmiutta ja parantaa heidän käytännön suojaustaitojaan
- koestaa asiakkaan omia järjestelmiä erilaisia hyökkäyksiä vastaan ja opetella hyökkäyksiltä puolustautumista ja ennakkovarautumista
- opettaa ja koestaa yrityksen omia kyberturvallisuusohjeita.

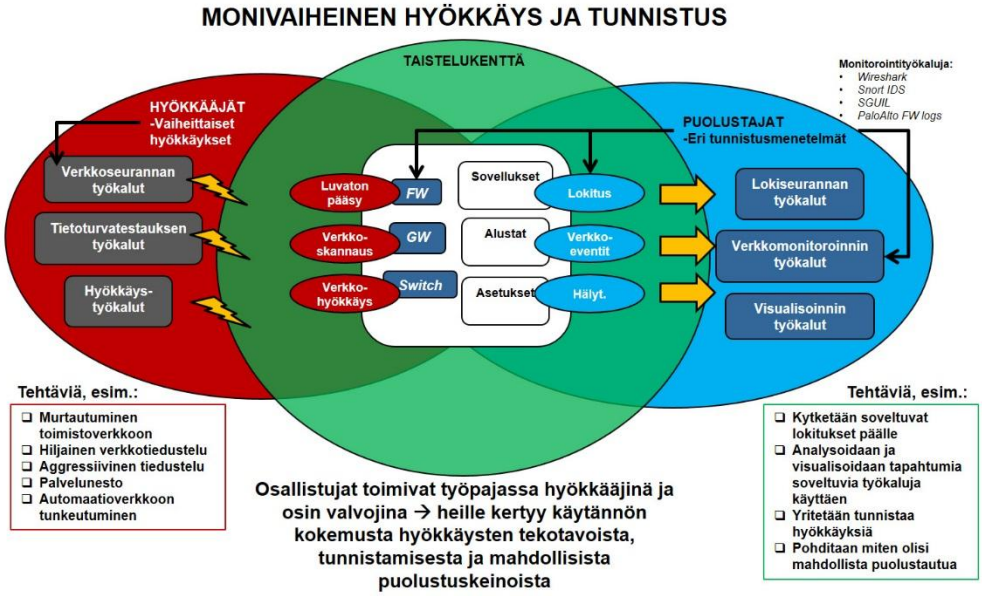
Harjoituksen pidettyämme havaitsimme näiden tavoitteiden olleen hieman liian laajat, eli uutta asiaa oli joillekin jo liikaakin.

7.1.2.4 Työpajan peruskonsepti

Kyberharjoittelu-työpajan peruskonseptin tulisi olla yksinkertainen ja ymmärrettävä, jotta kaikki osallistujat tietäisivät joka hetki, mitä ollaan tekemässä ja miksi. Yhdessä ja samassa työpajassa mm. tutustuttiin hyökkääjän, hyökkäyksen tunnistajan ja puolustajan näkökulmiin, toimittiin useissa erilaisissa kohdissa verkkoarkkitehtuuria hyökkäyksen vaiheesta riippuen sekä visualisoitiin tapahtumia muutamilla erilaisilla työkaluilla. Tällainen monipuolinen työpaja oli toimiva ja antoisa heille, jotka olivat tutustuneet syvällisesti kyberturvallisuuteen ja työkaluihin ennestään, mutta heille, jotka eivät ole kyberturvallisuuden ammattilaisia, työpaja saattoi käydä joiltain osiltaan liian haastavaksi ja asiasisältöä oli ehkä liikaakin.

Järjestävän tahon asiantuntijuutta ei voi liiaksi korostaa harjoituksen onnistumisen kannalta. Työpajojen toteutuksessa olikin haastavaa osallistujien ennakkotietojen ja -osaamisen vaihtelevuus. Toisaalta kyberturvallisuusasioihin vasta perehtyville tulisi järjestää konseptiltaan mahdollisimman yksinkertainen ja selkeä harjoitus, mutta

toisaalta jotkut hyvin edistyneet osallistujat voivat alkaa kouluttaa harjoituksen vetäjiä! Tärkeässä roolissa tulee olla osallistujien innostaminen itsenäiseen oppimiseen ja nykyisen toimintatapansa kehittämiseen.



Kuva 16. ”Hyökkäys & Suojautuminen” -työpajan peruskonsepti.

Kuvassa 16 esitetään eräs Kyberharjoittelu-työpajojen peruskonsepti, jota koestamalla uskomme saaneemme innostettua hankkeeseen osallistuneita pohtimaan entistä syvällisemmin oman automaatiojärjestelmänsä suojaamista kyberuhkia vastaan tai esimerkiksi hyökkäysten havaitsemiseen käytetyn prosessin tai menetelmän parantamista. Samalla on saatu mm. ensikäden tietoa kyberturvaamisen erilaisista vaatimuksista, menetelmistä ja työkaluista, mahdollisesti havahduttu tiimityöskentelyn tärkeyteen tai vaihdettu arvokkaita vertaiskokemuksia muiden yritysten edustajien kanssa. Kuvassa kerrotaan osallistujien eri rooleista hyökkääjinä ja puolustajina. Tästä voi saada virheellisen kuvan, että vastakkaiset toiminnot tapahtuivat yhtäaikaisesti, mutta käytännön toteutus osoittautui kuitenkin turhan hankalaksi, eikä yhtäaikaisuutta vielä sellaisenaan toteutettu.

7.1.2.5 Esimerkkikalvoja harjoituksesta

Seuraavassa esitämme muutamia otteita harjoituksessa käytetyistä kalvoista, joiden avulla mm. käytettäviä työkaluja esiteltiin, harjoituksen kulkua jäsennettiin ja pohdittiin yhdessä soveltuvaa suojautumista tiettyjä hyökkäyksiä vastaan.

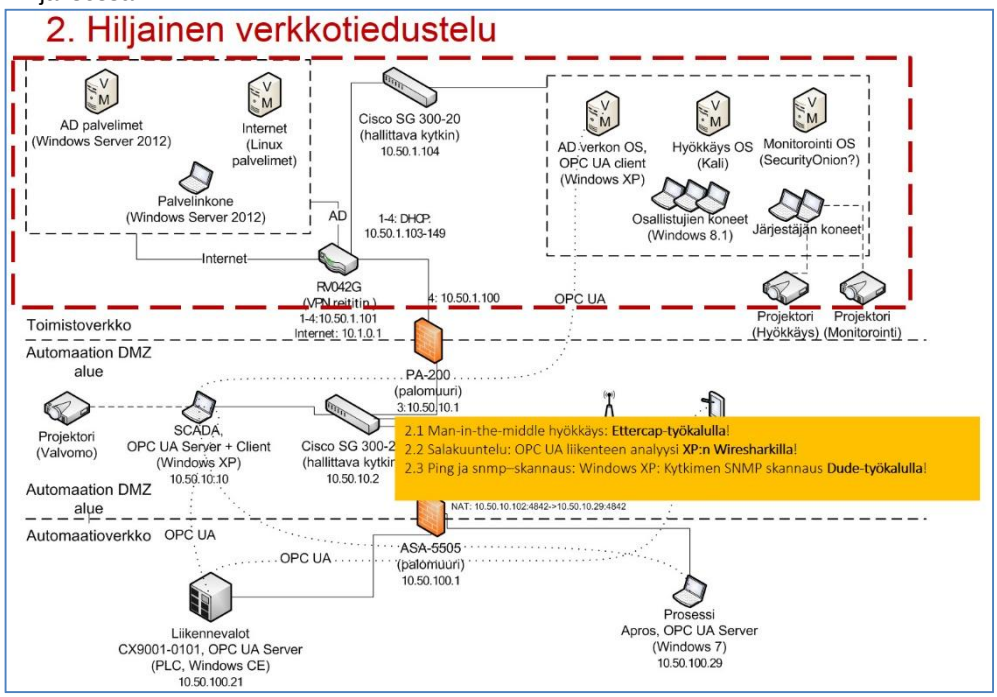
Hiljaisen verkkotiedustelun työkaluesimerkkejä
Ettercap - Man-in-the-Middle

Mahdollistaa kohdekoneiden ARP-viestien väärentämisen:

- Asettuu kohdekoneiden väliin ja mahdollistaa täten erilaiset hyökkäykset
- Tukee useita protokollia, myös salattuja
- Mahdollistaa verkon ja kohteiden tarkemman analyysin
- Eri moodeja:
  - ✓ IP-pohjainen: Lähde- ja kohde IP-osoitteiden pakettien filtteröinti
  - ✓ MAC-pohjainen: MAC osoitteen mukainen pakettien filtteröinti (yhdyskäytävien yhteydet!)
  - ✓ ARP-pohjainen: ARP:n saastuttaminen kahdelta kohdekoneelta
  - ✓ PublicARP-pohjainen: ARP:n saastuttaminen yhdeltä kohdekoneelta

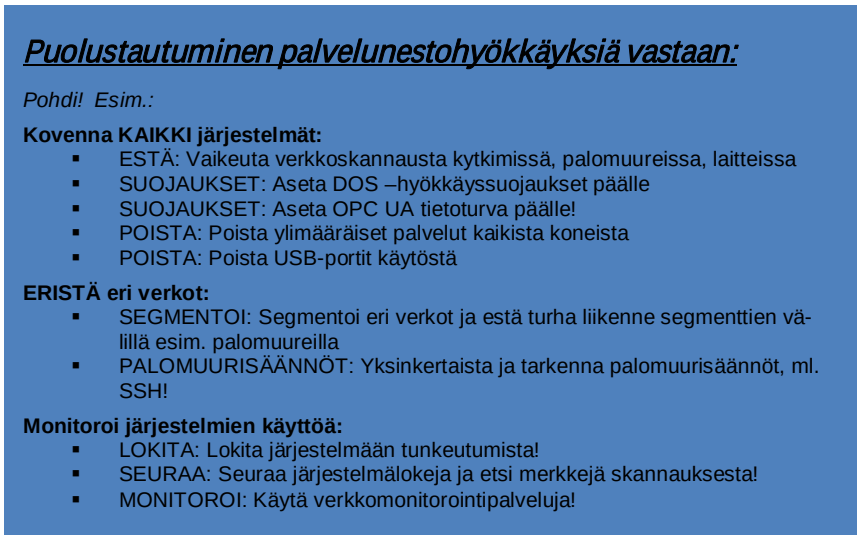
Kuva 17. Esimerkki hiljaisen verkkotiedustelun työkalusta.

Kuvassa 17 on esimerkkikalvo verkkotiedusteluun käytetyn työkalun esittelystä. Kuvassa 18 näkyy harjoituksen kulun jäsentelyä hiljaisen verkkotiedustelun harjoitusjaksossa.



Kuva 18. Hiljaisen verkkotiedustelutoiminnan sijainti (katkoviivoitus) harjoituksen arkkitehtuurissa.

Seuraavassa kuvassa on esimerkkikalvo palvelunestohyökkäyksiä vastaan puolustautumisen pohdinnasta.



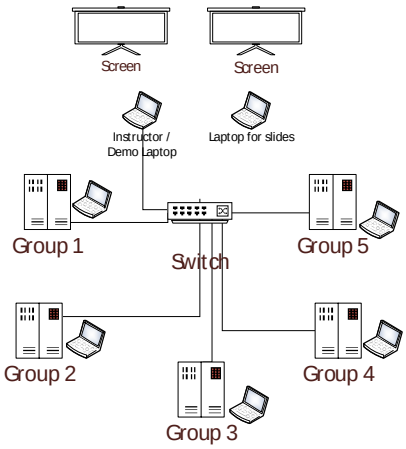
Kuva 19. Puolustautuminen palvelunestohyökkäyksiä vastaan.

7.1.3 ABB Drivesille räätälöity kyberharjoitustyöpaja

Tässä kohdassa esittelemme lyhyen yhteenvedon kyberharjoitustyöpajasta, jonka toteutimme kesäkuussa 2016 noin 20:lle ABB Drivesin insinöörille ja asiantuntijalle. Harjoituksen tavoitteena oli toteuttaa ABB Drivesin eri osastojen henkilöstölle käytännön kyberharjoittelua.

Työpajassa käytiin läpi kuusi skenaariota, joissa erilaisia ABB:n laitteita koestettiin soveltuvilla kyberturvallisuuden testityökaluilla. Skenaarioihin kuului yleensä skenaarion esittely, osallistujien omia harjoituksia sekä yhteistä keskustelua, jolla pyrittiin mm. oman työn kyberturvallisuuden kehittämiseen. Joissain skenaarioissa käytimme VTT:n testauksessa jo edellisenä vuonna löydettyjä haavoittuvuuksia, jotka oli uusiin tuotteisiin jo asiallisesti korjattu. Tällöin harjoituksessa käytettiin vanhaa, haavoittuvaista versiota testikohteesta. Esittelimme kuitenkin myös uusia haavoittuvuuksia, jotka olimme löytäneet testikohteesta vuonna 2016.

Osallistujat jaettiin viiteen ryhmään, joilla kaikilla oli sama järjestelmäkokoonpano käytettävissään. Testiympäristöön kuuluivat mm. toimiva ABB Drives -taajuusmuuttaja ja testi-PC tarvittavine testityökaluineen ja verkkoyhteyksineen. Verkkokytkentöjä vaihdettiin skenaarioiden välillä; osa harjoituksista tehtiin ainoastaan ryhmän sisäisillä yhteyksillä, kun taas joissain skenaarioissa kaikkien ryhmien verkot liitettiin yhteen.



Kuva 20. ABB Drives -harjoituksen verkkokokoonpano.

Ensimmäinen skenaario käsitteli hyökkääjän ajatusmaailmaan tutustumista kohdistuen lähinnä verkkokytkimeen/yhdyskäytävälaitteeseen. Aluksi tutustuttiin porttiskannauksen perusteisiin ja web-sovelluksiin kohdistuviin hyökkäyksiin. Sitten käytettiin Wireshark-työkalua verkkoliikenteen nauhoittamiseen ja laitekommunikaation yksityiskohtaisempaan tutkintaan. Verkkoliikenteen analyysiä hyödyntämällä voitiin lopuksi selvittää uhrin salasana *brute-force* (väsytys) -hyökkäyksen keinoin.

Toisessa skenaariossa VTT demonstroi ”mies välissä” (*man-in-the-middle*) -hyökkäystä HMI:n ja PLC:n väliselle dataliikenteelle. Käytimme kahta erilaista lähestymistapaa: PLC:n Ethernet-liikenteen salakuuntelua ja PLC:n verkkosegmentin tietoliikenteen häirintää ARP-liikennettä myrkyttämällä (*ARP poisoning*). Hyökkääjällä oli siis oltava fyysinen pääsy teollisuusautomaatioverkkoon ja ylimääräinen laite lisättynä tuohon verkkoon. Tässä demonstraatiossa käytimme hyökkääjän sulautettuna laitteena Raspberry Pi -alustaa (lisätyin Ethernet-liitynnöin). Olimme toteuttaneet alustaan skriptejä, joiden avulla demonstroimme taajuusmuuttajan kierrosluvun muuttamista ja pysäyttämistä.

Kuva 21. ABB Drives -kyberharjoitustyöpaja. VTT:n Pasi Keski-Korsun vuoro alustaa harjoitusta.

Kolmannessa skenaariossa VTT demonstroi hyökkäyksiä langattoman Bluetooth-verkon kautta. Hyökkäyksessä luotiin todentamattomia langattomia yhteyksiä, joiden avulla estettiin muita käyttämästä laitteen Bluetooth-rajapintaa. Demonstraatio toteutettiin käyttämällä vanhaa testikohdetta, sillä nykyisistä versioista haavoittuvuudet on jo korjattu.

Neljännessä ja viidennessä skenaariossa hyökkäyksen kohteena oli taajuusmuuttajan tietoliikenne-moduuli, jota kuormitettiin lähettämällä siihen uudelleen ja uudelleen virheellisiä tietoliikennepaketteja. Laitteen toimintakykyä heikennettiin kontrolloidusti VTT Cyber War roomissa aiemmin toimiviksi todettuja fuzz-testejä hyödyntäen. Testikohteen erilaisia järjestelmäversioita koeteltiin, jotta ryhmissä voitiin havaita vanhojen versioiden olevan haavoittuvia palvelunestohyökkäyksille, kun taas uudet versiot kestivät niitä hyvin.

Kuudes skenaario demonstroi verifioimattoman USB-laitteen tietokoneeseen liittämisen vaaroista. Toteutetussa harjoituksessa kohteena olleeseen tietokoneeseen oli asennettu ABB *Start-up tool* -ohjelmisto, joka oli yhdistetty taajuusmuuttajaan. Hyökkääjän laitteena käytettiin *Hak5* -yrityksen tuotetta USB Rubber Ducky, joka näyttää isolta USB-muistikulta. Todellisuudessa Rubber Ducky emuloikin näppäimistöä, jolla voi antaa kohdekoneelle Windows-komentorivikomentoja.

Työpajan lopuksi osallistujat saivat vapaasti kokeilla Kali Linuxin työkaluja käytössä oleviin testikohteisiin (30 minuuttia).

Osallistujien palaute

Positiiviset:

- Tällaisia harjoituksia pitäisi saada lisää.
- Omin käsin -harjoitukset ja demot olivat mielenkiintoisia.
- Sisältö oli mielenkiintoinen.
- Hyvä/keskimääräinen johdatus hyökkääjän asenteeseen.
- Hyvin organisoitu työpaja. Oli hienoa päästä tutustumaan Kali Linuxiin ja sen työkaluihin.

Negatiiviset:

- Joidenkin demojen idea oli vaikeasti hahmotettavissa. Tuolloin oli epäselvää, miten skenaariot liittyivät isompaan kokonaisuuteen.
- Joidenkin skenaarioiden haavoittuvuudet olivat vanhoja, joten jotkut osallistujat olivat niistä jo tietoisia.
- Kali Linux -osuuden (vapaan kokeilun) ohjeistus olisi voinut olla parempi.

7.1.4 Kyberharjoittelu-osuuden yhteenveto

Hankekokonaisuudessa kehitettiin ja toteutettiin käytännössä seuraavan tyyppiset kyberharjoitukset:

- Hyökkäys & Suojautuminen -harjoitus 2.12.2015
- Asiakaskohtainen (ABB Drives) -harjoitus 22.6.2016
- Hyökkäyksen tunnistus ja suojautuminen -harjoitus 10.–11.11.2016

Tärkeimpiä kyberharjoittelun onnistumiseen liittyviä asioita ovat mm. seuraavat:

- Harjoituksen järjestäjän tulisi olla ammattitaitoinen, puolueeton ja luotettava.
- Harjoitteluympäristön tulisi olla siirrettävä, jolloin harjoitus voidaan pitää myös asiakkaan tiloissa.
- Tehokkain harjoitusvaikutus voitaneen saavuttaa, mikäli käytetään asiakkaan omaa järjestelmää harjoituskohteena (asiakaskohtainen räätälöitävyys). Tämä edellyttää kuitenkin erityisen suurta luottamusta harjoituksen järjestäjää kohtaan.
- Riittävä valmistautuminen harjoitukseen.

7.2 Koulutus

Viimeisien vuosien aikana on mediassa ja lehdistössä puhuttu paljon siitä, ettei Suomessa ole riittävästi tietoturva-ammattilaisia kattamaan kyberturvallisen Suomen tarpeita. Kriittisen infrastruktuurin näkökulmasta ongelma ei ole tietoturva-ammattilaisten määrä vaan automaatiojärjestelmiä ja tietoturvaa ymmärtävien ammattilaisten vähäisyys. Ongelma ei ole vain kansallinen, mutta korostuu Suomen kokoisessa valtiossa.

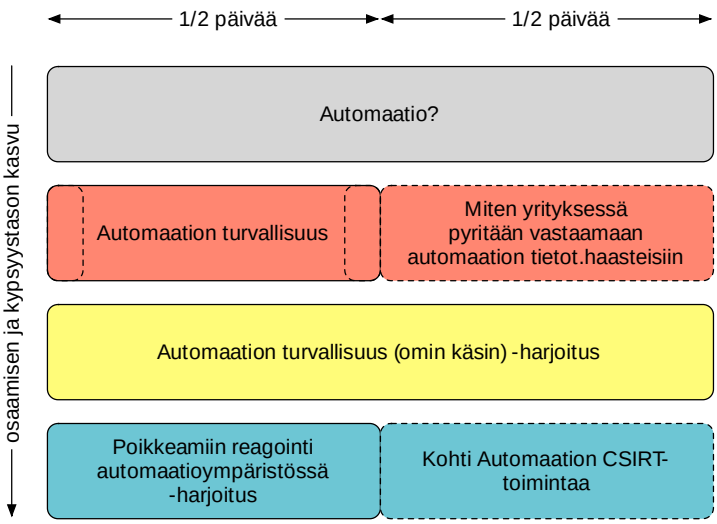
Automaation tietoturvatyötä on Suomessa tehty yli 17 vuotta. Pitkä kokemus on osoittanut, että on helpompaa jatkokouluttaa automaatioammattilaisesta riittävän tietoturvaosaamisen ammattilainen kuin toisinpäin. Automaatiojärjestelmät ovat eri suuruisia viiveitä sisältäviä reaaliaikajärjestelmiä, joilla on rajapinta fyysiseen maailmaan. Automaation toiminnallisuuden taustalla olevasta säätö- ja mittaustekniikasta johtuen on erittäin tärkeä kaikessa toiminnassa ymmärtää niiden tuomat rajoitteet. Automaatiotekniikan koulutus opettaa ajattelemaan nämä rajoitteet huomioon ottaen. Tietoturvakoulutuksessa maailma on enemmän internet- ja toimistoverkkolähtöistä ja rajapinnat fyysiseen maailmaan usein unohtuvat – tämä on siis toisenlainen tapa ajatella tekniikkaa.

Kokemus on myös osoittanut, että kriittisen infrastruktuurin kannalta paras yhdistelmä on riittävällä tietoturvaosaamisella varustetun automaatioammattilaisen ja riittävällä automaatio-osaamisella varustetun tietoturva-ammattilaisen yhdistelmä. Tämän aikaansaaminen tulee olla koulutuksen tavoitteena, jotta kyberturvallisuusharjoittelua on mielekästä tehdä. Riittävä pohjakoulutus on siis järkevän harjoittelun edellytys kriittistä infrastruktuuria ohjaavan automaation tapauksessa.

KYBER-TEO-hanketta edeltävän työn pohjalta KYBER-TEO-hankkeessa on Tampereen teknillisellä yliopistolla toteutettu koulutuskokonaisuus, jonka avulla saadaan taustasta riippumatta riittävää automaatio- ja tietoturvaosaaminen automaatiojärjestelmien parissa työskenteleville. Koulutus koostuu seuraavista moduuleista:

- **Automaatio.** 1 päivän mittainen kokonaisuus, jonka tavoitteena on antaa riittävä perustietämys automaatiosta, jotta pystyy toimimaan automaatioon liittyvissä tehtävissä. Kokonaisuus sopii esimerkiksi automaation pariin muilta aloilta työllistyneet, joiden erikoisosaamisalue on esimerkiksi ohjelmisto, tietoliikenne tai tietoturva.
- **Automaation turvallisuus.** 1/2 päivää. Tavoitteena on antaa riittävä perustuntemus automaation tietoturvan erityispiirteistä. Antaa ymmärrys, miten tietoturvatyökaluja voidaan käyttää luotettavan automaation aikaansaamiseksi. Kohdeyleisönä kaikki automaation parissa työskentelevät kuten automaatioyritysten johto, alihankkijat, kumppanit, tekniset ja kaupalliset henkilöt sekä sidosryhmät.
- **Yrityksen omat käytännöt**. 1/2 päivää. Yhdessä räätälöity kokonaisuus, jonka tavoitteena tuoda esiin, miten yrityksen toimintatavat, ohjeistus, dokumentaatio ja sopimukset pyrkivät vastaamaan Automaation turvallisuus-moduulin esiintuomiin haasteisiin. Kohdeyleisönä yrityksen oma henkilökunta sekä valitut yhteistyökumppanit.

- **Automaation turvallisuus (omin käsin) -harjoitus**. 1 päivän mittainen kokonaisuus, jossa luodaan ymmärrys murtautumisprosessiin; opetellaan keräämään verkosta ja järjestelmistä tietoa ja ymmärtämään mikä on kerätyn tiedon merkitys osana hyökkäyksiä; sekä luodaan ymmärrys työkalujen ja kerätyn tiedon merkityksestä automaatiojärjestelmän tietoturvan parantamisessa. Kohdeyleisö sama kuin Automaation turvallisuus-moduulissa.
- **Poikkeamiin reagoiminen automaatioympäristössä -harjoitus.** 1/2 päivän mittainen harjoitus, jossa yrityksen kanssa suunniteltujen esimerkkitapausten avulla kehitetään yrityksen automaatio-organisaatiolle sopiva tapa käsitellä tietoturvapoikkeamia osana normaalia automaation poikkeamahallintaa. Harjoituksen aikana käsitellään mm. vastuita, osaajia, toteuttajia, viestintää ja sopimuksia. Kohderyhmänä yrityksen oma henkilökunta sekä valitut yhteistyökumppanit.
    - **Kohti automaatioympäristön poikkeamahallintaryhmää.** 1/2 päivän valinnainen osuus. Aloitetaan tietoturvapoikkeamiin reagoivan ryhmän luominen, automaatio(CS)IRT. Tavoitteena esimerkiksi Security-Operations-Center (SOC) -palvelun käyttöönottoon valmistautuminen yhdessä SOC-palvelutoimittajan kanssa. Kohderyhmänä yrityksen oma henkilökunta sekä esimerkiksi valittu palvelutoimittaja.



Kuva 22. Koulutuskokonaisuus. Katkoviivalla on havainnollistettu valinnaisia osuuksia sekä osittaista sisältöjen päällekkäisyyttä. Moduulien sisällöt on suunniteltu sovitettavaksi yrityksen toimialaan sekä ennakkokeskusteluiden perusteella esitettyyn tarpeeseen.

Edellä mainittujen moduulien avulla on mahdollista rakentaa riittävä osaamis- ja kypsyystaso kehittyneempien kyberturvallisuuspalveluiden käyttöönottoon. Koulu-

tustarjontaa arvioidessa on hyvä tunnistaa, onko kouluttajilla itsellään riittävä osaaminen sekä automaatiosta että tietoturvasta. Paras lopputulos saavutetaan, ei vain kouluttamalla, vaan luomalla yhdessä osaamista yrityksen henkilökunnalle. Tämä vaatii kykyä toimia automaatio-IT-rajapinnassa, usein myös diplomaattisia kykyjä koulutusten aikana syntyvän keskustelun hallinnassa sekä tulkkausta eri erikois-osaamisalueiden terminologian yhteentörmäyksissä. Osa tietoturvaa kouluttavista toimijoista on jo tunnistanut tämän osaamistarpeen, osa ei. Samalla tavalla osa automaatiotoimijoista on tunnistanut tämän tarpeen, osa ei. Riittävä kypsyystaso kehittyneempien palveluiden käyttöönottoon saavutetaankin erikoisosaamisalueiden yhteistyöllä.

8. Testaus – Ympäristöt, menetelmät, työkalut, automaatio

Stuxnetista tiedottamisen jälkeen vuonna 2010 automaation tietoturvahaavoittuvuudet ja järjestelmien testaaminen alkoivat yhtäkkiä kiinnostaa teollisuuden toimijoita kansainvälisesti. Loppuasiakkaat ovat vähitellen alkaneet kysellä automaation järjestelmävalmistajilta kyberturvallisuuden testiraportteja, sertifikaatteja tai muita todisteita asianmukaisesta kyberturvallisuuden varmistamisesta. Kyberturvalliseksi todennettuja järjestelmiä on kuitenkin ollut vain vähän saatavilla, tai ne ovat olleet hyvin kalliita.

Tilanne on onneksi vähitellen edennyt oikeaan suuntaan, sillä tänä päivänä suurin osa automaatiojärjestelmätoimittajista ja konevalmistajista tehnee tuotteilleen vähintään kertaluonteista tietoturvatestausta. Tämä ei kuitenkaan riitä. Tietoturvatestauksen varsinainen kysyntä on pitkään ollut Suomen ulkopuolella, mutta viime vuosina tämän tärkeän osa-alueen kysyntä on kasvanut myös kotimaassa. Kannattaa hyödyntää sitä tosiasiaa, että Suomessa on tarjolla sekä osaavaa automaatiokehitystä että luotettavia ja kehittyviä kyberturvallisuuspalvelujen tarjoajia.

8.1 Automaation kyberturvallisuustestauksesta

Jo kyberturvallisuuden testaussuunnitelmaa laadittaessa kannattaa tehdä liiketoimintavaikutusten analyysi, jotta ymmärretään mitä kannattaa ensisijaisesti parantaa. Ennen itse kyberturvallisuustestauksen aloittamista olisi tärkeää tehdä myös uhkamallinnus ja esim. arkkitehtuurianalyysi, jotta ymmärretään, mikä on kriittistä testattavaa. Tämä auttanee myös testien tuloksena saatavien havaintojen priorisoinnissa. Esimerkiksi Microsoftin STRIDE tai vastaava uhkamallinnus voi olla toimiva menetelmä. Standardit, kuten IEC 62443-3-3/-4-2, eivät ole missään mielessä täydellisiä, mutta osoittavat eräitä hyviä lähtökohtia testaukselle. Oma malli turvalliselle ohjelmistokehitykselle on kuitenkin erittäin oleellista määrittää koko elinkaaren ajalle.

8.1.1 Testauksen edellytyksiä

Tietoturvatestauksen päätavoite on useimmiten, että kaikki toimitettavat automaatiojärjestelmät ja tukijärjestelmät saadaan jo kehitysvaiheessa korjattua riittävän kyberturvallisiksi. Niihin ei saisi jäädä vikoja tai haavoittuvuuksia joita voisi myöhemmin hyväksikäyttää. Tämä edellyttää järjestelmätoimittajien ja testaajien yhteistoimintaa, mm. seuraavien asioiden selvittämistä ja kehittämistä:

- TOIMINNALLISUUS: Testikohteen oikean toiminnan mahdollisimman tarkkaa tuntemusta ennen testausta, ml. automaatiotoiminnot
- TESTIKATTAVUUS: Realistisen testikattavuuden selvittämistä ja testauksen jakamista esim. erityyppisiin jaksoihin, jotta ainakin kriittisimmät toiminnot saataisiin testattua kunnolla
- TESTAUKSEN LAATU: Riittävää ajan allokointia, ko. kohteen tehokkaimpien testityökalujen ja -menetelmien selvittämistä ja osaamisen kehittämistä
- TESTAUKSEN SYVYYS: Riittävää perehtymistä ja fokusoitua ajankäyttöä testikohteen ongelmakohtiin pureutumiseksi soveltuvien testimenetelmien ja -työkalujen avulla
- ERI ALUSTOJEN JA INTEGROINTIEN VAIKUTUS: Testaajien tulisi ymmärtää testikohteen erilaiset käyttökohteet ja ympäristöt joihin se tullaan asentamaan. Tämä antaa usein viitteitä piilevistä mutta kriittisistä rajapinnoista ja toiminnallisuudesta.

Automaatiojärjestelmä (tai henkilöstö) ei saa myöskään paljastaa liikaa järjestelmätietoa hyökkääjälle, jotta hyökkääminen olisi mahdollisimman hankalaa. Jo järjestelmäsuunnittelussa olisi otettava mahdollinen hyökkääjä huomioon, kun määritellään mm. järjestelmätietojen ja vikakoodien sisällyttämistä järjestelmäkyselyjen vastauksiin, ja miten järjestelmä vastaa erilaisiin porttikyselyihin. Hyökkääjän tulisi olla vaikea selvittää mitä portteja käytetään mihinkin automaatiotoimintoon.

8.1.2 Testauksen haasteita

Automaation kyberturvallisuustestauksen perinteet ja käytännöt ovat vasta kehitteillä. Tunnistamiamme automaation kyberturvatestaamisen haasteita on listattu alla:

- Kyberturvallisuustestaus vaatisi automaatiokehitykseen tottuneelta normaalista poikkeavia työkaluja ja menetelmiä
    - ASENNE: Hyökkääjän mentaliteetin ja toimintatapojen perusteiden omaksuminen?
    - MENETELMÄT: Verkkokartoitus, haavoittuvuusanalyysi, fuzzaus, penetraatio, palvelunesto, sitkeys jne.?
    - OSAAMINEN: Kyberturvatestauksen käytännön osaamista puuttuu?
    - TYÖKALUT: Miten löytää ja valita tehokkaat työkalut? Satoja eri testityökaluja saatavilla ilmaiseksi

- LUOTETTAVUUS: Miten validoida esim. *open source* -testityökalujen luotettavuus? Luotatko kehitysyhteisöjen kaikkiin jäseniin, keitä he ovat?
- MÄÄRÄ: Mistä testaaja tietää, onko riittävä testikattavuus ja -syvyys saavutettu?

Automaatiokehittäjällä on kuitenkin myös etuja puolellaan. Koska hän ymmärtää testikohteen sisäisen toiminnan, hän pystyy tarvittaessa ohjaamaan passiivisen tai suljetun järjestelmän testaajia järkevään suuntaan, jotta testaus etenisi. Useimmiten on valtava salapoliisityö selvittää järjestelmän sisäinen viestitys ja toiminta ilman järjestelmän asiantuntijan konsultaatiota. Esimerkiksi jos jokin portti ei vastaa tiettyyn kyselyyn, se voi silti olla toiminnassa ja toimia oikein, mutta testaaja ei tiedä tätä.

Automaatiojärjestelmien kohdalla kyberturvallisuustestaajakaan ei siis ole vahvoilla ilman kehittäjän apua. Tällainen yhteistoiminta edellyttää kuitenkin suurta luottamusta, varsinkin automaatiokehittäjän luottamusta testaajiin. Yhteistoimintaa kuitenkin tarvitaan, mutta miten kattavaan kyberturvallisuustestaamiseen tarvittava luottamus ja osaamisen riittävä jakaminen saavutetaan? Pitkään se on kuitenkin ollut mahdotonta. Automaatiokehittäjien ja kyberturvallisuustestaajien tulisi toimia luottamuksellisessa yhteistyössä, jotta automaatiojärjestelmistä voitaisiin kehittää entistä kyberturvallisempia.

8.1.3 Testaajan luotettavuus

Testaajan luotettavuus on erittäin tärkeä mutta samalla erittäin vaikea kysymys. Tilaajan täytyy itse arvioida, keneen luottaa ja kelle antaa järjestelmänsä mahdollisine suunnittelutietoineen testattavaksi. Luottamus tiettyyn yritykseen vaihtelee tietysti maittain, koska kullakin maalla voi olla mm. omat tiedustelupalvelunsa ja erilaiset tiedustelu- ja yksityisyyslait. Miten eri testaajien luotettavuutta voisi arvioida Suomessa, jossa on pitkään ollut verrattain vahva lain suoja myös verkossa tarjottavien palvelujen yksityisyydelle?

Testaajan luotettavuutta voi yrittää arvioida mm. seuraavilla tavoilla:

- perusmuotoisen turvallisuusselvityksen vaatiminen
- vahvan ja pitkäkestoisen salassapitosopimuksen edellyttäminen
- eettisen hakkeroinnin koulutuksen tai vastaavan edellyttäminen testaajilta
- testaajan esittämien referenssien tarkistaminen alkuperäisistä lähteistä
- turvallisuuden arviointi aiemman yhteistyön perusteella

Toimijoiden välinen luottamus kasvaa vähittäisen yhteistyön lisäämisen kautta. Käytännössä tämä voi kestää jopa useita vuosia ja sisältää erilaisia yhteistyön muotoja ja esim. yhteishankkeita, joissa yhteisiä tehtäviä voidaan vähitellen lisätä luottamuksen lisääntyessä. Usein luottamus on henkilökohtaista ja toisaalta se voidaan myös menettää hetkessä. Soluttautuminen on luku sinänsä, joten asetettaessa kotimaistenkin toimijoiden ja palvelujen luotettavuus etusijalla, niidenkin ”toiminnan eheyttä” tulisi arvioida jatkuvasti.

Tietoturvallisuustestaajien osaamisvaatimuksia on myös aloitettu luonnostelemaan erilaisissa yhteyksissä, ks. esim. [CD19896-1]. Niiden onnistumisesta ei kuitenkaan ole vielä takeita.

8.1.4 Lyhyesti soveltuvista testimenetelmistä

Kyberturvallisuustestaus ja siihen liittyvät palvelut ovat kehittyneet viime vuosina hyvin nopeasti. Saatavilla on sekä ilmaisia että kaupallisia työkaluja ja palveluja, joita käyttämällä voidaan soveltuvin osin toteuttaa myös automaatiojärjestelmien kyberturvallisuuden testausta. Vaikka soveltuvimpien testityökalujen valinta onkin yksi tärkeimmistä menestystekijöistä, emme halua tässä julkisessa julkaisussa antaa suosituksia yksittäisistä työkaluista. Sen sijaan kehotamme lukijaa kääntymään suoraan asiantuntevien testaajien ja kehittäjien puoleen.

Alla on kuitenkin lyhyt katsaus ja joitain jalkautusohjeita automaation kyberturvallisuuden relevantteihin testimenetelmiin.

Lähdekoodianalyysissä lähdekoodista tunnistetaan heikkoja kohtia, esim. haavoittuvia komentoja, jolloin niiden määrää voidaan vähentää radikaalisti jo ohjelmointivaiheessa:

- Jalkauta turvalliset ohjelmistosuunnitteluprosessit ja ohjelmointisäännöt (ks. esim. SEI CERTin koodausstandardit [SEI CERT]), jotka luovat perustan virheettömän ohjelmiston tuotannolle:
    - Koko T&K-ympäristö tulee suojata sekä teknisesti että toimintaohjein. Esim. työasemaa ei saa käyttää harrastuksiin (tuo paljon uhkia).
    - Automaatio-ohjelmoijat tulee kouluttaa käyttämään turvallisia ohjelmistokirjastoja ja suojautumaan mm. luvattomalta urkinnalta.
- Automaatiosovelluksen lähdekoodi kannattaa lisäksi analysoida automaattisesti jo käännösvaiheessa. Soveltuva koodianalysaattori tulee asentaa kehitysympäristöön.

Fuzz-testauksessa kohderajapintaan lähetetään normaalista poikkeavia syötteitä:

- Testikohdetta vastaavan tietoliikennerajapinnan verkkoliikennettä on nauhoitettu ja mallinnettu, jotta tunnetaan sallitut syötteet. Testauksessa tätä syötettä varioidaan ja pusketaan testikohteen rajapintaan samalla tarkkaillen kohteen käyttäytymistä ja mahdollisia vastauksena saatavia viestejä. Testikohteen poikkeava käytös kirjautuu useissa työkaluissa automaattisesti testiraporttiin.

- Automaation ohjelmointivirheiden havaitsemisessa useimmiten erittäin tehokas menetelmä. Soveltuu hyvin myös 0-päivähaavoittuvuuksien tunnistamiseen sekä jopa palvelunestohyökkäysten testaamiseen.
- Tehokkainta fuzz-testaus on, mikäli voidaan käyttää ns. protokollatesteriä joka on erityisesti kehitetty testikohteen tukemalle automaatioprotokollalle. Haittapuolena saattaa olla tällaisen räätälöidyn työkalun kalleus, mutta sitä vastaavan testauspalvelun kokeilemista suositellaan, mikäli se on saatavilla ja turvallista.

Porttiskannauksessa & verkkotiedustelussa tietoverkkoa ja siinä olevia laitteita ja näiden avoimia tietoliikenneportteja etsitään ja löytyneet dokumentoidaan:
- Automaatiotoimittajan tulisi tutkia porttiskannauksella, mitä tietoliikennepalveluja (portteja) toimitettavan automaatioverkon järjestelmissä on avoimena, joten tämä menetelmä soveltuu hyvin kovennuksen testaamiseen. Jos palvelu (portti) ei vastaa tietyssä ajassa, testeri yleensä olettaa portin olevan poissa käytöstä. Automaatiojärjestelmiä testattaessa skannaavat testityökalut eivät välttämättä löydä kaikkia käytössä olevia palveluja vakioasetuksilla, koska tietoliikenneportteja voidaan käyttää eri tavalla kuin tavallisessa Ethernet-liikenteessä. Työkalun oikeita asetuksia on siis vaikea löytää ilman kohteena olevan automaatiojärjestelmän hyvää tuntemusta. Tuotantoverkossa on aina ruuhkautumisen vaara, jos sitä skannataan.
- Verkkotiedustelussa kuunnellaan passiivisesti verkossa kulkevaa liikennettä tai lähetetään aktiivisesti kyselyjä verkossa olevien laitteiden selvittämiseksi. Näin tunnistetaan automaatioverkkoon kuuluvat ja mahdollisesti sinne kuulumattomat palvelut. Vastaavia menetelmiä saatetaan käyttää myös tehdasverkkojen oikean toiminnan seurantaan, mutta vasta huolellisen suunnittelun ja riskianalyysin jälkeen.

Haavoittuvuusskannauksessa verkosta ja sen laitteista etsitään lähinnä ohjelmistohaavoittuvuuksia:
- Haavoittuvuusskannerit tutkivat automaattisesti verkossa olevien järjestelmien ohjelmistoversioita lähettämällä yksinkertaisia viestejä kohdejärjestelmien tietoliikennerajapintoihin. Haavoittuvat järjestelmät löytyvät, kun työkalu vertaa verkosta tulleita vastauksia tunnettuihin haavoittuviin versionumeroihin. Automaatiossa käytetään edelleen usein päivittämättömiä versioita, joten haavoittuvuuksista tiedetään ilman skannaustakin.
- Nykyään jotkin haavoittuvuusskannerit voivat automaattisesti hyväksikäyttää haavoittuvuuksia, joten vahinkojen välttämiseksi myös näiden työkalujen käytön ja asetusten kanssa tulee olla tarkkana automaatiota testattaessa.

Penetraatiotestauksessa kohdejärjestelmään yritetään tunkeutua kaikenlaisin menetelmin ja työkaluin:
- Tässä testausmuodossa kaikki kohteen murtamisen keinot voivat olla käytössä. Hyökkäystyökaluja on lukuisia. Usein myös sosiaalisen tiedustelun keinot luetaan penetraatiotestauksen piiriin, jolloin ihmisten käytöstäkin voidaan

koetella kohteen hyökkäyskestävyyden testaamiseksi. Testattavana saattaa olla myös automatisoituun tuotantoon liittyvät palvelut, ja ihmisethän niidenkin toimintaa viimekädessä ohjaavat. Jos väärä henkilö päästetään muutamaksi sekunniksi automaatiotilaan, saattaa hyökkääjän takaportti heti tämän jälkeen olla asennettu.

- Automaatiojärjestelmiä kannattaa testata suljetussa testiympäristössä. Tämä mahdollistaa turvallisen ja monipuolisen testimenetelmien käytön, sekä testiautomaation kehittämisen. Automatisoidut hyökkäystyökalut voivat olla niin helppokäyttöisiä, että niillä saa hyvin nopeasti vahinkoja aikaan pienellä huolimattomuudella.

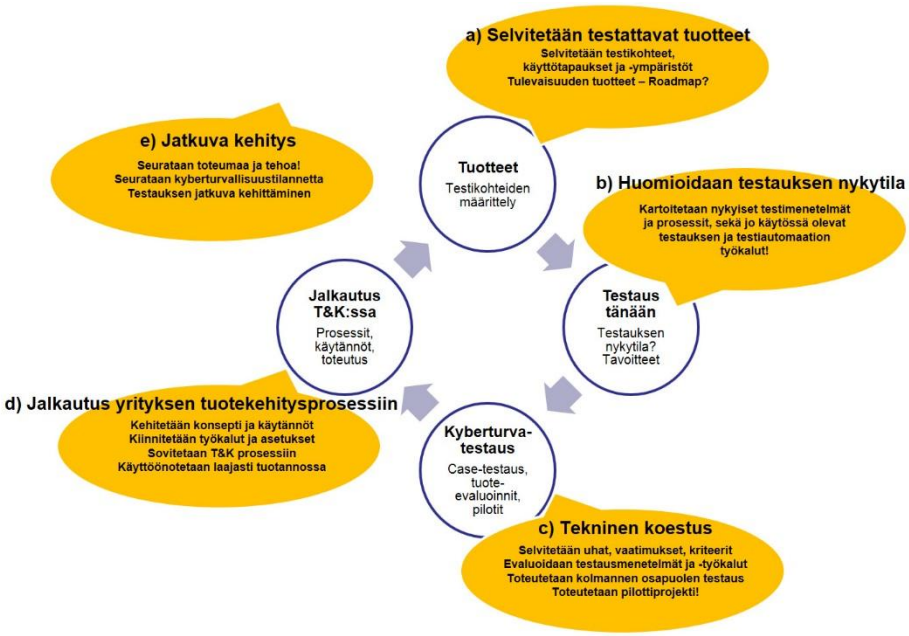
Seuraavassa kuvassa on vielä lyhyt yhteenveto automaation testaukseen soveltuvista kyberturvallisuuden testausmenetelmistä.

Testi-menetelmä	Käyttötarve	Käyttökohde	Käyttöajankohta
Lähdekoodi-analyysi	Riskialttiiden koodin osien tunnistaminen	Kaikki tilattu ohjelmakoodi	SW-kehitys & vika-korjaukset (jatkuva)
Fuzz-testaus	Virheellisen toteutuksen tunnistaminen	Tietoliikenne-rajapinnat: käyttöjärjestelmät, protokollat, sovellukset	SW-kehityksen testausvaiheet
Porttiskannaus & verkko-tiedustelu	Ylimääräisten verkkotoiminteiden tunnistaminen	Tietoliikenneverkon konfiguraatio	Hyväksymistestaus, käyttöönottotestaus, testauksen esisel-vitysvaihe
Haavoittuvuus-skannaus	Tunnettujen haavoittuvuuksien tunnistaminen	Ohjelmistojen versiot	Hyväksymistestaus, käyttöönottotestaus, testauksen esiselvitysvaihe
Penetraatio-testaus	Tietoturva-aukkojen tunnistaminen ja mahdollinen hyödyntäminen	Pääsynvalvonnan toteutus	Hyväksymistestaus, käyttöönottotestaus

Kuva 23. Automaatioon soveltuvia kyberturvallisuuden testausmenetelmiä.

8.2 Tietoturvatestauksen kehittämisen prosessi

Tietoturvatestausta toteuttaessamme olemme samalla tulleet kehittäneeksi prosessin, jolla automaation kyberturvallisuustestausta voisi jalkauttaa yrityksiin. Tämä prosessi on esitetty seuraavassa kuvassa.



Kuva 24. Automaation kyberturvallisuustestauksen kehittämisen prosessi.

Kehittämämme prosessimallin mukaan kyberturvallisuustestauksen jalkautus automaatiota kehittävään yritykseen koostuu viidestä päävaiheesta:

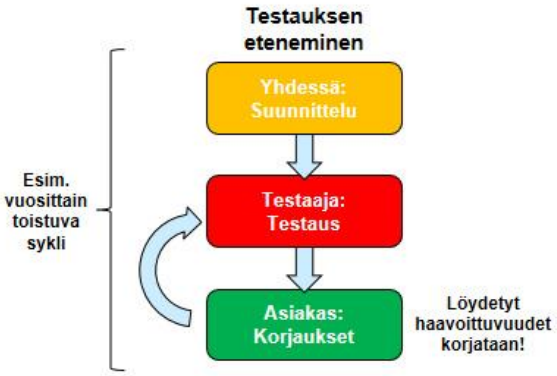
a) Selvitetään testausta vaativat tuotteet.
b) Huomioidaan testauksen nykytila.
c) Koestetaan soveltuvat testimenetelmät ja työkalut ja toteutetaan kyberturvallisuustestaus-case.
d) Jalkautetaan kybertestaus yrityksen tuotekehitysprosessiin.
e) Jatkuva kehitys.

Käytännössä näistä vaativimpia ovat vaiheet c) ja d), sillä ne edellyttävät tavallisesti eniten yhteistyötä ja osaamisen siirtoa automaatiokehittäjien ja kyberturvallisuustestauksen asiantuntijoiden välillä. Kattavan teknisen koestuksen onnistumiseksi automaatiojärjestelmän tuntemusta tulisi siirtyä riittävästi kyberturvallisuustestaajille, jotta testauksesta voitaisiin kehittää tehokasta. Kun soveltuvimmat menetelmät ja työkalut on saatu selvitettyä, onnistunut jalkautus yrityksen muihin testausprosesseihin vaatinee testikohteisiin soveltuvien kyberturvallisuustestausmenetelmien

ja -työkalujen syvää tuntemusta. Esimerkiksi testauksen automatisointi on yleensä paljon osaamista vaativa osa-alue, mutta esim. SPARTA (http://sparta.secforce.com/) voi olla testiemme mukaan yksi hyvä lähtökohta. Asiantuntijoiden välinen yhteistyö tulee jatkua yleensä pidempäänkin, jotta jalkautus saadaan toteutumaan.

8.2.1 Testauksen eteneminen – tekninen koestus

Kun automaatiotoimittaja kehittää kyberturvallisuustestausta yrityksensä automaatiojärjestelmille, tarvitaan usein ulkopuolista luottamuksellista apua. Yksinkertaistettu kaavio testauksen etenemisestä on esitetty seuraavassa kuvassa.



Kuva 25. Teknisen koestuksen eteneminen yksinkertaistettuna.

1) SUUNNITTELU: Aluksi suunnitellaan yhdessä testattavat kohteet, käyttötapaukset sekä erityisesti testauksen sisältö: millä menetelmällä ja työkalulla testaus toteutetaan ja kuinka laaja testaus tulee olemaan.
2) TESTAUS: Kyberturvallisuustestaaja suorittaa testauksen parhaan osaamisensa mukaan ja kirjoittaa tuloksista testiraportin. Usein parhaaseen tulokseen päästään, jos mukana on useita testaajia ja asiakasta voidaan konsultoida esim. testikohteen oikean käyttäytymisen suhteen testauksen alaisena.
3) KORJAUKSET: Asiakas korjaa tai korjauttaa tuotteensa testiraportin ilmoittamien löydösten mukaisesti. Tämän jälkeen korjattu tuote kannattaa uudelleen testata, jotta varmistutaan, että viat on saatu poistettua ja että korjaukset eivät sisällä uusia haavoittuvuuksia.

Lopullinen tavoite on, että asiakkaan oma tuotekehitys voisi itse testata pääosan tyypillisistä haavoittuvuuksista. Tämä edellyttää siirtymistä vaiheeseen, jossa kyberturvallisuustestausta automatisoidaan ja jalkautetaan kehittäjäyrityksen tuotekehitysprosessiin. Tämä on usein erittäin vaativaa, koska kyberturvallisuustestauksen menetelmät ja työkalut kehittyvät jatkuvasti, jolloin kehitysympäristöön integroitavat testityökalutkin todennäköisesti vaativat jatkuvia päivityksiä ja testauksia.

8.2.2 Testiraportti

Testiraportti on oleellinen osa luottamuksellista kommunikaatiota kyberturvallisuustestaajien ja kehittäjien tai asiakkaan välillä. Seuraavassa kuvassa on esitetty varhainen versio testiraporttipohjasta, joka syntyi kehittäessämme kyberturvallisuustestausta yhdessä asiakkaidemme kanssa.

<table>
<tr><td>1. Report ID</td><td colspan="2">2. Test target</td><td colspan="2">3. Testers</td></tr>
<tr><td><1, 2, 3…></td><td colspan="2"><Product ID, version>, <Vendor> or <Company>, <Location> etc.</td><td colspan="2"><Name></td></tr>
<tr><td colspan="3">4. Test name</td><td colspan="2">5. Category</td></tr>
<tr><td colspan="3"><e.g. Port scanning and fingerprinting></td><td colspan="2"><e.g. Information gathering></td></tr>
<tr><td colspan="5">6. Description and objectives</td></tr>
<tr><td colspan="5"><e.g. This test identifies the remote accessability of ports and the services running in the open ports>
<e.g. The objective is to find out if there are known vulnerable services running in open ports></td></tr>
<tr><td colspan="5">Testing tools</td></tr>
<tr><td colspan="2">7. Tool name</td><td colspan="3">8. Test scope</td></tr>
<tr><td colspan="2"><used test tool name and version></td><td colspan="3"><e.g. ports scanned, number of test cases, tested interfaces and protocols></td></tr>
<tr><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="5">Findings</td></tr>
<tr><td>9. ID</td><td>11. Severity</td><td colspan="2">12. Description</td><td>13. Evidence</td></tr>
<tr><td><1, 2, 3…></td><td><eg. Low, Medium, High, N/A></td><td colspan="2"><e.g. Vulnerable XYZ server identified on port xx></td><td><e.g. pcap-file name, screenshot, memory dump></td></tr>
<tr><td></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="5">14. Conclusions and suggestions</td></tr>
<tr><td colspan="5"><e.g.Define the achieved confidence level of reaching the objectives with the given scope>
<e.g. It is suggested that the vulnerable XYZ server is updated to the latest release>
<e.g. Additional test are needed to find the possible vulnerabilities of proprietary service running in port 34562></td></tr>
</table>

Kuva 26. Kyberturvallisuustestauksen raportointilomake.

8.2.3 Lausunto testauksesta

Joskus automaatiojärjestelmätoimittaja tarvitsee omalle asiakkaalleen lausunnon suoritetusta kyberturvallisuustestauksesta, jossa ei paljasteta löydettyjä ongelmia mutta kirjataan, mitä ja miten on testattu sekä mikä oli testauksen lopputulema (läpäistiinkö testit). Seuraavassa kuvassa on esitetty testilausuntopohja, joka myös syntyi asiakastarpeesta ja yhdessä asiakkaidemme kanssa.

Test target <Product ID, version>, <Vendor>	**Lead tester** <Name>	**Project owner** <Company>, <Name>
Orderer <Orderer details>. (Total man-hours ordered: <X> hours.)		
Description of the test target <Short overview of the test target.>		
List of tested software and hardware components:		

Vendor	**SW / HW component**	**Version**	**Purpose in product**

Test Scope: Testing of the <interfaces, protocols, other> of the components.
Test Methods: <e.g. Robustness testing with tool X>, <e.g. Penetration testing with tool Y>.
Test case volume: <e.g. Number of test cases run successfully.>
STATEMENT: ***<Approved, Approved with minor corrective actions, Approved with corrective actions, Disapproved>*** **Date:** <Date of statement.> **Signature**: _____ <Name of Approver>
Validity: Statement is only valid for the mentioned target in its tested configuration and for limited time <e.g. one year>. <Company> does not guarantee the security of any tested products, or that all security vulnerabilities are found during testing.

Kuva 27. Lausunto automaatiojärjestelmän kyberturvallisuustestauksesta.

8.3 Sertifiointi

Kyberturvallisuuden varmistamisen menettelyihin voi kuulua monenlaista sertifiointia. Esimerkiksi organisaatio tai sen tietty toiminto voidaan sertifioida, tuotannossa käytettäviä tuotteita voidaan sertifioida, tai kyberturvallisuudesta vastaava henkilö voi suorittaa erilaisia henkilösertifikaatteja. Tärkeänä esimerkkinä mainittakoon, että myös automaatiojärjestelmiä kehittävät ja hyödyntävät yritykset käyttävät ISO/IEC 27001-standardia parantaakseen omaa tietoturvallisuuden hallintajärjestelmäänsä (*Information Security Management System, ISMS*) tai sertifioidakseen vaikkapa tuotantotoimintansa 27001-standardin mukaisesti.

Kaksi tärkeää automaatiossa käytettävien järjestelmien kyberturvallisuuden sertifiointistandardia on lyhyesti esitelty seuraavaksi. IEC 62443 -sarjasta löytyvät monet muutkin relevantit automaatiojärjestelmien vaatimukset ja mallit, joten tähän standardisarjaan perehtyminen on erittäin suositeltavaa.

8.3.1 IEC 62443 – Embedded Device Security Assurance (EDSA)

Mielestämme relevantein sulautettujen järjestelmien sertifiointistandardi on "*IEC 62443 – EDSA Certification, Embedded Device Security Assurance (EDSA)"* [IEC-EDSA], jonka versio 2 tuli voimaan heinäkuussa 2016. Tämä ISASecure sertifiointi koestaa sulautetun laitteen todellisia ominaisuuksia ja sen kehittäjäyrityksen T&K-käytäntöjä kyberturvallisuuden näkökulmasta. Omien kokemustemme perusteella kyseessä on erittäin hyödyllinen standardi, jonka tutkiminen hyvin todennäköisesti auttaa parantamaan sekä tuotteen että sen kehittäjäyrityksen kyberturvallisuutta. Sertifiointi perustuu automaatiojärjestelmäkomponenttien teknisille kyberturvallisuusvaatimuksille (IEC 62443-4-2) sekä tuotekehitysvaatimuksille (IEC 62443-4-1).

Sertifioinnissa saavutettavia tasoja on kolme, *levels 1–3*. Mainittakoon, että tietoliikenteen osalta sertifikaatin edellyttämä verifiointi perustuu lähinnä *robustness*-testaukseen (CRT), joka on hyvin läheistä sukua *fuzz*-testaukselle.

8.3.2 IEC 62443 – System Security Assurance (SSA)

Toinen tärkeä sertifiointistandardi on "*IEC 62443 – SSA Certification, System Security Assurance (SSA)"* [IEC-SSA], josta myös tuli uusi versio kesällä 2016. Tämä ISASecure ryhmään kuuluva sertifiointi puolestaan sisältää automaatiojärjestelmien kyberturvallisuusvaatimukset ja -tasot (IEC 62443-3-3), jotka tulisi asettaa ja täten vaatia sertifioinnin kohteena olevan vyöhykkeen (*security zone*) järjestelmiltä.

SSA standardin mukaan sertifioitavan ohjausjärjestelmän (automaatiojärjestelmään kuuluvien tuotteiden osajoukon) on täytettävä lisäksi seuraavat kriteerit:

- Ohjausjärjestelmä sisältää integroidun järjestelmän, johon kuuluu enemmän kuin yksi laite, mutta kokonaisuus on tunnistettavissa uniikilla tuotekoodilla.
- Ohjausjärjestelmä on saatavilla ja kokonaisuudessaan tuettuna yhdeltä toimittajalta (voi sisältää komponentteja muilta valmistajilta).
- Järjestelmätuotteet ovat konfiguraatiohallinnan ja versionhallinnan alaisia.

Kyberturvallisuustestauksella voidaan pyrkiä arvioimaan tuotteen tai palvelun sietokykyä hyökkäyksiä vastaan, mutta testauksen lopputulema ei sitovasti todista, että testikohdetta ei voida murtaa.

8.4 Tuotteen kyberturvallisuustestaus – Netcontrol Case

Suomalainen Netcontrol Oy valmistaa ja toimittaa Netcon SCADA -järjestelmiä ja verkostoautomaatioratkaisuja sähköverkkoyhtiöille – yhteiskuntamme kriittisen infrastruktuurin toimijoille. Sähkönjakeluverkoissa käytettäviltä järjestelmiltä ja laitteistoilta vaaditaan monia alan standardien mukaisia kelpoisuuksia. Kelpoisuudet ja hyväksynnät voidaan todistaa monin tavoin vaatimuksista riippuen. Alan yleisiin vaatimuksiin käytetään riippumattomia, kansainvälisesti tunnustettuja sertifioituja laboratorioita, jolta tilataan laitteen/järjestelmän standardinmukaiset testit ja laboratorio kirjoittaa siitä sertifikaatin vaatiman raportin sekä todistuksen.

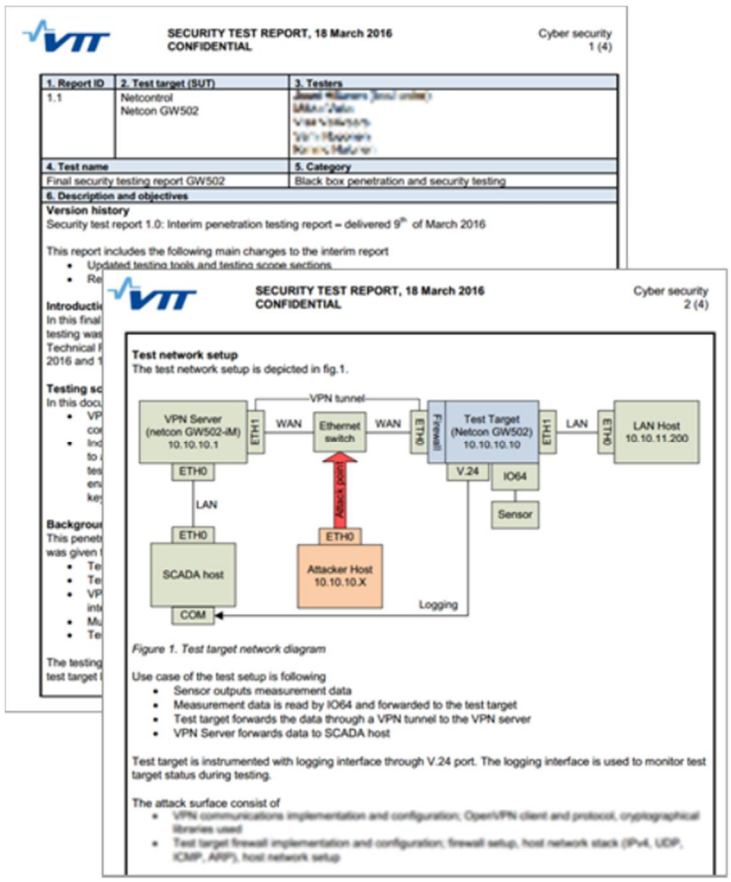
Alan tilaajien ja viranomaisten hankintavaatimukset kehittyvät ja kiristyvät jatkuvasti. Uusia tai uudistettuja hyväksyntöjä, sertifikaatteja ja testejä vaaditaan hankintavaatimusten kehittymisen tahdissa. Internetin voimakas hyödyntäminen on nostanut tieto- ja kyberturvallisuusvaatimukset ja standardit selkeästi esille uusiin hankintavaatimuksiin. Yhä useammin jo tarjouskilpailuun mukaanpääsy edellyttää tuotteen tietoturvahyväksynnän.

Netcontrol haki mukaan erääseen kansainväliseen tarjouskilpailuun ja mukaanpääsyn eräs vaatimus oli tuotteen tietoturvasertifikaatti tai riippumattoman mutta tunnetun laboratorion testiraportti. Netcontrol etsi sopivaa riippumatonta testaajaa ja lopulta löysi kriteerit täyttävän tahon liittymällä KYBER-TEO-projektiin.

8.4.1 Netcon GW502

Testattava tuote oli Netcon GW502, joka on Netcon 500 -ala-asemalaitteiston keskusyksikkö. Netcon 500 -ala-asemalaitteisto huolehtii sähköasemilla automaatiotoiminnoista, tietoliikenneyhteyksistä ja tietoliikenneyhteyksien suojaamisesta.

Netcon Gateway GW502 -yksikössä on sisäänrakennettu palomuuri, VPN ja salaustoimintoja, jotka testattiin VTT:n laboratoriossa. Testit suoritettiin keväällä 2016 ja tietoturvatestiraportti saatiin nopealla aikataululla. Kuvassa 28 on yleiskuva ja kuva eräästä tuloksena syntyneestä luottamuksellisesta testiraportista.



SECURITY TEST REPORT, 18 March 2016
CONFIDENTIAL

Cyber security
1 (4)

1. Report ID	2. Test target (SUT)	3. Testers
1.1	Netcontrol Netcon GW502	[redacted]

4. Test name	5. Category
Final security testing report GW502	Black box penetration and security testing

6. Description and objectives

Version history

Security test report 1.0: Interim penetration testing report – delivered 9th of March 2016

This report includes the following main changes to the interim report

- Updated testing tools and testing scope sections

SECURITY TEST REPORT, 18 March 2016
CONFIDENTIAL

Cyber security
2 (4)

Test network setup

The test network setup is depicted in fig.1.

Figure 1. Test target network diagram

Use case of the test setup is following

- Sensor outputs measurement data
- Measurement data is read by IO64 and forwarded to the test target
- Test target forwards the data through a VPN tunnel to the VPN server
- VPN Server forwards data to SCADA host

Test target is instrumented with logging interface through V.24 port. The logging interface is used to monitor test target status during testing.

The attack surface consist of

- [redacted]
- [redacted]

Kuva 28. VTT-raportti Netcon GW502 -tuotteen tietoturvatestistä.

VTT:n tietoturvatestiraportti GW502:sta hyväksyttiin tarjouskilpailun tietoturvaehtojen mukaiseksi, joten Netcontrol pääsi mukaan tarjouskilpailuun ja jatkamaan hankintaneuvotteluja.

8.4.2 Opetukset

Sähkönjakeluverkoissa käytettävien järjestelmien ja laitteistojen hankintaprosessit kestävät useita vuosia. Ostajat tekevät esikarsinnan ja muodostavat ”lyhyen listan” hyväksytyistä laitteista ja järjestelmistä, jolle pääseminen mahdollistaa varsinaiset hankintaneuvottelut. Sähköverkkoyhtiöiden SCADA-järjestelmiin ja verkostoautomaatioratkaisuihin liittyvät hankinnat vaativat pitkäjännitteisyyttä, laajaa alan kehitykseen osallistumista sekä jatkuvaa yhteistyöverkoston ja osaamisen kehittämistä.

Tarvitsemme alalle kansainvälisesti auktorisoituja tietoturvatestauspalveluja tarjoavia toimijoita, jotka voisivat sertifioida niin laitteita, järjestelmiä, yhtiöitä kuin henkilöitäkin. Suomessa ja suomalaisille toimijoille ja tuotteille tämä toisi uskottavuutta ja luottamusta – ja siten kilpailuetua maailmalla. Projektissa tehty kehitystyö on auttanut yrityksiä pääsemään mukaan kansainväliseen kilpailuun.

8.5 Varoituksen sana

Kyberturvallisuustestauksella voidaan pyrkiä arvioimaan tuotteen tai palvelun sietokykyä hyökkäyksiä vastaan, mutta testauksen lopputulema ei sitovasti todista, että testikohdetta ei voida murtaa. Testauksella voidaan toki vahvistaa, että järjestelmään on mahdollista tunkeutua, mutta ei sitä, että kohteeseen olisi mahdotonta tunkeutua, mikäli hyökkääjällä on riittävästi osaamista ja resursseja. Lisäksi kertaalleen suoritettu testaus on vain tietyn ajanhetken tilanne, joka ei päde kovin kauaksi tulevaisuuteen. Tämä johtuu mm. jatkuvasta teknologian ja uhkien kehittymisestä.

Toisaalta kyberturvallisuustestauksesta ja löydösten korjauksista huolimatta hyökkääjät voivat saavuttaa pääsyn tuotannon järjestelmätasolle ja sen hallintatyökaluihin käyttäen näiden järjestelmien sallittuja käyttäjätunnuksia ja pääsyoikeuksia. Tällainen penetraatio käynnistetään pääasiassa sosiaalisen tiedustelun keinoin, jolloin tavanomaiset tietoturvamekanismit eivät anna suojaa ja hyökkääjää on vaikea havaita pelkästään palomuureilla tai tunkeutumisen havaitsemisjärjestelmillä (IDS). Tarvitaan myös automaatiojärjestelmien tilannekuvaa, mm. sallittujen konfiguraatioiden, päivitysten ja tuotannon ohjauskäskyjen jatkuvaa seurantaa. Tästä kerrotaan lisää seuraavassa luvussa.

8.6 Referenssejä

Sertifiointi

[IEC-EDSA] IEC 62443 – EDSA Certification, Embedded Device Security Assurance (EDSA) – v2, effective 01 July 2016, http://www.isasecure.org/en-US/Certification/IEC-62443-EDSA-Certification

[IEC-SSA] IEC 62443 – SSA Certification, System Security Assurance (SSA) – v2, effective 01 July 2016, http://www.isasecure.org/en-US/Certification/IEC-62443-SSA-Certification

Testaajan osaaminen

[CD19896-1] ISO/IEC 1st CD 19896-1, Information technology – Security techniques – Competence requirements for information security testers and evaluators – Part 1: Introduction, concepts and general requirements

Turvallinen ohjelmistosuunnittelu ja turvalliset ohjelmointisäännöt
[SEI CERT] SEI CERT Coding Standards: https://www.securecoding.cert.org/confluence/display/seccode/SEI+CERT+Coding+Standards

9. Automaatioverkon havainnointi

9.1 Nykytilanne on hälyttävä

Teollisuuden tuotantoverkkoja ei voida enää ylläpitää tehokkaasti ilman riittävän tilannetietoisuuden ja koordinoidun ongelmanratkaisukyvyn kehittämistä. Tämä taas edellyttää erilaisten menetelmien ja palvelujen soveltamista tuotantoverkkojen tilannekuvan jatkuvaan seurantaan. Kyberuhat ovat jo todellisuutta lähes kaikkien yritysten tuotantoverkoissa, joten sisäisten uhkien seurannasta onkin tullut välttämättömyys erityisesti kriittistä infrastruktuuria ylläpitäville yrityksille. Viimeistään muutamia vuosia sitten olemme valitettavasti joutuneet havaitsemaan, että yhteiskunnan toimintoja ylläpitävää kriittistä infrastruktuuria vastaan on toteutettu vakavia kyberhyökkäyksiä myös Euroopassa. Yksi tärkeimmistä julkisuuteen tuoduista tapauksista koskee Ukrainan sähköverkkoon kohdistunutta kyberhyökkäystä.

Esimerkki. Kyberhyökkäys katkaisi sähköt noin 80 000 ihmiseltä Länsi-Ukrainassa [FIREEYE].

Kyberhyökkäys katkaisi sähköt noin 80 000 ihmiseltä Länsi-Ukrainassa:
December 23, 2015: Ukrainian sources reported finding the *BlackEnergy3* malware in three regional Ukrainian electricity distribution companies. Also *Killdisk* was used to disable system computers and call centers were overloaded with automated telephone calls.

Käytännössä tämä tarkoittaa sitä, että osaavilla rikollisilla ja/tai valtiollisilla tahoilla on jo todistetusti olemassa kyvykkyys aiheuttaa eurooppalaisen kriittisen infrastruktuurin toimintaan vakavia häiriöitä erilaisia kyberhyökkäyskampanjoita toteuttamalla. Todennäköisesti vakava häirintä edellyttää useimmiten ns. ”hiljaisen tiedustelun” jaksoa, jossa kriittisestä infrastruktuurista kerätään julkisesti saatavilla olevan tiedon lisäksi infrastruktuuria ylläpitävien yritysten turvaluokiteltua tai muutoin arkaluontoista tietoa. Tätä kriittistä tietoa voidaan hankkia esim. erikoistuneiden tieto-

murtajien palveluja hyödyntämällä peittäen tietomurron jäljet uusinta tekniikkaa hyödyntämällä. Tällöin tulevat uhrit eivät osaa epäillä tuotantonsa tietojärjestelmien heikkouksien ja ehkä myös turvakäytäntöjensä paljastumista ulkopuolisille, vihollisille tahoille.

Kansainvälisillä kyberturvallisuuspalvelujen tarjoajilla on jo jonkin aikaa ollut osaamista hiljaisen tiedustelun ja kyberhyökkäysten valmistelun tunnistamiseksi. Esim. *iSIGHT Partners* on löytänyt johtavien automaatiojärjestelmätoimittajien ohjelmistoja vastaan suunnattuja *BlackEnergy*-moduuleita, joiden tarkoituksena on ollut mahdollisesti laajemminkin valmistella automaatiojärjestelmiin kohdistuvia kyberhyökkäyksiä.

Organisaatioiden sisäinen toiminta- ja turvallisuuskulttuuri ovat erittäin merkittäviä tekijöitä kybertilanteen parantamisessa ja tietoisuuden kehittämisessä. Tehokkainkaan tekninen valvonta ei voi onnistua kaikissa tilanteissa, mikäli vastapuolen tiedustelu on kykenevä huijaamaan henkilöstöä. Käyttäjiä harhautetaan esim. luovuttamaan käyttäjätunnuksia ja salasanoja vääriin käsiin taikka tahattomasti saastuttamaan oman työasemansa esim. klikkaamalla web-linkkiä, minkä seurauksena haittaohjelma asentuu lähes välittömästi. Myös automaation sovelluskehittäjien täytyy havahtua haavoittuvuuksien seurauksiin käytännössä. Tämä edellyttää esim. kyberturvallisuusharjoitusta, joka avaa silmät karulle todellisuudelle – kaikki järjestelmät voidaan murtaa.

9.2 Tuotantoyksikön verkkojen monitorointi

Tässä kohdassa esitellään muutamia käytännön oppeja ja havaintoja KYBER-TEO-projekteissa testatuista monitorointikonsepteista, malleista tai menetelmistä. Ihanteellista olisi, mikäli kyberturvallisuuskontrollit ja kybertilannekuvan riittävän kehittynyt seuranta voitaisiin räätälöidä ja integroida tuotantoyksikköön jo sen suunnitteluvaiheesta alkaen. Tällöin vältyttäisiin kalliiden, esim. arkkitehtuurimuutoksia edellyttävien kyberturvallisuusratkaisujen lisäämiseltä jälkikäteen, mikä ei koskaan ole optimaalinen tilanne.

Valitettavasti automaation pitkän elinkaaren ja toisaalta kyberhyökkäysten erittäin nopean kehittymisen seurauksena esim. uusien uhkien seurannan toteuttaminen pelkästään yhden automaatiojärjestelmätoimittajan palveluihin nojautuen onnistunee harvoin. Automaatiotoimittajillakin on omat palvelurajoitteensa liittyen vanhojen tuotteiden tai alustojen tukeen sekä paine tuoda markkinoille uusia tuotteita. Lisäksi lähes aina kyseessä on monitoimittajaympäristö.

Tilaajan tulee siis ymmärtää tuotantoyksikön kyberturvaamisen vaatimukset ja niiden kehittyminen koko elinkaaressa, jotta esim. järjestelmien päivittäminen ja seu-

ranta voidaan toteuttaa asianmukaisesti yhteistyössä eri osapuolten kanssa. Asiantuntijoiden kanssa kannattaa selvittää yhdessä mm. mitä tulee lokittaa, esim. järjestelmään kirjautumiset, ohjelmistojen käynnistysyritykset, järjestelmäprosessien muutokset, datayhteyksien muutokset. Hyviä periaatteita ovat mm. seuraavat:

- Lokikirjaukset on suojattava vahvasti, jotta kukaan ei voi muuttaa niitä.
- On varmistettava, että lokikirjaukset eivät voi täyttää muistia ja täten jumiuttaa laitetta.
- Monimutkaisempien lokikirjausten osalta kannattaa tilata säännöllisesti ammattimainen lokianalyysi, mikäli oma osaaminen ei riitä.

Erityisesti teollisuusautomaatiossa saattaa kannattaa noudattaa YKSINKERTAISUUTEEN ja selkeään työnjakoon pakottavia ohjeita, kuten:

- Älä lisää erillisiä tietoturvaohjelmistoja toimilaitteeseen. Käytä laitteen omia suojaus-, tallennus- ja lokimenettelyjä, esim. Windowsin ”sisäänrakennetut” tietoturvamenettelyt.
- Mikäli erillisiä tietoturvajärjestelmiä kuitenkin lisätään, niiden hallinta ja käyttö tulee erottaa muista laitteistoista, koska ne itsessään mahdollistavat uusia haavoittuvuuksia ja hyökkäysvektoreita.

9.2.1 Seurannan tarkoitus

Tuotantoyksikön dataverkkojen seurantaa tarvitaan monista erilaisista syistä johtuen. Tyypillisesti on tarpeen selvittää ja hallita mm. seuraavia asioita:

- TUOTANNON TILA: Toimiiko tuotanto täsmälleen suunnitellulla tavalla, vai onko siinä tapahtunut poikkeamia?
- VERKKOVIAT: Ongelmat verkkojen normaalitoiminnassa ja vikaantumisen syyt tulee pystyä tunnistamaan (lähes) reaaliaikaisesti
- OMAISUUDENHALLINTA: Verkoissa olevien laitteiden (suojattavien kohteiden) tila tulee pystyä inventoimaan säännöllisesti ja kustannustehokkaasti
- KAPASITEETIN HALLINTA: Verkkojen ylikuormittuminen tulee pystyä ennaltaehkäisemään jatkuvalla seurannalla
- KYBERTURVALLISUUDEN TILANNEKUVA: Verkkoihin kohdistuvat kyberturvallisuuden loukkaukset ja tietovuodot tulee pystyä tunnistamaan.

Tässä julkaisussa keskitytään kyberturvallisuuden tilannekuvan parantamiseen ja seurantaan erityisesti automatisoituun tuotantoon käytettävissä dataverkoissa. Kyberturvallisuustilanteen teknisen seurannan kohdistamisessa tulee tänä päivänä käyttää vahvasti hyväksi myös tuotannon, verkon, omaisuuden ja kapasiteetin tilan seurantaa.

9.2.1.1 Trendien seuranta

Esimerkkinä kyberturvallisuuden tilannekuvan seurantaa tukevista toimista voidaan mainita laajasti eri järjestelmien muutostrendien seuranta. Tällaisessa toiminnassa seurataan esimerkiksi, miten yrityksen tuotantoverkkojen ja tuotantojärjestelmien uhkien toteumaan liittyvät indikaattorit (tai heikot signaalit) kehittyvät. Esimerkkejä trendien seurannasta:

- PÄIVITYKSET: Vikapaikkojen ja päivitysten määrä ja saatavuus sekä asentumisen onnistuminen
- HAAVOITTUVUUDET: Haavoittuvuuksien kohdistuminen omiin järjestelmiin ja yleinen lukumäärä
- SUORITUSKYKY: Järjestelmien saatavuuden ja suorituskyvyn muutokset
- TIETOKANNAT: Tietokantoihin kohdistuvat kyselyt ja rekisterimuutokset
- TIEDOSTOT: Tiedostoissa tapahtuvat odottamattomat muutokset
- TIEDUSTELU: Aliverkkoihin kohdistuvat odottamattomat kyselyt (*honeynettien* hyödyntäminen)
- TILIT: Käyttäjätileissä tapahtuvat odottamattomat muutokset
- PROFIILIT: Käyttäjäprofiileissa tapahtuvat odottamattomat muutokset
- Jne.

Trendeissä tapahtuvien muutosten avulla voidaan kohdistaa tarkempi kyberturvaseuranta epäilyttäviin kohteisiin. Trendiseuranta kannattaa myös yhdistää osaksi laajempaa toiminnan valvontaa, jossa poikkeava toiminta erottuu normaalitoiminnan kokonaisuudesta ylittämällä ”normaalin” raja-arvot. Yksityiskohtaisia trendejä voidaan seurata helposti räätälöitävissä olevien indikaattorien osalta nykyään myös graafisesti mm. kaupallisin ja avoimen lähdekoodin työkaluin. Erään kaupallisen tuotteen esimerkkinä toimikoon Paessler: https://www.paessler.com/prtg.

9.2.1.2 Tutkinta

Eräs lupaava uusi kotimainen lähestymistapa on nauhoittaa ja tallentaa turvallisesti kaikki sisäverkossa liikkuva data ja tarpeen tullen analysoida sitä valvotusti. Tämä vaatii erityismenettelyjä turvallisen toteutuksen ja tiedon luottamuksellisuuden varmistamisen osalta. Saatavana on Tamperelaisen Cysecin tuote https://www.cysec.fi/fi/, jonka mukaan ”Tietoliikenneholvi”™ nauhoittaa turvallisesti, huomaamatta ja autonomisesti kaiken tietoliikenteen, mikä mahdollistaa juurisyyn analysoinnin ja teknisen tutkinnan.

Tutkinnassa (erityisesti rikostutkinnassa eli forensiikassa) käytettävän datan autenttisuus ja eheys tulee pystyä varmistamaan vahvoin menettelyin. Myös laillisuuden varmistaminen, pääsynvalvonta ja lupamenettelyt datan käsittelyyn ja siirtoon tulee järjestää erittäin huolellisesti kussakin tilanteessa erikseen.

Havaintojen ja poikkeamien käsittelyyn kehittämämme toimintamalli on esitelty luvussa 10, Poikkeaman sattuessa – Yhteistoimintamalli.

9.2.2 Monitorointipalvelun evaluointi – Case

Projektin kuluessa olemme arvioineet erilaisia kaupallisia monitorointipalveluja. Tässä kohdassa esitämme prosessin ja työkaluja, joilla evaluoimme erästä kaupallista koneoppimiseen perustuvaa IDS-palvelua.

9.2.2.1 Evaluoidun palvelun toimintaperiaate

Tutkittu monitorointipalvelu havaitsee ja lokittaa ”normaalista poikkeavaa” verkkoliikennettä opettelujakson jälkeen. Epätyypillisestä liikenteestä saadaan pisteytetty hälytys, joka pohjautuu esiasetettuihin sääntöihin. Käyttäjä voi muokata sääntöjä graafisen käyttöliittymän avulla.

Evaluoitavan palvelun tarjoamiin hälytyksiin ja hälytysrajojen käyttöön kannattaa perehtyä hyvin. Ilman hälytystä jääneet tapahtumat löytyvät kuitenkin aina lokeista, sillä palvelu lokittaa kaikki tapahtumat. Käyttäjän tulee vain tietää, mitä on testattu ja mitä etsiä. Tehokkaassa uhkien tunnistamisessa saattaakin olla kyse pitkälti myös hälytysrajojen oikeasta asettelusta kussakin tilanteessa. Joidenkin erityisominaisuuksien testaaminen ei todennäköisesti ole helposti järjestettävissä koejärjestelyin. Erityisesti käyttäjäprofiilien testaaminen saattaa vaatia koeprofiilin luomista ja käyttöä pidemmällä aikavälillä.

Monitorointipalvelun suorituskyky on usein riippuvainen käytettyjen sääntöjen määrästä. Tuotteen testiversio on saatettu asettaa toimimaan minimisäännöin, jolloin sen uhkien tunnistuskykykin on puutteellinen.

9.2.2.2 Evaluoinnin tavoite ja periaate

Evaluoinnin tavoitteena oli testata käytännössä asiakkaan ehdottaman monitorointipalvelun soveltuvuutta ja uhkien tunnistamisen kyvykkyyttä erään tuotantoyksikön sisäverkon kyberturvallisuuden valvontaan.

Aluksi palvelussa käytettävään tuotteeseen tutustuttiin julkisesti saatavilla olevan materiaalin avulla. Tämän perusteella ei ollut todellisuudessa mahdollista arvioida tuotteen soveltuvuutta tai tehokkuutta verkon tietoturvan monitorointiin, koska materiaali oli markkinointihenkistä eikä pureutunut tekniikkaan.

Testauskohteessa saimme käyttöömme asiakkaan kannettavan testi-PC:n, johon oli asennettu mm. Kali Linux-virtuaalikone. Testit suoritettiin tältä testi-PC:ltä. Valitsimme toteutettavaksi seuraavissa kohdissa kuvatut evaluointitestit.

9.2.2.3 Evaluointitestit – Verkkoskannaus

Verkon skannaaminen on hyökkääjälle tyypillinen tapa saada tietoa kohdeverkosta. Skannaamalla on mahdollista kerätä tietoa verkon järjestelmistä ja niissä olevista ohjelmista, ja siten mahdollisista järjestelmä haavoittuvuuksista ja hyökkäyskeinoista. Skannaaminen on tyypillistä sellaiselle hyökkääjälle, joka on kiinnostunut verkon sisällöstä, muttei ole kovin varovainen hyökkäyksen paljastumisen suhteen. Jotkin aktiiviset skannaustekniikat ovat melko vaikeasti havaittavia, mutta suurin osa on varsin helposti näkyviä, mikäli verkossa on aktiivisessa käytössä oleva IDS-järjestelmä.

Verkkopohjaisen havainnoinnin lisäksi monet *host*-pohjaiset tietoturvajärjestelmät (esim. antivirusohjelmistot) voivat huomata aktiivisen verkkoskannauksen, joka kohdistuu kyseiseen laitteeseen.

Evaluointitestit
Passiivisen skannauksen jätimme testauksessa vaille huomiota, sillä evaluoitava palvelu ei pystyisi havaitsemaan sitä.

Aktiivisen verkkoskannaamisen tekniikoista olimme valinneet kaksi tyypillistä:

- Nmap: Monipuolinen verkkoskannaustyökalu, jolla saa yksityiskohtaista tietoa verkosta, sen toiminnasta ja tarkkaa tietoa siihen kytketyistä laitteista.
- Nessus: Syvempi skannaustyökalu joka on tarkoitettu järjestelmähaavoittuvuuksien löytämiseen verkosta.

Myös esim. ARP-tason skannauksen tunnistamiskyvykkyys testattiin.

Hitaiden (< 1/s) ja hyvin hitaiden (< 1/min) skannausten tunnistamisen todentaminen on erityisen tärkeää, sillä tavallisten käyttäjien ei ole tavallisesti tarpeen hidastaa skannauksiaan. Monitorointipalveluissa tulisikin olla kyvykkyys säätää eri nopeuksilla tapahtuvien verkkoskannausten tunnistamisen kynnysarvoja, esim. ”kansallisen kybersään” edellyttämälle tasolle.

9.2.2.4 Evaluointitestit – Tiedostojen lataaminen ulkoisesta verkosta

Esivalmistelut
Tiedostojen lataaminen verkon yli on usein oleellinen valvottava toiminto. Valmistelimme ennen testikohteeseen tulemista VTT:n testiverkkoihin muutamia tiedostoja, joiden siirtäminen verkon yli paljastaisi jotain evaluoitavan palvelun havainnointikyvykkyydestä.

Testattavan kohteen sisäverkossa kyseinen siirto tapahtuu käyttämällä HTTP-protokollan mukaista kutsua ulkoiseen IP-osoitteeseen (ilman DNS-palvelun käyttöä). Tämä on monesti epätyypillistä käyttäytymistä, joten evaluoitavan järjestelmän tulisi

se havaita. (Käytetty IP-osoite oli myös epätyypillinen eli osa testiverkkoa, jossa ei ole julkisia palveluja.)

Evaluointitestit
Evaluoinnissa ladattiin kaksi erilaista tiedostoa, suuri 500 Mb:n kokoinen pcap-tiedosto ja pieni PDF-tiedosto, joka sisälsi VTT:n valmistaman testihaittaohjelman. Haittaohjelma oli valmistettu Metasploit-alustalla ja hyödyntää haavoittuvuutta CVE-2010-1240 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2010-1240). Nykyaikaiset antivirus-ohjelmistot havaitsevat tämän PDF-haittaohjelman ja poistavat sen välittömästi, myöskään kyseisen tiedoston lähettäminen sähköpostilla ei onnistu, jos liitetiedostoja skannataan.

Huom! Monitorointipalveluissa hälytyksen olisi hyvä olla säädettävissä myös tiedoston koon mukaan, jottei hyökkääjä voisi toimia huomaamattomasti esim. pienien tiedostojen vähittäisillä siirroilla. Yleisesti ottaen koneoppimiseen perustuva monitorointipalvelu ei korvaa tunnisteisiin (signatures) pohjautuvaa havainnointia, sillä algoritmit eivät suoraan tunnista näitä uhkia.

Lisäksi testasimme tiedostonsiirtoa FTP-protokollan avulla:
- http-portin yli (selaimella) sekä
- FTP-protokollan tavanomaisen porttiavaruuden yli (mikäli paikallinen palomuurisäännöstö mahdollistaa tämän).

9.2.2.5 Evaluointitestit – Netcat testaus

Esivalmistelut
Netcat on pieni verkkokommunikaatio-ohjelma, jolla on helppo luoda datayhteyksiä eri koneiden välille. Sitä hyödyntämällä voi myös testata monitorointipalvelujen kykyä tunnistaa järjestelmien käyttäytymisen muutosta palvelutasolla. Verkkohyökkääjä voi nimittäin yrittää laajentaa sisäverkossa hallitsemiensa koneiden joukkoa, jonne ei ulkomaailmasta suoraan pääse esim. palomuurisääntöjen vuoksi.

Esimerkkejä netcat-yhteyden luomiselle:
- Asetetaan kohdekone kuuntelemaan porttia, esim. 12345: `nc -l 12345`
- Otetaan yhteys toiselta koneelta: `nc <kohde_ip> 12345`

Valmistelimme näillä keinoin useita testitapauksia, joiden tarkoituksena oli testata evaluoitavan palvelun kykyä havaita uusia datayhteyksiä verkon sisällä. Tätä varten testikoneelta avataan (virtuaalisia) yhteyksiä tyypillisten palveluiden (http, ftp) ja epätyypillisten palveluiden erilaisiin portteihin. Testaus havainnollistaa täten uusien verkkopalveluiden tunnistamisen tehokkuutta.

9.2.2.6 Evaluointitestit – Tor verkon käynnistäminen

Olimme valmistautuneet myös *Tor*-verkon tunnistuskyvykkyyden evaluointiin testauskohteena olevassa verkossa. *Tor*-verkkoahan käytetään datayhteyksien anonymisoinnissa, ja sen avulla hyökkäävän osapuolen on mahdollista salata oman järjestelmänsä IP-osoite liikennettä kuuntelevalta osapuolelta. (https://torproject.org/)

Keskustelujen jälkeen kävi kuitenkin ilmi, ettei *Tor*-verkon käytön testaaminen ollut sallittua kyseisessä verkossa. *Bittorrent*-ohjelmistoa voisi myös käyttää samalla tavalla dataliikenteen päätepisteen peittämiseen, mutta senkään testaaminen ei ollut sallittua.

9.2.2.7 Evaluointitestit – Salattu ulosmenoväylä tiedolle

Testasimme myös tiedon lähettämistä salattuna ulospäin testikohteena olevasta sisäverkosta. Lähetimme suuren tiedoston (pcap-tiedosto) julkiseen palveluun, joka salaa lähetettävän tiedon käytännössä jo päätelaitteella ennen lähetystä. Tarkoituksena oli arvioida sisäverkossa olevan hyökkääjän kykyä lähettää löytämäänsä arvokasta tietoa sellaiseen ulkoiseen järjestelmään, jonka kautta (hyökkääjä) pystyisi varastetun tiedon myöhemmin anonyymisti noutamaan. Tässäkin tapauksessa korostamme, että kannattaa testata uhkan havaitsemiskyvykkyyttä monella erilaisella tiedostokoolla (ja muodolla).

9.2.2.8 Evaluointitestit – Uusi IP-osoite verkossa

Testeihin käytetty Kali Linux -virtuaalikone ei ollut aiemmin ollut yhdistettynä testikohteena olevaan verkkoon, joten ”tuntemattoman koneen” pitäisi näkyä evaluoitavassa palvelussa hälytyksenä. Testasimme myös testi-PC:n IP-osoitteiden vaihdon ”näkyvyyden” evaluoitavassa palvelussa.

9.2.2.9 Evaluointitestit – Epätyypillinen TCP-liikenne

Eräs hyvin tyypillinen palvelunestohyökkäyksiin (*DoS*, *Denial of Service*) liittyvä tekniikka on *SYN-flood*, jossa TCP-yhteyden avauspaketteja lähetetään kohteeseen nopealla tahdilla ja vastausviestit jätetään kuittaamatta. Näin testikohteeseen syntyy ylimääräinen kuorma.

Testeihin käytettiin hping3-työkalua. Myös TCP xmas-scan kuului testeihin, joiden näkyvyys evaluoitavassa palvelussa testattiin.

Huom! *DoS*-testaamisessa vaarana on tuotannossa olevien palvelujen hidastuminen tai vikaantuminen. *DoS*-testaus onkin järkevintä tehdä testiverkossa, mutta mikäli jonkinlainen evaluointi on tehtävä tuotantoverkossa, testaus on suunniteltava

hyvin ja riskit arvioitava. Testaajan tulee olla hyvin kokenut, testityökalun hyvin tuttu, ja testejä kannattaa ajaa hitaalla pakettimäärällä (esim. 10 pakettia/s), jottei mitään tuotannossa olevaa palvelua oikeasti häirittäisi.

9.3 Automaatioverkon havainnointi – Case

Automaatiojärjestelmän tietoturvamonitorointi on ollut paljon esillä viimeisen viiden vuoden aikana, koska on ymmärretty sekä automaation rooli yhteiskunnan kriittisen infrastruktuurin ytimessä että ohjelmistotekniikan ja tietoliikenteen rooli automaation mahdollistajana. Tästä johtuen markkinoille on saapunut useita automaation tietoturvamonitorointiin palvelujaan kohdentavia yrityksiä ja tuotteita. Useat näistä palveluista ja tuotteista keskittyvät ratkaisemaan ongelman, jota voisi kuvata lauseella ”automaatiojärjestelmää tulee monitoroida tietoturvahyökkäysten varalta”. Tämä ongelman asettelu ei ole taloudellisesti eikä järjestelmään kohdistuvien uhkien kannalta järkevä seuraavista syistä:

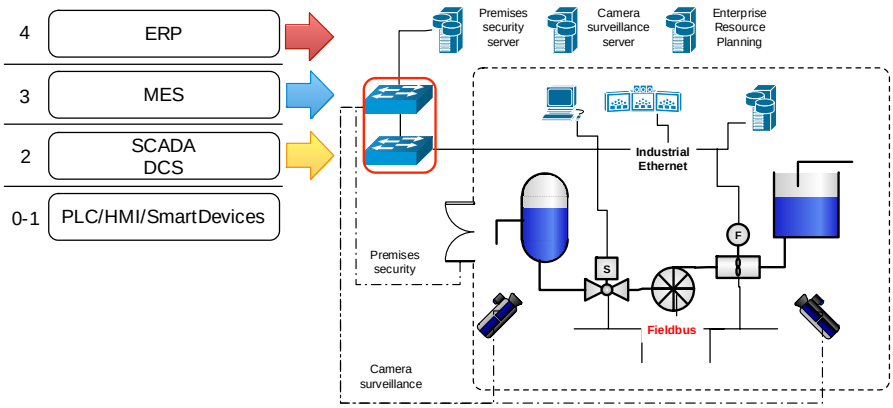
- Uuden tietoliikenneterminologiaa käyttävän ja erillisen monitorin tai käyttöliittymän tuominen automaatio-operointiin ei ole järkevää, koska nykyisinkin automaatiojärjestelmä monitoroidaan usealla käyttötarkoitukseen kohdennetulla ja käytettävyysanalyysin perusteella toiminnallisuuteen suunnitellulla käyttöliittymällä.
- Tietoturvan monitorointiin suunniteltu järjestelmä ei tarjoa riittäviä työkaluja automaation tietoliikenneongelmien selvittämiseen. Usein jo automaatiojärjestelmän ISO OSI -mallin L2-tason liikenne osoittaa tietoliikennemonitorointiohjelmistot riittämättömäksi – perinteinen tietoliikenneseuranta perustuu L3 (IP) -tasolla tapahtuvaan liikenteenseurantaan.
- Kohdennetun tietoturvahyökkäyksen havainnointi vaatii korkeamman kypsyystason kuin yleisen tietoliikenteeseen perustuvan tietoliikennemonitoroinnin sekä resurssit havainnoinnin jatkuvaan tulkitsemiseen.
- Tuotteiden ja palveluiden markkinointi tapahtuu valitettavan usein vaatimustenmukaisuuden (*compliance*) kautta, siis viestillä ”teidän tulee monitoroida, koska ennemmin tai myöhemmin regulaattori vaatii, että automaatiota monitoroidaan tietoturvaongelmien varalta”. Kiirehtiminen tulevaisuuden vaatimustenmukaisuuden täyttämiseen johtaa helposti hankkeeseen, jossa riittämätön resursointi ja suunnittelu saa aikaan yhden päivittäistä toimintaa hyödyttämättömän lisälaitteen ja/tai palvelun.

Automaation tietoturvamonitorointi erillisenä palveluna tai toimintana ei siis tuota riittävää hyötyä, jotta investoinneista vastaavat tahot olisivat valmiita investoimaan IT-ympäristöistä tuttuja summia automaation tietoturvamonitorointiin. Tällainen investointi tapahtunee vain ympäristöissä, joissa lainsäätäjän edellyttämään vaatimustenmukaisuuteen kuuluu tietoturvamonitorointi.

Automaatiota ei voi nykyisin olla olemassa ilman tietoliikennettä. Mittauksia ja ohjauksia toteutetaan tietoliikenneyhteyksien yli ja konfigurointia sekä kunnonvalvontaa halutaan tehdä etänä. Tietoliikenteen rooli automaatiossa on nykyisin niin merkittävä, että siinä olevien häiriöiden havainnointi on riittävä peruste monitorointiin

kohdistuville investoinneille. On siis järkevää poistaa tietoturvamonitoroinnista sana tietoturva ja jättää vain monitorointi sekä ottaa tietoturva huomioon monitorointia suunnitellessa.

Automaatiojärjestelmä on selkeä kohde tietoliikenteen monitoroinnille, koska automaatioliikenne on pääosin hyvin määriteltyä. Määrittely tehdään automaatiojärjestelmää suunniteltaessa, ja siihen liittyvät muun muassa säätö- ja mittaussyklit, prosessiasemien määrä, tietoliikennelaitteiden sijainti sekä erilaiset integraatiopisteet, joissa vanha tekniikka yhdistyy Ethernet- ja IP-tekniikkaan. Integraatioon kuuluu myös tietoliikenne reaaliaikajärjestelmien ja yrityksen tuotannon- ja toiminnanohjauksen välillä, kuva 29. Automaatiojärjestelmässä on mahdollista muodostaa tietoliikenteen perustaso (*baseline*), jonka avulla poikkeamien havainnointi on huomattavasti helpompaa kuin perinteisissä toimisto-IT-ympäristöissä. Tässä luvussa keskitytään kuvassa 29 esitettyjen ISA-95-kerrosten 0–2 monitorointiin.



Kuva 29. Puolustautuminen palvelunestohyökkäyksiä vastaan. Automaatiojärjestelmän integroituminen toiminnan- ja tuotannonohjaukseen tapahtuu suunnitellusti. Integraatiopisteen yläpuolella (MES/ERP) on toimisto-IT:n tietoliikenne ja alapuolella (SCADA/DCS/PLC/jne.) reaaliaikaisuutta ja luotettavuutta vaativa automaation tietoliikenne. Punaisella kehyksellä on korostettu automaatio-IT-rajapinnan kriittiset komponentit.

Automaatiojärjestelmän monitorointiin eivät sellaisenaan sovi normaalit IT-ympäristöistä lähtevät monitorointikäytännöt, koska:

1. Automaatiojärjestelmän normaali laiteidentiteetti ei ole IP-osoite vaan automaatiokomponentin toiminnallista roolia kuvaava positiotieto.

2. Automaatioliikenteestä merkittävä osa tapahtuu OSI-mallin L2-tasolla, koska liikenteen reitittäminen segmentin ulkopuolelle ei usein ole tarpeellista ja L2-tasolla automaation vaatiman reaaliaikaisuuden toteuttaminen on helpompaa.

3. Automaation tietoliikennepolut ja -laitteet on mitoitettu automaatiojärjestelmän liikenteelle, ja monitorointitiedon välittäminen olemassa olevia yhteyksiä käyttäen voi ylittää suunnitellun mitoituksen.
4. Kaikessa automaatioon liittyvässä toiminnassa pyritään ensisijaisesti luotettavuuteen. Tästä syystä muutosten ja ylimääräisten mahdollisesti verkkoa häiritsevien laitteiden lisääminen tehdään aina harkiten ja vaikuttavuusanalyysin jälkeen.

Kun nämä reunaehdot ymmärretään, on automaatiojärjestelmä erittäin sopiva kohde automaattiselle monitoroinnille. Monitorointi- ja hälytys-termit sisältävät sekä tietoturvaan liittyvät että tietoturvaan liittymättömät tietoliikenneongelmat.

Monitoroinnin kehittämisessä on oleellista päästä testaamaan oikean automaatiojärjestelmän tietoliikennettä. Tulokset pohjautuvat Tampereen teknillisen yliopiston (TTY) Systeemitekniikan laitoksen (2017 alkaen Automaatio ja hydrauliikan laboratorio) tislauskolonniympäristössä tehtyyn kehitystyöhön. Ympäristössä on teollisen mittakaavan automaatiojärjestelmä, tarvittavat monitorointiympäristöt sekä monitoroinnin aiheuttamia riskejä pienentävät tietoliikennediodit. Näiden avulla voitiin toteuttaa todelliseen kriittiseen ympäristöön soveltuva Proof-of-Concept (PoC). Ympäristö on myös jatkuvassa tuotantokäytössä, joten kehitystyötä tehdessä piti varmistua, ettei monitorointi ja siihen tehdyt muutokset häiritse tuotantoa – rajoite, joka on kriittinen myös teollisuusympäristöissä.

Tislauskolonni on osa Tampereen teknillisen yliopiston TUTCyberLabs-konseptia, joka koostuu kolmesta ympäristöstä: 1) TIECyberLab (mini-internet, yrityksen toimistoverkko), 2) DEECyberLab (sähkön siirto, kulutus, älyverkot) sekä 3) ASECyberLab (energian tuotanto, prosessiautomaatio). Tislauskolonni sijaitsee osana ASECyberLabin verkkoa, joka on suunniteltu kriittisen infrastruktuurin automaatiojärjestelmien tietoturvan tutkimiseen ja toteutettu aidoilla teollisuusautomaation verkkolaitteilla.

KYBER-TEO-projektin yhteydessä NIXU ja TTY toteuttivat monitoroinnin pilotointia tuotannossa olevaan teollisuusautomaatiojärjestelmään. Monitoroinnin todettiin olevan palvelumuotoisena mahdollista, mutta valvonta vahvisti myös TTY:n laboratoriossa tehdyt havainnot ja kehitystarpeet oikeiksi. Monitorointipalvelun tuottaminen palvelumuotoisena korosti myös hallinnollisten prosessien tärkeyttä: 1) asiakasorganisaation omia toimia poikkeamahavainnon saapuessa sekä 2) palvelutoimittajan ja asiakasorganisaation välisiä yhteydenpitotapoja havaintoa selvitettäessä. Ilman selkeää toimintatapaa hyvänkin havainnointikyvyn hyöty pienenee huomattavasti.

9.3.1 Monitoroinnin kehittäminen automaatioon

Automaatioverkon monitoroinnin kehittämisessä on tärkeää

- hälytysten toimittaminen operointihenkilöstölle, jotta heille voidaan viestiä ongelman johtuvan tietoliikenteestä eikä esimerkiksi laiteviasta

- automaatio-operoinnin tietoliikennehäiriöiden jalostaminen tukemaan parempaa kommunikaatiota
- suunnitella integraatio muihin yrityksen järjestelmiin tai ulkopuoliseen palveluun automaatiojärjestelmää vaarantamatta
- integroida havaintojen käsittely organisaation normaaliin poikkeamakäsittelyyn.

Seuraavaksi käsitellään hälytysten jalostamista ja integraatiota muihin järjestelmiin. Muita osa-alueita ei käsitellä.

9.3.1.1 Tietoliikennehälytysten jalostaminen

Automaatioihmisten ja IT-ihmisten välisen yhteistyön suuri kompastuskivi on kommunikaatio ja erityisesti yhteisen sanaston puuttuminen. Tilanteen parantaminen on oleellisen tärkeää (toimisto-)IT-tekniikoiden tunkeutuessa yhä syvemmälle kohti automaatiojärjestelmän ja fyysisen maailman välistä rajapintaa.

IT-maailmassa tietoliikenteestä aiheutuva hälytys yleensä identifioidaan IP-osoitteen perusteella, koska se on internettekniikoita hyödyntävissä verkoissa luonnollisin identiteettitieto. Tämä tieto ei kuitenkaan ole järkevää automaatioympäristöissä, koska yhden IP-osoitteen takana saattaa olla suuri automaatiosegmentti ja koska IP-osoite ei ole automaatiosovellusten toiminnan kannalta oleellinen tieto.

Tietoliikennehälytysten jalostamisessa automaatioympäristössä kannattaa lähteä miettimään, millä lisätiedoilla (metatiedot) hälytys on tulkittavissa myös automaatioorganisaatiossa. Koska automaatiohenkilöstö tunnistaa käsitteet positio, osaprosessi sekä tietynlaiset yhteyskäytännöt, kannattaa lähteä liikkeelle niistä.

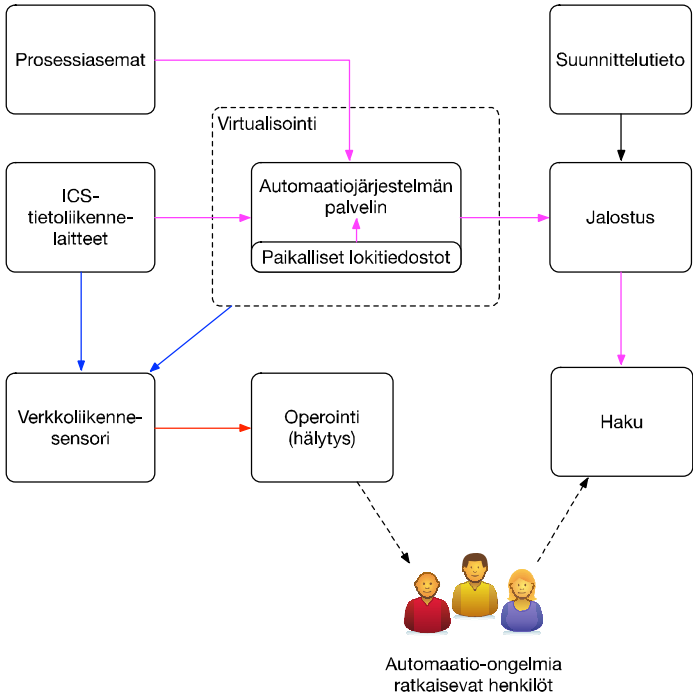
Jalostamisen vaatima toiminnallisuus vaatii perinteisestä IT-maailmasta poikkeavaa lähestymistä. Ratkaisua rakennettaessa päädyttiin hyvin nopeasti avoimen lähdekoodin hyödyntämiseen, koska avoimen lähdekoodin työkaluilla tietoliikennetiedon jalostaminen sekä lokitiedon kerääminen ja jalostaminen olivat helppoja toteuttaa. Työn osana evaluoitiin myös kahta kaupallista ratkaisua, jotka eivät toteutusaikana olleet riittävän kypsiä halutun toiminnallisuuden toteuttamisekseen. Vasta työmme jo päätyttyä toinen kaupallinen tuote sai päivittyneen dokumentaation perusteella sopivan integraatiorajapinnan, jolla tämän työn toteutus olisi voinut olla mahdollinen.

Ratkaisussa oletetaan, että tietoliikennehälytykset kulkevat käsittelijöille itsenäisinä lokiriveinä. Tämä oletus yksinkertaisti rakennettua ratkaisua, koska jalostaminen voidaan tehdä lokitietojen käsittelyyn suunnitelluilla välineillä. Hyvin nopeasti havaittiin, ettei tietoliikenteen monitorointi ole ongelmanratkaisua tukevaksi ratkaisuksi yksinään riittävä. Muun lokitiedon sisällyttäminen tulee hyvin nopeasti tarpeelliseksi, jos monitoroinnista halutaan saada riittävästi normaalitoimintaa tukevaa toiminnal-

lisuutta, katso kuva 30. On kuitenkin hyvä ymmärtää, ettei tämä tarkoita kaiken kattavan lokienhallinnan (SIEM, Security Information and Event Management) rakentamista, vaan valikoitujen lokilähteiden avulla voidaan saada taloudellisella tavalla riittävä näkyvyys järjestelmän ja sen komponenttien toimintaan.

Tämän ratkaisun työkaluksi valikoituivat

- LogStash: keräys-, muokkaus- ja tallennussovellus
- ElasticSearch: tietokanta sekä etsintä- ja analysointimoottori
- Kibana: käyttöliittymä ElasticSearch-moottoriin.



Kuva 30. Periaatekaavio tiedonjalostuksen toteutuksesta tislauskolonniprosessissa. Automaatiopäällikkö tarkoittaa henkilöä, joka etsii vikaa järjestelmästä ja jolla on riittävä tekninen osaaminen niin prosessin kuin tietoliikenteen osalta. Siniset viivat ovat tietoliikennemonitoroinnin liikennettä, violetit lokitietoja, musta ja punainen ovat tapauskohtaista integraatiota.

9.3.1.1.1 Positiotiedon lisääminen

Positiotieto on aina löydettävissä automaation suunnitteludokumentaatiosta. Automatisointi vaatii suunnitteludokumentaation olemassaoloa sähköisessä muodossa

ja jalostusta tekevän järjestelmän saatavilla. Tislauskolonnin suunnittelutieto on Excel-muodossa, joten hälytyksen rikastamiseksi tarvittiin tapa lisätä metatietoa hälytysriviin. Lisäysten tavoitteena on mahdollistaa hakeminen Kibana-käyttöliittymässä suoraan positionimillä sekä tukea hälytysten käsittelyä automaatio-organisaatiossa. Lisäykset tehtiin ajansäästön vuoksi rakentamalla manuaalisesti LogStash-konfiguraatio, joka teki tarpeelliset metatietolisäykset sekä poisti lokitietojen siirron ketjutuksesta aiheutuvia ylimääräisiä aikaleimoja.

Positiotiedon avulla on mahdollista esimerkiksi hälytysviestistä:

From: hälytysjärjestelmä@yritys.com
To: automaatiopäivystys@yritys.fi
Date: 2017-02-28T00:01:02 EET-EST
Subject: Security event report
Event: telnet connection to ip address 10.0.0.1 port 502

jalostaa alla oleva automaatio-organisaatiolle toimitettava viesti:

From: hälytysjärjestelmä@yritys.com
To: automaatiopäivystys@yritys.fi
Date: 2017-02-28T00:01:02 EET-EST
Subject: Tietoturvapoikkeamaraportti
Event: terminaaliyhteys MODBUS-porttiin prosessiasemalla PCS prosessialueella PROCESSAREA3.

Samoin Kibana-hakutyökalussa voidaan suorittaa esimerkiksi haku:

```
position:PCS (position:PROSESSAREA3 tags:MODBUS)
```

jonka avulla päästään lokitietomassassa helposti oikean tyyppisiin tapahtumiin ja voidaan nopeasti tutkia, mitä muita tapahtumia hälytysajan lähettyviltä löytyy.

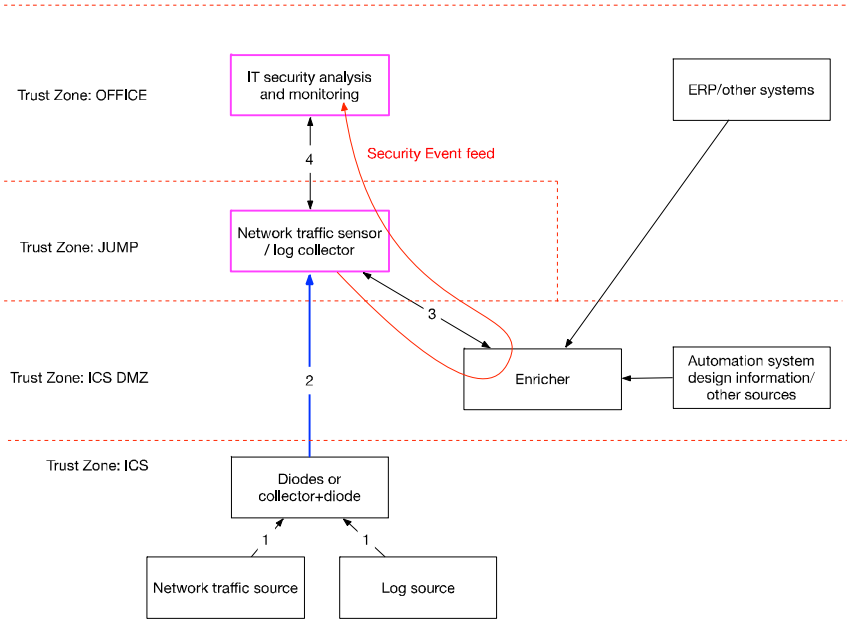
Jalostettu viesti on huomattavasti nopeampi käsitellä automaatio-organisaatiossa, koska sen sisältämä tieto on normaalia automaatiojärjestelmän terminologiaa. Lisätyn metatiedon avulla voidaan välittää mielekkäästi tietoa automaatio-IT-rajapinnassa, koska molempien päivittäisessä työssään käyttävä termistö on sisällytetty jokaiseen hälytykseen.

9.3.1.2 Integraatio yrityksen järjestelmiin

Monitoroinnin käyttöönotossa on aina varmistuttava, ettei monitorointi kuormita tai muulla tavalla vaaranna olemassa olevaa automaatiojärjestelmää. ISA/IEC 62443-standardissa on käsite *trust/security zone*, jolla tarkoitetaan tietyn turvallisuustason verkkoaluetta. IT-terminologiassa tällaisia ovat esimerkiksi DMZ (Demilitarized

Zone) ja toimistoverkko, joilla on erilaiset turvallisuustarpeet. ISA/IEC 62443 -standardissa myös jokaisella ISA95:n kerroksella on oma turvallisuustasonsa ja suunnitteluperiaatteena on, ettei minkään tason yli ole mahdollista liikennöidä ilman tietoturvakontrolleja.

Monitoroinnin toteuttamisessa on pidettävä huolta, ettei yllä kuvattua suunnitteluperiaatetta rikota eikä automaation kannalta vähäisemmältä turvallisuustasolta ole mahdollista vaarantaa korkeamman turvallisuustason toimintaa. Seuraavassa kuvassa esitetään yksi mahdollinen riittävän turvallinen toteutustapa. Soveltuva toteutusmalli riippuu siitä, miten eri toiminnallisuuksien kehittäminen ja vastuu on toteutettu yrityksessä.



Kuva 31. Tietoturvamonitoroinnin toteutus siten, että ei vaaranneta automaatiojärjestelmän luotettavuutta ja turvallisuutta. Suojausalueet (Trust Zone) kuvaavat eri turvallisuustason verkkosegmenttejä. ICS-verkosta kerätään tietoliikennetietoa ja lokitietoa (1), joka kuljetetaan datadiodin läpi (2) tietoliikennesensorille/lokienkeruuseen. Tieto jalostetaan automaation suunnittelutiedolla (3) ja toimitetaan tietoturvamonitoroinnista vastaavalle toimijalle (4).

Eräs merkittävä ongelma kaikessa automaatiojärjestelmien monitoroinnissa on väärät hälytykset. Myös tietoliikenteeseen ja tietoturvaan liittyvien väärien hälytysten määrä on pystyttävä pitämään mahdollisimman pienenä, jotta hälytykset otetaan vakavasti eikä niitä kytketä pois päältä. Väärien hälytysten vähentämisessä on hyvä hyödyntää olemassa olevaa tietoa. Yksi tapa on yo. kuvassa esitetty ”ERP/other

systems” -toiminnallisuus, joka voi olla esimerkiksi integraatio työlupajärjestelmään. Tietoa luvallisista huolloista voidaan lisätä päätöksenteon tueksi ja vähentää sen avulla vääriä hälytyksiä.

9.3.2 Yhteenveto

Mielekäs automaatiojärjestelmän monitorointiratkaisu tukee vahvasti automaatio-organisaation päivittäisen toiminnan ongelmanratkaisua ja IT- ja automaatiohenkilöstön kommunikaatiota. Automaatiojärjestelmä on hyvä kohde tietoliikennemonitoroinnille, koska suurin osa tietoliikenteestä on suunniteltua ja perustason rakentamiseksi voidaan hyödyntää automaation suunnittelutietoa. Tietoliikenteestä tehtävä monitorointi ei kuitenkaan ole riittävä, eikä perinteinen IP-tason tietoliikenteen seuranta ole riittävä automaation tietoturvaongelmien havainnoimiseksi.

Riittävä taloudellinen hyöty tietoturvamonitoroinnista saavutetaan lisäämällä hälytysviesteihin automaatiojärjestelmän suunnittelutietoa (metatietoa) sekä integroimalla relevanttia tietoa yrityksen muista järjestelmistä osaksi ongelmanratkaisua. Metatiedon lisäämisratkaisu on pilotoitu TTY:n ASECyberLab-ympäristössä ja todettu toimivaksi. Toteutuksen rakentamisessa ensiarvoisen tärkeää oli automaatiojärjestelmätoimittajan tuki.

Johtopäätöksenä voidaan todeta, että tietoturvamonitoroinnin käyttöönotto yksinomaan tietoturvasyistä ei tule olla ainoa uuden palvelun käyttöönoton peruste. Monitorointia tulee kehittää havainnoimaan ja paikantamaan myös muita verkon virhetilanteita sekä toimimaan yhdessä asiakkaan automaatio-organisaation kanssa.

KYBER-TEO-hankkeen automaatiomonitoroinnin kehittämisen tuloksena on havaittu tärkeimpinä seuraavat muutostarpeet klassiseen tietoturvamonitorointiin nähden:

- hälytysviestien toimittaminen sekä operointihenkilöstölle että automaatiojärjestelmän ongelmanratkaisua tekeville henkilöille
- osaprosessi- ja positiotietojen sisällyttäminen osaksi hälytysviestejä ja raportointia
- automaation tietoliikennettä ja komponentteja häiritsemätön toteutus
- integraatio muihin yrityksen tietojärjestelmistä saataviin tietoihin väärien hälytysten vähentämiseksi.

Esitetyt ratkaisut on testattu oikeassa teollisuusympäristössä ja todettu ne toimiviksi. Ratkaisujen vieminen tuotantoon vaatii merkittävää tukea ja yhteistyötä automaatiojärjestelmätoimittajan, tietoturvapoikkeamien havainnoinnista vastaavien ja automaatio-organisaation kesken.

9.4 Referenssit

[FIREEYE]: https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf

10. Poikkeaman sattuessa – Yhteistoimintamalli

Viime vuoden kuluessa mm. erilaisten lehtien toimitukset ovat heränneet yhteiskunnan mahdollisiin kyberturvallisuusongelmiin ja kysyvät, mikä on se pahin skenaario. Seuraavassa kuvataan lyhyesti eräs pelottava vaihtoehto. Useimmiten yrityksellä tai sen kumppanilla on vain muutamia ICT-tekniikkaa hyvin hallitsevia automaatioammattilaisia, yksilöitä joita välttämättä tarvitaan palauttamaan kriittiset toiminnot normaaleiksi todellisissa hätä- tai häiriötilanteissa.

Mitä yrityksen tarjoamalle kriittiselle palvelulle tapahtuu, jos automaatiojärjestelmää ylläpitävän yksilön työasema ja samalla hallintatunnukset (*admin/root*) onkin saatu hyökkääjän haltuun? Alussa tunkeutuja ainoastaan huomaamattomasti kerää tietoa työasemalla tehdystä hallintatoiminnasta ja vaivihkaa hieman sabotoi varmuuskopiotoimintoa (varmuuskopioiden toimivuutta ei aina testata). Yllättävä haitanteko toteutetaan vasta 2 kk jälkeen salakirjoittamalla kaikki ko. työaseman saavuttama data (ml. verkkolevyt ja pilvipalvelut).

Miten tästä palaudutaan ja miten tällaiseen tilanteeseen varaudutaan? Palautuminen ei tulisi olemaan helppoa ja voisi kestää useita päiviä. Jotta tällaiseen tilanteeseen ei koskaan päädyttäisi on ensiarvoisen tärkeää, että rikollinen henkilöstön ja järjestelmien tiedustelu esim. verkon sisällä tai yksittäisessä työasemassa kyetään havaitsemaan.

Joku voi tietysti väittää, että tällainen kohdistettu hyökkäys ei ole realistinen skenaario. Valitettavasti verkkorikollisuuden käytettävissä olevat kyberpalvelut ja niiden kustannukset ovat kuitenkin kehittyneet erittäin huolestuttavaan suuntaan viime vuosina. Jo nyt kaikkiin internetin kautta saavutettavissa oleviin järjestelmiin voi kohdistua tuhansia automaattisia skannauksia joka päivä. Satunnaisia hyökkäyksiä tehtailevat tahot eivät usein edes tiedä, mihin yrityksiin heidän hyökkäyksensä kohdistuvat. Saatu haavoittuvuustieto kuitenkin myydään eteenpäin ja rikollisten ymmärrys haavoittuvista ja rahakkaista kohteista lisääntyy koko ajan. Kun tällaisella rikollisella markkinapaikalla kysyntä kohtaa tarjonnan, rikos kohdistuu keneen tahansa. Sekä yksilöihin että yrityksiin kohdistuva rikollinen tiedonkeruu ja rahastaminen ovat jo arkipäivää.

Kyberhyökkäyksestä palautumisessa sellaiset osastot kuin ICT, automaatio, tuotanto, ylläpito, korjaus, turvallisuus jne. saattavat kukin olla keskeisessä roolissa. Tuotantojärjestelmien palauttamista toimivaan tilaan ei yleensä voida toteuttaa pelkästään esim. CSIRT (*Computer Security Incident Response Team*) -tiimin avulla, sillä kyberturvallisuuden monimutkaisiin ongelmiin erikoistunut tiimi ei yleensä tunne tarpeeksi hyvin lukuisia tuotannon eri järjestelmien ja toimintamallien yksityiskohtia. Esim. korjauksia tai tietoturvapaikkoja äkkipäätä asennettaessa automaatiojärjestelmän sovittuja muutostenhallinnan sääntöjä saatetaan rikkoa, jolloin tuotantoon aiheutetaankin testaamattomien muutosten kautta uusia häiriöitä ja näin tilanne eskaloituu hätäisten toimien seurauksena. Kyseessähän voi olla myös harhautus, jossa henkilöstö yritetään saada paniikkiin ja ajamaan järjestelmät ja täten myös tuotanto alas. Vasta myöhemmin tapahtuu varsinainen kyberhyökkäys, sillä tunkeutuminen on helpompaa murrostilanteissa kuten järjestelmien käynnistäminen tai korjaus. Tietoturvan seurantakin toimii valitettavan usein kunnolla ainoastaan normaalin tuotannon aikana.

10.1 Poikkeamahallinta

Poikkeamahallinnan toimeenpanon tärkeimpiä asioita ovat mielestämme

- automaation elinkaaren mukainen suunnittelu
- häiriöhallinnan tärkeimpien tehtävien määrittely
- luotettavien tahojen selvittäminen ja yhteistyön synnyttäminen
- vastuiden ja tehtävien jako
- kommunikointimallin määrittely
- harjoittelu.

Tietoturvahäiriöiden hallinta on parasta aikaa standardoinnin kohteena. Erityisesti ISO 27000 -sarjaa kehittävissä työryhmissä teemaa on ainakin alustavasti edelleen kehitelty. Esim. ISO/IEC 27035-1 kuvaa tietoturvahäiriöiden hallinnan periaatteita [ISO27035-1], ja seuraava kuva havainnollistaa sen esittelemiä hallintavaiheita (mukailtu lähteestä).

Kuva 32. Tietoturvahäiriöiden hallinnan vaiheet, mukailtu lähteestä [ISO27035-1].

Kokemustemme perusteella uskomme, että kehittämisen kulmakiveksi kannattaa ottaa esim. sisäisen tapahtumatiedon kerääminen ja täten ymmärryksen kasvattaminen todellisesta kybertilanteesta, omasta toimintakyvystä nykytilanteessa sekä ulkoisten ja sisäisten riippuvuuksien kartoittamisesta. Näin saadaan kehitettyä käytännöllisiä poikkeamahallinnan suunnitelmia, joiden toimivuutta tulee myös testata ja harjoitella. Kehittäminen voi olla liian myöhäistä, jos se tapahtuu ainoastaan suurten vahinkojen jo tapahduttua (esim. yrityksen maineen menettäminen pitkällisen tietomurron seurauksena). Häiriöiden vaikutukset tulisi aina pystyä hallitsemaan ja mahdollisuuksien mukaan minimoimaan.

Kyberturvallisuushäiriöiden käsittely ja hallinta kannattaa integroida tuotannon muuhun poikkeamahallintaan. Syitä tähän on mm. yrityksen osaavien omien resurssien ja ulkoistettavien voimavarojen rajallisuus sekä tarve varmistaa toimiva yhteistoiminta yrityksen ja tuotannon muun poikkeamanhallinnan kanssa.

Seuraavassa on kuvattu projektin sisäiseen kyberharjoitukseen kehitettyjä esimerkkejä kyberturvallisuushäiriöiden hallinnan ja sen kehittämisen tärkeimmistä tehtävistä.

Esimerkki. Poimintoja kyberturvallisuushäiriöiden hallinnan ja sen kehittämisen tehtävistä. Sisältö osin referenssistä [ISO27035-1].

SUUNNITTELU JA VALMISTELU -vaihe (PLAN AND PREPARE)

- Tee kriittisten järjestelmien, palvelujen ja verkostojen KARTOITUS (ml. riippuvuudet)
- Laadi häiriöhallinnan SUUNNITELMA ja TEHTÄVÄT, sitouta OSAPUOLET. Määrittele esim. kuka seuraa kybertapahtumia (*events*) ja mihin hallintavastuu siirtyy varsinaisissa häiriöissä (*incidents*)?
- Toteuta hallintasuunnitelmien TESTAUS ja HARJOITTELU. Toimivatko organisaatiot, tekniikka ja esim. tukitoiminnot yhteen kuten oletettiin?
- Luo tarvittavat SUHTEET JA YHTEYDET ulkoisiin organisaatioihin

HAVAITSEMINEN JA RAPORTOINTI -vaihe (DETECTION AND REPORTING)

- Kerää, seuraa ja hallinnoi jatkuvasti ja turvallisesti datan EHEYTTÄ ja TAPAHTUMATIETOA paikallisista ja ulkoisista ympäristöistä
- Vaadi ja seuraa myös informaatiovaikuttamisen, tietourkinnan ja hybridiuhkien HAVAITSEMISTA, ILMOITTAMISTA, ja RAPORTOINTIA

ARVIOINTI JA PÄÄTÖKSENTEKO -vaihe (ASSESSMENT AND DECISION)

- ÄLÄ TUHOA todistusaineistoa, tallenna saastuneiksi epäiltyjen järjestelmien tila turvalliseen mediaan
- ARVIOI häiriöiden vakavuus ja nykytila
- PÄÄTÄ miten tilanteeseen vastataan ja KUKA toimii

VASTEET-vaihe (RESPONSES)

- RAJOITA häiriön vaikutus minimiin esim. datayhteyksiä rajoittamalla
- Varmista UHKAN HÄVITTÄMINEN esim. palauttamalla kaikki altistuneet järjestelmät saastumattomista varmuuskopioista ja poista mahdolliset rootkitit
- Toteuta häiriöstä PALAUTUMISEN ja TOIPUMISEN toimenpiteet

OPPIMINEN-vaihe (LESSONS LEARNT)

- Pohtikaa yhdessä ja dokumentoikaa mitä häiriöstä OPITTIIN
- Toteuta tarvittavat PARANNUKSET

Häiriöhallinnan tehtäville tulisi sopia mm. tilaajan vastuut, järjestelmätoimittajan vastuut sekä kyberturvallisuuspalvelun tarjoajan vastuut. Tilaaja vastaa yleensä viime kädessä riittävän osaamisen, palvelujen ja järjestelmien hankinnasta, riskien ja muutosten hallinnan menettelyistä sekä kokonaistilanteen seurannan järjestämisestä. Automaatiojärjestelmätoimittajan vastuulla voisi olla esim. palvelusopimuksen alaisten järjestelmiensä haavoittuvuus- ja tapahtumaraportointi, ongelmatilanteiden tutkinta tarvittaessa, tarvittavien korjausten tekeminen, testaus ja asentaminen sekä esim. palautusjärjestelmien ylläpito ja toiminnan seuranta.

Olemme korostaneet selkeää työnjakoa ja yhteistoimintaa yhtenä tärkeimpänä onnistumisen elementtinä. Niinpä seuraavassa esittelemme yhdessä kehittämämme yhteistoimintamallin kyberhäiriöiden hallintaan.

10.2 Teollisuusautomaation häiriöiden yhteistoimintamalli

Yksinkertaisista osista rakennetut laitteet ja järjestelmät toimivat luotettavasti. Sovelsimme projektissa tätä yksinkertaisten elementtien periaatetta kyberhäiriöiden hallintamallin kehittämiseen. Yllättäen tapahtuvan nopean kyberhyökkäyksen alla psyykkinen paine kasvaa, ja ihmisen normaali reaktio on paniikinomainen tila, joka yleensä johtaa huonoihin päätöksiin. Yksinkertainen kaava tapahtumiin vastaamisessa toimii, minkä vuoksi teollisuusyrityksillä tulisi olla valmiiksi suunniteltu ja harjoiteltu yhteistoimintamalli mahdollisten kyberhyökkäysten varalta.

Tämän vuoksi olemme kehittäneet hierarkkisen mallin automaation kyberhäiriöiden hallitsemiseksi. Malli muodostuu viidestä eri tasosta:

- mahdollisen kyberhäiriön huomaaminen
- tapahtuman tutkiminen ja luokittelu
- johdon kommunikointi ja koordinointi
- lievennys, vastatoimet ja palautuminen
- mahdolliset opit ja parannukset.

Näihin tasoihin jaottelu mahdollistaa muun muassa

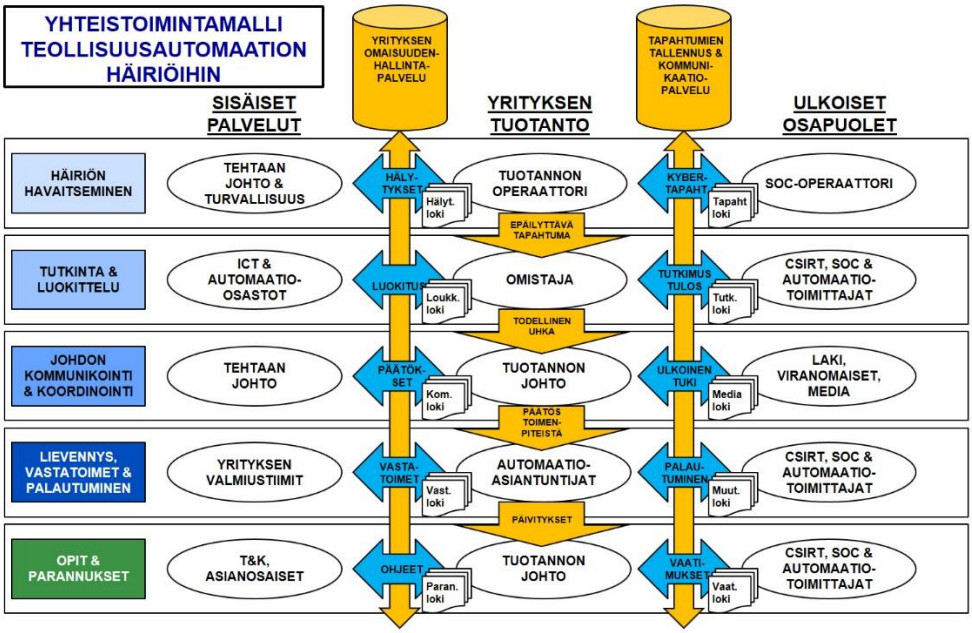
- mahdollisuuden määritellä ja hienosäätää tarkasti, millä perusteella hälytys annetaan eri tasoilla eteenpäin
- sen, että muilta tasoilta tuleva tuki helpottaa päätöksenteossa
- vakavassa tapauksessa mahdollisuuden työskennellä itsenäisesti.

Organisaatioille määritimme kolme eri kategoriaa: sisäiset palvelut, tuotanto ja ulkoiset osapuolet (partnerit). Kategoriat voivat sisältää useita eri osastoja, palveluita tai muita yrityksiä. Esimerkki on esitetty seuraavassa kuvassa.

Organisaatio	Ryhmän tarkoitus	Osaamisen laajentamisen tarpeita
Sisäiset palvelut		
Tehtaan johto	Vastaa kokonaisvaltaisesti tehtaan toiminnasta ja turvallisuudesta	Syvemmän kokonaiskuvan ymmärtäminen
Tehtaan turvallisuusosasto	Vastaa tehtaan turvallisuudesta	Tietoisuus kyberturvallisuuden tilasta
ICT-tuki	Ylläpitää ja kehittää ICT:tä	Ymmärtää tuotannon jatkuvuuden vaatimukset
Automaatiokehitys	Kehittää ja ylläpitää automaatiota	Ymmärtää riippuvuudet ICT:stä
Tuotekehitys	Tekee kehitysprojekteja	Tuntea paremmin alustan haavoittuvuudet
Tuotanto		
Operaattori	Ajaa tuotantoa	Huomata kyberpoikkeavuudet tuotannossa
Omistaja	Huolehtii omaisuudesta	Ymmärtää häiriöhallinnan haasteet
Tuotannon johto	Johtaa tuotantoa	Nähdä entistä laajempi kokonaiskuva
Automaatio-osaaja	Korjaa automaation vikoja	Ymmärtää kyberhaavoittuvuudet
Partnerit		
SOC-palvelun operaattori	Ajaa ja hallinnoi SOC-toimintoa	Ymmärtää myös tuotantojärjestelmää
CSIRT	Tutkii kyberhyökkäyksiä	Ymmärtää myös tuotantojärjestelmää
Automaatiotoimittajat	Ylläpitää ja kehittää automaatiota	Ymmärtää myös ICT-haavoittuvuudet
Laki, media	Auttavat maineen ylläpitämisessä julkisuuteen	Ymmärtää kyberturvallisuuden perusteet

Kuva 33. Esimerkki organisaatioiden ryhmittelystä: sisäiset palvelut, tuotanto ja ulkoiset osapuolet sisältävät erilaisia ryhmiä.

Seuraavassa kaaviossa on tarkemmin esitetty kehittämämme malli automaation kyberhäiriöiden hallitsemiseksi teollisuusyrityksessä.



Kuva 34. Kehittämämme yhteistoimintamalli automaation kyberhäiriöiden hallitsemiseksi teollisuusyrityksessä.

Häiriön havaitseminen -tasolla tuotanto ja sisäiset palvelut ovat vastuussa siitä, että automaatiojärjestelmien viimeisimmät konfiguraatiotiedot ovat aina päivitettynä yrityksen omaisuudenhallintapalveluun. Näiden tietojen avulla luotettu SOC-palveluoperaattori voi tarvittaessa tarkistaa, mitkä ovat senhetkiset haavoittuvimmat osat automaatiojärjestelmässä. SOC-palvelujen tulee myös tunnistaa mahdollisia kyberturvallisuusloukkauksia vertailemalla aiempaa tunnettua pohjatietoa ja eri sensoreista tulevaa tietoa.

Mikäli ylimmällä tasolla todetaan, että jokin epäilyttävä tapahtuma vaatii lisätutkintaa, lähetetään luottamuksellinen tutkintapyyntö *tutkinta ja luokittelu* -tasolle. Tällä tasolla ICT- ja automaatio-osastot arvioivat, millaisia vaikutuksia kyseessä olevan riskin toteutumisella olisi tuotannolle. Pyydettäessä myös ulkoiset partnerit, kuten SOC, CSIRT ja automaatiojärjestelmätoimittaja, tutkivat (yhdessä) tapahtuman yksityiskohtia ja pyrkivät varmistamaan, onko uhka todellinen vai väärä hälytys. Ulkoistetusti tutkitut tapaukset tulee aina kirjata luottamukselliseen kommunikaatiopalveluun. Mikäli hälytys todetaan oikeaksi, vaikutukset kriittisille järjestelmille arvioidaan ja tapahtumatiedot kommunikoidaan johtotasolle.

Johdon kommunikointi ja koordinointi -taso päättää lopulta, miten hälytyksen aiheuttaneen uhkan kanssa toimitaan. Tehtaan johdon vastuulla on päättää, tuleeko määrätä ylimääräinen tuotantokatkos (epätoivottua) ja mitä vastatoimia ja palautuksen

toimenpiteitä tehdään. Vastatoimenpiteille tulee myös määritellä maksimivaikutukset eli päättää esim., millä tuotantoalueilla järjestelmäkatkoksia saa tulla ja mikä niiden vaikutus tuotantoon saa olla. Olennaista on myös keskustella, missä määrin tarvitaan ulkoisia lakineuvoja, tarvitseeko tapauksessa neuvotella viranomaisten kanssa, halutaanko tapahtumasta tehdä rikosilmoitus ja kannattaako tiedottaa mediaa. Kaikki tehdyt päätökset tulee myös kirjata.

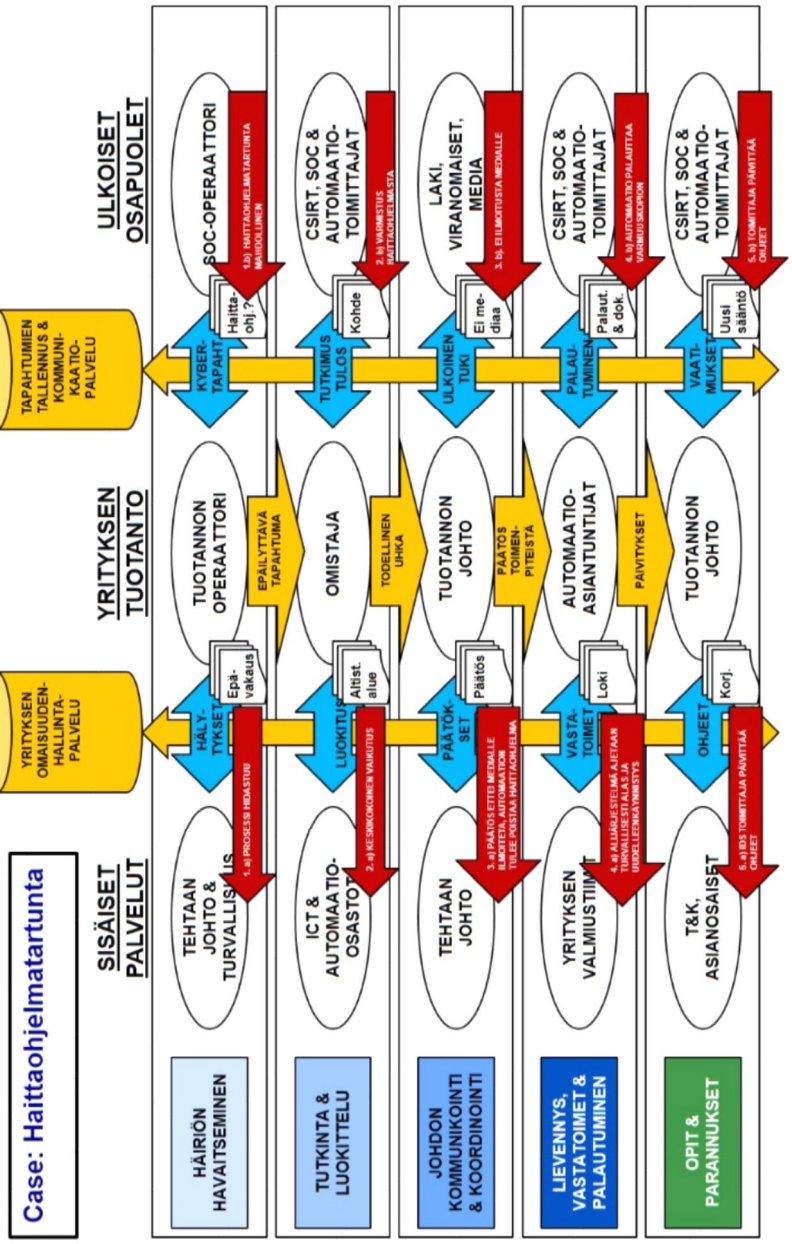
Lievennys, vastatoimet ja palautuminen -tason tulee toimia läheisessä kommunikaatiossa johdon kanssa, jotta nähdään mahdollisimman tarkasti vastatoimenpiteiden kokonaisvaikutus ja tilannekuva. Vastatoimien pitäisi perustua testattuun tietoon tai todella hyvin perusteltuun päätökseen. Sellaisia välittömiä vastatoimia pitäisi erityisesti välttää, joilla saattaa olla erityisen laaja tai merkittävä vaikutus nykyisiin järjestelmiin. Myös järjestelmän palauttaminen tulee testata jo etukäteen turvallisella hetkellä, jotta voidaan varmistaa palautuksen oikea toiminta. Käytännössä uhkan lopullinen poistaminen voi olla hyvin vaativaa ja erityisasiantuntijoiden käyttö onkin suositeltavaa. Kaikki tämän tason toimenpiteet tulee myös lokittaa ja dokumentoida huolellisesti.

Alin, mutta todella tärkeä vaihe on jatkuva parantaminen. Kun uhkaava tilanne on saatu hallintaan, käydään yhdessä läpi, miten yhteistoimintaa voitaisiin jatkossa parantaa. Kerättävän kokemuspohjaisen tiedon ja lokitiedon perusteella voidaan tarvittaessa kehittää uusia vaatimuksia, jotka takaavat eri tasojen tehokkaamman toiminnan ja paremman yhteistoiminnan uusia uhkia vastaan. Yhteisillä harjoituksilla testataan uusia ohjeita ja toimintatapoja käytännössä ja päivitetään ohjeet.

Malli sisältää maininnat kahdesta erityyppisestä työkalusta, joita voitaisiin käyttää mm. kommunikoinnin tukena. *Omaisuudenhallintapalvelun* avulla voitaisiin seurata tai jopa ylläpitää kutakin järjestelmää, tai vähintään tulisi ylläpitää turvallisesti saavutettavissa olevaa konfiguraatio- ja tilatietoa kaikista käytössä olevista laitteista. *Tapahtumien tallennus ja kommunikaatiopalvelussa* olisi ainakin kaksi toimintoa; tapaustiedon tallennus koko elinkaaressa, sekä esimerkiksi tapahtuman ja hälytystiedon kommunikoinnin tukeminen avainhenkilöiden välillä eri organisaatioissa. Ohjelman tulisi mahdollistaa myös tapausten järjestelmällinen luokittelu, jotta esimerkiksi järjestelmien huoltotarvetta voitaisiin helposti seurata. Myös tapausten vaikutuksia yrityksen maineeseen tai vaikutuksia ulkopuolisiin olisi tarpeen jotenkin seurata.

10.2.1 Haittaohjelmaesimerkki

Jotta malli olisi toimiva, tulisi sen soveltua moniin erilaisiin käyttötapauksiin. Seuraavassa esimerkissä olemme esittäneet tapauksen, jossa mallia käytetään haittaohjelmatartunnasta alkaneen häiriön hallintaan.



Kuva 35. Haittaohjelma-käyttötapaus yhteistoimintamallissa.

Kuvan 35 haittaohjelmatapauksessa kommunikaatio ja yhteistoiminta voisi edetä seuraavalla tavalla:

Häiriön havaitseminen: Tuotannon operaattori huomaa, että tuotantojärjestelmästä on tullut jollain lailla epävakaampi. Se vastaa komentoihin hitaammin kuin ennen, ja joitain sovelluksia joutuu käynnistämään uudelleen. Operaattori kirjaa muuttuneen käytöksen omaisuuden hallintapalveluun. Myöhemmin SOC-palvelun operaattori lukee lokia ja tutkii kyseessä olevan järjestelmän verkkoliikennettä tarkemmin. Verkkoliikenteessä näkyy epäilyttävä uusi tiedonsiirto toimistoverkkoa kohti, ja uusi tieto lisätään *tapahtumien tallennus ja kommunikaatiopalveluun*. Tuotannon operaattori saa vastaavasti tiedon uudesta tapahtumasta ja pyytää laitteen ylläpidosta vastaavaa henkilöä tutkimaan tapausta tarkemmin.

Tutkinta & luokittelu: Myös ICT:n ja automaation vastaavat omistajat saavat tiedon epäilyttävästä tapahtumasta. He huolehtivat epäiltyjen järjestelmien nykytilan tallentamisesta turvalliselle tutkintamedialle (jos näin ei ole jo tehty) ja alkavat tuotantojärjestelmään koskematta analysoida omiin tutkintatarkoituksiin varattuja kopioita lokeista (ja muita tietoja järjestelmän käyttäytymisestä) yhdessä järjestelmän toimittajan ja esim. CSIRT-tiimin kanssa. Analyysissä yritetään saada selville mm., onko kyseessä todellinen ongelma, mitkä kohteet ovat mahdollisesti tartunnan saaneet ja mitkä tuotantoalueet ovat mahdollisesti vaarassa (erityisesti niiden kriittiset järjestelmät). Lopputulokset dokumentoidaan sähköisesti käyttäen luottamuksellisia kommunikointityökaluja. Jos todetaan, että hyökkäys tai tartunta oli todellinen, tehdään hälytys ja tuotannon johtoa pyydetään päättämään, miten tapaukseen vastataan.

Johdon kommunikointi ja koordinointi: Tuotannon johto saa hälytyksen, ja järjestää tapaamisen tehtaan johdon ja mm. automaatio-osaston kanssa. He päättävät mm. lievennyksen ja vastatoimien tekemisestä, kuka ne tulee tekemään, mille järjestelmille ja milloin. Esimerkin tapauksessa automaatiojärjestelmätoimittaja tilataan poistamaan haittaohjelma palauttamalla saastumattomat varmuuskopiot, mutta ainoastaan tuotannon aikatauluihin parhaiten sopivalla hetkellä. Tässä tapauksessa päätetään myös, että mediaa ei tiedoteta, koska tapauksella ei ole ollut ulospäin näkyviä vaikutuksia. Päätökset dokumentoidaan työkalujen avulla, sisältäen myös tiedot tapauksen aikana tehdyistä työtilauksista.

Lievennys, vastatoimet ja palautuminen: Vastuussa oleva automaatio- tai ICT-tiimi saa kommunikointityökalun kautta tiedon päätöksestä ja tapahtuman yksityiskohdista, sekä mahdollisesta työtilauksesta. Johdon päätösten ja ohjeiden mukaan saastumattomat varmuuskopiot palautetaan ja järjestelmä puhdistetaan ja käynnistetään uudelleen toimittajan tuella ja ohjeiden mukaisesti. Tietoturvahenkilöitä kannattaa tarvittaessa käyttää puhdistamiseen ja sen varmistamiseen, että erilaiset turvallisuushaavoittuvuudet on otettu riittävästi huomioon ja myös että hyviä tietoturvakäytäntöjä noudatetaan. Kaikki tehdyt työt dokumentoidaan huolellisesti työkalujen avulla.

Opit ja parannukset: Esimerkkitapauksessa huomataan, että ohjeistusta ja hyökkäyksen havaitsemisjärjestelmän säännöstöä tulisi parantaa. Niiden päivittämisestä päätetään ja siitä tiedotetaan eri osapuolille.

10.2.2 Johtopäätökset

Tarvitsemme kiihkeästi käytännöllisiä yhteistoimintamalleja nykypäivän jatkuvasti monimutkaistuviin kyberhyökkäyksiin vastaamiseksi. Keskusteluun tulee saada mukaan eri osapuolet, kuten tuotannon operaattorit ja johto, ICT- ja automaatiovastaavat, automaatiojärjestelmätoimittajan asiantuntijat, ulkoiset SOC-operaattorit jne. Kun kommunikoinnille ja yhteistoiminnalle on määritelty malli, on yritysten helpompaa kehittää omia palautumissuunnitelmiaan sekä järjestää kyberharjoituksia myös eri toimijoiden kesken.

Ainakin mallin pääkohdat ovat jo käytössä Suomessa, joten mallin voidaan arvella olevan toimiva. Tarvitsemme kuitenkin jatkuvaa yhteistyötä, jotta mallin yksityiskohtia voidaan hioa tarkemmaksi ymmärtämällä paremmin eri yritysten rajoitteet. Tulevaisuudessa haluaisimme siis kehittää ja soveltaa tätä mallia edelleen yhdessä eri teollisuusalojen kanssa.

10.3 Referenssit

[ISO27035-1] ISO/IEC 27035-1, Informaatioteknologia. Turvallisuustekniikat. Tietoturvahäiriöiden hallinta. Osa 1: Tietoturvahäiriöiden hallinnan periaatteet (luonnoksen käännös).

Tulevaisuuden tarpeet

Huoltovarmuuskriittisten yritysten kyberturvallisuus

KYBER-TEO on ollut osa Huoltovarmuuskeskuksen hankekokonaisuutta kriittisen elinkeinoelämän suojaamiseksi kyberuhkatilanteiden varalta. Yhteiskunnan toimintojen verkottuessa ja digitalisoituessa tarve kyberturvallisuuden parantamiseksi kuitenkin korostuu entisestään. Kehitykseen vastatakseen Huoltovarmuuskeskus on valmistellut jatko-ohjelmaa, joka tähtää kriittisen elinkeinoelämän suojaamiseen myös vakavien ja laajojen kyberuhkatilanteiden varalta.

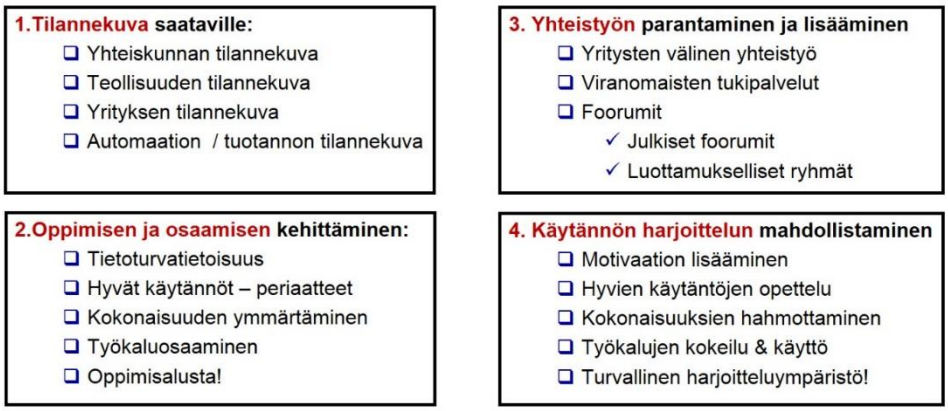
Tunnistettuja tarpeita

Kyberturvallisuuden jalkauttaminen riittävässä laajuudessa ja syvyydessä vaatii jatkuvaa pyrkimystä merkittävimpien avaintoimijoiden tunnistamiseen, toimijoiden sitouttamista yhteisesti määriteltyihin tavoitteisiin sekä parempaan yhteistoimintaan.

Automaation kyberturvallisuuden kipupisteitä Suomessa ovat mm.:

- Kyberuhkien määrä ja laajuus kasvavat nopeasti.
- Sektoreiden perusvalmiudet ovat riittämättömiä.
- Teknologinen murros ja teollinen internet aiheuttavat yllättäviä seurauksia.
- Järjestelmien elinkaarenaikainen ylläpito, seuranta ja valvonta ovat riittämättömiä.
- Kyberturvallisuuden yhteistyö ei toimi riittävän laajapohjaisesti.
- Kyberturvallisuusosaaminen on riittämätöntä.

Seuraavassa kuvassa on näkymä automaation kyberturvallisuuden kehittämisen yleisiin tarpeisiin:



Kuva 36. Kyberturvallisuuden kehittämisen yleistarpeita.

Johtopäätökset ja jatkotyö

Johtopäätökset

Jatkuvuus edellä – Valtavasti lisääntyneestä automaation ja ICT:n integraatiosta huolimatta automaatiojärjestelmien käyttötarkoituksella ja suunnitteluperiaatteilla on edelleen suuria eroavaisuuksia verrattuna yleisten IT-järjestelmien vastaaviin ominaisuuksiin. Yleisesti ottaen automaatiojärjestelmään ei saa tulla mistään syystä tuotannon aikaisia häiriöitä, jotka voisivat johtaa esim. automaatio-ohjauksen katkeamiseen tai väärään ohjaukseen. Ohjauksen häiriöthän voisivat johtaa mittaviin tuotannon menetyksiin, tuotantojärjestelmien tuhoutumiseen, henkilövahinkoihin, tai jopa vakavaan yhteiskunnan kriisiin. IT-järjestelmiä ja niiden ylläpitoa ei yleisesti ottaen ole suunniteltu täysin häiriöttömään reaaliaikaiseen toimintaan, joten IT-käyttöön kehitetyt tietoturvamenettelytkään eivät sellaisenaan suoraan sovellu automaation kyberturvaamiseen. KYBER-TEO-projekti tarvittiin juuri tämän vuoksi – lisäämään kyberturvallisuustietoisuutta sekä kokeilemaan ja kehittämään käytännön ratkaisuja, joilla automaation jatkuva oikea toiminta voidaan varmistaa myös kyberturvallisuusuhkia vastaan.

Teollisuuslähtöisesti – Tuotannon tietoturvamenettelyt tai niihin liittyvät tukitoimet eivät siis saa vaarantaa tuotannon jatkuvuutta missään olosuhteissa. Tämä edellyttää teollisuuden kriittisten järjestelmien tunnistamista, hyvää ymmärrystä niiden toiminnasta ja toimintaedellytyksistä sekä riippuvuuksista muista järjestelmistä ja palveluista, tietoturvallisuus mukaan lukien. KYBER-TEO-projektissa kyberturvallisuuden kehittäminen tehtiin teollisuuden tarpeista lähtien. Haluttiin yhdessä tunnistaa ja ratkaista teollisuustuotannon ja sen käyttämän automaation kyberturvallisuusongelmia tavoilla, jotka vastaavat tunnustettuja yleisen turvallisuuden, saatavuuden ja reaaliaikaisuuden vaatimuksia.

Uhat kasvavat – Tulevaisuuden haasteet ovat entistä vaikeampia. Kehittyneet kyberturvallisuusuhat näyttäisivät ajan myötä tunkeutuvan tuotantoyksiköiden ja -verkkojen sisäpuolelle odottamaan sopivaa hetkeä esim. laittomalle kiristykselle, luottamuksellisen tiedon varastamiselle tai tuotannon sabotaasille. Rikolliset käyttävät omia markkinapaikkojaan, joista esim. kiristys- ja haittaohjelmia voi ostaa hal-

valla, eikä esim. hyökkäystekniikoita tai huijausprosesseja tarvitse itse hallita. Valitettavasti myös hyvin kehittyneitä ja jopa räätälöityjä hyökkäyksiä voi tilata haluttuja uhreja vastaan. Jotain on siis pakko tehdä, mutta mistä turvaaminen pitäisi aloittaa? Yrityksen omiin uhkiin perehtymisestä on hyvä aloittaa.

Tietoisuutta lisää – Yhteisömme hyvinvoinnin säilyttäminen vaatii yhä kiihkeämpää kyberturvallisuustietoisuuden lisäämistä, joten tätä tehtiin varsinkin projektin viimeisenä vuonna kymmenissä tilaisuuksissa ja lehdissä, terveydenhuolto mukaan lukien. Vuosi 2016 huipentui osaltamme 14. joulukuuta kutsuvieraille pidetyssä tulosten esittelytilaisuudessa, johon osallistui yli 100 alan asiantuntijaa ja johtajaa. Lisäksi tämä julkaisu toivottavasti lisää tietoisuutta myös laajemmin yhteiskunnassa. Tiedottamisella yritämme samalla motivoida käynnistämään tarvittavat pohdinnat ja kehityshankkeet myös niissä yrityksissä, jotka eivät ole vielä riittävästi tiedostaneet kyberturvallisuuden jatkuvan kehittämisen tarvetta omassa toiminnassaan. Pyrkimyksemme on ollut, että laajamittaisempi kyberturvallisuuden parantaminen tapahtuisi jo ennen vakavaa yhteiskunnan häiriötilaa, joka väistämättä syntyy, mikäli kriittisten järjestelmien ja palvelujen kyberturvallisuuden jatkuva kehittäminen jätetään huomiotta.

Työnjakoa paremmaksi – Tarvitaan yhteistä työnjakoa. Kyberturvallisuuden kenttä on kasvanut jo niin laajaksi, että edes asiantuntijat eivät enää yksin hallitse sen kaikkia osa-alueita. Kokonaisuuden jäsentämiseksi ja tehtäväkentän selkeyttämiseksi olemme yhdessä määritelleet kyberturvallisuuden päätoimijat ja -tehtävät automaation koko elinkaaressa. Turvallisuuden kehittäminen käynnistyy ja kehittyy ainoastaan tilaajasta eli automaatiota hyödyntävästä yrityksestä lähtien. Aluksi määritellään kriittisimmät suojattavat alueet ja kohteet sekä näille sellaiset kyberturvallisuusvaatimukset ja ohjeet, jotka eivät vaaranna jatkuvuutta. Kehitetään ja testataan toimivat peruskonseptit, jotka muodostavat rungon koko tuotannon kyberturvaamiselle. Tulokset ja turvallinen toimintatapa tiedotetaan kaikkialle tuotantoverkostoon ja jaetaan toimijoille vastuut ja tehtävät. Tuotannossa riskejä arvioidaan säännöllisesti ja valvotaan toiminnan tilannekuvaa sekä kyberturvallisuuden kehittymistä.

Rajat ylittävä yhteistyö – Kyberrikollisuuden kansainvälistyminen ja uhkien kehittyminen yhä vaikeammin tunnistettaviksi voivat aiheuttaa vaaratilanteita, joita suurikaan yritys ei enää pysty ennustamaan suoraan omassa liiketoimintaverkostossaan. Tarvitaan kansallista ja kansainvälistä yhteistyötä mm. haavoittuvuus-, uhka- ja tilannetiedon kommunikoimiseksi yritysten ja viranomaisten välillä. Kansallisella tasolla koostetaan eri tietolähteistä muodostuvaa tilannekuvaa, jota jaetaan luottamuksellisesti kriittistä infrastruktuuria tuottaville ja ylläpitäville toimijoille. Tätä tehtävää hoitaa ja kehittää Viestintäviraston Kyberturvallisuuskeskus, jonka kanssa KYBER-TEO-projektilla oli toimiva yhteistyö, joka sisälsi mm. osaamistukea, jatkokehityksen pohdintaa sekä monia seminaareja ja työpajoja. Tarvittiin parempia automaation kyberturvallisuuden yhteistyöverkostoja ja niitä projektissa myös kehitettiin.

Luottamuksen rakentaminen – Kaikki rakentava yhteistoiminta edellyttää vahvaa luottamusta toiseen osapuoleen. Täytyy löytää osapuolia ja henkilöitä, joiden sanaan ja toimintaan voi luottaa pitkällä tähtäimellä. Projektin aikana vahvistui ajatus, että luottamus kehittyy parhaiten konkreettista yhteistyötä tekemällä, mm. vähittäisen yhteistyön syventämisen ja laajentamisen kautta. Aluksi voidaan lisätä yhteistyötä esim. jakamalla julkista tietoa, josta kaikki osapuolet hyötyvät lähes välittömästi, mutta ilman vaaraa oman luottamuksellisen tiedon tai maineen menettämisestä. Kun luottamusta on jo syntynyt, voidaan työstää esim. sopivaa riskitöntä projektia yhdessä jne. Luottamus alkaa olla jo varsin vahvaa silloin, kun pystytään tekemään yhteisiä pilottiprojekteja, joissa omaa tietopohjaa, kokemusta ja asiantuntijatyötä käytetään selkeästi myös toisen osapuolen hyödyksi. Tähän liittyy usein maksullisia toimeksiantoja, ja erityisesti pilotointiyhteistyö on ollut KYBER-TEO-projektin paljon hyödyntämä tapa luottamuksen edelleen kehittämiseksi. Usein tämä on vaatinut, että varsinkin tilaaja on tuntenut toimittajan jo ennalta. Projektissa syntyi ”luottamusryhmiä”, jotka todennäköisesti haluavat jatkaa ja mahdollisesti myös syventää yhteistyötään tulevaisuudessa. Tämä mahdollistaa kyberturvallisuuden skaalautuvan kehittämisen kansallisella tasolla. Tällöin vaarana saattavat olla asiattomat soluttautujat, joten myös tiedusteluun liittyvää osaamista täytyy kasvattaa.

Omin käsin tekeminen – Projektin kuluessa vahvistui käsitys, että vaikka paperilla ja suunnitelmien valossa kaikki olisi kunnossa, todellisuudessa yrityksen kyberturvallisuustilanne saattaakin olla heikko. Tämä vaikuttaisi johtuvan ainakin puutteista kyberturvallisuustestauksessa ja kyberturvallisen toiminnan käytännön harjoittelussa. Voidaan jopa väittää, että se, minkä toimivuutta ei ole käytännössä kokeiltu, sitä ei ole olemassakaan! Niinpä kehitimme KYBER-TEOssa käytännön harjoituksia, koulutusta ja teknisiä ympäristöjä sekä kyberturvallisuustestauksen (esim. VTT War Room) että *hands-on*-kyberharjoittelun tarpeisiin. Näitä kokeiltiin myös käytännössä koestamalla asiakkaiden automaatiojärjestelmiä ja testausta varten rakennettuja järjestelmäympäristöjä. Harjoitukset kantoivat hedelmää osallistujien silmien avautuessa samalla sille, miten välttämätöntä on kehittää oman toiminnan ja tuotteiden kyberturvallisuutta.

Tulokset jalkautuivat – Monet projektiin osallistuvat yritykset ovat ilmaisseet vahvasti, että mm. yhdessä pidetyt tilaisuudet ja yhdessä tehty työ ovat synnyttäneet tarvittavaa tietoisuutta, kyvykkyyksiä, osaamista, yhteistyötä ja valmiuksia sekä palveluja, joita ilman oman yrityksen ja sen automaation kyberturvallisuuden kehittäminen laajemmassa mittakaavassa olisi ollut varsin vaikeaa.

Jatkotyö

KYBER-TEOn jälkeen Huoltovarmuuskeskus on käynnistänyt Kyber 2020 -ohjelman, joka tähtää huoltovarmuuskriittisten yritysten kyberturvallisuuden merkittävään parantamiseen vuosina 2017–2020. Hanketta tehdään yhdessä yritysten, hallinnon, tutkimuslaitosten ja Kyberturvallisuuskeskuksen kanssa. Kyber 2020 -ohjelma on myös osa kansallisen kyberturvallisuusstrategian toimeenpano-ohjelmaa. Kyber 2020 -ohjelma sisältää sekä yhteiskunnan systeemisten kyvykkyyksien kehittämisen että huoltovarmuuskriittisten yritysten omien valmiuksien kehittämisen. Verkottuneista liiketoimintamalleista johtuen merkittävä osa yritysten valmiuksien kehittämistä on toimintamallien luomista ja harjoittelua kumppaniverkostoissa ja palveluntarjoajien kanssa.

Julkaisun sarja ja numero

VTT Technology 298

Nimeke	**KYBER-TEO – tuloksia 2014–2016** Julkisten tulosten kooste
Tekijä(t)	Pasi Ahonen et al.
Tiivistelmä	Kyberturvallisuuden kehittäminen edellyttää lähes aina tietoisuuden perustasoa, jotta yrityksen päättäjät ja käytännön toimijat ymmärtävät riittävästi kyberuhkien todellisista vaikutuksista ja kohdistumisesta omaan toimintaansa. Vasta tämän jälkeen yritykseen voi syntyä tarvittava vastuiden määrittely ja resursointi mm. tuotantoon soveltuvien kyberturvallisuusuhkien havaitsemiseen, torjuntaan ja ennakkovarautumiseen. Teollisuusautomaation kyberturvallisuuden kehittäminen Suomessa vaatii kaikkien toimijoiden osallistamista. Tämä johtuu mm. siitä, että kyberturvallisuuden ratkaisee lopulta "arvoketjun heikoin toimija" tai "järjestelmän huomaamaton haavoittuvuus". Turvallisen toiminnan vastuuta ei voi ulkoistaa, sillä viime kädessä tuotanto vastaa itse kaikkien tarvittavien turvamenettelyjen käyttöönotosta, käytön valvonnasta ja kehittämisestä. KYBER-TEO-projekteissa kehitettiin vuosina 2014–2016 yritysten yhteistyötä ja edellytyksiä parantaa monia erilaisia automaation kyberturvallisuuteen vaikuttavia asioita: - Alan edelläkävijäyrityksissä kehitettiin ja testattiin automaation kyberturvallisuuden kehittämisen palveluja, parhaita käytäntöjä ja ratkaisuja. - Määriteltiin kyberturvallisuuden työnjako ja tehtävät automaation elinkaaressa. - Parannettiin ammattilaisten kyberturvallisuustietoisuutta julkisten tulosten esittelytilaisuuksissa kertomalla uhkista ja seurauksista sekä varautumiseen kehitetyistä käytännöistä ja koetelluista ratkaisuista. - Kehitettiin ja koestettiin automaation kyberturvatestauksen ympäristöjä. - Kehitettiin ja koestettiin automaation kyberturvaharjoittelun ympäristöjä. - Kehitettiin ja koestettiin automaatioverkkojen kyberturvamonitoroinnin konsepteja ja menetelmiä. - Kehitettiin ja pilotoitiin automaation kyberturvallisuuden sähköistä yhteistyöfoorumia.
ISBN, ISSN, URN	ISBN 978-951-38-8541-0 (nid.) ISBN 978-951-38-8540-3 (URL: http://www.vtt.fi/julkaisut) ISSN-L 2242-1211 ISSN 2242-1211 (Painettu) ISSN 2242-122X (Verkkojulkaisu) http://urn.fi/URN:ISBN:978-951-38-8540-3
Julkaisuaika	Toukokuu 2017
Kieli	Suomi
Sivumäärä	145 s.
Projektin nimi	KYBER-TEO Kyberturvallisuuden kehittäminen ja jalkauttaminen teollisuuteen
Rahoittajat	Huoltovarmuuskeskus ja ja osallistujayritykset
Avainsanat	kyberturvallisuus, teollisuusautomaatio, tietoturvallisuus, huoltovarmuus, teollisuusyritykset, tietoisuus, mallit
Julkaisija	Teknologian tutkimuskeskus VTT Oy PL 1000, 02044 VTT, puh. 020 722 111

KYBER-TEO – tuloksia 2014–2016

Julkisten tulosten kooste

Julkaisun tavoitteena on parantaa kyberturvallisuustietoisuutta automaatiota hyödyntävän teollisuuden toimijoiden keskuudessa. Tietoisuuden lisäämisen avulla pyrimme helpottamaan kyberturvallisuuden jalkautusta käytännön toimintaan. Tällainen kehitys ei käynnisty itsestään, vaan se vaatii huolellista perehtymistä kyberturvallisuuden yleiseen kenttään, omiin erityisongelmakohtiin tuossa kentässä sekä luonnollisesti riittävää johdon sitoutumista.

KYBER-TEO-projekteissa vuosina 2014–2016 laajennettiin ja kehitettiin käytännön yhteistyöverkostoja, joiden kautta teollisuusyritykset saivat ja saavat konkreettista tukea omiin kyberturvallisuuden kehityshankkeisiinsa. Osallistuneet yritykset ilmaisivat vahvasti, että yhdessä tehty työ on synnyttänyt tarvittavaa tietoisuutta, kyvykkyyksiä, osaamista, yhteistyötä ja valmiuksia sekä palveluja, joiden avulla automaation kyberturvallisuuden kehittäminen tuli mahdolliseksi isossa mittakaavassa.

ISBN 978-951-38-8541-0 (nid.)
ISBN 978-951-38-8540-3 (URL: http://www.vtt.fi/julkaisut)
ISSN-L 2242-1211
ISSN 2242-1211 (Painettu)
ISSN 2242-122X (Verkkojulkaisu)
http://urn.fi/URN:ISBN:978-951-38-8540-3

VTT

HUOLTOVARMUUSKESKUS
FÖRSÖRJNINGSBEREDSKAPSCENTRALEN
NATIONAL EMERGENCY SUPPLY AGENCY