KYBERTURVALLISUUDEN KEHITTÄMINEN JA JALKAUTTAMINEN TEOLLISUUTEEN VUONNA 2014

KYBER-TEO 2014 -hankkeen tuloksia

HUOLTOVARMUUSKESKUS
FÖRSÖRJNINGSBEREDSKAPSCENTRALEN
NATIONAL EMERGENCY SUPPLY AGENCY

KYBERTURVALLISUUDEN KEHITTÄMINEN JA JALKAUTTAMINEN TEOLLISUUTEEN VUONNA 2014

KYBER-TEO 2014 -hankkeen tuloksia

Huoltovarmuuskeskus

Projektin ohjausryhmän puheenjohtaja,
varautumispäällikkö Tero Kauppinen

Projektipäällikkö, erikoistutkija
Pasi Ahonen, VTT Oy

www.huoltovarmuus.fi

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

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

www.vtt.fi

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

https://www.viestintavirasto.fi/kyberturvallisuus.html

Kyberturvallisuuskeskus on kansallinen tietoturvaviranomainen, joka kehittää ja valvoo viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta.

HUOLTOVARMUUSKESKUS
FÖRSÖRJNINGSBEREDSKAPSCENTRALEN
NATIONAL EMERGENCY SUPPLY AGENCY

Viestintävirasto
Kyberturvallisuuskeskus

VTT

Julkaisija: Huoltovarmuuskeskus
Teksti ja kuvitus: VTT Oy
Taitto ja paino: Erweko, Oulu
Julkaisuvuosi: 2015
ISBN: 978-952-5608-29-8 (nid.)
ISBN: 978-952-5608-30-4 (pdf)

SISÄLTÖ

SAATTEEKSI

Tero Kauppinen
Huoltovarmuuskeskus,
KYBER-TEO-hankkeen pj.

Automaatio, verkottuminen ja uudet toimintamallit leviävät teollisen toiminnan lisäksi useilla muilla toimialoilla kuten kiinteistöjen hallinnassa, vesihuollossa ja terveydenhuollossa. Liikenteenkin robotisoituminen on jo testivaiheessa.

Huoltovarmuuskeskus edistää laaja-alaista yhteistyötä teollisten toimijoiden kesken monivuotisessa **KYBER-TEO-hankkeessa**, joka on jatkoa useita vuosia kestäneelle yhteistyölle **yritysten, VTT:n, Kyberturvallisuuskeskuksen ja Huoltovarmuuskeskuksen kanssa**.

Liiketoimintalähtöisyys on keskeinen teema automaation turvallisuuden kehittämisessä. Hankkeessa on kehitetty konkreettisissa tilanteissa ja aidoissa teollisissa liiketoimintaympäristöissä käyttökelpoisia ratkaisuja, jotka voisivat olla hyödyllisiä monille muille toimijoille. Ratkaisumallit hyödyttävät alan ohjelmisto- ja järjestelmätoimittajia, palvelutarjoajia ja varsinaisia teollisia toimijoita, jotka ovat automaatiosta riippuvaisia.

Pitkäjänteistä ja hedelmällistä yhteistyötä jatketaan yritysten kanssa turvallisuuden osa-alueilla, jotka yritykset keskenään arvioivat tärkeäksi kehittää yhdessä. Teollisen internetin ratkaisut ja pilvipalvelut etenevät lähivuosina automaatioratkaisujen arkeen maailmalla ja myös Suomessa. Turvallisia toimintamalleja on pyrittävä hyödyntämään – liiketoimintalähtöisesti ja riskiperusteisesti.

YHTEENVETO

Pasi Ahonen
VTT, KYBER-TEO-hankekokonaisuuden projektipäällikkö

Tämä julkaisu on kirjoitettu Huoltovarmuuskeskuksen toimeksiannosta, ja sen kohdeyleisönä ovat kaikki teollisuuden kyberturvallisuudesta kiinnostuneet, mutta erityisesti teollisuuden ICT- ja automaatiojärjestelmien ammattilaiset, joiden työllä on vaikutusta kyberturvallisuuden toteumaan. Olen laatinut ja koostanut tämän julkaisun pääsisällön KYBER-TEO-hankekokonaisuuden vuoden 2014 osuuden valikoiduista tuloksista, jotka muodostavat toivoakseni jotakuinkin yhtenäisen, helppolukuisen kokonaisuuden. Jari Seppälä Tampereen Teknillisen Yliopiston (TTY) Systeemitekniikan laitokselta on avustanut hankkeen tutkimuksellisessa osuudessa. Kaikkia vuoden 2014 julkisia tuloksia ei sisällytetty mukaan, jotta tähän julkaisuun valitut fokusalueet, eli kyberturvallisuuden jalkautus, automaatioverkkojen kyberturvallisuuden monitorointi, sekä sopimusmallit automaatiohankinnoissa saatiin nostettua näkyvästi esiin mm. hankkeessa toteutettujen yritystapausten kautta.

Johdanto-osuudessa kuvataan ensin mm. projektijatkumo, joka edelsi nyt käynnissä olevaa (2014–2016) KYBER-TEO-projektikokonaisuutta, sekä KYBER-TEO-projektin yleisesittely. Sitten kuvataan yleisesti teollisuustuotannon kyberturvallisuuden kehityshankkeiden tavoitteita ja elementtejä mukaan lukien jatkuvuuden tavoitteet, sekä tekninen ja hallinnollinen tietoturva.

Kyberturvallisuuden jalkautus-osuudessa kuvataan aluksi työskentelymalli kyberturvallisuuden jalkauttamiseksi teollisuusyritykseen. Tämän jälkeen päästäänkin sitten jo projektissa vuonna 2014 toteutettujen yritystapausten julkisen osuuden kuvauksiin. Yritystapaukset olivat Outotecin ”Tietoturvavaatimusten jalkautus automaatiotoimituksiin”, sekä Neste Oilin ”Tietoturvaohjeistus automaatiohankintaa varten”.

Toivomme, että nämä lyhyet yhteenvedot avaavat lukijalle realistisen kuvan muutamien avainyritysten lähtökohdista, toimintaympäristönsä haasteista, saavutuksista, sekä edes hitusen siitä millaisia panostuksia tuloksiin pääseminen yritykseltä vaati. Jalkautusosuudessa kuvataan lisäksi automaatiojärjestelmien koventamisen tehtävät ja työnjako kolmen erilaisen käyttötapauksen kautta. Nämä tulokset laadittiin yhteistyössä projektin sisäisissä työpajoissa, mutta niiden hyödyntäminen haluttiin ulottaa mahdollisimman laajalle, joten yhteenveto julkistettiin pääosin tässäkin kirjasessa.

Automaatioverkkojen kyberturvallisuuden monitorointi-osuus onkin sitten hyvin yritystapaus painotteinen. Verkkomonitorointi nousi oikeastaan vasta viime vuonna suuremman kiinnostuksen kohteeksi teollisuuden puolella. Tämä johtunee siitä, että mm. erilaiset viranomaistahot ovat alkaneet vaatia myös tuotannon tietoverkkojen parempaa valvontaa ja tilannekuvan seurantaa. Toinen syy voi olla julkisuudessa esillä olleet verkkovakoilutapaukset, jotka ovat herättäneet yritysten johtoa ja asiantuntijoita tarkkailemaan myös omia verkkojaan. Tässä kohdassa kuvattuihin yritystapauksiin emme halunneet liittää tarkempaa tietoa case-yrityksistä, mm. koska tähän mukaan otettu informaatio kuvaa vain osaa yritysten tekemää laajempaa työtä tällä alueella.

Sopimusmallit automaatiohankinnoissa -osuudessa halusimme tuoda näkyväksi muutamia tietoturvaliitteiden malliluonnoksia, joita järjestelmiä hankkivat vastuuhenkilöt ja organisaatiot voisivat hyödyntää omassa työssään. Tavoitteenamme oli kehittää malleja, joilla yritykset voisivat helpommin tilata kyberturvallisia tuotteita ja palveluja automatisoidun teollisuustuotannon alueella. Otan mielellään vastaan näihin luonnoksiin liittyviä kommentteja, tavoitteena sopimusmallien edelleen kehitys.

Julkaisun loppuun olemme kirjanneet paitsi johtopäätöksiä, niin myös joitain tärkeimpiä jatkotyömme elementtejä. Aivan loppuun on lisätty vielä referenssit, dokumentteja tai paikkoja joista voitte etsiä soveltuvaa materiaalia jatkotyötänne varten.

Kaikkien mainittujen hankkeidemme materiaalit löytyvät Huoltovarmuuskeskuksen HUOVI-portaalista [HUOVI] Teollisuuden tietoturvan työpajat-hankealueelta. Pääsyä HUOVIin ko. hankealueelle voi tiedustella tämän kirjasen kirjoittajilta. Mainitut hankkeemme tukevat vahvasti myös kansallista kyberturvallisuusstrategiaa, katso: www.yhteiskunnanturvallisuus.fi

OSA 1

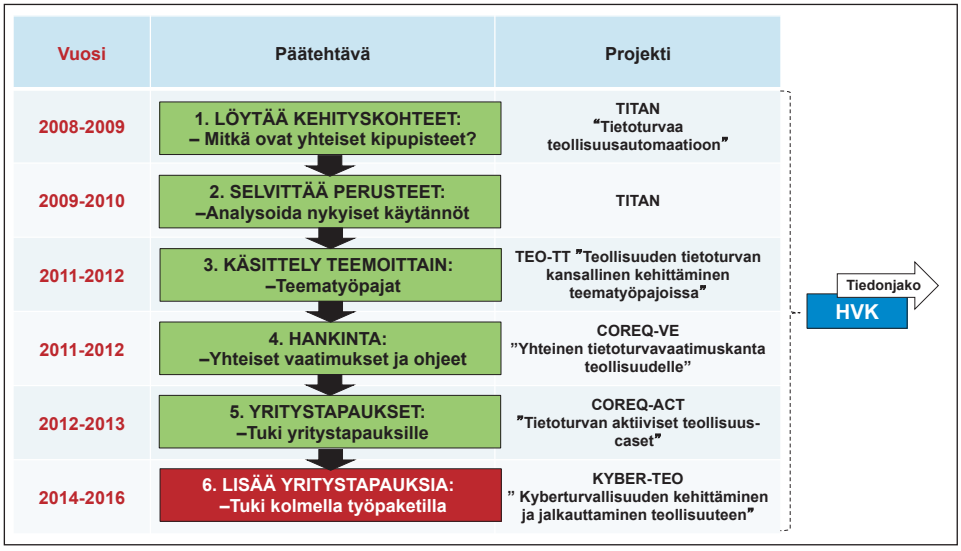
JOHDANTO

Kyberturvallisuuden kehittäminen on pitkäjänteistä työtä – Aluksi lyhyt johdatus teollisuuden kyberturvallisuustyöhön pitkällä aikajänteellä.

1. JOHDANTO

KYBER-TEO-hankekokonaisuus

Seuraavassa kuvassa on havainnollistettu HVK:n ja VTT:n viime vuosina toteuttamia teollisuuden kansallisia kyberturvallisuuden kehittämisprojekteja. Ensimmäinen [TITAN] oli Tekesin tavoitetutkimushanke, mutta seuraavat olivat teollisuuden ja Huoltovarmuuskeskuksen toimeksiantoja. Alinna KYBER-TEO 2014–2016 -hankkeet, eli tätä kirjoitettaessa käynnissä oleva hankekokonaisuus.



Kuva 1. Teollisuuden kyberturvallisuuden jatkuva kehittäminen Huoltovarmuuskeskuksen ja VTT:n avulla.

KYBER-TEO – "Kyberturvallisuuden kehittäminen ja jalkauttaminen teollisuuteen" kansallisen hankekokonaisuuden 2014–2016 pääomistaja on Huoltovarmuuskeskus. Hankkeen yritysasiakkaat vuonna 2014 näkyvät seuraavassa kuvassa sisältäen n. 10 osallistuvaa teollisuus- ja palveluyritystä.

KYBER-TEO-hankekokonaisuuden päätavoite on kehittää ja testata osallistuvissa yrityksissä PALVELUJA kyberturvallisuuden ja jatkuvuuden varmistamiseksi ja muun Suomalaisen teollisuuden hyödynnettäväksi.

Tausta

Voimakkaasti kasvavien tietoturvariskien hallitseminen edellyttää tuotannon kyberturvallisuuden nykytilanteen kartoittamista, tietoturvavaatimusten yritys- ja toimintokohtaista soveltamista, toteutusta ja käytäntöön panoa. Lisäksi tarvitaan kyberturvallisuuden toteuman aktiivista seurantaa niin automaatiojärjestelmien ja tietoverkkojen tasolla kuin normaaleissa työkäytännöissäkin.

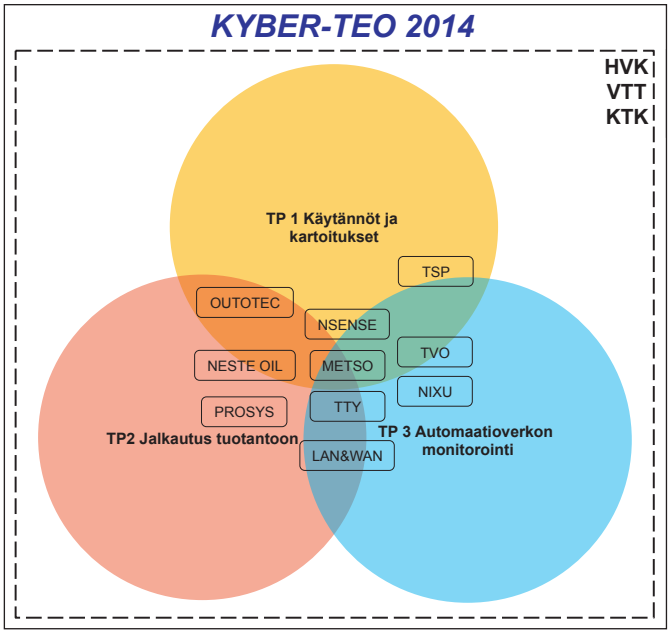
Työpaketit

TP 1: Kybersuojauksen käytännöt ja kartoitukset – vetäjä VTT Heimo Pentikäinen

TP 2: Kyberturvallisuuden jalkauttaminen kotimaiseen tuotantoon – vetäjä VTT Pasi Ahonen

TP 3: Tuotantoautomaatioverkon monitorointipalvelut – vetäjä VTT Sami Noponen

Kuten seuraavasta kuvasta näkyy, vuonna 2014 KYBER-TEO-hankkeen työ kohdistui hankkeen kaikkiin kolmeen työpakettiin.



Kuva 2. KYBER-TEO 2014 -projektin työpaketit ja osallistujayritykset.

KYBER-TEO 2014 Case yritykset

Teollisuusyritykset

- Metso Automation Oy
- Neste Oil Oyj
- Outotec Oyj
- Teollisuuden Voima Oyj (TVO)
- Turun seudun puhdistamo Oy (TSP)

Palveluyritykset

- Nixu Oyj
- Nordic LAN & WAN Communication Oy (LAN&WAN)
- nSense Oy
- Prosys PMS Oy

Tavoitteita

Kyberturvallisuuden käytännöt ja kartoitukset (TP1) on alue, jossa lähes kaikilla teollisuusyrityksillä tulisi olla jatkuvaa tilanteen kartoittamista ja kehittämistä. Samoin kyberturvallisuuden jalkautus tuotantoon (TP2) sisältää hallinnollisia ja teknisiä menettelyjä kuten tietoturvatestaus, joilla varmistetaan ja todennetaan tietoturvavaatimusten toteutuminen tuotantojärjestelmissä. Kolmantena alueena on automaatioverkon monitorointi (TP3), joka täydentää tuotannon ohjausverkon kyberturvallisuuden tilannekuvaa antaen täten suuntaa välittömille vastatoimille ja todentaa aktiivisten tietoturvaratkaisujen puutteita.

Jatkuvuuden tavoite

Teollisuuden tuotantotoiminta on tänä päivänä monien haasteiden edessä. Yhtäältä tulee vastata koventuneeseen hintakilpailuun eli yksikkökustannusten laskuun, mutta toisaalta myös tuotannon joustavuuteen eli tuotteiden nopeaan muokattavuuteen ja -toimitukseen. Tämä on aiheuttanut tuotannon automaatiojärjestelmien integroimista tuotannon (MES)- ja toiminnanohjausjärjestelmien (ERP) kanssa.

Erityisesti nykyisin usein vaadittavat tuotannon joustavuuden ja seurattavuuden vaatimukset edellyttävät järjestelmien integrointia entistä tiiviimpään tiedonsiirtoon toistensa kanssa. Tämä taas voi johtaa tuotannon jatkuvuuden heikentymiseen, sillä esim. onnistunut palvelunestohyökkäys ERP-järjestelmää kohtaan voi aiheuttaa jopa välittömiä tuotanto-ongelmia, mikäli verkko- tai järjestelmäarkkitehtuuri tai näiden toteutus on turvattomasti järjestetty.

Tuotannon jatkuvuuden varmistaminen edellyttää siis samanaikaisesti:

1. **Nykyisen** tuotantojärjestelmän jatkuvuuden ja kyberturvallisuuden parantamista erityisesti järjestelmien välisissä rajapinnoissa
1. **Uusien** tuotantojärjestelmien kehitysprojekteja, joissa kyberturvallisuus huomioidaan alusta lähtien verkkotasolla ja ulkoisissa rajapinnoissa, datayhteyksissä ja toimilaitteissa.

Case kehitysohjelma

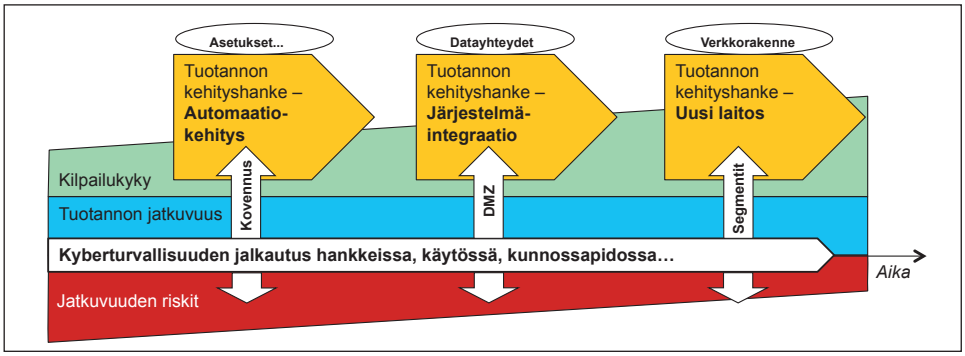
Edellä mainitut toimenpiteet voidaan toteuttaa yrityksessä esimerkiksi:

- Tuotannon *jatkuvuuden kehittämisohjelmalla* (hyödyntäen mm. Huoltovarmuuskeskuksen jatkuvuuden varmistamisen työkalut):
    - Jatkuvuuden hallinnan kypsyysanalyysit ja vaatimukset
    - Ohjeet varautumissuunnitelman laadintaan
    - Valmiussuunnittelu
    - SOPIVA-suositukset (nykyisin Kyberturvallisuuskeskuksessa)
- Tuotannon *kyberturvallisuuden kehittämisohjelmalla* (hyödyntäen mm. *COREQ-ACT* ja *KYBER-TEO*-hankkeiden tulokset), joista mainittakoon esim., katso [KOOSTE]:
    - Tuotannon kyberturvallisuuden nykytilan kartoitus ja tuotannon tietoturvaohjeet
    - Hankintojen tietoturvavaatimukset ja tietoturvatestauksen ja verifioinnin menetelmät
    - Automaatioverkon monitoroinnin menetelmät.

Yritysten kehitysohjelmat edellyttävät, että tuotantotoiminnan jatkuvuuden tavoitteet ja yksityiskohtaiset vaatimukset asetetaan tietylle tasolle, johon sitten esimerkiksi kyberturvallisuuden kehityshankkeiden avulla pyritään. Lisäksi jatkuvuuden ylläpitäminen edellyttää tietenkin myös käytön- ja kunnossapidon aikaisia turvatoimia, joilla tuotannon jatkuva ja häiriötön toiminta varmistetaan.

Jatkuvuus ja kyberturvallisuus kehityshankkeissa

Automaatiojärjestelmiä tulee siis entistä enemmän päivittää modernin joustavan tuotannon tarpeita vastaavaksi. Lisäksi niitä integroidaan enenevässä määrin muihin järjestelmiin, esim. laite- tai automaatiojärjestelmätoimittajan ylläpitoa ja etähuoltoa varten. Kyberturvallisuus tulee jalkauttaa mm. näiden tuotannon kehityshankkeiden yhteydessä kiinteäksi osaksi tuotantotoimintaa.



Kuva 3. Kyberturvallisuus tulee huomioida kehityshankkeissa jatkuvuuden varmistamisen lisäksi.

Kyberturvallisuus tulee siis huomioida tuotannon ja automaation kehityshankkeissa jo alusta alkaen siten, että jo kehityshankkeiden vaatimuksissa ja suunnittelussa kyberturvallisuus on vahvasti mukana.

Yllä oleva kuva havainnollistaa erilaisia tuotannon kehityshankkeita, kuten automaatiojärjestelmän kehittämistä (esim. uusi sovellus), automaatioverkon integroimista muihin järjestelmiin (esim. ERP) ja kokonaan uuden laitoksen suunnittelua ja rakentamista. Näissä kehityshankkeissa tietoturva voi painottua eri tyyppisiin asioihin, kuten:

- **Järjestelmäasetuksiin**: Automaatiojärjestelmien ja -sovellusten turvalliset asetukset määritetään, asennetaan ja testataan ennen järjestelmän hyväksymistä tuotantokäyttöön
- **Datayhteyksiin**: Automaatiojärjestelmää integroitaessa muihin järjestelmiin huolehditaan automaatioverkon datayhteyksien rajoittamisesta esimerkiksi automaation DMZ-vyöhykkeeseen sijoitettaviin sovelluspalvelimiin, joihin automaation kaikki datayhteydet terminoidaan
- **Verkkorakenteisiin**: Erityisesti uutta tuotantolaitosta tai -linjaa rakennettaessa kannattaa panostaa alusta alkaen turvalliseen arkkitehtuuriin myös dataliikenneverkkojen ja automaatiojärjestelmien osalta. Erityisesti automaatioverkot kannattaa erotella määrättyyn toimintaan omistettuihin saarekkeisiin, jotka voivat toimia itsenäisesti, vaikka esimerkiksi järjestelmäintegraation vaatima tiedonsiirto ylemmän tason verkkoihin katkeaisikin.

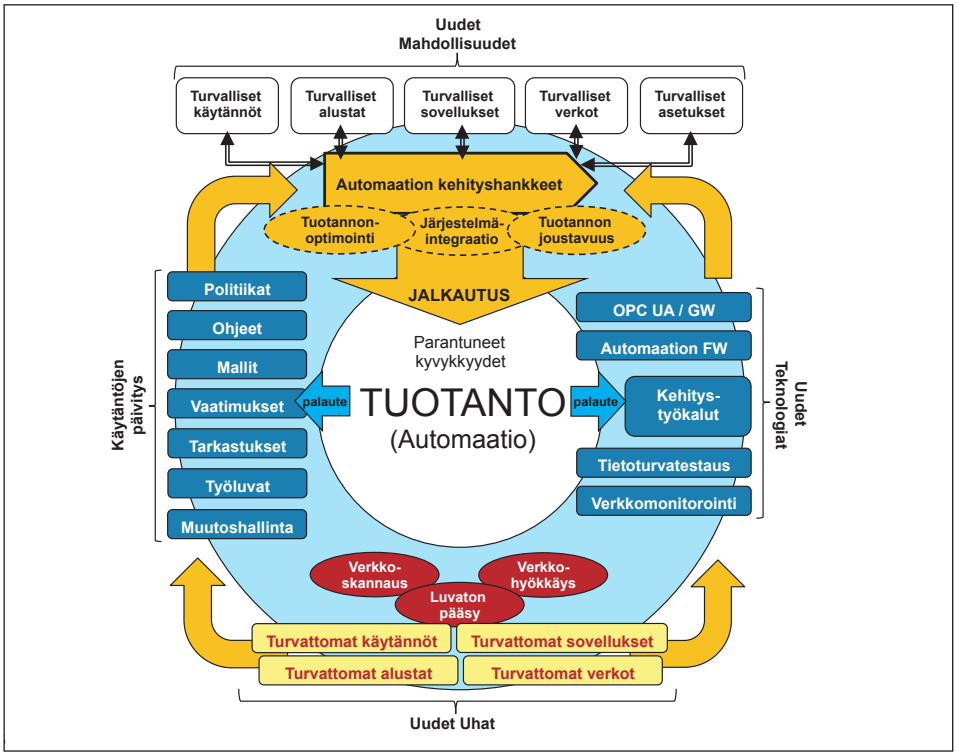
Kehityshankkeilla on merkitystä yrityksen tuloksen parantamisessa, mutta myös tuotannon jatkuvuuden riskien pienentämisessä. Jatkuvuuden varmistamisen tärkeä osa alue on myös kyberturvallisuuden parantaminen ulkoisia ja sisäisiä uhkatekijöitä vastaan. On tärkeää huomata myös, että jos automaation ja osaamisen kehittämispanoksia vähennetään, saattavat riskit kasvaa sekä tuloksen heikentymisen, että esim. kyberturvallisuuden vähittäisen rapautumisen kautta.

Kyberturvallisuuden kehityspotentiaali

Teollisuustuotannon ja erityisesti automatisoidun tuotannon teknologian ja prosessien kehittämiselle on siis hyvät perusteet. Koska kilpailukyky edellyttää uusien teknologioiden ja järjestelmäintegraation lisäämistä, kannattaa uusien mahdollisuuksien kirjoon samalla lisätä kyberturvallisuuden kehittäminen. Oikein sovellettuna tämä yhtälö parantaa monimutkaistuvien järjestelmien jatkuvuutta vähentäen häiriötekijöitä ja lisäten tuottavuutta. Erityisesti automaation kehityshankkeissa uusien teknologioiden tuomat uudet uhkatekijät tulee minimoida arvioimalla eri vaihtoehtoja ja ottamalla käyttöön ainoastaan turvallisia automaatioratkaisuja, katso kuva alla.

Hiukan kärjistäen voidaankin ehdottaa, että teollisuusyritysten kyberturvallisuuden kehittäminen kannattaa kohdistaa kilpailukyvyn kannalta välttämättömiin kehityshankkeisiin.

Automaation kehityshankkeissa käyttöönottoon tuleva uusi teknologia ja järjestelmäintegraatiot edellyttävät, että uudessakin arkkitehtuurissa luvaton pääsy verkkoihin ja järjestelmiin estetään systemaattisesti sekä teknisin että hallinnollisin menettelyin. Erityisesti on valvottava, että tuotantoverkkoon ei pääse verkkoa luotaavia (skannaavia) luvattoman tiedustelun-, häirinnän- tai hyökkäyksen elementtejä.



Kuva 4. Kyberturvallisuus on sisällytettävä automaation kehityshankkeisiin.

Tekninen tietoturva

Teknisen suojauksen ratkaisuja ovat esim.:

- Automaation palomuuri
  - Automaatioverkkoon kytkettäväksi suunniteltu palomuuri / VPN palvelu / VLAN kytkin / portaali
- Automaatiotiedonsiirron yhdyskäytävä, esim.:
  - Automaation DMZ - verkon laitteet
  - OPC UA - yhdyskäytävä
  - MQTT / CoAP / XMPP / AMQP / proxy: teollinen internet
- Automaation kehitystyökalut
  - OPC UA SDK:n tietoturvaominaisuudet
  - Lähdekoodianalysaattorit & -kääntäjät
  - Järjestelmäkohtaisten kehitystyökalujen turvalliset käyttötavat
- Automaation tietoturvatestaus
  - Verkkoskannerit
  - Fuzzerit, esim. Defensics TCF
  - Penetraatiotestauksen työkalut, esim. Metasploit
- Automaatioverkon monitorointijärjestelyt
  - Automaation järjestelmälokien analyysi ja raportointi
  - Signatuurien tunnistus (Verkko-IDS)
  - Verkkoliikenteen tietovuoseuranta ja yllättävien poikkeavuuksien tunnistus
  - Hälytysten raportointi valvomoon.

Hallinnollinen tietoturva

Hallinnollisen suojauksen käytäntöjä tai elementtejä ovat esim.:

- Tuotannon yhtenäinen tietoturvapolitiikka
- Käytännön ohjeet tietoturvan ylläpitämiseen tuotannossa ja tietoturvallisen suunnittelun ohjeet
- Mallien kiinnittäminen, esim. automaatioverkossa sallitut etäyhteyskäytännöt, tekniikat ja yhteyspisteet
- Kyberturvallisuuden vaatimuskanta: esim. hankintojen tietoturvavaatimukset todentamis- ja testauskäytäntöineen
- Automaatio- ja verkkojärjestelmien kyberturvallisuustarkastukset ja kartoitukset
- Työlupien myöntäminen ennen minkä tahansa työn aloittamista
- Muutosten hallinta kaikkien automaatiojärjestelmien, automaatioverkkojen, sekä näiden kyberturvallisuuteen liittyvien asetusten ja kokoonpanon osalta.

OSA 2

KYBERTURVALLISUUDEN JALKAUTUS

Kyberturvallisuus jalkautetaan tuotantoon parhaiten yhteistyöllä, ei pakottamalla.

2. KYBERTURVALLISUUDEN JALKAUTUS

Yhteenveto

Tässä osuudessa kuvataan työskentelymalli kyberturvallisuuden jalkauttamiseksi teollisuusyritykseen. Kuvatun mallin tarkoituksena on toimia inspiraation lähteenä systemaattiselle kyberturvallisuuden kehitystyön käynnistämiselle. Tarkoituksena on edistää hyvien käytäntöjen kehittämistä kyberturvallisuuden parempaan hallintaan teollisuudessa ja teollisuuden palveluyrityksissä.

Kyberturvallisuuden kehittämisen tehtävät sisältävät mm.:

- Tuotannon kyberturvallisuuden kehitystavoitteiden määrittelyn
- Kehitettävien toimintojen rajauksen
- Kyberturvallisuuden yleiskartoituksen suorittamisen, riskianalyysien hyödyntämisen (*käsitelty aiemmassa julkaisussa*)
- Työskentelymallin määrittely kyberturvallisuuden kehittämiseen, esim.:
    - Kyberturvallisuuden kehitysryhmän perustaminen
    - Kehityssuunnitelmien laadinta: tavoitteet, tehtävät, jne.
    - Kyberturvallisuusratkaisujen testaus ja pilotointi
    - Kyberturvallisuuden ratkaisujen käyttöönotto ja vaikutusten seuranta
    - Jatkokehittämisen suunnittelu

Jalkautuksen malli

Kuva 5. Esimerkkimalli tuotannon kyberturvallisuuden jalkautuksen päävaiheista.

Kehitystavoitteen määrittely

Yrityksen kyberturvallisuuden kehittämisen päätavoite määritellään yrityksen johtotasolla ja yhteistyössä yrityksen asiantuntijoiden kanssa. Asiaa edistää, mikäli yritysjohto hyödyntää tuotannon asiantuntijoita ja automaation vastuuhenkilöitä jo alkuvaiheessa, jolloin tavoitteista, haasteista ja nykyisistä olosuhteista saadaan riittävä ja realistinen kuva kyberturvallisuuden kehittämisen lähtökohdaksi.

Nämä tavoitteet saattavat kuitenkin muuttua ajan kuluessa, ja usein niin käykin. Tämä johtuu siitä, että toiminnan kyberturvallisuuden nykytila kirkastuu vasta kehittämisen aikana ja kybertoimintaympäristökin saattaa muuttua ajan kuluessa (usein haastavammaksi).

KYBERTURVALLISUUDEN JALKAUTUKSEN AAKKOSET

MITÄ – Kartoita toimintanne tavoitteet, toimintaympäristöt, sekä niiden pahimmat uhat ja riskit

MIKSI – Arvioi johdolle hyötyjen rahallinen arvo ja suojauksen kulut

KENELLE – Tunnista kehitettävät toiminnot, laitokset, ryhmät, henkilöt, partnerit, toimittajat, jne.

KUKA – Määritä millä porukoilla kehityskohteet määritetään, suunnitellaan, testataan ja pilotoidaan

MILLOIN – Aikatauluta suunnitelmat, vuosittaiset projektit ja tukitoimet ⇨ seuraa toteumaa

MITEN – Laadi kyberturvallisuuden konseptit, kiinnitä kybervaatimukset, -käytännöt, keinot ja yhteistyö.

Tavoitteiden tulisikin joustaa todellisen tilanteen selkiytymisen ja henkilöstön kybertietoisuuden kehittymisen mukaisesti kuitenkin siten, että tärkeitä kehitysalueita toteutetaan myös käytännössä.

Tyypillisiä kehitystavoitteita ovat mm.:

- Toiminnan ja tuotannon kyberturvallisuuden nykytilan selvittäminen
- Tuotannon ja/tai automaation tietoturvan kehitysryhmän perustaminen
- Kyberturvallisuuden kehityssuunnitelma
- Tuotannon tietoturvakonsepti
- Tuotannon tietoturvapolitiikka
- Tuotannon ja tuotekehityksen tietoturvaohjeet
- Tuotannon tietoturvavaatimukset
- Tuotannon tietoturvavaatimusten jalkauttaminen tuotantoon
- Tuotannon kyberturvallisuustilanteen valvonnan ja seurannan järjestäminen
- Tuotantoverkon kyberturvallisuuden monitoroinnin järjestäminen
- Tuotannon ja ylläpidon kyberturvallisuuspalvelujen kehittäminen.

Kehitysohjelman rajaus

Yrityksen kyberturvallisuuden kehitysohjelmaan sisällytettävät tuotantotoiminnot voivat sisältää esim. seuraavanlaisia toimintoja (rajauksineen):

- Tuotantoyksikkö kokonaisuutena (tuotantoyksikkö, -linja, osasto, tms.)
- Käyttötoiminta (normaalikäyttö, vikatilanne, hätätilanne, poikkeustilanne)
- Ylläpitotoiminta (seisokki, huolto, vikakorjaus, päivitys)
- Hankinta (toimittajien vertailuvaihe, projektineuvottelu, tarjous/tilaus, pilotti, kehitystyö, testaus, käyttöönotto)
- Rakentaminen (uusi tehdas, tuotantoyksikkö, tuotantolinja, -järjestelmä)
- Kehittäminen (järjestelmäuusinta, laajennus, integrointi, uusi mittaus, optimointi, tms.)
- Palvelutoiminta (käytön seuranta, etähuolto, etädiagnostiikka, korjaus, jne.).

Oleellisimmat asiat yrityksen tuotantotoiminnan kyberturvallisuuden kehittämisessä ovat avainhenkilöstön keskinäinen *yhteistyö* yhteisten tavoitteiden määrittämiseksi ja saavuttamiseksi.

Lisäksi tälle työlle täytyy olla johdon tuki. Yrityksen johdon tai sen nimeämän tuotanto- ja tukihenkilöstön aloittaessa kyberturvallisuuden kehittämistyön suunnittelua, kannattaa organisoitua hyvin ja varautua mahdollisesti pitkäkestoiseen toteutukseen.

Seuraavassa on kuvattu tarkemmin hyvään työskentelymalliin kuuluvia tehtäviä.

Kyberturvallisuuden kehitysryhmän perustaminen

Pitkän tähtäimen kehitysryhmä perustetaan tuotannon (tai tuotantoautomaation) kyberturvallisuuden kehittämiseksi, ellei sellaista ole jo olemassa. Sen jäseniksi määritellään (tavoitteista riippuen) esim. seuraavanlaisia henkilöryhmiä:

- Tuotannon johto
- Tuotannon kehityspäällikkö
- Automaation toiminnasta vastaavat henkilöt (esim. eri tuotantoyksiköistä)
    - Automaation toiminnasta vastaava (huolto, ylläpito, korjaus)
    - Automaation kehittämisestä vastaava (optimointi, sovellukset, jne.)
    - Automaation tietoturvavastaavat (esim. eri tuotantoyksiköistä)
- IT järjestelmävastaava (esim. eri tuotantoyksiköistä)
- Palveluntarjoajan edustaja (esim. eri tuotantoyksiköistä) soveltuvin osin
- Aihealueen asiantuntija soveltuvin osin, esim. järjestelmätoimittaja.

Ryhmää käynnistettäessä tärkeimpiä asioita ovat kehitysryhmän päätavoitteiden ja tehtävien määrittely, mutta myös jokaisen jäsenen tavoitteiden, osallistumisen ja kontribuution määrittelyt.

Kehityssuunnitelmien laadinta

Kehityssuunnitelmien määrittely yrityksen eri tasoilla tulee olla selkeää, esim. toimintotaso, tuotantoyksikkötaso, tms. Sama koskee tehtäväjakoa, seurantavastuita, resursointia, jne. Tätä varten yrityksen tulee yhteistyössä valmistella mm. seuraavaa:

- Selvitetään tuotannon nykyinen toimintatapa ja toimintaohjeet
- Kartoitetaan tulevaisuuden toiminta-edellytykset ja vaatimukset
- Määritellään toiminnan turvallisuuden tavoitetila eri osa-alueilla
- Määritellään kehittämisen vaiheittainen eteneminen, esim. askelmerkit
- Määritellään päätehtävät eri vaiheissa ja vastuutus (roolit)
- Aikataulusuunnittelu
- Määritellään vastuutahot eri alueiden toimenpiteiden jalkautumisen seurannalle
- Johto allokoi kehittämiseen tarvittavat resurssit, määrärahat ja tukitoimet.

Koeteltujen ratkaisujen testaus ja pilotointi

Tämä vaihe on riippuvainen yrityksen tuotannon kyberturvallisuuden kehitystavoitteista. Kehittämisen eri osa-alueiden toteutus voidaan usein tehdä rinnakkain tai peräkkäin, tai näiden erilaisina yhdistelminä. Tärkeintä on, että kehittämisen eri osa-alueet tukevat toisiaan hedelmällisellä tavalla. Esim. nykyisen toiminnan, ohjeiden tai järjestelmien kartoittaminen tukee uusien ohjeiden laadintaa, uusien tietoturvavaatimusten määrittelytyötä, jne. Samalla tavoin esim. vaihtoehtoisten tietoturvaratkaisujen evaluointi ja testaus tukevat tuotantokäyttöön otettavien menetelmien ja työkalujen valintaa, käyttöönottoon liittyvää päätöksentekoa, jne.

Kyberturvallisuuden ratkaisujen käyttöönotto ja vaikutusten seuranta

Valituksi tulleiden kyberturvallisuuden ratkaisujen esikokeilujen, testauksen ja mahdollisen pilotin jälkeen ne otetaan tuotantokäyttöön kyberturvallisuussuunnitelman ja riskiarviointien mukaisesti. Usein uusien ratkaisujen käyttöönotto kannattaa vaiheistaa, alkaen vähemmän kriittisistä järjestelmistä ja päätyen tuotannon kattavaan suojausratkaisuun.

Käyttöönotettujen uusien ratkaisujen tietoturvavaikutusten seuranta on erittäin tärkeää päätavoitteiden saavuttamisen ja johdon tuen varmistamisen kannalta. Lisäksi johdon kannattaa jatkuvasti tukea kehitysryhmää ja sen aikaansaamien tulosten vaikuttavuutta, esim.:

- Kehitysryhmän kokoonpanon, tavoitteiden ja toiminnan seurannalla ja tuella
- Raportoidun kyberturvallisuuden tilan seurannalla ja kommentoinnilla
- Antamalla riskianalyysiapua ennen potentiaalisesti vahingollisten toimenpiteiden toteuttamista
- Antamalla palautetta kehitysryhmän työskentelylle, ehdottamalla uusia tavoitteita, tms.

Jatkokehittämisen suunnittelu

Kuten edellä onkin jo mainittu, yrityksen tuotannon kyberturvallisuuden kehittäminen edellyttää pitkäjänteistä panostusta, suunnittelua ja seurantaa. Ongelmana on, että ympäröivän yhteiskunnan kyberturvallisuuden tilannekuva voi muuttua nopeastikin, joka aiheuttaa välittömiä tuotanto-ongelmia myös yritystasolla moninaisten riippuvuuksien johdosta.

Kyberturvallisuuden jatkokehittäminen tuleekin suunnitella yrityksen koko toimintaympäristön, toimintaedellytysten ja myös tulevaisuuden tarpeiden ja vaatimusten mukaisesti. Yksittäinen yritys ei pysty yksin hallitsemaan edes oman tuotantonsa jatkuvuutta kaikissa tilanteissa. Täten jatkuvuuden ja kyberturvallisuuden varmistamisen tehtävät ovat erittäin vaativia ja ne tulee myös ymmärtää sellaisiksi.

Seuraavaksi kuvaamme muutamia KYBERTEO 2014 -projektissa toteutettuja yrityscaseja, joissa oleellisena kehityselementtinä on ollut kyberturvallisuuden jalkautus tuotantokäyttöön.

Outotec Case: Tietoturvavaatimusten jalkautus automaatiotoimituksiin

Lähtökohdat

Outotecin tunnistamia lähtökohtia automaatiotoimitusten kyberturvallisuuden kehittämiselle olivat:

1. Uusi organisaatio mahdollistaa yhteisten hankkeiden eteenpäin viemisen:

- Globaalin automaatiokehitysfunktion perustaminen v. 2013
- Aikaisemmin kehitys hyvin hajautunutta eri puolille organisaatiota
- Lisäksi ulkopuolisten suunnittelijoiden käyttö yleistä

2. Automaation tietoturvan rooli on kasvamassa toimituksissa:

- Perinteinen, eristetty tehdasverkko jäämässä historiaan
- Järjestelmien vertikaalinen integrointi (esim. MES taso) ja etäyhteydet (toimittajalle / toimistoverkkoon) yleistyvät

3. Automaation tietoturva on strategisesti tärkeää

- Vrt. Kone- ja työturvallisuus
- Kilpailukyky
- Palveluliiketoiminnan kehitys

Haasteet

Kyberturvallisuuden kehittämisen alkuvaiheessa haasteita esiintyi mm. seuraavilla osa-alueilla:

Haaste 1: Maailmanlaajuinen toiminta – tietoturvakulttuuri vaihtelee siinä missä esim. työturvallisuusasiat

- T&K-, myynti- ja palvelukeskukset 27 maassa

Haaste 2: Laaja skaala erilaisia toimitusrajapintoja. Toimituslaajuus kattaa tasot 1-3 (ISA-95 mallista): Laite – toiminnanohjausjärjestelmät (MES) ja palveluliiketoiminta menee vielä tämänkin yli. Yhä enemmän sovelluksia, jotka kommunikoivat automaatioverkon ulkopuolelle:

- Automaatiojärjestelmien etävalvonta (*web server*)
- Erilaiset informaatiopalvelimet
- Etäyhteydet suunnitteluasemiin.

Edelleen lukumääräisesti suurin osa toimituksista on prosessilaitteita: Etäyhteys tarpeita kontrollereihin (PLC). Sulautetut järjestelmät laajentavat järjestelmäpalettia entisestään.

Haaste 3: Jaettu vastuu…monta omistajaa

Vastuu automaatiojärjestelmän tietoturvasta on voinut jakaantua laajalle:

IT:

- Kehittyneet prosessit, työkalut ja osaaminen yrityksen tietoturvan ylläpitämiseksi
- Eivät vastaa automaation tietoturvasta (pois lukien omien tuotantolaitosten verkot)

Automaatiokehitys:

- Tietoturvan kehitys automaatiossa projektiluonteisesti
- Haasteina automaatiosovellusten laaja kirjo ja sisäinen tiedonkulku

Suunnittelu / Toimitus:

- Vastaavat käytännössä toimitettavan järjestelmän tietoturvan suunnittelusta ja toteutuksesta

Palvelu / Asiakkaat:

- Toimitusprojekteissa vaatimuksia rajallisesti (asiakkaan vastuulla)
- Vastaavasti keskeisessä roolissa palveluliiketoiminnassa (riskien hallinta)

Päätavoitteet projektin alussa

Edellämainituista lähtökohdista ja haasteista johtuen Outotecin päätavoitteet kehitysprojektin alussa muodostuivat seuraavanlaisiksi:

- Riskien arviointi ja tavoitetaso automaatiosuunnittelussa
- Referenssiarkkitehtuurien muodostaminen
- Etäyhteysratkaisun kehitys eritasoisille toimituksille (laite, tehdasautomaatio, palveluliiketoiminta)
- Luoda perustaa automaation tietoturvaohjelmalle ja tehdä alustavat ohjeistukset sen tiimoilta

Toimintasuunnitelma

Outotecin kyberturvallisuuden kehittämisen toimintasuunnitelman perustana olivat laajapohjaisen työryhmän perustaminen (kehitys, suunnittelu, IT, palveluliiketoiminta) + VTT asiantuntijat

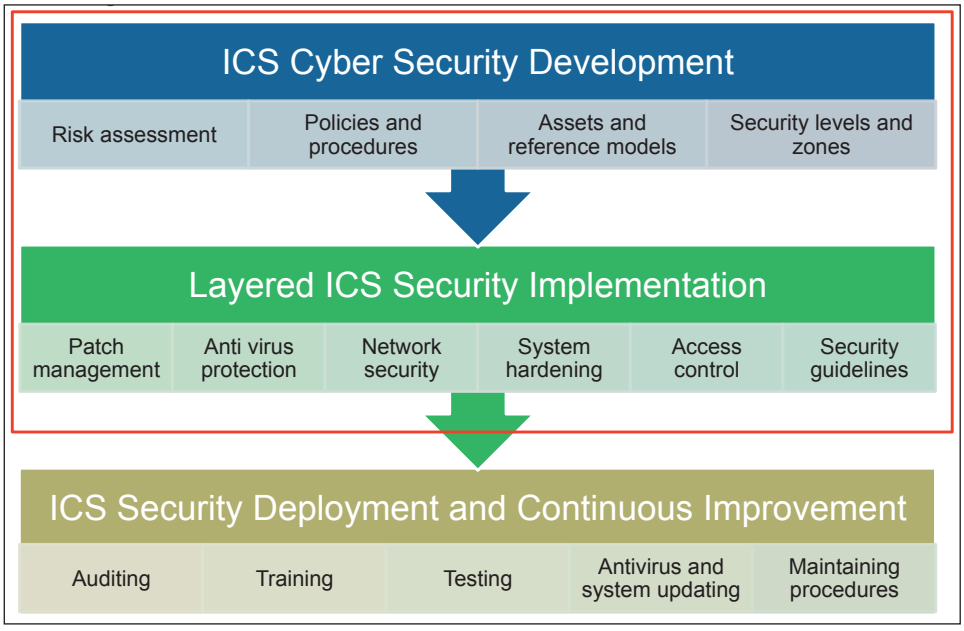
- Tiedonjako sisäisesti ja toisilta oppiminen
- Tiedostaminen

Toimintamuotona olivat pääosin erilaiset työpajat:

- Automaation riskien ja nykytilan arviointi
- Verkkoarkkitehtuuri ja etäyhteydet
- Automaatiosuunnitteluohjeistus (sis. kovennusta)
- OPC UA (yhteinen työpaja)

Kehitysprojektin vaiheet

Outotecin kyberturvallisuuden kehitysprojektin etenemisen vaiheet on pääpiirteittäin esitetty seuraavassa kuvassa:



Kuva 6. Outotecin kyberturvallisuuden kehitysprojektin päävaiheet.

Kehitysprojektin opetuksia

- Automaation tietoturvan merkitystä liiketoiminnan kannalta on korostettava ja se on otettava osaksi riskien hallintaa
- Tietoturvan eteenpäin vieminen on pitkäjänteistä työtä ja vaatii omat resurssit
- Asiat on pyrittävä pitämään riittävän yksinkertaisina ja ymmärrettävinä
- Priorisointi ennen projektia ja sen kuluessa on tärkeää.

Neste Oil Case: Tietoturvaohjeistus automaatiohankintaa varten

Lähtökohta

Neste Oil on jo aikaisemmin toiminut mm. seuraavilla tavoilla automaatiokyberturvallisuuden kehittämisessä:

Sisäisen tarkastuksen suorittamat automaation tietoturva-auditoinnit, niiden korjaavat toimenpiteet: liiketoiminnan jatkuvuuden varmistaminen

Ulkoinen ICT-lähtöinen automaation tietoturva-auditointi ja niiden korjaavat toimenpiteet

Hanke- ja toimittajakohtaiset kyberturvallisuuden määrittelyt eri projekteissa.

Neste Oilissa ei ole aiemmin ollut yhtiötasoista tietoturvavaatimusten ohjeistusta liittyen automaatiohankintoihin. Projektit ovat toimineet asiassa itsenäisesti, mikä on saattanut johtaa epätasaiseen toteutukseen projektien tietoturvakäytäntöjen osalta.

Päätavoitteet

Neste Oilin päätavoitteet KYBER-TEO 2014 -projektin osalta olivat:

- Kehittää ja testata automaation tietoturvan vaatimukset ja ohjeet hankintamäärittelyyn sekä tehdas- ja vastaanottotesteihin vaatimusten todentamiseksi ennen käyttöönottoa
- Valmistella vankka pohja kyberturvallisuuden jatkuvalle kehittämiselle ja ylläpidolle

Tietoturvayhteistyön laajentaminen ja syventäminen, erityisesti laajempialaisempi KYBER-TEO-tulosten hyödyntäminen (mm. kovennuksen ja monitoroinnin tulokset).

Kehityshankkeen rakentaminen

Neste Oilin kehitysprojekti jakaantui seuraaviin tasoihin:

- Sisäinen työskentely: Neste Oil, Neste Jacobs
- Projektityöpajat: Neste Oil, Neste Jacobs, VTT
- Toimittajatyöpajat: Neste Oil, Neste Jacobs, VTT, toimittaja(t)

Kehittämiseen liittyvän työn roolitus toteutettiin seuraavasti:

- Neste Oil: Sisällön ja painopistealueiden määrittely, substanssiosaaminen, sekä jatkotyön määrittely
- Neste Oilin hankintatoimi ja ICT-osasto: hankintamäärittely, hankintojen ja ICT:n asiantuntija
- Neste Jacobs: käytännön työ ohjeiden laatimiseksi
- VTT: kyberturvallisuuden asiantuntija, sisällön tuottaja
- Automaatiojärjestelmätoimittaja: yhteistyö, erityisesti FAT ja SAT testaus ja osallistuminen niiden määrittelyyn.

Neste Oil casen projektisuunnitelmaan kuului mm. seuraavanlaisten tapahtumien järjestäminen (*eng*):

- *Project meeting*
- *Preparation meeting & Workshop 0*
- *Workshop 1/2/3/4*
- *SIS workshop*
- *Security Level workshop*
- *FAT workshop*
- *FAT Pilot*
- *SAT Workshop*
- *Final get together*

Pohjamateriaali

Kehitysprojektissa käytettiin kyberturvallisuusvaatimusten ja -ohjeiden pohjana aiempien projektien tuloksia (mm. COREQ-ACT: vaatimuskanta, hankintojen ohjeet, muut tulokset), toimittajien omia määrittelyjä, ICT-osaston tietoturvaohjeistusta ja käytäntöjä, sekä yleisempiä turvaohjeita ja käytäntöjä. Lisäksi referensseinä käytettiin mm. seuraavia standardeja tai standardin luontoisia julkaisuja (selityksineen):

- Department of Homeland Security: Cyber Security Procurement Language for Control Systems (julkinen)
- IEC-61511: Turva-automaation tietoturvan riskianalyysi
- ISA/IEC 62443-sarjassa tietoturvariskien identifiointi ja analysointi
- ISA-62443-1-1 & 1-2: Termit, lyhenteet, käsitteet, mallit
- ISA-62443-2-1: Tietoturvaohjelman perustaminen
- ISA-62443-2-4: Vaatimukset ICS-järjestelmätoimittajille
- ISA-62443-3-1: Tietoturvateknologiat
- ISA-TR84.00.09-2013 Security Countermeasures Related to Safety Instrumented Systems (SIS)
- ISO/IEC 27001: Hallintavaatimukset
- ISO/IEC 27002: Hallinnan menettelyohjeet
- NIST 800-sarja: Erilaisia kyberturvallisuuden erityisjulkaisuja (julkisia)
- SFS Käsikirja 631-3: Automaatio. Osa 3: Tietoturvallisuus
- WIB: Process Control Domain - Security Requirements for Vendors

Pilotti

Pilotin tarkoituksena oli todentaa (ja edelleen kehittää) Neste Oilin tuotannon automaation hankintakäytäntöjä:

- Kattava, priorisoitu tietoturvavaatimuskanta ja -ohjeet automaatiohankkeiden toimittajille ja laitosten automaatiotoimitusten tietoturvalle

Pilottiprojektiksi valittiin Bensiinin Isomerointilaitos (BESSI), jossa kehityskohteena olivat erityisesti automaatiojärjestelmätoimituksen FAT ja SAT vaiheet. Järjestelmätoimittajalle annettiin tehtäväksi:

- Toimituksen arkkitehtuurimäärittely ISA-95 / ISA-99 tasojen mukaisesti
- Toimitukseen kuuluvan Ethernet-verkon testauksen määrittely
- Tuotantoon siirtovaiheen verkkotarkastukset
- FAT testauksen vaatimuskannan määrittelyyn osallistuminen, vaatimusten kommentointi ja arviointi.

Tuloksia: Projektin tehdasosuudet sisälsivät seuraavien tehtävien tai määrittelyjen koestamista käytännön pilottiprojekteissa

- Kyberturvallisuuden integrointi automaatiojärjestelmien FAT testaukseen
- Kyberturvallisuusvaatimukset FAT testaukseen – valmistelu- ja kehitysvaiheet
- Kyberturvallisuusvaatimukset FAT testaukseen – testaus- ja käyttöönottovaiheet
- Kyberturvallisuusvaatimukset teollisuusautomaation järjestelmätoimittajien hallintaan – katselmointi FAT vaiheessa

Turva-automaation SIS hankinta:

- Turva-automaatiojärjestelmän riskianalyysin toteutus

FAT vaiheen kokemuksia

- Tietoturvatestaamisen lisääminen onnistuu, mutta testiympäristöön panostaminen on tarpeen

SAT vaiheen kokemuksia

- Perusta: SAT tarkastuskohteiden listaaminen, tarkastaminen ja tulosten kirjaaminen
- Dokumentointiperiaatteisiin kannattaa panostaa: esim. terminologia, mäppäys ISA-95 tasoihin, liityntä kohdeympäristöön
- Kovennuksen testaus on tärkeää
- Käyttäjäoikeuksien hallinta on tärkeää
- Verkkomonitoroinnin työkalut ja ohjeet ovat hyödyllisiä
- Virustorjunta ja niiden lokiseuranta soveltuvin osin

Toimenpiteet

Seuraavilla osa-alueilla saatiin kehitettyä entistä turvallisempaa toimintaa ja käytäntöjä aikaisempaan verrattuna:

- Investointihankkeiden tietoturvan riskien arviointi
- Jatkuvuussuunnittelu, varaohjauspaikat ja niiden testaus
- Kokonaisuuksien hallinta yksittäisten järjestelmien sijaan, keskinäiset riippuvuudet ja integraatiot
- Kovennustoimenpiteet
- Parhaiden käytäntöjen hyödyntäminen
- RACI- eli vastuumatriisit
- Tietoturva osaksi koulutusaineistoa
- Tietoturvavaatimusten huomioiminen suunnittelussa ja riskien arvioinnissa (HAZOP)

- Turva-automaatiolle oma ohjeistus ja käsittely
- USB-portit
- Verkostojen ja tiedotuskanavien rakentaminen: jakelulistat, yhteiset työtilat
- Yhteistyö: Muiden yritysten caset ja niihin osallistuminen, työpajat.

Palaute

Hyvää:

+ Yleinen tietoisuus ja konkreettiset näkyvät toimenpiteet
+ Olemassa olevan aineiston hyödyntäminen ja soveltaminen Neste Oilin toimintaympäristöön
+ Turva-automaation hankinnan vaatimukset
+ Toimittajayhteistyö ja sen jatkuva kehittäminen
+ ICT-henkilöstön osaaminen ja kiinnostus.

Huonoa:

– Lisää ”byrokratiaa”, mutta tarpeellista
– Kehittäminen huomioitava projektisuunnitelmassa hyvissä ajoin: aikataulutus, resurssit, kustannukset
– Osittain päällekkäistä ja toistuvaa tekemistä.

Jatkokehitys

- Vastuumatriisi, jatkuvuuden edelleen parantaminen
- Seuranta osana automaation hallintomallia ja ICT-yhteistyötä
- Automaatioinvestointien *roadmap* huomioiden myös tietoturva
- Yrityksen kyberturvallisuusstrategia: Onko automaatio kyberturvallisuuden ytimessä vai onko paino ICT-puolella?
- Riskiarvioinnin jatkokehitys sisältäen tietoturvariskit
- Kokonaisintegraatio, standardien ja hyvien käytäntöjen laajempi noudattaminen
- Automaatioratkaisujen kehittäminen edelleen tietoturvallisemmiksi
- Valmiiksi kovennetut järjestelmäympäristöt.

Automaatiojärjestelmien koventamisen tehtävät

Tässä kohdassa käsitellään automaatiojärjestelmien koventamisen päätehtäviä muutamien tärkeimpien käyttötapausten kautta.

Käyttötapaukset

Jotta järjestelmän koventamiseen liittyvä asiayhteys olisi mahdollisimman selkeä, on tarkasteluun valittu ainoastaan muutamia automaatiojärjestelmien toimitusprojekteihin usein sisältyviä käyttötapauksia. KYBER-TEO 2014 -projektissa käsiteltiin lähemmin seuraavia kovennuksen käyttötapauksia liittyen automaatiojärjestelmien toimitusprojekteihin:

- Ohjelmistoasennukset ja SW-päivitykset
- Tiedon kerääminen automaatiopuolelta ja raportointi
- Miten kovennusohje tehdään ja toiminnot priorisoidaan?

Lisäksi näiden käyttötapausten tärkeimpien toimijoiden roolit on lyhyesti kuvattu seuraavassa (yksinkertaistettu malli). Huom: samalla toimijalla voi olla useampia eri rooleja. Roolien tehtävät voivat myös olla osin päällekkäisiä, jolloin ko. asiasta vastataan yhdessä.

Roolit

TILAAJA: Automaatiota laajasti hyödyntävä teollisuusyritys, jonka toiminta on huoltovarmuuskriittistä ja joka investoi merkittävästi tuotantoonsa. Vastaa oman tuotantonsa tietoturvallisuudesta ja jatkuvuudesta. (Esim. Neste Oil, TVO, TSP)

PÄÄPROJEKTITOIMITTAJA: Vastaa tilaajan hankkeen toteutuksesta, jossa esim. rakennetaan, laajennetaan tai päivitetään tilaajan automatisoitua tuotantoa. Pääprojektitoimittaja vastaa myös hankkeen muiden toimittajien ja alihankkijoiden työstä. (Esim. Neste Jacobs, Outotec)

INTEGRAATTORIT: Integraattorit asentavat ja yhdistävät toimitukseen kuuluvat järjestelmät kuten koneet, laitteet, sovellukset ja automaatiojärjestelmät projektin tilaajan tai pääprojektitoimittajan määrittelemäksi kokonaisuudeksi. Testaa kokonaisjärjestelmän toimivuuden. (Esim. Outotec, Insta Automation)

AUTOMAATIOJÄRJESTELMÄTOIMITTAJAT: Kehittävät ja toimittavat tilaajan hankintaan liittyvät automaatiojärjestelmät. Ylläpitävät järjestelmiään ja palvelevat tilaajaa esimerkiksi takuuaikana tai huoltosopimuksella myös toimituksen jälkeen. (Esim. Metso Automation, Honeywell, Siemens, ABB)

LAITE-, SOVELLUS- JA OHJELMISTOTOIMITTAJAT: Kehittävät ja ylläpitävät automaatiojärjestelmien koneita, laitteita tai niiden sovelluksia ja ohjelmistoja. Sovelluskehittäjät muokkaavat ja kehittävät automaatiossa hyödynnettäviä ohjelmistoja. (Esim. Prosys, Beckhoff, Microsoft)

TIETOTURVAEXPERTIT: Tietoturva-asiantuntijat, jotka voivat tulla eri organisaatioista. Tukevat omalla erityisosaamisellaan automaatiojärjestelmien tietoturvallisuutta. (Esim. nSense, Nixu, Kyberturvallisuuskeskus, VTT, TTY, Codenomicon)

Tehtävät

Jotta tehtäviä ja vastuita voidaan järkevästi jakaa kyseenä olevan automaatioprojektin toimituksen eri osapuolten kesken, täytyy tärkeimmät tehtävät tunnistaa. Automaatiojärjestelmien koventamisen tärkeimpiä tehtäviä on listattu hieman tarkemmin seuraavassa.

Tehtäväryhmien listaus:

- **Alustojen hallinta**: HW ja SW-alustojen ja käyttöjärjestelmien elinkaari ja käyttö suunnitellaan, ml. *Secure system boot*.
- **Sovellusten hallinta**: Käytettävät automaatiosovellukset, tukisovellukset, *3rd party*-ohjelmistot ja laiteajurit. Näiden elinkaaren hallinta suunnitellaan.
- **Toiminnallisuuden määrittely**: Toimitettavat järjestelmätoiminnallisuudet: esim. tuotantokäyttö, käyttötavat, seuranta, ylläpidon ja päivittämisen toiminnallisuudet määritellään. Voidaan myös määritellä mitä ei kuulu toimitukseen: esim. DNS, testerit, kääntäjät, verkonhallintaohjelmistot, tms.
- **Käyttäjätunnusten ja salasanojen hallinta**: Sovitaan erilaisten käyttäjätilien ja salasanojen luonnista, ylläpidosta ja poistosta (ml. *support ja admin*-tilit, jne.)
- **Sallittujen rajapintojen määrittely**: Erityisesti järjestelmän ulkoiset rajapinnat kuvataan yksityiskohtaisesti. Jokaisen erilliskomponentin rajapinnat ja niiden käyttötarkoitus kuvataan.
- **Sallittujen protokollien määrittely**: Toimituksessa käytettävän dataliikenteen yksityiskohdat kiinnitetään.
- **Sallittujen IP verkko-osoitteiden määrittely**: Toimituksen aliverkko-osoitteet, mahdolliset yhdyskäytävät, DMZ-alueen osoitteet, jne.
- **Projektikohtaisen kovennusohjeen kehittäminen**: Yksityiskohtainen kovennusohje kehitetään ja testataan käytännössä koventamalla järjestelmä testiympäristössä, sisältäen mm. edellä mainitut yksityiskohdat.
- **Toimitettavan järjestelmän koventaminen**: Järjestelmän eri osien koventaminen ja testaus hyväksyttyjen koventajien toimesta ohjeen mukaisesti, sovitussa paikassa ja aikataulussa ⇨ Kovennusraportti.
- **Kovennetun järjestelmän toimitus tilaajalle**: Sovitaan prosesseista joilla varmistetaan kovennuksen tila koko toimituksen elinkaaressa.
- **Kovennuksen ylläpito**: Sovitaan käytön ja ylläpidon aikaisesta käyttäjätilien hallinnasta, muutosten hallinnasta, vikakorjauksista, testauksesta, ym.

Käyttötapaus – Ohjelmistoasennukset ja -päivitykset

Jotta ymmärtäisimme paremmin miten koventaminen liittyy automaatiojärjestelmän pitkään elinkaareen kompleksisessa teollisuusympäristössä, tarvitaan yleiskuva eri toimijoiden osuudesta koventamisen eri tehtävissä.

Toimijoiden koventamiseen liittyvät päätehtävät teollisuuden laajan tuotantoyksikön valitsemien ja käyttämien erilaisten ohjelmistojen koko elinkaaressa on esitetty malliratkaisuna seuraavassa kuvassa. Tehtäväjakoa tietenkin rajaa käytännössä tuotanto-operaattorin tai omistajan tuotannossaan käyttämät toimijat ja heidän tarjoamansa soveltuvat palvelut ja tuotteet.

Toimija / Elinkaaren vaihe	TUOTEKEHITYS	HANKINTA	TESTAUS & KÄYTTÖÖNOTTO	TUOTANTO & YLLÄPITO	KÄYTÖSTÄ-POISTO
TILAAJA	• Anna tiedoksi *"OS-& App-roadmaps"*	• Sallitut sovellukset • Toimitussisältö ja –raja • Vaatimukset • Käytännöt, elinkaari	• IP osoiteskeemat • Vastaanotto	• Ylläpitäjät • Prosessit • Luvat • Tuotannon elinkaari	• Hävitys-menettelyt • Prosessit
PÄÄPROJEKTI-TOIMITTAJA		• Ohjelmistolisenssit • Toimituksen sisältö • Käyttäjätilien hallinta	• Fasilitointi, valvonta • Rajapintojen koordinointi • Liikennöintimenettelyt • Osoitteet, yhdyskäytävät		
INTEGRAATTORI		• Toimituskokonaisuuden ymmärtäminen	• Asennus & päivitys • Integrointi, rajapinnat • Konfigurointi, • Kovennus, testaus, raport.		
AUTOMAATIO-JÄRJESTELMÄ-TOIMITTAJA	• Alustojen tuki • Sovelluskehitys • Kehitys, testaus, ylläpito	• Kovennusohje	• Asennus & päivitys, esiasetukset, paketointi • Kovennusohje, kovennus, -testaus, -raportti	• Järjestelmätuki • Huoltosopimuksen alaiset toimet • Muutosten testaus	• Hävitys-menettelyt
LAITE-, SOVELLUS-, OHJELMISTO-TOIMITTAJA	• Alustakehitys • Kehittää, testaa ja ylläpitää tuotetta	• Kovennusohje	• Alusta, laite-, sovellus-, ja ajurituki • Paketointi, päivitykset • Kovennusohje, kovennus, -testaus, -raportti	• Tuotetuki • Huoltosopimuksen alaiset toimet • Muutosten testaus	• Hävitys-menettelyt
	TUOTE-KEHITYS	HANKINTA	TESTAUS & KÄYTTÖÖNOTTO	TUOTANTO & YLLÄPITO	POISTO

Kuva 7. Toimijoiden päätehtävät kovennuksen elinkaaressa - Ohjelmistoasennukset ja päivitykset.

Kovennuksen ylläpito

Tilaaja on viimekädessä itse vastuussa kovennuksen ylläpitäjien määräämisestä ja kovennuksen ylläpitoon liittyvistä prosesseista!

Edellä kuvatuilla toimijoilla (Roolit) voi tietenkin olla koventamiseen liittyen useampia eri rooleja. Roolien tehtävät voivat myös olla osin päällekkäisiä.

Seuraavissa kuvissa on esitetty malli koventamisen tehtävistä rooleittain ”Ohjelmistoasennusten ja -päivitysten” käyttötapauksessa. Avainroolit on kehystetty punaisella.

"Tehtävät"	Tilaaja	Pääprojekti-toimittaja	Integraattorit	Automaatio-järjestelmä-toimittajat	Laite-, sovellus- ja ohjelmisto-toimittajat	Tietoturva-expertit
ALUSTAT: Alustojen hallinta	Käyttö-järjestelmien *Roadmap* + käyttöönotto-suunnitelma	Koordinoi tarvittavat lisenssit ja *OS* tuen järjestelyt	Asennus & päivitys. Varmistaa HW&SW -yhteensopivuuden. Toimitukseen *Secure system boot*	Asennus & päivitys. Tukee käyttöönotto-suunnitelman alustoja	Alustakehitys. Laite- ja ajuri- ja sovellustuki alustoissa, tarjoaa päivitykset	Alustojen evaluointi & tietoturvatestaus
SOVELLUKSET: Sovellusten hallinta	Sallitut sovellukset (elinkaaressa) ja *3rd party* ohjelmistot	Lukitsee valitut sovellukset	Integroi sovellukset eri järjestelmiin. Asennus & päivitys.	Sovelluskehitys, testaus. Asennus & päivitys.	Kehittää ja ylläpitää tuotetta. Laite- ja ajurituki sovelluksille, päivitykset	Sovellusten evaluointi & tietoturvatestaus
TOIMINNALLI-SUUDET: Toiminnallisuuden määrittely	Toimitettava toiminnallisuus, toimitusraja, mitä toimitukseen ei kuulu	Suunnittelee toimituksen sisällön	Integroi eri järjestelmien toiminnallisuuden	Tukee toimitettavaa toiminnallisuutta	Kehittää ja ylläpitää toiminnallisuutta	Voi varoittaa aiemmin riskialttiista toiminnallisuudesta
TUNNUKSET: Käyttäjätunnusten ja salasanojen hallinta	Käytännöt ja vaatimukset käyttäjätilien ja salasanojen hallintaan	Määrittelee miten käyttäjätilit ja politiikat hallitaan projektissa	Käyttää eri käyttäjätilejä projektin aikana	Voi esiasentaa tarvittavat käyttäjätilit ja politiikat	Kehittää ja ylläpitää pääsynhallinnan toiminnallisuutta	Pääsynhallinnan arviointi & testaus
RAJAPINNAT: Sallittujen rajapintojen määrittely	Vaatii/määrittelee rajapinta-määrittelyjä komponenteille	Koordinoi/ määrittelee järjestelmien väliset rajapinnat	Integroi rajapinnat ja testaa yhteensopivuuden	Kehittää, testaa, käyttää ja ylläpitää rajapintoja	Kehittää, testaa, käyttää ja ylläpitää rajapintoja	Rajapintojen arviointi & tietoturvatestaus
PROTOKOLLAT: Sallittujen protokollien määrittely	Vaatii standardeja ja testattuja liikennöinti-menettelyjä	Koordinoi protokollat ja liikennöinti-menettelyt	Konfiguroi tarvittavat protokollat ja menettelyt	Kehittää, testaa ja ylläpitää protokollia	Kehittää, käyttää ja ylläpitää protokolla-toteutuksia	Protokollien ja menettelyjen arviointi ja tietoturvatestaus

Kuva 8. KOVENTAMISEN TYÖNJAKO: "Ohjelmistoasennukset ja -päivitykset"-käyttötapaus (osa-1).

"Tehtävät"	Tilaaja	Pääprojekti-toimittaja	Integraattorit	Automaatio-järjestelmä-toimittajat	Laite-, sovellus- ja ohjelmisto-toimittajat	Tietoturva-expertit
IP OSOITTEET: Sallittujen verkko-osoitteiden määrittely	Määrää IP osoiteskeemat ja verkko-alueet	Osoitteiden jako eri toimittajille, yhdyskäytävien & DMZ alueiden käyttö	Osoitteiden ja palomuurisääntöjen konfigurointi ja testaus	Mahdollinen verkko-osoitteiden esikonfigurointi ja palomuurisääntöjen asettaminen	Mahdollinen tuki IP protokollapinolle	Opastus
KOVENNUS-OHJE: Projektikohtaisen kovennusohjeen kehittäminen	Vaatii projektikohtaisen kovennusohjeen	Hallinnoi projektiin kovennusohjeet	Ymmärtää kokonai-suuden, joten varoittaa riskikohteista	Laatii ja testaa järjestelmän kovennusohjeen	Laatii ja testaa tuotteensa kovennusohjeen	Opastus, esimerkkimallien laadinta
KOVENNUS: Toimitettavan järjestelmän koventaminen	Vaatii koventamista	Koordinoi ja valvoo koventamista	Koventaa ja testaa kokonaisuuden käyttöönottoa varten ja laatii kovennusraportin	Koventaa ja testaa järjestelmänsä ja laatii kovennusraportin	Mahdollisesti koventaa ja testaa tuotteensa ja laatii kovennusraportin	Kovennuksen opastus ja mahdollinen testaus
TOIMITUS: Kovennetun järjestelmän toimitus tilaajalle	Vastaanottaa järjestelmä-komponentit sovituin menettelyin	Fasilitoi järjestelmän vastaanoton	Hyödyntää järjestelmä-komponentit sovituin menettelyin	Paketoi ja lähettää järjestelmän sovituin menettelyin	Paketoi ja lähettää tuotteen sovituin menettelyin	Opastus. Esim. PICARD-mallit
YLLÄPITO: Kovennuksen ylläpito	Hallinnoi ylläpitäjät, prosessit ja luvat ylläpidon toimille joilla säilytetään kovennus koko elinkaaren ajan			Tukee järjestelmäänsä. (Huoltosopimuksen alaiset toimet)	Tukee tuotetta (Huoltosopimuksen alaiset toimet)	Opastus, esimerkkimallien laadinta

Kuva 9. KOVENTAMISEN TYÖNJAKO: "Ohjelmistoasennukset ja -päivitykset"-käyttötapaus (osa-2).

Käyttötapaus – Tiedon kerääminen automaatiopuolelta ja raportointi

Seuraavissa kuvissa on esitetty malli koventamisen työnjaosta käyttötapauksessa ”Tiedon kerääminen automaatiopuolelta ja raportointi”, jossa tiedonsiirtoteknologiana käytettiin OPC UA:ta. Kuvissa avainroolit on jälleen kehystetty punaisella, lisäksi eroavaisuudet verrattuna edelliseen käyttötapaukseen on merkitty punaisella fontilla.

"Tehtävät"	Tilaaja	Pääprojekti-toimittaja	Integraattorit	Automaatio-järjestelmä-toimittajat	Laite-, sovellus- ja ohjelmisto-toimittajat	Tietoturva-expertit
ALUSTAT: Alustojen hallinta	Määrää esim. PLCt joista tieto kerätään sekä palvelimet johon tieto siirretään	<Koordinoi tarvittavat lisenssit ja *OS* tuen järjestelyt>	<Asennus & päivitys. Varmistaa HW&SW -yhteensopivuuden. Toimitukseen *Secure sys boot*>	<Asennus & päivitys. Tukee käyttöönotto-suunnitelman alustoja>	Tarvittaessa OPC UA sovelluksen porttaus alustaan ja/tai testaus alustassa	<Alustojen evaluointi & tietoturvatestaus>
SOVELLUKSET: Sovellusten hallinta	Määrää käytettävät turvalliset sovellukset ja yhdyskäytävät	<Lukitsee valitut sovellukset>	<Integroi sovellukset eri järjestelmiin. Asennus & päivitys>	<Sovelluskehitys, testaus. Asennus & päivitys>	OPC UA sovelluksen ja raportoinnin toteutus, testaus, sertifiointi ja päivitykset	<Sovellusten evaluointi & tietoturvatestaus>
TOIMINNALLISUUDET: Toiminnallisuuden määrittely	Määrää mitä tietoja kerätään ja mitä ei *"Konv/Aggr/Tunnel"* Mahdollisesti jopa OPC UA tietomalli	<Suunnittelee toimituksen sisällön>	<Integroi eri järjestelmien toiminnallisuuden>	<Tukee toimitettavaa toiminnallisuutta>	OPC UA sovelluksen ja raportoinnin toiminnallisuuden kuvaukset ja OPC UA tietomallit	<Voi varoittaa aiemmin riskialttiista toiminnallisuudesta>
TUNNUKSET: Käyttäjätunnusten ja salasanojen hallinta	<Käytännöt ja vaatimukset käyttäjätilien ja salasanojen hallintaan>	<Määrittelee miten käyttäjätilit ja politiikat hallitaan projektissa>	<Käyttää eri käyttäjätilejä projektin aikana>	<Voi esiasentaa tarvittavat käyttäjätilit ja politiikat>	Kehittää, määrittää ja ylläpitää pääsynhallinnan toiminnallisuutta	<Pääsynhallinnan arviointi & testaus>
RAJAPINNAT: Sallittujen rajapintojen määrittely	Määrää OPC UA GW:n ja -palvelimen DMZ alueelle	<Koordinoi järjestelmien väliset rajapinnat>	<Integroi rajapinnat ja testaa yhteensopivuuden>	<Kehittää, testaa, käyttää ja ylläpitää rajapintoja>	<Kehittää, testaa, käyttää ja ylläpitää rajapintoja>	<Rajapintojen arviointi & tietoturvatestaus>
PROTOKOLLAT: Sallittujen protokollien määrittely	Määrää OPC UA:n DMZ alueesta ylöspäin. Sertifikaattien hall.	<Koordinoi protokollat ja liikennöinti-menettelyt>	<Konfiguroi tarvittavat protokollat ja menettelyt>	<Kehittää, testaa ja ylläpitää protokollia>	Tietyt OPC UA profiilit, tietoturva-protokollat ja sertifikaatit	<Protokollien ja menettelyjen arviointi ja tietoturvatestaus>

Kuva 10. KOVENTAMISEN TYÖNJAKO: ”Tiedon kerääminen automaatiopuolelta ja raportointi” -käyttötapaus (osa-1).

"Tehtävät"	Tilaaja	Pääprojekti-toimittaja	Integraattorit	Automaatio-järjestelmä-toimittajat	Laite-, sovellus- ja ohjelmisto-toimittajat	Tietoturva-expertit
IP OSOITTEET: Sallittujen verkko-osoitteiden määrittely	<Määrää IP osoiteskeemat ja verkko-alueet>	<Osoitteiden jako eri toimittajille, yhdyskäytävien & DMZ alueiden käyttö>	<Osoitteiden ja palomuurisääntöjen konfigurointi ja testaus> OPC UA GW:n os.	<Mahdollinen verkko-osoitteiden esikonfigurointi ja palomuurisääntöjen asettaminen>	<Mahdollinen tuki IP protokollapinolle>	<Opastus>
KOVENNUS-OHJE: Projektikohtaisen kovennusohjeen kehittäminen	<Vaatii projektikohtaisen kovennusohjeen>	<Hallinnoi projektiin kovennusohjeet>	<Ymmärtää kokonaisuuden, joten varoittaa riskikohteista>	<Laatii ja testaa järjestelmän kovennusohjeen>	OPC UA sovelluksen kovennusohjeet (client, server, GW)	<Opastus, esimerkkimallien laadinta>
KOVENNUS: Toimitettavan järjestelmän koventaminen	<Vaatii koventamista>	<Koordinoi ja valvoo koventamista>	<Koventaa ja testaa kokonaisuuden käyttöönottoa varten ja laatii kovennusraportin>	<Koventaa ja testaa järjestelmänsä ja laatii kovennusraportin>	<Mahdollisesti koventaa ja testaa tuotteensa ja laatii kovennusraportin>	<Kovennuksen opastus ja mahdollinen testaus>
TOIMITUS: Kovennetun järjestelmän toimitus tilaajalle	<Vastaanottaa järjestelmä-komponentit sovituin menettelyin>	<Fasilitoi järjestelmän vastaanoton>	<Hyödyntää järjestelmä-komponentit sovituin menettelyin>	<Paketoi ja lähettää järjestelmän sovituin menettelyin>	<Paketoi ja lähettää tuotteen sovituin menettelyin>	<Opastus. Esim. PICARD-mallit>
YLLÄPITO: Kovennuksen ylläpito	<Hallinnoi ylläpitäjät, prosessit ja luvat ylläpidon toimille joilla säilytetään kovennus koko elinkaaren ajan> Oma sertifikaattien hallinta (CA) elinkaaressa			<Tukee järjestelmäänsä.> <(Huoltosopimuksen alaiset toimet)>	<Tukee tuotetta> <(Huoltosopimuksen alaiset toimet)> Sertifikaattien tuki elinkaaressa	<Opastus, esimerkkimallien laadinta>

Kuva 11. KOVENTAMISEN TYÖNJAKO: ”Tiedon kerääminen automaatiopuolelta ja raportointi” -käyttötapaus (osa-2).

Miten kovennusohje tehdään ja toiminnot priorisoidaan

Kovennusohjeen laadinta ei yleensä ole triviaali tehtävä, joten seuraavassa käymme läpi **kovennusohjeen** laadinnan yleisen käyttötapauksen.

Kovennusohjeen laadinnassa on huomioitava mm.:

- ALUSTAT: Sovi toimituksessa käytettävät alustat etukäteen. Alustoilla on erittäin suuri vaikutus koventamisen ja sen ylläpidon onnistumiseen. Esim. jos alustassa on paljon muuttuvia osia, koventaminen vaikeutuu.
- YMPÄRISTÖ: Selvitä millaiseen ympäristöön kovennettavat ohjelmistot ja järjestelmät asennetaan. Saat mm. tietää mitä mahdollisuuksia siellä on päivityksiin, vikakorjauksiin ja koventamisen ylläpitoon.
- SOVELLUKSET: Sovelluksista riippuu paljon miten kovennus tehdään ja miten sitä voi testata. Jos sovellus esim. käyttää dynaamisia TCP portteja ja/tai useita erilaisia protokollia, on testaaminen hankalaa.
- OSAAMINEN: Kovennusta tulee harjoitella. Koventamisen avaintehtäviin kannattaa allokoida siihen tottuneita osaajia.
- PRIORISOINTI: Tilaaja tietää mitkä toiminnot ovat kriittisiä ja mitkä eivät. Jos koventaminen edellyttää toimintojen priorisointia, ole yhteydessä pääprojektiin prioriteettien selvittämiseksi.

Kovennusohjeen laadinnan tehtäväjakoa on hahmoteltu seuraavissa kuvissa, jotka saattavat edistää yhteistyötä kovennuksen ohjeiden laadinnassa.

"Tehtävät"	Tilaaja	Pääprojekti-toimittaja	Integraattorit	Automaatio-järjestelmä-toimittajat	Laite-, sovellus- ja ohjelmisto-toimittajat	Tietoturva-expertit
ALUSTAT: Alustojen hallinta	Tietoa alustojensa elinkaaresta. Alustojen priorisointi	Kokemusta eri alustojen ongelmista	Tuntee alustojen integroinnin ongelmat	Seuraa alustojensa päivityksiä ja vikapaikkoja	Tukee alustoja	Alustojen tietoturva-ominaisuuksien tuntemus
SOVELLUKSET: Sovellusten hallinta	Suunnittelee sovellusten elinkaaren ja priorisoinnin	Suunnittelee sovellusten asentamisen	Tuntee sovellusten asennuksen ongelmakohdat	Tuntee sovelluksensa heikkoudet, esim. arkkitehtuurissa	Tuntee tuotteensa heikkoudet, esim. laiteajurit	Sovellusten heikkouksien tuntemus
TOIMINNALLI-SUUDET: Toiminnallisuuden määrittely	Tuntee kriittisen toiminnallisuuden. Priorisoi toiminnot	Tuntee toimituksen sisällön	Tuntee testauksen kautta heikkoudet	Tuntee järjestelmänsä toiminnallisuuden	Tuntee tuotteensa toiminnallisuuden	Voi ehdottaa kovennuskohteita
TUNNUKSET: Käyttäjätunnusten ja salasanojen hallinta	IAM järjestelmänsä ja politiikkojensa tuntemus	Kokemusta käyttäjätunnusten hallinnasta projekteissa	Tuntee esim. *admin*-tunnusten tarpeen projekteissa	Kokemusta käyttäjätunnusten hallinnasta projekteissa	Tuntee tuotteidensa pääsynhallinnan ominaisuudet	Voi ehdottaa hyviä käytäntöjä
RAJAPINNAT: Sallittujen rajapintojen määrittely	Tuntee järjestelmiensä liityntätarpeet	Ymmärtää rajapintojen määrän toimituksessa	Tuntee rajapintojen heikkoudet. Tunnistaa kriittiset rajapinnat	Tuntee järjestelmänsä rajapinnat	Tuntee tuotteidensa rajapinnat	Voi ehdottaa kovennettavia rajapintoja
PROTOKOLLAT: Sallittujen protokollien määrittely	Tarve yksinkertaistaa ja minimoida	Ymmärtää protokollien määrän toimituksessa	Tuntee yhteysmenettelyjen integroinnin ongelmat	Tuntee järjestelmänsä protokollat	Tuntee tuotteidensa protokollat	Voi ehdottaa testattavia protokollia

Kuva 12. Miten kovennusohje tehdään ja toiminnot priorisoidaan? (osa-1).

"Tehtävät"	Tilaaja	Pääprojekti-toimittaja	Integraattorit	Automaatio-järjestelmä-toimittajat	Laite-, sovellus- ja ohjelmisto-toimittajat	Tietoturva-expertit
IP OSOITTEET: Sallittujen verkko-osoitteiden määrittely	Tuntee sallitut IP osoitteet ja verkot laitoksessa	Tuntee sallitut IP osoitteet ja verkot projektissa	Kokemusta ICS verkkojen konfiguroinnista ja testauksesta	Kokemusta ICS verkkojen konfiguroinnista	Tuntee tuotteensa IP pinon ominaisuudet	Voi opastaa IP osoitteiden hallinnassa
KOVENNUS-OHJE: Projektikohtaisen kovennusohjeen kehittäminen	Tuntee projektin ja ympäristön vaatimukset	Tuntee projektin vaatimukset. Tuntee osaajat	Ymmärtää kokonaisuuden tarvitsemat käytännön tarpeet	Kokemusta koventamisesta. Testiympäristö kovennusohjeen kehittämiseen	Kokemusta tuotteensa heikkouksista ja koventamisesta	Voi ehdottaa soveltuvia ohjeita
KOVENNUS: Toimitettavan järjestelmän koventaminen	Priorisoi projektit. Tarvitsee tietoa kovennuksen tilasta	Kovennuksen aikataulutus ja seuranta	Tuntee integroinnin vaatimat kovennuksen purut. Kokemusta käyttöönotto-testaamisesta	Osaa koventaa järjestelmän projektin vaatimusten mukaisesti	Osaa koventaa tuotteensa eri ympäristöihin	Tuntee kovennukseen käytettäviä työkaluja. Voi testata kovennuksen
TOIMITUS: Kovennetun järjestelmän toimitus tilaajalle	Asettaa vaatimuksia toimitukseen ja sen sisältöön	Neuvoo projektikohtaisissa turvajärjestelyissä	Kokemusta komponenttien vastaanotosta ja testaamisesta	Kokemusta toimitukseen kuuluvien komponenttien paketoinnista	Osaa paketoida tuotteensa projektitoimitukseen	Voi ehdottaa turvallisia siirtomenettelyjä
YLLÄPITO: Kovennuksen ylläpito	Tuntee ylläpidon tehtävät ja aikataulut. Tilaa päivitykset			Tuntee järjestelmänsä päivitys- ja vikakorjaustarpeet ja tehtävät	Tuntee tuotteensa päivitys- ja vikakorjaustarpeet ja tehtävät	Voi ehdottaa ylläpidon käytäntöjä

Kuva 13. Miten kovennusohje tehdään ja toiminnot priorisoidaan? (osa-2).

OSA 3

AUTOMAATIOVERKKOJEN KYBERTURVALLISUUDEN MONITOROINTI

Tiedätkö varmasti kuka kalastelee teidän verkoillanne?

3. AUTOMAATIOVERKKOJEN KYBERTURVALLISUUDEN MONITOROINTI

Yrityscase 1 – Tuotantoautomaatioverkon monitorointi – Konseptin kehittäminen ja validointi

Tietoturvan todellisen tilannekuvan aikaansaaminen automaatiojärjestelmistä on yksi KYBER-TEO-hankkeen tavoitteista. Tilannekuva mahdollistaa muun muassa automaation tietoturvan seuraamisen sekä mielekkäämmän automaatio-IT-rajapinnan tietoturvayhteistyön. Tässä yritystapauksessa toteutettiin *proof-of-concept (PoC)* monitoroinnista konseptitasolla, sekä mietittiin käytännön haasteita ja toteutusmahdollisuuksia.

Tilannekuva

Tietoturvan tilannekuva on erilainen ulkoistetun tietotekniikkatoimijan kannalta kuin automaation kannalta. Tässä tilannekuva tulee määritellä automaation toiminnan kannalta: se on reaaliaikainen ja historiatiedon sisältävä kuva automaatioon vaikuttavista tekijöistä, joiden avulla voidaan tehdä luotettavia päätelmiä tuotannon jatkuvuuden suhteen.

Tietointegraatio

Automaation tilannekuva pitää integroida automaation operointiin, mutta koska automaation käyttäjä ei ole tietoturvan ammattilainen, tietoturvan monitorointiin suunnitellut kompleksiset ohjelmistot eivät sellaisenaan sovi automaation tietoturvan monitorointiin. Tämä oli helppo todeta tutkittuamme ohjelmistojen raportointi- ja ongelmanratkaisutyökaluja. Arvioidut tuotteet eivät sovellu esimerkiksi helppoon historiatiedon läpikäyntiin, puhumattakaan integrointiin automaatiojärjestelmän muihin tietovirtoihin. Historiatieto ja integraatio ovat automaatiojärjestelmissä perustoiminnallisuutta, jonka tavoitteena on tukea ongelmanratkaisua. Tästä perustoiminnallisuudesta luopuminen tietoturvan osalta on järjetöntä.

Automaation näkökulmasta tietoturvamonitorointiohjelmia on pidettävä uutena mittauksena. Kuten muutkin uudet mittaukset, on niillä oltava selkeä käyttötarkoitus ja niiden käyttöönoton tavoitteena pitää olla automaation luotettavuuden ja tuottavuuden parantuminen. Parhaiten tämä on saavutettavissa tietointegraation kautta. Automaatiojärjestelmät keräävät nykyisin merkittävän määrän tietoa. Prosessiin liittyvän tiedon lisäksi kerätään jo kytkinten tilatietoja sekä käyttöjärjestelmien lokitietoja. Monitoimittajaympäristössä on kuitenkin haastavaa tunnistaa kaikki tiedonkeruupisteet, joista kannattaa syöttää tietoa tietoturvasensoreille. Tarvittava tiedonsiirto onkin tapauskohtaista ja vaatii yleensä esim. projektiorganisaation tukea, jotta kokonaisuus saadaan hallintaan.

Selvitettäviä asioita

Automaation tilannekuvan aikaansaaminen vaatii mm. seuraavien asioiden läpikäyntiä

- Selvitetään mitä tietoturvaan liittyviä mittauksia on jo saatavilla ja mistä nämä mittaukset on saatavilla.
- Kannattaako aktiivista monitorointia käyttää?

- Selvitetään automaation kannalta järkevin tapa koostaa tilannekuva. Mihin se tuotetaan?
- Selvitetään tietoturvamonitoroinnin toteutus ja organisointi automaation ongelmaratkaisun kannalta.
- Voidaanko tietoliikennetieto tuottaa automaatiojärjestelmän tiedonkeruuta hyväksikäyttäen?
- Voidaanko integroida tietoturvasensorin ulostulo automaation tiedonkeruuseen, josta se on tuotavissa automaatio-operointiin?

Johtopäätökset

Johtopäätöksinä voidaan sanoa, että:

- tietoturvasensorit kannattaa integroida automaation operointiin
- tietoturvan monitorointi on automaation kannalta uusi mittaus
- mittauksen esitystapa pitää olla sellainen, että se toimii operoinnin päätöksenteon tukena
- tietoturvan monitorointi mahdollistaa tietoturvatilannekuvan yli automaatio-IT-rajapinnan

Tietoturvan monitorointi automaatioympäristössä on haastavaa. Automaatio-operaattorin rooli on merkittävä, koska hänellä on kyky arvioida ongelmia järjestelmän toiminnan kannalta. Kun integroidaan ”tietoturva” uutena mittauksena automaatiojärjestelmän tietovirtoihin, voidaan tietoturvan tilannekuva esittää helpommin operaattorille. Toisaalta tietoturvavalvomoon *(Security Operations Center, SOC)* ulkoistettu tietoturvan monitorointi voi hyvinkin olla järkevää tuotannon tukijärjestelmien seurantaan. Automaation osalta tarvitaan kumppanuus, jossa automaatio- ja tietoturvaorganisaatiot yhdessä tuovat tietoturvamonitoroinnin automaatiokäyttöä tukevaksi työkaluksi.

Yrityscase 2 – Tuotantoautomaatioverkon monitorointimenetelmien ja laitteiden kartoittaminen

Tässä yrityscasessa tavoitteena oli määritellä soveltuvimmat konseptit ja menetelmät valittujen tuotantoyksiköiden tuotantoverkkojen kyberturvallisuustilanteen yksityiskohtaiseen valvontaan.

Ensimmäiseksi määriteltiin yhdessä päätehtävät, jotka tulee yhdessä suunnitella ja sovitun osapuolen toteuttaa. Nämä päätehtävät olivat seuraavat:

1. Monitorointikohteiden ja toimintaympäristön kuvaus
2. Uhat joita vastaan monitoroitava
3. Monitorointimenetelmien ja työkalujen esiselvitys
4. Verkkovalvonnan datan lähettäminen
5. Monitorointimallin kehittäminen
6. Pilottiprojektin suunnittelu

Näitä päätehtäviä käsitellään seuraavassa hieman lähemmin.

Monitorointikohteiden ja toimintaympäristön kuvaus

Tuotannon monitoroinnin kohdejärjestelmien ja -verkkojen tarkentamiseksi tekemämme selvitykset sisälsivät mm. seuraavaa:

- Monitoroitavien tuotantoyksiköiden valitseminen
- Tuotantoyksikön verkkokaavion tarkastelu
    - Mukaanlukien tuotantoyksikön aliverkot
    - Perehdytään yhdessä tärkeimpiin tiedonsiirtoreitteihin
- Määritellään mitä verkkoja ja protokollia tulisi monitoroida per tuotantoyksikkö. Esim:
    - [Prosessiautomaatioverkko ja sen protokollien nimeäminen]
    - [Yksikön käyttöautomaatio ja sen protokollien nimeäminen]
    - [Järjestelmätoimittajan aliverkko ja sen protokollien nimeäminen]
- Määritellään miten monitoroitava verkkoliikenne kopioidaan analysoitavaksi:
    - [Peilaus kytkimistä]
    - [Käyttämällä *network tap*-ratkaisuja]
    - [Reitittinten tai kytkinten lokien hyödyntäminen]
- Pohditaan data-diodi ratkaisujen käyttöä yksisuuntaisuuden pakotukseen, jolloin tuotantoprosessit eivät voi vahingossakaan saada asiatonta dataa/ohjausta

Uhat joita vastaan monitoroitava - Esimerkki

Tässä kohdassa suositeltiin tuotannolle tehtävää kattavaa uhka-analyysiä, ellei sellaista oltu jo tehty. Uhka-analyysin tuloksena saadaan tunnistettua tarkemmin monitoroitavia kriittisiä kohteita ja toimintoja.

Monitoroitavat kyberuhat voivat sisältää esimerkiksi:

Haittaohjelmien tunnistaminen

- Yleiset haittaohjelmat tulee havaita liikenteestä

Häiriöiden tunnistaminen

- Oikea toiminta tunnistetaan ja tallennetaan se *baselineksi*
- Laite- ja ohjelmistovikoja tulee tunnistaa verkkoliikenteestä
- Luvaton uusi verkkolaite havaittava verkkoliikenteestä

Tunnettujen haavoittuvuuksien seuranta

- [Määrättyjen tunnettujen] haavoittuvuuksien hyväksikäyttöjen havaitseminen, jolloin *signaturet* tarvitaan

Kohdistetut hyökkäykset

- [Määrätyt] kohdistetut hyökkäykset on havaittava
- [Uudet verkkoyhteydet] *Netflows* on havaittava
- [Normaaliliikenteen poikkeavuudet] on havaittava
- [Ylimääräinen kuorma, dataliikenne, tms., on havaittava]

Monitorointimenetelmien ja työkalujen esiselvitys

Tässä päätehtävässä suoritettiin esiselvitykset, joiden tuloksena hahmottuivat yrityscaseen soveltuvat monitorointimenetelmät ja työkalut. Selvitykset sisälsivät mm.:

SOVELTUVA MONITOROINTI-TYYPPI:

- Passiivinen/aktiivinen?
- Staattinen/dynaaminen?
- Hajautettu/keskitetty?

ANALYYSIN AJANKOHTA:

Online VAI *Offline* analyysi tuotantokäyttöön?

- Halutaanko verkkoliikennettä analysoida reaaliaikaisesti vai jaksottaisesti?

TYÖKALUT: Soveltuvimmat työkalut

- Selvitetään CASEEN soveltuvimmat verkkomonitoroinnin menetelmät ja työkalut
- Työkaluesimerkkejä: *McAfee-tuotteet, Clarified Analyser, PaloAlto-tuotteet, ArcSight*
- *Open source*-tuotteet, arvioidaan näiden tuotevastuu-vaikutukset

MONITOROINTIPISTEET: Mistä monitoroitava data otetaan?

- Selvitetään sopivimmat pisteet monitorointidatan lähteiksi

HÄLYTYKSET: Hälytyksen tuottaminen

- Mistä tapahtumista hälytys generoidaan? Ylätason kuvaus hälytyksen aiheuttavista tekijöistä

Verkkovalvonnan datan lähettäminen

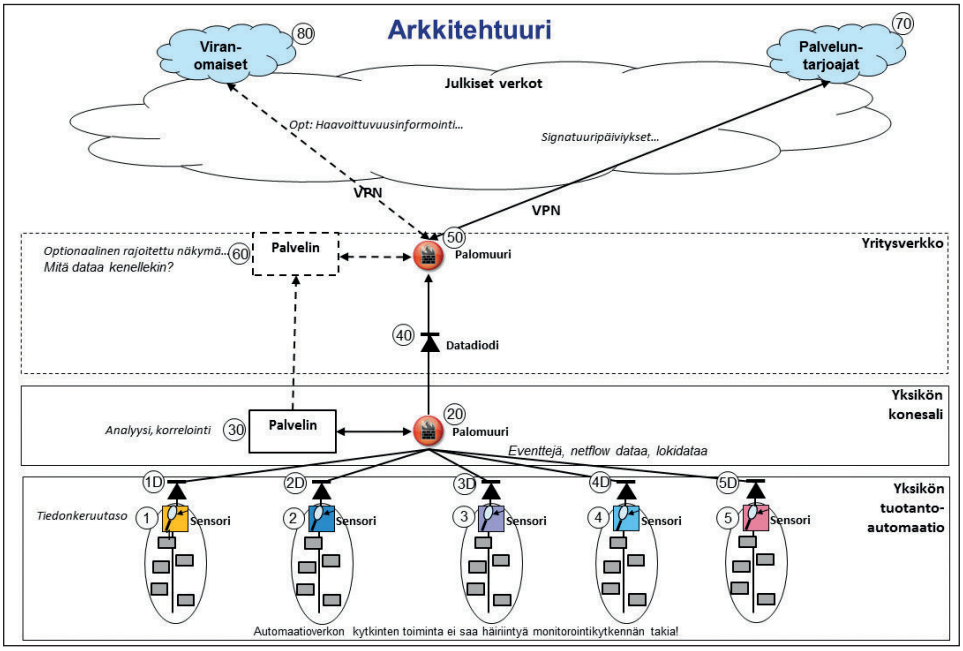
Tässä päätehtävässä selvitettiin mitä dataa lähetetään, mihin ja millä keinoin. Lisäksi määritettiin ne keinot joilla datan siirto suojataan asianmukaisesti:

- SISÄISESTI: Mitä dataa siirretään tuotantoyksikön sisällä: [Sensoreista eventtejä, tietovuo- ja lokidataa konesaliin.]
- MITÄ ULOS: Mitä lähetetään yksikön ulkopuolelle analysoitavaksi ja kuinka usein: [Kriittisimmät eventit/lokit/tietovuot siirretään ulkopuolelle tutkittaviksi tarvittaessa.]
- SUOJAUS: Miten siirto on suojattava:
  - [Data-diodi automaatioon, jonka jälkeen palomuuri ja palvelin. Palvelimen rajoitettuun näkymään vahvasti autentikoitu ja valvottu VPN yhteys vain rajatusta IP-avaruudesta (vain palveluntarjoajalta).]
- MIHIN:
  - [Raakadata konesaliin yksikön sisällä]
  - [Tulosraportit kunnossapitoon, valvomoon, keskushallintoon]
- MITEN:
  - [Kun tietty haavoittuvuus on monitoroitava (viranomainen, valmistaja): Keinoina esim. IDS-kuvauskantojen päivitys, datan lähetys analysoitavaksi tietoturvapalveluntarjoajalle, tms.]

Lisäksi on huomioitava, että yleensä tunkeutumisen havaitsemisjärjestelmän tehokas käyttö edellyttää säännöllistä valvontaa ja järjestelmän konfigurointia. Tämä vaatii erityisasiantuntijaosaamista.

Monitorointimallin kehittäminen

Yrityksen tuotantoyksikön tai yksiköiden automaatioverkkojen onnistunut kyberuhkien seuranta edellyttää soveltuvan monitorointimallin kehittämistä, joka sisältää järjestelmän arkkitehtuurin, pääominaisuuksien kuvaukset, käytettävien menetelmien kuvaukset, sekä yleensä myös pilottiprojektin suunnitelman, jossa mallin toimivuus todennetaan ennen käyttöönottoa tuotantoon. Seuraavassa kuvassa on esitetty eräs malliarkkitehtuuri esimerkki:



Kuva 14. Esimerkki – Arkkitehtuuri tuotantoautomaatioverkkojen kyberturvallisuuden monitoroimiseksi.

Monitorointikonseptin ominaisuuksia

Esimerkki monitorointikonseptille asetetuista ominaisuuksista on esitetty seuraavaksi:

A) Modulaarinen ratkaisu:

- Helppo laajentaa ajan kuluessa

B) Mahdollistaa eri menetelmät

- Lokianalyysi
- NetFlow: Tietovuomuutokset
- Signatuuripohjaiset menetelmät
- Evaasiotekniikoiden tunnistus?

C) Uhkien ja riskien mukainen seuranta

- Sisäiset uhat
- Ulkoiset uhat
- Tunnetut uhat, uudet uhat

D) Perustuu tutkittuun verkkoliikenteeseen

- Käytetyt protokollat, yhteydet, volyymit

E) Mahdollistaa tapahtumien analyysin aikajanalla; tallentaa historiatiedon

F) Mahdollistaa sovitun tiedon- ja työnjaon

- Operaattorille tieto tuotantoverkon muutoksista ja tietoturvahälytyksistä korkealla tasolla (uhka / ei uhkaa)
- Viranomaiselle tiedotus?
- Tietoturvapalvelun tarjoajalle dataa verkon eventeistä ja tarvittaessa *pcaps*

Monitoroinnin päämenetelmät

Caseen soveltuvat automaatioverkkojen monitoroinnin päämenetelmät tulee myös kuvata seikkaperäisesti. Seuraavassa kuvassa on esimerkki soveltuvista monitorointimenetelmistä:

Menetelmä	Monitorointi-kohde	Toiminta-periaate	Kypsyystaso	Laajennukset	Puutteita	Työkaluja	Raportointi
Tietovuo-seuranta (Netflow analysis)	Verkkoliikenne / pcap-tiedostot	Laitteiden välisten datayhteyksien seuranta	Laajasti käytössä tuotannossa	Hälytysrajat, uusien yhteyksien tunnistus	Yhden-suuntaiset yhteydet hankalampia	Ntop, Clarified Analyser, ym.	Tietovuot. Huom: kiinteät portit helpottaa
Lokianalyysi	Järjestelmä-lokit	Tallentaa määritellyt järjestelmä-tapahtumat	Laajasti käytössä tuotannossa	Eri lokien korrelointi	Vaatii kellojen synkronoinnin, lokien puutteet	Järjestelmä-kohtaisia	Lokitiedostot, syslog
Signature-tunnistus (Event patterns)	Verkkoliikenne / pcap-tiedostot	Tunnistaa tunnettuja hyökkäyksiä	Laajasti käytössä tuotannossa	Mm. Poikkeamien tunnistus	Tunnistaa vain tunnettuja uhkia	Lähes kaikki NIDS työkalut, Snort IDS	Eventit
Lähtötila-testaukseen	Verkkoliikenne / pcap-tiedostot	Tunnistaa protokolla-rakenteen	Laajasti käytössä tuotannossa	Uusien protokolla-rakenteiden määrittely	Vaatii protokollan perusrakenteen tuntemisen	Wireshark, KALI, Codenomicon TCF, ym.	Verkkoliikenne-raportti

Kuva 15. Esimerkki – Soveltuvia kyberturvallisuuden verkkomonitorointimenetelmiä.

Tämän lisäksi kullekin aliverkolle määritetään soveltuva(t) monitorointimenetelmät niissä käytettävien teknologioiden ja muiden rajoitusten ja tavoitteiden mukaisesti. Näitä yksityiskohtia ei kuitenkaan käsitellä tässä kirjasessa tarkemmin.

Pilottiprojektin suunnittelu

Pelkkä laboratoriossa tapahtuva monitorointimenetelmien testaus, evaluointi ja määrittely ei kuitenkaan vielä riitä mikäli halutaan varmistaa, että monitoroinnilla ei ole haittavaikutuksia tuotantoon. Tätä voidaan kuitenkin arvioida soveltuvissa pilottiprojekteissa, joissa monitorointikonsepti otetaan käyttöön normaalia pienemmässä mittakaavassa. Pilottikäyttö on usein myös toiminnallisesti rajoitetumpaa kuin normaali, tuotantoyksikön kattava käyttö. Tällä tavoin mahdolliset vahingot voidaan minimoida.

Seuraavassa kuvassa on esitetty eräs malliesimerkki monitoroinnin pilottiprojektin vaiheista ja päätehtävistä:

Vaihe	Päätehtävät	Kuvaus	Huom.
Kartoitus	Automaatiojärjestelmien ja verkkojen selvitykset	Kartoitetaan järjestelmien ja verkkojen nykytila	Yleiskuva yksikön verkoista
	Monitorointimenetelmien analyysit, työn suunnittelu	Analysoidaan soveltuvia monitorointi-menetelmiä ja potentiaalisia työkaluja. Tunnistetaan soveltuvia palveluntarjoajia	Suunnitellaan työn eteneminen, esim. partnerin kanssa
Pilottiprojekti	Pilotin tavoitteet ja rajaus	Selvitetään ja testataan soveltuvimmat menetelmät ja työkalut eri tilanteisiin	Rajoitettu pilotti jotta saadaan tuloksia
	Verkkoliikenteen analyysi	Selvitetään ja mitataan monitoroitavien verkkojen verkkoliikenne, kommunikoivat noodit, protokollat, sovellukset, liikennemäärät	Vaatii pääsyn verkkoliikenteeseen ja liikennetiedostojen tallennuksen
	Rakennetaan testiverkko	Verkkokartoituksen ja verkkoliikenteen perusteella rakennetaan testiverkko kokeita varten	Uudet kytkimet tarvitaan, arkkitehtuuri analysoidaan ja päivitetään
	Monitorointimenetelmien ja työkalujen testaus	Testataan soveltuvimmat menetelmät ja työkalut kuhunkin verkkoon ja käyttötarkoitukseen	*Open source*-alustat huomioidaan, kaupallisten tuotteiden evaluaatiot
Käyttöönottoprojekti	Suunnitelma	Sisältäen: Testaus, asennus, käyttöönotto, käyttö, ylläpito, ym.	Priorisoitu käyttöönotto eri verkoissa

Kuva 16. Esimerkki – Verkkomonitoroinnin pilottiprojektin suunnittelu.

Toteutetun yritystapauksen lopputuloksena voimme todeta, että tuotantoon soveltuvan monitorointikonseptin kehittäminen on vaativa tehtävä, joka vaatii monipuolista osaamista ja yhteistyötä tuotannon eri osa-alueiden erikoistuntijoiden kanssa.

Tärkeänä julkisena tuloksena saavutettiin toimintamalli, jota soveltamalla muutkin teollisuusyritykset voivat kehittää omalle tuotannolleen ja automaatioverkoilleen soveltuvat monitorointikonseptit.

OSA 4

SOPIMUSMALLIT AUTOMAATIO-HANKINNOISSA

Johdon tulee kiinnittää sopimusosapuolten työnjako ja varautumistehtävät.

4. SOPIMUSMALLIT AUTOMAATIOHANKINNOISSA

Aikaisemmissa projekteissamme olemme käsitelleet paljon automaatiojärjestelmien hankintoihin liittyviä kysymyksiä. Olemme määritelleet tietoturvavaatimuskannan, jota voi mm. käyttää pohjana vaatimuksille automaatiojärjestelmätoimittajien kyberkyvykkyyttä arvioitaessa, sekä varsinkin itse toimitettavan järjestelmän tai palvelun vaatimuksina, jne.

Laaja tietoturvavaatimuskanta saattaa kuitenkin olla vaikea hahmottaa kokonaisuutena vaatimusten suuren lukumäärän ja laajuuden vuoksi, siksi olemme aiemmissa projekteissa määritelleet myös lyhyet ohjeet automaatiohankintojen määrättyjen tietoturvakysymysten hallitsemiseksi. Nämä yhden A4-sivun ohjeet kirjoitettiin seuraaville osa-alueille: etäyhteydet, langattomat järjestelmät, kovennus, muutostenhallinta, sekä käyttäjäoikeudet.

Monien yritysten tuotannon, automaation, tai hankintaosaston henkilöstön kyberturvallisuustietoisuudessa on kuitenkin edelleen puutteita. Mm. erilaiset tietoturva- ja kyberturvallisuusliitteet ja säännöt saavat valitettavasti edelleen varsin vähäistä huomiota monessa automaation toimitus- tai palvelusopimuksessa. Tämän vuoksi edelleen lisää hyviä käytäntöjä ja esimerkkejä tälle alueelle tarvitaan.

Tässä kirjasessa esittelemmekin eräitä uusia mm. Kyberturvallisuuskeskuksen kanssa yhdessä kehitettyjä liiteluonnoksia, nimittäin: **”Automaatiojärjestelmien toimitus- tai palvelusopimusten tietoturvaliitteitä”**.

Yhdessä kehitetyt tietoturvaliitteiden malliluonnokset sisältävät tässä vaiheessa yhden ylätason tietoturvaliitteen ja kuusi siihen liittyvää alaliitettä. Yritykset voisivat soveltaa malliliitteitä tarpeensa mukaan, esim. jättää tarpeettomia tietoturvaliitteitä pois, muokata haluamiaan liitteitä ja/tai lisätä uusia, itselleen paremmin soveltuvia liitteitä.

Seuraavilla sivuilla luonnostelluissa liitemalleissa on pyritty siihen, että sopimuskohtainen määrittely kootaan ylimmän tason tietoturvaliitteeseen, ja toisaalta alaliitteet olisivat sitten mallikuvauksia ja määritelmiä asioista, joita halutaan yksityiskohtaisemmin pakottaa noudatettavaksi ko. toimituksessa. Luonnostelemamme liitteet sisältävät:

- TIETOTURVALIITE: ylätason liite
- Tietoturvaliite 2 – tietoturvakatselmoinnin esityslista
- Tietoturvaliite 3 – raportointikäytäntö
- Tietoturvaliite 4 – varmuuskopiointikäytäntö
- Tietoturvaliite 5 – etäyhteysjärjestelyt
- Tietoturvaliite 6 – etäyhteyskäyttösopimus
- Tietoturvaliite 7 – automaattisesti siirrettävä data

Yllä mainitut liitteet valittiin kehityskohteiksi siksi, että mielestämme niiden kattama työnjakomalli ja toiminta tulisi olla osa lähestulkoon kaikkien uusien automaatiojärjestelmien toimitus- tai palvelusopimusta.

Seuraavilla sivuilla on kuvattu luonnokset näistä malliliitteistä, ensimmäisenä on esitetty korkean tason kokoava ”TIETOTURVALIITE”.

TIETOTURVALIITE

Sisältö

Tämä tietoturvaliite liittyy osapuolten välillä ___.___.20____ solmittuun [projektitoimitus-sopimukseen / palvelusopimukseen], ja kuvaa kyseisessä sopimuksessa yksilöidyn toiminnan ja toimituksen tietoturvallisuutta.

Tämä liite voi sisältää useita alaliitteitä, joissa noudatetaan [projektitoimitussopimuksessa / palvelusopimuksessa] olevia ehtoja, jollei tässä liitteessä tai mainituissa, voimassaolevissa alaliitteissä ole erikseen muuta määritelty.

Noudattamisjärjestys

Jollei lainsäädännöstä muuta ilmene tai sopijapuolten välillä ole erikseen muuta sovittu, noudatetaan keskenään ristiriitaisissa ehtokohdissa ensisijaisesti [projektitoimitussopimuksessa / palvelusopimuksessa] mainittua sopimus- tai ehtojärjestystä. Jos sopimuksessa ei ole eritelty kyseistä asiaa noudatetaan ehtojen osalta seuraavaa järjestystä: velvoittava lainsäädäntö, kyseinen alaliite, tämä liite, projektisopimus, kauppatapa, ei-velvoittava lainsäädäntö.

Osapuolet

Sopimuksen osapuolet on mainittu [projektitoimitussopimuksessa / palvelusopimuksessa].

Tietoturvallisuuteen liittyvissä asioissa osapuolina, alihankkijoina tai palveluntarjoajina voivat olla [projektitoimitussopimuksessa / palvelusopimuksessa] mainittujen osapuolten lisäksi seuraavat toimijat. Nämä toimijat rinnastetaan osapuolten alihankkijoihin. Osapuolet vastaavat heidän [projektitoimitussopimuksen / palvelusopimuksen], tämän liitteen ja mahdollisten alaliitteiden mukaisesta toiminnastaan kuten omastaan.

Yritys/ organisaatio ja y-tunnus	Yrityksen yhteys-tiedot	Yhteyshenkilö	Yrityksen rooli / tehtävä

Voimassaoloaika

Tämä liite on voimassa:

- □ [projektitoimitussopimukseen / palvelusopimukseen määrätyn ajan tai]
- □ ___.____.20_____ - ____.____.20_____

Varmuuskopiointi

Datan varmuuskopioinnin suorittaminen on kuvattu tarkemmin alaliitteessä. Varmuuskopioinnissa tulee noudattaa seuraavia käytäntöjä aineiston osalta.

Aineiston nimi tai yksilöivä tunnus	Varmuuskopiointiväli tai työtehtävä jota ennen kopiot otetaan	Käytettävä varmitus-/ palautustekniikka	Varmistuksen sijoitus-paikka

Yhteydenottopiste ongelmatilanteissa

Molemmat osapuolet sitoutuvat ilmoittamaan toisilleen ja ylläpitämään omalla tahollaan keskitettyä yhteydenottopistettä, johon osapuolet voivat ilmoittaa automaatiojärjestelmässä tai sen tieto-aineistojen siirrossa esiintyvistä virheistä. Yhteydenottopiste voi olla esimerkiksi valvontakeskus, päivystäjä tai yksittäinen henkilö, jonka yhteystiedot annetaan toiselle osapuolelle. Muutostilanteissa on viipymättä ilmoitettava toiselle osapuolelle uusi yhteystieto.

Organisaatio	Yhteysosoite, puh. ja sähköposti	Päivystysaika

Alaliitteet

Tähän tietoturvaliitteeseen sisältyvät seuraavat alaliitteet, jotka tulee kuitata hyväksytyksi sopijapuolten allekirjoituksin:

Liitteen nimi	Sisältyy	Ei sisälly
Tietoturvaliite 2 - tietoturvakatselmoinnin esityslista		
Tietoturvaliite 3 - raportointikäytäntö		
Tietoturvaliite 4 - varmuuskopiointikäytäntö		
Tietoturvaliite 5 - etäyhteysjärjestelyt		
Tietoturvaliite 6 - etäyhteyskäyttösopimus		
Tietoturvaliite 7 – automaattisesti siirrettävä data		

Paikka ja päivämäärä

_____ ___.___.20___

[Osapuoli A] [Osapuoli B]

_____ _____

Nimi ja nimenselvennös Nimi ja nimenselvennös

_____ _____

LIITE – TIETOTURVAKATSELMOINNIN ESITYSLISTA

Tämä liite liittyy osapuolten välillä solmittuun [projektitoimitus-/palvelutoimitussopimuksen] tietoturvaliitteeseen ja määrittää tietoturvakatselmoinnissa läpikäytävät asiat.

Voimassaolo: [Projektitoimitussopimuksen/palvelusopimuksen mukainen tai]

___.___.20____ - ___.____.20____

Katselmoinnissa käsiteltävät asiat:

Jollei osapuolten välillä ole erikseen muuta sovittu, tulee tietoturvan katselmoinnissa käydä lävitse seuraavat asiat:

1) Edellisen katselmoinnin pöytäkirja ja toimenpiteiden seuranta.
2) Henkilö- tai yhteystietomuutokset osapuolten välillä.
3) Raportit: [Osapuolten] [toimittajien] [ja mahdolliset muut tietoturvaan liittyvät raportit].
4) Edellisen katselmoinnin jälkeen sattuneet tietoturvapoikkeamat ja muut merkittävät tapahtumat sekä niihin liittyvät toimenpiteet (perustuen esim. riskiarvioon).
5) Tietoturvaan tehdyt muutokset ja parannukset.
6) Koulutustapahtumat (ajankohta, sisältö, osallistujat, tavoite).
7) Voimassa olevat sopimukset: sisältävätkö ne tietoturvaosion ja onko se ajan tasalla.
8) Tietoturvan kehittämisen suunnitelma seuraavalle vuodelle, sisältäen mm:
    a. [Osapuolten] kehityssuunnitelmat
    b. toimittajien tietoturvan kehitysehdotukset ja muut parannusehdotukset,
    c. uudet tietoturvavaatimukset,
    d. uudet sopimukset,
    e. päivittyvät sopimukset.
9) Havaitut ongelmat tai muut esille tuotavat asiat.
10) Seuraavan kokouksen ajankohta.

LIITE – AUTOMAATIOJÄRJESTELMÄN RAPORTOINTIKÄYTÄNTÖ

Tämä liite liittyy osapuolten välillä solmittuun [projektitoimitus-/palvelutoimitussopimuksen] tietoturvaliitteeseen ja määrittää sopimuksessa mainitun järjestelmän tietoturvaraportointiin liittyvät käytännöt.

Voimassaolo: [Projektitoimitussopimuksen/palvelusopimuksen mukainen tai]

___.___.20____ - ___.___.20____

Raportointi:

Järjestelmän toimittajan tulee toimittaa raportti järjestelmän tietoturvallisuudesta raportin vastaanottajalle [vuosittaiset raportointipäivämäärät, esim. 2 krt/v] ellei muuta sovita.

Jollei osapuolten välillä ole erikseen muuta sovittu, järjestelmän tietoturvaraportoinnin tulee sisältää seuraavat asiat:

1) Merkittävät tietoturvatapahtumat koskien sopimuksessa määrätyn järjestelmän automaatiolaitteistoja ja -ohjelmistoja mukaan lukien:
    a. automaatiojärjestelmätoimittajan palvelimiin ja kehityslaitteisiin tulleet hyökkäykset ja vastaavat merkittävät tietoturvatapahtumat
    b. mikäli tietoja tallennetaan kolmannen osapuolen haltuun, heidän tietojärjestelmiinsä kohdistuneet hyökkäykset ja vastaavat merkittävät tietoturvatapahtumat
    c. tietojen välityskanavaan (operaattoriin, tietoliikennelaitteisiin) kohdistuneet hyökkäykset
2) Tietoturvaan tehdyt muutokset sopimukseen liittyvässä automaatiojärjestelmässä.
3) Tietoturvan parannusehdotukset sopimukseen liittyvään automaatiojärjestelmään.
4) Toteutuneen palvelutasoasteen vertailu sovittuun palvelutasoon.

Jos muuta ei ole sovittu, tarkoitetaan merkittävällä tietoturvatapahtumalla tilannetta, jossa ainakin yksi seuraavista kohdista toteutuu:

- järjestelmää vastaan hyökätään
- järjestelmä ei toimi tai sen normaalikäyttö estyy
- järjestelmä hidastuu huomattavasti vaarantaen järjestelmän käyttötarkoituksen
- järjestelmä toimii väärin
- järjestelmän sisältämät tiedot tai osa niistä on vääristynyt tai tuhoutunut
- järjestelmän sisältämät tiedot paljastuvat ulkopuoliselle
- järjestelmän käyttöoikeuksia on muutettu oikeudettomasti
- järjestelmän kautta on päästy tunkeutumaan toiseen järjestelmään

LIITE – AUTOMAATIOJÄRJESTELMÄN VARMUUSKOPIOINTIKÄYTÄNTÖ

Tämä liite liittyy osapuolten välillä solmittuun [projektitoimitus-/palvelutoimitussopimuksen] tietoturvaliitteeseen ja määrittää sopimuksessa mainitun järjestelmän varmuuskopiointiin liittyvät käytännöt.

Voimassaolo: [Projektitoimitussopimuksen/palvelusopimuksen mukainen tai]

___.___.20____ - ___.___.20____

Varmuuskopiointi:

Asiakas: [*Asiakas*]

Varmuuskopiointipalvelun tuottaja: [*Tuottaja*]

Asiakas omistaa varmuuskopioidun datan. *Tuottaja* saa käyttää varmuuskopion dataa vain Asiakkaan järjestelmien palautukseen tai muuten Asiakkaan kanssa erikseen sovittuun käyttötarkoitukseen.

[Asiakas ja tuottaja] vastaavat yhdessä, että häiriötilanteen sattuessa sopimuksen alainen järjestelmä tulee helposti ja nopeasti pystyä palauttamaan aiemmin testattuun ja määrätyllä tavalla toimivaan tilaan.

VASTUUT:

1) *[Asiakkaalla] tulee aina olla välittömästi käytettävissään sopimuksen alaisen järjestelmän toimivat varmuuskopiot.*
2) *[Tuottaja] vastaa, että tuotannossa olevaa järjestelmää vastaava varmuuskopio [ohjelmistokoodista, laiterekisteristä ja muista järjestelmäasetuksista] [ja vähintään yksi edellinen varmuuskopio] luodaan, siirretään ja säilytetään turvallisesti [Asiakkaan] tuotantoa häiritsemättä.*
3) *[Tuottaja] vastaa että ainoastaan [osapuolella] on turvallinen, luotettava ja välitön pääsy ko. varmuuskopioihin. [Pääsy taataan 24x7 tuntia viikossa].*
4) *[Tuottaja] vastaa, että käytöstä poistetut ja tarpeettomat varmuuskopiot tuhotaan turvallisesti. [Asiakkaalta] pyydetään kirjallinen lupa ennen varmuuskopion tuhoamista.*

KOHTEET:

1) *Varmuuskopioitavat kohteet sisältävät kaikki sopimuksen alaiset järjestelmät [käyttöjärjestelmät, sovellukset, laiterekisterit, asetukset ja kaikki automaatiojärjestelmän oikean toiminnan edellyttämät järjestelmäkuvaukset].*
2) *[Varmuuskopiointi sisältää myös automaatioon liittyvät apulaitteet ja tukijärjestelmät, kuten kytkinten asetukset, laiteajurit, …].*
3) *Varmuuskopiot arkistoidaan kotimaisille palvelimille [Asiakkaan] tuotannosta fyysisesti erillään olevaan sijaintiin ja niihin pääsy rajataan [ainostaan osapuolille].*

MUUT MENETTELYT:

1) *[Asiakas] varmistaa, että järjestelmästä otetaan toimiva varmuuskopio [ennen jokaisen järjestelmämuutoksen, esim. uuden päivityksen aloittamista].*
2) *[Osapuolet sopivat, että varmuuskopiointi koskee myös tuotantoprosessissa syntynyttä mittausdataa <X ja Y>].*

[Tuottajan] tulee dokumentoida palautusmenettely yksityiskohtaisesti ja testata sen oikea toiminta [vuosittain].

LIITE – AUTOMAATIOJÄRJESTELMÄN ETÄYHTEYSJÄRJESTELYT

Tämä liite liittyy osapuolten välillä solmittuun [projektitoimitus-/palvelutoimitussopimuksen] tietoturvaliitteeseen ja määrittää sopimuksessa mainitun järjestelmän etäkäyttöön liittyvät turvallisuusjärjestelyt.

Voimassaolo: [Projektitoimitussopimuksen/palvelusopimuksen mukainen tai]

___.___.20____ - ___.____.20____

Määräykset:

Jollei osapuolten välillä ole erikseen muuta sovittu, osapuolten tulee noudattaa seuraavia määräyksiä sopimuksessa mainitun automaatiojärjestelmän etäyhteyksien järjestämisessä.

ETÄYHTEYKSIEN LUPAMENETTELY:

1) Automaatioverkkoon kytkeytyminen tehdään ainoastaan virallisen lupamenettelyn kautta. Tämä koskee etäyhteyksiä ja paikallisia yhteyksiä.
2) LUVAT: Pääsyluvat ja tuen automaation kaikkiin järjestelmiin toimittaa [Osapuolen Automaatio-osasto]: Käyttäjätilit ja salasanat sopimuksessa mainitun järjestelmän automaation palomuuriin, säännöt / pääsylista automaatioverkon palomuurin läpäisyyn, sallitut etäyhteysohjelmistot ja niiden konfiguraatio, käyttäjätilit ja salasanat kohdetehtaan automaatiojärjestelmään
3) PÄÄSY: Oikeus automaation etäyhteyksiin myönnetään [toistaiseksi voimassaolevaksi] ja sovittuun käyttötarkoitukseen. Oikeuksien jatkotarve tarkistetaan [vuosittain].
4) KÄYTTÄJÄ: Henkilökohtaista etäyhteysoikeutta ei voi siirtää toiselle, ellei kyseessä ole erikseen sovittava Service-desk palvelutili.
5) KIRJANPITO: [Osapuolen IT osasto] pitää kirjaa etäyhteyksiin oikeutetuista henkilöistä, lupamenettelyistä ja lupien myöntäjistä.
6) Yritystason VPN-palvelujen pääsyluvat ja tuen toimittaa [Osapuolen IT käyttötuki: Yritystason VPN käyttäjätilit ja salasanat, sallitut etäyhteysohjelmistot ja niiden konfiguraatio]

ETÄYHTEYKSIEN TEKNISET JÄRJESTELYT:

1) KIELTO: Automaatiolaitetta tai -verkkoa ei saa koskaan kytkeä teknisesti suoraan Internetiin.
2) MALLIT: Etäyhteys muodostetaan ainoastaan käyttämällä [Osapuolen] määrittelemiä etäyhteysmalleja, -käyttösääntöjä, -ohjelmistoja, -asetuksia ja -ohjeita.
3) RAJOITUKSET: Kukin etäyhteys rajoitetaan teknisesti ainoastaan tarvittaviin automaatioverkon kohteisiin.
4) VALVONTA: Etäyhteyksien käyttöä valvotaan seuraamalla [etäyhteyspalvelimen ja palomuurien lokeja]. Etäyhteyksien käyttötapahtumat raportoidaan [kuukausittain tietoturvavastaavalle].

5) YRITYSTASON KYTKENTÄ: Automaation etäyhteyden synnyttämiseksi kytkeydytään aina [ensin Osapuolen yritystason VPN palveluun], jossa käyttäjä tunnistetaan.

6) AUTOMAATION KYTKENTÄ: Kryptografisesti tunneloitu etäyhteys kytketään [Osapuolen yritystason VPN-palvelusta] [Osapuolen laitoksen/yksikön] ylläpidettyyn automaation palomuuriin.

7) AUTOMAATIOLAITTEEN KYTKENTÄ: Pääsy [Osapuolen] automaation palomuurista [Osapuolen] automaatiolaitteeseen valvotaan automaatioverkon palomuurisäännöin [ja mahdollisesti palvelimen käyttäjäoikeuksin].

Päiväys ____._____.20_____

Allekirjoitus ja nimenselvennös:

_____

LIITE – AUTOMAATIOJÄRJESTELMÄN ETÄYHTEYSKÄYTTÖSOPIMUS

Tämä liite liittyy osapuolten välillä solmittuun [projektitoimitus-/palvelutoimitussopimuksen] tietoturvaliitteeseen ja määrittää sopimuksessa mainitun järjestelmän etäkäyttöön liittyvät turvallisuussäännöt.

Voimassaolo: [Projektitoimitussopimuksen/palvelusopimuksen mukainen tai]

___.___.20____ - ___.____.20____

Säännöt:

Jollei osapuolten välillä ole erikseen muuta sovittu, käyttäjän tulee noudattaa seuraavia määräyksiä käyttäessään automaatiojärjestelmiä etäyhteyksien kautta.

1) Käyttäjän tulee noudattaa tässä mainittuja määräyksiä ja muita etäyhteyden tarjoajan ja järjestelmän omistajan antamia turvallisuusohjeita.
2) Etäyhteyksissä käytetään liitteen [Etäyhteysjärjestelyt] mukaisia sääntöjä.
3) Tietokoneessa jolla etäyhteys muodostetaan (Etälaite), tulee olla käytössä ajantasainen [haittaohjelmien torjuntaohjelmisto]. Lisäksi Etälaitteessa tulee olla toiminnassa viimeisimmät toimivat tietoturvapäivitykset ja palomuuri. Palomuuri voi vaihtoehtoisesti sijaita myös Etälaitteen käyttäjäyrityksen turvallisen verkon ulkorajalla, mikäli etäyhteys otetaan yrityksen sisäverkosta.
4) Käyttäjä sallii, että Etälaitteelle voidaan tehdä turvallisuustarkistus ennen etäyhteyden sallimista.
5) Mainitulla etäyhteydellä saa olla yhteydessä vain yllämainitussa sopimuksessa mainittuun automaatioverkkoon [tai verkkoon X].
6) Käyttäjä sallii etäyhteyden valvonnan myös siirrettävän tiedon sisällön osalta ja vastaa asiattoman käytön seurauksista.
7) Etäyhteystunnuksia ei saa luovuttaa tai paljastaa muille missään muodossa.
8) Käyttäjä tekee kaikista epäilyttävistä tapahtumista välittömästi ilmoituksen [osapuolen yhteyshenkilölle]. Yhteyshenkilön tiedot löytyvät [tietoturvaliitteestä].
9) [Salassapitosopimus] koskee myös etäyhteyttä ja etäyhteyden kautta hankittuja aineistoja.

Etäyhteyden kautta hankitut aineistot tulee säilyttää ja tuhota turvallisesti [salassapitosopimuksen] mukaisesti.

Päiväys _____._____.20_____

Allekirjoitus ja nimenselvennös:

_____

LIITE – JÄRJESTELMIEN VÄLILLÄ AUTOMAATTISESTI SIIRRETTÄVÄ DATA

Tämä liite liittyy osapuolten välillä solmittuun [projektitoimitus-/palvelutoimitussopimuksen] tietoturvaliitteeseen ja määrittää sopimuksessa mainitun järjestelmän ulkopuolelle automaattisesti siirrettävän datan suojaussäännöt ja -käytännöt

Voimassaolo: [Projektitoimitussopimuksen/palvelusopimuksen mukainen tai]

___.___.20____ - ___.____.20____

Järjestelmien väliset rajapinnat:

[Osapuolten järjestelmien] väliset rajapinnat, sekä näiden välillä toteutettavaan automaattiseen tietoaineiston siirtoon käytettävät palveluntarjoajat, teknologiat, sovellukset, yhteysvälit (ml. lähetys- ja vastaanottopisteet), lähettäjän ja vastaanottajan tunnisteet, tietosisältö, dataformaatit [ja datan automaattinen uudelleen lähetys] on kuvattu erillisessä liitteessä, joka on [projektitoimitussopimuksen / palvelusopimuksen] liitteenä.

Automaattisesti siirrettävään dataan liittyvät turvallisuusmääritykset

Siirrettäessä aineistoa osapuolten järjestelmien välillä tulee noudattaa [projektitoimitussopimuksessa / palvelusopimuksessa], tietoturvaliitteessä ja tässä alaliitteessä mainittuja turvallisuusohjeita.

”Aineiston nimi / Yksilöivä tunnus” yksilöi siirrettävän aineiston, ”Eheyden varmistustekniikka” ilmaisee, millä mekanismilla tiedon autenttisuus ja eheys tulee varmistaa. ”Salaustekniikka” ilmaisee, millä salausmekanismilla siirrettävä/käsiteltävä tieto salataan. ”Max viive” määrittää mikä on suurin sallittu viive [verkoissa]. ”Korjaus (tuntia ilmoituksesta)” ilmaisee maksimiviiveen korjaukselle vikailmoituksen saapumisesta lukien. Jos jokin kohta on jätetty tyhjäksi, tarkoittaa se, että kyseisen aineiston suojaamista ei tarvitse tältä osin erityisesti varmistaa ja valvoa.

Aineiston nimi / Yksilöivä tunnus	Eheyden varmistustekniikka	Salaustekniikka	Max viive	Korjaus (tuntia ilmoituksesta)

OSA 5

JOHTOPÄÄTÖKSET JA JATKOTYÖ

Koeteltuja ratkaisuja on olemassa, joten rakentakaa yhdessä varautumisenne konseptit.

5. JOHTOPÄÄTÖKSET JA JATKOTYÖ

Johtopäätökset

Teollisuuden kyberturvallisuutta on kehitetty jo useita vuosia muutamien edelläkävijäyritysten johdolla. Kyseisissä kehityshankkeissa saavutetut julkiset tulokset ja toimiviksi todetut mallit ovat onneksi myös muiden kriittisten teollisuustoimijoiden käytettävissä, kunhan tukea tarvitseva toimija liittyy osaksi kansallista yhteistyöverkostoa. Verkoston yhteisiin sisäisiin tuloksiin pääsee käsiksi liittymällä Huoltovarmuuskeskuksen Huovi-portaalin ”Teollisuuden tietoturvan työpajat” hankealueen jäseneksi, sekä osallistumalla hankkeiden julkisten tulosten esittelytilaisuuksiin.

Koska materiaalia on kehitetty pitkään ja siten myös kertynyt paljon, ei sen läpi kahlaaminen yksin usein vielä riitä ymmärtämään vaativaa kokonaisuutta jota modernin, automatisoidun tuotannon laaja-alainen ja monitasoinen kyberturvaaminen edellyttää. Siksi suosittelemme osallistumista Huoltovarmuuskeskuksen ja VTT:n kyberturvallisuuden yhteisiin kehityshankkeisiin, joissa pääsee osalliseksi monien eri alueiden asiantuntijoiden osaamisesta ja käytännön kokemuksista. Tärkein esimerkki tällaisista hankekokonaisuuksista on alussa esitelty KYBER-TEO, jota pyöritetään peräti kolme vuotta (2014–2016), ja jossa kukin vuosi suunnitellaan erikseen ko. vuoteen osallistuvien yritysten tarpeista lähtien.

Meillä on lähes kaikki tarvittavat keinot ja työkalut ratkaista kyberturvallisuuteen liittyviä ongelmia, kunhan vain toimimme yhdessä ja omaa osaamistamme sitä tarvitseville jakaen. Tervetuloa mukaan yhteisöön!

Jatkotyö

Projekteissa laajennetaan mahdollisuuksien mukaan tulevaisuudessa tehtävää työtä mm. seuraavasti:

- Otetaan työn alle uusia teollisuuden sektoreita tai liiketoimintoja, joista mainittakoon erikseen teollisen internetin palvelut ja kiinteistöjen hallinta, mm. suurten riskien ja mahdollisuuksien vuoksi
- Selvitetään miten pilvipalvelut ja ”pilvenreuna” saadaan otettua hallintaan tärkeimmillä sektoreilla
- Selvitetään mitä uusia tai päivitettäviä kyberturvallisuuden rakenteita kilpailukyvyn ja joustavamman tuotannon edellyttämät toimet, kuten uusien sopimustoimittajien käyttö, uudenlainen vastuunjako, erilaiset ylläpitopalvelut, jne. edellyttävät.

KYBER-TEO-projektin osalta työpakettien otsikot säilyvät ainakin toistaiseksi ennallaan, eli kybersuojauksen käytännöt ja kartoitukset, kyberturvallisuuden jalkauttaminen kotimaiseen tuotantoon, sekä tuotantoautomaatioverkon monitorointipalvelut jatkavat työtään. Erityisesti kyberturvallisuuden testaus- ja monitorointipalveluja tullaan tulevaisuudessakin pohtimaan ja kehittämään vahvasti yhteistyössä osallistuvien yritysten kanssa.

REFERENSSIT

Aiempina tärkeinä referensseinä mainittakoon Suomen Automaatioseuran julkaisema ”Teollisuusautomaation tietoturva - verkottumisen riskit ja niiden hallinta”, sekä aihealueen perusteita selvittänyt TITAN-käsikirja. Alussa mainittujen hankkeidemme materiaalit löytyvät Huoltovarmuuskeskuksen HUOVI-portaalista ”Teollisuuden tietoturvan työpajat”-hankealueelta. Pääsyä HUOVIIN mainitulle hankealueelle voi tiedustella Huoltovarmuuskeskuksesta. Erityisesti KYBER-TEO-hankkeemme tukee vahvasti myös kansallista kyberturvallisuusstrategiaa, katso: www.yhteiskunnanturvallisuus.fi

Tärkeimmät lähteet:

[AUTOMAATIO]

Suomen Automaatioseuran julkaisema ”Teollisuusautomaation tietoturva - verkottumisen riskit ja niiden hallinta”: https://www.viestintavirasto.fi/attachments/tietoturva/TeollisuusautomaationTietoturva.pdf

[HUOVI]

HUOVI-portaali tukee huoltovarmuuskriittisiä toimijoita vakaviin häiriöihin varautumisessa: www.huoltovarmuus.fi/huovi

HUOVI-portaalista Teollisuuden tietoturvan työpajat -hankealueelta löytyvät omista hakemistoistaan TEO-TT, COREQ-VE, COREQ-ACT ja KYBER-TEO-projektien huoltovarmuuskriittisille yrityksille tarkoitetut tulokset

[KOOSTE]

Huoltovarmuuskeskus ja VTT: Tietoturvaa huoltovarmuuskriittisille yrityksille – Kooste automaatiota hyödyntävälle teollisuudelle suunnattujen tietoturvaprojektien tuloksista. Tämän julkaisun lopussa on esitetty pidempi lista standardeja ja referenssejä. http://www.huoltovarmuus.fi/static/pdf/723.pdf

[TITAN]

TITAN-käsikirja. VTT TIEDOTTEITA – RESEARCH NOTES 2545. VTT:n päätuloksia Tekesin Turvallisuusohjelman TITAN-projektissa: http://www.vtt.fi/inf/pdf/tiedotteet/2010/T2545.pdf

Teollisuuden käyttöön soveltuvia kansainvälisiä tietoturvastandardeja ja kotimaisia malleja on nyt saatavilla, niitä pitää vain osata hyödyntää ja soveltaa oikein. Mm. teollisuuden tuotanto- ja tietojärjestelmien räätälöidyistä sovelluksista ja niiden moninaisuudesta johtuen tietoturvamenetelmien soveltaminen saattaa joskus olla vaikeaa ja/tai työlästä. Niinpä eri ratkaisuja tulisikin etukäteen arvioida ja myös testata eri menetelmien soveltuvuutta käytännössä ennen lopullista valintaa ja käyttöönottoa. Tähän arviointiin tai testaamiseen tarvitaan usein tukea myös tuotantoyrityksen ulkopuolelta.

Yhteistyön merkitys korostuu tänä päivänä tietoturvallisuuden ylläpidossa kaikilla sektoreilla, ei ainoastaan teollisuudessa. Toimivaa yhteistyötä ja pelisääntöjä tarvitaan mm. hankintojen tietoturvan hallinnan yhteyteen, mutta myös laajemmin koko tuotannon tietoturvatason ylläpidon ja seurannan osalta. Erityisesti tietoverkkojen seurannan tarve on tänä päivänä korostunut, taustalla on mm. teollisuusvakoilu ja jopa tiedustelupalvelujen pitkälle kehittynyt urkinta.

Teollisuudelle tarjottujen tietoturvan ja jatkuvuuden varmistamisen palvelujen laajuus, räätälöinti ja osumistarkkuus tulee saada entistä paremmaksi. Myös huoltovarmuuskriittisen tuotannon ja toiminnan tulee ainakin osin täyttää kilpailukyvyn asettamat vaatimukset, jotka usein edellyttävät lisääntyvää integraatiota sekä julkisissa verkoissa olevien tietojen ja tietopalvelujen käyttöä. Tämä kehitys kuitenkin monimutkaistaa järjestelmiä ja tuo lisää hallittavia ja valvottavia ulkoisia tietovirtoja, joista osa voi olla myös kriittisiä. Silti nämäkin tietovirrat täytyy saada parempaan hallintaan.

HUOLTOVARMUUSKESKUS
FÖRSÖRJNINGSBEREDSKAPSCENTRALEN
NATIONAL EMERGENCY SUPPLY AGENCY